Akademia Sztuki Wojennej

Cybersecurity and Law

Nr 2(2) 2019

Warszawa 2019

ISSN 2658-1493

Adres redakcji

Akademia Sztuki Wojennej w Warszawie
Centrum Badań nad Bezpieczeństwem
Ośrodek Centrum Studiów nad Cyberbezpieczeństwem
al. gen. A. Chruściela „Montera" 103
00-910 Warszawa
e-mail: cyber.law@akademia.mil.pl

Skład, druk i oprawa: Wydawnictwo Akademii Sztuki Wojennej, zam. nr 349/20, nakład 100 egz.

Spis treści

Szanowni Państwo,

współczesne platformy internetowe pełnią centralną rolę w zapewnieniu bezpiecznego środowiska internetowego, ochronie użytkowników przed dezinformacją i umożliwianiu użytkownikom styczności z różnymi poglądami i ideami. W ostatnim czasie coraz bardziej przekonywujące staje się stanowisko, iż samoregulacja może przyczynić się do osiągnięcia tego celu, pod warunkiem że będzie skutecznie wdrażana, dostosowywana do rozwoju techniki i monitorowana. Podobnie w odniesieniu do współregulacji, która za każdym razem wymaga koordynacji i kompromisu, co w obszarze cyberbezpieczeństwa znacznie utrudnia działanie tak w aspekcie czasowym, jak i proceduralnym. Celem zasadniczym regulatorów staje się znaczna poprawa kontroli umieszczanych treści. Współczesne regulacje powinny być uzupełnione przez obowiązkowe repozytoria zawierające wyczerpujące informacje na temat sponsorowanych treści, takie jak dane identyfikacyjne rozpowszechniającego, charakter informacji, np. czy jest to przekaz reklamowy czy zawiera fake news, podobnie zresztą kiedy wdrażano regulacje dotyczące lokowania produktu w przekazie audiowizualnym. Możemy zastanawiać się dlaczego dana informacja jest skierowana do nas. Na czym polega zindywidualizowanie danego przekazu i z jakim zagrożeniem taka identyfikacja się wiąże. Tu pojawia się potrzeba ułatwienia użytkownikom oceny treści poprzez wskaźniki wiarygodności źródeł treści, oparte na obiektywnych kryteriach, z zasadą przejrzystości w zakresie własności mediów i zasadą zweryfikowanej tożsamości. Zatem kluczowe będzie zintensyfikowanie i wykazanie skuteczności działań na rzecz zamykania fałszywych kont. Zapewnienie cyberbezpieczeństwa powinno obejmować dodatkowe obowiązki informacyjne. Przekazywanie użytkownikowi szczegółowych informacji na temat sposobu działania algorytmów, które sprawiają, że niektóre informacje są wyświetlane w pierwszej kolejności, a także opracowanie metodyki testów, zapewnienia wiarygodnym organizacjom weryfikującym fakty oraz środowisku akademickiemu dostępu do danych będących

w posiadaniu platform (w szczególności poprzez interfejsy programowania aplikacji), z zachowaniem zasad prywatności, tajemnicy handlowej i własności intelektualnej to dopiero planowany początek wielkiej zmiany w regulacjach prawnych.

Wciąż jednak kluczowe będzie wspieranie odpowiedzialności w internecie, które ma następować poprzez zapewnienie identyfikowalności w całym procesie rozpowszechniania treści i świadczenia e-usług. Dobrowolne systemy internetowe umożliwiające identyfikację dostawców informacji w oparciu o wiarygodne elektroniczne środki identyfikacji i uwierzytelniania, w tym zweryfikowane pseudonimy, zgodnie z rozporządzeniem w sprawie identyfikacji elektronicznej to klucz do zmiany w myśleniu o e-usługach, także usługach administracji publicznej. Podobne działania przyczyniłyby się również do ograniczenia cyberataków, które często są połączone z kampaniami dezinformacyjnymi w ramach zagrożeń hybrydowych.

Zasygnalizowane zmiany będą wymagały wstępnych badań i analiz. Próbę niezbędnej weryfikacji i diagnozy podjęli autorzy niniejszego zeszytu, w którym prezentujemy jak zwykle tematy i cyber, i szeroko pojmowanego prawa bezpieczeństwa.

Życzymy dobrej lektury!

Redakcja

Katarzyna Chałubińska-Jentkiewicz*

Cyberbezpieczeństwo – zagadnienia definicyjne

Streszczenie

W obecnych warunkach prawnych podejście regulatorów do zagadnienia cyberbezpieczeństwa wynika z utożsamiania tego rodzaju zjawiska z potrzebą przeciwdziałania atakom przede wszystkim nakierowanym na sieci teleinformatyczne. Stanowisko takie wydaje się jednak nieuzasadnione, zwłaszcza w kontekście analizy pojęcia cyberprzestrzeni i zagrożeń z nią związanych. Cyberbezpieczeństwo jest pojęciem odnoszącym się do zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Na rzecz tego stanowiska przemawia również charakterystyka pojęcia cyberprzestępczości, obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni. Jednak powszechnie przyjmuje się, że świat cyfrowy powinien być uregulowany tak jak świat rzeczywisty. W artykule podjęto próbę uzasadnienia wskazanego powyżej stanowiska.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, informacja, inwigilacja, terroryzm

* Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

Pojęcie cyberprzestrzeni

Współczesny świat opiera się na wymianie informacji, komunikacji interpersonalnej i indywidualizacji przekazu. Informacja zyskała całkiem nowe znaczenie, stała się ważnym czynnikiem w obiegu cyfrowym. Dotarcie do źródeł wiedzy stało się prostsze. Taki stan rzeczy doprowadził do wyodrębnienia się nowych pojęć w obszarze prawnym takich jak sieć teleinformatyczna oraz cyberprzestrzeń. Za autora tego pojęcia uznaje się Wiliama Gibsona. W swojej powieści zatytułowanej „Neuroromancer" napisał „To jest cyberprzestrzeń, konsensualna, halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność"[1]. Sieć teleinformatyczną można określić przez syntezę dwóch pojęć legalnych zawartych w polskim ustawodawstwie, są to: system teleinformatyczny i sieć telekomunikacyjna. Definicję systemu teleinformatycznego określa ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[2]. Według tej definicji system teleinformatyczny to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla tego rodzaju sieci telekomunikacyjnego urządzenia końcowego", natomiast pojęcie sieć telekomunikacyjna zostało zdefiniowane w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[3]. W myśl tej ustawy przez sieć telekomunikacyjną rozumiemy „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju"[4]. Można zatem powiedzieć, że sieć teleinformatyczna to wszelkiego rodzaju oprogramowanie, obsługiwane przez urządzenia posiadające do niego dostęp, które umożliwiają tworzenie, wymianę danych oraz informacji.

1 W. Gibson, *Neuromancer*, Warszawa 2009.
2 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204 ze zm.).
3 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2014 r., poz. 243 ze zm.), dalej pr.tel.
4 Art. 2 pr.tel.

Natomiast jedną z powszechnie stosowanych definicji cyberprzestrzeni jest ta sformułowana przez Departament Obrony USA. Według tej definicji cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesy oraz kontrolery”[5]. Definicja ta pozbawiona jest czynnika ludzkiego i skupia się wyłącznie na aspektach technicznych i technologicznych. Polska definicja pojęcia cyberprzestrzeni znajduje się w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[6]. Kolejną definicję legalną pojęcia cyberprzestrzeni zawiera ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym[7]. Według powyższej ustawy przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[8], wraz z powiązaniami pomiędzy nimi, oraz relacjami z użytkownikami[9]. Taką samą definicję legalną zawiera ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[10]. Ustawy te odnoszą się do zachowań w płaszczyźnie wirtualnej, w jakiej poruszają się podmioty prawa w momencie wystąpienia jednego z trzech stanów nadzwyczajnych. Przyjęta w Założeniach Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej koncepcja krajowego systemu cyberbezpieczeństwa obejmuje m.in. przebudowanie definicji cyberprzestrzeni i jej rozciągnięcie na sferę kluczowych operatorów funkcjonujących w sferze gospodarczej.

Przy tworzeniu wskazanej powyżej strategii przyjęto, iż dotychczasowa definicja cyberprzestrzeni jest ograniczona do sektora publicznego. Jednak wskazana powyżej definicja odnosi się do systemów teleinformatycznych,

5 *Słownik terminów wojskowych oraz powiązanych*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf tłumaczenie za: J. Wasielewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9, s. 225.

6 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

7 Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).

8 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

9 Art. 2 ust. 1a ustawy o stanie wyjątkowym.

10 Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

które jak już wskazano stanowią zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Zatem definicja ta dotyczy wszystkich sytuacji odnoszących się do przetwarzania danych za pomocą systemów, a dodatkowo stanowi obszar powiązań systemów oraz relacji z użytkownikami, co wskazuje na szeroki zakres działania wszystkich użytkowników sieci i samych sieci. Oczywiście ustawodawca odniósł się do definicji samego systemu, przyjmując tę definicję za generalną.

Należy tu zauważyć, że definicja systemu teleinformatycznego na gruncie przepisów ustawy o świadczeniu usług drogą elektroniczną jest tożsama z definicją przyjętą w ustawie o informatyzacji[11], która reguluje kwestie stosunków cywilnoprawnych w handlu elektronicznym. Projektodawca założeń proponuje, aby definicja została wprowadzona do ustawy o krajowym systemie cyberbezpieczeństwa bądź ustawy o świadczeniu usług drogą elektroniczną, jednak równie właściwym miejscem byłaby przede wszystkim ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[12], gdzie w art. 3 ust. 2 zdefiniowano infrastrukturę krytyczną, przez którą należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna pojęciowo obejmuje także systemy sieci teleinformatycznych.

Można powiedzieć, że ład prawny i porządek publiczny przenikają do świata wirtualnego, i próbują znaleźć tam swoje odzwierciedlenie w formule cyfrowej. Pojęcie cyberprzestrzeni można bowiem sformułować jako syntezę wszystkich fizycznych i technicznych środków pozwalających na wymianę cyfrową drogą elektroniczną, oraz relacji użytkowników posiadających dostęp do jej zasobów. Całość tych zjawisk dzieje się w równoległej przestrzeni, która stanowi nowe pole dla ludzkich działań, na którą są przenoszone zachowania

11 System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu pr.tel.

12 Dz.U. z 2013 r., poz. 1166.

i rozwiązania stosowane w świecie realnym. Prawodawcy z różnych szczebli – zarówno międzynarodowego, jak i krajowego wprowadzają nowe regulacje. Doprowadziło to do dezaktualizacji zjawiska, jakim była bezkarność nielegalnego działania w sieci. Jednak podkreślić trzeba, iż cyberprzestrzeń pod względem przyjmowania czy tworzenia wzorców jest bardziej elastyczna niż rzeczywistość. Jej podatność niesie ze sobą udogodnienia, jak i zupełne wyzwania dla regulatora. Udogodnieniem jest łatwość wprowadzania regulacji adekwatnie do tych obowiązujących w świecie rzeczywistym, jednak przepisy tak ustalone często spotykają się z blokowaniem lub zwyczajną ignorancją ze strony użytkowników sieci teleinformatycznej, w szczególności ze względu na brak instrumentów dochodzenia roszczeń czy ścigania przestępczości. Każde społeczeństwo jest świadome możliwych zagrożeń, co powiązane jest z szeregiem doświadczeń i obserwacji, podczas gdy, w przypadku cyberprzestrzeni, która jest obszarem stosunkowo nowym wciąż nie jest możliwe określenie zamkniętego katalogu zagrożeń ani skonkretyzowanie grupy osób zagrożonych. Te zjawiska stanowią konsekwencję funkcjonowania w tzw. społeczeństwie informacyjnym. M. Castells przyjmuje, że jedną z ważniejszych cech społeczeństwa informacyjnego jest „nacisk na spersonalizowane urządzenia, interaktywność, sieciowość i bezustanne poszukiwanie nowych rozwiązań technologicznych[13]". Natomiast według J. Oleńskiego „Podstawowe cechy społeczeństwa informacyjnego, to m.in. globalny i totalny zakres procesów i systemów informacyjnych oraz możliwości globalnego i totalnego oddziaływania na społeczeństwa i gospodarki przez informacje"[14]. Przez obecność społeczeństwa informacyjnego w sieci teleinformatycznej zachodzi tzw. zjawisko transparentności jednostki, co oznacza, że przez wymianę informacji można bezproblemowo prześledzić aktywność konkretnej jednostki, co wzmaga jej podatność na zjawisko, jakim jest cyberprzestępczość[15]. Cyberprzestrzeń (cyberspace) już samą nazwą jest związana z cybernetyką tj. nauką o procesach sterowania oraz przekazywania i przekształcania informacji w systemach (maszynach, organizmach żywych i społeczeństwach)[16]. Analiza cech tej cybernetycznej przestrzeni prowadzi do wniosku, że jest to swoisty technosystem globalnej komunikacji społecznej,

13 M. Castells, *Społeczeństwo sieci*, Warszawa 2008, s. 23.
14 J. Oleński, *Ekonomika informacji*, Warszawa 2003, s. 33.
15 J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek (red.), *Demokracja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008, s. 52–79; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213.
16 J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.

który odznacza się interaktywnością i multimedialnością. Został on ukształtowany w wyniku trzech procesów: integracji form przekazu i prezentacji informacji, która przyniosła ucyfrowienie i powstanie tzw. infosfery, konwergencji systemów informatycznych i telekomunikacyjnych oraz mediów elektronicznych, integracji tzw. technosfery, która doprowadziła w rezultacie do powstania globalnej zintegrowanej platformy teleinformatycznej[17]. Cyberprzestrzeń stanowi zatem swego rodzaju przestrzeń komunikacyjną tworzoną przez system powiązań internetowych. Jest obszarem zarówno kooperacji pozytywnej, prowadzącej do rozwoju w sferze edukacji, komunikacji społecznej, gospodarki narodowej, bezpieczeństwa powszechnego itp., jak i zjawisk negatywnych. Ta ostatnia aktywność może przybierać różną postać: 1) cyberinwigilacji (obostrzonej kontroli społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach autorytarnych i totalitarnych); 2) cyberprzestępczości (wykorzystania cyberprzestrzeni do celów kryminalnych, w szczególności w ramach przestępczości zorganizowanej i przestępczości o charakterze ekonomicznym); 3) cyberterroryzmu (wykorzystania cyberprzestrzeni w działaniach terrorystycznych); 4) cyberwojny (użycia cyberprzestrzeni jako czwartego, obok ziemi, morza i powietrza, wymiaru prowadzenia działań wojennych[18].

Definicja cyberbezpieczeństwa

Jedna z definicji bezpieczeństwa przyjmuje, że „bezpieczeństwo jest pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzny w stosunku do jednostki, grupy społecznej, zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa[19]". Natomiast w ujęciu potocznym bezpieczeństwo m.in. oznacza stan, w którym jednostka ma poczucie pewności w sprawnie działającym systemie prawnym. Przeciwieństwem bezpieczeństwa jest stan zagrożenia. Bezpieczeństwa nie powinno się traktować jako zmiennej niezależnej,

17 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
18 Ibidem.
19 H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004, s. 9–11.

gdyż ma ono charakter: dynamiczny i procesualny – ulega ciągłym zmianom pod wpływem złożonych i wieloczynnikowych zjawisk; subiektywny i obiektywny. Wynika to z faktu, iż postawy społeczne wobec bezpieczeństwa tworzą się wskutek wpływu danego zjawiska na jednostkę, grupę społeczną, społeczeństwo; uszeregowany, strukturalizowany; relatywny – zależny od szeregu czynników[20]. Wpływ na bezpieczeństwo mają wszystkie interakcje społeczne, a sama kultura bezpieczeństwa określa jaki jest stosunek danej społeczności do ryzyka, zagrożeń i bezpieczeństwa oraz ,jakie wartości w tym zakresie uważane są za istotne.

W przypadku zachowań związanych z funkcjonowaniem cyberprzestrzeni, również ze względu na jej globalny charakter taka zależność wydaje się nieoczywista. Bowiem działania w przestrzeni wirtualnej cechuje własna, specyficzna kultura zachowań jej użytkowników – społeczności wirtualnej. Dlatego należy przyjąć, że nowe zjawisko, jakim jest bezpieczeństwo wymagane w kontekście funkcjonowania sieci teleinformatycznych stwarza potrzebę uwzględnienia sytuacji, które nie muszą mieć odzwierciedlenia w świecie poza cyberprzestrzenią. Samo ustalone już pojęcie cyberbezpieczeństwa odnosić się może do ściśle określonego obszaru działań związanych z bezpieczeństwem informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu) oraz bezpieczeństwem samej sieci umożliwiających komunikowanie, jednak nie wyczerpuje wszystkich kwestii związanych z potrzebami ochrony przed niepożądanymi działaniami w cyberprzestrzeni.

Podstawowa konstrukcja internetu opiera się na otwartości zarówno architektury jego infrastruktury, jak i kultury jego twórców i użytkowników. Prostota i łatwość łączenia różnych komputerów pozwoliła na ogromne rozszerzenie liczby użytkowników, a otwarta filozofia jego kształtowania stworzyła z niego ogromnie atrakcyjne, interakcyjne na wielu poziomach medium[21]. Dlatego definicja cyberbezpieczeństwa wymaga uwzględnienia wielu zjawisk już zdefiniowanych. Takimi pojęciami pomocniczymi w definiowaniu cyberbezpieczeństwa są: bezpieczeństwo informacyjne, cyberprzestępczość.

20 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000, s. 166.
21 T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

Bezpieczeństwo informacyjne w systemie cyberbezpieczeństwa

Bezpieczeństwem informacyjnym lub informacji możemy nazwać, według L. Ciborowskiego „obronę informacyjną, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych[22]". Kolejna definicja bezpieczeństwa informacyjnego M. Jabłońskiego i M. Mielus, została skonstruowana poprzez przedsięwzięcia, jakie należy zastosować, aby uzyskać stan bezpieczeństwa i składają się na nie: zapobieganie, odstraszanie, wskazywanie i ostrzeganie, wykrywanie, przygotowanie na sytuację awaryjną oraz reakcja na ewentualny atak[23]. Z kolei według M. Kaliskiego, A. Kierkowskiej oraz G. Tomaszewskiego „Bezpieczeństwo informacji to nie tylko zabezpieczenia fizyczne i techniczne zasobów informatycznych. Bezpieczeństwo informacji to przede wszystkim dążenie do zapewnienia i utrzymania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności informacji i systemów, w których są one przetwarzane. To także odpowiednio przeszkolony i świadomy zagrożeń personel, to odpowiednio zdefiniowane umowy z dostawcami, to również sformalizowane plany ciągłego działania i procedury postępowania. Bezpieczeństwo to proces – i jak każdy proces – wymaga ciągłego doskonalenia[24]". Bezpieczeństwem informacyjnym jest również każde działanie, system lub metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych[25]. Obok pojęcia bezpieczeństwa informacyjnego wykształciło się pojęcie cyberbezpieczeństwa, które można zdefiniować jako wszelkie działania – metody, procedury, rozwiązania prawne – podejmowane przez właściwe w tym względzie podmioty, które to zmierzają do integralności zgromadzonych, przechowywanych i przetwarzanych

22 L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 186.
23 M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] M. Kwieciński (red.), *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, Kraków 2010, s. 25.
24 M. Kaliski, A. Kierkowska, G. Tomaszewski, *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 34.
25 Ibidem, s. 71.

zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[26]. Jednak, wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się do wielu innych zagrożeń, które nie muszą być związane bezpośrednio z jakimkolwiek nielegalnym wykorzystaniem informacji a mogą dotyczyć działań przestępczych wykorzystujących narzędzia informatyczne lub samą informację. Sytuacja taka może dotyczyć obrotu towarami zakazanymi, pornografii dziecięcej czy wyłudzania pieniędzy. Zatem, w pierwszej kolejności należy ustalić czym jest cyberprzestępczość i jakich sytuacji dotyczy.

Cyberprzestępczość

Ze względu na szczególny charakter tej sfery funkcjonowania społecznego wykształcił się nowy katalog czynów zabronionych określany pojęciem cyberprzestępczości[27]. Cyberprzestępczość definiowana jest jako rodzaj przestępczości, w której komputer jest albo narzędziem albo przedmiotem przestępstwa. Pojęcie to obejmuje wszelkie rodzaje przestępstw, które popełniono przy pomocy komputera lub sieci teleinformatycznych. Cyberprzestępstwo to czyn zabroniony popełniony w obszarze cyberprzestrzeni. Cyberatak jest to celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu. Sam atak na sieci informatyczne to działania podejmowane w celu zniekształcenia, uniemożliwienia wykorzystania, degradacji lub zniszczenia informacji przechowywanej w komputerze i/lub sieci komputerowej, albo komputera i/lub sieci komputerowej[28]. Pojęcie cyberprzestępczości, zwanej również „przestępczością internetową" jako określenie zabronionych prawem działań, dokonywanych za pomocą komputera w sieci internetowej lub przy jej wykorzystaniu, godzących m.in. w bezpieczeństwo wykorzystania technologii informatycznych, znalazło już swoje miejsce zarówno w doktrynie

26 P. Potejko, *Bezpieczeństwo informacyjne* [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009, s. 194.
27 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 351.
28 *Słownik terminów i definicji NATO*, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf, s. 105.

nauk prawnych, jak i wśród ekspertów zajmujących się bezpieczeństwem teleinformatycznym[29]. Można przyjąć, że cyberprzestępczość obejmuje trzy kategorie przestępstw: tradycyjne przestępstwa popełniane z wykorzystaniem sieci i systemów informatycznych, publikację nielegalnych treści w mediach elektronicznych, inne przestępstwa typowe dla sieci łączności elektronicznej. Dotychczas zidentyfikowano wiele ich postaci, a wśród nich[30]: 1) usługi finansowe on-line (m.in. propozycje udziału w wirtualnym hazardzie, tzw. oszustwa nigeryjskie); 2) cyberlaundering, tzn. wykorzystanie bankowości i handlu elektronicznego do tzw. „prania brudnych pieniędzy"; 3) naruszanie praw autorskich; 4) rozpowszechnianie pornografii i pedofilii; 5) praktyki nieuczciwej konkurencji (np. spamming); 6) nielegalny handel (np. antykami i dziełami sztuki, zagrożonymi gatunkami roślin i zwierząt, medykamentami, bronią, materiałami wybuchowymi, materiałami radioaktywnymi, wraz z instruktażem ich użytkowania); 7) szpiegostwo gospodarcze; 8) propagowanie treści nazistowskich, rasistowskich, itp.; 9) hacking – włamania do komputera; 10) nielegalne podsłuchy; 11) cybersquatting.

Niektóre czyny związane z cyberprzestępczością są odzwierciedleniem przestępstw i wykroczeń mających miejsce w świecie realnym, ale zostały odpowiednio zaadaptowane do warunków, jakie oferuje sieć teleinformatyczna[31]. Jednak zauważyć należy, że cyberprzestępczość nie musi być symptomem działania jednostki wyłącznie w sieci, bowiem jednostka może być narażona na zagrożenie w konsekwencji ataku na sieci teleinformatyczne. Zarówno sektor prywatny, jak i coraz bardziej obecne w sieci państwo i władza publiczna mogą stać się potencjalnymi ofiarami cyberprzestępczości. Państwo musi utrzymać tempo dynamicznej zmiany, podyktowanej rozwojem nowych technologii, ponieważ w ten sposób może ono realizować swoje zadania względem rozwoju gospodarczego i roli służebnej wobec obywatela[32]. Potrzeba informatyzacji, otwartość zasobów i dostęp do sieci i przetwarzanych przez nią danych i informacji to kluczowe procesy umożliwiające rozwój państwa i samej jednostki. Jednocześnie istotnym zadaniem władz publicznych jest zapewnienie bezpieczeństwa w sieci oraz tzw. cyberbezpieczeństwa, czyli sytuacji skutecznie wypierającej cyberprzestępczość.

29 M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary. Automatyka. Kontrola" 2009, nr 7.
30 W. Filipkowski, *Internet – przestępcza gałąź gospodarki*, „Prokurator" 2007, nr 1.
31 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo…*, s. 351–352.
32 S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994, s. 16.

Cyberinwigilacja

Kolejnym pojęciem, które wpływa na definicję cyberbezpieczeństwa jest cyberinwigilacja. Jest to również zjawisko pokrewne cyberterroryzmowi. Za jedną z postaci terroryzmu uznawany jest bowiem terroryzm państwowy, którego istotą, a zarazem celem działań terrorystycznych, jest wymuszenie posłuszeństwa wobec aparatu władzy[33]. Jest oczywiste, że proceder taki nie jest możliwy bez inwigilacji społeczeństwa, w szczególności członków opozycji niedemokratycznego reżimu. Obecnie, cyberprzestrzeń i elektroniczne środki komunikacji to instrument działań aparatu bezpieczeństwa. Może on przyjąć zarówno formę ograniczenia obywatelom dostępu do internetu i jego zawartości (np. spowolnienie sieci, brak dostępu do wyszukiwarek oraz stron światowych, cenzura stron internetowych, profilowanie), jak i stosowania środków teleinformatycznych w procesie inwigilacji masowej (np. podsłuchy, inwigilacja zachowań w sieciach telekomunikacyjnych). Obie techniki stanowią obecnie doskonałe narzędzie kontroli społeczeństwa lub jednostki. Początkowo wykorzystywane do działań marketingowych, dzisiaj stanowią źródło zagrożeń i stan niepewności funkcjonowania w cyberprzestrzeni. W konsekwencji cyberbezpieczeństwo będzie sytuacją, w której zarówno jednostka, jak i całe społeczeństwo i poszczególne jego grupy będą wolne od cyberinwigilacji.

Cyberterroryzm

Cyberterroryzm to zagrożenie szczególne cywilizacji, społeczeństwa informacyjnego, bezpieczeństwa narodowego i obywateli, wymaga przeciwdziałania i zdecydowanego zwalczania. Współczesny terroryzm odznacza się trzema charakterystycznymi cechami[34]. Po pierwsze, akty terrorystyczne są przeprowadzane w sposób umożliwiający uzyskanie przez nie międzynarodowego rozgłosu. Po drugie, cechuje je wysoki stopień zorganizowania grup terrorystycznych. Po trzecie wreszcie, organizacje terrorystyczne dysponują obecnie pokaźnym zasobem środków ekonomicznych i technicznych, wykorzystując na masową skalę narzędzia teleinformatyczne, w tym internet, do działań skierowanych przeciwko społeczeństwu oraz aparatowi państwowemu wrogich

33 K. Sławik, *Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne*, Poznań 1993, s. 114–130.
34 Ibidem.

krajów. Zdaniem amerykańskiego eksperta do spraw cyberbezpieczeństwa D.E. Denninga, „Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody aby wywoływac poczucie strachu[35]". Zjawisko to jest przy tym obecnie najmniej przewidywalne, m.in. z uwagi na powszechne zastosowanie sieci teleinformatycznej będącej instrumentem oddziaływania zorganizowanych grup terrorystycznych na funkcjonowanie infrastruktury krytycznej państwa, a więc krajowych systemów cyberbezpieczeństwa: łączności, energetyki, transportu, zaopatrzenia w wodę, finansowych, itd. Metody korzystania przez zorganizowane grupy przestępcze i indywidualnych przestępców w działaniach cyberterrorystycznych to m.in. włamania do komputerów (hacking), włamania do systemów informatycznych dla osiągnięcia korzyści (cracking), wykorzystanie programu umożliwiającego wejście do serwera z pominięciem zabezpieczeń (back door), podsłuchiwanie pakietów między komputerami i przechwytywanie haseł i loginów (sniffing), podszycie się pod inny komputer (IP spoofing), wirusy i robaki komputerowe, bomby logiczne, wyłudzanie poufnych informacji (phishing)[36]. teleinformatycznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni. Jest oczywiste, że ze względu na szczególną szkodliwość społeczną cyberterroryzmu i zagrożenie, jakie stwarza dla współczesnego świata, spotyka się z wyraźną reakcją prawnokarną zarówno na gruncie prawa międzynarodowego, jak i ustawodawstwa krajowego. Zgodnie z art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[37] zdarzeniem o charakterze terrorystycznym jest sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[38], lub zagrożenie zaistnienia takiego przestępstwa. Zgodnie z § 20 przestępstwem

35 J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.

36 J. Szafrański, *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.

37 Dz.U. z 2016 r., poz. 796.

38 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2019 r., poz. 1950 ze zm.).

o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób; 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu. Istotną grupę stanowią przestępstwa komputerowe, których podstawa prawna może stanowić podstawę odpowiedzialności za działania cyberterrorystyczne. W szczególności trzeba tutaj zwrócić uwagę na przestępstwa udaremniania lub znacznego utrudniania dostępu do informacji zapisanej na komputerowym nośniku informacji osobie do tego uprawnionej (sprawca podlega pozbawienia wolności do lat 3), oraz sabotażu komputerowego. W Kodeksie karnym został określony również typ przestępstwa polegającego na niszczeniu, uszkadzaniu, usunięciu lub bezprawnej zmianie zapisu istotnej informacji na komputerowym nośniku informacji, którym jest materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej[39]. W przypadku sabotażu komputerowego, przedmiotem ochrony prawnokarnej jest informacja, która jest dobrem szczególnie ważnym w dobie społeczeństwa informacyjnego. Za taki czyn należy uznać znaczenie powszechnej informacji dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej lub innego organu państwowego, która musi mieć wymiar szczególny, a dotyczyć może: rozmieszczenia elementów infrastruktury obronnej państwa, systemów kierowania komunikacją kolejową, lotniczą, drogową i wodną. Czyn ten polega na niszczeniu, uszkadzaniu, usuwaniu lub zmianach zapisu informacji. Zatem w znaczeniu ścisłym pojęciem cyberterroryzmu należy określić działalność terrorystyczną prowadzoną wobec systemów teleinformatycznych, w celu zniszczenia lub modyfikacji zasobów informacyjnych znajdujących się w tych systemach, a w konsekwencji utraty życia, zdrowia lub mienia przez ofiary ataku terrorystycznego. Cyberterroryzm może też mieć miejsce w przypadku wykorzystywania cyberprzestrzeni i sieci teleinformatycznej do działań o charakterze terrorystycznym. W ujęciu szerokim natomiast, trzeba go utożsamiać z wszelkimi działaniami względem cyberprzestrzeni, w tym

39 M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1–2, s. 45.

również fizycznymi zamachami na infrastrukturę teleinformatyczną oraz aktywnością ideologiczną w internecie[40]. W konsekwencji zapewnieniem cyberbezpieczeństwa będzie ochrona cyberprzestrzeni, czyli zespół przedsięwzięć organizacyjno-prawnych, mający na celu zwalczanie cyberterroryzmu.

Zakończenie

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[41] cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Jednak na pojęcie bezpieczeństwa w sieci czy cyberbezpieczeństwa składa się ochrona zasobów – danych, informacji, a ogólnie treści cyfrowych, ochrona sieci teleinformatycznych, urządzeń czyli komputerów, a także ochrona przesyłu treści za pomocą sieci, a więc samego procesu komunikowania. Należy dodać tu jeszcze czynnik ludzki, czyli ochronę użytkownika sieci i komputerów. Wciąż kluczem do działań stwarzających wszelkiego typu zagrożenia w cyberprzestrzeni jest kwestia wykorzystywania luk i błędów w narzędziach programistycznych. Z całą pewnością należy podkreślić, że istotnym elementem tego procesu wciąż pozostaje działanie człowieka. Prawo bezpieczeństwa informacyjnego dotyka zagadnień związanych z prawną ochroną systemu telekomunikacyjnego, który zawiera określone dane umożliwiające świadczenie usług, ochroną samych usług świadczonych drogą elektroniczną i związanych z nimi treści oraz baz danych, a także samych sieci, za pomocą których następuje przekaz takich usług[42]. Jednak elementem wspólnym podlegającym ochronie jest wartość o szczególnym charakterze – informacja. W przepisach prawnych ustawodawca podjął próbę zdefiniowania czynów przestępczych, gdzie dochodzi do naruszeń związanych z informacją i systemami, które te informacje przetwarzają, a także ustalenia zakresu odpowiedzialności za działania nielegalne. Jednak obok pojęcia bezpieczeństwa informacyjnego wykształciło się pojęcie cyberbezpieczeństwa, które można

40 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
41 Dz.U. z 2018 r., poz. 1560.
42 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, s. 5.

zdefiniować jako wszelkie działania – metody, procedury, rozwiązania prawne – podejmowane przez właściwe w tym względzie podmioty, które zmierzają do integralności zgromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[43]. Wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się do wielu innych zagrożeń, które nie muszą być związane bezpośrednio z jakimkolwiek nielegalnym wykorzystaniem cyberprzestrzeni a mogą dotyczyć działań przestępczych wykorzystujących narzędzia informatyczne – oprogramowania, komputery lub samą informację. Podobnie jak wskazana powyżej definicja cyberbezpieczeństwa przyjmująca je za odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy, która odnosi się do bezpieczeństwa sieci teleinformatycznej i usług świadczonych za ich pomocą (art. 2 pkt 4 ustawy o krajowym systemie). Cyberbezpieczeństwo jest pojęciem odnoszącym się do stanu zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają samej cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni, a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Natomiast na rzecz tego stanowiska przemawia charakterystyka pojęcia samej cyberprzestępczości, cyberinwigilacji i cyberterroryzmu jako pojęcia obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni[44].

Bibliografia

Literatura

Castells M., *Społeczeństwo sieci*, Warszawa 2008.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Ciborowski L., *Walka informacyjna*, Toruń 1999.

Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary. Automatyka. Kontrola" 2009, nr 7.

43 P. Potejko, *Bezpieczeństwo*..., s. 194.

44 Zaznaczyć także trzeba, że jednym z wciąż podstawowych problemów dotyczących odpowiedzialności w sieci jest zagadnienie jurysdykcji terytorialnej, która znalazła zastosowanie w przepisach Konwencji o cyberprzestępczości. Problemy z ustaleniem osoby przestępcy a jak wiadomo większość przestępstw popełnianych jest w innych państwach niż faktyczne miejsce przebywania przestępcy utrudnia działania związane z efektywnością ścigania cyberprzestępczości.

Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1–2.
Dworecki S., *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994.
Filipkowski W., *Internet – przestępcza gałąź gospodarki*, „Prokurator" 2007, nr 1.
Gibson W., *Neuromancer*, Warszawa 2009.
Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.
Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] M. Kwieciński (red.), *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, Kraków 2010.
Kaliski M., Kierkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010.
Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.
Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004.
Oleński J., *Ekonomika informacji*, Warszawa 2003.
Potejko P., *Bezpieczeństwo informacyjne* [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009.
Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
Sławik K., *Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne*, Poznań 1993.
Sobczak J., *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007.
Sobczak J., *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek (red.), *Demokracja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008.
Szafrański J., *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000.
Wasielewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Akty prawne

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2014 r., poz. 243 ze zm.).
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).
Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204 ze zm.).
Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).
Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2019 r., poz. 1950 ze zm.).

Cyber security – definition issues

Abstract

In the current legal conditions, the regulators' approach to the issue of cybersecurity results from the identification of this type of phenomenon with the need to counteract attacks primarily targeted at IT networks. This position, however, seems unfounded, especially in the context of analyzing the concept of cyberspace and the threats associated with it. Cybersecurity is a term referring to ensuring protection and counteracting threats that affect cyberspace, as well as functioning in cyberspace, and this applies to both the public and private sectors and their mutual relations. This position is also supported by the characteristics of the concept of cybercrime, which generally covers in its scope threats that appear in cyberspace. However, it is widely accepted that the digital world should be regulated just like the real world. The article attempts to justify the position indicated above.

Key words: cybersecurity, cyberspace, information, surveillance, terrorism

Paweł Zając*

Tajność głosowania a i-voting. Wątpliwości prawne związane z głosowaniem przez internet

Streszczenie

Przymiot tajności głosowania stanowi jeden z fundamentalnych kanonów prawa wyborczego. Gwarantuje on prawo do anonimizacji oddanego głosu co wiąże się z zerwaniem więzi pomiędzy wyborcą a oddanym przez niego głosem na etapie ustalania wyników wyborów. Jednak w wyniku postępującego procesu technologizacji życia społecznego mającego za cel ułatwienie jednostkom funkcjonowania w życiu publicznym objawiającego się m.in. w możliwości głosowania przez internet z dowolnego miejsca (i-voting), zasada ta zostaje marginalizowana. I-voting nie zapewnia bowiem realnej gwarancji zapewnienia zachowania tajności podczas procesu głosowania, jednak mimo to rozwiązanie to przyjęte zostało w kilku krajach. Niniejszy artykuł porusza kwestie wątpliwości natury prawnej związane z zastosowaniem i-votingu w polskim porządku prawnym.

Słowa kluczowe: internet, wybory, głosowanie, e-głosowanie, prawo wyborcze

* Dr Paweł Zając, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: p.zajac@akademia.mil.pl, ORCID: 0000-0002-2188-5720.

„Technologia ma uwodzicielską naturę.
Zakładamy, że postępy w tej dziedzinie
prowadzą zawsze do korzystnych
dla ludzi udogodnień.
Oszukujemy sami siebie"

Brian Patrick Herbert, *Diuna. Bitwa pod Corrinem*[1]

Wstęp

Znakiem naszych czasów jest powszechna technologizacja życia mająca na celu w swoim założeniu polepszenie sytuacji jednostek funkcjonujących w danym społeczeństwie. Jednym z jej aspektów jest wykorzystanie nowych technologii w życiu publicznym, poprzez tworzenie instrumentów zarówno technicznych, jak i prawnych, ułatwiających obywatelom realizację ich praw, w tym m.in. prawa do uczestnictwa w wyborze swoich przedstawicieli na najważniejsze stanowiska w państwie. W tym miejscu pojawia się jednak pytanie, czy komfort obywateli wynikający z możliwości oddania głosu za pośrednictwem sieci internet z dowolnego miejsca (tzw. *i-voting*) nie stoi w sprzeczności z ogólnymi ideami oraz podstawowymi zasadami prawa. Innymi słowy, czy pęd za nowymi rozwiązaniami technologicznymi, może stanowić przesłankę do zmiany uznanych i powszechnie akceptowalnych norm prawnych.

Celem niniejszego artykułu jest zwrócenie uwagi na zagrożenia, jakie niesie ze sobą *i-voting* w aspekcie prawnym. Nie odpowiada on wprost na kluczowe i newralgiczne pytania, a jedynie zarysowuje problematykę, w szczególności związaną z zachowaniem konstytucyjnej zasady tajności wyborów podczas przeprowadzania głosowania z wykorzystaniem internetu. Jak orzekł Europejski Trybunał Praw Człowieka, zasada tajności wraz z innymi przymiotami wyborczymi, stanowi europejskie dziedzictwo konstytucyjne oraz „podstawę każdego prawdziwego systemu demokratycznego"[2]. Dlatego też tak istotnym zagadnieniem jest przeanalizowanie, czy system *i-votingu* nie narusza podstawowych zasad demokratycznego państwa prawa. Artykuł zwraca również uwagę na inne wątpliwości prawne, jakie mogą powstać przy wprowadzeniu takiego rozwiązania do krajowego porządku prawnego.

1 B.P. Herbert, K.J. Anderson, *Diuna. Bitwa pod Corrinem*, Poznań 2009.

2 Zob. Wyrok Europejskiego Trybunału Praw Człowieka z 11 stycznia 2007 r. w sprawie Russian Conservative Party of Entrerpreneurs i inni przeciwko Rosji, skarga nr 55066/00 i 55638/00.

Uwagi terminologiczne

Zgodnie z „Zaleceniem Komitetu Ministrów dla państw członkowskich w sprawie norm prawnych, operacyjnych i technicznych dotyczących głosowania elektronicznego”[3], przez pojęcie e-wyborów (*e-voting*), należy rozumieć wybory i referenda elektroniczne, przeprowadzane przy wykorzystaniu środków elektronicznych, co najmniej podczas procesu oddawania głosu. Na szerszy zakres *e-votingu*, zwrócono uwagę w *Stanowisku w sprawie głosowania elektronicznego w wyborach powszechnych*, zaproponowanym przez internet Society Poland. Wskazano w nim, że „wybory elektroniczne to pojęcie obejmujące szeroki zakres zastosowań technik informatycznych w referendach oraz wyborach powszechnych”, wśród których możemy wymienić: 1) elektroniczną wizualizację wyników wyborów – systemy komputerowe pełnią rolę pomocniczą przy prezentacji i wizualizacji wyników wyborów przeprowadzonych tradycyjnie; 2) głosowanie wspomagane elektronicznie – systemy komputerowe są głównym narzędziem służącym do przyjmowania i zliczania głosów. Głosy mają być oddawane przez wyborców osobiście w lokalach wyborczych na dedykowanych komputerach wyborczych (tzw. *voting machines*); 3) głosowanie przez internet – w tym przypadku głosy są oddawane zdalnie z dowolnej lokalizacji za pomocą internetu, a ich przyjmowaniem oraz zliczaniem zajmuje się centralny komputerowy system wyborczy[4].

Ostatnią z możliwości w literaturze określa się mianem *i-votingu*, który może przybrać dwie formy[5]. Pierwsza, polega na głosowaniu w lokalu wyborczym (*Internet Voting at the Polling Place*) poprzez specjalnie do tego przygotowane narzędzia techniczne podłączone do internetu. Druga forma to głosowanie zdalne (*Remote Internet Voting*), polegające na możliwości oddania głosu z każdego komputera podłączonego do sieci internet, niezależnie od miejsca, w którym się znajduje[6].

3 Council of Europe, Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp.

4 Stanowisko Stowarzyszenia Internet Society Poland w sprawie głosowania elektronicznego w wyborach powszechnych przyjęte przez Zarząd Stowarzyszenia w dniu 10 stycznia 2007 roku (uchwała Zarządu ISOC Polska nr 2/2007), http://isoc.org.pl/200701-wybory/.

5 Szerzej zob. J. Rzucidło, *Perspektywy głosowania za pośrednictwem internetu w Rzeczypospolitej Polskiej*, „Studia Wyborcze” 2013, t. 15, s. 67–92.

6 M. Musiał-Karg, *Analiza doświadczeń związanych z wykorzystaniem głosowania internetowego (i-voting) w wybranych państwach*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu” 2018, nr 1, s. 48–49.

Zasada tajność głosowania

Zgodnie z wolą Ustrojodawcy wyrażoną w *Konstytucji Rzeczypospolitej Polskiej*[7], jedną z podstawowych zasad prawa wyborczego jest tajność głosowania. Przymiot ten, cechuje wszystkie rodzaje wyborów przeprowadzanych na terytorium Rzeczypospolitej Polskiej[8]. Stanowi on wraz z zasadą powszechności, równości oraz bezpośredniości wyborów konieczną przesłankę, wręcz kanon „demokratyzmu wyborów"[9]. Zasada ta wyraża zarówno uprawnienie, jak i obowiązek. Każdy uprawniony do głosowania ma bowiem prawo do nieuzewnętrzniania swoich preferencji politycznych w procedurze wyborczej, co podkreśla Trybunał Konstytucyjny w wyroku z dnia 20 lipca 2011 r.[10], w którym wskazano, że „nikomu innemu poza wyborcą nie będzie znana treść jego decyzji wyborczej". Natomiast obowiązek odnosi się do organów władzy publicznej, które organizują i przeprowadzają wybory, a także do ustawodawcy. Ich zadaniem jest wprowadzenie konkretnych gwarancji, dzięki którym obywatele będą mogli skorzystać z przysługującego im prawa, wynikającego z Konstytucji RP. Do mechanizmów gwarantujących zachowanie zasady tajności możemy zaliczyć: warunki w lokalach wyborczych, urny wyborcze, karty do głosowania, procedury związane z głosowaniem korespondencyjnym, procedury związane z głosowaniem przez osoby niewidome oraz penalizację czynów godzących w tajność wyborów. Zgodnie z art. 52 § 5 KodeksWyb lokale wyborcze powinny być odpowiednio przygotowane, tj. posiadać odpowiednią liczbę łatwo dostępnych miejsc, umożliwiających każdemu wyborcy nieskrępowane zapoznanie się z kartą do głosowania oraz jej wypełnienie w sposób niewidoczny dla innych osób poprzez odpowiednie rozmieszczenie parawanów, kotar bądź innych elementów umożliwiających swobodne oddania głosu[11]. Również urny wyborcze powinny spełniać odpowiednie wymagania, określone w art. 41a KodeksWyb, czyli powinny być wykonane z przezroczystego materiału oraz

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

8 Wybory do Sejmu – art. 96 ust. 2; wybory do Senatu – art. 97 ust. 2; wybory prezydenckie – art. 127 ust. 1; wybory samorządowe – art. 169 ust. 2. W przypadku wyborów przedstawicieli RP do Parlamentu Europejskiego odpowiednia regulacja znajduje się w art. 328 ustawy z dnia 5 stycznia 2011 r. Kodeks wyborczy (Dz.U nr 21, poz. 112 ze zm.), dalej KodeksWyb.

9 L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2017, s. 175.

10 Wyrok Trybunału Konstytucyjnego z dnia 20 lipca 2011 r., K 9/11, Legalis nr 343106.

11 P. Czarny, *Komentarz do art. 96* [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*, t. II, *Komentarz do art. 87–243*, Legalis 2016.

opieczętowane w taki sposób, aby nie było możliwe wyjęcie kart z urny przed jej otwarciem. Same karty do głosowania natomiast powinny być zgodne ze wzorem ustalanym przez Państwową Komisję Wyborczą (art. 40 KodeksWyb), a głos winien być oddany w taki sposób, by zadrukowana strona karty do głosowania była niewidoczna (art. 52 § 6 KodeksWyb). Wśród mechanizmów gwarantujących tajność wskazano również szczególne procedury. Jedna z nich związana jest z postępowaniem z głosami oddanymi w drodze korespondencyjnej. Zgodnie z art. 53h § 6 KodeksWyb w tego typu przypadkach zaklejone koperty z kartami do głosowania powinny być umieszczane w urnach bez ich wcześniejszego otwierania. Inna procedura, zapewniająca udział w wyborach osobom niepełnosprawnym, polegająca na umożliwieniu głosowania przy użyciu nakładek na karty do głosowania sporządzonych w alfabecie Braille'a, również uznawana jest za element gwarancyjny tajności wyborów (tego typu procedura wyklucza udział osób trzecich, uniemożliwiając tym samym innym osobom zapoznanie się z treścią głosu przed umieszczeniem karty do głosowania w urnie). Należy bowiem mieć na uwadze, że zapoznanie się, wbrew woli głosującego, z treścią jego głosu, stanowi czyn zabroniony, zgodnie z art. 251 ustawy z dnia 6 czerwca 1997 r. Kodeks karny[12]. Elementem składającym się na tajność, jest również zakaz publicznego podawania list osób, które wzięły udział w wyborach, ponieważ przymiot tajności wyborów odnosi się do całej procedury wyborczej, a nie wyłącznie do momentu oddania głosu[13]. Wszystkie te działania ukierunkowane są na ochronę wyborcy przed wszelkimi skutkami związanymi z ujawnieniem jego preferencji wyborczych, choć skutki te mogą mieć charakter negatywny, jak i pozytywny[14].

Jak wcześniej wskazano, zasada tajności rodzi po stronie organów państwowych obowiązek zapewnienia odpowiednich warunków umożliwiających oddanie głosu przez wyborcę, bez jego ujawniania. Można zastanawiać się, czy obowiązek zachowania zasady tajności głosowania odnosi się również do samych wyborców. Zgodnie z przywołanym wcześniej wyrokiem Trybunału Konstytucyjnego „dla wyborcy tajność głosowania jest przywilejem, z którego może on skorzystać, choć nie ma takiego obowiązku. Oddanie głosu w sposób

12 Dz.U. nr 88, poz. 553 ze zm.

13 Europejska Komisja dla demokracji przez prawo (Komisja Wenecka), *Kodeks Dobrej Praktyki w Sprawach Wyborczych. Wytyczne i Raport wyjaśniający, przyjęty przez Komisję Wenecką na 52 Sesji (Wenecja, 18–19 października 2002)*, pkt 4c Kodeksu oraz pkt 54 raportu wyjaśniającego.

14 Wyrok Trybunału Konstytucyjnego z dnia 20 lipca 2011 r., K 9/11, Legalis nr 343106.

jawny, o ile nie stanowi formy agitacji wyborczej, nie wiąże się dla niego z żadnymi negatywnymi konsekwencjami prawnymi. Również dobrowolne poinformowanie o treści decyzji wyborczej innych osób, niezależnie od tego, czy ma miejsce przed wyborami, czy po wyborach, nie narusza zasady tajności głosowania"[15]. W tym samym wyroku Trybunał Konstytucyjny zauważa jednak, że „w sytuacji gdy wyborca decyduje się na głosowanie poza lokalem obwodowej komisji wyborczej, świadomie rezygnuje z tej gwarancji tajności głosowania stwarzanej przez państwo, przejmując jednocześnie obowiązek zorganizowania sobie we własnym zakresie odpowiednich warunków zapewniających tajność głosowania. Z tego też względu elementem pakietu wyborczego, który otrzymuje wyborca głosujący korespondencyjnie, jest oświadczenie o osobistym i tajnym oddaniu głosu na karcie do głosowania". Na tej kanwie, w doktrynie podkreśla się niekonsekwencje w przyjętym przez Trybunał rozumowaniu, bowiem „gdyby traktować oddanie głosu z zachowaniem tajności jako przywilej wyborcy, to trudno mówić o obowiązku zorganizowania sobie odpowiednich warunków, ponieważ to od woli wyborcy zależałoby, w jaki sposób odda on głos"[16]. W tej kwestii warto wskazać stanowisko Komisji Weneckiej, która stanowczo stwierdza, że wyborcy mają prawo do tajności, „lecz również sami muszą to prawo przestrzegać, a nieprzestrzeganie winno być karane przez unieważnienie każdej karty do głosowania, której zawartość została ujawniona"[17]. Opinia ta, choć restrykcyjna, wydaje się słuszna. Realizuje ona bowiem w pełni istotę przymiotu tajności głosowania. Ponadto, na taką interpretację w polskim porządku prawnym wskazywać może norma zawarta w art. 52 § 6 KodeksWyb, nakładająca na wyborców obowiązek oddania głosu w taki sposób, aby strona zadrukowana karty do głosowania była niewidoczna dla innych. Jest to przykład normy bezwzględnie obowiązującej, nieposiadającej jednakże sankcji za niezastosowanie się do dyspozycji normy prawnej. Należy jednak podkreślić, że brak ustawowej sankcji „nie redukuje obowiązku prawnego wynikającego z ustawy; wiele jest bowiem w systemie prawa przepisów nie obwarowanych karami, które jednak mają moc powszechnie obowiązującą"[18].

15 Ibidem.

16 P. Czarny, *Komentarz do art. 96* [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*, t. II, *Komentarz do art. 87–243*, Legalis 2016.

17 Pkt 52 raportu wyjaśniającego.

18 F. Rymarz, *Tajność głosowania – uprawnienie czy obowiązek?*, http://niezniknelo.pl/OK2/debaty/tajnosc-glosowania-uprawnienie-czy-obowiazek/index.html. Odmienne stanowisko zaprezentował B. Banaszek: „Sugestie zawierają także przepisy wymagające, aby wrzucać karty do urny tak, by nie była widoczna strona zadrukowana, na której znajdują się nazwiska

Mając na uwadze przedstawione wyżej przesłanki, gwarantujące realizację zasady tajności podczas głosowania, należy rozważyć, czy i-głosowanie również powinno je spełniać, a jeśli tak, to w jakim zakresie.

Kontrowersje wokół i-votingu

W raporcie stworzonym przez The International Institute for Democracy and Electoral Assistance, podkreśla się, że zachowanie tajności przy e-głosowaniu stanowi olbrzymie wyzwanie, ponieważ standardowe systemy teleinformatyczne są z natury ukierunkowane na śledzenie i monitorowanie dokonywanych na nich działań[19]. Ponadto, trudności przy zachowaniu anonimizacji wyborcy wynikać mogą z faktu, że „tajność głosowania stoi w sprzeczności z wymaganiem silnego uwierzytelnienia związanego z potwierdzeniem tożsamości wyborcy. (…) w stosowanych dotychczas systemach *i-votingu* anonimizacja głosów prowadzona jest jedynie w systemie centralnym, pozostającym poza jakąkolwiek kontrolą wyborcy”[20]. Uwagi te oznaczają, że co najmniej na jednym z etapów e-głosowania istnieje możliwość połączenia wyborcy z oddanym przez niego głosem, co sprzeciwia się zasadzie tajności[21]. Odpowiedzią na powyższe wątpliwości, może być zastosowanie odpowiednich protokołów czy algorytmów, które utajnią sposób oddania głosu. Zaliczyć do nich można: Diffie-Hellman, AES (*Advanced Encryption Standard*), Shamir's Secret Sharing, Blind Signature[22]. Zawsze istnieje jednak możliwość, że specjalista z dziedziny IT przełamie takie zabezpieczenia. Potwierdzeniem tego mogą być słowa A. Preisnera: „Stworzenie całkowicie bezpiecznego systemu głosowania nie jest możliwe, szczególnie jeżeli system jest dostępny w internecie, lecz osiągalne

kandydatów. Z tego opisu pożądanego zachowania się wyborcy podczas głosowania nie można wyprowadzić obowiązku oddania głosu w sposób uniemożliwiający rekonstrukcję treści jego głosu lub powzięcie wiadomości o tym, jak wyborca głosował. Oznacza to, że zasada tajności nakłada jedynie określone obowiązki na organy powołane do przygotowania i przeprowadzenia wyborów”, B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Legalis 2012.

19 The International Institute for Democracy and Electoral Assistance, *Introducing Electronic Voting: Essential Considerations*, Policy Paper, December 2011, s. 7.

20 G. Gacki, *Prawo do e-głosowania*, http://www.itwadministracji.pl/numery/lipiec-2009/prawo-do-e-glosowania.html.

21 Na problem anonimizacji głosów w aspekcie zachowania tajności wyborów uwagę zwrócił Trybunał Konstytucyjny Austrii w wyroku z dnia 11 grudnia 2011 r., V 85-96/11–15.

22 Szerzej zob. M. de Vries, W. Bokslag, *Evaluating e-voting: theory and practice*, CoRR abs/1602.02509.

jest takie jego zabezpieczenie, by pokonanie zabezpieczeń wymagało ogromnych nakładów czasu, pieniędzy i mocy obliczeniowej”[23]. Należy zatem zastanowić się, czy rozwiązanie jakim jest *i-voting*, które zapewnia nam współczesna technika, wpisuje się w konstytucyjny przymiot tajności głosowania. Zdaniem autora, każda realna możliwość dokonania identyfikacji wyborcy z oddanym przez niego głosem w systemie informatycznym stoi w sprzeczności z zasadą tajności głosowania. Możemy jednak wyobrazić sobie sytuację, w której przeprowadzenie głosowania w formie tradycyjnej staje się utrudnione bądź niemożliwe albo zagraża życiu bądź zdrowiu obywateli np. w wyniku powszechnie panującej pandemii. W takim wypadku *i-voting* mógłby stanowić bezpieczną alternatywę dla przeprowadzenia wyborów, pomimo faktu, że wiązałoby się to z ograniczeniem podstawowych zasad prawa wyborczego. Powstaje zatem pytanie, czy zasady prawa wyborczego, takie jak powszechność, bezpośredniość, równość czy tajność głosowania mogą ulec ograniczeniu? Ustrojodawca w art. 31 ust. 3 Konstytucji stanowi: „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw”. Przepis ten daje zatem możliwość, ograniczenia praw i wolności człowieka oraz obywatela. Jednym z takich praw, wyrażonym w art. 62 ust. 1 Konstytucji, jest udział „w referendum oraz prawo wybierania Prezydenta Rzeczypospolitej, posłów, senatorów i przedstawicieli do organów samorządu terytorialnego…”. Na tej podstawie, dokonując wykładni moglibyśmy uznać, że Ustrojodawca dopuszcza pod określonymi warunkami możliwość ograniczenia stosowania zasad prawa wyborczego (w tym tajność głosownia), które są immanentnie związane z prawem udziału w wyborach. W opinii autora nie możemy jednak dokonywać takiej interpretacji i dokonywać spłaszczenia analizowanego przepisu, ponieważ przy wykładni tego rodzaju należy stosować zasady wykładni wyjątków – czyli zakaz interpretacji rozszerzającej jego postanowienia[24]. Ponadto, zgodnie z wyrokiem Trybunału

23 A. Preisner, *e-Voting przyszłość e-demokracji? Szkic kilku niełatwych kwestii* [w:] S. Grabowska, R. Grabowski (red.), *Międzynarodowa Konferencja Naukowa nt. Prawo wyborcze do parlamentu w wybranych państwach europejskich, Rzeszów 3–4 kwietnia 2006 r.*, Rzeszów 2006, s. 212.

24 Szerzej zob. M. Wyrzykowski, *Granice praw i wolności – granice władzy* [w:] *Obywatel – jego wolności i prawa. Zbiór studiów przygotowanych z okazji 10. lecia Urzędu Rzecznika Praw Obywatelskich*, Warszawa 1998, s. 45–59.

Konstytucyjnego w przypadku ograniczeń praw i wolności, musimy rozważyć czy: „1) wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków; 2) regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest połączona; 3) efekty wprowadzonej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela”[25]. Istotne jest również, że zasady prawa wyborczego wynikają *stricte* z zasady demokratycznego państwa prawa, która jest zasadą ustrojową i absolutną, niepodlegającą żadnym ograniczeniom. To wszystko sprowadza się do stwierdzenia, że również w przytoczonej powyżej sytuacji niemożności przeprowadzenia wyborów w sposób tradycyjny, zastosowanie *i-votingu* naruszałoby przepisy Konstytucji Rzeczypospolitej Polskiej, poprzez niezachowanie zasady tajności głosowania.

Kwestią, której nie można pominąć przy analizie *i-votingu*, jest dostęp do internetu osób uprawnionych do głosowania. Na podstawie danych Eurostatu, 87% obywateli Polski posiada dostęp do internetu[26], co oznacza, że 13% społeczeństwa jest go pozbawiona, a wśród tych osób z pewnością znajdują się również osoby uprawnione do głosowania, które w przypadku wprowadzenia *i-votingu*, nie mogłyby skorzystać z praw wyborczych, co stanowić może pogwałcenie zasady powszechności wyborów. Dyskryminacja może również dotyczyć osób niepełnosprawnych (m.in. niewidomych), a także osób starszych, które nie potrafiłyby korzystać z dedykowanego wyborom systemu komputerowego. W tym celu zaistniałaby konieczność skorzystania z pomocy osób trzecich, co wiązałoby się z naruszeniem zasady bezpośredniości oraz tajności wyborów. Dlatego też Rada Europy w *Zaleceniu Komitetu Ministrów dla państw członkowskich w sprawie standardów głosowania elektronicznego z 2017 r.*, podkreśliła, że procedura głosowania elektronicznego nie może być jedyną procedurą oddawania głosu, ale powinna być traktowana jako alternatywna, dodatkowa[27].

Warto zwrócić uwagę również na aspekt ponoszenia odpowiedzialności za przeprowadzenie wyborów w formie *i-votingu*. W sytuacji wyborów tradycyjnych, obowiązujące prawo, wprost wskazuje na jakich podmiotach ciąży obowiązek przeprowadzania wyborów na danym szczeblu i etapie. Natomiast,

25 Wyrok Trybunału Konstytucyjnego z dnia 22 lutego 2005 r., K 10/04 (Dz.U. nr 39, poz. 377).
26 https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en.
27 Recommendation CM/Rec(2017)5' of the Committee of Ministers to member States on standards for e-voting, https://rm.coe.int/0900001680726f6f. Szerzej zob. J. Zbieranek, *Głosowanie przez internet (i-voting) w wybranych państwach*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu” 2018, nr 1, s. 9–45.

w przypadku *i-votingu* organy administracji publicznej byłyby zobowiązane przenieść część odpowiedzialności za przebieg procesu wyborczego na podmioty świadczące usługi drogą elektroniczną, w szczególności pośredników, a tym samym musiałyby określić na jakich zasadach, w jakich granicach i czy w ogóle ponosiliby oni odpowiedzialność. Problem potęguje również brak operatora narodowego sieci teleinformatycznych oraz brak państwowej infrastruktury. Organy administracji publicznej byłyby zatem zależne od infrastruktury podmiotów komercyjnych, co mogłoby skutkować brakiem pełnej kontroli nad zapewnieniem cyberbezpieczeństwa *i-votingu* oraz problemami z ochroną przed atakami cybernetycznymi. Stworzenie dedykowanego systemu do przeprowadzania *i-votingu* oraz jego obsługa najczęściej byłaby powierzana podmiotom zewnętrznym, specjalizującym się w branży IT. Tego typu działania mogłyby budzić wątpliwości w zakresie przekazywania tym podmiotom spisu wyborców w celu ich prawidłowej weryfikacji w systemie. Spis zawiera bowiem dane osobowe, które podlegają ochronie, na gruncie Konstytucji RP (art. 51) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[28], w którym wprost określono zasady przetwarzania, w tym przekazywania danych osobowych innym podmiotom.

M. Kutyłowski w analizie dotyczącej możliwości przeprowadzenia *i-votingu* w Polsce, wskazał ponadto na dwa problematyczne zagadnienia: kontrolę wyborcy nad składanym głosem, rozumianą jako uodpornienie systemu na możliwość modyfikacji głosu oraz ustalenie prawidłowości wyników, czyli analizę zgodności głosów oddanych z wynikami podanymi do publicznej wiadomości[29]. Do powyższego katalogu zagrożeń związanych z *i-votingiem* należy dołączyć również możliwość przeprowadzenia zmasowanego ataku cybernetycznego na cały system teleinformatyczny obsługujący platformę *i-votingu*, np. zinfiltrowanie dostawcy systemu przez zainstalowanie złośliwego oprogramowania fałszującego wyniki wyborów, bądź przez uniemożliwienie identyfikacji wyborcy w systemie wyborczym, co skutecznie sparaliżowałoby

28 Dz.Urz.UE L 119, 2016, s. 1–88.

29 M. Kutyłowski, *E-voting: głosowanie elektroniczne*, „Infos" nr 10(27), 21 maja 2009, http://orka.sejm.gov.pl/WydBAS.nsf/0/701C7F09ABFE5C84C12575BD002DE087/$file/Infos_57.pdf.

możliwość oddawania głosu, czego przykładem może być kazus amerykański[30]. Zagrożeniem związanym z *i-votingiem* jest także czynnik ludzki, w postaci samego wyborcy, który poprzez niefrasobliwe działania w sieci może udostępnić w jaki sposób budowane są loginy do systemu, kody dostępu, czy inne dane ułatwiające możliwość zaatakowania systemu. Wskazane powyżej działania mogą skutkować zmanipulowaniem wyników lub nieprawidłowym wynikiem wygenerowanym przez system głosowania elektronicznego, co z kolei może prowadzić do uznania nieważności wyborów. W tym miejscu pojawia się jeszcze jedna wątpliwość. W przypadku tradycyjnego głosowania, wyborcy mają prawo wnieść protest wyborczy, jeżeli w ich opinii dochodzi do naruszenia prawa wyborczego, np. jeśli zauważą jakiekolwiek manipulacje związane z oddanym głosem. W przypadku *i-votingu*, w wyniku zerwania powiązań między wyborcą a głosowaniem, wyborca pozbawiony zostaje możliwości weryfikacji, czy jego głos rzeczywiście został policzony i uznany za oddany na konkretnego kandydata, co konotuje, że potencjalnie pozbawiony zostaje on możliwości wniesienia protestu w razie naruszenia prawa[31].

Zakończenie

W 2013 r. wśród mieszkańców Norwegii przeprowadzono badania ankietowe dotyczące możliwości zastosowania *i-votingu* w procesie wyborczym[32]. Pytania dotyczyły możliwości wprowadzenia tego rozwiązania na terytorium

30 W raporcie stworzonym przez CIA, FBI i NSA i opublikowanym 6 stycznia 2017 r., wprost stwierdzono, że Rosjanom udało się przejąć kontrolę nad częścią infrastruktury biur wyborczych USA. Podkreślono jednak, że kontrolowane przez nich systemy nie miały możliwości ingerencji w maszyny do głosowania i liczenie głosów, powołując się na ich odseparowanie od sieci [The Intelligence Community, *Assessing Russian Activities and Intentions in Recent US Elections*, https://www.dni.gov/files/documents/ICA_2017_01.pdf]. Praktyka jednak okazała się zgoła odmienna, ponieważ pomimo zapewnienia przez najwyższe władze federalne o braku możliwości połączenia głosomatów z siecią, w wyniku eksperymentu przeprowadzonego podczas DefCon 2019 udowodniono, że maszyny same, automatycznie łączą się z lokalną siecią, przez co stają się podatne na wszelkiego rodzaju ataki cybernetyczne.

31 Na problem ten zwrócił uwagę Federalny Trybunał Konstytucyjny w Niemczech [Wyrok BVerfG z 3 marca 2009 r., sygn. akt 2 BvC 3/07 oraz 2 BvC 4/07]. Szerzej zob. M. Rulka, *Orzecznictwo dotyczące konstytucyjności regulacji umożliwiających głosowanie elektroniczne (Niemcy, Austria, Estonia, Indie)*, „Przegląd Sejmowy" 2015, nr 6, s. 217–228.

32 J. Saglie, S.B. Segaard, *Internet voting and the secret ballot in Norway: principles and popular understandings*, „Journal of Elections, Public Opinion and Parties" 2016, nr 2, s. 155–169.

Norwegii oraz postrzegania przez obywateli zasad związanych z jego zastosowaniem. Z badań wynikało, że 94% respondentów uważa, że należy umożliwić obywatelom Norwegii korzystanie z nowych technologii w procesie wyborczym, czyli wprowadzić *i-voting*. 8 na 10 przebadanych stwierdziło, że technologia wykorzystywana przy *i-votingu* jest bezpieczna i można jej ufać. Ankietowanym przedstawiono także niebezpieczeństwa, jakie związane są z e-głosowaniem, w tym wątpliwości związane z przestrzeganiem zasady tajności głosowania. Następnie poproszono ich o udzielenie odpowiedzi na pytanie, czy zasada tajnego głosowania jest tak istotna przy wyborach, że niemożność jej zagwarantowania uniemożliwia przeprowadzenie wyborów przez internet. Co ciekawe aż 81% ankietowanych nie zgodziła się z tym twierdzeniem uważając, że przymiot ten nie powinien mieć wpływu na przeprowadzenie wyborów w formie *i-votingu*. Ankietowanym zadano następnie pytanie, czy jeśli ktoś głosuje przez internet jego głos powinien być anonimowy. 82% respondentów uważało, że tak. Z przeprowadzonych badań wynika ponadto, że społeczeństwo inaczej pojmuje zasadę tajności głosowania przez internet, dopuszczając możliwość zaakceptowania faktu, że procedura głosowania może być obserwowana przez innych np. domowników czy przyjaciół.

Badania ta mogą stanowić przyczynek do podjęcia dyskusji w temacie pojmowana zasady tajności głosowania i dostosowania jej do *i-votingu*, a w przyszłości do przyjęcia takich rozwiązań prawnych które, stojąc w zgodzie z wymogami konstytucyjnymi, dopuszczą realną możliwość przeprowadzania wyborów z zastosowaniem sieci internet. Pozostaje jednak pytanie, czy takim działaniem nie naruszamy istoty oraz natury podstawowych zasad prawa wyborczego.

Bibliografia

Literatura

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Legalis 2012.

Czarny P., *Komentarz do art. 96* [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*, t. II, *Komentarz do art. 87–243*, Legalis 2016.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2017.

Herbert B.P., Anderson K.J., *Diuna. Bitwa pod Corrinem*, Poznań 2009.

Musiał-Karg M., *Analiza doświadczeń związanych z wykorzystaniem głosowania internetowego (i-voting) w wybranych państwach*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu" 2018, nr 1.

Preisner A., *e-Voting przyszłość e-demokracji? Szkic kilku niełatwych kwestii* [w:] S. Grabowska, R. Grabowski (red.), *Międzynarodowa Konferencja Naukowa nt. Prawo wyborcze do parlamentu w wybranych państwach europejskich, Rzeszów 3–4 kwietnia 2006 r.*, Rzeszów 2006.

Rulka M., *Orzecznictwo dotyczące konstytucyjności regulacji umożliwiających głosowanie elektroniczne (Niemcy, Austria, Estonia, Indie)*, „Przegląd Sejmowy" 2015, nr 6.

Rzucidło J., *Perspektywy głosowania za pośrednictwem internetu w Rzeczypospolitej Polskiej*, „Studia Wyborcze" 2013, t. 15.
Saglie J., Segaard S.B., *Internet voting and the secret ballot in Norway: principles and popular understandings*, „Journal of Elections, Public Opinion and Parties" 2016, nr 2.
Vries M., Bokslag W., *Evaluating e-voting: theory and practice*, CoRR abs/1602.02509.
Wyrzykowski M., *Granice praw i wolności – granice władzy* [w:] *Obywatel – jego wolności i prawa. Zbiór studiów przygotowanych z okazji 10. lecia Urzędu Rzecznika Praw Obywatelskich*, Warszawa 1998.
Zbieranek J., *Głosowanie przez internet (i-voting) w wybranych państwach*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu" 2018, nr 1.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483 ze zm.).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119, 2016, s. 1–88).
Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy (Dz.U. nr 21, poz. 112 ze zm.).
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. nr 88, poz. 553 ze zm.).

Orzeczenia

Wyrok Europejskiego Trybunału Praw Człowieka z 11 stycznia 2007 r. w sprawie Russian Conservative Party of Entrerpreneurs i inni przeciwko Rosji, skarga nr 55066/00 i 55638/00.
Wyrok Trybunału Konstytucyjnego z dnia 20 lipca 2011 r., K 9/11, Legalis nr 343106.
Wyrok Trybunału Konstytucyjnego z dnia 20 lipca 2011 r., K 9/11, Legalis nr 343106.
Wyrok Trybunału Konstytucyjnego z dnia 22 lutego 2005 r., K 10/04 (Dz.U. nr 39, poz. 377).

Secret ballot and i-voting. Legal doubts related to Internet voting

Abstract

The secret ballot is one of the fundamental canons of electoral law. It guarantees the right to anonymize the vote, which means breaking the bond between the voter and his voice at the stage of determining the election results. However, as a result of the progressing process of technologization of social life aimed at making a easier for individuals to function in public life, manifesting itself, inter alia, in the possibility of voting via the internet from anywhere (*i-voting*), this rule is marginalized. I-voting does not provide a real guarantee of ensuring secrecy during the voting process, but nevertheless these solutions have been adopted in several countries. This article raises questions of legal nature related to the use of i-voting in the Polish legal order.

Key words: internet, elections, voting, e-voting, voting rights

Małgorzata Czuryk*

Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity

Abstract

Local and regional governments play a special role in public life. They perform, on their own behalf and responsibility, certain tasks commissioned by the State by way of legal Acts. The objective of the local and regional governments' existence is to meet the collective requirements of their respective communities. Meeting the needs of residents also requires activities in the field of telecommunications, including support for the development of telecommunications services and networks. However, such development must be monitored. The role of local and regional governments, on the one hand, is to support this development, and, on the other, to protect the users of telecommunications services and networks from threats. Cybersecurity must therefore occupy the right place in the catalogue of local and regional governments' tasks; it cannot be marginalised, as cyberthreats are real, and can result in substantial damage that is not only virtual.

Key words: telecommunications services, telecommunications networks, cybersecurity, local and regional government, telecommunications infrastructure, the Internet

* Dr hab. Małgorzata Czuryk, Professor of the University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

Introduction

Local and regional governments are established in order to carry out public tasks at the local and regional levels. Depending on the type of public activities carried out by a body, they are referred to as local or regional governments. Despite the fact that all local and regional government bodies are entrusted with powers to perform tasks related to telecommunications, their impact on the development of telecommunications services and networks varies. This does not result solely from the authority vested in communes, districts, and provinces, but also from the financial resources of the respective entities and their policies, including the priorities and objectives of local and regional government bodies.

Local and regional governments, as separate legal entities, are forms of decentralisation[1]; when performing activities in the field of telecommunications, they must recognise the potential threats, and they are obligated to ensure security in cyberspace. Cybersecurity is particularly important in the context of supporting the development of telecommunications services and networks. Local and regional government bodies must remember that the dynamism of this development must not result in relaxing the protection of cyberspace against threats. Both these elements must evolve simultaneously - i.e. the development of telecommunications services and networks should enforce the application of new, more effective mechanisms of protection against cyberthreats, and improvements to the existing measures.

Local and regional governments participate in exercising public authority, and perform an essential part of the public tasks assigned to them on their own behalf and responsibility[2], i.e., they have been granted the authority to perform the entrusted tasks[3]. Supporting the development of telecommunications services and networks also belongs to the tasks of local and regional government; however, it should be remembered that this development must be monitored and protected from threats.

1 M. Karpiuk, *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008, s. 58.
2 M. Karpiuk, J. Kostrubiec, *Rechtsstatus der territorialenSelbstverwaltung in Polen*, Olsztyn 2017, s. 191.
3 M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014, s. 15.

Local and regional government activities in the fields of telecommunications and cybersecurity

The legislators have authorised the respective local and regional government bodies to carry out activities in the field of telecommunications, provided that their goal is to meet the collective needs of the local or regional governments' communities, depending on the level of the local or regional government. The telecommunications activities of local and regional governments cannot be carried out without regard for the necessity to simultaneously care for network security. Cybersecurity must be taken into consideration by local and regional government bodies when performing activities related to telecommunications, and must form part of the policy of supporting the development of telecommunications services and networks.

Cybersecurity is a notion relating to the provision of security and counteracting threats referring to cyberspace, as well as to functioning in cyberspace, which concerns both the public and private sectors, and their mutual relationships[4]. Cyberspace is becoming not only the space where people work, learn, communicate with each other, and seek entertainment, but also has become a space where people are exposed to various threats[5]. Cybersecurity is not limited to information security, as the latter is only one of the elements of cybersecurity[6].

4 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 21.

5 A. Pieczywok, *Cyber threats and challenges targeting man versus his education*, „Cybersecurity and Law" 2019, nr 1, s. 227.

6 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność…*, s. 20. More on information security and information protection: P. Zając, *Classified Information and its Protection in Polish Armed Forces. General Assumptions*, „Teka Komisji Prawniczej. Oddział PAN w Lublinie" 2017, t. X; M. Karpiuk, *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014; M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017; M. Karpiuk, *Cyfrowe transmisje radiofoniczne i telewizyjne i ich wpływ na bezpieczeństwo informacyjne* [w:] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

The legislators define cybersecurity as the immunity of information systems to violations of the integrity, availability, and authenticity of the processed data or related services afforded by these systems[7]. Cybersecurity is a specialised aspect of security[8] which includes the protection of information systems against threats.

Local and regional governments are part of the national cybersecurity system, whose objective, according to Article 3 of the Act on the national cybersecurity system (u.k.s.c.), is to ensure cybersecurity at the national level, including undisturbed provision of key services and digital services through

7 rt. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.), hereinafter u.k.s.c.

8 More on security: M. Karpiuk, *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3; M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016; M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia IuridicaLublinensia" 2017, nr 4; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2, M. Karpiuk, *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4; M. Karpiuk, J. Kostrubiec, *The VoivodeshipGovernor's Role in HealthSafety*, „Studia IuridicaLublinensia" 2018, nr 2; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016; M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019; J. Kostrubiec, *Status of a VoivodshipGovernor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5; M. Karpiuk, *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016; M. Karpiuk, *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1; M. Karpiuk, *Position of the LocalGovernment of Commune Level in the Space of Security and Public Order*, „Studia IuridicaLublinensia" 2019, nr 2; M. Karpiuk, *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.

achieving the appropriate security level of information systems intended for the provision of these services and managing incidents. The objective of the national cybersecurity system, including the bodies creating the system, will thus be to protect the provision of key services and digital services so that they can be delivered without disruptions.

The range and rules of operation of local and regional government bodies in the field of telecommunications

The legislators clearly state that a local or regional government body may perform the following activities in order to meet the collective needs of local or regional government communities: 1) build or use telecommunications infrastructure and networks and acquire the rights to telecommunications infrastructure and networks; 2) provide telecommunications networks or access to telecommunications infrastructure; 3) provide, with the use of the available telecommunications infrastructure and networks, services to: a) telecommunications companies, b) authorised entities, c) end users[9]. Article 3 section 1 of the Act on supporting the development of telecommunications services and networks (u.w.r.) specifies the major types of local and regional government tasks in the telecommunications sector, which can be carried out directly by the given local or regional government body. Thus, it can build telecommunications infrastructure and networks, provide them to businesses and other administrators, i.e. supply wholesale telecommunications services. The provision also facilitates direct activities in the field of telecommunication services provision for end users[10]. A local or regional government unit may not only build or operate telecommunications infrastructure and networks, but also acquire rights to telecommunications infrastructure and networks, and it may also provide services to external entities, deliver telecommunications networks, or provide access to telecommunications infrastructure. The competences of local and regional government in the field of telecommunications are therefore quite broad, which creates extensive possibilities for supporting the development of telecommunications services and networks, taking into consideration the provision of security in cyberspace.

9 Art. 3 ust. 1 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2019 r., poz. 2410 ze zm.), hereinafter u.w.r.
10 Wyrok NSA z dnia 18 września 2018 r., II FSK 2423, LEX nr 2601705.

Despite the fact that the legislators allow local and regional government bodies to construct telecommunications infrastructure and networks, such activities cannot be performed if in a given area: 1) telecommunications infrastructure and networks do not exist; 2) existing telecommunications infrastructure and networks are not available or do not meet the needs of the local or regional government body. These conditions are introduced by Article 3 section 1a of u.w.r. A local or regional government body may perform such public utility tasks only if in the area of a given commune, district, or province (depending on where the local or regional government body intends to perform activities related to the construction of telecommunications infrastructure and networks) there are no telecommunications infrastructure or networks, and, if they exist, they are inaccessible or do not meet the needs of the local or regional government body. The prerequisite according to which the construction of the telecommunications infrastructure and networks exist but do not meet the needs of the local or regional government body is not a clear-cut one. It is associated with the objectives of local and regional government related to the computerisation of a given area. However, computerisation must take into consideration threats present in cyberspace, so it must simultaneously adopt protective solutions.

Activities in the field of construction, or the operation of or acquiring rights to, telecommunications infrastructure and networks, and delivering telecommunications networks or providing access to telecommunications infrastructure, as well as the provision of services to other entities with the use of the available telecommunications infrastructure and networks according to Article 3 section 2 of u.w.r., should be performed in a way ensuring compatibility and connectivity with other telecommunications networks created by public bodies, or financed from public funds and guaranteeing telecommunications companies, on an equal treatment basis, the possibility of the joint use of telecommunications infrastructure and networks and access to them, in a transparent manner, not interfering with the development of equal and effective competition on telecommunications markets. Such public utility activities must not interfere with the competitiveness framework, i.e. must not lead to violations of market principles, violations in which local

and regional government would be in a privileged position in relation to telecommunications companies[11].

Local and regional governments' undertaking activities in the field of telecommunications must not violate regulations involving State aid. Any aid provided by an EU Member State, or with the use of national resources in any form, which disrupts or threatens to disrupt competition by favouring certain companies or the production of certain goods, is non-compliant with the EU internal market to an extent to which it impacts on trade between EU Member States. The following types of aid are considered compliant with the internal market: 1) aid designed to support the economic development of regions in which living standards are abnormally low or regions with a substantial level of underemployment, taking into consideration their structural, economic, and social situations; 2) aid intended for supporting the implementation of crucial projects of common interest in the EU or aimed at remedying major disturbances in an EU Member State's economy; 3) aid designed to facilitate the development of certain economic activities, or certain economic regions, as long as it does not precipitate a change in trade conditions contrary to the common interest; 4) aid intended for supporting culture and preserving cultural heritage, as long as it does not result in a change to trade conditions and competition in the EU contrary to the common interest[12]. The definition of State aid is broad, and includes an unlimited number of State support measures for enterprises. The definition of aid does not cover general funds which do not favour specific companies or entire sectors of the economy. Such funds can impact on trade between Member States; however, they do not constitute State aid[13].

The activities of local and regional governments may consist of the provision of Internet access services through publicly available Internet access points free of charge, or for a fee lower than the market price. In such cases, as stipulated in Article 3 section 7a of u.w.r., information on commencing such activities published in the Public Information Bulletin should include, i.a., the

11 M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1, s. 40.

12 Art. 107 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. nr 90, poz. 864/2 ze zm.).

13 B. Kurcz, *Komentarz do art. 107* [w:] K. Kowalik-Bańczyk, M. Szwarc-Kuczer, A. Wróbel (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. II, LEX 2012.

location of publicly available Internet access points and the identification of the area where the service is provided through these points.

A local or regional government may provide Internet access services through publicly available Internet access points without collecting any charges, or for a fee lower than the market price, which stems directly from Article 7 section 1a of u.w.r. The minimum bandwidth for Internet access services provided by local and regional governments through publicly available Internet access points free of charge, or for a fee lower than the market price, is 30 Mb/s[14].

The executive body of a local or regional government, pursuant to Article 3a of u.w.r., may provide entities not included in the public finance sector and not conducting business activities with a designated subsidy from the local or regional government's budget for financing or co-financing the costs of projects associated with meeting the needs of these entities related to access to a fast telecommunications network at the end user's location. The rules for the provision of such a designated subsidy, in particular the selection criteria for a project for financing or co-financing, and the procedure for granting such a subsidy and the manner of settling it, are specified by the governing body of the local or regional government entity by way of a resolution. The subsidy is provided on the basis of an agreement concluded by a local or regional government entity. The agreement should contain: 1) a detailed description of the task, including the purpose for which the subsidy was granted, and the date of its completion; 2) the amount of subsidy provided to the entity performing the task, and the payment method; 3) the time limit for using the subsidy, up to 31 December of a given budget year; 4) the procedure for controlling the performance of the task; 5) the date and settlement method of the subsidy; 6) the date for returning the unused part of the subsidy[15].

A local or regional government entity, pursuant to Article 4 of u.w.r., before commencing activities in the field of the construction or operation of, or acquiring rights to, telecommunications infrastructure and networks, or delivering telecommunications networks or providing access to telecommunications infrastructure, as well as the provision of services to other entities with the

14 § 1 rozporządzenia Ministra Cyfryzacji z dnia 18 października 2018 r. w sprawie minimalnej przepływności łącza dla świadczonej przez jednostki samorządu terytorialnego usługi dostępu do Internetu (Dz.U. z 2018 r., poz. 2087).

15 Art. 221 ust. 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2019 r., poz. 869 ze zm.).

available telecommunications infrastructure and networks, may apply to the President of the Office of Electronic Communications with a request for an assessment of the performance of these activities. The initiative of the local and regional governments in this respect is of a preventive nature, and makes it possible to avoid certain future problems as to the planned activities.

Pursuant to Article 8 of u.w.r., a local or regional government entity entrusting a telecommunications company with the performance of activities resulting from Article 3 section 1of u.w.r., in the event of the economic conditions' not enabling the company to perform financially profitable telecommunications activities in a given area, may: 1) provide a telecommunications company with telecommunications infrastructure or networks in return for charges lower than production cost; 2) co-finance the costs related to the provision telecommunications services to end users or telecommunications companies for the purpose of the provision of such services. A local or regional government entity entrusting a telecommunications company with the constructed telecommunications infrastructure or networks does not constitute a business activity[16]. The preferences arising from Article 8 of u.w.r. may apply only when conducting financially profitable business activity is not possible, as otherwise the competitiveness on the telecommunications market could be disrupted[17].

Article 8 of u.w.r. contains the rule that local and regional government entities shall not provide telecommunications infrastructure or network in return for charges below production cost, and shall not finance activities consisting of the provision of services to end users, except for situations in which, due to economic conditions, it is impossible to conduct financially profitable activities in a given field, and, with regard to financing, this must only entail the provision of telecommunications services to end users or the provision of services to telecommunications companies for the purposes of providing these services to end users[18].

Pursuant to Article 15 of u.w.r. local and regional government entities may carry out activities aimed at stimulating or aggregating users' demand for services associated with broadband Internet access[19], especially

16 Wyrok NSA z dnia 13 stycznia 2017 r., II FSK 2818/16, LEX nr 2227004.
17 M. Karpiuk, *Activities…*, s. 43.
18 Wyrok NSA z dnia 18 września 2018 r., II FSK 2423/16, LEX nr 2601705.
19 Internet access is considered broadband if the efficiency of the connection is not a factor limiting the possibility of launching applications available online, as per Art. 2 ust. 1 pkt 1 u.w.r.

educational and training services, consisting of providing consumers with telecommunications end devices or computer equipment, or funding telecommunications services for consumers. The governing body of a local or regional government entity specifies by way of a resolution the conditions and funding methods of such activities, in particular the conditions for qualifying the beneficiaries of the aid granted. The above-mentioned activities should be carried out in a non-discriminatory manner, in accordance with transparency and proportionality principles, and aim at maintaining technological neutrality. Each undertaking of a local or regional government entity carried out within the aforementioned activities requires a prior announcement, with a description, in a Public Information Bulletin on the website of the given local or regional government entity, and in its registered office. Local and regional government's efforts to increase residents' interest in broad access to the Internet, and ensuring such access, stimulates the activity of the community and contributes to the development of a given area.

Activities aimed at stimulating or aggregating user demand for services related to broadband Internet access cannot marginalise threats existing in cyberspace. A major role here is played by educational and training initiatives. The users of services associated with broadband Internet access must be aware of the mechanisms conducive to ensuring cybersecurity, i.e. protection from online threats. Local and regional governments have important tasks to perform in this regard as entities supporting the development of telecommunications services and networks.

Bibliography

Literature

Bożek M., Czuryk M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.

Bożek M., Karpiuk M., Kostrubiec J., Walczuk K., *Zasady ustroju politycznego państwa*, Poznań 2012.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.

Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.

Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.
Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016.
Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1.
Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.
Karpiuk M., *Cyfrowe transmisje radiofoniczne i telewizyjne i ich wpływ na bezpieczeństwo informacyjne* [w:] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014.
Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.
Karpiuk M., *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1.
Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1.
Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.
Karpiuk M., *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.
Karpiuk M., *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008.
Karpiuk M., *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Karpiuk M., Kostrubiec J., *Rechtsstatus der territorialen Selbstverwaltung in Polen*, Olsztyn 2017.
Karpiuk M., Kostrubiec J., *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.

Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Kostrubiec J., *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5.
Pieczywok A., *Cyber threats and challenges targeting man versus his education*, „Cybersecurity and Law" 2019, nr 1.
Zając P., *Classified Information and its Protection in Polish Armed Forces. General Assumptions*, „Teka Komisji Prawniczej. Oddział PAN w Lublinie" 2017, t. X.

Legal Acts

Traktat o funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. nr 90, poz. 864/2 ze zm.)
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2019 r., poz. 869 ze zm.).
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).
Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2019 r., poz. 2410 ze zm.).
Rozporządzenie Ministra Cyfryzacji z dnia 18 października 2018 r. w sprawie minimalnej przepływności łącza dla świadczonej przez jednostki samorządu terytorialnego usługi dostępu do internetu (Dz.U. z 2018 r., poz. 2087).

Rulings

Wyrok NSA z dnia 13 stycznia 2017 r., II FSK 2818/16, LEX nr 2227004.
Wyrok NSA z dnia 18 września 2018 r., II FSK 2423, LEX nr 2601705.
Wyrok NSA z dnia 18 września 2018 r., II FSK 2423/16, LEX nr 2601705.

Wspieranie rozwoju usług i sieci telekomunikacyjnych przez samorząd terytorialny a cyberbezpieczeństwo

Streszczenie

Szczególne miejsce w życiu publicznym zajmuje samorząd terytorialny. Wykonuje on we własnym imieniu i na swoją odpowiedzialność część zadań powierzonych przez państwo w drodze ustawy. Zaspokajanie zbiorowych potrzeb lokalnej lub regionalnej wspólnoty jest celem istnienia samorządu terytorialnego. Zaspokajanie potrzeb mieszkańców wymaga również działań w dziedzinie telekomunikacji, w tym wspierania rozwoju usług i sieci telekomunikacyjnych. Rozwój ten nie może być jednak pozostawiony sam sobie. Samorząd terytorialny z jednej strony ma go wspierać, z drugiej jednak ma chronić użytkowników usług i sieci telekomunikacyjnych przed cyberzagrożeniami. Cyberbezpieczeństwo musi zatem znaleźć odpowiednie miejsce w katalogu zadań samorządu terytorialnego, który nie może go marginalizować, ponieważ zagrożenia w sieci są rzeczywiste i mogące wyrządzić znaczne szkody, a nie wirtualne.

Słowa kluczowe: usługi telekomunikacyjne, sieci telekomunikacyjne, cyberbezpieczeństwo, samorząd terytorialny, infrastruktura telekomunikacyjna, internet

Kazimierz Pawelec*

Vehicle technical malfunctions and their impact on traffic safety

Abstract

Traffic safety is closely interrelated to the technical condition of vehicles participating in road transport. The said condition should be understood comprehensively, not only in terms of technical fitness, equipment, loading methods, and safe passenger transport, but also from the perspective of passive safety aimed at minimising the impact of accidents. Unfortunately, the issues of providing passive safety, and its deficiencies, are often neglected, yet it is also crucial to penal liability. It is certain that the deficiencies identified are part of cause-and-effect relationships which are very often difficult to define in a straightforward way.

Key words: Safety rules, active safety, passive safety, wilful misconduct, wilful negligence, joint liability, causal relationship

* Dr Kazimierz Pawelec, Department of Social Science, Siedlce University of Natural Sciences and Humanities, e-mail: pawelec.kancelaria@op.pl, ORCID: 000-0001-8669-0249.

In observing and studying practices in the field of the assessment of the technical malfunctions of vehicles, and their impact on the rates of accidents and other incidents referred to in Article 173 or 174 of the Polish Penal Code, it can be said that the views expressed by A. Gaberle[1] are still current. He wrote that a tendency could be observed, both in and outside Poland, to consider humans as the primary factors contributing to road safety hazards. Moreover, the cited author made germane observations stating "This can be substantiated by the basic situation for car accidents to happen, which is the fact of starting a vehicle by a driver. No accident can occur without such an action. Therefore, the approach involving examining whether human behaviour has produced such results, and taking other factors into consideration only after eliminating the human factor, is understandable". Hence, safety is of paramount importance here[2]. Such an approach puts the issue of perpetration first. It entails an assumption that the search for other causes can only begin after the possibility that the driver was in breach of the applicable road traffic rules has been eliminated. It seems reasonable to place a mandatory requirement on drivers to adapt their conduct to the existing

1 A. Gaberle, *Wypadki drogowe. Aspekty kryminologiczne*, Warszawa 1986, s. 172.

2 For detailed information on safety, see: M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2; M. Karpiuk, *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017; M. Karpiuk, *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1; M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017; M. Karpiuk, *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1; M. Karpiuk, *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.

conditions, and also those dictated by the state of their vehicles, which leads to the conclusion that vehicles should be designed and equipped in such a way as to minimise driver errors and to protect human life and health to the greatest extent possible if an accident or a disaster occurs.

Here it is worth taking up the important issue of the active and passive safety of the vehicle. Active safety, also referred to as primary safety, should ensure: 1) driving safety, entailing all the means which facilitate keeping vehicles in the right driving direction, 2) support for effective operation, and 3) reliability of perception. The factors of primary significance for safe driving include: vehicle efficiency, suspension, tyres, brakes, steering, and electronic support systems designed to warn about hazards, i.e. systems which help to prevent vehicles from skidding, to keep the right distance from other vehicles, intelligent speed assistance, etc.

In turn, operating safety includes the means to ensure sufficient driving safety, meaning technologies reducing unnecessary strain on the driver and helping to eliminate potential errors during vehicle operation. Passive safety entails technical equipment which prevents the occurrence of negative outcomes of accidents or other road incidents affecting vehicle drivers and passengers. These are, for example, design solutions which facilitate the reduction of kinetic energy from collisions with obstacles, devices designed to secure against falling out of vehicles, minimising the risk of injuries, and fire prevention solutions[3]. It can be assumed that drivers do not have any influence on a number of technical factors, aside from any technical failures which they can identify or failures which they are aware of. It is essential that drivers are conscious of the need to have the car serviced periodically according to instruction manual recommendations. It should be noted that specific fluids, for example brake fluid, tend to lose their properties after a certain period of operation, which can increase the risk of road traffic hazards. This issue is neglected, although it can be significant from the perspective of road safety.

Driving a vehicle which has technical malfunctions without doubt constitutes a violation of road safety rules. It can be intentional or unintentional[4]. This is closely related to offences referred to in Articles 173,174, 177, and additionally in Article 179, of the Penal Code. As regards the penal outcomes of such an action, they usually take the unintentional form (negligence), unless

3 A. Gaberle, *Wypadki*..., s. 184.
4 Postanowienie SN z dnia 8 marca 2017 r., III KK 345/16, LEX nr 2242366.

extraordinary circumstances occur in which the perpetrator can be found guilty of wilful misconduct with indirect intention, but only in relation to offences against Articles 173 and 174 of the Penal Code[5]. No penal liability may be imposed on a driver if a sudden and unexpected failure occurs, resulting in a road accident, disaster, or an immediate threat of an accident. This should be differentiated from the situation in which, for example, a driver knows about low air pressure in one of the tyres, and that he or she should not exceed a speed limit defined in a notice, or continue driving for more than a specified number of kilometres and disregards the warning and drives the car with excessive speed. This would mean that such a driver has wilfully violated road safety rules, and there are grounds for imposing liability for such actions.

The Road Traffic Act also includes procedural provisions which do not have a lot in common with safety rules. The breach of such provisions should not be linked with penal liability, even if it results in the committing of an offence under Articles 173, 174, and 177 of the Penal Code. Without doubt, traffic offences and misdemeanours are linked to the driver, and it is the driver who is obliged to adapt his or her driving to the road conditions and the technical state of the car. If significant technical deficiencies occur, this means negligence related to the technical state of the vehicle, which in certain circumstances is not necessarily incriminating, in particular where the driver involved, aware of the malfunction, takes reasonable steps to increase safety, by driving the vehicle in a special way, with reduced speed, greater caution, and by reasonably predicting the possible consequences of the existing malfunction[6]. The Supreme Court stressed "the obligation to predict the consequences of driving a vehicle with a defective assembly or component, affecting safe driving, may only be imposed if the driver could have predicted such a malfunction based on his/her work experience or knowledge of the technical properties of the vehicle in his/her possession[7]". Furthermore, in another judgement, the Supreme Court put forward the following thesis. "Driving a vehicle with a defective braking system is a violation of road safety rules, and consequently one of the substantive elements of the offence(...)" – a road accident[8].

5 More details in: K. Pawelec, *Sprowadzenie niebezpieczeństwa w ruchu drogowym*, Warszawa 2017, s. 25–48 together with the cited references and case law.

6 Cf.: K. Pawelec, *Na drodze*, Warszawa 1983, s. 69.

7 Wyrok SN z dnia 29 stycznia 1973 r., Rw 1421/72, WPP 1974, nr 1, s. 83.

8 Wyrok SN z dnia 27 lipca 1976 r., VI KRN 113/76, OSNKW 1976, nr 10–11, poz. 129.

It should be noted here that, as evidenced by practice, data on the number of road traffic offences resulting from technical malfunctions in vehicles can be highly unreliable. This can be attributable to the fact that it is easier and more convenient to assume that it was the driver who violated safety rules, usually by failing to keep at a safe speed or a safe distance from the vehicle in front of him/her, or by failing to give way, or to monitor the situation on the road properly, than to assess whether the vehicle was unfit for operation before the incident or the malfunction invoked or exacerbated improper behaviour[9].

The adoption of such reasoning without in-depth studies and analyses of non-thorough criminal proceedings can create a fiction which can prove dangerous, as can anything that blurs the actual course of events, or hinders the search for the real causes of road incidents, and thus their prevention. The author of the above statement wishes to place emphasis on the fact that computer systems currently in operation, which can be found in an increasing number of vehicles, help identify the actual technical state of the car, and inform the driver in a clear way that a malfunction or a defect has occurred, and whether it is safe to continue driving. Reading information encoded in controls, a one-off action which cannot be repeated in other circumstances, is not something of interest to law enforcement bodies, unless a VIP has taken part in a given accident. The reading of specified records would facilitate the assessment of the driver's conduct, including their relationship to the tool they were using and the tasks they were to perform, as A. Badrach pointed out, referring to the car[10].

It is necessary to think about whether the driver can be subject to penal liability for an offence involving putting other persons in danger because of defects or flaws identified in their vehicle, or vehicle defects in the field of active or passive safety, and the existence of a causal connection with injuries sustained by passengers which they would not have suffered if the passive safety systems had been in good working order. The aforementioned issues are significant, as they affect road safety directly, and encourage readers to generally reflect on the liability of other persons. Moving onto the discussion of issues related to the potential penal liability of drivers under Article 160 of the Penal Code, it is worth referring to the resolution of the Supreme

9 Cf.: A. Gaberle, *Wypadki*…, s. 182.

10 A. Bachrach, *Przestępstwa i wykroczenia drogowe w prawie polskim*, Warszawa 1980, s. 153–154; K. Pawelec, *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2016, s. 82–84.

Court, entered onto the rules-of-law register, in which the following opinion can be found. “Motor vehicle drivers who, by violating road traffic safety, put other individuals at risk of losing their life, or sustaining a severe injury or health impairment, shall not be held liable under Article 160 of the Penal Code”. However, in the statement of reasons, tempering the tenor of the aforementioned thesis, the Court stressed that the result entailing the potential occurrence of the said threats must be specifically proven or predictable with probability bordering on certainty[11]. For liability to be imposed, it is necessary to prove the occurrence of the result in the form of a potential threat to life or health, while such a threat must be specified and direct[12].

The last issue to discuss is essentially not noticeable in legal practice. It is the liability of a driver for the effects of his or her actions who has without doubt violated safety rules, but the vehicle driven by another traffic participant did not have functioning passive safety systems, of which the said driver had not been aware, and which he or she could not have controlled. He or she could not be held liable for the effects of an accident if, for example, the vehicle collided with did not have any air bags or safety belts, or the belts had not been fastened. The fact that the aforementioned devices were not in working order is not in causal relationship with the effects of the incident, because if they had been in working order, nothing bearing the traits of an offence would have occurred. Of course, no responsible expert witness would state a definite opinion on the issue, and for that reason unresolvable doubts would appear in such a matter which would have to be settled to the benefit of the perpetrator, and as a result the most favourable version would have to be accepted.

In one of the examined cases, a driver was accused of causing a road accident by failing to give way, and colliding with another vehicle, as a result of which the passenger of the other vehicle suffered rib fractures. The defendant agreed to voluntarily accept a penalty, following advice given by a police officer during the interrogation. the defendant’s submission to accept the penalty was approved by a public prosecutor, but the court had doubts. It was determined that the passenger in the front seat next to the other driver had been holding a crutch in front of him. As a result of air bag activation, the crutch fractured the passenger’s ribs. The passenger was not following the recommendations, and the driver agreed to that. The Court found that the perpetrator could not be

11 Uchwała SN z dnia 15 lutego 1977 r., VII KZP 22/76, OSNKW 1977, nr 3, poz. 17; glosa E. Szwedek, OSP 1978, z. 1, poz. 17.

12 Wyrok SN z dnia 15 listopada 2017 r., IV KK 293/17, LEX nr 2395394.

held liable for the accident because he had no influence on the aggrieved party's conduct, and could not have predicted that, and no such obligations could have been imposed on him. The defendant was indicted for a misdemeanour under Article 86(1) of the Misdemeanour Code, which was time-barred. The persons subject to joint liability for road traffic offences bearing specific results, i.e. acts under Articles 173, 174, and 177 of the Penal Code, may include not only other traffic participants, but also an extended number of persons, including those who are not participating in traffic but are responsible for its safety[13]. They are referred to in the judgement of the Appeals Court in Wrocław, in which the court applied the constructs of extended liability for a road accident[14] and wilful negligence[15] to a person responsible for occupational health and safety (Article 220(1) of the Penal Code) and certifying the roadworthiness of vehicles (Article 179 of the Penal Code). The application of the aforementioned constructs should not be accepted without any reservations in relation to penal liability towards a diagnostic technician, especially the liability for his or her failing to declare deficiencies in the vehicle's passive safety systems, as there are no legal instruments which would oblige the said diagnostic technician to reveal such deficiencies and take the appropriate legal steps. Therefore, appropriate legislative changes are necessary[16]. Practical measures will not provide a solution for the deficiencies, even if the construct of extended liability is applied similarly to the Appeals Court in Wrocław, which stated "The person responsible for the accident is not only the driver, but also every person who, in any form, expresses the view that the driver could operate the vehicle in violation of traffic safety rules, resulting in the circumstances referred to in Article 177(2) of the Penal Code. The liability of such persons is based on the construct of so-called 'extended perpetration'"[17].

13 Wyrok SA w Katowicach z dnia 26 stycznia 2018 r., II Aka 194/18, LEX nr 2645350; wyrok SN z dnia 15 listopada 2013 r., II KK 6/12, OSNKW 2013, nr 5, poz. 39; K. Pawelec, *Realizacja znamion przestępstwa dopuszczenia do ruchu pojazdu bezpośrednio zagrażającego bezpieczeństwu ruchu*, „Monitor Prawniczy" 2018, nr 21, s. 1166–1168.

14 Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 24 sierpnia 2016 r., II Aka 201/16, LEX nr 2115443. More details in: K. Pawelec, *Czynności niepowtarzalne w sprawach o wypadki drogowe*, Warszawa 2018, s. 214–219

15 More details in: K. Pawelec, *Czynności*…, s. 219–224.

16 See: D. Klewek, *Dopuszczenie pojazdów mechanicznych do ruchu i jego znaczenie dla bezpieczeństwa komunikacji drogowej*, Siedlce 2019, s. 27–28.

17 Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 24 sierpnia 2016 r., II Aka 201/16, LEX nr 2115443. More details in: K. Pawelec, *Sprowadzenie*…, s. 272–276.

Bibliography

Literature

Bachrach A., *Przestępstwa i wykroczenia drogowe w prawie polskim*, Warszawa 1980.
Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.
Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.
Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.
Gaberle A., *Wypadki drogowe. Aspekty kryminologiczne*, Warszawa 1986.
Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.
Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014; M. Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1.
Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2.
Karpiuk M., *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.
Karpiuk M., *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.
Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Klewek D., *Dopuszczenie pojazdów mechanicznych do ruchu i jego znaczenie dla bezpieczeństwa komunikacji drogowej*, Siedlce 2019.
Pawelec K., *Czynności niepowtarzalne w sprawach o wypadki drogowe*, Warszawa 2018.
Pawelec K., *Na drodze*, Warszawa 1983.
Pawelec K., *Realizacja znamion przestępstwa dopuszczenia do ruchu pojazdu bezpośrednio zagrażającego bezpieczeństwu ruchu*, „Monitor Prawniczy" 2018, nr 21.
Pawelec K., *Sprowadzenie niebezpieczeństwa w ruchu drogowym*, Warszawa 2017.
Pawelec K., *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2016.

Rulings

Postanowienie SN z dnia 8 marca 2017 r., III KK 345/16, LEX nr 2242366.
Uchwała SN z dnia 15 lutego 1977 r., VII KZP 22/76, OSNKW 1977, nr 3, poz. 17.
Wyrok SA w Katowicach z dnia 26 stycznia 2018 r., II Aka 194/18, LEX nr 2645350.
Wyrok SA we Wrocławiu z dnia 24 sierpnia 2016 r., II Aka 201/16, LEX nr 2115443.

Wyrok SN z dnia 15 listopada 2013 r., II KK 6/12, OSNKW 2013, nr 5, poz. 39.
Wyrok SN z dnia 15 listopada 2017 r., IV KK 293/17, LEX nr 2395394.
Wyrok SN z dnia 27 lipca 1976 r., VI KRN 113/76, OSNKW 1976, nr 10–11, poz. 129.
Wyrok SN z dnia 29 stycznia 1973 r., Rw 1421/72, WPP 1974, nr 1.

Niesprawność techniczna pojazdu i jej wpływ na bezpieczeństwo ruchu

Streszczenie

Z zapewnieniem bezpieczeństwa ruchu ściśle wiąże się sprawność techniczna pojazdów uczestniczących w komunikacji drogowej. Ową sprawność powinniśmy rozumieć szeroko, nie tylko przez sprawność techniczną, wyposażenie, sposób załadunku, przewożenia pasażerów, ale również z punktu widzenia bezpieczeństwa biernego zapewniającego zmniejszanie skutków wypadku. Niestety, problem zapewnienia bezpieczeństwa biernego, jego niedostatków umyka uwadze, a jest on niezwykle istotny również dla odpowiedzialności karnej. Wskazane niedostatki muszą się bowiem łączyć związkiem przyczynowym ze skutkiem, a powyższe wielokrotnie wcale nie należy do jednoznacznych.

Słowa kluczowe: zasady bezpieczeństwa, bezpieczeństwo czynne, bezpieczeństwo bierne, umyślność, świadoma nieumyślność, współodpowiedzialność, związek przyczynowy

Andrzej Pieczywok*

The use of selected social concepts and educational programmes in counteracting cyberspace threats

Abstract

This article demonstrates the importance of the aspects of social life which include prevention and education at all possible stages of using cyberspace. It encompasses a characterisation of the primary concepts and programmes associated with developing a sense of security in individuals in cyberspace. Focus was placed on major social and educational projects with an impact on security. The keynote of the article is that personal (individual) security, in addition to the sense of peace and stability and health security, have an essential impact on the sense of security of people using modern ICT technologies. All this is related to appropriate attitudes and experiences, at the same time defining the focus area for the responsible State bodies (services, organisations, institutions).

Key words: threats, cyberspace, security programmes and concepts, sense of security, education, cybersecurity

* Dr hab. prof. nadzw. Andrzej Pieczywok, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, e-mail: a.pieczywok@wp.pl.

Introduction

The issue of "individual security", which is increasingly often present in cyberspace, resonates in many discussions on modernity and changes in various domains of life. Concerns related to uncertainty and various related threats lead to an increased number of instances of addictions, aggression, violence, and brutality among people. It is increasingly common to see the reasons for the decline of the human condition, and people's willingness to close themselves in a world limited to their closest family and friends, or to themselves only. Such attitudes make it difficult to cooperate and be mutually responsible for oneself and for others.

Research carried out in recent years in Poland demonstrates a high level of fear of becoming a victim of crime[1]. As became apparent, almost 1/3 of Poles (30%) experience a fear of crime. Despite the favourable opinions of the work of the police, the Polish public, for fear of their own life and health, and the life and health of their closest family and friends, keep avoiding certain places, streets, parks, or squares. For this reason some Polish people avoid going out in the evenings for fear of becoming a victim of a break-in, assault, robbery, battery, or reckless driving. Another source of fear is the manifestations of aggression by alcohol and drug abusers, acts of vandalism, fights and batteries, and violent acts by adolescents[2].

Recently, new threats have emerged related to the organisation and functioning of individuals in public spaces. These include all types of anxiety accompanying individuals' activities in cyberspace and threats resulting from the development of technological civilisation. In the contemporary times it is possible to observe a demonstrable evolution of threats, among which the most oppressive are those arising from people's presence in cyberspace. They are a direct threat to an individual's personality and to society, impacting on the

1 More on the issue: A. Kossowska, *Uwarunkowania i konsekwencje lęku przed przestępczością* [w:] J. Królikowska (red.), *Problemy społeczne w grze politycznej*, Warszawa 2006, s. 191–194, A. Siemaszko (red.), *Geografia występku i strachu*, Warszawa 2007, s. 100; B. Hołyst, *Wiktymologia*, Warszawa 1997, s. 545.

2 The research carried out by J. Siemaszko shows that every fourth Pole (27%) feels unsafe during an evening walk, more than one third (36%) fear reckless drivers, assaults and robberies (24%), aggressive adolescents (24%), break-ins (23%), aggressive behaviour by alcohol and drug addicts (21%), fights and batteries (20%) [in:] A. Siemaszko (red.), *Geografia*..., s. 98, 102–103.

functioning of individuals, social groups, states and institutions, in particular economic and social[3].

People are currently spending a lot of time on contact with the media. Never before has the life of ordinary people been so dominated by the "realness" experienced through both the traditional media (television, the radio, the press, outdoor advertising, etc.) and the new media (the global information network, telecommunications, etc.). The paradox of the contemporary media is thus that as a result of an excess of out-of-context information and the fascination with the extreme and the unique, people are feeling lost, and actual knowledge of the world is declining.

Cyberspace is also used by terrorists as a tool for politically motivated activities. Due to controversies and problems with a clear-cut definition of cyberterrorism, it is difficult to uniformly classify specific examples of attacks as the results of terrorist activity in cyberspace. Many incidents for which the blame is placed on terrorists might be forms of vandalism, or acts secretly sponsored by or carried out with the silent approval of the State, which is, however, hard to prove.

In order to meet social expectations relating to an individual's security in cyberspace, it is extremely important to include not only acts meeting the definition of a crime but also all asocial behaviour. Based on an objective assessment of threats, a similar level of anxiety is felt by a person afraid of becoming a victim of a house break-in or a car theft, but also when experiencing aggression from individuals using modern ICT technologies.

Thus, the key issue is to prepare people to live in tolerance and respect towards others, to live in a safe society of the new digital era, the era of the information society, where hatred, violence, aggression and terror, are marginal and episodic.

In relation to the above, various educational and information concepts and programmes (projects) are gaining in significance, aimed at developing a sense of security in cyberspace. They largely contribute to delivering sufficient information on the consequences of risky behaviour, and develop crucial psychological and social skills (the ability to establish contacts with people,

3 See: M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018; J. Gierszewski, A. Pieczywok, *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018; A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa społecznego*, Lublin 2018; M. Karpiuk, *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.

coping with stress, solving conflicts, resisting pressures from the environment, etc.). They are based on the belief that people, especially the young, behave in a risky way because they do not know enough about the mechanisms and consequences of such behaviour.

The use of selected social concepts in developing an individual's sense of security in cyberspace

The major role in designing security[4] at the level closest to an individual is performed by two security entities, the first being the police and the municipal police, as institutions professionally trained in the field of threats to citizens' security.

The second security entity is the local community, i.e. citizens, such as the family, school, the media, social organisations, etc. The co-participation of the entity in the security of the State, society, social groups, and individuals in Poland is highly inadequate. Thus the continuation of the subject matter of the research is necessary, both in the diagnostic sense and for designing changes in order to increase security in cyberspace.

The basic category in the concept of preventing crime through designing secure spaces is "the defence space"[5].

4 More on security: M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2; M. Karpiuk, J. Kostrubiec, *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

5 More on defence: M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019; M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012; M. Karpiuk, *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017; M. Karpiuk, *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej*

The concept of the defence space has existed for over two generations. In both of these the defence space is especially strongly connected with the physical space. The elements of the concept of the defence space essential for its understanding include territoriality, supervision, access control, technical protection measures, level of maintenance, and support in its use.

For the defence space, supervision means primarily the performance of all activities such as observation, control, sometimes surveillance, and systematic and planned analysis of the movement of people in a specific territory or its surroundings. The essence of supervision is to "deter moving individuals from wrongdoing". Another element in the defence space is the control of access to it. This is undoubtedly one of the basic elements which can easily be assessed by a potential perpetrator or another person intending to commit an act of vandalism or theft. This is the type of entrance, fence, distance to be covered, by the possible perpetrators and many other features of the physical space impacting on the decisions of those potentially bent on theft or an act of vandalism. Depending on the type of defence space (private, semi-private, semi-public, public) access control is effective, i.a. through creating: 1) landscapes and physical environments delineating paths of pedestrian movement in the directions of popular locations; 2) public spaces encouraging, instead of discouraging, people to gather together; 3) limited access to internal areas or high-risk areas (such as car parks or rarely visited areas). These can often be achieved through physical barriers[6].

A. Urban points to the necessity of the local community's participation in creating its security, especially through preventive actions towards threats. "The security of the nearest environment, of children at school, on the way to school, citizens' security at home and during travel, during commuting, and in any other places, security in cyberspace, are more and more often challenges on which the satisfaction and development of society depends. The key to the delivery of these tasks in local communities is to include them in security-related activities. This is not about detaining perpetrators, as this is the task of

udzielana Policji, „Wojskowy Przegląd Prawniczy" 2018, nr 1; M. Karpiuk, *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4; M. Karpiuk, *Zadania i kompetencje samorządu terytorialnego w czasie stanów nadzwyczajnych* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017.

6 E. Szweda, *Bezpieczeństwo społeczności lokalnych. Najbliżej człowieka*, Warszawa 2016, s. 146.

specialised forces, but to take preventive measures stopping the committing of an offence or making it more difficult[7]".

An example of the concept of developing a person's security in cyberspace is the concept of "Social Eyes". According to J. Jacobs[8] describing the urban spaces in the United States: large city spaces, metropolitan areas, due to people's moving to the bedroom suburbs, were empty at night, devoid of the so-called social eyes, which created opportunities for offenders. Both J. Jacobs and other authors often refer to the idea of "Social Eyes" when discussing secure urban spaces. These are needed in every defence space, in each type of local community, in large cities and small towns, in estates, streets, in every village, every public and private space. "Social Eyes" notice every wrongdoing, threat, crime, and should be a source of information exchange and communication between individuals comprising smaller or larger local communities. "Social Eyes" are an opportunity for joint action by police and citizens to identify threats, counteract asocial behaviour, and exchange conclusions from the observation of the most challenging places in terms of people's security[9].

In his analyses A. Urban emphasises the significance of the so-called Nobody's Space, which facilitates asocial behaviour and crime, and is also present in cyberspace. Nobody's Space most often encompasses various areas of the public and semi-public space which do not receive due attention from the institutions managing them. These include uninhabited buildings, access roads to them, areas around them, vandalised entrances, and other elements, as well as illegal websites. The fact that these spaces become spaces for crime, such as thefts and assaults, is often confirmed in our reality. Neglected public and semi-public spaces are a danger to the even the best maintained, usually private, spaces. Developing secure spaces is connected with clearly defining the above-mentioned divisions into private, semi-private, semi-public, and public areas. These areas in the local security dimension should also have their "supervisors", residents in charge of them, or having the sense of responsibility for them[10].

7 A. Urban, *Wpływ ukształtowania przestrzeni publicznej na bezpieczeństwo społeczności lokalnych*, „Zeszyty Naukowe AON" 2012, „Dodatek", s. 11.

8 J. Jacobs, *The Death and Life of Great American Cities*, Random House Inc, 1992.

9 E. Szweda, *Bezpieczeństwo*..., s. 154.

10 A. Urban, *Wpływ*..., s. 104. More on the local security system: M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2; M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1;

The connection between the place of residence, everyday life in a specific area, and a person's security, was discussed by J. Pałkiewicz in his publication Dżungla miasta. Klucz do bezpieczeństwa[11]. According to the author, the major challenge in understanding threats to people's security is the contemporary urban space.

Security in the closest environment of a person is a particularly broad topic in social practice. Its condition is visible everywhere, especially, according to J. Pałkiewicz, in "the city jungle"[12]. Introducing the reader to his extraordinary publication, to the world of security challenges and threats faced by people, the author of the "city jungle" concept states "I am far from spreading fear psychosis, but the spread of threats in the contemporary world forces us to apply preventive and protective measures[13]". He wrote his compendium of knowledge with the deep conviction that it would be useful in such events as accidents, natural disasters, terrorist attacks, environmental contamination, fire, theft by a pickpocket, and any form of aggression. Perhaps it can protect people from fear, pain or even death.

J. Pałkiewicz states, among other things, "Large metropolises are considered the most dangerous jungles on our planet"[14]. Presenting "the panorama of the threats of the concrete jungle", he describes the public space: urban transport, taxis, the underground, bicycles, lifts, beaches and swimming pools, parks, the cinema, concert halls, stadiums, public buildings, demonstrations, riots, street fights, bad dogs, drugs, weapons for personal use, credit cards, and ATMs. He also identifies threats in the following types of offence: violence, pickpockets, car theft, plunder of apartments, snatching purses, rape, sexual abuse, stalking, fraud, forgery, fake products, pestering and aggressive beggars, usury, blackmail, kidnapping, homicide, international terrorism, bomb attack, plane hijacking, violence towards minors, cybercrime, identity theft[15].

M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016; M. Karpiuk, *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.

11 J. Pałkiewicz, *Dżungla miasta. Klucz do bezpieczeństwa*, Poznań 2013.

12 Ibidem, s. 14.

13 Ibidem, s. 13.

14 Ibidem, s. 39.

15 Ibidem, s. 36–37.

The concept of "human security" is evidently present both in the literature in the field of security sciences and in the works analysing the gamut of security issues, in various dimensions and scientific disciplines[16].

The security subject in this concept is the person, who, as a "social entity", co-creates various social groups and structures. Security in the nearest environment of a person can also mean that the main two trends in the "human security" concept, i.e. the broad and the narrow approaches, take this nearness into consideration. The broad approach, based on the Japanese school, in a concise interpretation, means "freedom from poverty", and the narrow approach, associated with the so-called Canadian school, means "freedom from threats"[17]. The goal of the analyses and the possibilities for applying the human security concept to security in the nearest environment of people is to regard it as a crucial theoretical construct for such security subjects as individuals and local communities.

The concept of human security relates to the global level, as sustainable development with the participation of the people of the world is supposed to form the basis for security, and, conversely, the very concept of human security is to be the source of understanding and the necessity for sustainable development. In social practice, realising this interdependence should take place not only on the basis of the directive on its adoption by particular States but also by multidirectional education, from a single individual in his/her environment to education in schools and universities, in all possible forms[18].

16 See, e.g., M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017; M. Karpiuk, *Zadania administracji publicznej w zakresie bezpieczeństwa społecznego dotyczące wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych i odnoszące się do systemu pieczy zastępczej*, „Społeczeństwo i Rodzina" 2018, nr 3; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3; M. Karpiuk, *Pomoc społeczna jako instytucja umożliwiająca rodzinom przezwyciężanie trudnych sytuacji życiowych i jej miejsce w sferze bezpieczeństwa socjalnego*, „Społeczeństwo i Rodzina" 2017, nr 1; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.

17 K.P. Marczuk, *Bezpieczeństwo wewnętrzne państw członkowskich Unii Europejskiej. Od bezpieczeństwa państwa do bezpieczeństwa ludzi*, Warszawa 2012, s. 18.

18 E. Szweda, *Bezpieczeństwo*…, s. 132–133.

Another concept is the so-called broken windows theory by James Q. Wilson and George L. Kelling[19], which sees the problem not in the essence of spatial solutions, but in space maintenance and management. The creators of the theory demonstrate that signs of vandalism and aggression which are not removed lead to the intensification of the problem, as they create acquiescence for further wrongdoing. The theory had a great impact on the concomitant concepts and measures aimed at removing the signs of vandalism, for instance through the creation of the "Quality of Life" programme for New York, implemented by William Bratton. In Poland the action is known under the name "Zero Tolerancji (Zero Tolerance)", and focused on immediate reaction and the lack of social consent to any forms of aggression.

The preventive value of educational programmes in developing an individual's sense of security in cyberspace

Two of the important theories and practices relating to developing human security in cyberspace are educational and preventive programmes.

One of these is undoubtedly the "Razem Bezpieczniej (Safer Together")project, which has been implemented by the Polish Government for many years now. The major areas with an impact on ensuring security and maintaining public order include: security in public places and in the place of residence, security at school, preventing domestic abuse, security on public transport, security in road traffic, security in business activities, and national heritage protection.

The analysis of the Razem Bezpieczniej programmes indicates that in accordance with the Polish Government's intention, it is being implemented by all 16 provinces and numerous district and communes, for which joining the programme is voluntary. Each province, with the participation of district and communes, has its own rules and regulations, schemes, work plans, and teams coordinating this Governmental project.

The entities carrying out research projects as part of this programme include in particular local government entities, and also non-governmental

19 B. Czarnecki, W. Siemiński, *Kształtowanie bezpiecznej przestrzeni publicznej*, Warszawa 2004, s. 16–21.

organisations, bodies ensuring public order, commune organisational units, and other institutions. Projects were most often implemented in the following areas: cities, districts, communes, provinces, estates, groups of communes, and groups of estates. The research report contains an analysis of tasks carried out as part of the respective subject areas.

The most popular was the "Secure School" area. The list of project activities mainly covered these fields: 1) supplementary classes for children and adolescents; 2) educational meetings, e.g., with police officers, with offenders; 3) creating or developing a video surveillance system.

Among many other activities as part of the "Secure School", the authors of the report also mention various infrastructural investment projects, teacher training, workshops for parents, competitions, festivals, tournaments, first aid courses and purchasing related equipment, and information campaigns on preventing pathological behaviour and violence in cyberspace.

The priority issues included in the "Secure School" projects were: 1) a low sense of security among learners; 2) aggression between learners; 3) the lack of space for spending free time.

The subject area with the second largest number of projects was "Domestic Abuse". As part of this area there were a number of projects regarding security and the sense of security. The most frequently implemented activities under these projects included psychological and legal assistance, as well as workshops aimed at breaking the silence on crime in cyberspace.

One of the best known programmes focusing on the security of city residents is the "Programme for Improving Security – a Secure City". The Act of 5 June 1998 on district local government includes local government bodies in activities supporting the counteracting of threats by obliging them to perform supra-commune public tasks in the area of public order and the security of citizens. The conditions for local government bodies' involvement in activities to ensure security are also created by other Acts (e.g. the Act on commune guards) and Acts of local law forming specific strategies, programmes, and creating local agreements aimed at improving the effectiveness of activities in the area of maintaining public order and security in general. Motivating numerous entities to cooperate and coordinate their activities as part of a consolidated objective must bring the desired effects, and will constitute substantial support for the operations of the police and other forces in charge of security. It is also necessary to ensure permanent cooperation mechanisms between the police, the central and local government administration, social organisations, and active citizens, in order to improve the level of security.

It is worth mentioning the "Sector" preventive programme, which defines implementing and partnering entities, provides a characterisation of threats in the centre of Warsaw, divided into threats within the area of the local Warsaw I Police Headquarters and the Railway Station Police Headquarters in Warsaw. Furthermore, the programme identifies measures taken before its implementation at the initiative of the Security and Crisis Management Department of the City of Warsaw, the assumptions, manpower and resources, tactics and tasks, the organisation of command and communications, effectiveness measures, actions correcting the found transgressions and departure from the planned directions, and also the motivation system and supervision over the programme's implementation[20].

On the basis of the characteristics of threats occurring in the centre of Warsaw, an action plan will be developed as response to the least socially accepted criminal activity and methodologies, which might also be connected with cyberspace threats. It was found that Warsaw's stations are often opinion-forming places, both in terms of the evaluation of security and order in the city and shaping the opinion of foreigners, e.g. tourists, on the city. It was assumed that material property theft, including pickpocketing and luggage theft, robberies and extortions by force, and fights and batteries, have the greatest impact on the sense of security of citizens. Furthermore, the area was a major place frequented by individuals from the environment associated with drug-related crime. Their activities also had an impact on the crime rate and public order disturbance. Changes to the local infrastructure were also taken into account[21].

Another informational and educational programme with an impact on the security level of residents is "The District Programme of Preventing Crime and Facilitating Public Order and the Security of Citizens", whose main goal is to increase the actual security of the district's residents. This goal can be reached if the entities participating in the programme are actively involved in implementing the programme assumptions and tasks, covering the following issues: 1) limiting the crime rate and the number of threats in cyberspace; 2) raising the sense of security in public places and places of residence; 3) improving the image of institutions dealing with ensuring security; 4) preventing social pathologies as criminogenic phenomena, e.g. alcohol and

20 T. Serafin, S. Parszowski, *Bezpieczeństwo społeczności lokalnych. Programy prewencyjne w systemie bezpieczeństwa*, Warszawa 2011, s. 266–267.
21 Ibidem, s. 268.

drug abuse, domestic violence; 5) raising the level of security and quality of life; 6) increasing security in transport and road traffic.

Preventive measures carried out in schools employ individual preventive programmes implemented regardless of the current curriculum. Most often these programmes cover the following thematic sections: the integrative section, the section on healthcare, psychological and the social aspects of risky behaviour (the use and abuse of alcohol or other intoxicants, aggression or early sexual activity, the mechanisms of developing disorders, etc.), the section on psychological skills (e.g. the ability to cope with stress and tension through relaxation exercises, the ability to make decisions), the section devoted to developing the ability to use the Internet safely, the section on social and interpersonal skills (e.g. the ability to establish and maintain positive, satisfying, contacts with others, solving conflicts, resisting peer pressure, the ability to say no).

In conclusion, it must be stated that the characterised (selected) concepts and programmes for preventing crime in cyberspace and protecting the security of citizens and public order are aimed at seeking and implementing effective prevention forms and methods in order to increase the sense of security, breach the barrier of fear, and, in consequence, creating secure spaces.

It should be emphasised that every educational concept and (preventive) programme with an impact on developing the sense of security of individuals in cyberspace should have an open form based on voluntariness and transparency.

Bibliography

Bożek M., Karpiuk M., Kostrubiec J., Walczuk K., *Zasady ustroju politycznego państwa*, Poznań 2012.

Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

Czarnecki B., Siemiński W., *Kształtowanie bezpiecznej przestrzeni publicznej*, Warszawa 2004.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.

Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016.

Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1.

Gierszewski J., Pieczywok A., *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018.

Hołyst B., *Wiktymologia*, Warszawa 1997.
Jacobs J., *The Death and Life of Great American Cities*, Random House Inc, 1992.
Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.
Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.
Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1.
Karpiuk M., *Pomoc społeczna jako instytucja umożliwiająca rodzinom przezwyciężanie trudnych sytuacji życiowych i jej miejsce w sferze bezpieczeństwa socjalnego*, „Społeczeństwo i Rodzina" 2017, nr 1.
Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.
Karpiuk M., *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.
Karpiuk M., *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania administracji publicznej w zakresie bezpieczeństwa społecznego dotyczące wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych i odnoszące się do systemu pieczy zastępczej*, „Społeczeństwo i Rodzina" 2018, nr 3.
Karpiuk M., *Zadania i kompetencje samorządu terytorialnego w czasie stanów nadzwyczajnych* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Kostrubiec J., *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.
Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Kossowska A., *Uwarunkowania i konsekwencje lęku przed przestępczością* [w:] J. Królikowska (red.), *Problemy społeczne w grze politycznej*, Warszawa 2006.
Marczuk K.P., *Bezpieczeństwo wewnętrzne państw członkowskich Unii Europejskiej. Od bezpieczeństwa państwa do bezpieczeństwa ludzi*, Warszawa 2012.

Pałkiewicz J., *Dżungla miasta. Klucz do bezpieczeństwa*, Poznań 2013.
Pieczywok A., *Działania społeczne w sferze bezpieczeństwa społecznego*, Lublin 2018.
Serafin T., Parszowski S., *Bezpieczeństwo społeczności lokalnych. Programy prewencyjne w systemie bezpieczeństwa*, Warszawa 2011.
Siemaszko A. (red.), *Geografia występku i strachu*, Warszawa 2007.
Szweda E., *Bezpieczeństwo społeczności lokalnych. Najbliżej człowieka*, Warszawa 2016.
Urban A., *Wpływ ukształtowania przestrzeni publicznej na bezpieczeństwo społeczności lokalnych*, „Zeszyty Naukowe AON" 2012, „Dodatek".

Wykorzystanie wybranych koncepcji społecznych oraz programów edukacyjnych w przeciwdziałaniu zagrożeniom człowieka w cyberprzestrzeni

Streszczenie

Teść artykułu pokazuje jak istotnym aspektem życia człowieka jest szeroko pojęta profilaktyka oraz edukacja we wszystkich możliwych etapach korzystania z cyberprzestrzeni. Artykuł zawiera charakterystykę podstawowych koncepcji i programów dotyczących kształtowania poczucia bezpieczeństwa człowieka w cyberprzestrzeni. Skoncentrowano się głównie na najważniejszych społecznych i edukacyjnych projektach mających wpływ na bezpieczeństwo człowieka. Idea przewodnia artykułu dowodzi, że bezpieczeństwo personalne (osobiste, ludzkie), wraz z poczuciem spokoju i stagnacji oraz bezpieczeństwem zdrowotnym, mają zasadniczy wpływ na poczucie bezpieczeństwa człowieka korzystającego z nowoczesnych technologii komunikacyjno-informacyjnych. Wszystko to łączy się w przyjmowaniu odpowiednich postaw i odczuć wyznaczając jednocześnie obszar koncentracji działania w tym zakresie odpowiednich podmiotów (służb, organizacji, instytucji) państwa.

Słowa kluczowe: zagrożenia, cyberprzestrzeń, programy i koncepcje bezpieczeństwa, poczucie bezpieczeństwa, edukacja, cyberbezpieczeństwo

Małgorzata Polkowska*

Space Security Policy in Japan and Poland

Abstract

This article refers to the Space security legislation in Japan and Poland. Both states have already prepared some legislation on Security in Space- the question is the following- if there is still a need of progress and if those presented legislation are sufficient for the practical purposes of the peaceful uses of Outer Space. Japan is a much more experienced state in using space than Poland; the same seems with the legislation. Poland as less experienced state in this matter has lots of ambitions to create the efficient legislation on Space security, so it must follow the good examples of states and institution in this matter. One of them is Japan. On the other state, Poland as a Member of EU must implement the European law in space security (in particular SSA), which seems to be priceless and efficient for the international cooperation in Space.

Key words: space security, legislation, policy, Space Situational Awareness, strategy

* Dr hab. Małgorzata Polkowska, Professor at the War Studies University, Publication financed under the project implemented in the RESEARCH GRANT Program of the Ministry of National Defense Republic of Poland.

Introduction

Space security is a very important topic for every state which is engaged in space activities. That is the reason why states are engaged in preparing legal background referring to this important issue. This article presents space legislation from "space power state" as Japan is and Poland approaches to establish some rules referring to space security as well based on the EU framework.

The legislation history in Japan is quite long and impressive. Fifty years ago, in 1969, a plenary session of Japan's House of Representatives enacted the Resolution on Principles of Japan's Space Development and Utilization, which has shaped Japan's space programs for "peaceful purposes". A week later, the words "peaceful purposes" were interpreted to mean non-military and non-aggressive. This principle of "peaceful purposes" is slightly different from how the international community generally understands it. In general, most countries read "peaceful purposes" as non-aggressive, which allows them to acquire military capabilities and conduct military missions. However, the Japanese government decided to include the non-military principle on top of the non-aggressive principle because of Article 9 of the Constitution of Japan that prohibits the possession of war potential. Since the decisions made in 1969, Japan's space programs were limited to scientific purposes. Space was considered neither an economic resource nor a military resource – the Self-Defense Forces (SDF), Japan's military forces, had limited access to space systems. The government's interpretations and perceptions of the space domain did not change until the Basic Space Law (Act No. 43, 2008) came into force.

Space Law in Japan

The Basic Space Law is the first domestic law that stipulates the government's role in space development. The law established a Cabinet-level council that determines Japan's national space policy. Relevant ministries and agencies are forming their own space objectives and programs to meet the goals addressed in the national space policy. The law also represents a clear transition from the previous science-focused space policy. Nowadays, priorities include the commercial sector and national security. Other states are leveraging commercial sector capabilities to meet government demands. Japan is also

accelerating its efforts to utilize more commercially available technologies and services to realize government objectives. With respect to national security, the government currently has a legal basis to develop and utilize space systems for national security reasons[1].

The important players in national space activities are a few incorporated administrative agencies and some governmental ministries (such as Ministry of Education, Culture, Sports, Science and Technology – MEXT). Thus, an explanation of the framework of authorization, supervision and control exercised towards such agencies which have special relationships with the government is important for puroposes of understanding how to implement international space law in Japan[2]. They are responsible for preparing space policy and law.

Space Law Act was divided into few chapters, such as general provisions (Art. 1–12), basic measures (Art. 13), the master plan of the space (Art. 24), Space Development Strategy Headquarters (Art. 25–34, establishment of legislation on space activities (Art. 35) and supplementary provisions. This law is applicable to the development and utilization of space in accordance with the progress of Science and technology and other changes in domestic and foreign circumstances. It aims to promote comprehensive and systematic measures related to space development and utilization through the establishment of a system to contribute to the improvement of people's lives and economic and social development, as well as to contribute to world peace and the improvement of the welfare of humankind. The act refers to the peaceful use of space in accordance with the convention on the use of space development and other international commitments, such as the convention on the principles governing national activities in the exploration and utilization of outer space including the moon and other celestial bodies. The use of space development must be carried out to contribute to the improvement of people's lives, the formation of a safe and secure society, the elimination of disasters, poverty, and various threats to the survival and livelihood of human beings, the securing of peace and security of the international community, and the security of Japan.

1 T. Wakimoto, *A guide to Japan's Space Policy Formulation: Structures, Roles and Strategies of Ministries and Agencies for Space*, „A Working Paper on Japan's Space Policy" 2019, vol. 19, p. 10.

2 S. Aoki, *Regulation of Space Activities in Japan* [in:] R. Jakhu, *National Regulation of Space Activities*, Springer 2010, p. 201.

According to article 4, the utilization of space development must be carried out to contribute to the promotion of Japan's space industry and other industries by strengthening the technical and international competitiveness of Japan's space industry through the active and systematic promotion of space development and utilization, the smooth commercialization of the results of R&D (research and development) related to space development and utilization, and so on. Based on the fact that the accumulation of knowledge related to the universe is an intellectual asset for mankind, the utilization of Advanced Space Development and the promotion of space science should contribute to the realization of the dream of mankind to the universe and the development of human society. Art. 6 of the Space law refer to the international cooperation.

The Japanese government is responsible to formulate and implement comprehensive measures related to space development and utilization in accordance with the laws and regulations of Japan. In accordance with the basic philosophy (the Art. 9), local public organizations should establish and implement independent measures based on the characteristics of local public entities based on the appropriate role allocation with the national government in space development and utilization. The government also shall take measures necessary for strengthening the cooperation between the national government, local public organizations, universities, private enterprises, etc., to promote the space development and utilization effectively by cooperating with each other (Art. 10).

The second chapter of the Space law is reflected to the basic policy. There are provisions referring to the use of artificial satellites to improve people's lives. The state shall take necessary measures to ensure peace and security of the international community and to promote space development and utilization that contribute to the security of Japan. In order to promote the utilization of space and to strengthen the technological capabilities and international competitiveness of Japan's space industry and other industries, the Ministry of Land, Infrastructure, Transport and tourism will use the capabilities of private-sector businesses to systematically procure goods and services, and will conduct launch facilities (lockets) to enhance the technology and competitiveness of Japan's space industry and other industries. Art. 19 promotes of international cooperation in the field of space development and utilization.

The third chapter of the Space law is about the Basic Space Plan. The plan specifies the following items, such as: a basic policy on the promotion of space development and utilization, measures to be comprehensively and systematically implemented by the government concerning the

utilization of space development, matters necessary for the government to comprehensively and systematically promote measures related to space development and utilization. The plan is prepared by the Space Development Strategy Headquarters agreed by the Cabinet and the Prime Minister (who must make a public announcement of the basic plan without delay through the use of the internet and other appropriate means). In case to implement the plan, the right budget must be secured.

The fourth chapter of the Law refers to the Space Development Strategy Headquarters (with the Director General of the Space Development Strategy Division at the top), established by the Cabinet. They are responsible to promote the preparation and implementation of the draft of the basic space program. The government shall comprehensively, systematically and promptly implement the development of legislation on matters necessary to implement the convention on space activities and other international commitments concerning space development and utilization.

In supplementary provisions of the Space law there is also some provisions related to the Japan Aerospace Exploration Agency JAXA[3]. The government reviews the purpose, functions, scope of operations, the form of organization, and the administrative organs in charge of the agency, etc., with the aim of going forward one year after the enactment of this law[4]. Japan has managed to fundamentally reorient its space policy from fundamentally anti-military use to one that supports hard domestic national security and regional security goals. Japanese space policy is now specifically designed to support the US in the region. As late as 2012, JAXA, Japan's major space agency, was committed to expressly non-military space development. Yet, in 2016, it is actively developing space-based BMD early-warning technologies (Ballistic Missile Defense Systems), SSA architecture and tactical reconnaissance satellites. Even as a quick snapshot, these developments show how far the orientation of Japan's space program has changed in the last decade, a change that has been purposely accelerated over the last four years[5].

3 More about JAXA's projects (such as the Kounotori – a cargo transporter to the International Space Station), organization, research on space science and cooperation and other activities, see "JAXA – explore to realize" – brochure presented at Colorado Springs Seminar in April 2019.

4 www8.cao.go.jp (22.08.2019).

5 P. Kallender, *Japan's New Dual-Use Space Policy The Long Road to the 21st Century*, Center for Asian Studies, IFRI (Institute Français des Relation Internationales), November 2016, Asie. visions 88.

The Basic Plan on Space Policy

The Basic Plan on Space Policy is formulated to propel policies regarding Japan's space development and use, comprehensibly and systematically based on Article 24 of the Basic Space Law (enacted in 2008, Law No. 43), and is considered to be the most fundamental plan of space exploitation. National Space Policy Secretariat plans and designs policies to be incorporated in the Basic Plan, including those discussed in the Committee on National Space Policy[6].

This plan is the first of its kind since the establishment of a system for prompting Japan's space policy in an integrated manner, including the establishments of the Office of National Space Policy and the Committee on National Space Policy in the Cabinet Office. Japan has been faced with increasing demands for safety and security in light of the international situation, as demands for security including recovery from the Great East Japan Earthquake, establishment of a social and economic structure that can deal with huge risks, and strengthening of disaster management and mitigation.

The previous version of the Basic Plan on National Space Policy was laid out on the assumption of a budget of up to 2.5 trillion yen in five years from both the government and the private sector. The private sector has been unable to find sufficient private or foreign demand. It was decided that the government should promote the space policy under which going forward it focuses on the areas with high priority, instead of deeming every project as essential, in order to achieve maximum effectiveness under limited resources. In chapter 1 (Status of the Basic Plan on Space Policy and the New Structure) there is stated that the Basic Plan on National Space Policy is established as the plan at the most fundamental level for Japan's development and utilization of space according to Article 24 of the Basic Space Law (Law No. 43, 2008) in order to promote integrated and systematic measures for Japan's development and utilization of space. The Basic Plan on National Space Policy covers a five-year period. However, it should be reviewed as needed.

The Cabinet Office (1.3) has been assigned a commanding role in Japan's space policy by an amendment of the act (Law for Partial Amendment of the Law for Establishment of Cabinet Office) in July 2012. This enables the government to promote Japan's space policy in a more integrated and systematic manner.

6 https://www8.cao.go.jp/space/english/index-e.html.

The Cabinet Office is now responsible for coordination between agencies concerned, e.g. promotion of the development and utilization of space, and estimation of expenditures for the development and utilization of space. It is also responsible for administrative work of the development, maintenance and operation of satellites for public or official utilization in a variety of sectors, such as Quasi-Zenith Satellite System (QZSS), whose objective is satellite positioning, navigation and timing (PNT). The Office of National Space Policy is responsible for the project. Satellite positioning, navigation and timing involves many government agencies, such as the Ministry of Land, Infrastructure, Transport and Tourism; the Ministry of Economy, Trade and Industry; the Ministry of Agriculture, Forestry and Fisheries; the Fire and Disaster Management Agency; and the National Police Agency. Also, the private sector has created a variety of service industries that use data from positioning, navigation and timing satellites. Using GPS, for example, there are monitoring services for children and elderly people, logistics monitoring systems for food and other things, and financial transaction processing systems that use highly accurate timing information. So today, services that use GPS cover all around our daily lives. The QZSS can contribute to stronger international competitiveness of Japan's industries; increased efficiency in both industrial and government activities, as well as daily life; and to the enhancement of Japan's international presence, such as in collaboration with not only the United States but also Asia-Pacific economies[7].

Japan Aerospace Exploration Agency (JAXA)[8] has been positioned as the core organization that provides technical support for the entire governmental development and utilization of space projects. It is stipulated in law that JAXA's Mid-Term Goal should be based on the Basic Plan on Space Policy. JAXA is therefore supposed to make necessary contributions to the governmental space policies specified in the Basic Plan. On this basis, the Prime Minister, as the head of the Cabinet Office which is responsible for the administrative work for the promotion of space utilization, has now become one of the competent ministers of JAXA. In addition, JAXA has begun to do support work, such as giving advice to private enterprises upon their requests. Now the Prime Minister and the Minister of Economy, Trade and Industry play a major role in promoting industry through JAXA in cooperation with the Minister

7 https://global.jaxa.jp/article/special/michibiki/kunitomo_e.html.
8 https://global.jaxa.jp (12.01.2019).

of Education, Culture, Sports, Science and Technology and the Minister of Internal Affairs and Communications. Japan Space Agency JAXA is very active on ensuring stable use of outer space. JAXA focuses on the following objectives during the new starting period, in order to support the government and achieve its goals in the space policy to: 1) strengthen the cooperation with National Bodies of the national security affairs; 2) extend Japanese space activities and related business by developing new partnerships with private companies; 3) promote international space exploration program with Japanese space science and technologies with cutting edges; 4) strengthen the international competitiveness in next-generation aircraft engine.

JAXA promotes projects in consideration of four policies below: Secure national security and realize safe and secure society, expand utilization of space and industrial promotion, creation of world class results in space science and exploration fields, keep and step up presence of JAXA in the world and promote the aeronautical industry and strengthen international competitiveness.

Chapter 2 of the Basic plan states about basic policy to promote the development and utilization of space. Space utilization enables us to provide services covering an area beyond national borders and detect phenomena in a global scale. Due to such characteristics, space utilization is actively prompted across the globe both in national security and civil activities, particularly in the fields such as satellite navigation, communications (broadcasting) and remote sensing. It has become widespread in the society to considerable extent as an important social infrastructure. Since the 1990s, the space industry has experienced reorganization and rapid commercialization as a result of the decrease in military demands after the end of the Cold War. The utilization of space has expanded in the private sector, and the private-sector services are increasingly adopted to fulfill the demands of national security and other government-driven sectors. For example, Europe pioneered in public-private partnerships in the commercialization of space technology, while the U.S. decommissioned its Space Shuttles and now purchases commercial services for the transportation of crews and materials to the International Space Station (ISS).

The governmental investment for space development has been more focused on research and development (R&D) since 1990. As a result, the industry became over-dependent on the governmental investment in R&D, and there is a concern that may undermine the industry base, as seen in the withdrawal of some enterprises. Space utilization should be promoted hereafter in fields of critical importance to the industry and human life such as

meteorological and communications/broadcasting satellites. For this purpose, government-supported research and development should be conducted in a manner that outcomes of such research and technology contribute to sophistication and improved efficiency of the industry, administration and people's lives.

The measures and policies listed in the plan will be promoted in order to promote the development and utilization of space comprehensively and systematically. It's about implementation of the measures based on the Basic Plan on Space Policy, follow-up of implementation status and public and linkage with policies in other areas[9].

Japanese Space Security Policy

The basics of Japan's space policy are designed to achieve the following through the utilization of space in accordance with the idea of the Basic Space Law: (1) advancement and efficiency of the industry, human life and the administration, national security in a broad sense, and economic development (expanding the utilization of space); and (2) maintenance of Japan's capacity of autonomous space-related activities by preserving and strengthening the industrial base based on generated demands from the private sector (ensuring autonomy).

Utilization of space is one of the most important means to strengthen the capabilities of continuous surveillance of sea and air surrounding Japan, the detection of signs of events, and the prompt delivery (sharing) of obtained information. For Japanese sustainable space development, establishing the Space Situational Awareness (SSA) system for the purpose such as to protect satellites from possible collision with space debris (junk in outer space, called as debris) has been gaining importance as utilization of space is extended for both civil and military purposes.

Space security in Japan is crucial. The priorities are the following: to strengthen international cooperation between like-minded states for integrated SSA/SST (Space Surveillance and Tracking)/STM (Space Traffic Management), to foster commercial activities and deepen academia

9 https://global.jaxa.jp (12.01.2019).

collaboration for sustainable SSA/SST/STM and maximize the use of existing ground facilities of the like-minded countries for SSA/SST/STM network[10].

Japan's Basic Plan sets Space Policy's objectives, such as ensuring National Security in Space and strengthening of national security ability. JAXA's activities contribute to Basic Plan are: 1) contribution for Space Situational Awareness (SSA); 2) R&D for Space debris threats and risks; 3) support government in making international standards and regulations on space utilization.

JAXA is a big contributor to Space Situational Awareness. Their tasks are: to develop and operate JAXA's SSA related facilities and conduct, R&D[11] activities to advance our SSA abilities, upgrade our SSA related facilities and contribute to the intergovernmental operational framework by 2023 and integrated with MOD (Ministry of Defense) and other Japanese governmental institutions. JAXA is obliged to support the government for making international rules on the space utilization. JAXA leads Japan delegation for Japan in Inter Agency Space Debris Coordination Committee (IADC[12]). Based on R&D and the international technical trend, JAXA contributes for IADC and other international committee, UN/COPUOS, ISO and others. In R&D (research and development) for Mitigating Space Debris threats and risks, JAXA continue researches for observation, collision avoidance, protection and ADR, make space debris removal service into a new market and demonstrate the world's first active debris removal at low cost. JAXA is a partner with private sectors; by joint programs including research, ground testing, and demonstration in orbit and so on[13].

Due to the fact, that space debris is a major threat for operational satellites[14], JAXA started some researches on atmosphere. One of JAXA

10 H. Yamakawa *Member of Committee on National Space Policy*, Cabinet Office, GOJ, Professor of Kyoto University, Symposium March 2018 Tokyo.

11 M. Matsuura, *JAXA's endeavor to SSA*, March 2nd 2017, Tokyo.

12 IADC- the Inter-Agency Space Debris Coordination Committee is an inter-governmental forum whose aim is to co-ordinate efforts to deal with debris in orbit around the Earth founded in 1993.

13 H. Yamakawa, *JAXA's Activities on Ensuring Stable Use of Outer Space*, Tokyo symposium, February–March 2019

14 M. Ohnishi, JAXA's debris removal program, JAXA has been promoting the comprehensive approach to space debris measures; Now JAXA focuses on the R&D for space debris removal in order to found the new enterprise. JAXA will proceed the R&D under the Industry-Academia-JAXA cooperation; Tokyo, International Symposium on Ensuring Stable Use of Outer Space, 28 February–1 March 2019; K. Yamanaka, Space debris research in JAXA, 1st of March 2019–JAXA continues researches on both technical and non- technical aspects. JAXA contributes continuously to the cooperation with international partners;

primary interests was how to increase the effectiveness of both of new SSA facilities. There are projects to be able to observe at least 10,000 objects, and obtain measurement data directly[15]. JAXA will also contribute to Japanese SSA activities by providing data with the future system as well as by supporting from a technical point of view. The development of the new SSA system is ongoing. Its operation is expected to start in 2023[16]. Implementation of basic plan on space policy and research and develop plan JAXA should change itself to an organization which leads society by science and technology and creates new values. JAXA promotes projects in consideration of 4 pillars below (secure national security and realize safe and secure society, expand utilization of space and industrial promotion, creation of world class results in space science and exploration fields, promote the aeronautical industry and strengthen international competitiveness). In 2017, MOD and JAXA concluded the partnership agreement which provides the framework of general cooperation concerning SSA. In the same year, ASO (Airforce Staff Office) and JAXA concluded another appendix to the agreement relating to design or construction of SSA system[17].

Space industrial basis is at stake. Industrial basis is essential for conducting space activities autonomously. The lack of foreseeability of investments led to continuous business withdrawals and made new entries stagnated into space industry. In new policy, growing importance of outer space for national security policy can be noticed. There is necessity to utilize space for the security area proactively based on the National Security Strategy (Advent of a new era for US-Japan space cooperation). There is lack of organic cycles among science & technology, national security and industrial vitalization – Insufficient efforts of R&D in use of space for security purpose and of making the most of outcomes of R&D in civil space areas for individual vitalization. Growing risks against stable use of outer space – increased number of space debris and growing threats of ASAT attacks; so there is a necessity to cope with such risks

JAXA will partner with private sectors in joint programs including research, ground testing, and demonstration in orbit etc. utilizing JAXA's experience and lessons learned; see more at: http://www.jaxa.jp/projects/ssa/.

15 S. Nakamura, *Research and Activities on SSA at JAXA*, Tokyo symposium, 8 March 2018.

16 S. Ogawa, *SSA activities at JAXA*, 28 February 2019, Tokyo symposium.

17 S. Yoshitomi, *SSA Capabilities and Policies in Japan, Space Situational Awareness Workshop: Perspectives on the Future Directions for j*, January 24–25, 2019.

sustainably and ensure stable use of outer space[18]. In 2017 budget plan half of percentage was sent to Ministry of Education, Culture, Sports, Science and Technology (MEXT); the rest to Cabinet Satellite Intelligence Center (CSICE) and Ministry of Defense (MOD)[19]. Those ministries are developing SSA related facilities. New system is being developed. It constantly monitors satellites of each countries and space debris, supporting safe operation of satellites, which strengthen system for collecting information of satellites.

JAXA contributes to space security with limited budget. Instruction by Prime Minister Abe (Excerpt)-16th strategic headquarters for space policy (12 December 2017) in recent years, as threat against the national security environment surrounding Japan increases, space security is extremely important. MOD and JAXA are cooperating. JAXA (Telescope Bisei, Control System, Space Radar Kamisaibarais) is sending to MOD (Surveillance Sensor, Operating System) the data obtained by sensors and MOD data utilized for research purpose. MOD is sharing data with the US. The discussions with France are ongoing.

In Space Security Maritime Domain Awareness (MDA) related ministries (National Security Secretariat, Secretariat of the Headquarters' for Ocean Policy, and National Space Policy Secretariat) are deepening study for utilization of comprehensive information of ships, aircraft, satellites and other vehicles etc. In the Space Policy there is a target to strengthen the Space Security Domain Mission Assurance. It can be done by preparations for developing measures, information sharing among ministries (threat & risk information sharing, interagency cooperation in emergency), implementation of vulnerability assessment (establishing of method of vulnerability assessment, related ministries conducting vulnerability assessment). The

18 H. Uchikura, *MOD'S SSA Project – Initiatives Taken by Koku-Jieitai*, Tokyo symposium 2019; H. Takahashi, *Trend in Military Satellite Communications*, Tokyo symposium February 2018.

19 MOD (Koku-Jieitai-Japan Air Self Defense Force) cooperates with the US Forces in SSA domain; the more value of use of space, the heavier dependence on the domain- the greater reliance on space, the more serious consequences if the use is impeded. [National Defense Program Guideline]; Defense Capability is the ultimate guarantor of its security, Priorities in strengthening Defense Capability means acquiring and reinforcing space capability [Mid Term Defense Program]; Acquiring and reinforcing capability to ensure stable use of space; Acquiring and reinforcing capability to continuously use space; Koku-Jieitai will contribute to safety, stability, prosperity and development of the human society by collaborating and cooperating with national related ministries, the ally and partners; acquiring and reinforcing space capability; ensuring stable use of space. See more at H. Sugai, *Toward Acquiring and Enhancing Space Capability*, Tokyo seminar 2019.

measures for Strengthening Mission Assurance are: Construction of resilient system (Diversification, proliferation), Defensive operations (SSA etc.) and Reconstruction after incident. Strengthening Space Technologies & Industries can be achieved by promotion and enhancement of civil space industries, development and utilization of new space technologies (ex. responsive small satellite and launch system); Ensure supply chain of space system (i.e. components and parts); Government procurements in space industries, Supporting companies reaching out to overseas markets.

Space Domain Mission Assurance is the first priority in space policy. Space Domain Mission Assurance (assuring the ability to achieve the objective of continuous and stable use of relevant space systems by detecting and avoiding threats and risks, strengthening the resiliency of systems, and early recovery of functions in the event of a situation where threats and risks related to space systems have been actualized). Space Domain Mission Assurance is: Defensive Operations (Strengthening threat and risk detection, timely provision of warning, strengthening and operational ability), Resilience (Protective Measures, Distribution of Equipment and Redundancy of Means) and Reconstruction (System recovery, Substitute systems)[20]. The future challenge is to strengthen collaboration towards integration of space, cyber, and intelligence.

Japanese Space industry

The development and utilization of space in Japan have already become common as an indispensable basis for everyday life. Examples include: weather forecast with meteorological satellites[21]; data communications

20 S. Takada, *Space Policy of Japan*, March 2017, Japan Forum February–March 2017.

21 M. Ishii, *Research and Operation of Space Weather forecast in Japan*, Tokyo symposium 2018; National Institute of Information and Communications Technology (NICT) is involved in Space Weather researches (SWE). It is eagerly required to estimate the quantitative social impact of SWx. Some national governments (e.g., US, UK, Korea), international organizations (e.g., ICAO), and private companies (e.g., Lloyd) reported documents related to SWx disaster and mitigation. NICT has been operating space weather forecast since 1988 and improving the precision of the forecast using cutting-edge technology. The framework of space weather services has been assigned in the thematic priorities of UNISPACE+50. This frame work should be required also in the operation of ICAO space weather centers. Many of Asian countries are aware of the importance to measure space weather and are interested in working for space weather service. A decade ago the ground based observatories had clustered on developed countries. Now we are on the phase to spread the points all around the world. We need to discuss the necessary tasks and strategy

and broadcasting via dedicated satellites; cartography, resource survey, agriculture, forestry, fisheries, and disaster monitoring in conjunction with land and ocean observation satellites; car navigation and geographical survey with GPS. However, applications other than those examples are still in the first stage. It is an urgent issue to exploit the maximum potential of the utilization of space in order to upgrade and streamline the industry, human life and the administration as well as to improve disaster management etc.

An important target is to develop the industry. Space industry is an important base for the national space activity. It is a promising source of innovation due to its aggregation of cutting-edge technologies and the wide range of supportive industries, which is expected to bring about far-reaching spin-off effects on the whole industry and significant economic effects. The space industry also has connections with the service industry through communications/broadcasting, map services using satellite imaging and positioning services, such as navigation. The current financial stringency limits the government to support the space industry with sufficient procurement orders. Some private surveys indicate that the sales and number of employees of the Japanese space industry is currently about 260 billion yen and 7,000 workers, respectively, down from over 350 billion and nearly 10,000 in the latter half of the 1990s.

A key factor for sustaining and strengthening the industry base of Japan is the growth of the Japanese space industry through satisfying the private and overseas demands in global competition. Promotion of international cooperation is crucial for the Japanese government. Japan has been active in addressing international issues through Group on Earth Observations (GEO), Asia-Pacific Regional Space Agency Forum (APRSAF), Sentinel Asia, and the Charter on Cooperation to Achieve the Coordinated Utilization of Space Facilities in the Event of Natural or Technological Disasters. For example, data from the Japanese satellites Himawari and DAICHI etc., have been provided for meteorology, disaster monitoring or climate change projection in Asia. Along with the participation in the ISS project and other space science and space exploration activities, Japan has built strong ties with other leading countries in space development and these performances have contributed to securing Japan's presence in the international scene.

how we drive the stream, for example, presentation to the decision-maker of the budget, education for glow up the next generation researchers/operators, framework of data sharing etc.

Development and utilization of space require a considerable amount of funds for developing and launching satellites. Since it is not realistic for Japan solely to cover the entire cost of such expensive programs, international cooperation and role sharing, as in the ISS project, are very important in order to cultivate a good international relationship that will realize effective utilization of space. For example, the Japanese remote-sensing satellite systems can be introduced to Asian and other emerging states where disaster management and monitoring are highly needed. A harmonious relationship beneficial to both Japan and a partner can be established through the joint operation of satellites and data sharing.

There is an increasing trend of taking into consideration the utilization of outer space for national security in foreign countries. In major countries of the world, information gathering based on remote sensing, satellite communications, satellite navigation and other practical applications of outer space for national security has been widely adopted and therefore, Japan considers also proper measures. In every country, there is an active effort toward establishment of cooperation with other countries despite severe finance constraints. Thus, the government takes part in the discussions about measures against debris, Space Situational Awareness (SSA) and other programs. There is an obligation to present a 5-year development and utilization plan for the national security of Japan, utilization of space serves as an effective means, and it is especially essential for the enhancement in interpretation of information, information sharing, and command and control means[22].

International law and space diplomacy

Japan's contribution has been highly regarded by the international community, and it should utilize such recognition as a diplomatic asset in order to conduct "space diplomacy". Japan's international activities should not be limited to responding to requests from other countries but should involve efforts to build frameworks for mutually beneficial cooperation with partner countries, including support for overseas expansion of Japan's space-related businesses and industrial cooperation.

22 https://www8.cao.go.jp/space/english/index-e.html (11.11.2019).

An important issue on the global level is the establishment of international rules concerning utilization of space in order to ensure stable and sustainable space environment. In addition to the discussions at the Committee on the Peaceful Uses of Outer Space (COPUOS) and Conference on Disarmament (CD) in Geneva, Japan has to make a major contribution to the establishment of appropriate rules on utilization of space in both civil and national security sectors, such as an International Code of Conduct for Outer Space Activities proposed by EU.

Next target of the space diplomacy is the environment. From the viewpoint of friendliness to the global environment, space programs for effective and efficient solution of global environmental problems, such as climate change, are important. From the viewpoint of friendliness to space environment, prevention and reduction of space debris are important issues for space development and utilization. Some upper stages of launchers and fragments of decommissioned satellites remain on their orbits as space debris and may collide with satellites to cause heavy losses.

A large amount of debris was produced due to the experimental destruction of a man-made satellite with a ballistic missile by China in January 2007 and the collision between U.S. and Russian satellites in February 2009. It is expected that the number of debris particles will increase in a chain collision between the particles. Japan has proposed this concept to ASEAN states[23] in 2011 in order to enhance disaster response capabilities of the region through sharing disaster risk information obtained with satellites. Japan contributes to disaster monitoring and response in the whole ASEAN region via cooperative operation of satellites.

Japan prepared in G7[24] the statement on Non-Proliferation and Disarmament, (Hiroshima, in April 11, 2016). The statement is pointing out the need to evolve and implement principles of responsible behavior for all outer space activities in a prompt and pragmatic manner. It calls for taking appropriate measures to cooperate in good faith to avoid harmful interference with outer space activities. It suggests refraining from any action which brings

23 As of 2010, the Association of Southeast Asian Nations (ASEAN) has 10 member states, one candidate member state, and one observer state. ASEAN was founded on 8 August 1967 with five members: Indonesia, Malaysia, the Philippines, Singapore, and Thailand.

24 G7-The Group of Seven (G7) is an international intergovernmental economic organization consisting of the seven largest IMF – advanced economies in the world: Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

about damage, or destruction, of space objects and implementing TCBMs, such as information exchange on space policies, information exchange and notifications related to outer space activities in a timely manner and an effective consultation mechanism.

Other Japanese initiatives The "Outline of Basic Objectives for Capacity-Building with regards to Developing Countries in the Space Field" has been announced in December 2016. Japan calls for continuing to support and utilize the Asia-Pacific Regional Space Agency Forum (APRSAF) and other dialogues to address Japan's initiatives. There is a need to establish an integrated, harmonized, and comprehensive Space Traffic Management system is a very important challenge for future space activities. At present, developing rules regarding on-orbit space activities is a most urgent priority, in light of the clear threats of increasing space debris and orbital congestion. It is very important for policy makers to build consensus on some basic principles for outer space activities, which can form the basis for "technical and regulatory provisions", meanwhile experts from related fields keep on analyzing these issues. Japanese policy makers must always take into consideration the possibilities of innovation caused by new technologies or business models, which can give birth to new types of space activities, as well as new tools for verification[25]. STM issue can be connected with broaden issue, such as global space governance[26].

In addition to the countermeasures by the government, relevant agencies have to take appropriate measures from the standpoint of civil use, diplomacy and national security. The space development and utilization for national security are conducted in accordance with the Basic Space Law, international agreements concluded by Japan and principle of pacifism enshrined in the Constitution of Japan, in the light of the situation in Northeast Asia. Their main purpose is the enhancement of information gathering, surveillance and communications capabilities that will contribute to Japan's national security. It is important for JAXA to make contributions to the utilization of space for national security, because its objectives were updated in the 2012 amendment of the act (Law of Partial Amendment of the Cabinet Office Establishment Law).

25 A. Saito, *Japan's efforts for the rule of law in outer space – STM perspectives*, Tokyo, March 2nd 2017.

26 K. Suzuki, *How to Establish Space Governance?*, Tokyo symposium 2019.

Amendments of the Basic Plan for Space Policy

Japan changed its governmental structure in promoting space policy in 2012. But due to the shortage of materials translated into English, it seems not to be broadly known internationally about the Japanese government's space activities including governmental structure and behavior. The US system for developing space policy is more visible than Japan. This is beneficial for the space communities, including space industries, to anticipate what will happen in the near future. If the plan can't be implemented as initially planned, changes and actions tend to occur in space-related sectors. This seems to contribute to the active movement of US space communities.

On the other hand, Japan does not publish a new policy until the resources that are needed to execute the plan are prepared. It takes more time than the US government, but the Japanese government makes sure that the policy will be executed. This mechanism contributes to increased reliability of the Japanese government, and it is beneficial international cooperative projects like International Space Station and other space exploration efforts. Also, Japan started an effort to compile the roadmap of the Basic Plan on Space Policy in order to increase the visibility of governmental space activities for the space community, both domestically and internationally[27].

In January 2015, the new "Basic Plan for Space Policy" was determined. This policy sufficiently reflects the new national security policy. This policy is a long-term and concrete public activities plan for next 10 years and foreseeing coming 20 years. Comprehensive National Strategy is a first goal of Space Policy; the second is Space Policy Environmental Awareness surrounding Space Policy. There is a change in balance of power on space policy made by transformation from the US-Soviet bipolar structure to multi-polarized structure and by greater number of countries involved in space activities, and a corresponding growth in commercial space market.

In policy from 2015 the growing importance of the role of outer space to solve global challenges can be noticed. Global challenges such as energy, environment, food and natural disasters have come to the forefront and posing severe threats to the international community or necessity to contribute to solve global challenges using space systems are present. It can be also observed the growing importance of outer space for national security policy: necessity

27 www8.cao.go.jp.

to utilize space for the security area proactively based on the National Security Strategy and advent of a new era for US-Japan space cooperation.

This cooperation is crucial in SSA domain. SSA sharing agreements also allow the U.S. to share more information in a timely manner with the broadest range of partners. The U.S. aims to promote an interactive, exchange-based relationship with satellite owners and operators where all parties gain. This open exchange of information also supports efforts to detect, identify, and attribute actions in space that are contrary to responsible use and the long-term sustainability of the space environment. Sharing SSA information and collaborating with other nations and commercial firms promotes safe and responsible space operations. It reduces the potential for debris producing collisions and other harmful interference and builds international confidence in the responsible use of space systems[28].

The last Japanese Basic Plan, released on April 1, 2016, forges Japan's current national space policy. It is constituted by three goals: (1) ensure the security of outer space and national security through the use of space; (2) promote the utilization of space in the civil sector; (3) strengthen and maintain the competitiveness of the space industry as well as the science and technology foundation. A particular feature of the Basic Plan is that, since 2015, Japan's national space policy explicitly incorporates national security as well as industrial promotion. According to Defense Policies (as of January 2019) Japan's military space policy is formulated based on three national policies. The National Security Council (NSC) of Japan issues these policies. At the top of the hierarchy is the National Security Strategy (NSS) of 2013. The NSS aims to set comprehensive national security goals including energy, economic and military policies. Under this fundamental strategy, there is a long-term (about 10-year) defense strategy called the National Defense Program Guidelines for FY 2019 and beyond (2018 NDPG), which was amended in December 2018. The NDPG aims at defining the level of defense capability that Japan shall have to achieve the goals of NSS. More short-term goals (five

28 Space should be used for peaceful purposes so all can take advantage of the benefits that it brings to our planet. While we all continue to face new challenges in outer space, the space community must continue to work towards meeting these challenges through multinational collaboration. Speech presented at the Tokyo symposium by Col. Scott Trinrud, Tokyo, 2nd of March 2017. Despite governmental organization frameworks that appear almost same, the internal scheme of the development and implementation of space policy are different in the two countries. It is important for those studying national strategy to analyze each country's policy with this point of view.

years) are included in the Medium-Term Defense Program FY2019-FY2023 (2018 MTDP), which was also enacted in December 2018 to address major government acquisition plans and amount of equipment as well as estimated acquisition cost for the next five years. The 2018 NDGP objectives in space are built on previous NDGPs. The 2010 NDPG focused on establishing missile defense capacities and effective utilization of space-based ISR systems. The 2013 NDPG emphasized securing and protecting space assets by monitoring the space environment. Today, actual installation of SSA systems under the JASDF has been decided[29].

Poland in space security

Poland is not as experienced in space security as Japan. Poland is more active in space and legislation since the Polish Space Agency was created (POLSA). This Agency is a governmental executive body, subject to the Prime Minister. It consists of civilian and military personnel. It was established by the Act of 26 September 2014 and became fully operational at the end of 2015. The agency participates in fulfilling the strategic goals of the Republic of Poland by supporting the utilization of satellite systems and the development of space technologies. The main tasks of POLSA cover the following 5 areas: coordinating the activity of the Polish space sector on the national and international level, representing Poland in relations with international space sector organizations, supporting national science and business projects associated with space technologies, popularizing the use of satellite data by public administration and increasing the defensive capabilities of the country. The agency is executive in nature in accordance with the Act from 27 August 2009 in public financing (art. – Act of 26 September 2014) and it can create local branches of the agency. The headquarters of the Agency is located in Gdansk (Art. 3). The activities of the Agency are under the auspice of the President of the Council of Ministers (Art. 2). The duties of the agency are written in Article 3 of the Act. The President of the POLSA Council is composed of representatives of the government - one from each administration and four representatives of scientists and the industry with recognized achievements in research or business

29 T. Wakimoto, *A Guide to Japan's Space*..., p. 23–33.

and chosen based on their knowledge competence in areas concerning POLSA activities (Art. 14).

Polish Space law is still waiting for the Parliamentary approval. Several versions of the draft have been developed; at present, the Government Legislation Centre website has published a draft law on space activities and the National Register of Space Objects. The Act regulates: the rules of performing space activities and the rules of maintaining the National Register of Space Objects. Earlier, however, the amendment of the Act on POLSA will be processed. The changes proposed in the draft act are aimed at: to streamline and clarify the scope of tasks of the Polish Space Agency, as an executive agency to provide the necessary expert support and technological knowledge to other public administration bodies involved in space activities, and responsible for the preparation and coordination of the implementation of the National Space Programme; and to adapt the supervision of POLSA to the solutions in force in other European countries, especially in the Member States of the European Space Agency (ESA), as well as to introduce improvements in the organisation of POLSA.

Polish Space Strategy was published by the Polish Ministry of Economic Development in February 2017. The objectives are: increasing competitiveness of the Polish space sector and its share in turnover (increasing participation in the EU space programmes: SST Support Framework), Development of satellite applications, strengthening capacities in the area of security and defense using space (establishment of Space Situational Awareness System), creating favorable conditions for the development of space sector in Poland, building human resources for the Polish space sector. The Strategic issue is to obtain 3% of the EU market in 2030. National Space Plan (2019–2021) from 2018 states about the establishment, development and operation of a National Space Situational Awareness System (SSA) in cooperation with the EU SST consortium. The objective of the project is to enhance the security of citizens and infrastructure (Earth and space) in the context of space threats, to build national Space Situational Awareness (SSA) capabilities and to prepare for commercial exploitation of services provided in the area of SSA. The first stage of the activity is to launch basic functionalities of the national SST system (Space Surveillance and Tracking), inter alia, through the development of infrastructure and capabilities enabling the implementation of tasks envisaged within the framework of Poland's future membership in the European SST consortium. 19th of December 2018– Poland joined the

European SST Consortium related to the tracking of space debris threatening infrastructure in space and on Earth.

Poland has become a full member of the European Space Surveillance and Tracking Consortium. The accession agreement was signed on 19 December 2018 at the seat of the Polish Space Agency in Warsaw. Joining the consortium will enable national entities to participate in projects financed by the EU, whose budget in the current and future financial perspective may amount to more than EUR 350 million. Membership in the consortium will allow for faster development of the Polish SST system, which will provide our country with data necessary to protect the planned missions of Polish satellites and will support national security and defense in monitoring threats from artificial space objects. Participation in the European programme also brings great scientific and business potential. Ensuring the operability of the observation sensors forming the Polish SST infrastructure, the possibility of their modernization and the demand for new ones – all this will facilitate a faster growth of competence in the area of SST and optical and radar observations for Polish entities, which already today gain experience by implementing projects under the optional SSA programme in ESA.

In view of the progressing commercialization of products related to situational awareness in space, domestic entities providing solutions and services in this area will be able to direct their offer also to the global market, which will grow as a result of the New Space trend, the increasing number of micro and smaller satellites, the planned development of mega-constellations and new areas such as satellite in-orbit servicing or, in the longer term, the sourcing of raw materials from celestial bodies. The Polish National Space Programme comes from December 2018 and still is in public consultations. Polish Space Agency (POLSA) will be responsible for the implementation of the programme. POLSA has considered a few areas of public support within the programme, such as, "Development of satellite systems" – with one of the priority projects: "Space Situational Awareness System". The vital goal of the project is to provide a long-term access to the European and national space infrastructure and the services crucial for securing its operations. As a consequence, a network of sensors (telescopes, lasers, radars) responsible for space object observation and tracking is to function on the territory of Poland and staff is to be trained in order to perform tasks in the frame of SST.

Polish and European SSA

The European Space Situational Awareness System (SSA) consists of three separate segments: Space Surveillance and Tracking, especially in the context of Space Debris (Space Weather) and Near Earth Orbit (NEO) observation. The European SSA system has dual-use civilian and military applications. Additional components to the SSA system may be added in the near future. They are built on the basis of military requirements and compiled by the European Defence Agency (EDA). The conference also devoted a lot of space to the development of the STM (Space Traffic Management) system, which does not yet exist in Europe, unlike the USA. The goals for Space Situational Awareness are the following: society heavily dependent on critical space and ground assets, critical assets need to be protected against adverse effects from space, SSA Programme Declaration calls for independent European access to SSA data and services. There are three main areas: Space Weather, Near Earth Objects, Space Debris clean space. The participants in ESA SSA programs are 19 participating states. The good progress in the development of a SSA system in Europe has been observed and many actors involved: Member States, ESA, and EU. Distribution of roles needs to be finalized: development vs exploitation. There is still a performance gap in surveillance radars that is why there is a need to agree on a suitable governance scheme for the exploitation of future high performance European surveillance radar. There is a development of a high performance radar can be achieved within 3 years SWE and NEO systems will reach pre-operational status by 2020.

Thus, Europe has started its own preparatory programme of the SSA. International negotiations on permanent exchange of information and coordination, mainly with the USA, are also foreseen. Poland should also participate in these studies, which this year is to eventually become a member of the European SSA Consortium, where they play the biggest role: France, Germany, Great Britain and Italy. Much of the data to be dealt with by the established Consortium can be found in public satellite catalogues created by the USA and other countries, which are available on the Internet and can be freely used. That is why transatlantic cooperation is so crucial. Orbital paths are constantly changing or are disturbed by a number of factors, such as inconsistent degrees of attraction, solar activity or the effects of gravity of other orbital objects. International cooperation on SSA data sharing is weakened by issues such as liability and property concerns, data formatting standards and compliance with catalogued tools, and finally security (some satellites

do not provide data to the public). These issues are still being discussed in various international fora, including UN COPUOS (United Nations Committee on the Peaceful Uses of Space). The author follows these discussions on an ongoing basis and makes use of them in her scientific work. Space security has a multidimensional concept. It can be understood as Security in Outer Space, Outer Space for Security or Security for Space. The first means the protection of the space infrastructure against natural and man-made threats or risks, ensuring the safety and sustainability of space activities. The second means the use of space systems for security and defence purposes. Security for Space means the protection of human life and the Earth environment against natural threats and risks coming from space.

There are also several meanings of such definitions as: Space Situational Awareness (SSA) which can be understood as current and predictive knowledge and understanding of the outer space environment including space weather and location of natural and manmade objects in orbit around the Earth; SEPP (Space Environment Protection and Preservation, which is preventive and curative mitigation of negative effects of human activity in outer space on the safety and sustainability of the outer space environment and Space Infrastructure Security (SIS) as assurance of the infrastructure ability to deliver a service that can justifiably be trusted despite a hazardous environment.

There are some challenges to space infrastructure security, such as unintentional hazards (space debris, accidental interferences), Intentional threats (ASAT, malicious interferences, and cyberattacks), Space weather hazards (geomagnetic storms, solar storms).

There are rising challenges to space infrastructure security. Space is an increasingly congested and contested resource. Space is multiple and diverse, there are different mitigation and protection measures. There are many actors playing in the Space, so interdependence between them has been noticed. There are various trends in Space, such as increasing space activity, new concepts, connected space, strategic target, “space control” capabilities, etc. The most important is growing dependence on space for society and economy at large.

Growing security threats to civilian space programmes (access to space, cybersecurity in space, safe operations in space). Space is a critical infrastructure: satellites (jamming, spoofing, blinding), ground stations (hacking). Threats (military, non-military, natural) are understood and accepted and now are more properly and precisely assessed. Readiness to face

and respond to threats is growing in governments and private sector. It seems that there is a possibility to invest in handling a threat is developing and to find political solutions in managing threats[30].

Conclusions

In this article the attention was paid to the legislation issue on space security. It seems that both states: Japan and Poland (as an EU state) find this topic important and regulate this issue in the internal and regional (EU) law. Policy, strategy or plans on Space security are sensitive for both states, even though Poland has not achieved yet such a progress in this matter as Japan. The reason is probably very simple- Japan is much more experienced state as a regulator because of the longer history of using Outer Space on daily basis (institutions, regulators and space activities). Japan though is a good example to follow in the legislation on space security- SSA for Poland. The proper and practical legislation should be updated in case to serve to the public and not making not necessary barriers to the space market, having still the priority of security for all entities engaged in Space. This stabilized legislation is a great tool for international collaboration and cooperation in Space.

Bibliography

Aoki S., *Regulation of Space Activities in Japan* [in:] R. Jakhu, *National Regulation of Space Activities*, Springer 2010.
Ishii M., *Research and Operation of Space Weather forecast in Japan*, Tokyo 2018.
Matsuura M., *JAXA's endeavor to SSA*, Tokyo 2017.
Nakamura S., *Research and Activities on SSA at JAXA*, Tokyo 2018.
Ogawa S., *SSA activities at JAXA*, Tokyo 2019.
Polkowska M., *Prawo bezpieczeństwa w Kosmosie*, Warszawa 2018.
Saito A., *Japan's efforts for the rule of law in outer space – STM perspectives*, Tokyo 2017.
Sugai H., *Toward Acquiring and Enhancing Space Capability*, Tokyo 2019.
Suzuki K., *How to Establish Space Governance?*, Tokyo 2019.
Takada S., *Space Policy of Japan*, Tokyo 2017.
Takahashi H., *Trend in Military Satellite Communications*, Tokyo 2018.
Uchikura H., *MOD'S SSA Project – Initiatives Taken by Koku-Jieitai*, Tokyo 2019.
Wakimoto T., *A guide to Japan's Space Policy Formulation: Structures, Roles and Strategies of Ministries and Agencies for Space*, "A Working Paper on Japan's Space Policy" 2019, vol. 19.
Yamakawa H., *JAXA's Activities on Ensuring Stable Use of Outer Space*, Tokyo 2019.

30 M. Polkowska, *Prawo bezpieczeństwa w Kosmosie*, Warszawa 2018, p. 135–140.

Yamakawa H., *Member of Committee on National Space Policy*, Tokyo 2018.
Yoshitomi S., *SSA Capabilities and Policies in Japan, Space Situational Awareness Workshop: Perspectives on the Future Directions for j*, Tokyo 2019.

Polityka bezpieczeństwa w Japonii i w Polsce

Streszczenie

Niniejszy artykuł odnosi się do przepisów dotyczących bezpieczeństwa kosmicznego w Japonii i w Polsce. Oba państwa przygotowały już pewne akty prawne dotyczące bezpieczeństwa w przestrzeni kosmicznej – pytanie jest następujące – czy nadal istnieje potrzeba zmian i czy te przedstawione akty prawne są wystarczające do realizacji praktycznych celów pokojowego użytkowania przestrzeni kosmicznej. Japonia jest znacznie bardziej doświadczonym państwem w korzystaniu z przestrzeni kosmicznej niż Polska; to samo wydaje się w przypadku ustawodawstwa. Polska jako mniej doświadczone państwo w tej dziedzinie ma wiele ambicji co do stworzenia skutecznego ustawodawstwa dotyczącego bezpieczeństwa kosmicznego, dlatego musi podążać za dobrymi przykładami państw i instytucji. Jednym z nich jest Japonia. Z drugiej strony Polska jako członek UE musi wdrożyć europejskie prawo w zakresie bezpieczeństwa kosmicznego (w szczególności SSA), które wydaje się bezcenne i skuteczne dla międzynarodowej współpracy państw w Kosmosie.

Słowa kluczowe: bezpieczeństwo kosmiczne, prawo, polityka, świadomość sytuacyjna w kosmosie, strategia

Darejan Tsutskiridze*
Nino Petriashvili**

Commonly Misused Terms: War, Armed Conflict, Civil War and Military Coup D'Etat

Abstract

The aim of the article is linguistic and semantic analysis of concepts such as armed conflict, war, civil war and coup d'etat. In the author's opinion, these concepts do not coincide, and their correct classification will lead to a better understanding of the nature of international conflicts. Authors also draws attention to the need for cooperation between scientists and politicians in the aspect of greater effectiveness of international humanitarian law.

Key words: peacebuilding, law, civilizations, states, conflicts

* Assistant Professor Darejan Tsutskiridze, Georgian Technical University.
** PhD Student Nino Petriashvili, Ilia State University.

Modern international society has been focused on conflict resolution and peacebuilding, improving international relations and intrastate consolidation. Politicians and scholars made some noticeable progress in developing the means of peaceful resolution of conflicts, but the world political map is still covered with slaughterous conflicts because countries across the world are intensively involved in disputes over power and resources.

The article seeks to analyze and isolate the following terms from one another: armed conflict, war, civil war and military coup d'etat. These terms are confusing because the distinction between them is vague, which is caused by the abundance of the similar features, rapid escalation, ability of quick transformation from one condition into another, spreading information and disinformation, etc. We assume that isolation of these terms will contribute to the better understanding of conflict situations. Correct classification will lead to accurate diagnosis and promote conflict prevention and resolution.

Firstly, it is very important to define that current International Humanitarian Law is based on just war theory. In general, there are three major war theories: The just war theory, Realism and Pacifism. "The core, and controversial, proposition of just war theory is that, sometimes, states can have moral justification for resorting to armed force. War is sometimes, but of course not all the time, morally right". Realism believes "moral appeals are strictly wishful thinking" when it comes to power and national security. As for the pacifism "war is always wrong"[1]. The just war theory is the most influential theory and existing bodies of laws applicable to war are strictly based on it. As for the realism, it is a very popular theory between politicians and political scientists. International or non-international status of conflict determines the means of regulations and the body of law applicable to the particular situation. Sadly, the frequent distortion and concealment of facts blocks the correct identification of the status.

There are no doubts that war is as old as our civilization. The oldest civilizations of Egypt, Sumer, Ancient Greece, Rome, etc. contributed to the development of war science and philosophy. They sought the reasons to justify war and set the rules for launching and waging it. The origin of just war theory is deeply rooted in Ancient Philosophy and Christianity and is related to Augustine. He assumed that to launch the war there had to be right reasons and means. Morality has a great significance. Morality and dignity are the values

1 *Stanford Encyclopedia of Philosophy*, 2000; substantive revision Jul 28, 2005.

which establish justice in the field. The ICRC brochure states: "Measures must be taken to ensure respect for international humanitarian law. States have an obligation to teach its rules to their armed forces and the general public. They must prevent violations or punish them if these nevertheless occur"[2].

Besides its destructive character, war has brought changes and novelties to our world. Over the last two centuries society has been more mobilized to control the war and its impacts. The intensity and high mortality rate of World War II was a trigger, which made society think again about the existing organizations and leverages to control conflicts. The war dramatically altered the political map of Europe. Political leaders felt the necessity of extending the law of war. This attempt to widen the applicability of the law of war lead to the future blurriness.

The confusion around the terms began after the Geneva Conventions broadened the term "war". "Historically, the applicability of the law of armed conflict often depended upon a State subjectively classifying a conflict as a "war". Recognition of a state of war is no longer required to trigger the law of armed conflict. After the 1949 Geneva Conventions, the law of armed conflict is now triggered by the existence of "armed conflict" between States"[3]. Change clarified the situation considerably. It made the IHL more applicable to conflicts, but scientists still were left in confusion. "The scenario has therefore arisen that states have been adamant to recognize a situation as an armed conflict for certain political reasons"[4]. The above tendencies cause the discussion about which contradiction is war and which is armed conflict, which is international conflict, and which is non international conflict, civil war or coup d'etat. Scholars argue about the origin and features of terms and parties to the conflict as well. In the meantime, the definitions of the terms broaden. This fact draws an absolutely new picture of armed conflicts. As a result of our research, we attempt to state our point of view about armed conflicts and make a humble contribution to the resolution of one of the most significant dilemmas.

2 ICRC brochure – What is International Humanitarian Law, Advisory service on International Humanitarian Law.

3 Low of Armed Conflict Deskbook, International and Operational law Department, The Judge Advicate General's Legal Center and School, U.S. Army Charlottesville, Virginia 2014.

4 C. Chelimo, *Defining Armed Conflict*, „International Humanitarian Law" 2011, vol. 3, no. 04.

War – International Conflict

International armed conflict is defined by the 1949 Geneva Convention "the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them"[5]. The Commentary to the Geneva Conventions states: "It makes no difference how long the conflict lasts, or how much slaughter takes place"[6]. The significance of this commentary is enormous. The urgency of an armed conflict is not supposed to measure by the level of mortality or its duration. Additional Protocol I to the Conventions supplements the definition of International Armed Conflict: "armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self determination"[7]. The British Defence Doctrine also uses the terms war and armed conflict synonymously and describes war as a condition "when differences between states reach a point at which both parties resort to force, or one of them does acts of violence, which the other chooses to look on as a breach of the peace, the relation of war is set up"[8].

Internationalized Armed Conflict

International humanitarian law recognizes an internationalized armed conflict as well. "The situation of an internationalized armed conflict can occur when a war occurs between two different factions fighting internally but supported by two different states"[9]. Internationalized armed conflict is more latent and even if an armed conflict is obvious the support groups (foreign states) are not always officially involved. Internationalized armed conflicts transform

5 The Geneva Conventions of 12 August 1949, ICRC, art. 2.

6 J.S. Picted (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition Of the Wounded Sick In Armed Forces in the Field 32*, Geneva 1952.

7 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). Geneva, June 8, 1977, art. 1(4), art. 1.

8 Uk Defence Doctrine, (JDP) 0-01, 2014, Ministry of Defence.

9 G.S. Stewart, *Towards a single definition of armed conflict in international humanitarian law: A critique of internationalized armed conflict*, „International Review of the Red Cross" 2003, no. 850, p. 313–350.

local conflicts into international conflicts because external powers frequently support actual parties to the conflict. "When a foreign State extends its military support to the government of a State within which a non-international armed conflict is taking place, the conflict remains non-international in character. Conversely, should a foreign State extend military support to an armed group acting against the government, the conflict will become international in character"[10].

Noninternational Armed Conflict. Civil War and Coup d'etat

Civil war and coup d'etat besides their clear characteristics and definitions are often blurred. According to Vitit Muntarbhorn noninternational armed conflicts are called civil wars by public[11]. In order to understand civil war and coup d'etat it is important to understand internal armed conflict. Noninternational armed conflicts are more frequent than International armed conflicts. Noninternational armed conflict is less covered by IHL. According to the Common Article 3 of Geneva Conventions noninternational armed conflict is an "armed conflict not of an international character occurring in the territory of one of the High Contracting Parties"[12]. The manual on the law of Noninternational Armed Conflict specifies: Noninternational armed conflicts are armed confrontations occurring within the territory of a single State and in which the armed forces of no other State are engaged against the central government[13]. Additional Protocol II Art. 1 supplements GC common Art. 3: noninternational armed conflicts "take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military

10 M.N. Schmitt, G.C. Marshall, C.H.B. Garraway, Y. Dinstein, *The Manual on the Law of Noninternational Armed Conflict*, *International Institute of Humanitarian Law*, Sanremo 2006.

11 V. Muntarbhorn, *Legal Qualification and International Humanitarian Law as „lex specialis": 10 Basic Questions Concerning International Armed Conflicts... and answers?* [in:] *Current Problems of Humanitarian Law*, Sanremo 2003.

12 The Geneva Conventions of 12 August 1949, ICRC, art. 3.

13 M.N. Schmitt, G.C. Marshall, C.H.B. Garraway, Y. Dinstein, *The Manual on the Law of Noninternational Armed Conflict*, *International Institute of Humanitarian Law*, Sanremo 2006.

operations and to implement this Protocol"[14]. Often the given status of the conflict does not reflect the reality. States attempt to avoid giving international status to the conflict because then IHL becomes applicable. In the case of noninternational armed conflicts "Domestic law still applies. Unlike combatants during international armed conflict, guerrillas do not receive combatant immunity for their war-like acts. They may be punished by the sovereign as any other criminal"[15]. Besides not every distinction can reach the level of internal armed conflict. Geneva Conventions do not define civil war or coup d'etat but the criteria given by the Commentary about noninternational conflict defines civil war as well.

"I. Does the group have an organized military force? II. Are members of the group subject to some authority? III. Does the group control some territory? IV. Does the group demonstrate respect for the law of armed conflict? V. Does the government respond to the group with regular armed forces?"[16] and politicians disagree on the meanings of terms armed conflict, war, civil war and military coup d'etat. These terms are confusing because the distinction between them is vague, which is caused by the abundance of the similar features, rapid escalation, ability of quick transformation from one condition into another, spreading information and disinformation, etc. We assume these questions clearly indicate that civil war and coup d'etat definitely are noninternational armed conflicts. The main distinction between these terms is the duration of the conflict and the composition of the parties. "A war has to challenge the sovereignty of internationally recognized state and the rebels were able to mount an organized military opposition to the state and to inflict significant casualties on the state"[17]. The average duration of civil wars is 4–5 years while coups are shorter. It may take a couple hours and an adversary of the state is represented by military elite mostly. "Coups are dramatic events that can happen during civil wars. Coups may also provide the initial spark to

14 Protocol Addtional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non - International Armed Conflicts (Protocol II), of 8 June 1977, ICRC, art. 1.

15 Low of Armed Conflict Deskbook, International and Operational law Department, The Judge Advicate General's Legal Center and School, U.S. Army Charlottesville, Virginia 2014.

16 J.S. Picted (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition Of the Wounded Sick In Armed Forces in the Field 32*, Geneva 1952.

17 M.W. Doyle, N. Sambanis, *Making War and Building Peace. United Nations Peace Operations*, New Jersey 2006.

a civil war. However, regardless of their bloodiness or long-term consequences, coups are not civil wars"[18].

Scholars ere is a distinction between the definitions they give to the specific terms and there is a distinction between the assessment they give to the specific situations. Managing and resolving conflict requires understanding parties as well. Development of International relations broadened the boundaries of cooperation and accordingly of conflict. We assume that isolation of these terms will contribute to the better understanding of conflict situations. Correct classification will lead to accurate diagnosis and promote conflict prevention and resolution. In order to limit the applicability of IHL, parties attempt of the very essence of the problem, its history and content and of the interest of the to avoid declaring war, recognizing international armed conflict and even noninternational armed conflict. States fear of non-state groups who become stronger and more organized when the law of armed conflict applies. The application of bodies of law strictly depends on the understanding and assessment of conflict situations. In spite of many existing popular standpoints, the vagueness around the terms remains permanent. For international humanitarian law to become more effective, scholars and politicians have to combine their efforts and continue work together.

Bibliography

Chelimo C., *Defining Armed Conflict*, "International Humanitarian Law" 2011, vol. 3, no. 04

Doyle M.W., Sambanis N., *Making War and Building Peace. United Nations Peace Operations*, New Jersey 2006.

Muntarbhorn V., *Legal Qualification and International Humanitarian Law as "lex specialis": 10 Basic Questions Concerning International Armed Conflicts... and answers?* [in:] *Current Problems of Humanitarian Law*, Sanremo 2003.

Picted J.S. (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition Of the Wounded Sick In Armed Forces in the Field 32*, Geneva 1952.

Schmitt M.N., Marshall G.C., Garraway C.H.B., Dinstein Y., *The Manual on the Law of Noninternational Armed Conflict*, *International Institute of Humanitarian Law*, Sanremo 2006.

Stewart G.S., *Towards a single definition of armed conflict in international humanitarian law: A critique of internationalized armed conflict*, "International Review of the Red Cross" 2003, no. 850.

Thyne C., *The Impact of Coups d'etat on Civil War Duration*, "Conflict Management and Peace Science" 2015, no. 34(3).

18 C. Thyne, *The Impact of Coups d'etat on Civil War Duration*, „Conflict Management and Peace Science" 2015, no. 34(3).

Niewłaściwie stosowane terminów: wojna, konflikt zbrojny, wojna domowa i wojskowy zamach stanu

Streszczenie

Celem artykułu jest analiza językowa oraz znaczeniowa takich pojęć jak: konflikt zbrojny, wojna, wojna domowa i zamach stanu. W opinii autorów pojęcia te nie są ze sobą zbieżne, a dokonanie ich prawidłowej klasyfikacji doprowadzi do lepszego zrozumienia istoty konfliktów międzynarodowych. Autorzy zwracają ponadto uwagę, na konieczność współpracy naukowców z politykami w aspekcie większej skuteczności międzynarodowego prawa humanitarnego.

Słowa kluczowe: budowanie pokoju, prawo, cywilizacja, państwo, konflikty

Maciej Ciesielski*

Socjologia bezpieczeństwa jako subdyscyplina nauk o bezpieczeństwie

Streszczenie

Artykuł porusza dwie kluczowe kwestie: Co powoduje, że bezpieczeństwo wchodzi w obszar zainteresowania socjologów? Dlaczego socjologia bezpieczeństwa może być rozpatrywana jako subdyscyplina z obszaru nauk o bezpieczeństwie a nie wyłącznie jako subdyscyplina socjologiczna?

Z punktu widzenia socjologii bezpieczeństwo jest kluczowym elementem życia społecznego, który zapewnia równowagę społeczną. Socjologowie zwracają uwagę, że bezpieczeństwo ma przede wszystkim charakter subiektywny, jest konstruowane przez aktorów ze względu na ich własne oczekiwania i interesy, ale odnosi się także do konkretnych okoliczności o charakterze obiektywnym – zjawisk, struktur i procesów społecznych. W publikacji przybliżono strukturę systemów bezpieczeństwa rozpatrywanych jako przedmiot badań socjologii bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo, socjologia bezpieczeństwa, systemy bezpieczeństwa, nauki o bezpieczeństwie

* Dr Maciej Ciesielski, Ośrodek Szkolenia Służby Kontrwywiadu Wojskowego, ORCID: 0000-0001-6868-884X.

Wstęp

Nauki społeczne zajmują się problematyką bezpieczeństwa w ramach takich dyscyplin naukowych jak psychologia, nauki polityczne, pedagogika, a także socjologia. W ostatnich latach bezpieczeństwo stało się tak mocno eksplorowanym polem badawczym w Polsce, że pojawiła się osobna dyscyplina – nauk o bezpieczeństwie, obok nauk o obronności. Nie ma już natomiast nauk wojskowych, z których wyżej wymienione zostały wyodrębnione[1]. Z kolei w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 25 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych nie ujęto już nauk o obronności, pozostawiając jedynie nauki o bezpieczeństwie (Dz.U. z 2018 r., poz. 1818). Przedmiotem nauk o bezpieczeństwie są współczesne systemy bezpieczeństwa w wymiarze militarnym i niemilitarnym, a także ich funkcjonowanie na różnych poziomach organizacyjnych. Wskazuje się, że systemy bezpieczeństwa obejmują działania instytucji o charakterze państwowym, rządowym i samorządowym, przedsiębiorców i organizacji społecznych. Takie ujęcie obszaru badawczego nauk o bezpieczeństwie świadczy nie tylko o tendencji do większej specjalizacji poszczególnych dyscyplin naukowych, ale również o koniecznym współdziałaniu badaczy zajmujących się tematem bezpieczeństwa w ramach różnych dyscyplin. Bezpieczeństwo ma tak wiele wymiarów i płaszczyzn, że wyjaśnienie konkretnych procesów i zjawisk wpisujących się w jego problematykę wymaga od naukowca podejścia interdyscyplinarnego.

Na zachodnich uniwersytetach bezpieczeństwo już od dłuższego czasu jest obszarem badawczym dyscypliny naukowej, czy też dyscypliny wiedzy akademickiej, zwanej *security studies*, które w ujęciu historycznym stanowią jeden z kluczowych działów nauki o stosunkach międzynarodowych[2]. Jednak naukowcy zajmujący się problematyką bezpieczeństwa coraz wyraźniej akcentują potrzebę wyprowadzenia studiów bezpieczeństwa z obszaru nauki o stosunkach międzynarodowych. Chociażby dlatego, że bezpieczeństwo to coś więcej niż wypadkowa powiązań i relacji zachodzących pomiędzy

1 Uchwała Centralnej Komisji do Spraw Stopni i Tytułów z dnia 28 stycznia 2011 r. zmieniająca uchwałę w sprawie określenia dziedzin nauki i dziedzin sztuki oraz dyscyplin naukowych i artystycznych (M.P. nr 14, poz. 149) oraz rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. nr 179, poz. 1065).

2 P.D. Williams, *Badania bezpieczeństwa. Wprowadzenie* [w:] P.D. Williams (red.), *Studia bezpieczeństwa*, Kraków 2012, s. 2–3.

państwami czy instytucjami międzynarodowymi – pomimo że ten wymiar także ma istotny wpływ na funkcjonowanie systemów bezpieczeństwa. Dobrym przykładem świadczącym o zakorzenieniu postrzegania bezpieczeństwa w perspektywie relacji międzynarodowych jest struktura administracji państwowej Stanów Zjednoczonych, gdzie kompetencje Doradcy ds. Bezpieczeństwa Narodowego częściowo nakładają się z zakresem uprawnień Sekretarza Stanu[3], czyli uprawnień w zakresie kierowania polityką zagraniczną.

W podejściu przyjętym w 2011 r. przez Centralną Komisję do Spraw Stopni i Tytułów oraz przez Ministra Nauki i Szkolnictwa Wyższego, w ramach nauk o bezpieczeństwie znajdzie się miejsce zarówno dla obszarów badawczych typowych dla pierwotnego zakresu badawczego security studies, ale z drugiej strony ontologia nauk o bezpieczeństwie zdaje się umożliwiać rozwój w ramach tej dyscypliny całej gamy innych podejść, które z czasem mogą być określone jako subdyscypliny nauk o bezpieczeństwie. Ze względu na dziedzinę nauk społecznych, do których nauki o bezpieczeństwie się zaliczają, szczególna relacja będzie je łączyć z socjologią, która oferuje przetestowany empirycznie oraz ugruntowany teoretycznie aparat pojęciowy. W ramach rozwoju socjologii, na gruncie tej dyscypliny naukowej, udało się także rozpoznać określone mechanizmy społeczne, które mają bezpośredni związek z instytucjonalizacją i funkcjonowaniem systemów bezpieczeństwa.

W związku z powyższym warto spróbować udzielić odpowiedzi na dwa istotne pytania: Co powoduje, że bezpieczeństwo wchodzi w obszar zainteresowania socjologów? Dlaczego socjologia bezpieczeństwa może być rozpatrywana jako subdyscyplina z obszaru nauk o bezpieczeństwie a nie wyłącznie jako subdyscyplina socjologiczna?

Z punktu widzenia socjologii bezpieczeństwo jest kluczowym elementem życia społecznego, który zapewnia równowagę społeczną. Socjologowie zwracają uwagę, że bezpieczeństwo ma przede wszystkim charakter subiektywny, jest konstruowane przez aktorów ze względu na ich własne oczekiwania i interesy, ale odnosi się także do konkretnych okoliczności o charakterze obiektywnym – zjawisk, struktur i procesów społecznych. Określony stopień poczucia bezpieczeństwa jednostek i całych zbiorowości jest niezbędny do prawidłowego funkcjonowania społeczeństwa. Kiedy w społeczeństwie poczucie bezpieczeństwa – ekonomicznego, bądź szerzej rozumianego, publicznego – spada do poziomu granicznego (który nie jest jednoznacznie zdefiniowany),

3 Por. Z. Brzeziński, *Cztery lata w Białym Domu. Wspomnienia*, Warszawa 1990, s. 52–58.

powstaje chaos, anomia, wybuchają rewolucje, a obowiązujące normy życia społecznego są zawieszane. Taką sytuacją jest m.in. wojna, która cechuje się permanentnym zagrożeniem życia i zdrowia wszystkich obywateli (tak w ujęciu subiektywnym, jak i obiektywnym). Bezpieczeństwo i jego percepcja istotnie przyczyniają się do zmiany społecznej, wpływają na kształt struktur i systemów bezpieczeństwa oraz pozostałych systemów społeczeństwa. Dotyczy to nie tylko bezpieczeństwa fizycznego, ochrony na płaszczyźnie militarnej i porządku publicznego, ale także bezpieczeństwa ekonomicznego czy obywatelskiego, związanego z prawami i wolnościami przysługującymi każdemu obywatelowi państwa demokratycznego.

Bezpieczeństwo to stan braku zagrożenia, albo poczucia braku zagrożenia – względnie jego niskiego poziomu. Zagrożenie to strach, a strach to najbardziej pierwotny i skuteczny motywator ludzkich działań. Z punktu widzenia psychologii, bezpieczeństwo jest podstawową potrzebą każdej jednostki[4], konieczność jej zaspokojenia – w skali grup społecznych, szerszych zbiorowości, bądź całych społeczeństw – może prowadzić do gwałtownych i nieprzewidzianych działań i zjawisk. Bezpieczeństwo jest zawsze rozpatrywane i analizowane przez ludzi w konkretnym kontekście, chociaż bardziej pasuje tutaj liczba mnoga – kontekstach społecznych. Posiada dwa zasadnicze składniki: gwarancje nienaruszalnego przetrwania podmiotu oraz swobodę jego rozwoju[5]. Bezpieczeństwo to również wartość, ceniona i wpływająca na ludzkie zachowania praktycznie na każdym poziomie.

W wąskim ujęciu bezpieczeństwo ma głównie wymiar militarny, kojarzony z obronnością, w rozumieniu szerokim dotyczy z kolei obrony konkretnych wartości (ideologii, dobrobytu, niezależności) oraz odwołuje się do zaspokajania takich potrzeb jak przetrwanie, istnienie, tożsamość, całość[6]. Bezpieczeństwo wchodzi w relację z ładem i porządkiem społecznym, jest niezbędne do osiągnięcia równowagi społecznej (equilibrium). Relacja ta opiera się na założeniu sprzężenia zwrotnego, gdyż bezpieczeństwo zarazem warunkuje i jest warunkowane przez ład, równowagę, czy porządek społeczny. Stanowi

4 Por. A. Korwin-Szymanowska, *Psychospołeczne aspekty poczucia bezpieczeństwa* [w:] *Bezpieczeństwo jako wartość*, Kraków 2010, s. 29–46.

5 J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 19.

6 D. Biłous-Szrejder, O. Nowaczyk, *Metodologia bezpieczeństwa narodowego* [w:] J. Maciejewski (red.), *Socjologiczne aspekty bezpieczeństwa narodowego*, Wrocław 2001, s. 9–10.

fundamentalną okoliczność niezbędną do ukonstytuowania się organizacji społecznej[7].

Socjologia zajmuje się bezpieczeństwem w dwóch podstawowych wymiarach, w których może być ono definiowane jako: 1) fakt społeczny, albo 2) system społeczny. W pierwszym wymiarze, idąc za Emilem Durkheim'em, powiemy, że bezpieczeństwo to fakt społeczny, który „(…) poznaje się po sile zewnętrznego przymusu, jaki wywiera lub jest w stanie wywierać na jednostki; obecność tej siły poznaje się z kolei bądź po istnieniu jakiejś określonej sankcji, bądź po oporze, jaki fakt stawia każdemu przedsięwzięciu indywidualnemu, które zmierza do zadania mu gwałtu"[8].

Bezpieczeństwo rządzi się swoimi prawami, odnosi się do specjalnych środków zaradczych, instrumentów politycznych, w wyniku których może dojść do zawieszenia powszechnych reguł społecznych (np. praw obywatela, czy zasady transparentności itp.). Nawiązuje do systemu wartości, w którym stanowi wartość najwyższą i najbardziej pożądaną.

Z drugiej strony z bezpieczeństwem nierozerwalnie powiązane jest pojęcie systemu społecznego, które bezpośrednio odnosi się do konkretnych koncepcji socjologicznych, a nawet szerzej – koncepcji pojmowania i rozumienia zjawisk społecznych. Systemy bezpieczeństwa to właśnie przedmiot nauk o bezpieczeństwie, co powoduje, że subdyscyplina jaką jest socjologia bezpieczeństwa znajduje się na przecięciu socjologii oraz nauk o bezpieczeństwie, tak jak socjologia prawa jest zarówno przedmiotem rozważań z obszaru nauk prawnych, jak i samej socjologii.

Socjologia bezpieczeństwa zajmuje się badaniem współczesnych systemów bezpieczeństwa kładąc duży nacisk na ich instytucjonalizację, rozumianą jako wyłanianie się, artykułowanie i utrwalanie struktur normatywnych, czyli reguł społecznych: wzorów, norm i wartości[9], związanych z bezpieczeństwem. W zakres zainteresowania socjologii bezpieczeństwa wchodzić będą także relacje i powiązania pomiędzy poszczególnymi strukturami odpowiedzialnymi za zapewnianie bezpieczeństwa, tj. elementami systemu bezpieczeństwa. O potencjale instytucjonalnym całych systemów bezpieczeństwa, jak i ich poszczególnych segmentów stanowi prawo, moralność, zwyczaje oraz podkultury organizacyjne. Takie podejście sugeruje, aby analizując komponenty systemów bezpieczeństwa i relacje, powiązania pomiędzy nimi, koniecznie wyjść poza

7 Por. E. Moczuk, *Socjologiczne aspekty bezpieczeństwa lokalnego*, Rzeszów 2009, s. 14.
8 E. Durkheim, *Zasady metody socjologicznej*, Warszawa 1979.
9 P. Sztompka, *Socjologia. Analiza społeczeństwa*, Kraków 2003, s. 432.

same służby mundurowe. Chodzi konkretnie o uchwycenie wpływu otoczenia społecznego na system bezpieczeństwa, przepływu zasobów stanowiących o jego potencjale, które są pozyskiwane od innych systemów społeczeństwa i dystrybuowane w obszarze samego systemu bezpieczeństwa. Niebagatelną rolę odgrywa tutaj cywilne zwierzchnictwo nad systemami bezpieczeństwa. Poza tym na pierwszy plan wysuwają się także obszary polityki oraz gospodarki jako podstawowe sfery rzeczywistości społecznej, których przedstawiciele wchodzą w relacje z systemem bezpieczeństwa, a nawet stanowią ich trzon – np. żołnierze i cywilni pracownicy resortu obrony narodowej, albo przedsiębiorcy zaliczani do tych o szczególnym znaczeniu dla bezpieczeństwa i obronności państwa – zwłaszcza z polskiego przemysłu zbrojeniowego. W związku z tak zdefiniowanym obszarem badawczym socjologii bezpieczeństwa, który jest ujęty przedmiotowo i odwołuje się do szeroko rozumianych systemów bezpieczeństwa, będzie ona korzystać z podejść właściwych takim ugruntowanym już subdyscyplinom socjologicznym, jak socjologia gospodarki, socjologia polityki, socjologia prawa czy socjologia wojska. Bezpieczeństwo analizowane jako stan, fakt, a w końcu jako proces społeczny, ogniskuje różne podejścia socjologiczne, które składają się na jej wymiar ontologiczny (czyli struktury problemu badawczego), wymiar metodologiczny (postępowania badawczego), oraz wymiar epistemologiczny (rezultatów)[10].

Systemy bezpieczeństwa jako systemy społeczne

W połowie XX wieku, w związku z rozważaniami nad istotą społeczeństwa, socjologowie wprowadzili w miejsce metafory organizmu pojęcie systemu społecznego. Porównanie do organizmu towarzyszyło socjologii od początków jej akademickiej instytucjonalizacji. Już August Comte uważał, że społeczeństwo (jak organizm biologiczny) jest złożoną i nieredukowalną do swoich części składowych całością[11]. Z kolei w systemie społecznym uczestniczą już nie tyle konkretne jednostki, co zróżnicowane pozycje społeczne lub związane z nimi role[12]. Przez system społeczny można rozumieć pojedyncze instytucje, bądź całe segmenty i rodzaje struktur. Struktury bezpieczeństwa państwa, takie

10 Patrz: M. Ciesielski, *Co to jest socjologia bezpieczeństwa (publicznego)?* [w:] G. Bryda (red.), *Światy i konteksty społeczne. Krakowskie Spotkania Socjologiczne*, t. II, Kraków 2011.
11 J. Szacki, *Historia myśli socjologicznej*, Warszawa 2002, s. 254–255.
12 P. Sztompka, *Socjologia…*, s. 30.

jak wojsko, polityka, pozostałe służby dyspozycyjne oraz gospodarka mogą być analizowane jako jeden system społeczny, w ramach którego poszczególni aktorzy (osoby oraz instytucje) wykonują przypisane do ich pozycji i wzajemnie uzupełniające się funkcje. Z systemów można wyodrębnić sieci relacji i powiązań, a następnie szukać pewnych prawidłowości[13]. Warto zwrócić uwagę, że pojęcie systemu uległo generalizacji i relatywizacji[14], a ujęcie systemowe próbowano zastosować również do mniejszych układów w ramach społeczeństwa. Dla systemów społecznych właściwa jest świadomość jednostek ludzkich wypełniających poszczególne role i zajmujących określone pozycje oraz to, że ich własne cele mogą się różnić od celów systemu jako całości[15].

Autorem, który starał się dotrzeć do podstawowych zasad funkcjonowania poszczególnych sektorów społeczeństwa, aby ukazać złożoność ich wzajemnych powiązań, był amerykański socjolog Talcott Parsons[16]. W 1951 roku ukazała się jego książka *The Social System* opisująca system społeczny jako zinstytucjonalizowane wzory interakcji określane przez układy wartości, przekonań, norm oraz innych idei rozumianych jako system kulturowy. Punktem wyjścia teorii Parsonsa jest normatywna organizacja statusów – ról[17]. Inaczej mówiąc, teoria systemu społecznego tego autora skupia się na zjawiskach instytucjonalizacji wzorów orientacji wartościujących w rolach[18]. Systemy społeczne są nierozerwalnie połączone z działaniem i wpisują się w schemat o charakterze relacyjnym. Działania są zorientowane na inne podmioty, mają znaczenie motywacyjne dla indywidualnego podmiotu lub zbiorowości. Stąd też ciągłe nawiązywanie Parsonsa do wcześniejszych dzieł *Structure of Social Action i Toward a General Theory of Action*. Działanie składa się bowiem nie tylko z reakcji na bodźce sytuacyjne, ale także z rozwijania przez podmiot całego systemu oczekiwań względem różnych obiektów sytuacji. System społeczny może też być jednym z trzech aspektów ustrukturyzowania systemu działania, dwa pozostałe to system osobowości i system kulturowy. Pierwszy odwołuje się do podmiotów indywidualnych, drugi jest wbudowany w ich działanie[19]. Każdy

13 Ibidem.
14 P. Sztompka, *Logika analizy funkcjonalnej w socjologii i antropologii społecznej* [w:] S. Nowak (red.), *Metodologiczne problemy teorii socjologicznych*, Warszawa 1971, s. 219.
15 M. Ziółkowski, *Teorie systemu i funkcjonalizm* [w:] A. Jasińska-Kania, L.M. Nijakowski, J. Szacki, M. Ziółkowski (red.), *Współczesne teorie socjologiczne*, t. I, Warszawa 2006, s. 263.
16 Por. M. Kaczmarczyk, *System społeczny a dylematy działania*, t. VII, Kraków 2009, s. IX.
17 J.H. Turner, *Struktura teorii socjologicznej*, Warszawa 2005, s. 36–37.
18 T. Parsons, *System społeczny*, Kraków 2009, s. 5.
19 Ibidem, s. 9–11.

z trzech systemów (społeczny, osobowości oraz kulturowy) należy rozważać jako niezależny rodzaj organizacji elementów systemu działania, który jest niezbędny pozostałym. Inaczej mówiąc, bez kultury i osobowości nie istniałby system społeczny.

Nauki o bezpieczeństwie – jak już wcześniej wskazano – zajmują się badaniem współczesnych systemów bezpieczeństwa zarówno w ujęciu militarnym, jak i niemilitarnym. Socjologia bezpieczeństwa, korzystając z dorobku teorii socjologicznej, daje odpowiednią podbudowę naukom o bezpieczeństwie systematyzując pewien katalog pojęciowy właściwy dla nauk społecznych. Bez względu na to czy bezpieczeństwo będziemy rozpatrywać jako termin socjologiczny, prawny, ekonomiczny, czy politologiczny, to w każdym z tych obszarów naukowych będziemy mieli do czynienia z uniwersalnymi mechanizmami społecznymi, które definiują systemy bezpieczeństwa. Do funkcjonowania każdego systemu – nie tylko społecznego – niezbędne są zasoby umożliwiające mu przetrwanie i reprodukcję. Każdy rozwinięty system wymaga zasobów, które wykraczają poza cechy, które są mu dostępne. Zasoby – stosowane jako środki do osiągania jakiegoś przyszłego celu – stanowią przedmioty posiadania przeznaczone do produkcji dalszych pożytków[20]. Z kolei „(…) regulacja praw do zasobów lub dostępu do nich oraz możliwości nabywania tych praw drogą wymiany jest zatem innym fundamentalnym problemem funkcjonowania relacyjnego systemu orientacji instrumentalnej"[21].

Przedmiot posiadania (zasób, produkt) jest wynikiem kooperacji wielu indywidualnych podmiotów. Kooperacja jest powiązaniem działalności, której wynikiem jest jednostkowa całość, która może stać się częścią procesu wymiany. System relacji kooperatywnych można nazwać organizacją[22]. W tym przypadku organizacją systemu bezpieczeństwa. Na system bezpieczeństwa państwa składa się całość sił (podmiotów), środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana (w podsystemy i ogniwa), utrzymywana i przygotowywana[23]. System bezpieczeństwa składa się z podsystemów (systemów) kierowania oraz powiązanych ogniw wykonawczych, w tym operacyjnych

20 W przypadku wojska i przemysłu zbrojeniowego: Know-how, wyposażenie, uzbrojenie itp.

21 T. Parsons, *System…*, s. 60 i 61.

22 Ibidem.

23 *Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 36.

(obronny i ochronny) i wsparcia (społeczny i gospodarczy)[24]. Kluczowe znaczenie dla funkcjonowania systemu bezpieczeństwa państwa mają służby mundurowe[25] oraz ich cywilni zwierzchnicy, którzy kształtują bieżącą koncepcję i długoterminową strategię działania. W celu zrealizowania poszczególnych zadań, służby dyspozycyjne (w tym armia), jak i pozostałe ogniwa systemu bezpieczeństwa państwa, korzystają z różnego rodzaju zasobów: osobowych, finansowych, materialnych (materiałowych) oraz informacyjnych. Przede wszystkim jednak korzystają z sankcjonowanych przez prawo zasobów politycznych, które są bezpośrednio powiązane z władzą (pozwalają uczestniczyć w jej sprawowaniu). Odpowiedni poziom zasobów politycznych pozwala na efektywne sprawowanie władzy w ramach danego systemu bezpieczeństwa oraz w relacji z jego otoczeniem. Zasoby polityczne są generowane w wyniku tworzenia i stosowania prawa, czyli są pochodną konstrukcji aktów prawnych legitymizujących relacje władzy i dających odpowiednie instrumentarium do jej sprawowania. W praktyce, za pośrednictwem władzy i prawa, możliwe jest regulowanie procesu dystrybucji zasobów niezbędnych do funkcjonowania wojska, polityki i gospodarki, a także kształtowanie koniecznych powiązań strukturalnych w ramach systemu bezpieczeństwa państwa.

Struktura systemów bezpieczeństwa jako przedmiot badań socjologii bezpieczeństwa

Na szczególną uwagę badaczy współczesnych systemów bezpieczeństwa zasługuje pięć obszarów, na których opiera się ich funkcjonowanie, a które są jednocześnie związane z przepływem i charakterystyką poszczególnych rodzajów zasobów konstytuujących systemy bezpieczeństwa: 1) niejawność zasobów informacyjnych; 2) nieprzejrzystość zasobów personalnych; 3) przepływy zasobów finansowych; 4) funkcjonowanie przemysłu zbrojeniowego i infrastruktury krytycznej (czyli właściwości zasobów materiałowych systemów bezpieczeństwa); 5) aktywność zagranicznych firm zbrojeniowych jako przykładu wpływu podmiotów zewnętrznych na krajowy system bezpieczeństwa.

24 Ibidem.

25 W literaturze socjologicznej mówi się częściej o *grupach dyspozycyjnych*, kładąc nacisk na ciągłą gotowość aktorów do realizowania przypisanych im zadań z obszaru bezpieczeństwa państwa – por. J. Maciejewski (red.), *Grupy dyspozycyjne społeczeństwa polskiego*, Wrocław 2006.

Mówiąc o zasobach osobowych systemu bezpieczeństwa państwa (w tym podsystemu wsparcia gospodarczego), w dużym uproszczeniu można wskazać, że o ich kształcie i charakterze decydują przeważnie służby (wojsko, policja, straż graniczna, służby specjalne) oraz państwowe i prywatne firmy realizujące zadania na rzecz bezpieczeństwa państwa. Zasoby materialne są pozyskiwane oraz uzupełniane głównie przez gospodarkę (przede wszystkim koncerny zbrojeniowe). Zasoby informacyjne przepływają kanałami łączącymi służby dyspozycyjne (ogólnie) między sobą nawzajem, a także w ramach ich własnych struktur. Są również konsekwencją powiązań, jakie łączą służby z obszarem polityki, biznesu, mediów oraz nauki. Natomiast zasoby polityczne w największym stopniu determinują potencjał wszystkich służb dyspozycyjnych i pozostałych ogniw systemu bezpieczeństwa, przekładając się na praktyczny wymiar bezpieczeństwa państwa i obywateli.

Wszystkie mechanizmy sterujące opisanymi powyżej relacjami, polegającymi głównie na dystrybucji zasobów, zależą od, po pierwsze, potencjału instytucjonalnego będącego konsekwencją charakteru struktur systemu politycznego państwa. Po drugie natomiast, od kształtu regulacji prawnych sterujących przepływem zasobów pomiędzy poszczególnymi elementami systemu bezpieczeństwa, a także pomiędzy tym systemem a jego otoczeniem zewnętrznym. W tym kontekście kluczowa jest analiza drugiego z wyżej wymienionych czynników, czyli regulacji prawnych. Nauki o bezpieczeństwie, w tym wykorzystując socjologię bezpieczeństwa, powinny być m.in. nastawione na identyfikowanie konkretnych dziedzin systemu prawa wykorzystywanych przez aktorów do tworzenia i petryfikowania powiązań, ze szczególnym uwzględnieniem relacji patologicznych – m.in. osłabiających zdolność bojową armii, czy prowadzących do dysfunkcji systemu bezpieczeństwa państwa. Chodzi nie tyle o krytykę, czy też dezawuowanie poszczególnych aktów normatywnych, ale istotne jest wskazanie i podkreślenie konsekwencji, które wynikają z obowiązujących przepisów prawa. Tutaj socjologia bezpieczeństwa będzie wykorzystywać dorobek socjologii prawa.

System bezpieczeństwa państwa jest zbudowany na trzech filarach: siłach zbrojnych, cywilnych zwierzchnikach-kierownictwie (system polityki reprezentowany przez resorty obrony narodowej, spraw wewnętrznych oraz inne ośrodki władzy politycznej), oraz systemie gospodarki reprezentowanym przez przemysł obronny/zbrojeniowy. Podstawowe relacje, jakie występują pomiędzy armią a polityką i gospodarką bezpośrednio przekładają się na wydolności całego systemu bezpieczeństwa państwa. Charakter interakcji łączących aktorów tych obszarów życia społecznego determinuje zarówno

wizerunek, jak i faktyczny kształt administracji państwowej oraz ekonomiki w kontekście bezpieczeństwa, kreowanych przez bieżącą pozycję sił zbrojnych. Nie zawsze zdajemy sobie sprawę z trywialnej prawidłowości, że charakter i sposób oddziaływania, zwłaszcza na siły zbrojne, oraz możliwość ich kontroli odbijają się na naszym realnym bezpieczeństwie.

Ustrój demokratyczny daje społeczeństwu wiele instrumentów, które można wykorzystać do kontrolowania władzy, są to m.in. regularne wybory, możliwość stowarzyszania się, powszechne i niezawisłe sądy czy też działalność mediów. We wszystkich demokracjach świata jest jednak pewien obszar, którego reguły bezpośredniej kontroli obywatelskiej nie dotyczą, są zawieszone albo zmodyfikowane. Jest to obszar bezpieczeństwa państwa. Obszar nieprzejrzysty i tajemniczy dla zwykłych obywateli, a przez to narażony na pewne zagrożenia, natomiast powiązani z nim aktorzy przeważnie noszą mundury. Głównym i najważniejszym elementem każdego systemu bezpieczeństwa państwa zawsze jest armia.

Do zakresu badań empirycznych, którym powinna zajmować się socjologia bezpieczeństwa należy zaliczyć: 1) służby dyspozycyjne – takie jak wojsko, policja, służby specjalne; 2) systemy bezpieczeństwa oraz relacje pomiędzy jego elementami; 3) problematykę komunikacji w systemach bezpieczeństwa – niejawności informacji; 4) formy przestępczości najmocniej osłabiające bezpieczeństwo publiczne; 5) zagrożenia asymetryczne; 6) systemy aksjonormatywne i ich segmenty (zwłaszcza prawo, moralność i zwyczaje), jako czynniki bezpieczeństwo kształtujące i przez bezpieczeństwo kształtowane; 7) wymiar socjalny bezpieczeństwa publicznego oraz instytucje z nim związane; 8) relacje pomiędzy systemem bezpieczeństwa a systemami polityki i gospodarki; 9) jawne i ukryte grupy interesu wpływające na stan bezpieczeństwa publicznego (np. wyższe kadry oficerskie poszczególnych służb, związek zawodowy policjantów, najemne armie, politycy, przedstawiciele sektora zbrojeniowego, ale również przedstawiciele firm farmaceutycznych czy prywatnych agencji ochrony); 10) bezpieczeństwo jako problem społeczny – w tym proces definiowania konkretnych kwestii bezpieczeństwa; 11) programy i polityki publiczne zwiększające bezpieczeństwo; 12) ruchy społeczne[26].

26 Por. M. Ciesielski, *Co to jest socjologia*…, s. 68–69.

Na chwilę obecną można wskazać, że socjologia bezpieczeństwa wykorzystuje cztery podstawowe podejścia teoretyczne[27], które jednocześnie stanowią jej wkład do szeroko rozumianych nauk o bezpieczeństwie.

Pierwsze podejście to koncepcja teorii bezpieczeństwa państwa socjalnego Niklasa Luhmanna[28], który wskazuje na proces inkluzji politycznej, związanej z bezpieczeństwem socjalnym, ale także z bezpieczeństwem ogólnie oraz towarzyszącymi procesami jurydyzacji i racjonalizacji życia społecznego, a także niebezpieczeństwa totalizacji i infantylizacji[29]. Jednak Niklas Luhmann oferuje socjologii bezpieczeństwa nie tylko swoją teorię bezpieczeństwa państwa socjalnego, ale przede wszystkim jest on twórcą kierunku zwanego teorią systemów autopojetycznych, która pozwala wychwycić pewne mechanizmy właściwe dla współczesnych systemów bezpieczeństwa oraz dla ich styku z otoczeniem społecznym. Wykorzystując dorobek filozofii fenomenologicznej Luhmann położył bowiem mocny nacisk na relację system–środowisko (otoczenie społeczne), gdzie poszczególne funkcjonalne systemy cząstkowe całego społeczeństwa permanentnie się do siebie odnoszą wykorzystując informacje czerpane z dotychczasowych wzajemnych oddziaływań, koncentrując się na wiedzy w jaki sposób skutecznie działać w danym otoczeniu i jak osiągać własne cele. Podstawowym celem systemu jest przetrwanie, możliwe dzięki zdolności dostosowania się do warunków zewnętrznych oraz ciągłemu odróżnianiu się od otoczenia. System według Luhmanna jest autoreferencyjny, czyli sam konstytuuje elementy, jednostki funkcjonalne, z których się składa. Niemiecki teoretyk w swojej koncepcji odwołuje się też do konstruktywizmu[30], w ramach którego istnienie systemów społecznych musi być stwierdzone przez obserwatora – którym jest sam system. W miejsce klasycznej dla funkcjonalizmu różnicy pomiędzy całością i częścią, u Luhmanna uwaga jest skoncentrowana właśnie na różnicowaniu systemu od otoczenia. System jednak odnosi się do otoczenia, a jego tożsamość jest budowana w opozycji do środowiska.

Luhmann podkreślał, że w przypadku niewystarczającego wyodrębnienia się systemu od otoczenia społecznego będziemy mieli do czynienia z osłabieniem możliwości osiągania jego celów. Granice pełnią podwójną funkcję –

27 Por. D. Biłous-Szrejder, O. Nowaczyk, *Metodologia…*, s. 12.

28 N. Luhmann, *Teoria polityczna państwa bezpieczeństwa socjalnego*, Warszawa 1994.

29 „Inkluzja oznacza objęcie wszystkich członków społeczeństwa skutkami działania poszczególnych systemów funkcjonalnych (…)", G. Skąpska, *Prawo a dynamika społecznych przemian*, Kraków 1991, s. 36.

30 W jego własnym ujęciu nawet radykalnego konstruktywizmu.

oddzielania oraz łączenia systemu i środowiska. Dla badania systemów bezpieczeństwa oraz występujących w nich powiązań szczególnie ważne jest spostrzeżenie Luhmanna mówiące, że „jeśli granice są ostro zdefiniowane, to elementy muszą być przypisane albo do systemu, albo do jego środowiska. Relacje natomiast mogą istnieć także między systemem a środowiskiem. Granica oddziela więc elementy, niekoniecznie jednak relacje. Oddziela ona zdarzenia, ale nie blokuje relacji przyczynowych”[31].

Luhmann podkreślał konieczność jasnego wytyczenia granic pomiędzy systemami, granic, które nie są jednak barierami w nawiązywaniu i podtrzymywaniu relacji, ale które będą miały całkowicie inny charakter w każdym systemie bezpieczeństwa. Systemy bezpieczeństwa są bowiem systemami o bardzo ekspansywnym charakterze, ponieważ dążą do częściowego podporządkowania sobie pozostałych systemów społeczeństwa[32]. W ujęciu niemieckiego teoretyka systemy dążą do poszerzenia swoich granic i włączenia nowych obszarów.

Systemy bezpieczeństwa poszczególnych państw z całą pewnością są najbardziej zamkniętymi systemami społeczeństwa w wymiarze operacyjnym. Mocno odróżniają się w relacjach od otoczenia społecznego – tutaj przykładem jest chociażby noszenie mundurów przez żołnierzy i innych przedstawicieli służb mundurowych, którzy w ten sposób, już w chwili nawiązywania interakcji z aktorami innych systemów, akcentują swoją przynależność systemową.

Społeczeństwo, funkcjonując jako całość, wyraźnie nakreśla i chroni swoje granice ze środowiskiem zewnętrznym, organizując w tym celu m.in. wojsko, oraz własny system bezpieczeństwa – wykorzystując do tego administrację państwową. W ramach samego systemu bezpieczeństwa możemy wyróżnić inne podsystemy, które kierują się tymi samymi zasadami autopojetyczności. Przede wszystkim chodzi tutaj o siły zbrojne, które będąc samodzielnym systemem, w celu dokonania własnej reprodukcji będą się koncentrować na innych rodzajach zagrożeń, z którymi mogą się spotkać w ramach danego społeczeństwa. Armia – tak jak inne ogniwa systemu bezpieczeństwa – musi rywalizować o zasoby niezbędne do funkcjonowania i realizacji właściwych sobie zadań. W relacjach międzysystemowych zachodzących na styku systemu bezpieczeństwa z otoczeniem społecznym pojawiają się zagrożenia ekonomiczne

31 N. Luhmann, *Systemy społeczne. Zarys ogólnej teorii*, Kraków 2007, s. 34.

32 Przykładem takiego ekspansywnego mechanizmu przez 1989 r. było wprowadzenie w Polsce stanu wojennego i podporządkowanie wszystkich reguł życia społecznego pod system wojska, czy szerzej – właśnie system bezpieczeństwa.

(niedobór zasobów finansowych) – typowe dla systemu gospodarki – albo zagrożenia sprawowania władzy i podejmowania decyzji – właściwe polityce (niedobór zasobów politycznych). Stąd też bezpieczeństwo, tak jak prawo, władza czy pieniądz, jest medium uniwersalnym. System bezpieczeństwa, w ramach którego znajduje się wojsko, ale także i przemysł zbrojeniowy, odpowiada za ochronę interesów całego społeczeństwa – czyli najszerszej płaszczyzny identyfikacji pozostałych systemów funkcjonalnych – zabezpiecza granice i umożliwia jego reprodukcję, co pośrednio wpływa na bezpieczeństwo wszystkich innych systemów. Najważniejszym procesem systemów społecznych jest komunikacja. W jej wyniku produkowane są ich poszczególne elementy składowe. Autor „Systemów społecznych", nawiązując do Parsonsa, mówi o rozwoju symbolicznie zgeneralizowanych mediów komunikacji, do najważniejszych z nich zalicza prawo, obok pieniądza i władzy.

Prawo jest szczególnym rodzajem komunikacji co powoduje, że podlega właściwym jej prawidłowościom. To w komunikacji właśnie muszą być transponowane fakty i normy. Jak zwraca uwagę Jan Winczorek, takie stanowisko Luhmanna jest redukcjonistyczne – ponieważ opiera się na sprowadzaniu zjawisk normatywnych do zjawisk innego rodzaju[33]. Jednak badając systemy bezpieczeństwa zawsze wychodzimy od analizy aktów prawnych stanowiących o zakresach funkcjonowania poszczególnych instytucji bezpieczeństwa. Za każdą normą prawną kryją się określone cele i wartości, oraz funkcje jawne i ukryte. Stąd też tak istotne jest podejście wykorzystujące analizę prawa, w celu określenia funkcjonalności badanego systemu bezpieczeństwa.

Drugie podejście teoretyczne wykorzystywane w socjologii bezpieczeństwa to koncepcja badań nad bezpieczeństwem narodowym proponowana przez Zdzisława Zagórskiego (również socjologa), odnosząca się do ładu wewnątrzspołecznego, organizującego relacje pomiędzy społeczeństwem, narodem a państwem w otoczeniu zewnętrznym[34]. Zdzisław Zagórski pisząc o socjologii bezpieczeństwa wskazywał na możliwość podjęcia w jej ramach takich tematów, jak specyficzne role segmentów społeczeństwa, przede wszystkim grup powołanych na rzecz szeroko rozumianej obsługi bezpieczeństwa

33 J. Winczorek, *Niklas Luhmann – nowoczesna socjologia prawa* [w:] J. Zajadło (red.), *Przyszłość dziedzictwa*, Gdańsk 2008. Por. także: J. Winczorek, *Niklas Luhmann jako socjolog prawa*, „Rubikon" 2004, nr 1–4.

34 Z. Zagórski, *Wojsko, naród i społeczeństwo w toku polskiej transformacji i integracji europejskiej* [w:] T. Leczykiewicz, Z. Zagórski (red.), *Wojsko w badaniach społecznych*, Wrocław 1998, s. 41–54.

społecznego. Chodzi o role rozmaitych grup dyspozycyjnych policji, wojska, strażaków, ochroniarzy, ratowników, dyplomatów, szpiegów i in., a także pracowników służb socjalnych i zdrowotnych. W tym obszarze dochodzi do częściowego nakładania się na siebie socjologii bezpieczeństwa z socjologią grup dyspozycyjnych – również rozwijaną przez wrocławski ośrodek socjologiczny. Ponadto Zagórski zwraca uwagę także na subiektywne i obiektywizowane sposoby postrzegania zagrożeń i ryzyka, które wchodzą w relacje z rozmaitymi układami i sytuacjami społecznymi, stabilizującymi ład i poczucie bezpieczeństwa grupowego. Innym tematem właściwym dla socjologii bezpieczeństwa jest aktywność ruchów społecznych, związanych z bezpieczeństwem[35].

Trzecie podejście to konstruktywizm (lub konstrukcjonizm). Niniejsze stanowisko teoretyczne jest popularne w socjologii problemów społecznych, ponieważ wskazuje, że podstawową właściwością rzeczywistości społecznej są wyobrażenia oraz przekonania na temat zjawisk społecznych, które same w sobie są nasycone znaczeniami i symboliczną wiedzą. Chodzi o subiektywizację konkretnych zdarzeń i mechanizmów, przez co pewne wyobrażenia i postrzegania stają się realne, rzeczywiste[36]. Duży wkład do konstruktywizmu wnosi językoznawstwo, a sam język jest podstawowym instrumentem tworzenia ram rzeczywistości społecznej. Konstruktywizm jest wartościową koncepcją wykorzystywaną w socjologii bezpieczeństwa nie tylko dlatego, że samo bezpieczeństwo jest jednocześnie podstawowym problemem społecznym[37] – a raczej poszczególne zagrożenia wpływające na jego obniżenie – ale konstruktywizm kładzie nacisk na dynamikę tworzącej się oraz odtwarzanej rzeczywistości, na pewne procesy, które opierają się na kreowaniu przez kluczowych aktorów schematów interpretacyjnych bezpośrednio przekładających się na obiektywne konsekwencje dla systemów społecznych w tym systemów bezpieczeństwa. W proces konstruowania konkretnych ram, obszarów bezpieczeństwa wplatają się wartości oraz interesy reprezentowane i artykułowane przez różne jednostki, w celu przedstawienia społecznej diagnozy takiego stanu rzeczy – czyli zdefiniowania źródeł zagrożeń, często wskazania winnych (personalnie) takiego stanu rzeczy, a na koniec zaprezentowania autorskich środków i metod zaradczych. W takim przypadku zawsze pojawiają się

35 Z. Zagórski, *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?* [w:] T. Leczykiewicz, Z. Zagórski (red.), *Socjologiczne aspekty bezpieczeństwa narodowego*, Wrocław 1999, s. 16.
36 Por. K. Frysztacki, *Socjologia problemów społecznych*, Warszawa 2009, s. 57.
37 A konstruktywizm jest zakorzeniony w socjologii problemów społecznych – patrz: K. Frysztacki, *Socjologia problemów społecznych*, Warszawa 2009.

pytania o to czyje tak naprawdę interesy, i w imieniu jakich wartości, są podejmowane działania mające na celu wzmacnianie bezpieczeństwa. Konstruktywizm ułatwia analizę polityk bezpieczeństwa.

Ostatnie, czwarte podejście teoretyczne wykorzystywane w socjologii bezpieczeństwa to koncepcja bezpieczeństwa międzynarodowego Zbigniewa Brzezińskiego, będąca wypadkową analiz prowadzonych na poziomie mega struktur społecznych – chodzi głównie o zjawisko globalnego przebudzenia, które stanowi rezultat zbiorowej aktywności jednostek do tej pory wykluczanych z dyskursu bezpieczeństwa, a które w konsekwencji potrafią doprowadzić do istotnych zmian społeczno-politycznych, przekładających się także na sferę bezpieczeństwa międzynarodowego. Generalnie koncepcja Brzezińskiego jest wykorzystywana także do tłumaczenia wydarzeń, które miały miejsce 11 września 2001 roku i mocno zakorzenia się w naukach o bezpieczeństwie. Podejście Brzezińskiego wynika także ze zmiany układu sił po zakończeniu zimnej wojny oraz z pojawienia się nowych zagrożeń charakteryzowanych, jako ogromna liczba mikroproblemów powstałych w miejsce dominującego egzystencjalnego zagrożenia, charakteryzującego okres zimnowojenny (dwubiegunowego układu sił)[38].

Przedstawione powyżej koncepcje teoretyczne są tylko punktem wyjścia do pogłębionych rozważań na temat socjologii bezpieczeństwa jako względnie autonomicznej subdyscypliny nauk o bezpieczeństwie. Subdyscypliny, która nie musi być rozpatrywana wyłącznie jako socjologia szczegółowa, ale jako perspektywa analityczna wykorzystywana w naukach o bezpieczeństwie. Socjologia bezpieczeństwa oferuje nie tylko pewną siatkę pojęciową, ale również dysponuje metodami badawczymi, które pozwalają na zbadanie tych wymiarów bezpieczeństwa, które są typowe dla nauk społecznych.

Bezpieczeństwo jest najważniejszą potrzebą społeczną, którą zaspokajają struktury państwa. Jednostki na podstawie umowy społecznej zrzekają się części przysługujących im praw (do prywatności, do dostępu informacji itp.) na rzecz zorganizowanego systemu nadzorowanego i kierowanego przez państwo. Dlatego badając i analizując systemy bezpieczeństwa podstawowe pytanie dotyczy tego, czy spełniają one swoją funkcję, a jeżeli nie, to w jakich obszarach i dlaczego nie zapewniają oczekiwanego poziomu bezpieczeństwa.

38 W dużym zakresie sposób myślenia, postępowania oraz same instytucje są dalej przystosowane do potrzeb dawnego niebezpieczeństwa – stąd też „wojna z terroryzmem", por. Z. Brzeziński, B. Scowcroft, *Ameryka i świat: rozmowy o globalnym przebudzeniu politycznym*, Łódź 2009.

W tym zakresie dużą wartość przedstawia analiza funkcjonalna, jako podejście empiryczne. W socjologii mamy do czynienia z relatywnie dużą swobodą wykorzystania analizy funkcjonalnej. Właściwości przedmiotu badań i konkretnych analiz, którymi są systemy społeczne, uniemożliwiają pełną standaryzację pojęć i procedur analitycznych – zresztą nie tylko w kontekście funkcjonalnym. Bez względu na to, czy procedura badawcza ma charakter diagnostyczny, eksploracyjny bądź eksplanacyjny, to przyjęta terminologia, definicje oraz poziom analizy, pozwalają wyodrębnić i uchwycić różne mechanizmy działania społecznego – obojętnie, czy socjolog chce je tylko opisać, czy wyjaśnić. Tym bardziej jeżeli chodzi o badania całych systemów/podsystemów społecznych, co jest właściwe wszystkim naukom społecznym – zwłaszcza socjologii.

Barry Buzan i Richard Little, autorzy dokonujący analizy historycznej systemów międzynarodowych[39] sprawnie wychwycili pewne uniwersalne właściwości systemów. Odnieśli się bowiem do trzech kluczowych cech, które stanowią o ich właściwościach i pomagają zrozumieć w jaki sposób powstają, działają oraz ewoluują. Są to: 1) zdolność do interakcji; 2) proces; 3) struktura[40].

Autorzy zaznaczyli, że nie kto inny, jak właśnie badacz dysponuje swobodą określania poziomu analizy i może go zdefiniować w skali planetarnej, bądź też może jednostką analizy uczynić całe państwo. W prezentowanym podejściu do pojęcia systemu bezpieczeństwa mówimy o dwóch wymiarach: 1) całego systemu oraz jego 2) poszczególnych podsystemach – np. wojska, polityki, gospodarki i służb specjalnych – które wchodzą ze sobą w stałe interakcje, regulowane przede wszystkim przez prawo.

Zdolność do interakcji oznacza możliwości i predyspozycje do wchodzenia w relacje z innymi systemami społeczeństwa, w celu realizacji właściwych sobie funkcji, ale określa również charakter struktury samego systemu i jego elastyczność. W ten sposób jesteśmy w stanie powiedzieć, że system bezpieczeństwa ma bardzo małą zdolność do interakcji, ponieważ opiera się na zasadzie niejawności stanowiącej integralną część procesu zapewnienia bezpieczeństwa – również w wymiarze całego społeczeństwa, w związku z realizowanymi przez system zadaniami. Komunikacja międzysystemowa w obszarze wymiany informacji jest normatywnie ograniczona poprzez ustawę o ochronie informacji niejawnych, która odwołuje się i umożliwia kategoryzowanie informacji ważnych z punktu widzenia bezpieczeństwa, a co za tym idzie, mocno

39 B. Buzan, R. Little, *Systemy międzynarodowe w historii świata*, Warszawa 2011.
40 Ibidem, s. 109–110.

ogranicza ich dystrybucję. Dlatego też interakcje i powiązania systemu bezpieczeństwa z otoczeniem społecznym powinny wynikać z realizacji zadań na rzecz bezpieczeństwa państwa i obywateli, poprzez stałe utrzymywanie zdolności do walki, obrony całego społeczeństwa.

Na drugim krańcu kontinuum, jeżeli chodzi o zdolność do interakcji, znajduje się gospodarka, ponieważ odwołuje się do reguł o charakterze inkluzywnym, uniwersalnym – do zasad wolnego rynku. Zdolność do interakcji jest wypadkową zależności powstałych pomiędzy pozostałymi dwoma cechami systemu, czyli struktury i procesu. Te natomiast wynikają z właściwości systemów aksjonormatywnych rozumianych także jako podsystemy regulacyjne bądź systemy podtrzymywania wzorów. To na nich oparte jest działanie systemu bezpieczeństwa, polityki czy gospodarki. Najważniejszym podsystemem aksjonormatywnym, to znaczy o największym wpływie na życie społeczne – jest prawo.

Zakończenie

Bezpieczeństwo wchodzi w obszar zainteresowania socjologów, ponieważ analiza społeczeństwa nie może być rzetelnie prowadzona z pominięciem kwestii bezpieczeństwa, które mają bezpośredni i realny wpływ na pozostałe zjawiska, zdarzenia i procesy społeczne. Szczególna relacja jaka łączy bezpieczeństwo z władzą, polityką, prawem czy wojskiem powoduje, że socjolodzy cały czas poszukują sposobu na naukowe (socjologiczne) podejście do tego zagadnienia. Tym bardziej, że kwestie bezpieczeństwa wyraźnie pojawiają się przy rozpatrywaniu zagadnień gospodarczych, edukacyjnych, migracji, tożsamości kulturowej i wielu innych kluczowych dla badań socjologicznych.

Dlaczego natomiast socjologia bezpieczeństwa może być (i powinna być) rozpatrywana jako subdyscyplina z obszaru nauk o bezpieczeństwie a nie wyłącznie jako subdyscyplina socjologiczna? Odpowiedź na to pytanie jest konsekwencją definiowania nauk o bezpieczeństwie jako dyscypliny nauk społecznych. Przy czym należy podkreślić, że tożsamość nauk o bezpieczeństwie w Polsce dopiero się kształtuje. W dyskursie naukowym na temat bezpieczeństwa cały czas ścierają się różne koncepcje jego pojmowania oraz sposobu

definiowania samych nauk o bezpieczeństwie[41]. W Polsce nauki o bezpieczeństwie zalicza się do nauk społecznych, które od 2011 r. cały czas są jeszcze na wczesnym etapie[42]. Stąd też ograniczanie, redukowanie i przyjmowanie utartych schematów z innych dyscyplin naukowych może być problemem dla samego procesu kształtowania się nauk o bezpieczeństwie. Ze względu na fakt, że mówimy o dziedzinie nauk społecznych niektórzy mogliby redukować pojmowanie bezpieczeństwa do perspektywy socjologicznej – wówczas podkreślanie odrębności socjologii bezpieczeństwa, czy też jej specyfiki na tle nauk o bezpieczeństwie nie miałoby sensu. Wówczas nauki o bezpieczeństwie ograniczałyby podejście do teorii bezpieczeństwa, która nie może być redukowana do perspektywy socjologicznej. Wydaje się, że powinno być odwrotnie: to socjologia bezpieczeństwa ma pomóc budować teorię bezpieczeństwa zwracając uwagę m.in. na kwestie procesów społecznych wpływających na bezpieczeństwo w ujęciu subiektywnym (poczucie bezpieczeństwa) oraz obiektywnym (procesy społeczne zachodzące na styku polityki, wojska, gospodarki, służb itp.).

Socjologia bezpieczeństwa może się sprawdzić zarówno w socjologii, jak i naukach o bezpieczeństwie. W tym kontekście warto zwrócić uwagę chociażby na socjologię prawa, która z powodzeniem jest wykładana na wydziałach prawa, ale także i w instytutach socjologii w Polsce i na świecie. Pisząc pracę doktorską z zakresu socjologii prawa na Wydziale Prawa można uzyskać stopień doktora nauk prawnych, w Instytucie Socjologii – doktora nauk społecznych w zakresie socjologii. Broniąc pracę dyplomową z zakresu socjologii religii można zarówno uzyskać stopień naukowy z socjologii, jak i religioznawstwa. Nie chodzi więc o wytyczenie ścisłych granic między autonomicznymi dyscyplinami, ale o zwrócenie uwagi, jak te subdyscypliny przenikają granice poszczególnych dyscyplin (łączą je?) i wskazują mnogość wykorzystania. Taką subdyscypliną może stać się socjologia bezpieczeństwa. W socjologii prawa doszło do wyodrębnienia się nurtu socjocentrycznego i prawnocentrycznego, gdzie pierwszy ujmuje tę dyscyplinę (subdyscyplinę) jako część socjologii obok socjologii religii, socjologii moralności, socjologii medycyny i innych. Natomiast drugi traktuje socjologię prawa jako część prawoznawstwa[43]. War-

41 Por. A. Misiuk, *O tożsamości nauk o bezpieczeństwie*, „Historia i Polityka" 2018, nr 23, s. 9–19.

42 Od 2018 roku do nauk o bezpieczeństwie zalicza się również obszar wcześniej właściwy dla nauk o obronności.

43 A. Pieniążek, M. Stefaniuk, *Socjologia prawa. Zarys wykładu*, Warszawa 2014, s. 9.

to zastanowić się czy do takiej sytuacji może dość w przypadku socjologii bezpieczeństwa. W przypadku socjologii (a konkretnie samych socjologów) wydaje się, że nic nie stoi na przeszkodzie, pod warunkiem dostrzeżenia wartości naukowej prac badawczych ujmujących zagadnienia bezpieczeństwa z perspektywy socjologicznej. Kolejnym krokiem jest instytucjonalizacja socjologii bezpieczeństwa m.in. poprzez tworzenie odpowiednich zakładów i katedr w instytutach socjologii na uniwersytetach i uczelniach w całej Polsce. Pomimo ugruntowanej pozycji socjologii na polskich uniwersytetach, trudno spotkać katedrę czy zakład socjologii bezpieczeństwa. Tutaj należy podkreślić wysiłki profesorów Zdzisława Zagórskiego i Jana Maciejewskiego z Uniwersytetu Wrocławskiego – w przypadku tego drugiego w dużym zakresie z perspektywy socjologii grup dyspozycyjnych – ale także profesora Andrzeja Zybertowicza z Uniwersytetu im. Mikołaja Kopernika w Toruniu, którzy jako nieliczni podejmują próby instytucjonalizacji socjologii bezpieczeństwa w Polsce. Warto również zwrócić uwagę na aktywność profesora Eugeniusza Moczuka z Politechniki Rzeszowskiej.

Podobnie ścieżka powinna wyglądać w przypadku nauk o bezpieczeństwie. Nic nie stoi na przeszkodzie aby zaczęły powstawać odpowiednie zakłady, katedry i instytuty na uczelniach specjalizujących się w badaniu bezpieczeństwa i obronności – nie tylko wojskowych. O ile tradycja socjologii wojska w Polsce i na świecie jest bogata – zwłaszcza w socjologii amerykańskiej – to już socjologia bezpieczeństwa rzadko jest postrzegana jako odrębna subdyscyplina. W przypadku socjologii, tak jak i nauk o bezpieczeństwie, w chwili obecnej mamy bardziej do czynienia z badaniem socjologicznych aspektów bezpieczeństwa. Nie chodzi wyłącznie o słabą instytucjonalizację socjologii bezpieczeństwa, ale o brak syntetycznej i kompleksowej teorii bezpieczeństwa bazującej na dorobku socjologów. Istotne jest aby przejść od badania fragmentów rzeczywistości społecznej, pojedynczych tematów związanych z bezpieczeństwem; takich jak poczucie bezpieczeństwa poszczególnych społeczności czy społeczeństwa, wpływ migracji na bezpieczeństwo obywateli, organizacja struktur administracyjnych państwa odpowiadających za bezpieczeństwo. Oczywiście są to właściwe tematy dla socjologii bezpieczeństwa, ale ważne jest aby podjąć próbę identyfikowania bezpieczeństwa jako problemu, wokół którego może być budowana teoria socjologiczna tłumacząca złożoność życia społecznego, jego organizację, zmiany struktur społecznych oraz pozwalająca podjąć próbę przewidywania zjawisk społecznych. Możliwe, że na obecnym etapie jest to bardziej realne na gruncie nauk o bezpieczeństwie niż samej socjologii. Właśnie ze względu na ciągły proces poszukiwania tożsamości

i kształtowania się nauk o bezpieczeństwie – w odróżnieniu od konkretnych nurtów i tendencji panujących we współczesnej polskiej socjologii.

Dlatego też w ujęciu nauk o bezpieczeństwie analityczne wyodrębnienie bezpieczeństwa jako przedmiotu badań nie powinno prowadzić do marginalizacji pozostałych problemów badawczych, którymi zajmują się badacze społeczni. Badacz zajmujący się bezpieczeństwem, które jest zdefiniowane jako przedmiot badań nauk społecznych jest poniekąd zobligowany do uwzględnienia pozostałych wymiarów życia społecznego. Nie oznacza to jednak, że jedynie socjologia i socjolodzy reprezentują właściwe podejście. Dotyczy to również pozostałych badaczy społecznych, tj. zajmujących się naukami politycznymi, ekonomicznymi, prawnymi, pedagogicznymi, o zarządzaniu i jakości czy właśnie naukami o bezpieczeństwie[44].

Od pewnego czasu mamy do czynienia z bardzo interesującą sytuacją w obszarze szeroko rozumianego bezpieczeństwa. Można powiedzieć, że następuje pewna zmiana paradygmatu, w wyniku której zagrożenia terrorystyczne powoli ustępują miejsca zagrożeniom o charakterze ekonomicznym – mniej więcej od przełomu 2008/2009 roku. Poszczególne rodzaje bezpieczeństwa są jednak ze sobą bardzo mocno powiązane, a to wpływa na specyfikę działania poszczególnych służb zajmujących się bezpieczeństwem państwa. W zależności od potrzeb, konkretne instytucje są w odpowiedni sposób profilowane, także dlatego, że rodzaje niektórych zagrożeń wzajemnie się warunkują. Takim przykładem jest przestępczość o charakterze ekonomicznym w obszarze bezpieczeństwa państwa, związana m.in. z pozyskiwaniem sprzętu wojskowego. Jakość i skuteczność pozyskiwanego dla armii sprzętu bezpośrednio przekłada się na bezpieczeństwo żołnierzy, a pośrednio na potencjał obronny armii i bezpieczeństwo państwa. Ewentualna niegospodarność narażająca na straty budżet resortu obrony oznacza obniżenie zdolności obronnych państwa. Subiektywne odczucia społeczne rzadko zakładają powyższą zależność. Przypadki korupcji przy zakupach uzbrojenia nie są identyfikowane przez opinię publiczną jako zagrożenie dla bezpieczeństwa państwa i obywateli. Inaczej niż w przypadku zamachów terrorystycznych w USA, Londynie i Madrycie. Pomimo iż na terytorium Polski w okresie ostatnich lat doszło tylko do jednego istotnego incydentu o charakterze terrorystycznym – udaremnienia zamachu na najwyższe władze państwa planowanego przez Brunona K., to jednak opinia

44 Por. rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

publiczna zarówno nad Wisłą, jak i w innych krajach Unii Europejskiej, czuje realne zagrożenie ze strony potencjalnych terrorystów. Ewidentny wpływ na to ma aktywność mediów i widowiskowość ataków terrorystycznych – oglądanych live na całym świecie.

Na tym polu krystalizuje się właśnie zakres badań nad drugim wymiarem bezpieczeństwa – wymiarem systemu społecznego. Procesy polityczno-społeczne dotyczące bezpieczeństwa są tu rozpatrywane z perspektywy działania otwartego i rozwijającego się systemu. Niniejszy wymiar bezpieczeństwa orientuje badacza na poszukiwanie związków między istniejącymi, wchodzącymi w jego skład podsystemami (konkretnymi strukturami) a otaczającym środowiskiem[45]. W tym kontekście wojsko prezentuje się jako kluczowy podsystem, element struktur bezpieczeństwa państwa, wchodzący w permanentne interakcje ze swoim otoczeniem[46]. Siły zbrojne są najważniejszym ogniwem każdego systemu bezpieczeństwa, generującym największe koszty w utrzymaniu. Wymiar militarny jest natomiast najważniejszym wymiarem bezpieczeństwa państwa, ponieważ stanowi o jego możliwościach obronnych i – wbrew temu co zdają się sugerować niektórzy naukowcy – jego znaczenie nie zmniejszyło się w ostatnim czasie na rzecz bezpieczeństwa ekonomicznego, ekologicznego, środowiskowego itp. Bezpieczeństwo było, jest i najprawdopodobniej nadal będzie przede wszystkim domeną państw narodowych, a tutaj kluczową rolę odgrywają siły zbrojne oraz służby specjalne.

Pomiędzy poszczególnymi typami bezpieczeństwa możemy dostrzec wyraźne zależności. Bezpieczeństwo ekonomiczne wpływa na bezpieczeństwo militarne, bezpieczeństwo energetyczne kształtuje ekonomiczne, wewnętrzne narażone jest na zagrożenia o charakterze ekologicznym, militarnym oraz ekonomicznym itp. Zależności te znajdują swoje odzwierciedlenie w strukturach społecznych, które w dużym zakresie będą na siebie nachodzić, a także wchodzić ze sobą w intensywne relacje, oraz w decyzjach politycznych. W niektórych przypadkach będziemy mogli dostrzec zmiany pojedynczych obszarów życia społecznego, w innych – całej, kompleksowej polityki względem społeczeństwa. Tak dzieje się w przypadku konieczności zapewnienia bezpieczeństwa socjalnego, czyli określonych świadczeń socjalnych kierowanych

45 Por. E. Moczuk, *Socjologiczne aspekty bezpieczeństwa lokalnego*, Rzeszów 2009, s. 60.
46 Por. Z. Zagórski, *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?* [w:] T. Leczykiewicz, Z. Zagórski (red.), *Socjologiczne aspekty bezpieczeństwa narodowego*, Wrocław 1999.

do konkretnych warstw społecznych[47]. Wyjątkowe miejsce odgrywa zależność bezpieczeństwa militarnego od czynników ekonomicznych związanych z przepływem i wymianą zasobów. Zagrożenia ekonomiczne w tym przypadku są wypadkową powiązań sił zbrojnych i pozostałych służb dyspozycyjnych z dwoma głównymi rodzajami struktur społecznych – polityki oraz gospodarki. Armia ze względu na swoją ważną rolę ochrony bezpieczeństwa państwa jest – albo przynajmniej powinna być – beneficjentem tych powiązań, ponieważ tylko w ten sposób, nawiązując interakcje ze środowiskiem zewnętrznym, może zdobyć niezbędne do swojego funkcjonowania zasoby. Przepływ zasobów oraz relacje wojska z polityką i gospodarką są regulowane przez prawo. Charakter prawa, jego efektywność i adekwatność, nie tylko określa relacje w ramach systemu bezpieczeństwa i na jego styku z otoczeniem społecznym, ale wskazuje na możliwości ich ewentualnego wykorzystania do zaspokajania innych potrzeb, typowych dla sfery polityki i biznesu.

Socjologia bezpieczeństwa rozpatruje bezpieczeństwo uwzględniając jego złożoność i wieloaspektowość, co oznacza możliwość jego badania na trzech płaszczyznach: 1) płaszczyźnie obiektywnej – rzeczywistych uwarunkowań bezpieczeństwa; 2) płaszczyźnie subiektywnej – społecznej percepcji bezpieczeństwa, jego uwarunkowań i technik identyfikacji zagrożeń; 3) płaszczyźnie responsywnej – społecznych reakcji na subiektywnie rozpoznane i zdefiniowane zagrożenia dla bezpieczeństwa. Przedmiotem refleksji socjologicznej może być każda z tych płaszczyzn z osobna, jak i relacje pomiędzy nimi – wzajemne zależności, sprzężenia zwrotne – na tle ładu społecznego i reprodukowania wzorów zachowań w różnych kontekstach społecznych[48].

Badając bezpieczeństwo należy pamiętać o jego dużej dynamice, którą można wychwycić wykorzystując podejście procesualne, które – parafrazując socjologa Piotra Sztompkę – zakłada proces stawania się bezpieczeństwa. Sztompka mówiąc o stawaniu się społeczeństwa miał na myśli ustawiczny proces samoprzekształcania się i samotworzenia społeczeństwa w wyniku stale odtwarzającego się, nieuchronnego napięcia między potencjalną podmiotowością społeczeństwa, a jego aktualną praktyką społeczno-historyczną (zdarzeniami społecznymi)[49]. W przypadku bezpieczeństwa natomiast, także można powiedzieć o jego stawaniu się, do którego dochodzi w wyniku napięcia

47 Zob. N. Luhmann, *Teoria polityczna państwa bezpieczeństwa socjalnego*, Warszawa 1994.
48 M. Ciesielski, *Co to jest socjologia…*, s. 64.
49 P. Sztompka, *Socjologia…*, s. 536.

zachodzącego pomiędzy rzeczywistymi uwarunkowaniami, stanami systemu bezpieczeństwa (płaszczyzna obiektywna), a społeczną percepcją bezpieczeństwa, jego uwarunkowań i technik identyfikacji zagrożeń (płaszczyzna subiektywna). W rezultacie cały czas jest odtwarzany proces polegający na złożonych społecznych reakcjach na subiektywnie rozpoznane i zdefiniowane zagrożenia, a te reakcje niekoniecznie muszą być adekwatne do rzeczywistego stanu zagrożenia (płaszczyzna responsywna). Inaczej mówiąc, identyfikowanie i postrzeganie stanu bezpieczeństwa przez społeczeństwo, nawet w sposób nieuzasadniony, przerysowany, bądź nieadekwatny, może prowadzić do realnych działań tworzących nową rzeczywistość. W konsekwencji dochodzi do ciągłego stawania się bezpieczeństwa – czyli zmian w strukturach systemu bezpieczeństwa, spowodowanych nie tylko jego samoprzekształcaniem, ale przede wszystkim wpływem opinii publicznej.

Socjologia bezpieczeństwa nie przyjęła się jako subdyscyplina socjologiczna – nie tylko w Polsce – o czym świadczą nieliczne publikacje z tego zakresu w socjologicznych periodykach. Można zaryzykować tezę, że środowisko polskich socjologów[50] nie dostrzegało – i nadal nie dostrzega – potencjału tej subdyscypliny, kwestionując jej wartość naukową. Powszechnie przywołuje się w tym kontekście tendencję do tworzenia coraz liczniejszych subdyscyplin socjologicznych, które nie są w stanie nawet precyzyjne zdefiniować swojego obszaru badawczego. Z drugiej strony warto podkreślić, że środowisko socjologiczne zaakceptowało i dostrzegło wartość takich subdyscyplin jak socjologia emocji, socjologia wizualna, socjologia internetu, socjologia filmu, socjologia jedzenia czy socjologia muzyki. W świetle powyższego trudno zaakceptować stanowisko, że socjologia bezpieczeństwa nie jest w stanie zaoferować więcej niż socjologia jedzenia, czy socjologia filmu, zwłaszcza pamiętając, że bezpieczeństwo jest identyfikowane na płaszczyźnie całych systemów społecznych i odwołuje się do złożonej struktury administracyjnej organizującej chociażby służby dyspozycyjne, takie jak wojsko, czy policja. W odróżnieniu od muzyki, filmu czy emocji, które odwołują się do bardzo wąskich kontekstów społecznych, które są problematyczne chociażby dla rozwoju i możliwości aplikacyjnych bardziej złożonych koncepcji teoretycznych. Jednak z chwilą, kiedy powołano do życia nauki o bezpieczeństwie, zdefiniowane jako nauki o współczesnych systemach bezpieczeństwa, które mają przede wszystkim wymiar

50 Poza wskazanymi już powyżej nielicznymi wyjątkami skoncentrowanymi przede wszystkim wokół ośrodków akademickiej socjologii we Wrocławiu, Toruniu oraz Rzeszowie.

społeczny, warto podjąć działania, aby popularyzować socjologię bezpieczeństwa jako subdyscyplinę nauk o bezpieczeństwie, dla których wyżej opisany przedmiot badań socjologii bezpieczeństwa z pewnością wpisuje się do głównego nurtu teoretycznego oraz empirycznego. Socjologia bezpieczeństwa wydaje się być bardzo interesującą propozycją subdyscypliny nauk o bezpieczeństwie, wokół której mogą się ogniskować zainteresowania badawcze właściwe dla pierwszej tendencji – nurtu badań mechanizmów społecznych systemów bezpieczeństwa.

Bibliografia

Literatura

Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2013.
Biłous-Szrejder D., O. Nowaczyk, *Metodologia bezpieczeństwa narodowego* [w:] J. Maciejewski (red.), *Socjologiczne aspekty bezpieczeństwa narodowego*, Wrocław 2001.
Brzeziński Z., *Cztery lata w Białym Domu. Wspomnienia*, Warszawa 1990.
Brzeziński Z., Scowcroft B., *Ameryka i świat: rozmowy o globalnym przebudzeniu politycznym*, Łódź 2009.
Buzan B., Little R., *Systemy międzynarodowe w historii świata*, Warszawa 2011.
Ciesielski M., *Co to jest socjologia bezpieczeństwa (publicznego)?* [w:] G. Bryda (red.), *Światy i konteksty społeczne. Krakowskie Spotkania Socjologiczne*, t. II, Kraków 2011.
Durkheim E., *Zasady metody socjologicznej*, Warszawa 1979.
Frysztacki K., *Socjologia problemów społecznych*, Warszawa 2009.
Kaczmarczyk M., *System społeczny a dylematy działania*, t. VII, Kraków 2009.
Korwin-Szymanowska A., *Psychospołeczne aspekty poczucia bezpieczeństwa* [w:] *Bezpieczeństwo jako wartość*, Kraków 2010.
Luhmann N., *Systemy społeczne. Zarys ogólnej teorii*, Kraków 2007.
Luhmann N., *Teoria polityczna państwa bezpieczeństwa socjalnego*, Warszawa 1994.
Maciejewski J. (red.), *Grupy dyspozycyjne społeczeństwa polskiego*, Wrocław 2006.
Misiuk A., *O tożsamości nauk o bezpieczeństwie*, „Historia i Polityka" 2018, nr 23.
Moczuk E., *Socjologiczne aspekty bezpieczeństwa lokalnego*, Rzeszów 2009.
Parsons T., *System społeczny*, Kraków 2009.
Pieniążek A., Stefaniuk M., *Socjologia prawa. Zarys wykładu*, Warszawa 2014.
Skąpska G., *Prawo a dynamika społecznych przemian*, Kraków 1991.
Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.
Szacki J., *Historia myśli socjologicznej*, Warszawa 2002.
Sztompka P., *Logika analizy funkcjonalnej w socjologii i antropologii społecznej* [w:] S. Nowak (red.), *Metodologiczne problemy teorii socjologicznych*, Warszawa 1971.
Sztompka P., *Socjologia. Analiza społeczeństwa*, Kraków 2003.
Turner J.H., *Struktura teorii socjologicznej*, Warszawa 2005.
Williams P.D., *Badania bezpieczeństwa. Wprowadzenie* [w:] P.D. Williams (red.), *Studia bezpieczeństwa*, Kraków 2012.
Winczorek J., *Niklas Luhmann jako socjolog prawa*, „Rubikon" 2004, nr 1–4.
Zagórski Z., *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?* [w:] T. Leczykiewicz, Z. Zagórski (red.), *Socjologiczne aspekty bezpieczeństwa narodowego*, Wrocław 1999.
Zagórski Z., *Wojsko, naród i społeczeństwo w toku polskiej transformacji i integracji europejskiej* [w:] T. Leczykiewicz, Z. Zagórski (red.), *Wojsko w badaniach społecznych*, Wrocław 1998.

Ziółkowski M., *Teorie systemu i funkcjonalizm* [w:] A. Jasińska-Kania, L.M. Nijakowski, J. Szacki, M. Ziółkowski (red.), *Współczesne teorie socjologiczne*, t. I, Warszawa 2006.

Akty prawne

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. nr 179, poz. 1065).

Uchwała Centralnej Komisji do Spraw Stopni i Tytułów z dnia 28 stycznia 2011 r. zmieniająca uchwałę w sprawie określenia dziedzin nauki i dziedzin sztuki oraz dyscyplin naukowych i artystycznych (M.P. nr 14, poz. 149).

Sociology of Security as Subdiscipline of Security Sciences

Abstract

The article addresses two key issues: What causes security to include in the area of interest of sociologists? Why can sociology of security be considered as a subdiscipline of security science and not as a sociological subdiscipline?

From a sociological point of view, security is a key element of social life that ensures social balance. Sociologists point out that security is primarily subjective, it is constructed by actors because of their own expectations and interests, also refers to specific circumstances of an objective nature – phenomena, structures and social processes.

The publication presents the structure of security systems considered as the subject of sociology of security.

Key words: security, sociology of security, security systems, security sciences

Monika Nowikowska*

Odpowiedzialność za naruszenie prawa autorskiego w internecie

Streszczenie

Internet jest podstawowym źródłem informacji. Z punktu widzenia prawa autorskiego, zauważa się coraz więcej problemów prawnych związanych z korzystaniem z utworów w internecie. Artykuł ma na celu omówienie zjawiska naruszenia prawa autorskiego w internecie. W pierwszej części zostały wskazane przypadki naruszenia prawa twórców w internecie. W dalszej części omówione zostało zagadnienie odpowiedzialności. W rozpowszechnianiu materiałów w internecie bierze udział wiele podmiotów. Zasady odpowiedzialności zostały uregulowane w ustawie o świadczeniu usług drogą elektroniczną. Wśród podmiotów tych ustawodawca wyróżnia *access providera, service providera i host providera*. Kryterium uznania odpowiedzialności prawnej administratorów serwerów uczestniczących w wymianie informacji w sieci dotyczy głównie tego, czy mają oni wpływ na umieszczane w sieci treści.

Słowa kluczowe: prawo autorskie, internet, access provider, service provider, host provider, utwór, odpowiedzialność

* Dr Monika Nowikowska, Akademia Sztuki Wojennej, e-mail: monika.nowikowska@gmail.com, ORCID: 0000-0001-5166-8375.

Wstęp

Postęp nowych technologii oraz rozwój społeczeństwa informacyjnego[1] wywierają ogromny wpływ na prawo autorskie, otwierając jednocześnie nowe możliwości naruszeń prawa autorskiego. Podstawowym źródłem informacji w społeczeństwie informacyjnym jest internet, który umożliwia łatwy dostęp do zasobów informacyjnych. Internet stanowi nierozerwalną część życia niemal każdego społeczeństwa. Należy podkreślić, że trudna do przecenienia jest pozytywna rola internetu. Z punktu widzenia prawa autorskiego, zauważa się jednak coraz więcej problemów prawnych związanych z korzystaniem z utworów w internecie. Wiele nowych zjawisk wymyka się tradycyjnym rozwiązaniom prawnym zwartym w ustawie o prawie autorskim i prawach pokrewnych[2]. Rodzi to trudności związane z dopasowaniem istniejących już rozwiązań do nowych stanów faktycznych związanych z eksploatacją utworów w internecie[3].

Podjęte w artykule rozważania mają na celu udzielenie odpowiedzi na pytanie, jakie są przyczyny zjawiska naruszania praw autorskich w internecie. Powszechnie przyjmuje się, że dostępność internetu przekłada się na fakt, że wszystko, co się w nim „znajduje", jest darmowe i można z tego swobodnie korzystać. Takie przekonanie wynika z braku świadomości prawnej i wiedzy użytkowników internetu na temat konieczności poszanowania własności intelektualnej. Powyższe implikuje kolejne pytanie, mianowicie: kto ponosi odpowiedzialność za naruszenie prawa autorskiego w internecie oraz jaka jest świadomość użytkowników w przedmiocie odpowiedzialności za naruszenie prawa autorskiego. Wreszcie, czy obowiązujące rozwiązania prawne skutecznie chronią prawa autorskie w internecie.

1 W literaturze przedmiotu wskazuje się, że informacja i internet wzbogacają zasoby wiedzy, przy czym internet pozwala na swobodny przepływ wartości i ideałów. Kategorie te mają wpływ na jakość życia ludzi, politykę, wspieranie procesów decyzyjnych, rozwój gospodarczy, poznanie obszarów rzeczywistości i zdobyczy kulturowych człowieka, stąd mowa o „społeczeństwie informacyjnym". Zob. szerzej: W. Kitler, *Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne* [w:] W. Kitler, J. Taczkowska-Olszewska (red.), *Bezpieczeństwo informacyjne*, Warszawa 2017, s. 32; T. Globan-Klas, P. Senkiewicz, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999.

2 Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2019 r., poz. 1231).

3 Z. Zawadzka, *Prawo autorskie w Internecie* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej*, cz. I, *Prawo autorskie i prawa pokrewne*, Warszawa 2018, s. 309.

W literaturze przedmiotu wskazuje się, że do najczęstszych sposobów nieuprawnionego korzystania z utworów w internecie zalicza się zamieszczanie cudzego utworu (np. fotograficznego) jako ilustracji do strony internetowej, zapisywanie utworów w pamięci komputera, udostępnianie odesłań (linków) do cudzych stron internetowych, pobieranie utworów muzycznych, w tym również takich, które nie zostały rozpowszechnione za zezwoleniem twórcy czy przesyłanie strumieniowe (streaming)[4]. Przywołane wyżej sposoby eksploatacji utworów w internecie mogą stanowić naruszenie prawa autorskiego. Ustawa o prawie autorskim i prawach pokrewnych nie reguluje wprost wskazanych zagadnień. Innym zagadnieniem jest dostarczanie usług, posługiwanie się sieciami komputerowymi oraz związane z tym problemy ponoszenia odpowiedzialności za treści rozpowszechniane w internecie. Jak zatem w całym systemie dostępu do informacji za pośrednictwem internatu rozkłada się odpowiedzialność za naruszenie praw autorskich twórcy, którego utwór bezprawnie umieszczono, udostępniono i rozpowszechniono. Kiedy odpowiedzialność za naruszenie prawa autorskiego w internecie ponosi użytkownik, a kiedy dostawca zawartości sieci lub usług w sieciach? Czy prawo autorskie nadąża za postępem technologicznym? Dyskusja przedmiotowego zagadnienia determinowana będzie przez wyżej postawione pytania.

Odpowiedzialność za naruszenie prawa autorskiego przez podmioty uczestniczące w rozpowszechnianiu materiałów w internecie

Ważnym problemem z punktu widzenia ochrony praw autorskich w internecie jest bezprawne udostępnianie poprzez sieci informatyczne chronionych na gruncie ustawy o prawie autorskim i prawach pokrewnych materiałów – „utworów”[5]. W rozpowszechnianiu materiałów w internecie bierze udział wiele podmiotów. Wśród podmiotów tych można wymienić trzy kategorie[6]: *contetnt provider*, *access provider*, *service provider* (*host provider*). Rozróżnienie

4 J. Barta, R. Markiewicz, *Prawo autorskie*, Warszawa 2016, s. 461.

5 Zob. szerzej nt. utworu jako przedmiotu prawa autorskiego M. Nowikowska, *Utwór jako przedmiot prawa autorskiego* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo…*, s. 64–89.

6 J. Barta, R. Markiewicz, A. Matlak, *Prawo autorskie w społeczeństwie informacyjnym* [w:] *System Prawa Prywatnego*, t. 13, *Prawo autorskie*, Warszawa 2017, s. 1307.

to rodzi pytanie o zakres ich odpowiedzialności z tytułu naruszenia praw autorskich.

Content provider jest to dostawca treści, dostawca zawartości sieci, który dostarcza i wprowadza do sieci treść, w tym chroniony prawem autorskim materiał. *Access provider* jest to dostawca dostępu do sieci i dysponent sieci telekomunikacyjnej, który oferuje dostęp do obcych źródeł internetu, zapewniając „techniczny transfer" danych. Natomiast *service provider* jest to dostawca usług internetowych, który świadczy usługi związane z przechowywaniem, przekazywaniem i udostępnianiem informacji na rzecz końcowych użytkowników sieci[7].

Zasady odpowiedzialności za naruszenie prawa autorskiego w internecie ww. podmiotów uzależnione są od rodzaju świadczonej usługi. Na gruncie prawa polskiego zagadnienie odpowiedzialności za naruszenie praw autorskich w internecie reguluje ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[8]. Na gruncie tej ustawy można wyróżnić odrębne zasady odpowiedzialności w odniesieniu do trzech różnych sfer działalności dokonywanych przez usługodawców: *mere conduit*, *caching* oraz *hosting*[9].

Mere conduit obejmuje usługi, które polegają wyłącznie na pośrednictwie w dostępie do sieci telekomunikacyjnej. Usługi ograniczają się do przenoszenia w sieci informacji wprowadzonej przez użytkownika tzw. zwykły przesył[10]. Podmiot świadczący te usługi to tzw. *internet service provider*, czyli dostawca usług internetowych.

Caching obejmuje przechowywanie, czyli automatyczne, pośrednie i czasowo ograniczone (krótkotrwałe) zapisywanie informacji, które ma na celu podniesienie efektywności i przyspieszenie ich udostępnienia na życzenie użytkownika usługi. Dzięki stosowaniu powyższego procesu kopia ściągniętych z odległego serwera danych, po ich dalszej transmisji do urządzenia końcowego użytkownika, jest przez pewien czas przechowywana na najbliższym serwerze. Przy ponownym transmitowaniu na żądanie użytkownika sieci telekomunikacyjnej danych przechowywanych w ramach *cachingu* transmisja

7 Z. Zawadzka, *Prawo…*, s. 319.

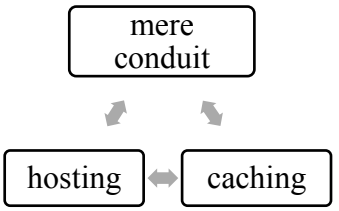
8 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344) dalej ustawa ś.u.d.e.

9 G. Rączka, *Prawne zagadnienia hostingu*, „Przegląd Prawa Handlowego" 2009, nr 4, s. 31; wyrok SA w Łodzi z dnia 13 stycznia 2017 r., I ACa 884/16, LEX nr 2250053; wyrok SA w Warszawie z dnia 12 stycznia 2017 r., VI ACa 1579/15, LEX nr 2249981.

10 M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011, s. 231.

następuje nie z pierwotnego (dalszego) serwera, lecz z bliższego, na którym przy poprzedniej transmisji została wykonana kopia danych[11]. *Caching* polega zatem na przechowywaniu danych w celu zwiększenia efektywności późniejszych transmisji dokonywanych na rzecz innych osób na ich żądanie[12].

Natomiast *hosting* polega na zapewnieniu miejsca na serwerach włączonych do sieci telekomunikacyjnej dla osób trzecich, które przechowują, gromadzą i udostępniają wprowadzane przez siebie informacje[13].



Usługę *cachingu* trzeba wyraźnie oddzielić od usługi automatycznego i krótkotrwałego pośredniego przechowywania transmitowanych danych oraz usługi *hostingu*. Wszystkie trzy usługi polegają na przechowywaniu danych, natomiast tym, co je odróżnia od siebie, jest cel, w jakim dane są przechowywane. Celem usługi automatycznego i krótkotrwałego pośredniego przechowywania danych jest umożliwienie przeprowadzenia transmisji danych. Istotą *cachingu* jest przyspieszenie transmisji danych i zwiększenie efektywności samej sieci internet poprzez ograniczenie zbędnych transmisji danych. W ramach usługi *hostingu* nie jest w ogóle związane z transmisją danych w sieci telekomunikacyjnej. W ramach tej usługi usługodawca udostępnia użytkownikom internetu lub innej sieci telekomunikacyjnej zasoby systemu teleinformatycznego, dzięki czemu mogą oni przechowywać tam swoje własne dane. Odmienne cele tych usług determinują również różny czas przechowywania danych w ich ramach[14].

11 A. Matlak, *Prawo autorskie w społeczeństwie informacyjnym*, Kraków 2004, s. 176; W. Chomiczewski, *Komentarz do art. 13* [w:] D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, LEX 2011.

12 Szerzej: K. Wójcik, *Usługa cachingu. Wyłączenie odpowiedzialności z tytułu świadczenia usług drogą elektroniczną* [w:] A. Niewęgłowski, M. Chrzanowski (red.), *Internet a prawo autorskie*, Lublin 2016, s. 104; D.K. Gęsicka, *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników*, Warszawa 2014, s. 222.

13 Z. Zawadzka, *Prawo autorskie w Internecie* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo…*, s. 321.

14 W. Chomiczewski, *Komentarz do art. 13* [w:] D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, LEX 2011.

Najmniej wątpliwości budzi kwestia odpowiedzialności dostawcy zawartości treści (*content provider*) za naruszenie prawa autorskiego w internecie. Dostawcą zawartości treści jest osoba lub instytucja, która udostępnia innym osobom poprzez sieci komputerowe treści. Jeśli udostępnia materiały własne (przez siebie stworzone), a więc jest ich autorem lub posiada autorskie prawa majątkowe do tych materiałów, problem odpowiedzialności prawnoautorskiej w internecie nie istnieje. Podmiot taki może ponosić odpowiedzialność na innych zasadach, np. prawa karnego, jeśli udostępniane treści dotyczą pedofilii.

Odpowiedzialność dostawcy usług (*service provider*) za naruszenie prawa autorskiego w internecie została szczegółowo uregulowana w ustawie ś.u.d.e. Ustawodawca w art. 1 ust. 1 pkt 2 określił odpowiedzialność usługodawcy od strony negatywnej, tj. poprzez określenie zasad wyłączania odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną.

Zgodnie z dyspozycją art. 12 ust. 1 ustawy ś.u.d.e. usługodawca, który świadczy usługi drogą elektroniczną obejmujące transmisję w sieci telekomunikacyjnej danych przekazywanych przez odbiorcę usługi lub zapewnienie dostępu do sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[15], nie ponosi odpowiedzialności za treść tych danych, jeżeli: 1) nie jest inicjatorem przekazu danych; 2) nie wybiera odbiorcy przekazu danych; 3) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie[16].

Wyłączenie odpowiedzialności obejmuje także automatyczne i krótkotrwałe pośrednie przechowywanie transmitowanych danych, jeżeli działanie to ma wyłącznie na celu przeprowadzenie transmisji, a dane nie są przechowywane dłużej, niż jest to w zwykłych warunkach konieczne dla zrealizowania transmisji. Zgodnie z ustawą ś.u.d.e., dostawca usług nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych.

Wyłączenie odpowiedzialności dostawcy usług internetowych za *mere conduit* na podstawie przepisu art. 12 ustawy ś.u.d.e. dotyczy zarówno działalności operatora sieci telekomunikacyjnej, dostawcy dostępu do internetu, jak

15 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r., poz. 2460).

16 P. Podrecki, *Prawo Internetu*, Warszawa 2007, s. 209; X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 131; P. Litwiński, *Zasady odpowiedzialności pośredników w dostarczaniu informacji w Internecie (Intermediary Service Providers – ISP)*, *„Gospodarka Elektroniczna"*, „Monitor Prawniczy" 2002, nr 24, s. 12; M. Wilkowska, *Wybrane zagadnienia związane z pobieraniem nielegalnych kopii utworów z Internetu*, „Przegląd Prawa Handlowego" 2007, nr 12, s. 24.

i dysponenta sieci telekomunikacyjnej (*access provider*). Warunkiem wyłączenia odpowiedzialności jest dokonanie przekazu bez poznania treści i bez ingerencji w nią[17].

Usługodawca nie ponosi także odpowiedzialności za *caching*, czyli automatyczne i krótkotrwałe pośrednie przechowywanie danych w celu przyspieszenia ponownego dostępu do nich, jeśli: nie modyfikuje danych; posługuje się uznanymi i stosowanymi zwykle w tego rodzaju działalności technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania oraz nie zakłóca posługiwania się technikami informatycznymi uznanymi i stosowanymi zwykle w tego rodzaju działalności w zakresie zbierania informacji o korzystaniu ze zgromadzonych danych. Dostawca nie poniesie odpowiedzialności za *caching* także, jeśli postępując w powyżej opisany sposób, niezwłocznie usunie dane albo uniemożliwi do nich dostęp, gdy uzyska wiadomość, że dane zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony, albo gdy sąd lub inny właściwy organ nakazał usunięcie danych lub uniemożliwienie do nich dostępu. Do przesłanek wyłączenia odpowiedzialności dostawcy usługi *cachingu* należy zatem: 1) krótkotrwałość przechowywania danych – przy czym oceny krótkotrwałości należy dokonywać w odniesieniu do konkretnego przypadku; 2) pośredniość przechowywania danych – chodzi o czysto techniczne przekazywanie i zapisywanie informacji, w toku którego usługodawca nie posiada wiedzy o charakterze przesyłanych informacji i nie ma możliwości ich kontroli; 3) zakaz modyfikowania przechowywanych danych – co oznacza, że kopia danych przechowywanych na *proxy-cache* serwerze powinna być zgodna treściowo z danymi znajdującymi się na serwerze źródłowym; 4) obowiązek posługiwania się uznanymi i stosowanymi zwykle w tego rodzaju działalności technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania – w literaturze przedmiotu wskazuje się, że celem tego warunku jest zapewnienie, aby skopiowana i przechowywana na *proxy-cache* serwerze strona była dostępna dla użytkowników na tych samych zasadach i w tym samym zakresie, co strona internetowa znajdująca się na serwerze źródłowym; 5) nieingerowanie w posługiwanie się przez użytkowników technikami informatycznymi uznanymi i stosowanymi zwykle w tego rodzaju działalności w zakresie zbierania informacji o korzystaniu ze zgromadzonych danych –

17 M. Siwicki, *Nielegalna*…, s. 247.

informacje te umożliwiają podmiotowi udostepniającemu dane na serwerze źródłowym obliczenie liczby odsłon[18].

Odpowiedzialność *host providera* za naruszenie prawa autorskiego w internecie budzi najwięcej wątpliwości. *Hosting* polega na tym, że tworzone są internetowe platformy dla użytkowników, którym udostępniana jest określona ilość pamięci na serwerach w celu przechowywania na nich materiałów pochodzących od tych użytkowników. *Host provider* jest zatem podmiotem, który udostępnia zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, będąc jednocześnie podmiotem pasywnym (biernym, neutralnym) w stosunku do przechowywanych treści, tj. nie dokonuje ich weryfikacji pod kątem bezprawności[19]. Jak trafnie zauważa Z. Zawadzka, *host provider* pełni rolę łącznika między dostawcą treści (*content provider*) a użytkownikami je przeglądającymi. Należy podkreślić, że kategoria *host providerów* jest bardzo szeroka i zalicza się do nich zarówno usługodawcę, który zapewnia przechowywanie stron www, jak również portal społecznościowy w odniesieniu do treści dostarczanych przez swoich użytkowników[20]. Sąd Apelacyjny w Warszawie w wyroku z 23 maja 2014 r. stwierdził, że zakres art. 14 ustawy ś.u.d.e. obejmuje nie tylko podmioty prowadzące działalność polegającą na przechowywaniu danych w swoich zasobach systemu teleinformatycznego, ale również na ich udostępnianiu[21].

W zakresie określania przypadków naruszenia prawa autorskiego w internecie istotną rolę odgrywa także orzecznictwo TSUE. Trybunału Sprawiedliwości Unii Europejskiej, dokonując wykładni poszczególnych przepisów m.in. dyrektywy w sprawie harmonizacji niektórych aspektów prawa autorskiego i praw pokrewnych w społeczeństwie informacyjnym[22] zapewnia jednolite stosowanie prawa w Unii Europejskiej, udzielając wskazówek, w jaki sposób dokonywać oceny prawnej i kwalifikować naruszenia prawa autorskiego w internecie. TSUE w wyroku z 5 czerwca 2014 r. w sprawie Public Relations

18 K. Wójcik, *Usługa…*, s. 105–109.

19 Wyrok SA w Krakowie z dnia 18 września 2017 r., I ACa 1494/15, LEX nr 2354397; D. Lubasz, W. Chomiczewski, *Wyłączenia odpowiedzialności host providerów – w poszukiwaniu równowagi pomiędzy dobrami prawnie chronionymi* [w:] J. Kępiński, K. Klafkowska-Waśniowska, R. Sikorski (red.), *Zarys Prawa Własności Intelektualnej*, t. 5, *Własność intelektualna w obrocie elektronicznym*, Warszawa 2015, s. 22.

20 D. Lubasz, W. Chomiczewski, *Wyłączenia…*, s. 22.

21 Wyrok SA w Warszawie z dnia 23 maja 2014 r., I ACa 477/14, LEX nr 1515312.

22 Dyrektywa Parlamentu Europejskiego i Rady Nr 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz.WE 2001 L 167/10).

Consultants Association Ltd v. Newspaper Licensing Agency Ltd i in.[23] uznał, że czynność polegająca na oglądaniu strony internetowej bez jej drukowania lub ściągania, prowadząca do stworzenia kopii strony internetowej poprzez jej wyświetlenie na ekranie oraz w pamięci podręcznej urządzenia, mieści się w przepisie art. 5 ust. 1 dyrektywy w sprawie harmonizacji niektórych aspektów prawa autorskiego i praw pokrewnych w społeczeństwie informacyjnym. Warunkiem jest jednak, aby nie została wykonana trwała kopia przeglądanej strony w postaci np. zrzutu ekranu, jej wydruku, czy pobrania treści w niej zawartych. Tym samym w opinii TSUE przeglądanie stron internetowych na komputerze, które warunkuje tworzenie ich kopii na ekranie urządzenia oraz w jego pamięci podręcznej nie powoduje naruszenia prawa autorskiego do utworów znajdujących się na tych stronach.

Zgodnie z dyspozycją art. 14 ust. 1 ustawy ś.u.d.e. *host provider* nie ponosi odpowiedzialności za przechowywane dane usługobiorcy, jeżeli nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych[24]. *Host provider*, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych[25]. Sąd Apelacyjny w Łodzi w wyroku z 13 stycznia 2017 r. wskazał, że fakt, że podmioty świadczące usługi *hostingu* – podobnie jak podmioty umożliwiające sprawny dostęp do portali internetowych – tylko pośredniczą w udostępnianiu drogą elektroniczną treści pochodzących od osób trzecich, rzutuje na ukształtowanie zasad ich odpowiedzialności za naruszenie praw podmiotowych osób trzecich lub naruszenie obowiązujących przepisów prawa w związku z treścią przechowywanych danych. Podmioty pośredniczące są zwolnione z odpowiedzialności cywilnoprawnej, administracyjnej oraz karnej za zawartość udostępnionych materiałów, nie są one bowiem zobowiązane do sprawdzania (monitorowania) przekazywanych, przechowywanych lub udostępnianych danych. Niewiedza

23 Wyrok TS UE z dnia 5 czerwca 2014 r. w sprawie *Public Relations Consultants Association Ltd v. Newspaper Licensing Agency Ltd i in*., skarga Nr C-360/1.

24 Wyrok SA w Warszawie z dnia 11 czerwca 2015 r., I ACa 1842/14, LEX nr 1751205.

25 J. Barta, *Przechowywanie utworów na stronach internetowych*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2009, nr 3.

o treści udostępnionych informacji jest zasadniczym warunkiem uchylenia odpowiedzialności tych podmiotów[26]. Odmiennie stwierdził SA w Krakowie, który w wyroku z 18 września 2017 r. wskazał, że serwisy przechowujące pliki powinny monitorować sieć i likwidować nielegalne kopie filmów oraz kasować konta użytkowników zamieszczających takie treści[27].

Sąd Apelacyjny w Warszawie w wyroku z 25 września 2018 r., I ACa 110/18, (Legalis) stwierdził, że z treści art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną jednoznacznie wynika, że uzyskanie wiedzy usługodawcy o bezprawnym charakterze danych wyłącza od tej chwili brak jego odpowiedzialności za dalsze udostępnianie tych wpisów, bez względu na to co jest źródłem tej wiedzy. Nie ma zatem znaczenia czy wiedza usługodawcy o bezprawnym charakterze danych wynika z zawiadomienia osoby dotkniętej takim bezprawnym wpisem, czy też z działań moderatora lub została uzyskana w inny sposób.

Także w doktrynie wskazuje się, że nie ma obowiązku moderowania na bieżąco forum i usuwania nielegalnych wpisów na bieżąco, bez uzyskania uprzednio zawiadomienia o pojawieniu się nielegalnych wpisów. Tym samym, dla przyjęcia odpowiedzialności *hosting providera*, kluczowe jest zawiadomienie go o fakcie naruszenia dóbr osobistych[28].

Konkludując powyższe można stwierdzić, że usługodawca świadczący usługi polegające na umożliwieniu bezpłatnego korzystania z internetu oraz zamieszczania wpisów na uruchomionym przez siebie portalu dyskusyjnym nie ponosi odpowiedzialności za naruszenie dóbr osoby trzeciej, chyba że wiedział, że wpis na portalu narusza te dobra i nie usunął go niezwłocznie. Usługodawca nie ma wprawdzie obowiązku monitorowania sieci, jednakże sytuacja, w której po stronie usługodawcy istnieje stan wiedzy o fakcie naruszenia czy też bezprawnym charakterze tego naruszenia, prowadzi do wystąpienia odpowiedzialności po stronie usługodawcy[29]. Oznacza to, że jedynie pozytywna i konkretna wiedza usługodawcy odnosząca się do bezprawnego charakteru danych lub związanej z nimi działalności wyłącza zastosowanie zwolnienia

26 Wyrok SA w Łodzi z dnia 13 stycznia 2017 r., I Aca 884/16, LEX nr 2250053.

27 Wyrok SA w Krakowie z dnia 19 września 2017 r., I ACa 1494/15, „ Gazeta Prawna" 2017, nr 182, s. 5.

28 Ł. Wydra, *Glosa do wyroku SN z dnia 30 września 2016 r., I CSK 598/15*, Glosa 2017, nr 4, s. 91 i n.

29 Wyrok SN z dnia 14 stycznia 2015 r., II CSK 747/13, OSNC 2016, nr 1, poz. 9; wyrok SA w Warszawie z dnia 11 czerwca 2015 r., I ACa 1842/14, LEX nr 1751205; wyrok SA w Katowicach z dnia 13 lutego 2014 r., I ACa 1086/13, LEX nr 1437961; wyrok SN z dnia 8 lipca 2011 r., IV CSK 665/10, OSNC 2012, nr 2, poz. 27.

z odpowiedzialności. Nie jest wystarczająca sama możliwość uzyskania wiedzy, lecz jej faktyczne posiadanie[30]. Podobnie SN w wyroku z 30 września 2016 r. uznał, że jako wiedzę administratora o inkryminowanych komentarzach internautów należy zakwalifikować sytuację, kiedy administrator w związku z doświadczeniem z dotychczasowej działalności na polu świadczenia usług hostingu liczy się z realną możliwością dokonywania przez internautów wpisów o treści naruszającej dobra osobiste konkretnych osób[31]. Przesłanką odpowiedzialności administratora portalu internetowego może być zatem tylko świadomość bezprawnej działalności użytkownika portalu, bądź brak reakcji z jego strony na powyższe działanie, polegające na nieusunięciu sprzecznych z prawem treści po otrzymaniu zawiadomienia o nich[32]. Dodatkowo należy podkreślić, że wiedza usługodawcy hostingu na temat bezprawnego charakteru wpisów internautów niekoniecznie musi pochodzić od osób dotkniętych inkryminowanymi komentarzami. Źródło wiarygodnej informacji jest tutaj prawnie obojętne do tego stopnia, że informacja taka może być również wynikiem własnych spostrzeżeń pracowników bądź przedstawicieli administratora portalu internetowego oraz zastosowanych przez niego środków technicznych[33].

Na końcu systemu korzystania z przedmiotów prawa autorskiego w internecie znajduje się użytkownik końcowy. Z punktu widzenia jego odpowiedzialności za naruszenie prawa autorskiego w internecie, podstawowe znaczenia odgrywa dyspozycja art. 23 i 23^1 pr. aut. Zgodnie z tymi przepisami, dozwolone jest korzystanie z już rozpowszechnionego utworu w zakresie własnego użytku osobistego. Nie wymaga zezwolenia twórcy także tymczasowe zwielokrotnianie, o charakterze przejściowym lub incydentalnym, niemające samodzielnego znaczenia gospodarczego, a stanowiące integralną i niezbędną część procesu technologicznego, którego celem jest wyłącznie umożliwienie: przekazu utworu w systemie teleinformatycznym pomiędzy osobami trzecimi przez pośrednika lub zgodnego z prawem korzystania z utworu.

Instytucja dozwolonego użytku upoważnia do korzystania z chronionego utworu bez zgody uprawnionego z uwagi na zasługujący na ochronę interes publiczny oraz interesy osobiste użytkowników. Ze względu na kryterium

30 D. Lubasz, W. Chomiczewski, *Wyłączenia*…, s. 29.
31 Wyrok SN z dnia 30 września 2016 r., I CSK 598/15, LEX nr 2151458.
32 Wyrok SA w Warszawie z dnia 13 października 2017 r., I ACa 1208/16, LEX nr 2402446.
33 Wyrok SA w Warszawie z dnia 21 kwietnia 2017 r., VI ACa 1910/16, LEX nr 2481496; wyrok SA w Warszawie z dnia 18 kwietnia 2017 r., I ACa 55/16, LEX nr 2317742.

interesu, z uwagi na który następuje ograniczenie monopolu prawnoautorskiego twórcy, wyróżnia się dozwolony użytek publiczny i dozwolony użytek osobisty (prywatny). W orzecznictwie sądowym przyjmuje się, że przepisy o dozwolonym użytku, wprowadzające wyjątki w sferze bezwzględnych praw autorskich, podlegają ścisłej interpretacji i nie można ich stosować w drodze analogii. Ewentualne wątpliwości należy rozstrzygać na korzyść autora i uznać, że określona sfera eksploatacji, która nie jest wyraźnie wyłączona, wymaga jego zezwolenia[34].

Warunkami dopuszczalności korzystania z utworu w ramach dozwolonego użytku są: 1) wymóg wcześniejszego rozpowszechnienia utworu; 2) zakres korzystania z utworu w ramach dozwolonego użytku osobistego; 3) niekomercyjny cel korzystania z utworu; 4) nieodpłatność[35].

Rozpowszechnienie utworu oznacza udostępnienie utworu publicznie w jakikolwiek sposób za zezwoleniem twórcy. W doktrynie i orzecznictwie dominował pogląd, że powoływanie się na dozwolony użytek osobisty było dopuszczalne także wówczas, gdy źródło, z którego pozyskany był utwór wykorzystywany w ramach dozwolonego użytku osobistego było nielegalne[36]. Stanowiska tego nie poparł TSUE. Trybunał w wyroku z 10 kwietnia 2014 r. w sprawie ACI Adam BV uznał, że nie można akceptować uregulowań krajowych, które nie rozróżniają sytuacji, w której źródło służące za podstawę sporządzenia kopii na użytek prywatny jest legalne, od sytuacji, w której źródło to jest nielegalne[37].

Natomiast niekomercyjny cel korzystania z utworu w ramach dozwolonego użytku osobistego musi polegać na własnym użytku osobistym osoby eksploatującej cudzy utwór. W doktrynie wskazuje się, że może to być cel rozrywkowy, hobbystyczny, naukowy, kolekcjonerski[38]. Instytucja dozwolonego użytku osobistego nie ma zastosowania do osoby prowadzącej działalność gospodarczą i osiągającej zyski z tej działalności[39].

34 Wyrok SA w Łodzi z dnia 18 września 2013 r., I ACa 406/13, LEX nr 1372327.
35 Z. Zawadzka, *Autorskie prawa majątkowe* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo…*, s. 158.
36 J. Barta, R. Markiewicz, *Prawo autorskie*, Warszawa 2016, s. 231.
37 Wyrok TSUE z dnia 10 kwietnia 2014 r. w sprawie *ACI Adam BV i inni v. Stichting de Thuiskopie i Stichting Onderhandelingen Thuiskopie vergoeding*, skarga Nr C-435/12, LEX nr 1446594.
38 J. Preussner-Zamorska, *Dozwolony użytek chronionych utworów* [w:] J. Barta (red.), *System Prawa Prywatnego*, t. 13, *Prawo autorskie*, Warszawa 2007, s. 423.
39 Wyrok SA w Warszawie z dnia 5 lutego 2003 r., I ACa 601/02, LEX nr 1680981.

Zakończenie

Przeprowadzone rozważania pozwalają stwierdzić, że internet jest ogromnym wyzwaniem dla ustawodawcy. Dynamiczny rozwój nowych technologii wpływa nie tylko na możliwości korzystania z utworów w internecie, ale także zmienia sposób powstawania utworów i ich dystrybucji.

Należy pamiętać, że w internecie obowiązują takie same prawa autorskie jak w realnym świecie. Wszystkie rozwiązania w zakresie pojęcia utworu, twórcy, rodzajów przysługujących mu praw czy sposobów ich ochrony są aktualne w stosunku do zasobów internetu. Internet nie jest zjawiskiem całkowicie pozbawionym kontroli. Istnieją firmy świadczące usługi dostępu do internetu, podmioty udostępniające serwery, mamy też osobę, która za ich pośrednictwem umieszcza materiały w sieci oraz osobę, która ostatecznie korzysta z tych materiałów.

Przepisy ustawy o świadczeniu usług drogą elektroniczną określają zasady odpowiedzialności usługodawcy. Zostały one skonstruowane w sposób horyzontalny. Oznacza to, że dotyczą każdego reżimu odpowiedzialności zarówno cywilnej, jak i karnej i administracyjnej[40]. Twórcy i podmioty praw pokrewnych mogą starać się dochodzić swoich praw przed sądem, ale tylko wobec operatorów, którzy konstruują sieci P2P tak, by komunikacja odbywała się przez ich serwery. Jakkolwiek ustawa o prawie autorskim i prawach pokrewnych zawiera jedynie przepisy pozwalające na wytoczenie powództwa przeciwko osobie, która naruszyła prawo autorskie, to jednak odpowiedzialność dostawców sieci i usług internetowych możliwa jest ze względu na przepisy ustawy o świadczeniu usług drogą elektroniczną. Kryterium uznania odpowiedzialności prawnej administratorów serwerów uczestniczących w wymianie informacji w sieci dotyczy głównie tego, czy mają oni wpływ na umieszczane w sieci treści[41].

Do głównych przyczyn zjawiska naruszania praw autorskich w internecie zalicza się z jednej strony powszechność internetu, która przekłada się na możliwości dostępu do wszelkich informacji w nim zawartych. Z drugiej strony to sami użytkownicy mogą w wyniku podejmowanych działań prowadzić do naruszenia praw twórców. Brak świadomości prawnej i wiedzy na temat

40 M. Kręcisz, *Glosa do wyroku TS z dnia 24 listopada 2011 r., C-70/10 oraz do wyroku TS z dnia 16 lutego 2012 r., C-360/10*, LEX 2012.

41 M. Król, *Rozpowszechnianie utworów w sieciach typu peer-to-peer*, „Państwo i Prawo" 2008, nr 3, s. 96 i n.

konieczności poszanowania własności intelektualnej jak również chęci przestrzegania określonych zasad prowadzi do naruszenia praw twórców w internecie.

Bibliografia

Literatura

Barta J., Markiewicz R., Matlak A., *Prawo autorskie w społeczeństwie informacyjnym* [w:] *System Prawa Prywatnego*, t. 13, *Prawo autorskie*, Warszawa 2017.

Barta J., Markiewicz R., *Prawo autorskie*, Warszawa 2016.

Barta J., *Przechowywanie utworów na stronach internetowych*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2009, nr 3.

Chomiczewski W., *Komentarz do art. 13* [w:] D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, LEX 2011.

Gęsicka D.K., *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników*, Warszawa 2014.

Globan-Klas T., Senkiewicz P., *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999.

Kitler W., *Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne* [w:] W. Kitler, J. Taczkowska-Olszewska (red.), *Bezpieczeństwo informacyjne*, Warszawa 2017.

Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004.

Kręcisz M., *Glosa do wyroku TS z dnia 24 listopada 2011 r., C-70/10 oraz do wyroku TS z dnia 16 lutego 2012 r., C-360/10*, LEX 2012.

Król M., *Rozpowszechnianie utworów w sieciach typu peer-to-peer*, „Państwo i Prawo" 2008, nr 3.

Litwiński P., *Zasady odpowiedzialności pośredników w dostarczaniu informacji w Internecie (Intermediary Service Providers – ISP)*, *„Gospodarka Elektroniczna"*, „Monitor Prawniczy" 2002, nr 24.

Lubasz D., Chomiczewski W., *Wyłączenia odpowiedzialności host providerów – w poszukiwaniu równowagi pomiędzy dobrami prawnie chronionymi* [w:] J. Kępiński, K. Klafkowska-Waśniowska, R. Sikorski (red.), *Zarys Prawa Własności Intelektualnej*, t. 5, *Własność intelektualna w obrocie elektronicznym*, Warszawa 2015.

Matlak A., *Prawo autorskie w społeczeństwie informacyjnym*, Kraków 2004.

Nowikowska M., *Utwór jako przedmiot prawa autorskiego* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej*, cz. I, *Prawo autorskie i prawa pokrewne*, Warszawa 2018.

Podrecki P., *Prawo Internetu*, Warszawa 2007.

Preussner-Zamorska J., *Dozwolony użytek chronionych utworów* [w:] J. Barta (red.), *System Prawa Prywatnego*, t. 13, *Prawo autorskie*, Warszawa 2007.

Rączka G., *Prawne zagadnienia hostingu*, „Przegląd Prawa Handlowego" 2009, nr 4.

Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011.

Wilkowska M., *Wybrane zagadnienia związane z pobieraniem nielegalnych kopii utworów z Internetu*, „Przegląd Prawa Handlowego" 2007, nr 12.

Wójcik K., *Usługa cachingu. Wyłączenie odpowiedzialności z tytułu świadczenia usług drogą elektroniczną* [w:] A. Niewęgłowski, M. Chrzanowski (red.), *Internet a prawo autorskie*, Lublin 2016.

Wydra Ł, *Glosa do wyroku SN z dnia 30 września 2016 r., I CSK 598/15*, Glosa 2017, nr 4.

Zawadzka Z., *Autorskie prawa majątkowe* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej*, cz. I, *Prawo autorskie i prawa pokrewne*, Warszawa 2018.

Zawadzka Z., *Prawo autorskie w Internecie* [w:] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej*, cz. I, *Prawo autorskie i prawa pokrewne*, Warszawa 2018.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady Nr 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. WE 2001 L 167/10).
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r., poz. 2460).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344).
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2019 r., poz. 1231).

Orzeczenia

Wyrok SA w Katowicach z dnia 13 lutego 2014 r., I ACa 1086/13, LEX nr 1437961.
Wyrok SA w Krakowie z dnia 18 września 2017 r., I ACa 1494/15, LEX nr 2354397.
Wyrok SA w Krakowie z dnia 19 września 2017 r., I ACa 1494/15, „ Gazeta Prawna" 2017, nr 182.
Wyrok SA w Łodzi z dnia 13 stycznia 2017 r., I ACa 884/16, LEX nr 2250053.
Wyrok SA w Łodzi z dnia 13 stycznia 2017 r., I Aca 884/16, LEX nr 2250053.
Wyrok SA w Łodzi z dnia 18 września 2013 r., I ACa 406/13, LEX nr 1372327.
Wyrok SA w Warszawie z dnia 11 czerwca 2015 r., I ACa 1842/14, LEX nr 1751205.
Wyrok SA w Warszawie z dnia 11 czerwca 2015 r., I ACa 1842/14, LEX nr 1751205.
Wyrok SA w Warszawie z dnia 12 stycznia 2017 r., VI ACa 1579/15, LEX nr 2249981.
Wyrok SA w Warszawie z dnia 13 października 2017 r., I ACa 1208/16, LEX nr 2402446.
Wyrok SA w Warszawie z dnia 18 kwietnia 2017 r., I ACa 55/16, LEX nr 2317742.
Wyrok SA w Warszawie z dnia 21 kwietnia 2017 r., VI ACa 1910/16, LEX nr 2481496.
Wyrok SA w Warszawie z dnia 23 maja 2014 r., I ACa 477/14, LEX nr 1515312.
Wyrok SA w Warszawie z dnia 5 lutego 2003 r., I ACa 601/02, LEX nr 1680981.
Wyrok SN z dnia 14 stycznia 2015 r., II CSK 747/13, OSNC 2016, nr 1, poz. 9.
Wyrok SN z dnia 30 września 2016 r., I CSK 598/15, LEX nr 2151458.
Wyrok SN z dnia 8 lipca 2011 r., IV CSK 665/10, OSNC 2012, nr 2, poz. 27.
Wyrok TSUE z dnia 10 kwietnia 2014 r. w sprawie ACI Adam BV i inni v. Stichting de Thuiskopie i Stichting Onderhandelingen Thuiskopie *vergoeding*, skarga Nr C-435/12, LEX nr 1446594.
Wyrok TSUE z dnia 5 czerwca 2014 r. w sprawie Public Relations Consultants Association Ltd v. Newspaper Licensing Agency Ltd i in., skarga Nr C-360/1.

Protection of Copyright in the Internet

Abstract

The Internet is the primary source of information. From the point of view of copyright, there are more and more legal problems related to the use of works in the Internet. The article presents the problem of protection of copyright in the Internet. The first part of the article indicates cases of violation of the authors' rights in the Internet. Many entities participate in the dissemination of materials in the Internet. The principles of liability in Poland have been regulated in the Act on the provision of electronic services. Among these entities, the legislator distinguishes access provider, service provider and host provider. The criterion for recognizing the legal liability of server administrators participating in the exchange of information on the network mainly concerns whether they affect the content posted on the network.

Key words: copyright, Internet, access provider, service provider, host provider, responsibility

Paweł Pelc*

Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa

Streszczenie

Regulacje dotyczące rynku finansowego zawierają regulacje dotyczące tajemnicy zawodowej, w tym tajemnicy bankowej, przy czym brak jest jednolitej regulacji – dla każdego typu instytucji finansowej regulacja w tym zakresie jest odrębna. Tajemnica zawodowa nie jest jednak bezwzględna i ustawodawca określa zasady jej udostępniania i wymiany z innymi podmiotami. Część instytucji finansowych może być operatorami usług kluczowych w ramach krajowego systemu cyberbezpieczeństwa, część może być traktowana jako dostawcy usług cyfrowych, a dwie Bank Gospodarstwa Krajowego i Narodowy Bank Polski są podmiotami publicznymi stanowiącymi część krajowego systemu cyberbepieczeństwa. Elementem cyberbezpieczeństwa jest także zachowanie poufności, zatem w przypadku przetwarzania informacji stanowiących tajemnicę zawodową w systemach informacyjnych zastosowanie mogą mieć także regulacje dotyczące krajowego systemu cyberbezpieczeństwa. Mimo nietożsamych celów stosowanie regulacji dotyczących tajemnicy zawodowej i regulacji dotyczących cyberbezpieczeństwa może się wzajemnie wzmacniać, czemu dodatkowo może sprzyjać stosowanie odrębnej regulacji przyjętej na szczeblu europejskim w zakresie ochrony danych osobowych.

Słowa kluczowe: cyberbezpieczeństwo, tajemnica zawodowa, tajemnica bankowa, instytucja finansowa, rynek finansowy

* Paweł Pelc, Akademia Sztuki Wojennej w Warszawie, Centrum Badań nad Bezpieczeństwem, Ośrodek Centrum Studiów nad Cyberbezpieczeństwem, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Instytucje działające na rynku finansowym swoją działalność w dużym stopniu opierają na zaufaniu, jakim obdarzają je ich klienci. Utrata zaufania rodzi ryzyko niewypłacalności takich instytucji, na przykład w razie wystąpienia tzw. runu na banki, czyli klasycznej paniki bankowej[1], stąd w systemach finansowych podejmowane są różne działania mające na celu zachowanie zaufania do instytucji finansowych. Do działań tych należą różnego rodzaju systemy ochrony klientów instytucji finansowych (w tym w szczególności gwarantujące ich depozyty na wypadek upadłości banków lub innych instytucji kredytowych[2]), nadzór nad nimi oraz mechanizmy zapewnienia płynności zwłaszcza instytucjom depozytowym. Oprócz powyższych mechanizmów ochronnych, czynnikiem budowania zaufania do instytucji rynku finansowego umożliwiającym wykonywanie ich funkcji jest także kwestia ochrony informacji o klientach przyjmująca postać tajemnicy bankowej[3] lub innych form tajemnicy zawodowej. Chronione są zarówno informacje pozyskane przez instytucje rynku finansowego, jak i przez podmioty publiczne, w szczególności tworzące. tzw. sieć bezpieczeństwa finansowego, czyli Komisję Nadzoru Finansowego, Narodowy Bank Polski, Ministra Finansów i Bankowy Fundusz Gwarancyjny[4].

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[5] nie zawiera definicji rynku finansowego, a nadzór nad rynkiem finansowym definiuje jako m.in. nadzór bankowy, emerytalny, ubezpieczeniowy, nad rynkiem kapitałowym, instytucjami płatniczymi, małymi instytucjami płatniczymi, dostawcami świadczącymi wyłącznie usługę dostępu do informacji o rachunku, biurami usług płatniczych, instytucjami pieniądza elektronicznego, oddziałami zagranicznych instytucji pieniądza elektronicznego, agencjami ratingowymi, spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową poprzez odwołanie do regulacji dotyczących poszczególnych segmentów rynku finansowego. Nie każdy podmiot

1 Por. M. Iwanicz-Drozdowska (red.), *Kryzysy bankowe. Przyczyny i rozwiązania*, Warszawa 2002; T. Obal, *System gwarantowania depozytów w USA* [w:] W. Baka (red.), *Systemy gwarantowania depozytów w Polsce i na świecie. Dziesięć lat Bankowego Funduszu Gwarancyjnego*, Warszawa 2005, s. 187–188.

2 W Polsce takimi instytucjami są także spółdzielcze kasy oszczędnościowo-kredytowe, w których depozyty ich członków zostały objęte ochroną przez Bankowy Fundusz Gwarancyjny w 2013 r. w wyniku nowelizacji ustawy o spółdzielczych kasach oszczędnościowo-kredytowych oraz wówczas obowiązującej ustawy o Bankowym Funduszu Gwarancyjnym.

3 J. Byrski, *Tajemnica prawnie chroniona w działalności bankowej*, Legalis 2010.

4 K. Stępień, *Instytucje Sieci Bezpieczeństwa Finansowego w Polsce z perspektywy instrumentów zapewniających stabilność finansową*, „Roczniki Ekonomii i Zarządzania" 2017, nr 3, s. 48.

5 T.j. Dz.U. z 2020 r., poz. 180 ze zm.

podlegający nadzorowi Komisji Nadzoru Finansowego może być uznany za instytucję finansową – w szczególności nie można bowiem uznać za instytucje finansowe emitentów papierów wartościowych.

Regulacje dotyczące tajemnicy zawodowej zawierają ustawy regulujące funkcjonowanie instytucji sieci bezpieczeństwa finansowego. W przypadku Narodowego Banku Polskiego Pracownicy NBP oraz członkowie Rady i organów opiniodawczo-doradczych przy Zarządzie NBP są obowiązani do nieujawniania osobom nieupoważnionym informacji, z którymi zapoznali się w trakcie wykonywania swoich obowiązków, w tym informacji objętych tajemnicą bankową na podstawie ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, informacji objętych ochroną na podstawie przepisów dotyczących ochrony informacji niejawnych, jak również innych informacji chronionych ustawowo. Obowiązek ten trwa również po rozwiązaniu stosunku pracy, a także po ustaniu członkostwa w Radzie lub wspomnianych wyżej organach[6]. W odniesieniu do Komisji Nadzoru Finansowego przewodniczący Komisji Nadzoru Finansowego, jego zastępcy, członkowie Komisji Nadzoru Finansowego, pracownicy Urzędu Komisji Nadzoru Finansowego i osoby zatrudnione w Urzędzie Komisji na podstawie umowy o dzieło, umowy zlecenia albo innych umów o podobnym charakterze są obowiązani, na podstawie art. 16 ust. 1 ustawy o nadzorze nad rynkiem finansowym do nieujawniania osobom nieupoważnionym informacji chronionych na podstawie odrębnych ustaw. Obowiązek ten trwa również po ustaniu pełnienia funkcji, rozwiązaniu stosunku pracy lub rozwiązaniu umowy o dzieło, umowy zlecenia albo innych umów o podobnym charakterze.

W konsekwencji należy wskazać, że szczegółowa regulacja dotycząca tajemnicy w instytucjach finansowych, określona jest przede wszystkim w regulacjach dotyczących funkcjonowania tych instytucji. Niezależnie od zachowania tajemnicy instytucje rynku finansowego muszą także stosować się do reguł dotyczących przetwarzania danych osobowych[7].

Zgodnie z art. 104 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[8] tajemnica bankowa określona jest następująco: bank, osoby w nim zatrudnione

6 Art. 55 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2019 r., poz. 1810 ze zm.).

7 J. Byrski, L. Sytniewski, *Zmiany w praktyce działania instytucji finansowych na skutek ogólnego rozporządzenia o ochronie danych. Wybrane zagadnienia prawne* [w:] W. Rogowski (red.), *Regulacje Finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, s. 77–92; M. Krzysztofek, *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.

8 T.j. Dz.U. z 2019 r., poz. 2357 ze zm.

oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

Norma ta ma także zastosowanie do oddziałów banków z innych krajów Unii Europejskiej oraz spoza niej[9]. Na tajemnicy bankowej w dużym stopniu wzorowane są także rozwiązania dotyczące tajemnicy w regulacjach dotyczących innych instytucji finansowych.

Najbliższą do działalności banków jest działalność spółdzielczych kas oszczędnościowo-kredytowych. Zgodnie z art. 9e ust. 1 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych[10] spółdzielcza kasa oszczędnościowo-kredytowa jest obowiązana do zachowania tajemnicy zawodowej obejmującej wszystkie informacje dotyczące czynności, o których mowa w art. 3 ust. 1 tej ustawy (czyli gromadzenie środków pieniężnych wyłącznie swoich członków, udzielanie im pożyczek i kredytów, przeprowadzanie na ich zlecenie rozliczeń finansowych oraz wykonywanie dystrybucji ubezpieczeń), w tym także informacje uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której kasa tę czynność wykonuje.

Zgodnie z art. 35 ust. 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej[11] zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia.

W odniesieniu do działalności funduszy inwestycyjnych tajemnica zawodowa została określona w art. 280 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[12] tajemnicą zawodową jest tajemnica obejmująca informację uzyskaną w związku z podejmowanymi czynnościami służbowymi w ramach zatrudnienia, stosunku zlecenia lub innego stosunku prawnego o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z działalnością funduszu inwestycyjnego, alternatywnej spółki inwestycyjnej, funduszu zagranicznego, unijnego AFI lub zbiorczego

9 M. Krzysztofek, *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.
10 T.j. Dz.U. z 2019 r., poz. 2412 ze zm.
11 T.j. Dz.U. z 2019 r., poz. 381 ze zm.
12 T.j. Dz.U. z 2020 r., poz. 95 ze zm.

portfela papierów wartościowych, w szczególności z lokatami oraz rejestrem uczestników funduszu inwestycyjnego, alternatywnej spółki inwestycyjnej, funduszu zagranicznego, unijnego AFI lub zbiorczego portfela papierów wartościowych, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji, organu nadzoru państwa członkowskiego lub organu nadzoru państwa trzeciego, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru.

Podobnie na rynku kapitałowym tajemnica zawodowa jest zdefiniowana w art. 147 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[13], zgodnie z którym tajemnica zawodowa obejmuje informację uzyskaną w związku z podejmowanymi czynnościami służbowymi w ramach pozostawania w stosunku pracy, zlecenia lub w innym stosunku prawnym o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z obrotem instrumentami finansowymi, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji lub zagranicznego organu nadzoru, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru, w szczególności informację zawierającą: 1) dane identyfikujące stronę umowy lub innej czynności prawnej; 2) treść umowy lub przedmiot czynności prawnej; 3) dane o sytuacji majątkowej strony umowy, w tym oznaczenie rachunku papierów wartościowych, innego rachunku, na którym zapisywane są instrumenty finansowe niebędące papierami wartościowymi, lub rachunku pieniężnego służącego do obsługi tych rachunków, liczbę i oznaczenie instrumentów finansowych, oraz wartość środków zgromadzonych na tych rachunkach; 4) oznaczenie rachunku zbiorczego, liczbę i oznaczenie zapisanych na nim instrumentów finansowych oraz dane osób uprawnionych z tych instrumentów finansowych.

Natomiast w ustawie z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych[14] w art. 49 ust. 2 zakres tajemnicy zawodowej określono w następujący sposób: tajemnica zawodowa, obejmuje informacje związane z lokatami funduszu, rejestrem członków funduszu, rozporządzeniami członków funduszu na wypadek śmierci oraz oświadczeniami, o których mowa w art. 83 tej ustawy (oświadczenia o stosunkach majątkowych), których ujawnienie mogłoby naruszyć interes członków funduszu lub interes

13 T.j. Dz.U. z 2020 r., poz. 89 ze zm.
14 T.j. Dz.U. z 2020 r., poz. 105 ze zm.

uczestników obrotu na rynku regulowanym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

W przypadku dostawców usług płatniczych tajemnica zawodowa została określona w art. 11 ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[15] i obejmuje informacje dotyczące użytkownika lub posiadacza pieniądza elektronicznego w związku ze świadczonymi mu usługami płatniczymi, wydawanym mu pieniądzem elektronicznym lub udzielonym mu kredytem w tym oznaczenie rachunku płatniczego użytkownika oraz stan tego rachunku, a także inne informacje związane z transakcjami płatniczymi oraz zawieranymi z użytkownikiem lub posiadaczem pieniądza elektronicznego umowami, jeżeli nieuprawnione ujawnienie takiej informacji mogłoby narazić na szkodę prawnie chroniony interes użytkownika lub posiadacza pieniądza elektronicznego, którego ta informacja dotyczy.

Z porównania tych regulacji wynika, że co do zasady chronią one informacje o kliencie instytucji finansowych związanych z zawieranymi przez niego transakcjami czy czynnościami, w których uczestniczy, a w szczególności wszelkie informacje dotyczące stanu majątkowego klienta instytucji finansowej. Dostęp do informacji i obowiązek przestrzegania tak określonej tajemnicy zazwyczaj mają wszystkie osoby działające w imieniu instytucji finansowej bez względu na formę i typ stosunku prawnego łączącego je z tymi instytucjami[16] i obowiązek ten nie wygasa także po ustaniu stosunku prawnego danej osoby z instytucją finansową[17]. Zasady udostępnienia informacji objętych tak określoną tajemnicą zawodową są ściśle określone[18], a w instytucjach, które są uprawnione do ich pozyskania objęte są one stosowną ochroną[19]. Instytucje finansowe obowiązane są jednak także do zawiadamiania właściwych organów ścigania w przypadku uzasadnionego podejrzenia wykorzystania ich

15 T.j. Dz.U. z 2019 r., poz. 659 ze zm.

16 Por. art. 11 ust. 1 ustawy o usługach płatniczych, odmiennie w art. 9e ust. 2 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, gdzie dostęp do tajemnicy zawodowej ograniczony jest do członków organów kasy i osób pozostających z nią w stosunku pracy.

17 Por. art. 11 ust. 2 ustawy o usługach płatniczych, art. 9e ust. 3 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

18 Por. np. art. 105 Prawa bankowego, art. 9f ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, art. 12 ustawy o usługach płatniczych, art. 35 ust. 2 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

19 Por. np. art. 16 ustawy o nadzorze nad rynkiem finansowym.

działalności w celu ukrycia działań przestępczych itp i działalności takiej nie chroni tajemnica[20].

Podkreślić należy, że Prawo bankowe w art. 105a wprowadziło szczególne zasady przetwarzania przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów (w Polsce są to przede wszystkim spółdzielcze kasy oszczędnościowo-kredytowe), instytucje pożyczkowe (w tym z innych państw), a także biura informacji kredytowej informacji stanowiących tajemnicę bankową, które umożliwiają m.in. profilowanie ich klientów w oparciu o te informacje.

W przypadku, gdy ustawodawca dopuszcza korzystanie przez instytucje finansowe z outsourcingu[21], wprowadza też stosowne uregulowania pozwalające na dostęp podmiotów świadczących takie usługi także do informacji objętych tajemnicą[22].

Zazwyczaj informacje stanowiące tajemnicę zawodową (w tym bankową) są przetwarzane w formie elektronicznej, zwłaszcza, że w szeregu przypadków ustawodawca wprost przewiduje możliwość składania oświadczeń woli związanych z czynnościami i usługami świadczonymi przez instytucje finansowe w postaci elektronicznej[23]. Oznacza to, że ochrona informacji stanowiących tajemnicę zawodową (w tym tajemnicę bankową) w instytucjach finansowych obejmuje także ochronę ich systemów teleinformatycznych i stosowanych przez nie systemów przetwarzania danych.

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[24] cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. A zatem zabezpieczenie informacji stanowiących tajemnicę zawodową w instytucjach finansowych stanowi element cyberbezpieczeństwa.

20 Por. art. 106a Prawa bankowego, art. 35 ust. 6 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

21 Por. np. art. 6a–6e Prawa bankowego, art. 9a–9d ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

22 Por. np. art. 104 ust. 2 pkt 2 Prawa bankowego, art. 9f ust. 1 pkt 2 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, art. 35 ust. 2 pkt 26 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

23 Por. art. 7b Prawa bankowego, art. 3a ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

24 Dz.U. z 2018 r., poz. 1560 ze zm.

Zgodnie z art. 4 pkt 9 i 10 ustawy o krajowym systemie cyberbezpieczeństwa, krajowy system cyberbezpieczeństwa obejmuje bank centralny (Narodowy Bank Polski) i jedyny obecnie działający w Polsce bank państwowy (Bank Gospodarstwa Krajowego).

Do usług kluczowych zaliczono przyjmowanie przez instytucje kredytowe depozytów pieniężnych lub innych funduszy podlegających zwrotowi od klientów; udzielanie kredytów na swój własny rachunek; wykonywanie przez bank następujących czynności: przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów lub prowadzenie innych rachunków bankowych, lub udzielanie kredytów, lub przeprowadzanie bankowych rozliczeń pieniężnych, lub udzielanie pożyczek pieniężnych, lub świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego, lub terminowe operacje finansowe, lub nabywanie i zbywanie wierzytelności pieniężnych, lub wykonywanie czynności zleconych, związanych z emisją papierów wartościowych, lub dokonywanie obrotu papierami wartościowymi, lub świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania, lub przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku, lub wykonywanie transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy: a) przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty, przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, przez wykonywanie usług polecenia przelewu, w tym stałych zleceń, lub wykonywanie transakcji płatniczych wymienionych w pkt 13, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, lub wydawanie instrumentów płatniczych, lub umożliwianie akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (*acquiring*), lub świadczenie usługi inicjowania transakcji płatniczej; wykonywanie przez oddział banku

zagranicznego następujących czynności: przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów lub prowadzenie innych rachunków bankowych, lub udzielanie kredytów, lub przeprowadzanie bankowych rozliczeń pieniężnych, lub udzielanie pożyczek pieniężnych, lub świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego, lub terminowe operacje finansowe, lub nabywanie i zbywanie wierzytelności pieniężnych, lub wykonywanie czynności zleconych, związanych z emisją papierów wartościowych, lub dokonywanie obrotu papierami wartościowymi, lub świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania, lub przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku, lub wykonywanie transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy: przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty, przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, przez wykonywanie usług polecenia przelewu, w tym stałych zleceń, lub wykonywanie transakcji płatniczych wymienionych w pkt 13, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, lub wydawanie instrumentów płatniczych, lub umożliwianie akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (*acquiring*), lub świadczenie usługi inicjowania transakcji płatniczej; wykonywanie przez oddział instytucji kredytowej jednej z czynności bankowych, o których mowa w art. 5 ust. 1 pkt 1–3, 6 oraz ust. 2 pkt 1 i 2 ustawy – Prawo bankowe, wykonywanie czynności, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych w zakresie określonym w tym przepisie; prowadzenie rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz giełdy towarowej, organizowanie alternatywnego systemu obrotu

instrumentami finansowymi, działanie pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, polegające na staniu się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy (CCP); prowadzenie rozliczeń i transakcji zawieranych w obrocie instrumentami finansowymi[25].

Zgodnie z załącznikiem nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa instytucjami finansowymi, które w trybie art. 5 tej ustawy mogą być uznane za operatora usługi kluczowej w drodze decyzji o uznaniu za operatora usługi kluczowej mogą być instytucje kredytowe, banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe, podmiot prowadzący rynek regulowany na podstawie ustawy o obrocie instrumentami finansowymi, CCP (osobę prawną, która działa pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, stając się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy[26]), spółka, której Krajowy Depozyt Papierów Wartościowych przekazał wykonywanie określonych zadań.

W konsekwencji należy uznać, że nie wszystkie czynności i usługi świadczone przez instytucje finansowe zostały uznane za usługi kluczowe, a także nie wszystkie instytucje finansowe mogą być uznane za operatorów usług kluczowych stanowiących część krajowego systemu cyberbezpieczeństwa. Zatem nie na wszystkie instytucje finansowe nałożono obowiązki określone w art. 8–16 ustawy o krajowym systemie cyberbezpieczeństwa. W przypadku, gdy instytucje finansowe korzystają z internetowej platformy handlowej rozumianej jako usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową[27] traktowane będą jak dostawcy usługi cyfrowej[28], co wiązać się będzie z nałożeniem

25 Załącznik do rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018 r., poz. 1806).

26 Art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. UE L.2012.201.1 ze zm.).

27 Załącznik nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa.

28 Na nieprecyzyjność zawartej w załączniku nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa wskazuje M. Siwicki, *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski

na nich obowiązków określonych w art. 17–20 ustawy o krajowym systemie cyberbezpieczeństwa. Na Narodowym Banku Polskim i Banku Gospodarstwa Krajowego jako podmiotach publicznych, o których mowa w art. 4 pkt 9 i 10 ustawy o krajowym systemie cyberbezpieczeństwa ciążą obowiązki określone w art. 21–25 tej ustawy.

O ile zatem tajemnica zawodowa w instytucjach finansowych, co do zasady nie zależy od rodzaju usługi lub czynności świadczonej przez tę instytucję, to zakres obowiązków związanych z incydentami w zakresie cyberbezpieczeństwa dotyczącymi naruszenia poufności danych chronionych taką tajemnicą objęty jest zróżnicowaną regulacją ustawy o krajowym systemie cyberbezpieczeństwa w zależności zarówno od instytucji finansowej i jej typu, jak i rodzaju usługi lub czynności, z którą związana była tajemnica zawodowa. Mimo to należy uznać, że regulacja rangi ustawowej nakładająca na poszczególne instytucje finansowe uznane za dostawców usług kluczowych obowiązki związane z cyberbezpieczeństwem, szacowaniem ryzyka, wdrożenia odpowiednich środków technicznych i organizacyjnych, zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty, zarządzanie incydentami i zapobieganie i ograniczanie wpływu incydentów na bezpieczeństwo systemu informacyjnego, a także audytami bezpieczeństwa systemów informacyjnych[29] powinna wpływać na bezpieczeństwo danych chronionych tajemnicą zawodową, także jeżeli są przetwarzane z wykorzystaniem systemów informatycznych przez instytucje finansowe. W stosunku do części instytucji finansowych Komisja Nadzoru Finansowego wydała także stosowne rekomendacje[30] i wytyczne[31]. Do banków zastosowanie ma Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska

Przegląd Sądowy" 2019, nr 9, s. 15–17 oraz M. Kruk, *Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom*, „Prawo Mediów Elektronicznych" 2019, nr 1, s. 29.

29 Por. art. 8 i 15 ustawy o krajowym systemie cyberbezpieczeństwa.

30 O roli rekomendacji nadzorczych w działalności Komisji Nadzoru Finansowego – A. Jakubiak, *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich* [w:] W. Rogowski (red.), *Polityka i praktyka regulacji rynków finansowych*, Kraków–Warszawa 2015. O roli rekomendacji i wytycznych – Z. Ofiarski, *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] A. Jurkowska-Zeidler, M. Olszak (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Warszawa 2016, s. 137–160.

31 Por. C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*, Warszawa 2020, s. 28–31; C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 339–361.

teleinformatycznego w bankach[32], zawierająca m.in. rekomendacje w zakresie zarządzania bezpieczeństwem środowiska teleinformatycznego, a do spółdzielczych kas oszczędnościowo-kredytowych Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych[33]. Komisja Nadzoru Finansowego wydała także Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych[34], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji[35], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych[36], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji[37], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego[38], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych[39], których w każdym przypadku częścią są m.in. wytyczne w zakresie zarządzania bezpieczeństwem środowiska teleinformatycznego. Ponadto Komisja Nadzoru Finansowego wydała Rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego

32 https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.
33 https://www.knf.gov.pl/knf/pl/komponenty/img/Reko_SKOK_D_47953.pdf.
34 https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf.
35 https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf.
36 https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne_IT_TFI_39999.pdf.
37 https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf.
38 https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne%20_IT_infrastruktura_40003.pdf.
39 https://www.knf.gov.pl/knf/pl/komponenty/img/wytyczne_IT_firmy_inwestycyjne_40002.pdf.

i spółdzielcze kasy oszczędnościowo-kredytowe[40], wskazując w niej m.in. zagrożenia w zakresie bezpieczeństwa i ochrony danych użytkowników[41].

Zarówno regulacje prawne, jak i działania właściwych organów państwowych mają na celu zwiększenie zaufania do działających w Polsce instytucji finansowych także w zakresie przetwarzanych przez nie informacji dotyczących ich klientów i dokonywanych przez nich czynności i usług, z których korzystają, tak by zapewnić mechanizmy ochrony posiadanych przez instytucje finansowe informacji dotyczących ich klientów, niezależnie od ochrony mającej zastosowanie do danych osobowych, także jeżeli są przetwarzane przez instytucje finansowe. Podkreślić należy, że nawet jeżeli celem poszczególnych regulacji i rozwiązań nie jest wprost ochrona tajemnicy zawodowej, to jednak służą także tej ochronie. Ochrona tajemnicy zawodowej nie jest jednak bezwzględna, a informacje nią chronione mogą trafiać do innych podmiotów uprawnionych do ich otrzymania od instytucji finansowych (właściwe instytucje publiczne, inne instytucje finansowe, outsourcerzy, doradcy prawni itp.). Choć zatem ochrona poufności jest jednym z elementów cyberbezpieczeństwa, to charakter regulacji dotyczących cyberbezpieczeństwa i ochrony informacji objętych tajemnicą zawodową w instytucjach finansowych jest odmienny ze względu na stawiane im cele. Mimo to regulacje te mogą ułatwiać osiąganie dóbr chronionych – zarówno w zakresie cyberbezpieczeństwa, jak i tajemnicy zawodowej w tym tajemnicy bankowej, a dodatkowym elementem wpływającym pozytywnie w tym zakresie mogą być odrębne regulacje w zakresie ochrony danych osobowych[42] wprowadzone na poziomie europejskim, których adresatami są także instytucje finansowe.

Zwiększenie bezpieczeństwa systemów informacyjnych instytucji finansowych oraz poziomu ochrony danych osobowych niewątpliwie pozytywnie wpływa zatem na poziom ochrony tajemnicy zawodowej przez te instytucje i jest jednym z czynników zwiększających bezpieczeństwo ich funkcjonowania.

40 https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf.

41 Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, s. 2.

42 Por. C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo…*, s. 31–32, 52–57, 109–111; C. Banasiński (red.), *Cyberbezpieczeństwo…*, s. 381–432; W. Hydzik, *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 3, s. 84–87.

Bibliografia

Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.
Byrski J., Sytniewski L., *Zmiany w praktyce działania instytucji finansowych na skutek ogólnego rozporządzenia o ochronie danych. Wybrane zagadnienia prawne* [w:] W. Rogowski (red.), *Regulacje Finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017.
Byrski J., *Tajemnica prawnie chroniona w działalności bankowej*, Legalis 2010.
Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 3.
Iwanicz-Drozdowska M. (red.), *Kryzysy bankowe. Przyczyny i rozwiązania*, Warszawa 2002.
Jakubiak A., *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich* [w:] W. Rogowski (red.), *Polityka i praktyka regulacji rynków finansowych*, Kraków–Warszawa 2015.
Kruk M., *Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom*, „Prawo Mediów Elektronicznych" 2019, nr 1.
Krzysztofek M., *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.
Obal T., *System gwarantowania depozytów w USA* [w:] W. Baka (red.), *Systemy gwarantowania depozytów w Polsce i na świecie. Dziesięć lat Bankowego Funduszu Gwarancyjnego*, Warszawa 2005.
Ofiarski Z., *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] A. Jurkowska-Zeidler, M. Olszak (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Warszawa 2016.
Siwicki M., *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9.
Stępień K., *Instytucje Sieci Bezpieczeństwa Finansowego w Polsce z perspektywy instrumentów zapewniających stabilność finansową*, „Roczniki Ekonomii i Zarządzania" 2017, nr 3.

A professional secrecy in financial market institutions in the context of Polish cybersecurity regulations

Abstract

Financial market regulations contain regulations on professional secrecy, including banking secrecy, while there is no uniform regulation – for each type of financial institution the regulation in this respect is separate. Professional secrecy is not absolute, however, and the legislator sets out the rules for its sharing and exchange with other entities. Some financial institutions may be operators of key services under the national cybersecurity system, some may be treated as providers of digital services, and two of them – National Bank of Poland and the National Economy Bank (Bank Gospodarstwa Krajowego) are public entities that are part of the national cybersecurity system. Confidentiality is also an element of cybersecurity, so when processing information that is a professional secrecy in information systems, the regulations regarding the national cybersecurity system may also apply. Despite the same objectives, the application of regulations on professional secrecy and regulations on cybersecurity can be mutually reinforcing, which can be additionally supported by the application of separate regulations adopted at European level in the field of personal data protection.

Key words: cybersecurity, professional secrecy, banking secrecy, financial institution, financial market

Mirosław Karpiuk*

The legal grounds for revoking weapons licences

Abstract

Firearms, ammunition, incapacitating sprays, and certain tools and devices with the potential to pose a risk to health or life, may only be possessed with a weapons licence issued by a competent authority. Firearms licences are both issued and revoked as administrative decisions. A revocation decision must meet the general requirements for this type of administrative act, and also specify the applicable legal grounds. When a negative decision is issued, resulting in a right being taken away (such as firearms licence revocation), special consideration should be given to the grounds, making it clear why the authority chose to take such a decision. Pursuant to the generally applicable administrative procedure laws, a statement of factual grounds should, in particular, specify the facts the court considered proven, including the underlying evidence, provide the reasons why the court dismissed other evidence as implausible, and inconclusive, and state the legal reasons for the decision, including references to the relevant laws.

Key words: safety, public order, Police, administrative decision, medical certificate, ammunition

* Dr hab. Mirosław Karpiuk, Professor of the University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

The law stipulates clearly that firearms and ammunition may only be possessed with a weapons licence issued by a Provincial Police Chief in charge of the area in which the interested person resides, or in which the interested entity has its registered office. In the case of professional soldiers, the licence is issued on the basis of a permit issued by a competent Provost Marshal[1].

To recapitulate, the authorities with the power to issue a weapons licence are the Provincial Police Chief, and, for professional soldiers, the Provost Marshal.

Within a province (voivodeship), the government administration authority in charge of protecting the population and maintaining public safety and order is the Provincial Police Chief, acting in his or her own name in matters involving the issue of individual administrative acts[2].

Military Police Divisions are field organisational units of the Military Police[3]. They are headed by Provost Marshals.

The firearms types listed under Article 4 (1) (1) of the FAA include assault, hunting, sporting, gas, signal, and alarm weapons[4]; under Article 4 (1) (3) of the FAA ammunition is defined as bullets intended for firearms.

Article 4 (1) (1) of the FAA provides an incomplete, ostensive, definition of firearms. The definition is incomplete because it does not provide a comprehensive list of all the devices described as firearms, including only, as an example (as the expression "including" suggests), gas pistols. Hence, firearms may include devices other than assault, hunting, sporting, gas, signal, and alarm weapons. These may be any non-standard devices which are more than likely to emerge as weapons technology continues to develop at an ever-growing pace, and these weapons will satisfy the criteria set out in the definition provided by Article 7 of the FAA, despite not being assault, hunting, sporting, gas, alarm, or signal weapons. Evidently, then, Article 7 of the FAA sets out a well-considered definition of firearms, specifying all the distinctive

1 Art. 9 ust. 1 ustawy z dnia 21 maja 1999 r. o broni i amunicji (t.j. Dz.U. z 2019 r., poz. 284. ze zm.), further referred to as „the FAA".

2 Art. 6 ust. 1 pkt 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2019 r., poz. 161 ze zm.).

3 Art. 7 ust. 2 pkt 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz.U. z 2019 r., poz. 518 ze zm.).

4 Since the relevant legislation uses simultaneously two firearms terms (assault and hunting), and given that a synonymous interpretation is prohibited, these two terms may not be given the same meaning, wyrok NSA z dnia 6 marca 2014 r., II OSK 2406/12, LEX nr 1495283.

features which all the elements of the set of devices described as firearms must have, and not only the ones listed as examples in the scope-based definition adopted in Article 4 (1) (1) of the FAA. Therefore, firearms are all the devices considered as such under Article 4 (1) (1) of the FAA, as well as such unnamed devices as might emerge in the future[5].

As defined by Article 7 of the FAA, a firearm is a portable barrelled weapon which expels, or is designed to expel, or can be converted to expel, one or more bullets or substances by the action of a propellant, with the caveat that any object which is easily convertible for expulsion purposes may be considered as adaptable for expelling one or more bullets or substances by the action of a propellant. A signal weapon is a multiple-use device which, through the combustion of a propellant, can fire a pyrotechnic charge from a barrel with a calibre of at least 25 mm, to produce a visual or acoustic effect. An alarm weapon is a multiple-use device which produces an acoustic effect through the action of compressed gases generated by the combustion of a propellant, and the substance fired from the barrel or a substitute thereof has a range of no more than 1 metre. By extension, a firearm is any object or device which meets the requirements laid down in Article 7 (1-3) of the FAA. It is of no relevance how the device was made, or whether originally manufactured or improvised. When comparing the features of individual firearms devices, it becomes evident that they share a mode of action based on compressed gases produced by the combustion of a propellant[6].

Under Article 4 of the FAA a weapon may be understood not only as a firearm, but also as 2) a pneumatic weapon; 3) an incapacitating spray; 4) any tools and devices with the potential to pose a risk to health or life: a) a cold weapon in the form of: blades concealed in objects which do not have the appearance of a weapon, knuckledusters and nunchuks, clubs with the end made of a heavy and hard material, or containing an inlay made of such material, clubs made of wood or other heavy and hard material as baseball bat imitations; b) bowstring weapons in the form of crossbows; c) electric incapacitation devices.

In accordance with Article 9 (3) of the FAA, incapacitating sprays and the tools and devices listed in the said law (cold weapons, bowstring weapons in

5 Postanowienie SN z dnia 22 stycznia 2003 r., I KZP 40/02, OSNKW 2003, nr 1–2, poz. 11.

6 S. Maj, *Komentarz do art. 7* [w:] S. Maj, *Ustawa o broni i amunicji. Komentarz*, LEX 2010.

the form of crossbows, and electric incapacitation devices) may be possessed with a weapons licence issued by a Provincial Police Chief in charge of the area in which the interested person resides, or in which the interested entity has its registered office. In the case of professional soldiers, the licence is issued on the basis of a permit issued by a competent Provost Marshal.

Mandatory licensing does not apply to pneumatic weapons, as the only requirement applicable to them under Article 9 (4) of the FAA is to hold a pneumatic-weapon registration card.

However, pursuant to Article 11 of the FAA, the licence rule is subject to certain exceptions. These include cases in which: 1) weapons are part of museum collections under separate legislation; 2) weapons are used for sporting, training, or recreational purposes on a shooting range issued with an operating licence by a competent authority; 3) signal and alarm firearms are used to call for help, or conduct search and rescue operations, and where used by the licensee to signal the start of a sporting competition, if needed; 4) weapons and ammunition are possessed by businesses selling weapons under applicable permissions, or supplying gunsmith services pursuant to separate legislation, provided that such services are directly part of the business activity; 5) a particular possessed weapon has been submitted for deactivation or confirmation of deactivation; 6) the possessed firearm has been deactivated; 7) the possessed weapon is an electric incapacitation device with an average current intensity output of no more than 10mA; 8) the possessed weapon is a hand-held incapacitating spray; 9) the possessed weapon is a pneumatic weapon; 10) the possessed weapon is a muzzle-loading firearm made before 1885, or a replica thereof; 11) the possessed weapon is an alarm weapon with a calibre of 6 mm. Since the catalogue of exceptions set out in Article 11 of the FAA is closed, a weapons licence will be required in all cases other than those described in that provision.

Any possessed weapon in violation of the FAA requirements, i.e. without the mandatory licence, thus rendering it impossible for the relevant authorities to supervise whether it is properly used and stored, represents a threat to public order[7]. Public order involves the maintenance of legal and public order[8]

7 Wyrok WSA z dnia 16 października 2007 r., VI SA/Wa 1502/07, LEX nr 399259.

8 M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, vol. 1, p. 45. For more on public order, also see: M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2, s. 32; M. Karpiuk, K. Prokop, P. Sobczyk,

(a certain organised system of entities, tools and rules), and as such it determines whether or not a weapons licence may be issued. This type of administrative control (exercised through the requirement to obtain permission from a competent authority) prevents individuals who could disrupt the public from using weapons legally.

The conditions for revoking weapons licences are set out in Article 18 of the FAA. In accordance with Article 18 (1) of the FAA, a competent Police authority may revoke a weapons licence if the person issued with such a licence: 1) fails to meet the conditions laid down in the weapons licence; 2) is one of the persons referred to in Article 15 (1) (2-6) of the FAA; 3) fails to report the loss of his or her weapon; 4) is moving or carrying an unloaded weapon when under the influence of alcohol, a psychoactive substance or psychotropic drug, or a substitute drug.

Pursuant to Article 10 (7) of the FAA, a competent Police authority (a Provincial Police Chief or a District [Poviat] Police Chief) may decide that a specific licence restricts the use of a weapon or prohibits the holder from carrying it, in which case an appropriate note is included in the weapon-holder's ID card. If the holder of a licence involving such a restriction fails to comply with it, the Police authority may revoke the licence pursuant to Article 18 (1) (1) of the FAA. The law stipulates clearly that in such circumstances the weapons licence *is*, not *may be*, revoked, and the competent authority acts accordingly.

The individuals referred to in Article 15 (1) (2-6) of the FAA must have their weapons licences revoked. These include individuals: 1) with mental disorders[9]

Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny, Siedlce 2017, s. 14–21; K. Chałubińska-Jentkiewicz, *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów* [w:] G. Blicharz, M. Delijewski (red.), *Klauzule porządku publicznego i moralności publicznej*, Warszawa 2019, s. 244–245; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017, s. 96–102; A. Pieczywok, *Profesjonalność funkcjonariuszy wybranych służb w obszarze bezpieczeństwa i porządku publicznego* [w:] M. Karpiuk, A. Pieczywok (red.), *Służba w formacjach bezpieczeństwa i porządku publicznego*, Warszawa 2016, s. 10; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9, p. 11.

9 A mentally disturbed individual is a person who 1) is mentally ill (suffering from psychotic disorders); 2) is intellectually disabled; 3) or exhibits other mental disturbances recognised by state-of-the-art medicine as mental disorders, and requires healthcare services or other forms of assistance and care essential for them to function in their family and social environments, art. 3 pkt 1 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (t.j. Dz.U. z 2018 r., poz. 1878 ze zm.). Under the applicable law a person

or substantial psychophysical limitations; 2) with serious psychological dysfunctions; 3) addicted to alcohol or psychoactive substances; 4) having no permanent place of residence on the territory of the Republic of Poland; 5) representing a threat to themselves, or to public order or security[10]: a) lawfully convicted of an intentional crime[11] or a fiscal crime, b) lawfully convicted of an unintentional crime against life and health, and against traffic safety, when under the influence of alcohol or a psychoactive substance, or guilty of a hit-and-run accident.

A final medical or psychological certificate is binding on Police authorities as they determine the factual and legal grounds for licence revocation. Once the administrative procedure is pending before the Police authorities, such certificates are no longer subject to review. This means that the relevant administrative decision is binding, as the law does not provide Police authorities with the right to choose the manner in which they settle the matter. A final medical or psychological certificate may, then, effectively preclude the possession of a licensed weapon[12].

A decision to revoke a weapons licence is not a penal, but an administrative, measure. Indeed, under the law the very fact of having been legally convicted of an intentional crime or fiscal crime represents a valid legal ground to

exhibiting other mental disturbances may be considered a mentally disturbed individual on the condition that such disturbances affect the functioning of that individual to the degree that they require health services (e.g. outpatient psychiatric or psychological care, inpatient or day psychiatric treatment) or other forms of assistance (occupational therapy, social assistance, nursing or social care, psychiatric rehabilitation, community integration) in order to be able to function in their families and communities, K. Bobińska, P. Gałecki, *Komentarz do art. 3* [w:] K. Bobińska, K.Z. Eichstaedt, P. Gałecki, *Ustawa o ochronie zdrowia psychicznego. Komentarz*, LEX 2016. Instead of „mental disease", the currently preferred term is „mental disorder". The latter encompasses all disorders involving psychotic symptoms: hallucinations, delusions, severe mood and emotional disorders, postanowienie SA w Krakowie z dnia 14 marca 2016 r., II AKz 53/16, LEX nr 2229232.

10 It is not necessary for the „threat to themselves, or to public order or security" to exist jointly to be considered a legal ground, as each of such threats individually can represent a separate legal ground for weapons licence revocation, wyrok WSA z dnia 18 kwietnia 2018 r., II SA/Wa 1728/16, LEX nr 2522178.

11 Each conviction of an intentional crime is penalised with a weapons licence revocation ruling, wyrok NSA z dnia 19 stycznia 2018 r., II OSK 781/16, LEX nr 2442801. Where a weapons licence holder has been lawfully convicted of any intentional crime, it is reasonable to assume by default that such legal grounds exist to deem such a person as representing a threat to themselves, or to public order or security, resulting in a mandatory decision to revoke the weapons licence, wyrok WSA z dnia 16 maja 2017 r., II SA/Ol 1391/16, LEX nr 2315183.

12 Wyrok WSA z dnia 28 lutego 2018 r., II SA/Wa 1448/17, LEX nr 2469185.

revoke a weapons licence. By committing such unlawful acts, the individual creates reasonable doubt as to his or her capacity for possessing a weapon. Due to their potential to pose a threat to human life or health, weapons and ammunition must be controlled, and access to them must be restricted to emotionally stable, law-abiding, even-tempered, and mature individuals. Hence, the laws under which people may possess weapons and ammunition must be interpreted as rigorously as possible[13].

Under Article 25 of the FAA a weapons licence is revoked in the case of failure to comply with the obligation to report the loss of the weapon. In accordance with this provision, where a weapon is lost, the individual who possessed it is required to report the loss immediately, within 24 hours at the latest, to the Police or Military Police.

The time limit referred to in Article 25 of the FAA runs from the time the individual becomes aware that the weapon has been lost[14]. However, considering how important it is to quickly report that the weapon has been lost in order to recover the weapon and, consequently, to prevent its use to breach public order or security, and, given the unique nature of having a weapons licence, which, as a rule, should be issued to persons who are aware of the risks associated with the improper storage, carrying or use of weapons, it should be assumed that the time limit under Article 25 of the FAA runs not only from the time the individual actually becomes aware that they have lost his or her weapon, but also from the time he or she *should have* become aware of such a loss, had due care been exercised as required from individuals given a right as special as a weapons licence[15].

It is the obligation of every weapon holder to report the loss of the weapon immediately to the Police or Military Police, with the caveat that in this specific situation "immediately" means no more than 24 hours from the time of becoming aware of the loss of the weapon. The loss of a weapon should be understood as losing control over it and not knowing where, and in whose possession, it is. The circumstances in which the weapon was lost are irrelevant. A lost weapon report should be submitted to the closest Police or

13 Wyrok WSA z dnia 19 lipca 2017 r., II SA/Wa 218/17, LEX nr 2354933.
14 Wyrok WSA z dnia 26 sierpnia 2016 r., II SA/Wa 95/16, Legalis nr 1513770.
15 Wyrok NSA z dnia 5 grudnia 2012 r., II OSK 1419/11, Legalis nr 817178.

Military Police unit, regardless of whether it issued the licence for the weapon. What matters is that the search for the weapon starts as quickly as possible[16].

In addition to the mandatory legal grounds for weapons licence revocation, where the authority may not use its administrative discretion, the law provides for optional grounds on which the authority may or may not make a decision. Pursuant to Article 18 (4) of the FAA, a competent Police authority may revoke a weapons licence where the factual circumstances underlying its issue have ceased to exist. In such a case the authority may, but is not required to, revoke the weapons licence.

A weapons licence may also be revoked under Article 18 (5) of the FAA. In accordance with this provision, a competent Police authority may revoke a weapons licence where the holder of the licence is found to be in breach of: 1) the obligation to register the weapon within 5 days from its purchase; 2) the obligation to undergo medical and psychological examinations, and to provide medical and psychological certificates confirming that they have no mental disorders, substantial psychophysical limitations or serious psychological dysfunctions, or that they are not addicted to alcohol or psychoactive substances, and that they are capable of possessing and using the weapon; 3) the obligation to notify a competent Police authority of a change to the permanent place of residence; 4) the rules for storing, carrying, and keeping a record of weapons and ammunition; 5) the requirement to obtain a permit to export weapons and ammunition; 6) the rule under which any firearm or other weapon capable of hitting a target from a certain distance may only be used for training and sporting purposes at shooting ranges; 7) the prohibition from lending the weapon to unauthorised persons.

A person whose weapons licence has been revoked is required to return the documents confirming the legal possession of the weapon and ammunition to a competent Police authority within 7 days from the date of the final decision to revoke the weapons licence. This requirement is stipulated in Article 18 (8) of the FAA.

Such a regulation allowing weapons licence revocation is typical for administrative law. The approach adopted here by the legislators is typical for public law, allowing public authorities to influence the addressees of the legal

16 B. Kurzępa, *Komentarz do art. 25* [w:] B. Kurzępa, *Ustawa o broni i amunicji. Komentarz*, Legalis 2010.

norms they adopt, and to enforce these norms[17]. Non-conformance with the rules established by the FAA with regard to the legal possession of weapons leads to, or can lead to, licence revocation.

Bibliography

Literature

Chałubińska-Jentkiewicz K., *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów* [w:] G. Blicharz, M. Delijewski (red.), *Klauzule porządku publicznego i moralności publicznej*, Warszawa 2019.

Hoffman I., *Jedynie teoretyczna możliwość wprowadzenia katastralnego systemu opodatkowania nieruchomości – uregulowania w zakresie podatków od nieruchomości na Węgrzech*, „Analizy i Studia" 2019, nr 2.

Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.

Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2.

Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.

Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.

Pieczywok A., *Profesjonalność funkcjonariuszy wybranych służb w obszarze bezpieczeństwa i porządku publicznego* [w:] M. Karpiuk, A. Pieczywok (red.), *Służba w formacjach bezpieczeństwa i porządku publicznego*, Warszawa 2016.

Legal Acts

Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (t.j. Dz.U. z 2018 r., poz. 1878 ze zm.).

Ustawa z dnia 21 maja 1999 r. o broni i amunicji (t.j. Dz.U. z 2019 r., poz. 284. ze zm.).

Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz.U. z 2019 r., poz. 518 ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2019 r., poz. 161 ze zm.).

Rulings

Postanowienie SA w Krakowie z dnia 14 marca 2016 r., II AKz 53/16, LEX nr 2229232.

Postanowienie SN z dnia 22 stycznia 2003 r., I KZP 40/02, OSNKW 2003, nr 1–2, poz. 11.

Wyrok NSA z dnia 19 stycznia 2018 r., II OSK 781/16, LEX nr 2442801.

Wyrok NSA z dnia 5 grudnia 2012 r., II OSK 1419/11, Legalis nr 817178.

Wyrok NSA z dnia 6 marca 2014 r., II OSK 2406/12, LEX nr 1495283.

Wyrok WSA z dnia 16 maja 2017 r., II SA/Ol 1391/16, LEX nr 2315183.

Wyrok WSA z dnia 16 października 2007 r., VI SA/Wa 1502/07, LEX nr 399259.

Wyrok WSA z dnia 18 kwietnia 2018 r., II SA/Wa 1728/16, LEX nr 2522178.

17 I. Hoffman, *Jedynie teoretyczna możliwość wprowadzenia katastralnego systemu opodatkowania nieruchomości – uregulowania w zakresie podatków od nieruchomości na Węgrzech*, „Analizy i Studia" 2019, nr 2, s. 75.

Wyrok WSA z dnia 19 lipca 2017 r., II SA/Wa 218/17, LEX nr 2354933.
Wyrok WSA z dnia 26 sierpnia 2016 r., II SA/Wa 95/16, Legalis nr 1513770.
Wyrok WSA z dnia 28 lutego 2018 r., II SA/Wa 1448/17, LEX nr 2469185.

Przesłanki cofnięcia pozwolenia na broń

Streszczenie

Broń palną i amunicję do tej broni, miotacze gazu obezwładniającego oraz narzędzia i urządzenia, których używanie może zagrażać życiu lub zdrowiu, można posiadać na podstawie pozwolenia na broń wydanego przez właściwy organ. Pozwolenie na broń wydaje się w formie decyzji administracyjnej. W tej formie również organ cofa pozwolenie. Decyzja w sprawie cofnięcia pozwolenia na broń musi spełniać wymogi ogólne stawiane tego rodzaju aktom administracyjnym, a także dokładnie wskazywać, która z przesłanek znalazła zastosowanie w sprawie. Szczególne znaczenie w przypadku decyzji negatywnej, odbierającej określone uprawnienie (a taką jest cofnięcie pozwolenia na broń) będzie miało uzasadnienie, z którego powinno jasno wynikać, dlaczego organ podjął właśnie takie rozstrzygnięcie. Uzasadnienie faktyczne, w myśl ogólnych, administracyjnych przepisów procesowych, powinno w szczególności zawierać wskazanie faktów, które organ uznał za udowodnione, dowodów, na których się oparł, oraz przyczyn, z powodu których innym dowodom odmówił wiarygodności i mocy dowodowej, a uzasadnienie prawne – wyjaśnienie podstawy prawnej decyzji, z przytoczeniem przepisów prawa.

Słowa kluczowe: bezpieczeństwo, porządek publiczny, Policja, decyzja administracyjna, orzeczenie lekarskie, amunicja

Jacek Sobczak*

Problem destabilizującego gromadzenia i rozpowszechniania broni strzeleckiej i broni lekkiej oraz amunicji w prawie Unii Europejskiej

Streszczenie

Coraz bardziej zauważalny staje się problem destabilizującego gromadzenia i rozpowszechniania broni strzeleckiej i broni lekkiej oraz amunicji, nawet do tego stopnia, że stosowne regulacje przyjęła również Unia Europejska. Rada Europejska przyjęła strategię dotyczącą zwalczania nielegalnego gromadzenia broni strzeleckiej i broni lekkiej oraz amunicji do tych rodzajów broni, obejmującą przy tym również nielegalny handel nimi. Strategia ta wzywa do tego, aby wesprzeć przyjęcie prawnie wiążącego instrumentu pozwalającego na śledzenie i oznaczanie broni strzeleckiej i broni lekkiej oraz amunicji do tych rodzajów broni. Przyjmując międzynarodowy instrument umożliwiający śledzenie, takiej broni państwa zobowiązują się do przyjęcia wielu środków zapewniających odpowiednie oznaczanie i rejestrowanie tej broni oraz do zacieśnienia współpracy w śledzeniu nielegalnego handlu nią.

Słowa kluczowe: bezpieczeństwo, zagrożenia, polityka obronna, handel bronią i amunicją, Unia Europejska

* Prof. zw. dr hab. nauk prawnych w zakresie prawa, Akademia Ekonomiczno-Humanistyczna w Warszawie.

W opracowaniach poświęconych funkcjonowaniu Unii Europejskiej zapomina się zwykle lub spycha na margines kwestie dotyczące działań zewnętrznych Unii, wspólnej polityki zagranicznej i bezpieczeństwa, regulowane przez tytuł V Traktatu o Unii Europejskiej (dalej: TUE)[1]. Akcentując kwestie gospodarcze mające pierwszorzędne znaczenie do funkcjonowania Unii, nie pamięta się, że ma ona także kompetencje w zakresie wspólnej polityki zagranicznej i bezpieczeństwa, które obejmują wszelkie dziedziny polityki zagranicznej i ogół kwestii dotyczących bezpieczeństwa Unii, w tym stopniowe określanie wspólnej polityki obronnej, która jak stwierdza się w art. 24 TUE „może prowadzić do wspólnej obrony". Nie wdając się w kwestie dotyczące wspólnej polityki zagranicznej wypada jedynie zauważyć, że realizuje ją Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa, który przewodniczy Radzie ds. Zagranicznych (art. 27 ust. 1 i 2 TUE). W wykonywaniu swojego mandatu jest on wspomagany przez Europejską Służbę Działań Zewnętrznych. Zawarowano jednocześnie, że jeżeli sytuacja międzynarodowa wymaga działań operacyjnych Unii, Rada przyjmuje niezbędne decyzje, które określają zasięg tych działań, cel, zakres i środki, jakie mają być oddane do dyspozycji Unii. Zasady podejmowania tych decyzji precyzuje art. 31 ust. 1–4 TUE[2].

Pamiętać należy, iż podejmowane w tym obszarze decyzje odnoszą się do bardzo zróżnicowanych treści. Jednymi z pierwszych były działania dotyczące rozpowszechniania broni. Wiązało się to z utworzeniem pod auspicjami Programu ONZ na Rzecz Rozwoju (*United Nations Development Programme*, dalej: UNDP) w ramach Paktu Stabilności dla Europy Południowo-Wschodniej (znanego od 2008 r. jako Rada Współpracy Regionalnej). Powołano wówczas w ramach Unii Centrum Kontroli Broni Strzeleckiej i Lekkiej dla Europy Wschodniej i Południowo-Wschodniej (*South Eastern and Eastern Europe*

1 Dz.U. z 2004 r., nr 90, poz. 864/30 ze zm.

2 Art. 31 został dodany i zmieniony według numeracji ustalonej przez art. 1 pkt 34 i art. 5 ust. 1 i 2 Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat Ustanawiający Wspólnotę Europejską (Dz.Urz. UE C 2007, nr 306, s. 1 – z dniem 1 grudnia 2009 r.). W kwestii tej zob. K.J. Gruszczyński, *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej – cele i wyzwania*, „Studia Prawnicze i Administracyjne" 2016, nr 18 (4), s. 17–36. Porównaj także: R. Grzeszczak, *Globalna rola Europy oraz Wspólna Polityka Zagraniczna i Bezpieczeństwa – od słów do rzeczywistości*, „Centrum Europejskie Natolin", Warszawa 2013, s. 25 i n.; J. Jaskiernia, *System instytucjonalny polityki bezpieczeństwa UE po Traktacie z Lizbony*, „Unia Europejska – Perspektywy Społeczno-Ekonomiczne" 2013, t. 5, s. 83–91; P. Turczyński, *Aspiracje UE jako kreatora ładu międzynarodowego: lata 2005–2012*, Wrocław 2013.

Clearinghouse for the Control of Small Arms and Light Weapons, dalej: SEESAC)[3].

3 Siedzibą tej organizacji jest Belgrad. SEESAC składa się z jednostki wsparcia technicznego podejmującej działania operacyjne na szczeblu regionalnym i krajowym. SEESAC jest wspólną inicjatywą Programu Narodów Zjednoczonych ds. Rozwoju i Rady Współpracy Regionalnej (następcy paktu stabilizacji dla Europy Południowo-Wschodniej) i jako taka jest centralnym punktem w zakresie działań związanych z BSiL w Europie Południowo-Wschodniej. Jako agencja wykonawcza regionalnego planu wdrożeniowego w Europie Południowo-Wschodniej dotyczącego zwalczania rozprzestrzeniania broni strzeleckiej i lekkiej (BSiL), SEESAC ponad jedenaście lat współpracował z podmiotami krajowymi w Europie Południowo-Wschodniej nad wdrożeniem całościowego podejścia do kontroli BSiL dzięki prowadzeniu szerokiego zakresu działań obejmujących: kampanie informacyjne i kampanie zbierania BSiL, zarządzanie zapasami, zmniejszanie nadwyżek, zwiększanie zdolności w zakresie znakowania i śledzenia oraz zwiększanie kontroli eksportu broni. W ten sposób SEESAC zdobył wyjątkowe zdolności i doświadczenie w prowadzeniu na poziomie regionalnym działań obejmujących wiele podmiotów, z wykorzystaniem wspólnego zaplecza politycznego i gospodarczego państw regionu, zapewniając odpowiedzialność podmiotów na poziomie krajowym i regionalnym oraz długoterminową stabilność działań oraz kreując się na podstawowy organ w regionie w zakresie kontroli BSiL. SEESAC stworzył dwustronne i wielostronne kanały komunikacji ze wszystkimi właściwymi podmiotami i organizacjami. Prowadzi również Sekretariat Regionalnej Grupy Sterującej Europy Południowo-Wschodniej ds. Broni Strzeleckiej i Lekkiej (RSG). Ponadto SEESAC jest członkiem i byłym przewodniczącym Komitetu Sterującego Inicjatywy Regionalnego Podejścia do Zmniejszania Zapasów (RASR). Jest regularnie zapraszany do udziału we wszystkich właściwych forach regionalnych, takich jak coroczne spotkania ministrów sprawiedliwości i spraw wewnętrznych UE-Bałkany Zachodnie, organizowany przez NATO proces wymiany informacji strukturalnych na temat BSiL, proces współpracy ministrów obrony Europy Południowo-Wschodniej (SEDM). SEESAC ma szeroką sieć formalnych i nieformalnych partnerstw z organizacjami takimi jak RACVIAC (Regionalne Centrum Wspierania Weryfikacji i Wdrażania Kontroli Zbrojeń) – Centrum Współpracy w zakresie Bezpieczeństwa, Forum OBWE ds. Współpracy w zakresie Bezpieczeństwa (FSC). Dzięki działaniom koordynacyjnym ONZ w zakresie broni strzeleckiej (CASA) i innym mechanizmom odbywają się regularne spotkania koordynacyjne z innymi agendami ONZ, takimi jak UNODC i UNODA. SEESAC rozwinął się i stał się regionalnym punktem koordynującym szerokie spektrum działań związanych z reformą sektora bezpieczeństwa, koncentrującym się szczególnie na kontroli BSiL oraz zarządzaniu zapasami broni. SEESAC z siedzibą w Belgradzie działa obecnie w całej Europie Południowo-Wschodniej: Albanii, Bośni i Hercegowinie, Chorwacji, Czarnogórze, Republice Mołdawii, Serbii i byłej jugosłowiańskiej republice Macedonii (FYROM). Odpowiedzialność regionu za działania zapewnia Rada Współpracy Regionalnej oraz Regionalna Grupa Sterująca ds. BSiL, na forach których wszystkie państwa Europy Południowo-Wschodniej przedstawiają wytyczne strategiczne, inicjatywy i wnioski o działania SEESAC. Radzenie sobie ze wspólnymi problemami dzięki inicjatywom regionalnym okazało się korzystne dla Europy Południowo-Wschodniej nie tylko z powodu wynikłego z tego dzielenia się kluczowymi informacjami i propagowania zdrowego współzawodnictwa regionalnego, ale także z uwagi na fakt, że pomaga osiągać stałe i dające się łatwo zmierzyć rezultaty dzięki całościowemu wdrożeniu. Udział SEESAC we wszystkich właściwych procesach i inicjatywach regionalnych (takich jak SEDM, RASR i RACVIAC) zapewnia terminową i uczciwą wymianę informacji, dobrą znajomość sytuacji i perspektywę koniecznie, by umożliwić wdrożenie działań bez ich powielania, zgodnie z obecnymi potrzebami rządów i regionów oraz z rozwijającymi się tendencjami. SEESAC opiera wszystkie swoje działania

SEESAC ma zapobiegać rozprzestrzenianiu się i nadmiernemu gromadzeniu broni strzeleckiej i lekkiej oraz amunicji do niej w Europie Południowo-Wschodniej, przy czym szczególny nacisk kładzie ona na opracowanie przedsięwzięć regionalnych, służących rozwiązywaniu problemu transgranicznych przepływów broni[4].

Działania SEESAC Unia Europejska wspierała najpierw Wspólnym Działaniem 1999/34/WPZiB w sprawie zwalczania destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej[5], a następnie Wspólnym Działaniem Rady z 12 lipca 2002 r. (2002/589/WPZiB) w sprawie wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej oraz uchylające Wspólne Działanie 1999/34/WPZiB[6]. W jego treści określono działania, zasady dotyczące aspektów prewencji i reagowania środki prowadzące do celów oraz wkład finansowy Unii. W treści Wspólnego Działania wskazano, że Unia ma na celu budowanie zgody na stosownych płaszczyznach międzynarodowych uznając za właściwe w kontekście regionalnym urzeczywistnianie zasad i środków mających zapobiegać dalszemu destabilizującemu gromadzeniu broni lekkiej[7]. Uznano także za konieczne udzielanie pomocy państwom

na zebranych danych podstawowych, zapewnia zatwierdzanie działań i polityczne poparcie przez podmioty krajowe jako warunek wstępny działań. Wdrażał on bardzo skutecznie poprzednie projekty finansowane przez UE, zapewniając zrównoważone wyniki dzięki rozwijaniu krajowej odpowiedzialności za projekty i działania oraz zachęcaniu do niej, dzięki propagowaniu koordynacji regionalnej, wymiany doświadczeń i najlepszych praktyk oraz badań regionalnych. Jego wiedza na temat BSiL oraz pogłębiona znajomość kwestii regionalnych i właściwych podmiotów czyni z SEESAC najlepszego partnera w realizacji tego konkretnego działania.

4 W kwestii realizacji strategii Unii Europejskiej na Bałkanach Zachodnich zobacz: P. Chlebowicz, *Nielegalny handel bronią*, Warszawa 2015, s. 241–243.

5 Dz.Urz. UE L 1999, nr 9, s. 1.

6 Dz.Urz. UE L 2002, nr 191, s. 1.

7 Do tych zasad i środków zaliczono: zobowiązanie się wszystkich krajów do importu i posiadania broni lekkiej tylko dla ich słusznych potrzeb w zakresie bezpieczeństwa oraz do poziomu proporcjonalnego do ich słusznych wymogów obronności i bezpieczeństwa, łącznie z ich zdolnością do uczestnictwa w operacjach pokojowych ONZ; zobowiązanie się krajów wywożących do dostarczania broni lekkiej wyłącznie rządom (bezpośrednio albo poprzez należycie licencjonowane jednostki upoważnione do dostarczania broni w ich imieniu) zgodnie z odpowiednimi restrykcyjnymi międzynarodowymi i regionalnymi kryteriami wywozu broni, jak w szczególności przewidziano w kodeksie postępowania UE, łącznie z wydawanymi na podstawie oficjalnego zezwolenia świadectwami ostatecznego przeznaczenia lub, gdy właściwe, innych stosownych informacji w sprawie ostatecznego przeznaczenia; zobowiązanie się wszystkich krajów do produkcji broni lekkiej wyłącznie do celów posiadania lub eksportu. Ponadto w celu zapewnienia kontroli uznano za konieczne

żądającym wsparcia dla kontroli i wyeliminowania broni lekkiej i amunicji do niej, popieranie środków budowy zaufania i zachęty w celu dobrowolnego składania nadwyżek broni lekkiej i broni posiadanej nielegalnie, wreszcie demobilizacji wojowników, środków mierzących do kontroli zbrojeń, skuteczne usuwanie nadwyżek broni lekkiej oraz szybkie i skuteczne jej niszczenie, najlepiej pod nadzorem międzynarodowym. We Wspólnym Działaniu określono także wkład finansowy i techniczny Unii oraz zasady podejmowania decyzji o przydzielaniu finansowego i technicznego wsparcia, zmierzającego do realizacji celów Wspólnego Działania.

W art. 6 Wspólnego Działania z dnia 12 lipca 2002 r. odnoszącym się do wkładów finansowych Unii stwierdzono, że Unia udzieli finansowego i technicznego wsparcia programom i projektom, które wnoszą bezpośredni i rozpoznawalny wkład do zasad i środków dotyczących aspektów prewencji i reagowania łącznie ze stosownymi programami i projektami kierowanymi przez Narody Zjednoczone, Międzynarodowy Komitet Czerwonego Krzyża, inne organizacje międzynarodowe oraz struktury i organizacje pozarządowe. Wskazano, że projekty te mogą obejmować odbieranie broni, reformę sektora bezpieczeństwa oraz programy demobilizacji i ponownej integracji, jak również specjalne programy pomocy ofiarom[8].

utworzenie i utrzymywanie narodowych spisów legalnie posiadanej broni będącej własnością władz kraju oraz ustanowienie restrykcyjnego narodowego prawodawstwa dotyczącego broni lekkiej obejmującego sankcje karne i skuteczną kontrolę administracyjną. Wskazano na konieczność stworzenia środków budowy zaufania, obejmujących środki popierania przejrzystości i otwartości, przez regionalne rejestry broni lekkiej i wymianę dostępnych informacji dotyczących wywozu, przywozu, produkcji i własności broni lekkiej oraz narodowego prawodawstwa dotyczącego broni, a także przez konsultacje z udziałem właściwych stron w sprawie wymienionych informacji. Podniesiono także konieczność zaangażowania się w zwalczanie nielegalnego handlu bronią lekką przez wprowadzenie w życie skutecznych kontroli krajowych, takich jak sprawne mechanizmy graniczne i celne, regionalna i międzynarodowa współpraca oraz wzmożona wymiana informacji, a także zaangażowanie się w walkę i odwrócenie „kultur przemocy" przez wzmaganie społecznego zaangażowania dzięki szkolnictwu publicznemu i programom uświadamiającym (art. 3 Wspólnego Działania z dnia 12 lipca 2002 r.).

8 W nawiązaniu do treści tego przepisu wydano kolejno kilka decyzji Rady, a mianowicie: z dnia 21 października 2002 r. dotyczącą Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej w Europie Południowo-Wschodniej (Dz.Urz. UE L 2002, nr 289, s. 1 ze zm.); z dnia 14 kwietnia 2003 r. dotyczącą Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zniszczenie amunicji do ręcznej broni strzeleckiej i boni lekkiej w Albanii (Dz.Urz. UE L 2003, nr 99, s. 60 ze zm.). W decyzji tej nawiązano do wspólnego stanowiska z dnia 2 czerwca 1997 r. określonego przez Radę na podstawie art. J. 2 Traktatu o Unii Europejskiej w sprawie

Warto zauważyć, że niejako w wykonaniu treści art. 4 Wspólnego Działania Rady z 12 lipca 2002 r. wydana została decyzja Rady 2005/852/WPZiB z 29 listopada 2005 r. w sprawie zniszczenia broni strzeleckiej i broni lekkiej (SALW) oraz amunicji do tego rodzaju broni na Ukrainie[9]. W motywach tej decyzji wywiedziono, że Ukraina w przeszłości posiadała znaczny kompleks przemysłowy, trzeci co do wielkości na świecie, arsenał broni jądrowej oraz była bazą strategicznych rezerw broni i amunicji ZSRR. Wskazano, że według niektórych szacunków na Ukrainie znajduje się aż 7 milionów sztuk ręcznej broni strzeleckiej i broni lekkiej (SALW) oraz 2 miliony ton amunicji, z których znaczna część pochodzi z czasów ostatnich wojen światowych. Te duże ilości SALW i amunicji stanowią nie tylko ogromną nadwyżkę w stosunku do aktualnej liczebności sił zbrojnych Ukrainy, lecz również zawierają wiele niezdatnych do użycia i niebezpiecznych sztuk amunicji. Odwołując się do planu działania UE–Ukraina, który został przyjęty przez Radę Współpracy UE–Ukraina w dniu 21 lutego 2005 r., przypomniano, że Ukraina została wezwana do przeciwstawienia się zagrożeniom dla bezpieczeństwa, zdrowia publicznego i środowiska naturalnego związanym z ukraińskimi składami starej amunicji, m.in. min przeciwpiechotnych[10].

Albanii (Dz.Urz. UE L 1997, nr 153, s. 4). Kolejną decyzją była decyzja Rady 2003/543/WPZiB, z dnia 21 lipca 2003 r. dotyczącą wykonania Wspólnego Działania 2002/589/WPZiB w związku wkładem Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej w Ameryce Łacińskiej i na Karaibach (Dz.Urz. UE L 2003, nr 185, s. 59). W decyzji tej przywołano decyzję Rady 2001/200/WPZiB (Dz.Urz. UE L 2001, nr 72, s. 1), w której Unia Europejska zdecydowała się wnieść wkład w zwalczanie niekontrolowanego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej, która stanowiła zagrożenie dla pokojui bezpieczeństwa i zmniejszała perspektywy stałego rozwoju m.in. w Ameryce Łacińskiej i na Karaibach. W ten sposób Unia Europejska wniosła wkład do Regionalnego Centrum Organizacji Narodów Zjednoczonych na Rzecz Pokoju, Rozbrojenia i Rozwoju w Ameryce Łacińskiej i na Karaibach (UN-LiREC) w Limie, działającego w imieniu Departamentu ds. Rozbrojenia (DDA) Organizacji Narodów Zjednoczonych. W treści art. 6 i 7 wiąże się także obowiązująca nadal decyzja Rady 2006/1000/WPZiB z dnia 11 grudnia 2006 r. dotycząca wdrożenia Wspólnego Działania 2002/589/WPZiB w związku z wkładem Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania broni strzeleckiej i lekkiej w Ameryce Łacińskiej i na Karaibach (Dz.Urz. UE L 2006, nr 367, s. 77).

9 Dz.Urz. UE L 2005, nr 315, s. 27.

10 Podkreślono także w motywach, że Agencja NATO ds. Zabezpieczenia Technicznego i Zaopatrzenia (NAMSA), w ramach Funduszu Powierniczego Partnerstwa dla Pokoju (PdP), zarządza dwunastoletnim projektem, który ma być realizowany w czterech fazach i którego celem jest zniszczenie nadwyżki wynoszącej 1,5 miliona sztuk SALW oraz 133 000 ton amunicji konwencjonalnej. Unia Europejska jest zdania, że wkład finansowy w realizację pierwszej fazy projektu pomógłby Ukrainie zmniejszyć ryzyko związane ze zgromadzoną

W treści decyzji Rady z 29 listopada 2005 r. wskazano, że Unia Europejska wspiera niszczenie ręcznej broni strzeleckiej i broni lekkiej (SALW) oraz amunicji do tych rodzajów broni na Ukrainie. W tym celu Unia Europejska udziela Agencji NATO ds. Zabezpieczenia Technicznego i Zaopatrzenia (NAMSA) wsparcia finansowego podczas realizacji pierwszej fazy dwunastoletniego projektu mającego na celu pozbawienie cech użytkowych 400 000 sztuk SALW, 15 000 ton uzbrojenia konwencjonalnego oraz 1000 sztuk przenośnych przeciwlotniczych zestawów rakietowych (MANPAD).

Kolejnym dokumentem opartym o treść art. 3 Wspólnego Działania Rady z 12 lipca 2002 r. była decyzja Rady 2004/833/WPZiB z dnia 2 grudnia 2004 r. dotycząca wykonania Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej do CEDEAO w ramach moratorium dotyczącego ręcznej broni strzeleckiej i broni lekkiej[11]. W jego treści stwierdzono, że nadmierne i niekontrolowane gromadzenie oraz rozpowszechnianie broni strzeleckiej i broni lekkiej stanowią zagrożenie dla pokoju i bezpieczeństwa oraz zmniejszają perspektywy trwałego rozwoju, co dotyczy zwłaszcza Afryki Zachodniej. W związku z tym Unia Europejska deklaruje chęć działania w ramach właściwych organizacji międzynarodowych w celu wspierania środków służących budowaniu zaufania, uważając, że wkład finansowy oraz pomoc techniczna przyczyniłyby się do skonsolidowania inicjatywy wspólnoty gospodarczej państw Afryki Zachodniej (CEDEAO) w zakresie ograniczenia

dużą ilością SALW i amunicji, jak również dostosować poziom SALW i amunicji do aktualnej liczebności jej sił zbrojnych. W dniu 18 maja 2005 r. parlament Ukrainy ratyfikował Konwencję o zakazie używania, magazynowania, produkcji i transferu min przeciwpiechotnych i o ich zniszczeniu (Konwencję ottawską). Unia Europejska zamierzała w związku z tym zaoferować Ukrainie wsparcie finansowe zgodnie z przepisami tytułu II wspólnego działania 2002/589/WPZiB. Zapewniona zostanie odpowiednia widoczność tego wsparcia finansowego poprzez, m.in., stosowne środki przedsięwzięte przez NAMSA. Godzi się także przypomnieć podpisaną 14 stycznia trójstronną deklarację prezydentów Ukrainy, Rosji i USA, z której treści wnika, że cała broń nuklearna rozmieszczona na terytorium Ukrainy zostanie zniszczona, bądź usunięta z tego obszaru. Przed ratyfikacją tego dokumentu władze ukraińskie zażądały formalnych gwarancji bezpieczeństwa ze strony mocarstw nuklearnych. W efekcie 5 grudnia 1994 r. w Budapeszcie doszło do podpisania Memorandum o gwarancjach bezpieczeństwa, w którym Stany Zjednoczone, Federacja Rosyjska i Wielka Brytania zobowiązały się do respektowania suwerenności i integralności terytorialnej Ukrainy oraz powstrzymania się od wszelkich gróźb użycia siły przeciwko jej niepodległości i integralności terytorialnej, w zamian za co Ukraina zgodziła się przekazać strategiczną broń nuklearną Rosji i przystąpić do układu o nierozpowszechnianiu broni jądrowej. W kwestii Memorandum Budapesztańskiego zob. M. Gołda-Sobczak, *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016, s. 194–196.

11 Dz.Urz. UE L 2004, nr 358, s. 65.

przywozu, wywozu i produkcji ręcznej broni strzeleckiej i broni lekkiej. W tym celu postanowiła wnieść wkład finansowy i udzielić pomocy technicznej stwarzając jednostkę ds. ręcznej broni strzeleckiej w ramach sekretariatu technicznego CEDEAO oraz przekształcić moratorium w konwencję o ręcznej broni strzeleckiej i broni lekkiej między członkami CEDEAO. Powołano jednocześnie technika tego projektu, którego stwierdzając, że jego siedzibą będzie Abudża w Nigerii. Określono także, że finansowa kwota referencyjna celów określonych w decyzji 2004/833/WPZiB wynosi 515 tys. Stwierdzono, że decyzja wygaśnie 31 grudnia 2005 r.[12].

Kolejnym dokumentem była decyzja Rady z dnia 21 października 2002 r. dotycząca wykonania Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej w Europie Południowo-Wschodniej[13]. Decyzją tą zapewniono UNDP oraz ustanowionej Regionalnej Agencji Informacyjnej dla Europy Południowo-Wschodniej o Redukcji Ręcznej Broni Strzeleckiej z siedzibą w Belgradzie pomoc finansową w kwocie referencyjnej 330 tys. euro. Wspomniana decyzja została przedłużona i zmieniona najpierw decyzją Rady 2003/807/WPZiB rozszerzającą i zmieniającą decyzję 2002/842/WPZiB dotyczącą wykonania wspólnego działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania broni strzeleckiej i broni lekkiej w Europie Południowo-Wschodniej[14], a następnie decyzją 2004/791/WPZiB Parlamentu Europejskiego i Rad z dnia 21 kwietnia 2004 r. ustanawiającą Wspólny Program Działań w celu promowania działań jednostek działających na poziomie europejskim oraz wspierania określonych działań w obszarze edukacji i szkolenia[15], w której odniesiono się do kwestii finansowania z budżetu ogólnego wspólnot europejskich programów unijnych, wreszcie przez decyzję Rady 2010/179/WPZiB z dnia 11 marca 2010 r. wspierającą kontrolę uzbrojenia SEESAC na Bałkanach Zachodnich w ramach strategii UE

12 Wyrokiem Trybunału Sprawiedliwości UE (Wielka Izba) z dnia 20 maja 2008 r. w sprawie C 91/05 Komisja Wspólnot Europejskich przeciwko Radzie Unii Europejskiej stwierdzono, że decyzja Rady 2004/833/WPZiB z dnia 2 grudnia 2004 r. dotycząca wykonania Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej do CEDEAO w ramach moratorium dotyczącego ręcznej broni strzeleckiej i broni lekkiej jest nieważna (Dz.Urz. UE C 2008, nr 171, s. 2/2).

13 Dz.Urz. UE L 2002, nr 289, s. 1. Decyzja ta wygasła 31 grudnia 2005 r.

14 Dz.Urz. UE L 2003, nr 302, s. 39.

15 Dz.Urz. UE L 2004, nr 138, s. 31.

w zakresie zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni oraz handlu nimi[16]. W tej ostatniej decyzji przeznaczono na osiągnięcie celów decyzji kwotę 1600 tys. euro.

Problemu broni strzeleckiej i lekkiej dotyczy także pomijane częstokroć w innych dokumentach wspólne działanie Rady 2008/113/WPZiB z dnia 12 lutego 2008 r. wspierające międzynarodowy instrument umożliwiając państwom identyfikowanie i śledzenie w odpowiednim czasie i niezawodny sposób nielegalnej broni strzeleckiej i lekkiej (BSiL) w ramach strategii UE zwalczania nielegalnego gromadzenia BSiL i amunicji do tych rodzajów broni oraz nielegalnego handlu nimi[17]. W treści motywów tego dokumentu stwierdzono, że w dniu 8 grudnia 2005 r. Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych przyjęło międzynarodowy instrument umożliwiający państwom identyfikowanie i śledzenie, w odpowiednim czasie i w niezawodny sposób, nielegalnej broni strzeleckiej i lekkiej (BSiL) (zwany dalej „międzynarodowym instrumentem umożliwiającym śledzenie"). Podkreślono, że w dniach 15 i 16 grudnia 2005 r. Rada Europejska przyjęła strategię UE w zakresie zwalczania nielegalnego gromadzenia BSiL i amunicji do tych rodzajów broni oraz nielegalnego handlu nimi („strategia BSiL") wzywającą do tego, by wesprzeć przyjęcie prawnie wiążącego instrumentu międzynarodowego umożliwiającego śledzenie i oznaczanie BSiL i amunicji do niej. Przyjmując międzynarodowy instrument umożliwiający śledzenie, państwa zobowiązały się do przyjęcia wielu środków zapewniających odpowiednie oznaczanie i rejestrowanie BSiL oraz do zacieśnienia współpracy w śledzeniu nielegalnej BSiL. Państwa miały w szczególności zapewnić sobie możliwość śledzenia i odpowiadania na wnioski o śledzenie zgodnie z wymogami międzynarodowego instrumentu umożliwiającego śledzenie. Zgodnie z tym instrumentem państwa mają we właściwy sposób współpracować z Organizacją Narodów Zjednoczonych, tak by wesprzeć jego skuteczne wdrożenie. Dodano, że nieco później, 6 grudnia 2006 r. Zgromadzenie Ogólne Narodów Zjednoczonych przyjęło rezolucję 61/66 w sprawie „Nielegalnego handlu bronią strzelecką i bronią lekką we wszystkich jego aspektach" wzywającą państwa do wdrożenia międzynarodowego instrumentu umożliwiającego śledzenie, którego wdrożenie będzie rozpatrywane podczas odbywającego się co dwa lata i wypadającego w 2008 r. spotkania państw.

16 Dz.Urz. UE L 2010, nr 80, s. 48.
17 Dz.Urz. UE L 2008, nr 40, s. 16.

W treści normatywnej Wspólnego Działania zadeklarowano, że Unia Europejska dąży do promowania wspomnianego wyżej międzynarodowego instrumentu wdrażając działania techniczne, pragnie się także włączyć do serii regionalnych i subregionalnych warsztatów organizowanych przez Departament ds. Rozbrojenia Sekretariatu ONZ. Wskazano, że obejmować one będą swoim zasięgiem obszar Afryki Zachodniej, Azji, Ameryki Łacińskiej i Karaibów.

Kwestii tej dotyczy także decyzja Rady 2013/730/WPZiB z 9 grudnia 2013 r. wspierająca działania SEESAC[18] w zakresie rozbrojenia i kontroli zbrojeń w Europie Południowo-Wschodniej w ramach strategii UE w zakresie

18 W załączniku do decyzji stwierdzono, że sformułowany w decyzji projekt uzupełnia również równoległą inicjatywę SEESAC dotyczącą kontroli transferu broni, której celem jest zwiększenie zdolności w zakresie kontroli handlu bronią dzięki zwiększonej przejrzystości i współpracy regionalnej. Ponadto, jeżeli chodzi o Bośnię i Hercegowinę, projekt uzupełnia dwa inne projekty: projekt EXPLODE – finansowany z krótkoterminowego komponentu unijnego Instrumentu na rzecz Stabilności i realizowany przez biuro UNDP w Sarajewie we współpracy z misją OBWE w Bośni i Hercegowinie – na rzecz zwiększenia bezpieczeństwa ludności Bośni i Hercegowiny poprzez zmniejszenie zagrażających stabilności zapasów amunicji i zwiększenie bezpieczeństwa składowania; projekt SECUP w Bośni i Hercegowinie, którego celem są usprawnienia w składach amunicji i broni, realizowany wspólnie przez misję OBWE w Bośni i Hercegowinie oraz Ministerstwo Obrony Bośni i Hercegowiny, i w przypadku którego EUFOR zapewnia doradztwo techniczne i monitoruje aspekty realizacji projektu związane z bezpieczeństwem i ochroną, SEESAC będzie regularnie współpracował z EUFOR Althea, misją OBWE w Bośni i Hercegowinie oraz biurem UNDP w Sarajewie, aby zapewnić stałą koordynację i komplementarność z tymi projektami oraz z prowadzonymi obecnie przez społeczność międzynarodową działaniami dotyczącymi kwestii nadwyżek zapasów amunicji do broni konwencjonalnej przetrzymywanymi przez Ministerstwo Obrony Bośni i Hercegowiny oraz z uwagi na ewentualne przyszłe plany kampanii na rzecz zbierania nielegalnej broni konwencjonalnej w Bośni i Hercegowinie. Jeżeli chodzi o inne państwa objęte projektem, SEESAC będzie koordynował prace z następującymi międzynarodowymi działaniami pomocowymi: projekt MONDEM w Czarnogórze, zarządzany przez Program Narodów Zjednoczonych ds. Rozwoju we współpracy z OBWE, zmierzający do zmniejszania ryzyka proliferacji dzięki rozwijaniu bezpiecznej i zapewniającej ochronę infrastruktury związanej ze składowaniem amunicji do broni konwencjonalnej i systemami zarządzania, zmniejszaniu ryzyka wybuchów, jakie zagraża ludności, poprzez demilitaryzację mało szkodliwą dla środowiska, zniszczenie toksycznych odpadów niebezpiecznych (ciekłe paliwo rakietowe) oraz wsparcie reformy sektora bezpieczeństwa dzięki zniszczeniu ograniczonej liczby systemów broni ciężkiej wskazanych przez Ministerstwo Obrony Czarnogóry; projekt KOSSAC w Kosowie, zaplanowany początkowo w celu zmniejszenia w Kosowie skali przemocy z użyciem broni i zwiększenia bezpieczeństwa ludności, z czasem stał się jednak kompleksowym projektem zapobiegania przemocy z użyciem broni, skoncentrowanym na reformie sektora bezpieczeństwa i rozwijaniu zdolności; projekt CASM w Serbii, finansowany przez Program Narodów Zjednoczonych ds. Rozwoju i Organizację Bezpieczeństwa i Współpracy w Europie, ma na celu zwiększenie bezpieczeństwa i ochrony w uprzednio wskazanych składach amunicji do broni konwencjonalnej oraz unieszkodliwienie określonych nadwyżek amunicji. SEESAC współpracuje również regularnie z OBWE, NATO i norweską organizacją *Norwegian People's Aid* oraz innymi właściwymi

zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni oraz handlu nimi[19]. W motywach decyzji z 9 grudnia 2013 r. stwierdzono, że Centrum kontroli broni strzeleckiej i lekkiej dla Europy Wschodniej i Południowo-Wschodniej (SEESAC), ustanowione w 2002 r. w Belgradzie i działające na mocy wspólnego mandatu Programu Narodów Zjednoczonych ds. Rozwoju (UNDP) i Rady Współpracy Regionalnej (następcy paktu stabilizacji dla Europy Południowo-Wschodniej), pomaga podmiotom krajowym i regionalnym kontrolować rozprzestrzenianie i niewłaściwe wykorzystywanie broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni, a także pomaga redukować te zjawiska, przyczyniając się do większej stabilności, bezpieczeństwa i rozwoju Europy Południowo-Wschodniej i Wschodniej. SEESAC kładzie szczególny nacisk na opracowywanie przedsięwzięć regionalnych służących rozwiązywaniu problemu transgranicznych przepływów broni[20].

podmiotami, by zapewnić komplementarność działań, terminowość prac i oszczędne wykorzystanie zasobów.

19 Dz.Urz. UE L 2013, nr 332, s. 19.

20 W załączniku do tej decyzji charakteryzując cele stwierdzono, że przypadki gromadzenia na dużą skalę w Europie Południowo-Wschodniej zapasów broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni, niewystarczająca liczba bezpiecznych składów i ciągły brak wystarczających zdolności w zakresie ich pełnego zabezpieczania uczyniły z państw tego regionu przedmiot szczególnych obaw oraz ważne wyzwanie w ramach strategii Unii Europejskiej w zakresie zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej (dalej: BSiL) i amunicji do tych rodzajów broni oraz handlu nimi. Z tego względu dalsze udzielanie zapewnianego wcześniej unijnego wsparcia na rzecz zwalczania zagrożeń związanych z rozprzestrzenianiem i nielegalnym handlem BSiL w Europie Południowo-Wschodniej i z jej obszaru stanowi istotną część działań zmierzających do wypełniania celów strategii UE dotyczącej BSiL. Ogólnym celem projektu jest propagowanie międzynarodowego pokoju i bezpieczeństwa dzięki stałemu wspieraniu działań zmierzających do zmniejszenia zagrożeń, jakie niesie ze sobą gromadzenie na szeroką skalę BSiL oraz amunicji do tych rodzajów broni i nielegalny handel nimi w Europie Południowo-Wschodniej. Projekt zmniejszy przede wszystkim dostępność nadwyżki BSiL i amunicji do tych rodzajów broni, zwiększy bezpieczeństwo jej składowania, ulepszy śledzenie broni dzięki lepszej rejestracji i znakowaniu, a także zwiększy przekazywanie informacji i wiedzy oraz świadomość zagrożeń związanych z BSiL. Ponadto program przyczyni się do stabilności w Europie Południowo-Wschodniej, dzięki pracom w ramach Rady Współpracy Regionalnej. Wykorzystując w szczególności skuteczną realizację decyzji Rady 2010/179/WPZiB i zgodnie ze strategią UE dotyczącą BSiL, ten projekt zakładający kontynuację działań zmierza do dalszego wzmocnienia krajowych systemów kontroli i dalszego wspierania wielostronności, przy opracowaniu regionalnych mechanizmów zwalczania dostaw i destabilizującego rozprzestrzeniania BSiL i amunicji do tych rodzajów broni. Ponadto w celu zapewnienia bardziej kompleksowego wymiaru regionalnego ten projekt zakładający kontynuację działań obejmie również regionalne procesy w Republice Mołdawii i w Kosowie dotyczące kontroli BSiL, tak aby zapewnić absolutnie całościowe, regionalne podejście oraz długoterminowe i zrównoważone skutki.

Kolejna decyzja Rady 2015/2051/WPZiB w sprawie zmiany decyzji 2013/730/WPZiB wspierającej działania SEESAC w zakresie rozbrojenia i kontroli zbrojeń w Europie Południowo-Wschodniej w ramach strategii UE w zakresie zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni oraz handlu nimi[21] zmieniła treść wspomnianej decyzji i załącznika w ten sposób, że stwierdzono, że dodatkowo Albania będzie beneficjentem komponentu bezpieczeństwa składowania. W decyzji Rady 2016/2356/WPZiB z dnia 19 grudnia 2016 r. dotyczącej wspierania działania SEESAC w zakresie rozbrojenia i kontroli zbrojeń w Europie Południowo-Wschodniej w ramach strategii UE w zakresie zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni oraz handlu nimi[22] stwierdzono, że Unia zamierza sfinansować kolejny projekt SEESAC dotyczący zmniejszenia zagrożenia nielegalnego rozprzestrzeniania broni strzeleckiej i lekkiej oraz amunicji do tego rodzaju broni. Powtarzając w załącznikach treści dotyczące celów, wyboru agencji wykonawczej, opisu projektu, beneficjentów z wcześniejszej decyzji 2013/730/WPZiB, określając czas realizacji projektu na 41 miesięcy, przy czym stwierdzono, że umowa zawarta zgodnie z decyzją wygasa w dniu 29 grudnia 2019 r.

Podsumowaniem wcześniejszych działań była decyzja Rady WPZiB 2018/1788 z 19 listopada 2018 r. w sprawie wsparcia Centrum Kontroli Broni Strzeleckiej i Lekkiej dla Europy Wschodniej i Południowo-Wschodniej (SEESAC) w realizacji regionalnego planu działania w sprawie zwalczania nielegalnego handlu bronią na Bałkanach Zachodnich[23]. W motywach decyzji dokonano przeglądu działań stwierdzając, że W dniu 16 grudnia 2005 r. Rada Europejska przyjęła strategię UE w zakresie zwalczania nielegalnego gromadzenia broni strzeleckiej i lekkiej i amunicji do tych rodzajów broni oraz handlu nimi, którą następnie poddano przeglądowi w 2018 r., i która przedstawia wytyczne działań Unii w dziedzinie broni strzeleckiej i lekkiej (zwanej dalej „BSiL"). W strategii UE dotyczącej BSiL odnotowano, że Unia będzie priorytetowo traktowała wspieranie regionalnych inicjatyw zmierzających do zwalczania nielegalnej BSiL i amunicji do tego rodzaju broni, zapewniając wsparcie finansowe i techniczne organizacjom regionalnym i krajowym odpowiedzialnym za wdrażanie odpowiednich instrumentów regionalnych. W strategii UE dotyczącej BSiL wskazano na Bałkany jako region, w przypadku którego

21 Dz.Urz. UE L 2015, nr 300, s. 19.
22 Dz.Urz. UE L 2016, nr 348, s. 60 ze zm. Dz.Urz. UE L 2019, nr 318, s. 161.
23 Dz.Urz. UE L 2018, nr 293, s. 11.

udzielanie wsparcia jest priorytetem. Podkreślono, że w dniu 17 maja 2018 r. na szczycie UE–Bałkany Zachodnie w Sofii przywódcy UE uzgodnili deklarację z Sofii, do której przyłączyli się partnerzy z Bałkanów Zachodnich. Obejmuje ona zobowiązanie do znaczącego zwiększenia współpracy operacyjnej w walce z międzynarodową przestępczością zorganizowaną w priorytetowych dziedzinach, takich jak broń palna, narkotyki, przemyt migrantów i handel ludźmi. Jest to jak stwierdzono wynikiem faktu, że region Bałkanów Zachodnich pozostaje jednym z głównych źródeł nielegalnego handlu bronią w Unii.

Zauważono, że w dniu 13 czerwca 2018 r. Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili wspólny komunikat do Parlamentu Europejskiego i Rady w sprawie elementów strategii UE na rzecz zwalczania nielegalnej broni palnej, BSiL oraz amunicji do tych rodzajów broni, zatytułowany *Zabezpieczenie broni, ochrona obywateli*. Nieco później w dniu 10 lipca 2018 r. Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej było gospodarzem szczytu Bałkanów Zachodnich w Londynie, na którym przyjęto regionalny plan działania na rzecz trwałego rozwiązania kwestii nielegalnego posiadania i niewłaściwego wykorzystywania BSiL i broni palnej oraz amunicji do nich, a także nielegalnego handlu taką bronią i amunicją na Bałkanach Zachodnich do roku 2024, który został przygotowany przez komisje ds. BSiL z Bałkanów Zachodnich w ramach francusko-niemieckiej inicjatywy darczyńców dotyczącej nielegalnego handlu bronią palną na Bałkanach Zachodnich. Komisje te przygotowują swoje harmonogramy realizacji planu działania.

Podniesiono, że Organizacja Narodów Zjednoczonych (ONZ) w Agendzie na rzecz zrównoważonego rozwoju 2030, przyjętej w dniu 25 września 2015 r., stwierdziła, że nie jest możliwe osiągnięcie zrównoważonego rozwoju bez pokoju i bezpieczeństwa oraz że nielegalne przepływy broni są jednym z czynników prowadzących do przemocy, braku bezpieczeństwa i niesprawiedliwości. Na trzeciej konferencji ONZ poświęconej przeglądowi postępów w realizacji programu działania na rzecz zapobiegania nielegalnemu handlowi bronią strzelecką i lekką, zwalczania i eliminowania go we wszystkich aspektach, która miała miejsce w czerwcu 2018 r. państwa członkowskie ONZ zobowiązały się do wzmocnienia partnerstw i współpracy na wszystkich szczeblach w celu zapobiegania nielegalnemu handlowi BSiL oraz zwalczania go, a także w celu promowania i wzmacniania współpracy granicznej i koordynacji regionalnej i subregionalnej. Zauważono, że cele planu działania uzgodnione przez partnerów z Bałkanów Zachodnich są spójne z wysiłkami w ramach Unii i ONZ w zakresie zwalczania nielegalnego gromadzenia BSiL i amunicji do tych rodzajów

broni oraz handlu nimi. Dlatego też Unia, jak stwierdzono w motywach powinna zatem wspierać Bałkany Zachodnie w realizacji planu działania.

W treści decyzji nakreślono program działania zwalczania nielegalnego handlu bronią palną oraz bronią strzelecką i lekką, stwierdzając, że do 2023 r. powinny zostać wprowadzone przepisy dotyczące kontroli broni w pełni zharmonizowane z ramami regulacyjnymi UE i innymi powiązanymi zobowiązaniami międzynarodowymi, ustandaryzowane w całym regionie. Natomiast do 2024 r. należy zapewnić, aby polityki i praktyki w zakresie kontroli broni na Bałkanach Zachodnich były oparte na dowodach i danych wywiadowczych. Do tegoż roku należy znacząco ograniczyć nielegalny przepływ broni palnej, amunicji i materiałów wybuchowych, a także zmniejszyć podaż, popyt i niewłaściwe wykorzystanie broni palnej, przez zwiększenie świadomości, edukację, działania informacyjne i promocję oraz znacznie zmniejszyć szacowaną liczbę nielegalnie posiadanych sztuk broni. Podkreślono ponadto, że konieczne jest systematyczne niszczenie nadwyżek i skonfiskowanej broni strzeleckiej, lekkiej oraz amunicji. Konieczne jest przeciwdziałanie nielegalnemu handlowi broni w Republice Mołdawii, na Ukrainie i Białorusi. Wypada jednak zauważyć, że osiągnięcie tych ostatnich celów jest co najmniej wątpliwe, gdyż wymienione trzy państwa nie należą do Unii, a Białoruś nie jest także członkiem Rady Europy. Przypomnieć należy, że z państw bałkańskich członkami Unii są: Słowenia, Bułgaria, Rumunia, Chorwacja. Status kandydata przysługuje: Albanii, Czarnogórze, Macedonii Północnej i Serbii. Natomiast Bośnia i Hercegowina oraz Kosowo[24] aspirują do tego miana.

24 W decyzji używa się terminu Kosowo, podkreślając jednocześnie w przepisie, że posługiwanie się tą nazwą nie wpływa na stanowisko w sprawie statusu Kosowa, lecz jest zgodne z rezolucją Rady Bezpieczeństwa ONZ 1244/1999 oraz z opinią Międzynarodowego Trybunału Sprawiedliwości w sprawie deklaracji niepodległości Kosowa. Zob. w tym przedmiocie: K. Pawłowski, *Państwowość Kosowa. Geneza, uwarunkowania, współczesność*, Lublin 2018, s. 388–412, 646 i n.; M. Ickiewicz-Sawicka, *Serbsko-albański konflikt o Kosowo. Studium Kryminologiczne*, Białystok 2019, s. 213 i n.; K. Grabowska, *Piętno casusu Kosowa*, „Świat Idei i Polityki" 2016, nr 15, s. 396–417; A. Potyrała, *Unia Europejska wobec nowych tworów państwowych (Casus Kosowa, Abchazji i Osetii Południowej)*, „Środkowoeuropejskie Studia Polityczne" 2010, nr 1, s. 17 i n.; P. Szeląg, *Od interwencji Sojuszu Północnoatlantyckiego do orzeczenia Międzynarodowego Trybunału Sprawiedliwości – aktywność Organizacji Narodów Zjednoczonych w celu rozwiązania konfliktu w Kosowie* [w:] P. Czubik, *Problemy współczesnego prawa międzynarodowego, europejskiego i porównawczego*, Kraków 2012, t. 10, s. 217; *Opinia doradcza MTS w sprawie deklaracji niepodległości Kosowa*, „Biuletyn Polskiego Instytutu Spraw Międzynarodowych", http://pm.ukw.edu.pl/opinia-doradcza-mts-w-sprawie-deklaracji-niepodleglosci-kosowa/ odczyt 01.03.2020 r., 16:01; A. Brzezińska, *Polityka Unii Europejskiej wobec Kosowa jako przedmiot debaty przedwyborczej w Serbii*, „Analizy Natolińskie" 2008, nr 5, s. 1–10. Por. Wspólne Działanie Rady 2008/124/WPZiB z dnia

Chcąc osiągnąć zamierzone cele Unia deklaruje w decyzji wspieranie, koordynowanie i monitorowanie realizacji planu działania na rzecz trwałego rozwiązania kwestii nielegalnego posiadania broni strzeleckiej, lekkiej i broni palnej oraz amunicji do nich, a także nielegalnego handlu taką bronią i amunicją na Bałkanach Zachodnich. Ma także zamiar wspierać władze na Bałkanach Zachodnich w pełnej harmonizacji ich prawodawstwa dotyczącego broni z unijnymi ramami regulacyjnymi i innymi powiązanymi zobowiązaniami międzynarodowymi. Gotowa jest – jak stwierdzono w decyzji – zapewnić wsparcie w zakresie przeciwdziałania nielegalnemu handlowi bronią na Bałkanach Zachodnich, a także, co wydaje się pozostawać w niejakiej sprzeczności z celami decyzji w Mołdawii, Ukrainie i Rumunii poprzez pomoc techniczną dla organów ścigania i straży technicznej.

W decyzji wskazano, że bezpośrednimi beneficjentami projektu będą Albania, Bośnia i Hercegowina, Kosowo, Czarnogóra, Serbia i była jugosłowiańska Republika Macedonii. W ramach projektu zamierza się jednak dążyć do utrzymania wsparcia dla Mołdawii, Ukrainy i Białorusi.

Zwrócić na koniec wypada uwagę na sprawozdania roczne dotyczące realizacji wspólnego działania Rady 2002/589/WPZiB z dnia 12 lipca 2002 r. w sprawie wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania BSiL[25]. W szóstym z tych sprawozdań[26] zanalizowano krajowe działania wykonawcze państw unijnych, w tym także Polski, przy czym rozważania dotyczące Polski są niezwykle wnikliwe i szczegółowe. Przedstawiono w nich zarówno podstawy prawne, jak i administracyjne, a także kwestie dotyczące egzekwowania prawa, również w aspekcie nielegalnego obrotu i przemytu. Odnotowano, że polskie Ministerstwo Gospodarki zorganizowało, współfinansowało i uczestniczyło w spotkaniach dwustronnych i międzynarodowych, w czasie których przedstawiano zasady polskiego systemu kontroli wywozu broni oraz doświadczenia związane z tym systemem. W 2006 roku zorganizowano rozmaite dwustronne seminaria i konsultacje dotyczące powyższych tematów, w tym z: Ukrainą w styczniu i sierpniu; Chorwacją w marcu i listopadzie; Słowacją w kwietniu; Bułgarią, Serbią i Czarnogórą w maju; Bośnią i Hercegowiną w czerwcu; Węgrami we wrześniu i Niemcami

4 lutego 2008 r. w sprawie misji Unii Europejskiej w zakresie praworządności w Kosowie EULEX KOSOWO, Dz.Urz. UE L 2008, nr 42, s. 92.

25 Czwarte sprawozdanie Dz.Urz. UE C 2005, nr 109, s. 1; piąte sprawozdanie Dz.Urz. UE C 2006, nr 171, s. 1.

26 Dz.Urz. UE C 2007, nr 299, s. 1.

w październiku. W trakcie spotkań omówiono pełen zakres spraw związanych z systemem kontroli wywozu. Strona polska przedstawiła aktualny przegląd krajowego ustawodawstwa i systemu związanego z kontrolą wywozu, omawiając również kwestie polityczne uwzględniane w procesie wydawania zezwoleń. Specjalny nacisk położono na zobowiązania powiązane z członkostwem Polski w UE (kluczowa rola Kodeksu postępowania UE) oraz porozumieniem z Wassenaar (rezolucje i postanowienia), jak również na działania ONZ w zakresie BSiL. Eksperci zaangażowani w proces wydawania zezwoleń przedstawili działanie polskiego procesu kontroli wywozu przy pomocy praktycznych przykładów współpracy między agencjami.

W siódmym sprawozdaniu zwrócono uwagę, że w dniu 23 listopada 2004 r. Rada Ministrów wydała rozporządzenie w sprawie wprowadzenia zakazu i ograniczenia obrotu towarami o znaczeniu strategicznym dla bezpieczeństwa państwa[27], w którym zdefiniowano listę państw objętych zakazem lub ograniczeniem eksportu broni, rozporządzenie to, jak zauważono w sprawozdaniu w dniu 1 sierpnia 2007 r. zostało zmienione i uaktualnione zgodnie z zobowiązaniami międzynarodowymi Polski, wynikającymi z członkostwa w ONZ i UE[28].

W ósmym sprawozdaniu ograniczono się do stwierdzenia, że Polska zmieniła ustawę z dnia 22 czerwca 2001 r.[29] o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, aby dostosować przepisy polskie do prawa Unii Europejskiej, ponadto zaś wprowadziła obowiązek znakowania plastycznych materiałów wybuchowych. Dokonała także zmian w ustawie z 21 maja 1999 r. o broni i amunicji, ale nie dotyczyły one kwestii wytwarzania broni i handlu nią[30].

Znacznie bardziej ascetyczne sprawozdanie dziewiąte ogranicza się do stwierdzenia, że „Polska nadal promowała międzyinstytucjonalną wymianę informacji, aby zapobiegać nielegalnemu handlowi"[31].

Powyższe rozważania wskazują, że Unia przywiązuje istotną wagę do kwestii gromadzenia i rozpowszechniania broni strzeleckiej i broni lekkiej oraz amunicji do tej broni, widząc w obrocie tą bronią poważny czynnik destabilizujący. Identyfikuje jednak zagrożenie jako dotyczące w pierwszym rzucie

27 Dz.U. 2004, nr 255, s. 2557.
28 Dz.Urz. UE C 2010, nr 14, s. 1.
29 Dz.U. 2001, nr 67, poz. 679.
30 Dz.Urz. UE C 2010, nr 14, s. 35.
31 Dz.Urz. UE C 2010, nr 198, s. 1.

Bałkanów Zachodnich, dostrzegając jednak niebezpieczeństwo w handlu bronią za pośrednictwem Białorusi, Mołdawii i Ukrainy. Podkreślenia wymaga fakt, że Unia nie wskazała żadnych niedociągnięć w zakresie przeciwdziałania obrotowi taką bronią po stronie polskiej.

Bibliografia

Literatura

Brzezińska A., *Polityka Unii Europejskiej wobec Kosowa jako przedmiot debaty przedwyborczej w Serbii*, „Analizy Natolińskie" 2008, nr 5.

Chlebowicz P., *Nielegalny handel bronią*, Warszawa 2015.

Gołda-Sobczak M., *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016.

Grabowska K., *Piętno casusu Kosowa*, „Świat Idei i Polityki" 2016, nr 15.

Gruszczyński K.J., *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej – cele i wyzwania*, „Studia Prawnicze i Administracyjne" 2016, nr 18.

Grzeszczak R., *Globalna rola Europy oraz Wspólna Polityka Zagraniczna i Bezpieczeństwa – od słów do rzeczywistości*, „Centrum Europejskie Natolin", Warszawa 2013.

Ickiewicz-Sawicka M., *Serbsko-albański konflikt o Kosowo. Studium Kryminologiczne*, Białystok 2019.

Jaskiernia J., *System instytucjonalny polityki bezpieczeństwa UE po Traktacie z Lizbony*, „Unia Europejska – Perspektywy Społeczno-Ekonomiczne" 2013, t. 5.

Pawłowski K., *Państwowość Kosowa. Geneza, uwarunkowania, współczesność*, Lublin 2018.

Potyrała A., *Unia Europejska wobec nowych tworów państwowych (Casus Kosowa, Abchazji i Osetii Południowej)*, „Środkowoeuropejskie Studia Polityczne" 2010, nr 1.

Szeląg P., *Od interwencji Sojuszu Północnoatlantyckiego do orzeczenia Międzynarodowego Trybunału Sprawiedliwości – aktywność Organizacji Narodów Zjednoczonych w celu rozwiązania konfliktu w Kosowie* [w:] P. Czubik, *Problemy współczesnego prawa międzynarodowego, europejskiego i porównawczego*, t. 10, Kraków 2012.

Turczyński P., *Aspiracje UE jako kreatora ładu międzynarodowego: lata 2005–2012*, Wrocław 2013.

Akty prawne

Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat Ustanawiający Wspólnotę Europejską (Dz.Urz. UE C 2007, nr 306).

Decyzja Rady z dnia 21 października 2002 r. dotycząca Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej w Europie Południowo-Wschodniej (Dz.Urz. UE L 2002, nr 289, s. 1 ze zm.).

Decyzja Rady z dnia 14 kwietnia 2003 r. dotyczącą Wspólnego Działania 2002/589/WPZiB w celu wniesienia wkładu Unii Europejskiej w zniszczenie amunicji do ręcznej broni strzeleckiej i broni lekkiej w Albanii (Dz.Urz. UE L 2003, nr 99, s. 60 ze zm.).

Decyzja Rady 2003/543/WPZiB z dnia 21 lipca 2003 r. dotyczącą wykonania Wspólnego Działania 2002/589/WPZiB w związku z wkładem Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania ręcznej broni strzeleckiej i broni lekkiej w Ameryce Łacińskiej i na Karaibach (Dz.Urz. UE L 2003, nr 185, s. 59).

Decyzja Rady 2006/1000/WPZiB z dnia 11 grudnia 2006 r. dotycząca wdrożenia Wspólnego Działania 2002/589/WPZiB w związku z wkładem Unii Europejskiej w zwalczanie destabilizującego gromadzenia i rozpowszechniania broni strzeleckiej i lekkiej w Ameryce Łacińskiej i na Karaibach (Dz.Urz. UE L 2006, nr 367, s. 77).

The issue of the destabilising activities of accumulating and trafficking small arms and light weapons and their ammunition, in the legislation of the European Union

Abstract

The issue of the destabilising activities of accumulating and trafficking small arms and light weapons (SALW) and their ammunition is becoming increasingly noticeable, even to the extent that the European Union has adopted commensurate regulations. The European Council has adopted a strategy to combat the illicit accumulation of SALW and their ammunition, as well as their trafficking. This strategy calls for promoting the adoption of a legally binding instrument on the tracing and marking of SALW and their ammunition. By adopting an internationally binding instrument on the tracing and marking of SALW and their ammunition, countries undertake to take multiple measures which will allow them to effectively mark and register such weapons and tighten cooperation in tracing their illicit trafficking.

Key words: security, threats, defence policy, weapons and ammunition trafficking, European Union

Filip Radoniewicz*

Zwalczanie cyberterroryzmu w ramach UE – wybrane aspekty karnomaterialne

Streszczenie

Celem artykułu jest przedstawienie postanowień aktów prawa unijnego dotyczących prawa karnego materialnego. Cyberterroryzm nie doczekał się odrębnej regulacji. Nie oznacza to oczywiście, że unormowanie tej problematyki nie istnieje. Jest ona po prostu rozproszona i żeby odtworzyć regulację odpowiedzialności karnej za czyny, które można zakwalifikować jako cyberterroryzm, czyli przestępstw o charakterze cyberterrorystycznym, należy sięgnąć do dwóch aktów prawa unijnego: dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW oraz dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW. Stąd niniejszy artykuł składa się z dwóch części: pierwszej dotyczącej dyrektywy 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu oraz drugiej, której przedmiotem jest dyrektywa 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne.

Słowa kluczowe: prawo karne, cyberprzestępczość, terroryzm, dyrektywa 2017/541, dyrektywa 2013/40

* Dr Filip Radoniewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Terroryzm

Termin „terroryzm" pochodzi od łacińskiego słowa *terror*, oznaczającego „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenia, zniszczenia przeciwnika[1]". W języku potocznym rozumiany jest jako „stosowanie terroru, zwłaszcza działalność niektórych ugrupowań ekstremistycznych, usiłujących za pomocą zabójstw politycznych, porwań zakładników, porwań samolotów i podobnych środków zwrócić uwagę opinii publicznej na wysuwane przez siebie hasła lub wymusić na rządach państw określone ustępstwa bądź świadczenia na swoją korzyść[2]". W piśmiennictwie dotyczącym terroryzmu znajdziemy wiele definicji tego pojęcia[3]. W tym miejscu warto przytoczyć jedną, która jest niezwykle syntetyczna, a jednocześnie bardzo przydatna dla dalszych rozważań zawartych w niniejszym opracowaniu, sformułowaną przez Mariana Flemminga. Zdefiniował on terroryzm jako „umyślne działania stanowiące naruszenie prawa karnego i zmierzające w drodze aktów przemocy lub zagrożenia takimi aktami do zastraszenia organów państwowych lub znaczących odłamów społeczeństwa oraz do wymuszenia określonego postępowania[4]"

Zgodnie z powyższym „czyn terrorystyczny" wypełnia znamiona przestępstwa pospolitego (np. zabójstwa, bezprawnego pozbawienia wolności, czyli „wzięcia zakładników" czy zakłócenia pracy sieci teleinformatycznej), czemu jednocześnie jednak towarzyszy zamiar spowodowania określonego efektu w postaci np. wywołania stanu zagrożenia w społeczeństwie czy określonej reakcji ze strony organów państwowych.

Pierwszym unijnym instrumentem prawnym, którego celem miało być przeciwdziałanie terroryzmowi, była decyzja ramowa Rady z dnia 13 czerwca 2002/475/WSiSW w sprawie zwalczania terroryzmu[5] (dalej jako decyzja ramowa 2002/475). Akt ten został zastąpiony dyrektywą Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (dalej jako dyrektywa 2017/541), bazującą na nim, zasadniczo powtarzając jego rozwiązania (dotyczy to

1 M. Szymczak (red.), *Słownik języka polskiego*, t. III, Warszawa 1995, s. 463.
2 Ibidem.
3 Zob. szerzej: I. Resztak, *Zjawisko terroryzmu*, „Prokuratura i Prawo" 2012, nr 7–8, s. 148–152.
4 M. Flemming, *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 3–4, s. 31.
5 Dz.Urz. WE 2002 L 164/3.

w zasadzie np. definicji przestępstwa terrorystycznego), jednocześnie niektóre z nich uszczegóławiając oraz dodając nowe.

Dyrektywa 2017/541 ustanawia przede wszystkim normy minimalne dotyczące definicji przestępstw i sankcji w dziedzinie przestępstw terrorystycznych[6], przestępstw dotyczących grupy terrorystycznej oraz przestępstw związanych z działalnością terrorystyczną, jak również środki ochrony i wsparcia ofiar terroryzmu i pomocy tym ofiarom. Definicja przestępstwa terrorystycznego zawarta w treści art. 3 dyrektywy 2017/541 (analogicznie jak ta sformułowana w decyzji ramowej 2002/475) ma charakter dwuelementowy: przedmiotowo-podmiotowy. By czyn zabroniony mógł zostać uznany za przestępstwo terrorystyczne musi – po pierwsze – spełniać kryterium przedmiotowe, czyli być jednym z czynów wymienionych w zamkniętym katalogu zawartym w art. 3 ust. 1 lit. a)–i)[7] lub grożeniem jego popełnienia (art. 3 ust. 1 lit. j)). Po drugie – spełniać co najmniej jedną z wymienionych w drugiej części definicji przesłanek podmiotowych w postaci celu działania sprawcy, tj. musi być popełniony w celu: 1) poważnego zastraszenia ludności, lub 2) bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia

6 W decyzji ramowej 2002/475 oraz dyrektywie 2017/541 mowa jest o „przestępstwach terrorystycznych" (ang. *terroristic offences*), natomiast w polskim kodeksie karnym z dnia 6 czerwca 1997 r. (t.j. Dz.U. z 2016 r., poz. 1137 ze zm., dalej jako k.k.) użyto pojęcia „przestępstwo o charakterze terrorystycznym".

7 Wskazano w niej następujące zachowania: a) ataki na życie ludzkie, które mogą powodować śmierć; b) ataki na integralność fizyczną osoby; c) porwania lub branie zakładników; d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze; e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego; f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i rozwój broni chemicznej, biologicznej, radiologicznej lub jądrowej; g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego; h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego; i) niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW, w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy (zob. dalsze uwagi).

lub zaniechania jakiegoś działania, lub 3) poważnej destabilizacji lub zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur danego państwa lub danej organizacji międzynarodowej[8].

Natomiast w art. 4 dyrektywy 2017/541 zobowiązano państwa członkowskie do kryminalizacji kierowania grupą terrorystyczną[9] oraz uczestnictwa w działaniach takiej grupy. Wskazano, że pod tym ostatnim pojęciem rozumieć należy również dostarczanie informacji lub zasobów materialnych oraz wszelkiego rodzaju finansowanie działań takiej grupy, ze świadomością, że takie uczestnictwo będzie stanowiło wkład w działalność przestępczą grupy terrorystycznej.

8 Wspomnianą decyzję ramową 2002/475 do polskiego porządku prawnego implementowano ustawą z dnia 16 kwietnia 2004 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2004 r. nr 93, poz. 889). Jak wspominano jej postanowienia są zbliżone do zawartych w dyrektywie, a definicja przestępstwa terrorystycznego ma podobny kształt. Polski ustawodawca nie zdecydował się na dosłowną jej transpozycję. Stworzył własną, znacznie bardziej syntetyczną (art. 115 § 20 k.k.). Położono w niej nacisk na kryterium celu działania sprawcy, wskazując w przepisie – tak jak ma to miejsce w treści art. 1 ust. 1 decyzji ramowej 2002/475 oraz art. 3 ust. 2 dyrektywy 2017/541– alternatywnie jako cel działania sprawcy: 1) poważne zastraszenie wielu osób; 2) zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; 3) wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej. Drugi element definicji z art. 115 § 20 k.k. został skonstruowany odmiennie niż w pierwowzorze z decyzji ramowej 2002/475 (a co za tym idzie – odmiennie niż w dyrektywie 2017/541). Katalog przestępstw, które w przypadku popełnienia, w którymś ze wskazanych w definicji celów, są uznawane za mające charakter terrorystyczny został zastąpiony kryterium formalnym – wymogiem, aby czyn zabroniony zagrożony był karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat. Przepis ten nie tworzy zatem *delictum sui generis* lecz powoduje, iż przestępstwem o charakterze terrorystycznym będzie każde przestępstwo (każda zbrodnia i poważniejszy występek zagrożony karą pozbawienia wolności, której górna granica przekracza 5 lat) popełnione w którymś ze wskazanych w pierwszej części definicji celu. Stosownie do postanowień decyzji ramowej 2002/475, przestępstwem terrorystycznym jest również groźba popełnienia takiego czynu (art. 115 § 20 *in fine*) [w:] J. Giezek (red.), *Kodeks karny. Część ogólna*, Warszawa 2012, s. 738. Zob. szerzej: F. Radoniewicz, *Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego*, „Przegląd Prawa Konstytucyjnego" 2015, nr 3, s. 192–196.

9 Stosownie do definicji zawartej w art. 2 pkt 3) dyrektywy 2017/541 pod pojęciem tym należy rozumieć „grupę zorganizowaną złożoną z więcej niż dwóch osób, ustanowioną na pewien czas i działającą w uzgodniony sposób w celu popełniania przestępstw terrorystycznych". Natomiast „grupą zorganizowaną" – zgodnie z definicją zawartą w dalszej części cytowanego przepisu – jest grupa, która „nie jest przypadkowo sformowana w celu natychmiastowego popełnienia przestępstwa oraz w której nie ma potrzeby formalnego określenia ról członków grupy, ciągłości członkostwa lub rozwiniętej struktury".

W kolejnych artykułach dyrektywy 2017/541 nałożono na państwa członkowskie obowiązek kryminalizacji „przestępstw związanych z działalnością terrorystyczną", polegających na pewnych czynnościach, które nie stanowią same w sobie aktów terroru, ale mogą stanowić czynności przygotowawcze do ich popełnienia[10].

W świetle art. 15 ust. 1 dyrektywy 2017/541 przestępstwa, o których w niej mowa powinny podlegać skutecznym, proporcjonalnym i odstraszającym sankcjom karnym, które mogą pociągać za sobą wydanie lub ekstradycję.

Przestępstwa terrorystyczne, o których mowa w art. 3 dyrektywy 2017/541, oraz przestępstwa, o których mowa w jej art. 14 (podżeganie i pomocnictwo do przestępstw wskazanych w dyrektywie oraz ich usiłowanie)[11], powinny podlegać karom pozbawienia wolności w wymiarze wyższym niż orzekane na mocy prawa krajowego za takie przestępstwa, gdy nie przyświeca im „cel terrorystyczny" (art. 15 ust. 2).

Czyny wymienione w art. 4 dyrektywy 2017/541 powinny być zagrożone karą pozbawienia wolności w wymiarze maksymalnym nie niższym niż 15 lat w przypadku przestępstwa, o którym mowa w art. 4 lit. a), oraz w wymiarze maksymalnym nie mniejszym niż osiem lat w przypadku przestępstw wymienionych w art. 4 lit. b) (art. 15 ust. 3).

Natomiast w przypadku, gdy przestępstwo, o którym mowa w art. 6 lub 7 dyrektywy 2017/541, dotyczy dziecka, okoliczność ta powinna, zgodnie z prawem krajowym, być uwzględniana przy osądzaniu sprawców (art. 15 ust. 4).

10 Są to następujące przestępstwa: publiczne nawoływanie do popełnienia przestępstwa terrorystycznego (art. 5), werbowanie na rzecz terroryzmu (art. 6), prowadzenie szkolenia na potrzeby terroryzmu (art. 7), odbywanie szkolenia na potrzeby terroryzmu (art. 8), podróżowanie w celach terrorystycznych (art. 9), organizowanie lub ułatwianie w inny sposób podróżowania w celach terrorystycznych (art. 10), finansowanie terroryzmu (art. 11), a także „inne przestępstwa związane z działalnością terrorystyczną", wymienione w art. 12: a) kradzież kwalifikowana dokonana w celu popełnienia jednego z przestępstw wymienionych w art. 3; b) wymuszenie dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 3; c) sporządzanie lub korzystanie z fałszywych dokumentów urzędowych dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 3 ust. 1 lit. a)–i), w art. 4 lit. b) oraz w art. 9.

11 Za przestępstwo powinno zostać uznane pomocnictwo do popełnienia jednego z przestępstw, o których mowa w art. 3–8, 11 i 12 (art. 14 ust. 1), podżeganie do popełnienia jednego z przestępstw, o których mowa w art. 3–12 (art. 14 ust. 2) oraz usiłowanie popełnienia jednego z przestępstw, o których mowa w art. 3, 6, 7, art. 9 ust. 1 i art. 9 ust. 2 lit. a) oraz art. 11 i 12, z wyjątkiem posiadania, o którym mowa w art. 3 ust. 1 lit. f), oraz przestępstwa, o którym mowa w art. 3 ust. 1 lit. j) (art. 14 ust. 3).

Cyberterroryzm, czyli terroryzm w cyberprzestrzeni

Pojęcie cyberprzestrzeni (ang. *cyberspace*, słowo powstałe z połączenia dwóch angielskich słów: *cybernetics* i *space*, oznacza przestrzeń cybernetyczną) pojawiło się w latach 80. Za jego autora uważa się kanadyjskiego pisarza Williama Gibsona, który go użył w wydanej w 1984 r. powieści *Neuromancer* na określenie rzeczywistości wirtualnych, generowanych przez komputer, w których znajdowali się jego bohaterowie. Termin ten przeniknął do kultury masowej i obecnie określa się nim przede wszystkim wirtualną przestrzeń, czyli przestrzeń komunikacji za pomocą sieci komputerowych[12]. Często używa się tego pojęcia jako synonimu internetu[13].

Definicji cyberterroryzmu, podobnie jak terroryzmu, znajdziemy w literaturze znaczną ilość[14]. Z uwagi na ograniczoną objętość niniejszego opracowania, ograniczę się – analogicznie jak w przypadku terroryzmu – do przytoczenia dwóch (poniekąd skrajnych) jednej, niezwykle zwięzłej, a w związku z tym ogólnej i syntetycznej, sformułowanej przez Susan Brenner, która przyjęła, że cyberterroryzm jest to terroryzm planowany, dokonywany i koordynowany za pomocą komputerów i sieci komputerowych[15].

Druga, najczęściej zresztą przytaczana, definicja cyberterroryzmu, sformułowana przez D. Denning, jest znacznie węższa. Zdaniem tej autorki

12 W polskim prawie definicję cyberprzestrzeni znajdziemy m.in. w art. 2 ust.1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2016 r., poz. 886 ze zm.), art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz.U. z 2014 r., poz. 333 ze zm.) oraz art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2016 r., poz. 851 ze zm.), zgodnie z którymi należy przez to pojęcie rozumieć „przestrzeń przetwarzania i wymiany informacji tworzoną 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 2014 r., poz. 1114), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Zob. szerzej: J. Kosiński, *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 462–463.

13 Por. K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 62–63; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 10–11.

14 Zob. szerzej: M.F. Gawrycki [w:] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 63–73.

15 S.W. Brenner [w:] *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012, s. 16. Por. M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 111–112.

cyberterroryzm jest połączeniem terroryzmu i cyberprzestrzeni. Generalnie rozumie się, że oznacza on bezprawne ataki i groźby ataku komputerów, sieci i informacji tam zgromadzonych w celu zastraszenia lub zmuszenia rządu lub jego mieszkańców do realizacji celów politycznych lub społecznych. Ponadto w celu zakwalifikowania jako cyberterroryzm, atak powinien skutkować przemocą wobec osób lub majątku lub przynajmniej spowodować wystarczającą szkodę, aby wywołać strach. Przykładami mogą być ataki, które prowadzą do śmierci lub uszkodzenia ciała, eksplozji, katastrof samolotów, zanieczyszczenia wody lub dotkliwych strat gospodarczych. Poważne ataki na infrastrukturę krytyczną mogą być atakami cyberterrorystycznymi w zależności od ich skutków. Do takich nie można zaliczyć ataków, które zakłócają nieistotne usługi lub powodują głównie kłopoty finansowe[16]".

Pierwszym wiążącym unijnym aktem prawnym dotyczącym zamachów na bezpieczeństwo w cyberprzestrzeni była decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[17] (dalej jako decyzja ramowa 2005/222). Prace nad nią rozpoczęły się już w 2001 r. w następstwie ogłoszenia przez Komisję Europejską w 2001 r. tzw. komunikatu o cyberprzestępczości[18], zawierającego pewne propozycje przepisów materialnych i proceduralnych, mających służyć zwalczaniu przestępstw komputerowych, zarówno na poziomie krajowym, jak i wspólnotowym. Efektem podjętych wówczas działań był m.in. projekt wskazanej wyżej decyzji ramowej[19].

W preambule decyzji ramowej 2005/222 wskazano, że jej celem jest usprawnienie współpracy między organami sądowymi i organami ścigania państw członkowskich poprzez zbliżanie przepisów prawa karnego w tych państwach w dziedzinie ataków na systemy informatyczne. Podjęcie działań legislacyjnych na poziomie unijnym uzasadniano koniecznością przeciwdziałania atakom na systemy informatyczne, z uwagi na możliwe związki między tego typu przestępstwami a działalnością zorganizowanych grup przestępczych

16 Cyt. za: D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Gliwice 2004, s. 20.
17 Dz.Urz. UE 2005 L 69/67.
18 Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2000)890 w sprawie tworzenia bezpiecznego społeczeństwa informacyjnego poprzez zwiększenie bezpieczeństwa struktur informacyjnych i zwalczanie przestępczości komputerowej z dnia 26 stycznia 2001 r.
19 Projekt decyzji ramowej Rady w sprawie ataków na systemy informatyczne (*Proposal for a Council Framework Decision on attacks against information systems*), COM (2002) 0173.

oraz atakami terrorystycznymi na systemy informatyczne stanowiące część infrastruktury państw członkowskich.

W decyzji ramowej 2005/222 przede wszystkim zdefiniowano najistotniejsze pojęcia („systemu informatycznego", „danych komputerowych", „osoby prawnej", „bezprawności"), zobowiązano państwa członkowskie do stypizowania przestępstw uzyskania bezprawnego dostępu, bezprawnej ingerencji w system informatyczny oraz bezprawnej ingerencji w dane komputerowe, odniesiono się do kwestii odpowiedzialności osób prawnych, jurysdykcji oraz wykorzystania sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu w celu wymiany informacji dotyczących ataków na systemy informatyczne.

Ograniczona liczba przestępstw określonych w decyzji ramowej 2005/222, konieczność uwzględnienia nowych zagrożeń, a także chęć dostosowania regulacji do nowych inicjatyw Unii Europejskiej w dziedzinie cyberbezpieczeństwa i uzupełnienia ich w celu stworzenia całościowej regulacji tej materii doprowadziła do decyzji o podjęciu prac nad nowym instrumentem prawnym w dziedzinie cyberprzestępczości. Ich efektem jest dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[20] (dalej jako dyrektywa 2013/40).

W preambule tego aktu podkreślono m.in., że ataki na systemy informatyczne, w szczególności ze względu na zagrożenie ze strony przestępczości zorganizowanej oraz możliwość powiązania z działaniami o charakterze terrorystycznym lub mającymi podłoże polityczne, są coraz bardziej niebezpieczne. Zwłaszcza że mogą stworzyć realne zagrożenie dla systemów informatycznych stanowiących element infrastruktury krytycznej państw członkowskich i Unii.

W treści dyrektywy 2013/40 zasadniczo powtórzono postanowienia z decyzji ramowej, jednocześnie przewidując pewne nowe rozwiązania (nowe typy czynów zabronionych – nielegalne przechwytywanie danych komputerowych oraz przestępstwa dotyczące „narzędzi hackerskich" – oraz określono dodatkowe okoliczności, których wystąpienie powinno skutkować zaostrzeniem odpowiedzialności karnej.

Dla potrzeb dyrektywy 2013/40 (a wcześniej decyzji ramowej 2005/222) przyjęto, że „systemem informatycznym" (ang. *information system*) jest urządzenie lub grupa wzajemnie połączonych lub powiązanych ze sobą urządzeń,

20 Dz.Urz. UE 2013 L 218/8.

z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania (art. 2 lit. a).

Powyższa definicja ma szeroki zakres przedmiotowy. Pod pojęciem systemu informatycznego należy bowiem rozumieć zarówno pojedyncze urządzenie przetwarzające dane (np. komputer czy smartfon), jak i sieć komputerową, zarówno małą (np. sieć LAN[21]), obejmującą kilka komputerów, jak i wielką strukturę, składającą się z połączonych ze sobą sieci (np. tzw. sieć MAN[22])[23].

W art. 2 lit. b dyrektywy 2013/40 zdefiniowano „dane komputerowe" jako „przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny".

Natomiast w świetle art. 2 lit. d) dyrektywy 2013/40 za bezprawne uważa się działanie, o którym w niej mowa, w tym dostęp, ingerencję lub przechwycenie, na które właściciel lub inny podmiot uprawniony do systemu lub jego części nie udzielił zgody, lub które nie jest dozwolone na mocy prawa krajowego.

W art. 3 dyrektywy 2013/40 nałożono na państwa członkowskie obowiązek kryminalizacji umyślnego i bezprawnego uzyskania dostępu do całości lub jakiejkolwiek części systemu informatycznego, jeżeli wiąże się to z naruszeniem przez sprawcę środków bezpieczeństwa. Przez uzyskanie dostępu do systemu informatycznego należy rozumieć zdobycie możliwości korzystania z jego zasobów (czyli przechowywanych w nim danych oraz używanie sprzętu, co w zasadzie sprowadza się również do dostępu do danych – oprogramowania nim sterującego).

Kolejnym przestępstwem określonym w dyrektywie 2013/40 jest ingerencja w system informatyczny, polegająca na umyślnym, bezprawnym i poważnym utrudnieniu lub zakłóceniu funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie,

21 Sieć LAN (ang. *local area network*) – sieć lokalna.

22 Sieć MAN (ang. *metropolitan area network*) – sieć miejska, składająca się z wielu połączonych sieci lokalnych. Sieci tego typu tworzone są przez instytucje państwowe, uczelnie (sieci akademickie), czy podmioty prywatne (np. przedsiębiorstwa).

23 Z uwagi na ograniczenia objętościowe niniejszego opracowania, szczegółowe rozważania dotyczące tej kwestii zostaną pominięte. Zob. szerzej: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 244–249.

zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi (art. 4 dyrektywy 2013/40). Chodzi zatem przede wszystkim o działania o charakterze logicznym skierowane przeciw systemom informatycznym, mające na celu utrudnienie lub uniemożliwienie działania systemu poprzez oddziaływanie na przetwarzane przez system dane komputerowe lub oprogramowanie odpowiadające za jego funkcjonowanie.

Natomiast w art. 5 dyrektywy 2013/40 zobowiązano państwa członkowskie do kryminalizacji ataków logicznych, których przedmiotem są dane komputerowe. Określono w nim przestępstwo nielegalnej ingerencji w dane, jako usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi. Taką ingerencją jest np. zarówno kasowanie danych, jak i instalacja przez sprawcę w zaatakowanym komputerze programu, umożliwiającego podjęcie przy jego użyciu dalszych działań (np. kradzieży danych) czy – poprzez włączenie zaatakowanego komputera przy jego pomocy w botnet – przeprowadzenie rozproszonego ataku odmowy usługi (dDoS – ang. *Distributed Denial of Service*).

Pierwszym „nowym" (w stosunku do decyzji ramowej 2005/222) typem czynu zabronionego jest określone w treści art. 6 dyrektywy 2013/40 przestępstwo nielegalnego przechwytywania (ang. *illegal interception*), polegające na umyślnym przechwytywaniu środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych wytwarzanych przez system informatyczny zawierający takie dane komputerowe.

W art. 7 dyrektywy 2013/40 przewidziano drugi typ przestępstwa, którego nie przewidywała decyzja ramowa 2005/222. W przepisie tym zobowiązano państwa członkowskie do kryminalizacji bezprawnego i umyślnego wytwarzania, sprzedaży, dostarczania, przywozu, posiadania, rozpowszechniania lub udostępniania w inny sposób narzędzia służącego do popełnienia wskazanych w art. 3–6 dyrektywy 2013/40 przestępstw (potocznie „narzędzia hackerskiego"), w przypadkach, w których czyn ten dokonany był w celu popełnienia któregokolwiek z określonych w dyrektywie przestępstw. Przez „narzędzie" rozumie się: 1) program komputerowy zaprojektowany lub przystosowany głównie dla celów popełniania przestępstw, o których mowa w art. 3–6; 2) hasło komputerowe, kod dostępu lub podobne dane umożliwiające dostęp do całości lub części systemu informatycznego.

W art. 9 ust. 1 dyrektywy 2013/40 wskazano, że przewidziane w niej czyny (łącznie z pomocnictwem i podżeganiem do nich oraz usiłowaniem popełnienia przestępstw z art. 4 i 5 – zob. art. 8 ust. 1 i 2) powinny być zagrożone

skutecznymi, proporcjonalnymi i odstraszającymi sankcjami o charakterze karnym. Jednocześnie jednak zastrzeżono, by czyny określone w art. 3–7 dyrektywy 2013/40 (co oznacza, że nie dotyczy to usiłowania ich popełnienia oraz pomocnictwa i podżegania do nich) podlegały karze w maksymalnym wymiarze nie mniejszym niż dwa lata pozbawienia wolności co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 9 ust. 2).

Ponadto w art. 9 dyrektywy 2013/40 przewidziano szereg okoliczności, których wystąpienie powinno skutkować zaostrzeniem odpowiedzialności karnej. Dotyczą one jednak jedynie czynów określonych w art. 4 i 5 (tj. bezprawnej ingerencji w system informatyczny oraz bezprawnej ingerencji w dane komputerowe). Pierwszą jest wykorzystanie do jego popełnienia jednego z narzędzi, o których mowa w art. 7 dyrektywy 2013/40, zaprojektowanego lub dostosowanego głównie do tego celu, i umyślne spowodowanie skutku w postaci oddziaływania na znaczną liczbę systemów informatycznych. Sprawca powinien w takim wypadku podlegać karze, której górna granica powinna wynosić co najmniej trzy lata pozbawienia wolności (art. 9 ust. 3 dyrektywy 2013/40).

W art. 9 ust. 4 dyrektywy 2013/40 – jako okoliczności obciążające, których wystąpienie skutkować powinno możliwością orzeczenia kary pozbawienia wolności w wymiarze co najmniej pięciu lat wskazano popełnienie czynu w ramach organizacji przestępczej określonej w decyzji ramowej 2008/841 z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej[24], spowodowanie znacznej szkody, popełnienie przestępstwa przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej[25].

24 Dz.Urz. UE 2008 L 300/42. Zgodnie z art. 1 pkt 1 tejże decyzji jest to zorganizowana grupa, istniejąca przez pewien czas, składająca się z więcej niż dwóch osób, działających wspólnie w celu popełnienia przestępstw, których maksymalne zagrożenie karą wynosi co najmniej cztery lata pozbawienia wolności lub aresztu lub które podlegają surowszej karze, w celu osiągnięcia, bezpośrednio lub pośrednio, korzyści finansowej lub innej korzyści materialnej. „Zorganizowaną grupą" jest grupa, która nie jest przypadkowo utworzona w celu natychmiastowego popełnienia przestępstwa, ale której członkowie nie muszą mieć formalnie określonych ról, w której nie musi istnieć ciągłość członkostwa ani rozwinięta struktura (art. 1 pkt 2 decyzji ramowej 2008/841). W dyrektywie 2013/40 przyjęto rozwiązanie analogiczne, jak wcześniej w decyzji ramowej 2005/222, uniezależniając uznanie zorganizowanej grupy za organizację przestępczą od wysokości sankcji, grożącej za przestępstwo popełnione przez osoby działające w jej ramach.

25 Zgodnie z art. 2 lit. a) dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. UE 2008 L 345/75) – pod pojęciem tym rozumie się składnik, system lub część infrastruktury zlokalizowane na terytorium państw

Natomiast jako ostatnią okoliczność zaostrzającą odpowiedzialność karną (art. 9 ust. 5) przewidziano posłużenie się przez sprawcę w celu popełnienia przestępstwa określonego w art. 4 lub 5, tożsamością osoby trzeciej (tzw. kradzież tożsamości).

Obecnie jednak powyższe zastrzeżenia należy uznać za nieaktualne. Rozważając bowiem kwestię zaostrzenia odpowiedzialności karnej w przypadku terrorystycznego charakteru czynu sprawcy, należy mieć na względzie regulację zawartą w dyrektywie 2017/541. Zgodnie bowiem z art. 3 ust. 1 lit. i) w zw. z art. 3 ust. 2 tej dyrektywy (zob. wcześniejsze uwagi), niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach, gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy. Oznacza to, że za przestępstwa terrorystyczne powinny zostać uznane czyny polegające na nielegalnej ingerencji w systemy informatyczne popełnione w celu określonym w art. 3 ust. 2 dyrektywy 2017/541, w przypadku, gdy do ich dokonania wykorzystano jedno z narzędzi, o których mowa w art. 7 dyrektywy 2013/40, zaprojektowanego lub dostosowanego głównie do tego celu, i umyślne spowodowanie skutku w postaci oddziaływania na znaczną liczbę systemów informatycznych lub spowodowano znaczną szkodę. Ponadto czyn z art. 5 powinien zostać uznany za takowy, gdy skierowany był przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej.

Bibliografia

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Flemming M., *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 3–4.

Giezek J. (red.), *Kodeks karny. Część ogólna*, Warszawa 2012.

Kosiński J., *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji.

Radoniewicz F., *Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego*, „Przegląd Prawa Konstytucyjnego" 2015, nr 3.
Resztak I., *Zjawisko terroryzmu*, „Prokuratura i Prawo" 2012, nr 7–8.
Szymczak M. (red.), *Słownik języka polskiego*, t. III, Warszawa 1995.
Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
Verton D., *Black Ice. Niewidzialna groźba cyberterroryzmu*, Gliwice 2004.
Wall D., *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013.

Combating cyberterrorism in the EU – selected substantive criminal law aspects

Abstract

The purpose of the article is to present EU law provisions on substantive criminal law. Cyber terrorism is not regulated independently. This, of course, does not mean that there is no regulation for this problem. It is scattered and to decode the regulation of criminal liability for acts that can be classified as cyberterrorism, i.e. cyber-terrorist offences, two EU legal acts should be refered: Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017. Combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and repeals Council Framework Decision 2005/222/JHA. This article therefore consists of two parts: the first on Directive 2017/541 of 15 March 2017 on the fight against terrorism and the second on Directive 2013/40/EU of 12 August 2013 on attacks against information systems.

Key words: criminal law, cybercrime, terrorism, directive 2017/541, directive 2013/40