http://dx.doi.org/10.18778/8088-164-8.08

Izabela Oleksiewicz
Politechnika Rzeszowska

POLITYKA ANTYTERRORYSTYCZNA UNII EUROPEJSKIEJ JAKO PRZYKŁAD REGIONALNEGO SYSTEMU BEZPIECZEŃSTWA

Celem niniejszego artykułu będzie przybliżenie kwestii związanych z polityką bezpieczeństwa Unii Europejskiej na przykładzie ochrony przed terroryzmem, która wymaga od poszczególnych członków społeczeństwa zrzeczenia się części osobistej wolności i swobody dla wspólnego dobra i zapewnienia sobie oraz pozostałym jednostkom bezpiecznych warunków egzystencji i umożliwienia realizacji własnych życiowych celów. Tekst będzie miał na celu określenie zależności pomiędzy bezpieczeństwem wewnętrznym UE a zakresem funkcji ochronnych, jakie bezpieczeństwo ma realizować. Ukaże również, do jakich celów powinna zmierzać współczesna polityka antyterrorystyczna na gruncie prawa unijnego. To z kolei umożliwi poznanie odpowiedzi, w jakim zakresie integracja europejska wpłynęła na poziom harmonizacji polityki antyterrorystycznej Polski, która z uwagi na swoją sytuację geopolityczną zostanie potraktowana jako szczególny przypadek państwa narażonego na różnorodne zagrożenia, w tym terrorystyczne. Jako jeden z najistotniejszych elementów polityki antyterrorystycznej RP zostanie ukazane uczestnictwo naszego państwa w sojuszach militarnych i politycznych.

PODSTAWA PRAWNA REGULACJI POLITYKI ANTYTERRORYSTYCZNEJ W UNII EUROPEJSKIEJ

Należy przypomnieć, że w przypadku państw europejskich terroryzm miał przede wszystkim charakter wewnętrzny. Spowodowało to następstwa dwojakiego rodzaju. Państwa uznawały i w dużej mierze nadal uznają, że przeciwdziałanie terroryzmowi to zagadnienie należące do ich wyłącznej kompetencji. Współpracę międzynarodową w tym zakresie postrzegają jako konieczną, ale stanowiącą jedynie uzupełnienie i poszerzenie zdolności do walki z terroryzmem[1]. Dopiero

[1] M. Madej, *Instytucjonalizacja współpracy międzynarodowej w dziedzinie zwalczania terroryzmu w Europie* [w:] *Instytucjonalizacja wielostronnej współpracy międzynarodowej w Europie*, pod red. S. Parzymiesa i R. Zięby, Warszawa 2004 s. 239.

po wejściu w życie Traktatu z Maastricht polityka antyterrorystyczna znalazła się oficjalnie w III Filarze Unii Europejskiej, czyli współpracy międzyrządowej w dziedzinie sprawiedliwości i spraw wewnętrznych. Umiejscowienie tej gałęzi polityki właśnie w omawianym filarze spowodowało, że współpraca od samego początku była często mało efektywna. Co prawda, w programie ramowej współpracy w sprawach należących do wymiaru sprawiedliwości i spraw wewnętrznych polityka antyterrorystyczna stała się przedmiotem wspólnego zainteresowania wszystkich państw członkowskich, jednak w pierwszych latach obowiązywania Traktatu Unia Europejska prowadziła politykę nastawioną na konsolidację wewnętrzną, przy pewnym zaniedbaniu stosunków z państwami trzecimi. Właśnie w obszarze III Filaru okazało się, że bez kooperacji z państwami ościennymi UE nie uda się osiągnąć założonych celów. Ponadto o fakcie tym przesądziły niewielka rola Komisji Europejskiej i marginalizacja Parlamentu Europejskiego. Przez cały ten czas istniało przekonanie, że współpraca na poziomie międzyrządowym jest wystarczająca[2]. Od momentu wejścia w życie Traktatu Amsterdamskiego i utworzenia strefy wolności, bezpieczeństwa i sprawiedliwości państwa członkowskie wzmocniły środki działań poprzez integrację instrumentów odnoszących się do kontroli na granicach zewnętrznych, azylu i migracji w ramach Wspólnoty oraz zapobieganie i zwalczanie przestępczości międzynarodowej[3].

W wyniku szybkiego rozwoju wymiaru sprawiedliwości i spraw wewnętrznych UE w latach 90. ubiegłego wieku znacznie poprawiły się strukturalne podstawy do walki z terroryzmem na poziomie UE. Luźne międzyrządowe struktury Trevi zostały w pełni włączone w strukturę Rady, z Wymiarem Sprawiedliwości i Spraw Wewnętrznych (JHA Council) na jej szczycie. Rada skupiała przedstawicieli państwowych ministerstw spraw wewnętrznych i sprawiedliwości oraz odpowiedzialnego członka Komisji Europejskiej. Dzieli ona środki zwalczania terroryzmu z wymiarem sprawiedliwości i spraw wewnętrznych. Aspekty związane z WPZiB pozostawia się Radzie do Spraw Ogólnych, która skupia wokół siebie ministrów spraw zagranicznych. Ogólna koordynacja nad procesem podejmowania decyzji przebiega poniżej szczebla ministerialnego i jest formalnie zadana Komitetowi Stałych Przedstawicieli (COREPER). Jednak w domenie wymiaru sprawiedliwości i spraw wewnętrznych COREPER zwykle odgrywa aktywną rolę tylko wtedy, gdy występują trudności w osiągnięciu porozumienia w wyspecjalizowanych komisjach Rady, lub jeśli pojawiają się zagadnienia przekrojowe, takie jak koordynacja między filarami bądź wykorzystanie środków z budżetu WE. W praktyce istotną rolę w przygotowaniu decy-

[2] M. Vink, *Limits of European Citizenship: European Integration and Domestic Immigration Policies*, Constitutionalism Web-Papers, ConWEB No. 4/2003, s. 13–14.

[3] Art. 2 Traktatu o Unii Europejskiej (O.J.C. 340, 27.11.1997).

zji ministerialnych na temat walki z terroryzmem odgrywał art. 36 TUE, stanowiący podstawę prawną dla funkcjonowania dobrze zakorzenionego już od TUE Komitetu Koordynacyjnego, którego polem działania jest koordynacja zadań państw członkowskich w ramach dawnego III Filaru. Tym samym pomaga on w realizacji zobowiązania wyrażonego w art. 34 ust. 1 TUE[4]. Komitet ma możliwość wpływania na kierunki rozwoju i pomaga w przygotowaniu prac Rady, gdy ma się ona zająć współpracą policyjną i sądową w sprawach karnych[5]. Komitet (CATS) skupia wyższych urzędników państwowych i komisje zajmujące się współpracą sądową i policyjną. Wydaje również instrukcje Radzie Grupy Roboczej ds. Terroryzmu (WPT), która skupia państwowych i europejskich urzędników Komisji zajmujących się zwalczaniem terroryzmu w kontekście III Filaru. Podczas gdy WPT jest odpowiedzialna za opracowanie szczegółów walki z terroryzmem, kwestie bardziej szczegółowe, odnoszące się do współpracy policyjnej oraz sądowej, zostały omówione i uzgodnione w innych wyspecjalizowanych grupach roboczych Rady[6].

Traktat z Lizbony dokonał rozdziału zadań między UE i państwa w sposób o wiele bardziej precyzyjny w porównaniu do dawnych przepisów. Już w art. 4 TUE stwierdza się, że Unia szanuje podstawowe funkcje państw. Koreluje to częściowo z postanowieniami art. 67 TFUE. Tradycyjnie zastrzeżono, że w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego, chociaż mogą one organizować między sobą i na swoją odpowiedzialność uznane przez niezastosowane formy współpracy i koordynacji między właściwymi służbami ich administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego (art. 73 TFUE)[7].

Należy zwrócić uwagę na fakt, że w przypadku podziału kompetencji między Unią i państwami członkowskimi istotną rolę odgrywają te przepisy, w których dodano wyraźnie, że:

- Środki przyjmowane przez Parlament Europejski i Radę w celu promowania i wspierania działania państw członkowskich w dziedzinie zapobiegania przestępczości nie mogą dotyczyć jakiejkolwiek harmonizacji przepisów ustawowych i wykonawczych państw członkowskich (art. 84 TFUE);

[4] W dziedzinach objętych niniejszym tytułem państwa członkowskie wzajemnie się informują i konsultują ze sobą w ramach Rady, mając na względzie koordynację swoich działań. W tym celu ustanawiają współpracę między właściwymi jednostkami administracyjnymi. I. Oleksiewicz, *Polityka antyterrorystyczna Unii Europejskiej*, Lublin 2013, s. 194.

[5] K. Lankosz, *Traktat o Unii Europejskiej – komentarz*, Warszawa 2003, s. 443.

[6] Ibidem, s. 445.

[7] Por.: *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*, red. J. Barcz, Warszawa 2008, s. 270–276.

- Utrzymano proponowane w Traktacie Konstytucyjnym tzw. hamulce bezpieczeństwa;
- Stosowanie środków przymusu w przypadku działań operacyjnych prowadzonych przez Europol[8] wspólnie z organami państw członkowskich zastrzeżono do wyłącznej kompetencji organów państwowych (art. 88 ust. 3 TFUE).

Polityka antyterrorystyczna, zgodnie z obecnym art. 75 Traktatu o Unii Europejskiej i o Funkcjonowaniu Unii Europejskiej, oparta jest na zasadzie współdecydowania. Podstawą prawną procedury współdecydowania (kodecyzji) jest art. 294 TL. Organami współdecydującymi o przyjęciu lub odrzuceniu aktu prawnego są Rada i Parlament Europejski, natomiast inicjatywa ustawodawcza należy do Komisji[9]. Głównym założeniem tej zasady jest uniknięcie podejmowania decyzji[10] bez uzgodnienia wspólnego stanowiska pomiędzy tymi dwoma ciałami i Komisją Europejską[11]. Takie rozwiązanie okazało się sukcesem w przypadku rozbieżnych często stanowisk poszczególnych grup interesów pojawiających się na poszczególnych etapach procesu legislacyjnego[12].

REALIZACJA POLITYKI ANTYTERRORYSTYCZNEJ I ANTYCYBERTERRORYSTYCZNEJ W UNII EUROPEJSKIEJ

Odpowiedzialność za terroryzm oraz legislację spoczywa na państwach członkowskich, ponieważ są to sprawy, które stanowią przedmiot wspólnego zainteresowania. Państwa członkowskie nieustannie deklarowały, że powinna zostać stworzona wspólna polityka i prawo unijne w tym zakresie. Jednak kroki w tym kierunku zostały przedsięwzięte dopiero od Traktatu Amsterdamskiego. W okresie przed Traktatem z Maastricht udało się ustanowić międzyrządową współpracę na pewnych szczeblach. Oczywiście najważniejszym międzyrządowym porozumieniem było porozumienie z Schengen, które wprowadziło

[8] W 1999 r., kiedy niewyłączne prawo inicjatywy Komisji Europejskiej zostało rozciągnięte na wszystkie obszary sprawiedliwości i spraw wewnętrznych, Komisja Europejska powołała Dyrekcję Generalną do spraw Sprawiedliwości i Spraw Wewnętrznych. Początkowo rola Komisji była ograniczona zarówno ze względu na brak personelu, jak i stosunkowo ostrożną strategię polityczną w tej dziedzinie. Przewodniczący Komisji Romano Prodi przyjął bardziej aktywną rolę w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych niż jego poprzednik, wraz z komisarzem Antonio Vitorino wybierając ambitny porządek obrad oraz szerokie wykorzystanie prawa inicjatywy Komisji, choć brak jej niewyłącznego charakteru i wymogu jednomyślności w dalszym ciągu ograniczały wagę polityczną Komisji w procesie podejmowania decyzji. I. Oleksiewicz, op. cit., s. 256.

[9] Zob.: K. Lankosz, op. cit., s. 63–75.

[10] „Decyzji" nie należy tu rozumieć zbyt formalnie, tj. w takim znaczeniu, w jakim pojęcie to występuje w art. 249 TWE. Wydaje się, że tak określona kompetencja stanowi ogólną podstawę wykonywania przez nie kompetencji prawodawczej. Ibidem, s. 85.

[11] Zob.: J. Galster, Z. Witkowski, *Kompendium wiedzy o Unii Europejskiej*, Toruń 1997, s. 72.

[12] P. Craig, G. de Búrca, *EU Law. Text, Cases and Materials*, Oxford 2003, s. 146–147.

wspólne środki kontroli granicznej. Z momentem wejścia w życie Traktatu z Maastricht sprawy antyterrorystyczne stały się częścią regulacji traktatowych. Były to jednak sprawy umieszczone w III Filarze, co oznaczało, że instytucje wspólnotowe ciągle nie miały nad nimi kontroli.

W tym miejscu należy podkreślić i zgodzić się ze stanowiskiem M. Grajny[13], że duża liczba niepotrzebnych dokumentów powstała w wyniku instytucjonalnego wyścigu między Radą UE a Komisją, ponieważ oba te organy chciały zaprezentować swoje zaangażowanie w politykę antyterrorystyczną. Ponadto, zarówno międzyrządowy charakter III Filaru, jak i brak zaufania między państwami członkowskimi osłabiały działania antyterrorystyczne. Walka z terroryzmem była usytuowana w III Filarze do momentu wejścia w życie Traktatu Lizbońskiego, czyli opierała się na zasadzie jednomyślnej współpracy państw, co również oznaczało, że brak współpracy między działaniami podejmowanymi w ramach różnych filarów był poważnym podważaniem polityki antyterrorystycznej i stanowił przeszkodę jej realizacji jako całości. Poza tym wykluczenie Parlamentu Europejskiego i Trybunału Sprawiedliwości[14] oraz brak przejrzystości w procesie podejmowania decyzji zdecydowanie utrudniały skuteczną współpracę między państwami członkowskimi. Dopiero wprowadzenie nowego systemu podejmowania decyzji w Radzie od 1 listopada 2014 r. na zasadzie większości kwalifikowanej daje odejście, niemal całkowite, od jednomyślnego podejmowania decyzji w ramach współpracy policyjnej i współpracy sądowej w sprawach karnych, natomiast w ramach polityki zagranicznej z udziałem Unii wymagana będzie jednomyślna zgoda. Potrzeba jednak nadal co najmniej dziewięciu państw członkowskich do ustanowienia wzmocnionej współpracy na podstawie danego projektu dyrektywy (art. 329 TFUE). Konsekwencją przejścia do podejmowania decyzji w Radzie kwalifikowaną większością głosów jest to, że w sprawach współpracy sądowej, w sprawach karnych i współpracy policyjnej wprowadzone zostały szczególne „wentyle bezpieczeństwa", które po-

[13] M. Grajny, *The European Union Counterterrorism Policy before and after the 9/11 Attacks: To Extend What Does EU Have an Integrated Policy Towards Terrorism*, Kraków 2008, s. 20.

[14] Na podstawie art. 19 TFUE należy stwierdzić, że Trybunał Sprawiedliwości Unii Europejskiej jest właściwy w PWBiS w następujących sprawach: 1) w zakresie skarg wniesionych przez państwa członkowskie, instytucje lub osoby fizyczne lub prawne; 2) w trybie prejudycjalnym, na wniosek sądów państw członkowskich, w sprawie wykładni prawa Unii lub ważności aktów przyjętych przez instytucje; 3) w innych sprawach przewidzianych w traktatach. Oznacza to ogromny postęp w stosunku do obecnych rozwiązań, w których istnieją liczne ograniczenia w zakresie procedury prejudycjalnej. Trybunał nie będzie właściwy w zakresie kontroli ważności lub proporcjonalności działań policji lub innych organów ścigania w państwie członkowskim, ani do orzekania w sprawie wykonania przez państwa członkowskie obowiązków dotyczących utrzymania porządku publicznego i ochrony bezpieczeństwa wewnętrznego. Warto jednak zwrócić uwagę, że nastąpiło odejście od jednego ograniczenia istniejącego do tej pory w art. 68 ust. 2 TWE. Tymczasem ograniczenie przewidziane w TFUE będzie miało zastosowanie wyłącznie do spraw należących do współpracy sądowej w sprawach karnych i współpracy policyjnej. I. Oleksiewicz, op. cit., s. 268–269.

legają na możliwości przeniesienia dyskusji, we wskazanych w Traktacie sytuacjach, z poziomu Rady na poziom Rady Europejskiej.

Na poziomie Unii Europejskiej jakościowa zmiana w zakresie tworzenia narzędzi do przeciwdziałania cyberprzestępczości nastąpiła w 2007 r. po wejściu w życie Traktatu z Lizbony[15], na mocy którego prawo karne stało się osobną, choć specyficzną polityką współpracy[16]. Otwarta została droga do harmonizacji ustawodawstwa w zakresie materialnego i procesowego prawa karnego. Artykuł 83 ust. 1 TFUE ustanowił zasadę, że w ramach prawa unijnego mogą być ustanawiane normy minimalne odnoszące się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym. Jednocześnie wyraźnie wskazano, że chodzi tu także o przestępczość komputerową.

Przykładem unijnej regulacji dotyczącej problemu cyberprzestępczości jest Dyrektywa nr 2013/40/UE[17] z dnia 12 sierpnia 2013 r. Zastąpiła ona dotyczącą tej problematyki wcześniejszą decyzję ramową Rady 2005/222/WSiSW[18] z dnia 24 lutego 2005 r. i stanowi jej rozwinięcie oraz uszczegółowienie. Celem dyrektywy jest usprawnienie współpracy właściwych organów państw członkowskich w dziedzinie ataków na systemy informatyczne oraz ustanowienie minimalnych norm dotyczących określania przestępstw i kar w dziedzinie ataków na systemy informatyczne.

W ustawodawstwie Unii Europejskiej odnaleźć można również regulacje odnoszące się do kryminalizacji działań mających na celu rozpowszechnianie informacji zakazanych przez prawo, także za pośrednictwem sieci komputerowych. Dyrektywa nr 2011/93/UE z 13 grudnia 2011 r.[19] zawiera przepisy dotyczące zwalczania wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej rozpowszechnianej za pośrednictwem Internetu.

Zwalczanie różnych form terroryzmu wymaga wspólnej strategii UE, a wobec globalizacji terroryzmu, równoległej do globalizacji gospodarczej, działania na skalę państwową lub współpraca międzyrządowa państw członkowskich w ramach UE przestają wystarczać, stąd konieczne jest sprecyzowanie strategii międzynarodowej[20].

---

[15] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat Ustanawiający Wspólnotę Europejską sporządzony w Lizbonie dnia 13 grudnia 2007 r. (DzU z 2009 r., nr 203, poz. 1569).

[16] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 41.

[17] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (DzU UE L, nr 218 z dnia 14 sierpnia 2013 r.).

[18] Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (DzU UE L, nr 69, z dnia 16 marca 2005 r.).

[19] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (DzU UE L, nr 335 z dnia 17 grudnia 2011 r.).

[20] Zob. szerzej: dok. nr DT\547811PL.doc 3/2 PE 350.051.

Występują jednak co najmniej cztery czynniki, które sprawiają, że konsensus polityczny pomiędzy państwami członkowskimi jest nieco mniej jednorodny, niż wskazują na to oficjalne deklaracje. Po pierwsze, różnice w państwowych doświadczeniach z terroryzmem: percepcja zagrożeń różni się pomiędzy państwami członkowskimi, które były zaangażowane w przewlekłą walkę z terroryzmem, np. Francją, Hiszpanią, Wielką Brytanią, Włochami czy Niemcami, a innymi państwami, które doświadczyły tylko tymczasowo, a nawet prawie wcale, zagrożenia terrorystycznego. Sprawia to, że Radzie trudniej jest osiągnąć wspólne priorytety i programy działania.

Po drugie, różnice w możliwościach państw członkowskich dotyczą także wyspecjalizowanych struktur organizacyjnych, szkoleń i wyposażenia. Podczas gdy niektóre państwa członkowskie, takie jak Wielka Brytania, posiadają ugruntowaną, zintegrowaną strukturę antyterrorystyczną, która wykracza poza granice ministerstw (spraw wewnętrznych i obrony), oraz angażują skutecznie policję, siły zbrojne i służby wywiadowcze, to inne nie wyszły poza małe dochodzenia i jednostki operacyjne. Jest to często przyczyną frustracji osób zaangażowanych we wspólne wysiłki[21].

Po trzecie, pojawienie się nieformalnych, dwustronnych[22] i wielostronnych stosunków współpracy często wiąże się z udziałem państw spoza UE, takich jak USA. Władze wykonawcze w państwach członkowskich nadal preferują „sprawdzone" stosunki współpracy zamiast często kłopotliwych „nowych" struktur z udziałem wszystkich państw członkowskich. Dotyczy to również wymiany poufnych informacji.

Po czwarte, rozbieżne stanowiska polityczne i prawne. Nie było konfliktu np. w Hiszpanii i Belgii w latach 90. w sprawie sposobu traktowania podejrzanych terrorystów z ETA oraz przyznania im azylu na terytorium Belgii. Główne różnice pojawiły się również w odniesieniu do aktów przemocy popełnianych przez Palestyńczyków oraz w kontekście zamieszek z okazji szczytu G8 w Genui. Problemem było sklasyfikowanie niektórych aktów przemocy popełnianych przez demonstrantów jako akty terrorystyczne.

Ogólnie rzecz biorąc, można przyjąć wysoki stopień zgodności wśród państw członkowskich co do potrzeby stworzenia wspólnego frontu w walce z terroryzmem i cyberterroryzmem, ale jeśli chodzi o podejmowanie decyzji w sprawie

[21] R. Sawicki, *Z orzecznictwa Europejskiego Trybunału Sprawiedliwości. Orzeczenie Sądu I Instancji z dnia 11 lutego 2003 r. w połączonych sprawach C–187/01 i C–385/01*, „Prokuratura i Prawo" 2005, nr 2, s. 79–93.

[22] Decyzja Rady nr 2011/318/WPZiB z dnia 31 marca 2011 r. w sprawie podpisania i zawarcia Umowy ramowej między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie udziału Stanów Zjednoczonych Ameryki w operacjach zarządzania kryzysowego prowadzonych przez Unię Europejską (O.J.L. 143, 31.05.2011).

wspólnych działań, różnice nadal pozostają widoczne. Walkę z terroryzmem i cyberterroryzmem można podzielić na dwa rodzaje. Pierwszy z nich to walka doraźna – walka z terrorystami oraz organizacjami terrorystycznymi. Jest to sposób mało skuteczny, ponieważ nie można wyeliminować wszystkich terrorystów. Porównać to można do zwalczania objawów choroby bez jej usuwania przyczyn. Drugim, skuteczniejszym sposobem jest likwidowanie przyczyn różnych form terroryzmu, u podstaw którego leży zwykle niezadowolenie społeczne, połączone z przekonaniem, że terroryzm jest najlepszą, a często nawet jedyną drogą do poprawienia sytuacji. Przyczyny można likwidować poprzez poprawianie sytuacji ekonomicznej ludzi w obszarach, w których terroryzm jest największy, zaspokajanie ich innych potrzeb (wolność religijna, światopoglądowa, akceptowalny system polityczny), łącząc je z edukacją, która tworzy dojrzałe społeczeństwo, będące w stanie zmieniać swoją sytuację za pomocą innych środków niż terror, społeczeństwo niepoddające się łatwo manipulacjom prowadzącym do stosowania przemocy[23].

REALIZACJA NOWEJ POLITYKI ANTYCYBERTERRORYSTYCZNEJ W POLSCE

Zagrożenie terroryzmem ma w przypadku Polski charakter zagrożenia zewnętrznego. W naszym kraju nie występuje bowiem zagrożenie terroryzmem wewnętrznym ze strony ekstremistycznych grup narodowych czy innych mniejszości, także rozpoznane w Polsce sekty religijne nie posiadają charakteru ekstremistycznego. Niewątpliwie obecny terroryzm jest zjawiskiem i zagrożeniem czerpiącym siłę z procesów globalizacji, które marginalizują lub wykluczają wiele grup społecznych, a przez to przyczyniają się do tworzenia nowej, transgranicznej przestrzeni wykorzystywanej przez podmioty transnarodowe, które wkraczają do tradycyjnych, terytorialnych form życia społecznego i politycznego[24]. Zjawisko, które zagraża Polsce, to właśnie terroryzm międzynarodowy, przede wszystkim związany z fundamentalizmem religijnym. Z tą formą terroryzmu związane są natomiast zamachy samobójcze, ataki bombowe, branie zakładników i porwania środków transportu. Aktywne uczestnictwo Polski w walce z międzynarodowym terroryzmem sprawiło, że zaczęto rozważać możliwości przeprowadzenia ataku terrorystycznego w naszym państwie. Przesłanki decydujące o skali i randze terroryzmu wiążą się zazwyczaj ze specyficznymi

[23] Por.: Sprawa McCann i inni vs. Wielka Brytania, 27.09.1995; Sprawa Yasa vs. Turcja, 2.09.1998; Raport Europejskiej Komisji Praw Człowieka z 4.03.1994 r. Por. też: B. Bolechów, *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2002, s. 412.

[24] M. Pietraś, *Transnarodowość zagrożeń asymetrycznych* [w:] *Zagrożenia asymetryczne współczesnego świata*, red. S. Wojciechowski, R. Fiedler, Poznań 2009, s. 80.

cechami poszczególnych, regionów geopolitycznych oraz położonych w nich państw. Na znaczeniu zyskują wówczas określone cechy polityczne, ekonomiczne, społeczne, kulturowe definiujące dany obszar, a tym samym przyczyny terroryzmu[25]. Działalność grup terrorystycznych skierowana jest bowiem przeciwko „zachodniemu" stylowi życia, zasadom i porządkowi – kręgowi kulturowemu, którego Polska niewątpliwie jest częścią. Można wytypować pewne szczególne cechy terroryzmu, tj.: ideologiczne, religijne czy separatystyczno-narodowościowe, które jednocześnie można identyfikować jako jego uwarunkowania. Uwarunkowania te wynikają z zaspokajania wartości, interesów, potrzeb i celów o charakterze: politycznym, historyczno-politycznym, społeczno-ekonomicznym, społeczno-kulturowym, psychologicznym. Są one ściśle związane z rozwojem państw i narodów, ich polityką sąsiedzką[26].

Analizując zjawisko terroryzmu na poziome Polski, należy podkreślić, że nie ma jednolicie zdefiniowanego poglądu na temat zagrożeń terrorystycznych, a ryzyko ich zaistnienia określane jest w zależności od potrzeb politycznych i towarzyszących im działań. Co prawda, choć Rzeczpospolita Polska nie jest postrzegana jako cel bezpośredniego ataku terrorystycznego, to jednak istnieje realne zagrożenie i niebezpieczeństwo przeprowadzenia na jej terytorium ataku o charakterze cyberterrorystycznym[27].

Nowym rodzajem terroryzmu jest cyberterroryzm – produkt ery informatyzacji. Jego podstawową cechą jest sieciowość, co oznacza nie tylko odejście od klasycznej struktury hierarchicznej organizacji, ale przede wszystkim brak stałej lokalizacji, bezterytorialność. Działania i koordynacja elementów systemu nie są formalnie skodyfikowane przez relacje hierarchiczne, lecz wyłaniają się i zmieniają w zależności od konkretnego zadania. Kolejną z cech takich organizacji jest to, że więzy zewnętrzne i wewnętrzne nie stanowią skutku decyzji biurokratycznych, ale efekt wspólnych norm, wartości, interesów i wzajemnego zaufania[28]. Jego podłoże ma naturę religijną, stąd dla nowych cyberterrorystów liczy się już nie sam zamach, a masowość ofiar. Walczą oni o globalną wspólnotę wiernych, chcą zburzyć dotychczasowy porządek świata[29].

W dniu 9 marca 2009 r. Rada Ministrów przyjęła *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009–2011*[30]. Dokument zakłada, że „z uwagi na wzrost zagrożeń ze strony sieci publicznych (…) oraz fakt rozproszonej odpowiedzial-

[25] S. Pikulski, *Prawne środki zwalczania terroryzmu*, Olsztyn 2000, s. 30 i nast.

[26] Szerzej: S.P. Huntington, *Zderzenie cywilizacji,* Warszawa 2001, s. 180–182.

[27] J. Cymerski, *Terroryzm a bezpieczeństwo Rzeczypospolitej*, Warszawa 2013, s. 144.

[28] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 33–34.

[29] S. Koziej, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, s. 35.

[30] Http://bip.msw.gov.pl/bip/programy/17938,Rzadowy-program-ochrony-cyberprzestrzeni-RP-na-lata-2009-201-skierowany-do-rozp.html [dostęp 25.10.2013].

ności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie zapobiegania i zwalczania cyberterroryzmu, które umożliwią szybkie i efektywne reagowanie na zagrożenia i ataki wymierzone przeciwko krytycznym systemom i sieciom teleinformatycznym", nieodzowne jest wdrożenie działań prawnych, organizacyjnych i technicznych oraz edukacyjnych środków zapobiegających i zwalczających wspomniane zagrożenia.

Zapewnienie bezpieczeństwa w cyberprzestrzeni zostało uznane za jeden z celów strategicznych w obszarze bezpieczeństwa państwa, skutkiem czego było opracowanie *Rządowego Programu Ochrony Cyberprzestrzeni*. Obecnie realizowany jest już kolejny taki program, opracowany na lata 2011–2016[31]. Stanowi on kontynuację działań zapoczątkowanych w programie ochrony cyberprzestrzeni na lata 2009–2011. Przedmiotem obecnego programu jest opracowanie propozycji działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności organów państwa do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Program ten słusznie zakłada, że bezpieczeństwo jest procesem ciągłym, a nie stanem definitywnym lub produktem końcowym. Zmieniające się nieustannie uwarunkowania wymagają ciągłej dbałości o właściwą adaptację wdrożonych rozwiązań. W programie wskazano więc działania legislacyjne, które powinny zostać podjęte w celu uregulowania wszelkich aspektów związanych z zarządzaniem i bezpieczeństwem cyberprzestrzeni RP. W pierwszej kolejności wyszczególniono konieczność zdefiniowania pojęć dotyczących cyberprzestrzeni, w tym cyberbezpieczeństwa RP, cyberprzestępczości oraz cyberterroryzmu. Częściowo propozycja ta została już zrealizowana poprzez dokonanie nowelizacji ustaw o stanach nadzwyczajnych, gdzie wprowadzone i zdefiniowane zostało pojęcie cyberprzestrzeni. Natomiast pozostałe pojęcia nadal nie posiadają legalnej definicji. Ich wprowadzenie byłoby zasadne w przepisach prawa karnego, jak też w regulacjach ustrojowych i kompetencyjnych poszczególnych organów administracji publicznej biorących udział w ochronie bezpieczeństwa państwa[32].

Warto również zaznaczyć, że 25 czerwca 2013 r. przyjęty został dokument *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*[33], opracowany w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego. Niniej-

[31] Zob.: *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*, http://bip. msw.gov.pl/bip/programy/19057,dok.html [dostęp 25.10.2013].

[32] Szerzej zob.: M. Polinceusz, M. Pomykała, *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat* [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Warszawa 2013, s. 378.

[33] Zob.: www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp 14.04.2015].

szą *Polityką* rząd RP przyjmuje, że poprzez swoich przedstawicieli bierze czynny udział w zapewnieniu bezpieczeństwa zasobów informacyjnych Państwa, jego obywateli oraz realizuje swoje konstytucyjne obowiązki. W jej ramach przyjmuje się wsparcie dla inicjatyw społecznych mających na celu realizację zadań zbieżnych z niniejszym dokumentem. Rząd RP przy wypełnianiu obowiązków konstytucyjnych realizowanych za pomocą cyberprzestrzeni konsultuje się ze zorganizowanymi grupami społeczeństwa, a w szczególności z przedstawicielami przedsiębiorców telekomunikacyjnych oraz dostawców świadczących usługi drogą elektroniczną, celem uzgodnienia akceptowalnego poziomu bezpieczeństwa realizacji przedmiotowych obowiązków[34].

Jak zapisano we wstępie, przyjmując status *Polityki* dla przedmiotowego dokumentu, należy wskazać, że w ramach obowiązującego systemu rządowych dokumentów strategicznych *Polityka* mieści się w grupie dokumentów strategicznych doprecyzowujących kierunki działań wskazanych w strategiach, programach rozwoju i innych dokumentach programowych, które nie wskazują nowych priorytetów i działań. Określają one wizję rozwoju danego sektora oraz sposoby jej realizacji, opierając się na zapisach odpowiednich dokumentów. *Polityka* nie obejmuje swoim obszarem zadaniowym niejawnych systemów teleinformatycznych[35].

Z kolei 22 stycznia 2015 r. ukazała się *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*[36]. Prezydent RP Bronisław Komorowski w przesłaniu do *Doktryny* napisał m.in.: „Celem niniejszej doktryny jest stworzenie warunków do zespolenia i strategicznego ukierunkowania tych wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Dokument przygotowany został w wyniku analiz prowadzonych z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Główne założenia doktryny zostały rozpatrzone i zaakceptowane przez Radę Bezpieczeństwa Narodowego. Doktryna cyberbezpieczeństwa wskazuje strategiczne kierunki działań dla zapewnienia pożądanego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku pu-

[34] I. Oleksiewicz, K. Stachurska-Szczesiak, *Oszustwo komputerowe a polityka bezpieczeństwa informacyjnego Polski* [w:] *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Dęblin 2015, s. 289.

[35] Ibidem, s. 290.

[36] Zob.: www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp 14.04.2015].

blicznego, siły zbrojne, sektor prywatny oraz obywateli. Dzięki temu doktryna cyberbezpieczeństwa może stanowić punkt wyjścia do dalszych prac nad rzecz wzmocnienia bezpieczeństwa Polski i Polaków w cyberprzestrzeni".

WNIOSKI

Konkludując, należy stwierdzić, że aktywność państw zachodnioeuropejskich w ramach szeroko rozumianej polityki antyterrorystycznej w latach 90. koncentrowała się na zapewnieniu możliwości efektywnej kooperacji na płaszczyźnie współpracy operacyjnej policji, służb granicznych itp. Państwa UE nie podejmowały natomiast prób stworzenia regulacji odnoszących się do terroryzmu na wzór umów zawartych w ramach ONZ, wychodząc z założenia, że normy międzynarodowe są najwłaściwsze dla działalności w tym zakresie[37]. Brak potrzeby tworzenia w tym obszarze nowych rozwiązań był podyktowany faktem przyjęcia przez Radę Europy Konwencji o zwalczaniu terroryzmu z 1977 r., a następnie porozumienia dublińskiego z 1979 r., gdyż oba te akty w sposób niezwykle szeroki definiowały pojęcie przestępstwa terrorystycznego, dając tym samym podstawę państwom członkowskim do współpracy w celu ich zwalczania. Takie podejście do współpracy w Europie wynikało głównie z percepcji samego zagrożenia terroryzmem na kontynencie. Państwa unijne doświadczały terroryzmu wewnętrznego lub międzynarodowego, ale ograniczonego do konkretnego obszaru. To z kolei doprowadziło do wykształcenia się charakterystycznej dla państw europejskich postawy wobec terroryzmu, polegającej na zdecydowanym zwalczaniu działań grup terrorystycznych aktywnych na terenie Unii, przy względnie łagodnym stanowisku w kwestiach pozaeuropejskich[38].

Ponadto współpraca państw unijnych w ramach polityki antyterrorystycznej i antycyberterrorystycznej jest w dużej mierze uwarunkowana procesem integracji europejskiej. Wzrost różnych form zagrożeń terrorystycznych jest rzeczą oczywistą dla bezpieczeństwa europejskiego wraz ze znoszeniem granic i nawiązywaniem coraz ściślejszej współpracy między państwami. Dlatego też zwalczanie terroryzmu międzynarodowego i stworzenie odpowiednich mechanizmów współpracy na szczeblu unijnym stało się dziedziną objętą procesem integracji. Współpraca międzynarodowa w walce z działalnością terrorystyczną winna też obejmować szczególne wysiłki polityczne, dyplomatyczne i ekonomiczne, aby z odwagą i determinacją rozwiązywać ewentualne sytuacje ucisku i izolacji, które mogą prowokować powstawanie programów terrorystycznych. Łatwiej jest werbować terrorystów w kontekście społecznym, w którym deptane są prawa i zbyt długo toleruje się niesprawiedliwość[39].

[37] M. Madej, op. cit., s. 88.

[38] B. Hoffman, op. cit., s. 80; M. Madej, op. cit., s. 89.

[39] Por. M. Madej, op. cit., s. 90–91.

Terroryzm stanowi poważne wyzwanie dla światowego bezpieczeństwa. W sytuacji, gdy pojęcie terroryzmu nabiera tak szerokiego znaczenia lub kiedy ta sama akcja może być podjęta przez dwie różne osoby czy dwie różne grupy w dwu różnych celach, znaczenia nabiera zakwalifikowanie tego aktu przemocy. Fakt ten oraz proces globalizacji współczesnego terroryzmu powodują, że odpowiedź na to wyzwanie również musi być globalna, a współpraca w zwalczaniu omawianego zjawiska powinna być efektywna, ścisła i skoordynowana, obejmująca jak największą liczbę państw i organizacji międzynarodowych[40]. Jedyną możliwość stwarza w tym względzie prawo państwowe, międzynarodowe i unijne. Jego przestrzeganie i egzekwowanie niewątpliwie może przyczynić się do wzmocnienia bezpieczeństwa, lecz nie wyeliminuje aktów terroryzmu, co najwyżej je ograniczy.

Uświadomienie sobie tego faktu ma istotne znaczenie dla rozpatrywania polityki poszczególnych państw i regionów w kontekście zwalczania terroryzmu. Jak wiemy z ostatnich doświadczeń, umocnienie władzy bądź jej objęcie za pomocą aktów terrorystycznych jest rzeczą stosunkowo prostą. Prowadzi to do konkluzji, że dopóki terroryzm nie dotyczy ogółu państw lub dużej grupy państw, jest niedostrzegany przez opinię publiczną. Jest to bardzo niebezpieczna sytuacja, ponieważ wskazuje na ignorancję ze strony decydentów i prowadzoną przez nich politykę reaktywną. Z faktu tego wynika również słabość międzynarodowego prawa publicznego, a tym samym brak skutecznych mechanizmów przeciwdziałania terroryzmowi ze strony społeczności międzynarodowej. Dlatego tak ważną rzeczą jest pogodzenie działań antyterrorystycznych poszczególnych państw z wykładnią prawa międzynarodowego. Prawo międzynarodowe zdołało już wypracować odpowiednie instrumenty prawne, pomocne przy przeciwdziałaniu i zwalczaniu procederu finansowania terroryzmu, uznawanego za poważne przestępstwo. Jednak skuteczna walka możliwa będzie tylko wówczas, gdy państwa wyrażą polityczną wolę jej prowadzenia i będą czynnie w niej uczestniczyć, nie tylko w granicach własnego terytorium, ale również współpracując z innymi państwami i organizacjami międzynarodowymi.

Reasumując, warto podkreślić, że w dzisiejszych czasach to właściwa i skuteczna ochrona dostępu do systemów informatycznych jest czynnikiem decydującym o bezpieczeństwie informacji. Odpowiedzialność za odpowiedni wybór i ustanowienie środków zabezpieczających spoczywa na właścicielach systemów, ich zarządcach czy też administratorach. Jak podkreśla A. Adamski[41], środkom karnym przypada w tym zakresie rola zdecydowanie pomocnicza.

[40] Sprawa Irlandia vs. Wielka Brytania, 18.01.1978; Sprawa Soering vs. Wielka Brytania, 7.07.1989; Sprawa Clauhal vs. Wielka Brytania, 15.11.1966; Sprawa Aksoy vs. Turcja 18.12.1966; Sprawa Tomasi vs. Francja, 27.08.1992

[41] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 166.

Czasem niewielka manipulacja może wywołać znaczne straty finansowe lub wręcz spowodować zagrożenie dla bezpieczeństwa osób. Dlatego też regulacje zawarte w polskich art. 268 i 268a kodeksu karnego (k.k.)[42] są niezwykle ważne i istotne w tym zakresie. Wydaje się jednak, że ujęcie przestępstwa polegającego na naruszeniu integralności komputerowego zapisu informacji w dwóch przepisach prawnych jest zbyteczne i niepotrzebnie komplikuje przejrzystość regulacji. Dodatkowo warto zauważyć, że – jak podkreśla B. Kunicka-Michalska[43] – art. 268 k.k. ujęty został przez ustawodawcę w sposób skomplikowany. Wymienione w przepisie sposoby działania godzące w dostęp do danych informatycznych bardzo często ściśle się ze sobą łączą, wzajemnie przenikają, a co więcej, mogą istotnie wpływać na poprawność procesu przetwarzania. Dlatego rozróżnienie ich na potrzeby prawidłowej kwalifikacji może powodować trudności.

Podkreślając znaczenie prawidłowego funkcjonowania systemów i sieci teleinformatycznych dla współczesnej gospodarki, zdrowia i bezpieczeństwa obywateli, w tym zagrożenie, jakie niesie za sobą cyberterroryzm, słuszne wydaje się poparcie sugestii zaproponowanej przez D. Habrat[44] o wprowadzenie do polskiego kodeksu karnego kwalifikowanego typu przestępstwa z art. 269a k.k. – naruszenia integralności systemu finansowego. Obecnie bezpieczeństwo finansowe państwa w dużym stopniu zależy od prawidłowego funkcjonowania systemów i sieci informatycznych. Zaburzenie bezpiecznego przetwarzania danych finansowych nie powoduje bezpośredniego zagrożenia życia lub zdrowia ludzi, choć może wywołać chaos, doprowadzić do paraliżu państwa i narazić zarówno je, jak i poszczególnych obywateli na ogromne straty. Z tego powodu postulowane przez D. Habrat rozszerzenie regulacji zawartej w art. 269a k.k. wydaje się słuszne i uzasadnione.

[42] Dz.U. 1997, nr 90, poz. 557 z późn. zm.

[43] B. Kunicka-Michalska [w:] *Komentarz*, t. II, red. A. Wąsek, s. 513. Por. też: P. Kardas, *Prawnokarna ochrona informacji z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, z. 1, s. 67 i nast.

[44] D. Habrat, *Ochrona informacji w kodeksie karnym na tle postanowień Konwencji o cyberprzestępczości* [w:] T. Bojarski, K. Nazar, A. Nowosad, M. Szwarczyk, *Zmiany w polskim prawie karnym po wejściu w życie kodeksu karnego z 1997 roku*, Lublin 2006, s. 79.