Bezpieczeństwo infrastruktury krytycznej

wybrane opracowania

Zeszyt nr 1

Bezpieczeństwo infrastruktury krytycznej

wybrane opracowania

Zeszyt nr 1

Spis treści

II. Wybrane opracowania

1. Czy tworzenie nowych regulacji prawnych, będących odpowiedzią na nowe rodzaje zagrożeń, może doprowadzić do ignorowania normatywnego aspektu prawa? Ochrona infrastruktury krytycznej w stanach nadzwyczajnych.

(Opracowanie: ***Mateusz Kamm***, Kancelaria J. Bójko i Wspólnicy)

„Prawo nie ma żadnego bytu dla samego siebie.
Jego istotą jest raczej samo życie ludzi,
jeśli spojrzeć na nie z pewnej określonej strony."
(Carl von Savigny)

Wprowadzanie nowych systemowych regulacji prawnych, zwłaszcza będących reakcją na nowe rodzaje pojawiających się zagrożeń zewnętrznych, każdorazowo prowokuje do przemyślenia kwestii relacji między porządkiem państwowym i porządkiem prawnym – na ile może sobie pozwolić suwerenna władza?

Instrumentem prawnym, pozwalającym na zwalczanie najpoważniejszych zagrożeń, mającym na celu przygotowanie zarówno państwa, jak i jego obywateli, na funkcjonowanie w warunkach szczególnego zagrożenia, jest instytucja stanu wyjątkowego (w polskiej Konstytucji określana mianem stanu nadzwyczajnego). Kwestią podstawową jest zadbanie o taką konstrukcję norm prawnych, która pozwoli na skuteczne zabezpieczenie przed sytuacjami kryzysowymi, a zarazem nie stanie się narzędziem ułatwiającym nadużywanie władzy. Wprowadzenie stanu wyjątkowego w pewnym stopniu prowadzi do zawieszenia dotychczasowego porządku prawnego i powoduje przekierowania go inne tory. Zawieszenie norm nie jest jednak równoznaczne z ich zniesieniem, a wytworzony w rezultacie obszar anomii nie jest pozbawiony związków z porządkiem prawnym. Odwołując się do poglądu słynnego niemieckiego teoretyka prawa, Carla Schmitta: stan wyjątkowy może zaistnieć tylko wtedy, gdy wcześniej zostanie wytworzona taka sytuacja prawna, w której reguły prawne mogą obowiązywać.

Paradoksalnie, stan wyjątkowy pozostaje więc specyficznym elementem systemu prawnego, który może być wprowadzony jedynie wówczas, gdy reguły prawne obowiązują. Można nawet zaryzykować stwierdzenie, że to właśnie w decyzji o wprowadzeniu stanu nadzwyczajnego ukazuje się fundamentalna natura prawa: oto w niedającej się do końca unormować osobliwej decyzji wprowadzającej stan nadzwyczajny, prawo nie zostaje po prostu zawieszone; prawo zostaje na nowo ugruntowane, obowiązując jedynie poprzez decyzję o jego wprowadzeniu (zgodnie z art. 228 ust. 2 Konstytucji RP, wprowadzenie stanu nadzwyczajnego następuje tylko na podstawie ustawy, w drodze rozporządzenia). Konstytucyjna lub ustawowa legalizacja stanów wyjątkowych (stanów nadzwyczajnych) jest jednak elementarnym dziedzictwem demokracji, w innym ustroju politycznym tego rodzaju formalne regulacje nie byłyby konieczne. Zgodnie z poglądem włoskiego filozofa, Giorgio Agambena, stan wyjątkowy, jako forma konieczności, jawi się jako środek „nielegalny", a jednocześnie w pełni „prawny i konstytucyjny". Stan wyjątkowy jest więc legalną formą tego, co w ustroju demokratycznym nie powinno mieć miejsca.

Należy więc zapytać, czy wobec tak nieprzejrzystej instytucji prawnej, jaką jest stan nadzwyczajny, w polskim systemie prawnym odpowiednio uregulowano kwestię ochrony najbardziej kluczowej państwowej infrastruktury: infrastruktury krytycznej. Ochrona infrastruktury krytycznej powinna być bowiem rozważana przez pryzmat stanów nadzwyczajnych.

W rządowym projekcie „Strategii rozwoju sytemu bezpieczeństwa narodowego 2012-2022" zapisano: *„Ustawa o zarządzaniu kryzysowym nie rozwiązała jednoznacznie istotnych problemów kierowania bezpieczeństwem narodowym. Przede wszystkim mało precyzyjnie wskazała zależności zachodzące między organizacją podsystemu kierowania bezpieczeństwem narodowym (który w świetle obowiązującego prawa jest elementem Systemu Obronnego Państwa), a organizacją kierowania w sytuacjach kryzysowych. W sposób wystarczający nie wskazała zadań wspólnych dla sytemu obronnego państwa i systemu zarządzania kryzysowego oraz nie ustaliła mechanizmów płynnego przechodzenia od stanu zwyczajnego do nadzwyczajnego i odwrotnie*". I być może ta niedefiniowalność istoty stanu nadzwyczajnego znalazła także tutaj swoje potwierdzenie. Przypuszczalnie, trudność odpowiedniego uregulowania relacji stanu nadzwyczajnego do kwestii ochrony infrastruktury krytycznej wynika właśnie z tego, że w stanie nadzwyczajnym prawo stanowione manifestuje się w ten sposób, że podlega legalnym ograniczeniom. Wystarczy przywołać art. 228 ust. 3 Konstytucji RP: „Zasady działania organów władzy publicznej oraz zakres, w jakim mogą zostać ograniczone wolności i prawa człowieka i obywatela w czasie poszczególnych stanów nadzwyczajnych, określa ustawa". Należy zaznaczyć, że pogłębiona refleksja nad stanem wyjątkowym (stanem nadzwyczajnym) jest ważna, gdyż jego granice są tak naprawdę widoczne jedynie w momentach poważnego kryzysu politycznego, w chwilach przełomowych dla struktury społecznej i prawnej, stanowiących poważne zagrożenie dla bezpieczeństwa publicznego. Konieczne jest jednak podejmowanie odpowiednich działań już w czasie pokoju, ze względu na specyfikę i intensywność współczesnych konfliktów zbrojnych oraz niemalże nieograniczone możliwości odziaływania nowoczesnych środków militarnych.

Kryzys ukraiński, do którego doszło po aneksji Krymu przez Rosję, w sposób jednoznaczny zaktualizował konieczność pogłębionego namysłu na tą problematyką. W Białej Księdze Bezpieczeństwa Narodowego (2013) zaakcentowano aktualność zagrożeń militarnych jako kryzysów polityczno-militarnych prowokowanych dla wywierania presji strategicznej w ramach bieżącej polityki, bez przekraczania progu wojny, które mogą również przejawiać się w formie skokowej rozbudowy potencjału militarnego w pobliżu polskich granic – czy zatem grozi nam permanentny stan wyjątkowy? Zapewne nie byłaby to korzystana sytuacja, gdyż skazywałaby instytucje państwowe na funkcjonowanie w stanie nierównowagi – permanentne trwanie pomiędzy prawem publicznym, a faktem politycznym, w niejednoznacznej i zawsze niedookreślonej sferze.

Wypracowanie prawnej definicji stanu nadzwyczajnego stało się współcześnie głównie domeną prawa konstytucyjnego, która przez to pojęcie rozumie pojawienie się w państwie sytuacji szczególnego zagrożenia, którego rozwiązanie wymaga sięgnięcia do takich środków szczególnych jak: 1) koncentracja władzy w rękach egzekutywy; 2) ograniczenia praw i wolności obywateli; 3) zmiany w strukturze i zasadach funkcjonowania organów państwowych; 4) zmiany w systemie stanowienia prawa. W Konstytucji Rzeczypospolitej Polskiej stany nadzwyczajne zostały wyodrębnione w rozdziale XI, gdzie wymieniono trzy rodzaje stanów nadzwyczajnych: stan wojenny, który może być wprowadzony w razie zewnętrznego zagrożenia państwa, zbrojnego napadu na terytorium RP lub konieczności wypełnienia obowiązków sojuszniczych (art. 229 Konstytucji RP); stan wyjątkowy, który jest wprowadzany w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego (art. 230 ust. 1 Konstytucji RP) i stan klęski żywiołowej, wprowadzany w przypadku konieczności zapobieżenia skutkom katastrof naturalnych lub awarii technicznych o dużym zasięgu (art. 232 Konstytucji RP). Wprowadzenie stanu nadzwyczajnego zależy od oceny podmiotów uprawnionych do podjęcia decyzji o jego wprowadzeniu, specyfiki zagrożenia i adekwatności środków pozostających w dyspozycji władz publicznych służących do usunięcia istniejących zagrożeń. Należy jednak zauważyć, że doktryna prawa publicznego nie wypracowała zadowalającej teorii stanu wyjątkowego, a traktowanie go wyłącznie w kategoriach stanu faktycznego nie wydaje się wystarczające.

Z kolei odpowiednie zabezpieczenie państwa na okoliczność wystąpienia stanów nadzwyczajnych związane jest z kwestią ochrony

infrastruktury krytycznej. Instrumenty ochrony infrastruktury krytycznej muszą być stosowane z uwzględnieniem współzależności jej poszczególnych elementów – ta współzależność prowadzi jednak równocześnie do zwiększonej podatności infrastruktury krytycznej na potencjalne zagrożenia, zwłaszcza te związane z cyberprzestępczością. W projekcie „Strategii rozwoju systemu bezpieczeństwa narodowego 2012 – 2022" z kwietnia 2012 r. czytamy: *„Słabą stroną infrastruktury krytycznej jest jej podatność na zagrożenia. W przeszłości elementy tworzące infrastrukturę krytyczną funkcjonowały, jako niezależne lub też zależne w niewielkim stopniu systemy. Obecnie w dobie postępującej globalizacji i rozwoju technologicznego poszczególne obiekty infrastruktury krytycznej są coraz bardziej współzależne nie tylko w wymiarze jednego państwa, ale i w skali regionalnej, europejskiej, a nawet światowej. Postęp, poza oczywistymi korzyściami, spowodował równocześnie zwiększenie ich podatności na potencjalne zagrożenia, w tym zagrożenia nowego typu związane z cyberprzestrzenią. Sieć powiązań powoduje, że uszkodzenie lub utrata części infrastruktury krytycznej w jednym systemie, generuje straty i uszkodzenia w innych."*

Ochrona infrastruktury krytycznej jest przedmiotem regulacji uchwalonej 26 kwietnia 2007 r. ustawy o zarządzaniu kryzysowym. Infrastruktura krytyczna stanowi kluczową dla funkcjonowania nowoczesnego państwa infrastrukturę, zapewniającą m.in. zaopatrzenie w energię, surowce energetyczne, paliwa, żywność, wodę i prawidłowe działanie sieci teleinformatycznych. Ze względu na jej newralgiczne znaczenie, zagadnienie ochrony infrastruktury krytycznej bezpośrednio wiąże się z polityką zarządzania kryzysowego – obie kwestie cechuje istotny związek merytoryczny. Co ważne, art. 2 ustawy o zarządzaniu kryzysowym (wprowadzający pojęcie zarządzania kryzysowego) wprost zalicza zadanie odtwarzania zasobów infrastruktury krytycznej do priorytetów zarządzania kryzysowego. Ochrona infrastruktury krytycznej i polityka zarządzania kryzysowego ustanawiają zarazem silny związek ze sferą bezpieczeństwa narodowego. Obie polityki mają na celu przygotowanie państwa na wypadek wystąpienia zagrożeń dla jego funkcjonowania – przy czym nadrzędnym celem jest zapewnienie ciągłości funkcjonowania infrastruktury w najbardziej niesprzyjających okolicznościach. Odpowiednie zabezpieczenie infrastruktury krytycznej i zapewnienie ciągłości jej funkcjonowania gwarantuje odpowiedni poziom bezpieczeństwa narodowego, przy czym to polityka zarządzania kryzysowego dostarcza efektywne procedury i praktyki reagowania w stanach zagrożeń i na wypadek wystąpienia sytuacji kryzysowych. Nie chodzi zatem o przygotowanie ad hoc, lecz o całościowe i permanentne przygotowanie państwa na sytuacje zagrożenia.

Ustawa o zarządzaniu kryzysowym obowiązuje tylko w czasie pokoju i dotyczy sytuacji, w których nie występują jeszcze przesłanki do wprowadzenia jednego ze stanów nadzwyczajnych (stanu wyjątkowego, stanu wojennego lub stanu klęski żywiołowej), a w których należy już wdrożyć mechanizmy, które pozwolą na skuteczne monitorowanie zagrożeń i umożliwią podjęcie działań prowadzących do ich eliminacji lub znacznego ograniczenia. Zarządzanie kryzysowe jest w Polsce polityką komplementarną wobec problematyki stanów nadzwyczajnych i jest zarazem ważnym elementem służącym zapewnieniu bezpieczeństwa narodowego.

Podstawowym instrumentem mającym służyć przygotowaniu organów administracji publicznej do działań w sytuacjach kryzysowych jest całokształt przedsięwzięć planistycznych (organizacyjnych), określanych jako planowanie cywilne. Zakres planowania cywilnego zdefiniowany został w art. 4 ust. 1 Ustawy o zarządzaniu kryzysowym. Podstawowym elementem planowania cywilnego na szczeblu centralnym jest Krajowy Plan Zarządzania Kryzysowego. Do dokumentów planistycznych szczebla centralnego należy również zaliczyć przyjmowany w drodze uchwały przez Radę Ministrów, Narodowy Program Ochrony Infrastruktury Krytycznej (odnosi się do niego art. 5b ustawy o zarządzaniu kryzysowym). Celem Narodowego Programu Ochrony Infrastruktury Krytycznej jest m.in. stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej w zakresie zapobiegania zakłóceniom jej funkcjonowania i skuteczne przygotowania jej na okoliczność wystąpienia sytuacji kryzysowych. Program jest przygotowywany przez dyrektora Rządowego Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych. Co zrozumiałe, zagadnienia związane z ochroną infrastruktury krytycznej, zarządzaniem kryzysowym i problematyką stanów nadzwyczajnych poruszane są w opracowaniach bezpośrednio związanych z zagadnieniem bezpieczeństwa narodowego, np.: „Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej" (Warszawa 2013); „Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczy-

pospolitej Polskiej 2022" przyjęta uchwałą nr 67 Rady Ministrów z 09.04.2013 r. oraz „Strategia bezpieczeństwa Narodowego Rzeczypospolitej Polskiej", której druga już edycja została zatwierdzona przez Prezydenta 5 listopada 2014 r.

Większość podejmowanych przez państwo działań nadzwyczajnych jest efektem czasowych kryzysów politycznych, dlatego też najczęściej rozważane są głównie na płaszczyźnie politycznej, a nie prawno-konstytucyjnej. Zarazem należą jednak do grupy paradoksalnych środków prawnych, których nie da się do końca włączyć w obszar prawa – w konsekwencji, prawny charakter instytucji stanu nadzwyczajnego pozostaje wysoce niejednoznaczny. *„Jeśli wyjątek uznamy za swoiste narzędzie, za pośrednictwem którego prawo odwołuje się do życia i – poprzez zawieszenie samego siebie włącza je w swój obręb, to teoria stanu wyjątkowego okazuje się wstępnym warunkiem niezbędnym do określenia związku łączącego jednostkę z prawem i jednocześnie wydającego ją na jego pastwę. W rezultacie, pomiędzy prawem publicznym a faktem politycznym odsłania się ziemia niczyja. Zerwanie zasłony pokrywającej ten obszar jest konieczne do zrozumienia kwestii różnicy pomiędzy tym co polityczne, a tym, co prawne, pomiędzy jednostką a prawem"* (G. Agamben, *Stan wyjątkowy*). Wprowadzanie przez ustawodawcę nowych regulacji prawnych, będących reakcją na zewnętrzne zagrożenia, rodzi ryzyko przekształcenia środków tymczasowych i nadzwyczajnych w technologię władzy; w takiej sytuacji, prawo pokrywające się z rzeczywistością staje się niewidzialne, a sama niewidzialność jest źródłem normy – stan nadzwyczajny przekształca się w próg nierozróżnialności pomiędzy demokracją i nie-demokracją. Nadaktywność ustawodawcy w sferze wprowadzania nowych regulacji prawnych odnoszących się do aktualnych zagrożeń zewnętrznych, może więc rodzić ryzyko przejścia prawa w stan permanentnej nieuchwytności, kiedy przepisy prawa stają się nieodróżnialne od aktów władzy, a norma prawna nieodróżnialna od wyjątku. Podatność na pochopne działania ustawodawcy jest tym bardziej realna z uwagi na to, że ochrona infrastruktury krytycznej integruje środki różnych państwowych polityk. W przypadku zarządzania kryzysowego, są to działania organów właściwych w sprawach zarządzania kryzysowego oraz plany zarządzania kryzysowego.

W odniesieniu do infrastruktury krytycznej podstawą integracji jest Narodowy Program Ochrony Infrastruktury Krytycznej wraz z normatywnie określonym obowiązkiem współpracy w zakresie jego realizacji (§ 7 Rozporządzenia Rady Ministrów w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej z dnia 30 kwietnia 2010 r.). Także organy właściwe w sprawach zarządzania kryzysowego realizują zadania z zakresu ochrony infrastruktury krytycznej (art. 6 ust. 1 ustawy o zarządzaniu kryzysowym). Podstawę polityczną ochrony infrastruktury krytycznej stanowi ponadto wyznaczający kierunki działania dla zarządzenia kryzysowego i istotny dla ochrony infrastruktury krytycznej Raport o zagrożeniach bezpieczeństwa narodowego (art. 5a ust. 1 ustawy o zarządzaniu kryzysowym).

Ochrona infrastruktury krytycznej jest realizowana przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe, inne organy i służby publiczne, lecz główny ciężar realizacji i odpowiedzialności spoczywa na operatorach infrastruktury krytycznej, którzy muszą stworzyć plan ochrony własnej infrastruktury krytycznej, uzgodniony z organami administracji publicznej – można to uznać za zadanie publiczne, które powierzono do wykonania operatorom infrastruktury krytycznej (art. 6 ust. 5 ustawy o zarządzaniu kryzysowym). Jednakże nawet tak rozległy zasięg regulacji polityk zarządzania kryzysowego i ochrony infrastruktury krytycznej nie daje gwarancji sprawnego funkcjonowania państwa w obliczu stanu nadzwyczajnego, który w każdym przypadku będzie rodzajem „skoku w nieznane".

Bibliografia:

1. G. Agamben, *Stan wyjątkowy*, tłum. Monika Surma-Gawłowska, Kraków 2008
2. E. Geulen, *Giorgio Agamben: wprowadzenie*, tłum. Mikołaj Ratajczak, Warszawa 2012
3. R. Radziejewski, *Ochrona infrastruktury krytycznej. Teoria a praktyka*, Warszawa 2014
4. T. Długosz, *Ochrona infrastruktury krytycznej w sektorach energetyki sieciowej*, Warszawa 2015

2. Czy przepisy TFUE pozwalają na wzmocnienie bezpieczeństwa narodowego?

(Opracowanie: *Justyna Bójko, Edyta Niemyska, Krzysztof Mielech*, Kancelaria J. Bójko i Wspólnicy / LSW Leśnodorski Ślusarek i Wspólnicy)

Celem niniejszego artykułu jest zaprezentowanie wybranych aspektów stosowania przez państwa członkowskie przepisów art. 106 ust. 2 Traktatu o Funkcjonowaniu Unii Europejskiej („TFUE") oraz art. 346 ust. 1 lit. b) TFUE, art. 347 TFUE, jako mechanizmów mających zagwarantować państwu członkowskiemu skuteczną realizację zadań z zakresu szeroko rozumianego bezpieczeństwa narodowego. Przy czym, ze względu na zwięzłą formę niniejszego artykułu, koncentruje się on na aspektach praktycznych, tj. wskazaniu zakresu zastosowania danego wyłączenia, przesłanek jego zastosowania oraz skutków dla państwa członkowskiego.

Stosowanie przepisów TFUE stanowi przejaw poszukiwania równowagi pomiędzy dążeniem do zacieśniania integracji w sferze gospodarczej i społecznej państw członkowskich, z uwzględnieniem konieczności zagwarantowania poszczególnym państwom członkowskim mechanizmów umożliwiających efektywną realizację polityki bezpieczeństwa narodowego. W szczególności takie obszary jak transport, energia, spójność gospodarcza jak również rynek wewnętrzny, zostały wymienione w art. 4 TFUE jako kompetencje dzielone pomiędzy państwem członkowskim a Unią. TFUE przewiduje szereg mechanizmów stanowiących przejaw dążenia do zagwarantowania państwom członkowskim możliwość realizacji wspomnianych wyżej interesów politycznych i gospodarczych. Przykładami wskazanych wyżej mechanizmów są m.in. przepisy:

(i) art. 106 ust. 2 TFUE – dotyczący możliwości wyłączenia stosowania przepisów prawa europejskiego do przedsiębiorców, którym powierzono świadczenie usług w ogólnym interesie gospodarczym;

(ii) art. 346 TFUE – dotyczący wyłączenia stosowania przepisów prawa europejskiego do środków, jakie państwa członkowskie podejmują w celu ochrony podstawowych interesów bezpieczeństwa, a które odnoszą się do produkcji lub handlu bronią, amunicją lub materiałami wojennymi;

(iii) art. 347 TFUE – dotyczący wyłączenia stosowania przepisów prawa europejskiego do środków podejmowanych przez państwa członkowskie w przypadku poważnych zaburzeń wewnętrznych zagrażających porządkowi publicznemu oraz poważnego napięcia międzynarodowego stanowiącego groźbę wojny;

(iv) art. 36 TFUE, art. 45 TFUE, art. 52 TFUE, art. 65 TFUE – dotyczące wyłączenia stosowania przepisów traktatowych w zakresie swobód rynku w związku z ochroną bezpieczeństwa i porządku publicznego, jak też doktryną wymogów imperatywnych sformułowaną w orzecznictwie TSUE.

I. Powierzenie świadczenia usług w ogólnym interesie gospodarczym (dalej: „UOIG")

I. 1. Definicja UOIG

Brak jest jednolitej i uniwersalnej definicji usług w ogólnym interesie gospodarczym (UOIG). Pomimo, że pojęcie usług świadczonych w ogólnym interesie gospodarczym pojawia się w art. 14 TFUE i art. 106 ust. 2 TFUE oraz w Protokole nr 26 do TFUE, nie zostało ono jednak zdefiniowane w żadnym z wyżej wskazanych aktów ani w prawie wtórnym. Praktyka decyzyjna Komisji oraz orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej („TSUE") wskazują, że pod pojęciem usług świadczonych w ogólnym interesie gospodarczym należy rozumieć sektor działalności gospodarczej, który oferuje usługi w ogólnym interesie publicznym, które nie byłyby świadczone na rynku (lub byłyby świadczone na innych warunkach, jeżeli chodzi o jakość, bezpieczeństwo, przystępność cenową, równe traktowanie czy powszechny dostęp) bez interwencji publicznej. Obowiązek świadczenia usługi publicznej nakłada się na usługodawcę

poprzez powierzenie mu świadczenia danej usługi na podstawie kryterium interesu ogólnego, co gwarantuje, że usługa zostanie wykonana na warunkach umożliwiających wypełnienie jej zadania.

TSUE w swoim orzecznictwie podkreślił, że usługi świadczone w ogólnym interesie gospodarczym są usługami posiadającymi szczególne cechy charakterystyczne w porównaniu z innymi rodzajami działalności gospodarczej.[1]Prawo UE nie nakłada żadnego obowiązku formalnego uznawania poszczególnych usług za usługi świadczone w ogólnym interesie gospodarczym; o tym, czy dana usługa ma charakter usługi w ogólnym interesie gospodarczym nie decyduje jej nazwa, lecz charakter tej usługi i opisane wyżej cechy odróżniające ją od pozostałych usług gospodarczych świadczonych na rynku.

Pomocne przy definiowaniu UOIG jest stanowisko Komisji zawarte w Komunikacie z 2000 r. „Usługi o charakterze powszechnym w Europie" (COM/2000/0580 final) DzUrz. UE 2001, C 17. Komisja we wskazanym wyżej komunikacie „Usługi o charakterze powszechnym w Europie" wyjaśniła, że UOIG różnią się od zwykłych usług tym, że muszą być świadczone, choćby rynek nie był nimi zainteresowany np. z uwagi na brak opłacalności ekonomicznej. Uznając, że niektóre usługi są dla społeczeństwa niezbędne, a siły rynkowe nie są w stanie ich satysfakcjonująco zapewnić, władze publiczne mogą zdecydować o nadaniu tym usługom charakteru UOIG. Przykładem mogą być usługi publicznego transportu kolejowego, gdzie państwo dla zapewnienia ich powszechnej dostępności, zarówno pod względem cenowym jak i siatki połączeń, rekompensuje część kosztów ponoszonych przez przedsiębiorstwa kolejowe.

I. 2. Ograniczenia w możliwości uznania usługi za UOIG

Swoboda Państw Członkowskich w zakresie uznawania danej usługi za usługę w ogólnym interesie gospodarczym może być więc ograniczona następczo, jeśli Komisja bądź TSUE negatywnie zweryfikują istnienie ogólnego interesu gospodarczego i uznają, że dane świadczenie nie mieści się w zakresie przedmiotowym art. 106 ust. 2 TFUE.[2] Ponadto, w sektorach, w których osiągnięto harmonizację na poziomie prawa europejskiego w zakresie definicji usług w ogólnym interesie gospodarczym[3], jak również w tych, w których uwzględniono cele leżące w interesie ogólnym[4], państwa członkowskie nie mogą korzystać z tej swobody definiowania usług w ogólnym interesie gospodarczym w sposób sprzeczny z zasadami dotyczącymi takiej harmonizacji.

Tym niemniej, w przypadku gdy przepisy prawa UE w sprawie harmonizacji dotyczą wyłącznie pewnych szczególnych usług, państwa członkowskie dysponują dużym zakresem swobody w określaniu usług dodatkowych jako usług świadczonych w ogólnym interesie gospodarczym.

W orzecznictwem TSUE za UOIG uznano m.in. budowę infrastruktury łączności szerokopasmowej na terytorium danego państwa członkowskiego, jeżeli na przedmiotowym obszarze występuje brak odpowiedniej infrastruktury, a inwestorzy nie mogą zagwarantować odpowiedniego zasięgu łączności szerokopasmowej.[5] W przypadku Poczty Greckiej (ELTA) dopuszczono zdefiniowanie usług świadczonych w ogólnym interesie gospodarczym jako zestawu różnych usług wraz z powszechną usługą pocztową, gdyż dzięki rekompensacie Poczta Grecka była w stanie przeprowadzić modernizację swojej infrastruktury i wykonywać

1 Sprawa C-179/90 Merci convenzionali porto di Genova, Rec. 1991, s. I-5889, pkt 27; sprawa C-242/95 GT-*Link A/S* Rec. 1997, s. I-4449, pkt 53; i sprawa C-266/96, Corsica Ferries France SA Rec. 1998, s. I-3949, pkt 45.

2 Sprawa T-17/02 Fred Olsen, Zb.Orz. 2005 s. II-2031, pkt 216; Sprawa T-289/03 BUPA i in. Przeciwko Komisji, Zb.Orz. 2008 s. II-81, pkt 165 i nast.; sprawa C-179/90 Merci convenzionali porto di Genova, Rec. 1991, s. I-5889, pkt 27; sprawa C-242/95 GT-Link Rec. 1997, s. I-4449, pkt 53; oraz sprawy połączone C-34/01 do C-38/01 Enrisorse, Rec. 2003, s. I–14243, pkt 33-34; Decyzja Komisji w sprawie pomocy państwa SA.25051 – przyznanej przez Niemcy na rzecz Zweckverband Tierkörperbeseitigung; sprawa C-126/01 Ministère de l'Économie, des Finances et de l'Industrie przeciwko GEMO SA., Rec. 2003, s. I-13769; Decyzja Komisji w sprawie pomocy państwa nr C 28/1998 przyznanej przez Włochy na rzecz Centrale del Latte di Roma, Dz.U. L 265 z 19.10.2000

3 Na poziomie UE zharmonizowano m.in. sektor telekomunikacyjny, pocztowy i energetyczny. Zob. dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej) Dz.U. L 108 z 24.4.2002, s. 51 (zmieniona dyrektywą 2009/136/WE, Dz.U. L 337 z 18.12.2009, s. 11); dyrektywa 97/67/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie wspólnych zasad rozwoju rynku wewnętrznego usług pocztowych Wspólnoty oraz poprawy jakości usług, Dz.U. L 15 z 21.1.1998, s. 14 (zmieniona dyrektywą 2002/39/WE, Dz.U. L 176 z 5.7.2002, s. 21 i dyrektywą 2008/06/WE, Dz.U. L 52 z 27.2.2008 s. 3); dyrektywa Parlamentu Europejskiego i Rady 2009/72/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego energii elektrycznej, Dz.U. L 211 z 14.8.2009, s. 55.

4 Sprawa C-206/98 Komisja przeciwko Belgii, Rec. 2000, s. I-3509, pkt 45.

5 Wytyczne wspólnotowe w sprawie stosowania przepisów dotyczących pomocy państwa w odniesieniu do szybkiego wdrażania sieci szerokopasmowych", Dz.U. C 235 z 30.9.2009, s.7.

zobowiązania wynikające z Powszechnej Konwencji Pocztowej, jak też poprawić jakość usługi publicznej w celu spełnienia wymogów ustanowionych w dyrektywie 2002/39/WE.[6] Ponadto za UOIG uznano:

- działalność portu rzecznego obsługującego najważniejszą w państwie drogę wodną;
- usługi cumowania w porcie świadczone celem zapewnienia bezpieczeństwa na wodach portowych;
- działalność w zakresie tworzenia i zarządzania sieciami telekomunikacyjnymi;
- dostawę wody;
- działalność w zakresie radia i telewizji;
- dystrybucję energii elektrycznej;
- świadczenie usług transportu pasażerskiego zbiorowego;
- prowadzenie pośrednictwa pracy;
- podstawowe usługi pocztowe;
- utrzymania sieci usług pocztowych na wsi;
- działalność nakierowaną na rozwój regionalny w ramach danego państwa członkowskiego;
- usług w zakresie gospodarki odpadami.

I. 3. Charakter prawny powierzenia UOIG w świetle art. 106 ust. 2 TFUE

Zgodnie z treścią art. 106 ust. 2 TFUE *„przedsiębiorstwa zobowiązane do zarządzania usługami świadczonymi w ogólnym interesie gospodarczym lub mające charakter monopolu skarbowego podlegają normom Traktatów, zwłaszcza regułom konkurencji, w granicach, w jakich ich stosowanie nie stanowi prawnej lub faktycznej przeszkody w wykonywaniu poszczególnych zadań im powierzonych. Rozwój handlu nie może być naruszony w sposób pozostający w sprzeczności z interesem Unii*."

Praktyka stosowania przez państwa członkowskie art. 106 ust. 2 TFUE jako podstawy wyłączenia stosowania przepisów TFUE w zakresie, w jakim stanowiłyby one przeszkodę w powierzeniu lub świadczeniu UOIG, ma długą tradycję. Przepis ten został wprowadzony do treści Traktatów Rzymskich jako forma swoistego zabezpieczenia silnej obecności państw członkowskich w szczególnie istotnych dla nich sektorach gospodarki, tj. energetyka, transport, poczta, czy telekomunikacja. Wraz z postępującą integracją gospodarczą i społeczną w ramach Unii Europejskiej, postrzeganie roli w/w przepisu uległo jednak znaczącej zmianie.

Zmiana ta dotyczy przede wszystkim przeniesienia nacisku w zakresie przesłanek stosowania art. 106 ust. 2 TFUE z zabezpieczania interesów państw członkowskich, na ochronę istotnego interesu ogólnego. Powierzenie świadczenia UOIG jest bowiem obecnie postrzegane w kontekście miejsca, jakie usługi świadczone w ogólnym interesie gospodarczym zajmują wśród wspólnych wartości Unii, jak również ich znaczenia we wspieraniu jej spójności społecznej i terytorialnej. W treści art. 14 TFUE wyraźnie wskazane jest, że „Unia i Państwa Członkowskie, każde w granicach swych kompetencji i w granicach stosowania Traktatów, zapewniają, aby te usługi funkcjonowały na podstawie zasad i na warunkach, w szczególności gospodarczych i finansowych, które pozwolą im wypełniać ich zadania."

Pomimo opisanych wyżej zmian w zakresie podejścia do art. 106 ust. 2 TFUE nadal stanowi on istotne źródło uprawnień dla państw członkowskich. Jest to bowiem jeden z nielicznych przepisów umożliwiających państwom członkowskim wprowadzenie, na poziomie prawa krajowego, regulacji niezgodnych z TFUE i aktami prawa wtórego wydanymi na jego podstawie, jeśli mają one służyć zabezpieczeniu ogólnego interesu gospodarczego istotnego dla danego państwa. Co więcej, pozostawienie państwom członkowskim daleko idącej swobody w zakresie definiowania UOIG, jak i interesu ogólnego stanowiącego podstawę jej powierzenia, skutkuje częstym powoływaniem tej regulacji przez państwa.

Poniżej przedstawiamy kilka uwag ilustrujących zagadnienia istotne z punktu widzenia praktyki stosowania art. 106 ust. 2 TFUE jako mechanizmu ochrony szeroko rozumianego bezpieczeństwa państwa.

I. 4. Powierzenie świadczenia UOIG

Pojęcie powierzenia UOIG także nie zostało zdefiniowane w treści art. 106 ust. 2 TFUE. Tym niemniej, TSUE rozwinął je w wyroku w sprawie Altmark[7], wskazując że niezbędne jest aby akt powierzenia miał formę co najmniej jednego wiążącego aktu prawnego zgodnie z przepisami prawa krajowego. Szczególna forma takiego

6 Decyzja Komisji dotycząca pomocy państwa nr SA.32562 – Grecja – pomoc na rzecz Poczty Greckiej, Dz.U. C 99 z dnia 3.4.2012

7 Sprawa C-280/00 Altmark Trans GmbH i Regierungspräsidium Magdeburg przeciwko Nahverkehrsgesellschaft Altmark GmbH, przy udziale Oberbundesanwalt beim Bundesverwaltungsgericht, Zb.Orz. s. I-7747

aktu może zostać określona przez każde państwo członkowskie w zależności od jego organizacji politycznej lub administracyjnej oraz przepisów prawa krajowego.

Akt powierzenia powinien określać charakter i czas trwania obowiązków wynikających ze świadczenia usług w ogólnym interesie gospodarczym, podmioty, którym powierzono świadczenie tych usług. Przedsiębiorcy, którym powierzono świadczenie UOIG przysługuje prawo do rekompensaty. Powyższe wynika z istoty UOIG, jako usług, które co do zasady nie są świadczone na rynkowych zasadach, są mniej opłacalne niż pozostałe usług, lub wręcz wymagają od przedsiębiorcy dodatkowych nakładów finansowych w celu ich prawidłowej i skutecznej realizacji. W Komunikacie Komisji 2012/C 8/03 w sprawie zasad ramowych Unii Europejskiej dotyczących pomocy państwa w formie rekompensaty z tytułu świadczenia usług publicznych (wskazano wprost, że: *„W przypadku niektórych usług świadczonych w ogólnym interesie gospodarczym (UOIG), wykonywanie ich na zasadach i warunkach umożliwiających wypełnienie związanych z nimi zadań może wymagać wsparcia finansowego ze strony organów publicznych, o ile przychody z tytułu świadczenia tych usług nie pozwalają na pokrycie kosztów związanych z wywiązywaniem się ze zobowiązań z tytułu świadczenia usług publicznych*". Dlatego też akt powierzenia powinien wskazywać na parametry obliczania rekompensaty (nie musi to być dokładna kwota należna tytułem rekompensaty o czym niżej) oraz środki ochronne mające zabezpieczać przed nadwyżką rekompensaty.

Przepisy prawa UE nie przesądzają, w jakiej formie ma nastąpić powierzenie UOIG na rzecz przedsiębiorcy.

W swojej praktyce Komisja i TSUE dopuszczały następujące formy aktu powierzenia jako prawidłowe:

– umowa udzielenia koncesji i zamówienie na świadczenie usługi publicznej,[8]
– umowy programowe z ministerstwami,[9]
– polecenia ministerialne,[10]
– ustawy i inne akty legislacyjne,[11]
– roczne oraz wieloletnie umowy wskazujące określone wyniki, jakie mają być osiągnięte,[12]
– dekrety ustawodawcze i wszelkiego rodzaju decyzje wykonawcze oraz decyzje lub dokumenty władz centralnych lub lokalnych.[13]

Jak wynika z powyższego, państwa członkowskie posiadają pewną w swobodę w wyborze formy, w jakiej nastąpi powierzenie UOIG na rzecz danego przedsiębiorcy i prawo unijne nie nakłada w tym zakresie wyraźnych ograniczeń. We wskazanym wyżej Komunikacie Komisji 2012/C 8/03 stwierdzono jedynie w pkt. 15, że: *„Odpowiedzialność za wykonywanie UOIG musi być powierzona odnośnemu przedsiębiorstwu lub przedsiębiorstwom na mocy jednego lub większej liczby aktów, których formę mogą określić poszczególne państwa członkowskie. Pojęcie „państwo członkowskie" obejmuje władze centralne, regionalne i lokalne".* Co istotne wiec, powierzającym mogą więc być zarówno władze rządowe (np. minister), jak i samorządowe (np. gmina lub miasto), a sam akt powierzenia może przybrać formę jednego, lub kilku dokumentów.

I. 5. Konsekwencje prawne i faktyczne powierzenia świadczenia UOIG (tj. zakres wyłączenia oraz rekompensata)

W przypadku przedsiębiorstw, którym prawidłowo powierzono świadczenie usług w ogólnym interesie gospodarczym dopuszcza się wyłączenie zastosowania przepisów traktatowych (oraz wydanych na ich podstawie aktów prawa pochodnego), w takim zakresie, w jakim zastosowanie prawa europejskiego miałoby stanowić prawną

8 Decyzja Komisji w sprawie N 562/05 – Włochy – Proroga della durata della concessione della Società Italiana del Traforo del Monte Bianco (SITMN), Dz.U. C 90 z 25.4.2007

9 Decyzja Komisji w sprawie NN 51/06 – Włochy – Poste Italiane SpA: zwrot kosztów przekazany przez państwo w ramach świadczenia międzynarodowych usług pocztowych w latach 2000-2005, Dz.U. C 291 z 30.11.2006

10 Decyzja Komisji w sprawie N 166/05 – Zjednoczone Królestwo – Fundusz państwa dla Poczty wspierający sieci na obszarach wiejskich, Dz.U. C 141 z 16.6.2006

11 Wyrok w sprawie T-289/03 BUPA i in. przeciwko Komisji, Zb.Orz. 2008, s. II-741, pkt 182 i 183; decyzja Komisji w sprawie NN 8/07 – Hiszpania – Financiamento de las medidas de reducción de plantilla de RTVE, Dz.U. C 109 z 15.5.2007; decyzja Komisji w sprawie N 395/05 – Irlandia – Gwarancje pożyczkowe na rzecz programów infrastruktury społecznej przyznawane przez Housing Finance Agency, Dz.U. C 77 z 5.4.2007

12 Decyzja Komisji w sprawie C 24/2005 – Francja – Laboratoire national de métrologie et d'essais, Dz.U L 95 z 5.4.2007, s. 25.

13 Wyrok w sprawie C-451/03 Servizi Ausiliari Dottori Commercialisti przeciwko Giuseppe Calafiori, Zb.Orz. 2006, s. I-2941.

lub faktyczną przeszkodę w świadczeniu powierzonych mu usług.[14]

Przy czym, warto doprecyzować, że przepis art. 106 ust. 2 TFUE pozwala na wyłączenie stosowania określonych reguł konkurencji, w szczególności:

– przepisów traktatowych skierowanych do państwa członkowskich w zakresie, w jakim ograniczałyby one możliwość powierzenia przez państwo usług w ogólnym interesie gospodarczym lub wykonywania ich przez przedsiębiorcę, któremu je powierzono;
– przepisów traktatowych skierowanych do przedsiębiorców w zakresie, w jakim ograniczałyby one możliwość powierzenia przez państwo usług w ogólnym interesie gospodarczym lub wykonywania ich przez przedsiębiorcę, któremu je powierzono;
– przepisów aktów prawa wtórnego skierowanych zarówno do państw członkowskich, jak i do przedsiębiorców, w zakresie, w jakim ograniczałyby one możliwość powierzenia przez państwo usług w ogólnym interesie gospodarczym lub wykonywania ich przez przedsiębiorcę, któremu je powierzono.[15]

Co jest niezwykle istotne, wyłączenie zastosowania przepisów prawa europejskiego w przypadku przedsiębiorstw, którym powierzono świadczenie usług w ogólnym interesie gospodarczym, będzie skuteczne jedynie, jeśli będzie spełniało przesłankę proporcjonalności. Wymóg spełnienia tej przesłanki jest tym bardziej istotny, w przypadku kiedy rekompensata za świadczenie usług w ogólnym interesie gospodarczym przyjmuje formę praw wyłącznych lub specjalnych. [16]Mając na względzie syntetyczny charakter niniejszego artykułu, w tym miejscu zasygnalizować jedynie trzeba, że orzecznictwo i doktryna wypracowały specjalny mechanizm, dzięki któremu badana jest przesłanka proporcjonalności[17]

Jednocześnie, należy mieć na względzie, że o ile samo powierzenie świadczenia usług w ogólnym interesie gospodarczym podlega ocenie na podstawie art. 106 ust. 2 TFUE, to w przypadku rekompensaty przyznawanej za świadczenie w/w usług (także rekompensaty przyjmującej formę praw wyłącznych lub specjalnych), konieczne jest dokonanie analizy, czy w świetle orzecznictwa TSUE[18], jak i szeregu ak0tów prawa wtórego dotyczących rekompensaty za świadczenie usług w ogólnym interesie gospodarczym[19], może być ona uznana za pomoc zgodną z rynkiem wewnętrznym, a więc nie naruszającą art. 107 TFUE.

14 Artykuł 106 TFUE

1. Państwa Członkowskie, w odniesieniu do przedsiębiorstw publicznych i przedsiębiorstw, którym przyznają prawa specjalne lub wyłączne, nie wprowadzają ani nie utrzymują żadnego środka sprzecznego z normami Traktatów, w szczególności z normami przewidzianymi w artykułach 18 oraz 101–109.
2. Przedsiębiorstwa zobowiązane do zarządzania usługami świadczonymi w ogólnym interesie gospodarczym lub mające charakter monopolu skarbowego podlegają normom Traktatów, zwłaszcza regułom konkurencji, w granicach, w jakich ich stosowanie nie stanowi prawnej lub faktycznej przeszkody w wykonywaniu poszczególnych zadań im powierzonych. Rozwój handlu nie może być naruszony w sposób pozostający w sprzeczności z interesem Unii.

15 Sprawa C-3/59 Federalna Republika Niemiec przeciwko Wysoka Władza Europejskiej Wspólnoty Węgla i Stali [1960] Zb.Orz. 119, 133; zob. też Jose Luis Buendia Sierra w „Exclusive Rights and State Monopolies under EC Law", Oxfrod University Press, str. 288-299, 355-363.

16 Sprawa C-320/91 Corbeau, Rec. 1993, s. I–2533, pkt 14–16, sprawa C–67/96 Albany, Rec. 1999, s. I–5751, pkt 107

17 Test proporcjonalności stosuje się do oceny działań państw członkowskich podejmowanych w celu wykonania prawa UE (np. TSUE w spr. C-285/98 Tanja Kreil), a także w ramach dopuszczalnych derogacji (np. 120/78 Cassis de Dijon, 36/75 Rutil, 116/81 Adoui and Cmornuaille). Zakłada on, że stosowanie wyłączeń z zakresu prawa europejskiego, w tym wyłączeń na podstawie art. 106 ust. 2 TFUE, jest dopuszczalne, kiedy środki przyjęte przez państwo członkowskie są jednocześnie:

– odpowiednie – to znaczy takie, przy pomocy których ten cel da się osiągnąć;
– niezbędne – to znaczy takie, których nie sposób osiągnąć efektywniej za pomocą innego środka, bardziej właściwego do osiągnięcia zamierzonego celu;
– proporcjonalne sensu stricto – takie, które w najmniejszym stopniu ograniczają realizację celów prawa europejskiego, czyli są najmniej restrykcyjne.

Mając na względzie opisany powyżej test proporcjonalności, w przypadku powierzenia UOIG na rzecz Przedsiębiorstwa należałoby zatem wykazać, że działanie takie jest niezbędne do zapewnienia wykonania zadań leżących w interesie ogólnym na warunkach dopuszczalnych pod względem gospodarczym. Podobnie, w przypadku wyboru praw wyłącznych jako formy rekompensaty, należałoby wykazać, że inne formy finansowania kosztów świadczenia UOIG byłyby, mniej efektywne z punktu widzenia zamierzonych celów.

18 Sprawa C-280/00 Altmark Trans GmbH i Regierungspräsidium Magdeburg przeciwko Nahverkehrsgesellschaft Altmark GmbH, przy udziale Oberbundesanwalt beim Bundesverwaltungsgericht, Zb.Orz. s. I-7747.

19 Decyzja Komisji nr 2005/842/WE w sprawie stosowania art. 86 ust. 2 TWE do pomocy państwa w formie rekompensaty z tytułu świadczenia usług publicznych przyznawanej niektórym przedsiębiorstwom, którym zostało powierzone świadczenie usług w ogólnym interesie gospodarczym; Wspólnotowe ramy prawne dotyczące pomocy państwa w formie rekompensaty z tytułu świadczenia usług publicznych; Dyrektywa Komisji 2005/81/WE nowelizująca dyrektywę Komisji 80/723/EWG z 25.06.1980 r. w sprawie przejrzystości stosunków finansowych między państwami członkowskimi i przedsiębiorstwami publicznymi, a także przejrzystości finansowej wewnątrz określonych przedsiębiorstw.

I. 6. Zasady wykonywania UOIG

Organy administracji publicznej dysponują dużą swobodą przy wyborze sposobu zarządzania i finansowania usług świadczonych w ogólnym interesie gospodarczym. Zasady pomocy państwa pozwalają organom publicznym na organizację i finansowanie usług świadczonych w ogólnym interesie gospodarczym wedle własnego uznania, o ile rekompensaty z tytułu świadczenia tych usług nie wykraczają poza to, co jest niezbędne do zagwarantowania (zasada proporcjonalności). Zgodnie z wyrokiem TSUE w przywoływanej powyżej sprawie Altmark, rekompensata z tytułu świadczenia usługi publicznej przyznana usługodawcy przez organ publiczny nie będzie stanowiła pomocy państwa, jeżeli spełnia łącznie następujące kryteria:

– po pierwsze, przedsiębiorstwo będące beneficjentem powinno być rzeczywiście obciążone wykonaniem zobowiązań do świadczenia usług publicznych i zobowiązania te powinny być jasno określone;
– po drugie, parametry, na podstawie których obliczona jest rekompensata, muszą być wcześniej ustalone w sposób obiektywny i przejrzysty;
– po trzecie, rekompensata nie może przekraczać kwoty niezbędnej do pokrycia całości lub części kosztów poniesionych w celu wykonania zobowiązań do świadczenia usług publicznych, przy uwzględnieniu związanych z nimi przychodów oraz rozsądnego zysku;
– ponadto jeżeli wybór przedsiębiorstwa, któremu ma zostać powierzone wykonywanie zobowiązań do świadczenia usług publicznych, nie został w danym wypadku dokonany w ramach procedury udzielania zamówień publicznych, pozwalającej na wyłonienie kandydata zdolnego do świadczenia tych usług po najniższym koszcie dla danej społeczności, poziom koniecznej rekompensaty powinien zostać ustalony na podstawie analizy kosztów, jakie poniosłoby przeciętne przedsiębiorstwo, prawidłowo zarządzane i wyposażone.

Poniżej kilka przykładów praktycznych związanych z zagadnieniem pomocy państwa w kontekście świadczenia przez przedsiębiorcę usług w ogólnym interesie gospodarczym:

a) w decyzji Poste Italiane – Banco Posta, Komisja stwierdziła, że prowizje zapłacone przez „Casa Depositi e Prestiti" – jednostkę finansową kontrolowaną przez państwo – na rzecz „Poste Italiane" nie stanowią pomocy państwa:
   – sprzedaż pocztowych książeczek oszczędnościowych została uznana za usługę świadczoną w ogólnym interesie gospodarczym;
   – wysokość opłaty rynkowej odpowiadała właściwym szacunkom dotyczącym poziomu kosztów, które poniosłoby przeciętne przedsiębiorstwo odpowiednio zarządzane i wyposażone, działające w tym samym sektorze, przy uwzględnieniu przychodów i rozsądnego zysku z tytułu wywiązywania się z tych zobowiązań. W rezultacie spełniony został czwarty warunek z wyroku w sprawie Altmark.[20],
b) w Komunikacie Komisji C(2004)42 Wytyczne Wspólnoty w sprawie pomocy państwa dla transportu morskiego uznano, że *„inwestycji w infrastrukturę zazwyczaj nie traktuje się jako pomocy publicznej (…), o ile państwo gwarantuje wszystkim zainteresowanym przewoźnikom swobodny i równy dostęp do danej infrastruktury…"*. Niemniej jednak na gruncie konkretnych stanów faktycznych, w wyniku badania korzyści bezpośrednich i pośrednich uzyskiwanych przez właścicieli statków/infrastruktury, mogą zaistnieć podstawy do uznania danej inwestycji za niedozwoloną pomoc państwa. Kwestia bezpośrednich i pośrednich korzyści uzyskiwanych przez przedsiębiorcę powinna więc stanowić przedmiot szczegółowej analizy np. w decyzji Komisji z dnia 20 października 2004 r. w sprawie N 520/2003 – Belgia – Wsparcie finansowe na prace infrastrukturalne w portach flamandzkich stwierdzono, że budowa i utrzymanie (w tym pogłębianie) morskich dróg dostępu do portu (tk. Kanałów żeglownych, w tym w zalewowych częściach portu, kanałów zapewniających dostęp do śluz morskich i innych powiązanych urządzeń, doków w kanałach itp.) stanowi zadanie publiczne władz regionalnych, a realizowanie tych zadań nie wchodzi w zakres pojęcia działalności gospodarcze; na powyższe nie ma wpływu nawet fakt otrzymywania przez zarządcę rekompensaty za utrzymywanie dróg do portu, o ile nie jest ona nadmierna i jest wykorzystywana zgodnie z przeznaczeniem (podobnie stanowisko Komisji w decyzji z dnia 21 grudnia 2005 r. w sprawie N 503/2005 – Zjednoczone Królestwo – Great Yarmauth Outer Harbour odnośnie do inwestycji w infrastrukturę ogólnodostępnych, lecz

20 Decyzja Komisji dotycząca pomocy państwa C 49/06 – Poste Italiane – Banco Posta – Wynagrodzenie wypłacane z tytułu dystrybucji pocztowych produktów oszczędnościowych, Dz.U. C 31 z 13.2.2007.

odpłatnych dróg dostępu do portu oraz budowy falochronów),

c) w orzeczeniu TSUE z dnia 22 listopada 2001 r. w sprawie Ferring S.A. (C-53/00) sąd uznał, że przyznanie na rzecz przedsiębiorcy ulg podatkowych stanowi niedozwoloną pomoc państwa wyłącznie w zakresie, w jakim korzyści płynące z ulg przewyższają dodatkowe koszty, jakie ponosi przedsiębiorca w związku ze świadczeniem usług publicznych,

d) w orzeczeniu Sądu I Instancji z 15 czerwca 2005 r. w sprawie Fred Olsen S.A. (T-17/02) sąd stwierdził, że nie jest niedozwoloną pomocą państwa subwencja przyznana na rzecz przedsiębiorcy obsługującego morskie połączenia między wyspami Archipelagu Kanaryjskiego, jeśli subwencja ta jest niższa niż szacowane dodatkowe koszty związane z zobowiązaniami z tytułu świadczenia usług publicznych. Co więcej, we wskazanym wyżej orzeczeniu uznano, że brak jest wymogów prawnych, aby „misja interesu ogólnego" była powierzona podmiotowi gospodarczemu w wyniku zastosowania procedury zaproszenia do składania ofert. Dokonując oceny, czy dany przedsiębiorca jest w stanie zapewnić świadczenie usług transportu morskiego w interesie publicznym należy uwzględniać m.in. ciągłość, regularność rejsów i częstotliwość na wszystkich połączeniach

Aby zastosować drugą część czwartego kryterium orzecznictwa w sprawie Altmark, państwa członkowskie mogą stosować ustalony wcześniej koszt odniesienia, pod warunkiem że mogą takie postępowanie uzasadnić. Jeżeli koszt ten zostanie obliczony w wiarygodny sposób, na podstawie rzetelnych danych i zgodnie z wartościami rynkowymi, można uznać, iż odpowiada on kosztom, jakie poniosłoby przeciętne przedsiębiorstwo, prawidłowo zarządzane i odpowiednio wyposażone w rozumieniu czwartego kryterium orzecznictwa w sprawie Altmark.

W przypadku spełnienia kryteriów orzecznictwa w sprawie Altmark rekompensata z tytułu świadczenia usług publicznych nie stanowi pomocy państwa. W przypadku gdy co najmniej jedno z kryteriów orzecznictwa w sprawie Altmark nie jest spełnione, natomiast spełnione są pozostałe kryteria świadczące o pomocy państwa, rekompensata z tytułu świadczenia usług publicznych stanowi pomoc państwa. W celu uniknięcia ryzyka uznania rekompensaty za pomoc państwa można zastosować tzw. mechanizm wycofania rekompensaty. Jest to mechanizm, który zobowiązuje usługodawcę do zwrotu rekompensaty w określonych okolicznościach (tzn. gdyby w trakcie świadczenia usługi w ogólnym interesie gospodarczym okazało się że jedno z kryteriów wskazanych w wyroku Altmark nie jest spełnione).

Szczególnie, w przypadku gdy trudno jest przewidzieć wysokość przychodów z tytułu świadczenia usługi, mechanizm wycofania w akcie powierzenia może być właściwym narzędziem zmniejszenia ryzyka nadwyżki rekompensaty (tj. rekompensaty przekraczającej koszty netto powiększone o rozsądny zysk przy uwzględnieniu istniejącego ryzyka). Należy zauważyć, że w przypadkach, w których usługodawca ponosi wysokie ryzyko (np. w przypadku niektórych rodzajów umów koncesji lub usług świadczonych na rynku, na którym wahania krzywej popytu są znaczne i trudne do przewidzenia), poziom dochodów może się wahać od ujemnego (straty) do wyższego niż przeciętny. Nie oznacza to automatycznie, że w tym drugim przypadku usługodawca otrzymałby nadwyżkę rekompensaty, pod warunkiem że poziom zysku byłby nadal uzasadniony z uwagi na poziom ryzyka. W takich przypadkach państwa członkowskie mogłyby jednak uwzględnić w ramach mechanizmu rekompensaty także klauzulę dotyczącą wycofania, tak aby ustalić górną granicę zysku, który zostanie wypłacony.

W przypadku, kiedy zaistniałyby poważne obawy, czy pomoc udzielona Przedsiębiorstwu w związku z przyznaniem rekompensaty spełnia warunki szczególne określone w wyroku w sprawie Altmark, państwo członkowskie może powiadomić o planowanych działaniach Komisję i uzyskać jej zgodę na planowane działanie na podstawie art. 93 TFUE.

Na zakończenie, odnosząc się do kwestii sposobu interpretacji opisywanego wyżej m.in. art. 106 TFUE, należy zwrócić uwagę na treść art. 14 TFUE, który ustanawia ogólną regułę interpretacyjną odnoszącą się do zasad funkcjonowania usług w ogólnym interesie gospodarczym. Zgodnie z art. 14 TFUE, bez uszczerbku dla m.in. art. 106 i 107 TFUE oraz zważywszy na miejsce, jakie usługi świadczone w ogólnym interesie gospodarczym zajmują wśród wspólnych wartości Unii, jak również ich znaczenie we wspieraniu jej spójności społecznej i terytorialnej, Unia i państwa członkowskie, każde w granicach swych kompetencji i w granicach stosowania TFUE, powinny zapewnić, aby te usługi funkcjonowały na podstawie zasad i na warunkach, w szczególności gospodarczych i finansowych, które pozwolą im wy-

pełniać ich zadania. Umiejscowienie wskazanego wyżej przepisu w systematyce traktatów, wśród zasad naczelnych, interpretowane może być jako intencja prawodawcy do zaakcentowania roli usług świadczonych w ogólnym interesie gospodarczym. Ponadto, niekiedy w doktrynie wskazuje się, że wynikający z art. 14 TFUE nakaz wspierania i protegowania usług w ogólnym interesie gospodarczym jest ogólną zasadą traktatową, mającą zasięg i znaczenie horyzontalne (A. Wróbel (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, LEX nr 445507).

Podsumowanie

W przypadku posługiwania się przez państwa członkowskie art. 106 ust. 2 TFUE szczególnie istotne znaczenie mają szeroko zakrojona swoboda państw w zakresie definiowania interesu ogólnego, treści UOIG, jak też wskazywania formy rekompensaty za świadczenie UOIG. Ponadto, należy zwrócić uwagę na fakt, że wyłączenie z zakresu stosowania TFUE obejmuje zarówno przepisy skierowane do państw członkowskich, jak i te skierowane do przedsiębiorców. Wreszcie, dla zastosowania art. 106 ust. 2 TFUE niezbędne jest wykazanie, że zarówno zakres UOIG, jak i forma rekompensaty spełniają przesłankę proporcjonalności, a dodatkowo wysokość rekompensaty została wyznaczona z poszanowaniem dla przepisów dotyczących pomocy państwa.

3. Cyberbezpieczeństwo infrastruktury krytycznej

I. Aktualny stan prawny i konieczność zmian

(Opracowanie: ***Kinga Rochalska***, LSW Leśnodorski Ślusarek i Wspólnicy)

A. Rola systemów teleinformatycznych dla infrastruktury krytycznej

Infrastruktura krytyczna („IK") to kluczowy element bezpieczeństwa państw i ich obywateli. W skład IK wchodzą obiekty służące zapewnieniu sprawnego funkcjonowania zarówno organów administracji publicznej, jak również przedsiębiorstw oraz zapewniające ochronę życia i zdrowia obywateli i bezpieczeństwo środowiska naturalnego. IK jest również gwarancją minimalnego funkcjonowania gospodarki państwa. Obecnie, zdecydowana większość systemów należących do IK jest skomputeryzowana. Systemy teleinformatyczne są zatem bezpośrednio wykorzystywane przez IK. Zgodnie z art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, definiującym pojęcie infrastruktury krytycznej, IK obejmuje również między innymi systemy sieci teleinformatycznych. Ponadto, chociaż nie wynika to wprost z ustawowej definicji infrastruktury krytycznej, do IK należy zaliczyć także tzw. infrastrukturę wirtualną – informacyjną, w tym na przykład informacje z baz danych, która ma również kluczowe znaczenie dla bezpieczeństwa państwa.

Zagrożenia dla prawidłowego działania, jak również istnienia IK mogą mieć różne podłoże i mogą być spowodowane siłami przyrody, awarią systemu, czy też (intencjonalnym lub nie) działaniem człowieka. Wspólną cechą wszelkich sytuacji mogących stanowić zagrożenie dla IK jest utrudnienie lub uniemożliwienie korzystania z jej zasobów, a w konsekwencji nawet sparaliżowanie funkcjonowania państwa. Należy zwrócić uwagę, iż IK zagrażają nie tylko ataki konwencjonalne, lecz także tzw. cyberataki. Do szczególnie niebezpiecznych zagrożeń należą działania sabotażowe oraz ataki terrorystyczne wymierzone wprost w IK lub jej otoczenie. Powszechne jest również stosowanie cyberszpiegostwa przez organizacje terrorystyczne lub organizacje wspierane przez państwa pozostające w konflikcie. W związku z powyższym, niezbędne jest istnienie w porządku prawnym danego państwa odpowiednich regulacji zapewniających kompletny i powszechny system ochrony IK.

Niniejsze opracowanie ma na celu wskazanie regulacji prawnych aktualnie obowiązujących w polskim porządku prawnym w zakresie cyberbezpieczeństwa IK, jak również zaznaczenie zmian ustawodawstwa europejskiego w tej dziedzinie. Ponadto, zostały również wskazane postulaty, jakie powinny zostać spełnione, aby system ochrony IK w cyberprzestrzeni był dokładniej zabezpieczony.

B. Systemy teleinformatyczne wykorzystywane w ramach IK

Systemy teleinformatyczne, które są wykorzystywane w ramach Infrastruktury krytycznej, jak również będące jednocześnie komponentem tej infrastruktury, można podzieli na dwie grupy, to jest systemy informatyczne (ang. Information Technology – IT) oraz systemy sterowania przemysłowego (ang. Operational Technology – OT)[21]. Zastosowanie każdego ze wskazanych rozwiązań w dużej mierze zależy od branży, w której są wykorzystywane. I tak, IT znajdzie zastosowanie w obszarach IK świadczących usługi dla obywatela, takich jak finanse, komunikacja czy administracja publiczna, natomiast OT przeznaczone są dla obiektów IK związanych z wszelkimi procesami technologicznym, w tym wydobycia, wytwarzania lub przetwórstwa (energetyka, przemysł chemiczny czy zaopatrzenie w żywność).

Pomiędzy przedstawionymi systemami istnieją podstawowe różnice determinujące ich rolę, charakter, jak również rodzaj zastosowanych środków

21 M. Ryba, *Rola elementów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej*; [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, G. Abgarowicz, R. Antkiewicz, P. Ciepiela, M. Dyk, D. Dziwisz, Z. Fałek, P. Gajek, R. Kasprzyk, W. Kotłowski, M. Maj, A. Najgebauer, D. Pierzchała, A. Poniewierski, M. Pyznar, M. Ryba, K. Rzecki, J. Świątkowska, Z. Tarapata, A. Wiercińska-Krużewska;

ochrony wykorzystywanych w poszczególnych obiektach IK. Wśród kluczowych rozbieżności wskazuje się przede wszystkim na:

1) Kwestie związana z wydajnością i dostępnością rozwiązań,
2) Okres działania, na jaki rozwiązania są projektowane,
3) Różnice w postrzeganiu bezpieczeństwa[22].

Należy zwrócić uwagę, iż z perspektywy systemów informatycznych (IT), mających zastosowanie na przykład w finansach, przerwa w ciągłości działania systemu, choć może skutkować poniesieniem straty ekonomicznej, nie przyczyni się do dezintegracji całego obszaru IK, w którym dany system jest wykorzystywany, jak również nie wpłynie znacząco na bezpieczeństwo tego obszaru. Odmiennie, w przypadku OT, przerwy w działaniu systemu są niemożliwe do zaakceptowania, gdyż poza stratami finansowymi, mogą skutkować zagrożeniem lub naruszeniem bezpieczeństwa obywateli, państwa lub środowiska naturalnego.

Ponadto, różny jest okres działania, na jaki rozwiązania poszczególnych systemów są projektowane. O ile dla rozwiązań IT jako średni czas eksploatacji wskazuje się 3-5 lat, to w przypadku rozwiązań OT ten czasookres wynosi nawet 15 lat. Zatem, w środowisku IT częściej spotykane będą instrumenty innowacyjne, łatwiej dostosowujące się do postępu technologicznego, podczas gdy system OT nie będzie podlegał tak częstym zmianom oraz będzie zawierał technologie niejednokrotnie przestarzałe.

Warto również zwrócić uwagę, iż rozbieżne są aspekty bezpieczeństwa pomiędzy IT i OT, ze względu na odmienne priorytety tych systemów. Celem rozwiązań IT jest bowiem zabezpieczenie poufności danych, podczas gdy rozwiązania OT są skoncentrowane na zapewnieniu stałości i dostępności produkcji. W celu ochrony poszczególnych systemów infrastruktury teleinformatycznej może być zatem konieczne zapewnienie odmiennych środków.

Zagrożenia dla cyberbezpieczeństwa IK

Ze względu na fakt, iż technologia teleinformatyczna jest jednym z komponentów IK państwa i jest wykorzystywana do zarządzania takimi obiektami jak sieci energetyczne, transportowe czy telekomunikacyjne, ataki (w tym cyberataki) na IK zagrażają bezpieczeństwu całego państwa. Technologia teleinformatyczna będzie zatem miała ogromne znaczenie w przypadku konfliktu, sytuacji kryzysowej lub wojny. Technologia ta staje się głównym elementem zarządzania siłami zbrojnymi i zasobami strategicznymi, jak również może stać się bezpośrednim celem działań wojennych. W związku z powyższym, należy uznać, iż cyberprzestrzeń stanowi jedną ze strategicznych sfer z punktu widzenia obronności kraju.

Podkreślenia wymaga również fakt, iż cyberataki są tanim, w porównaniu z atakami konwencjonalnymi, i skutecznym środkiem dezintegracji funkcjonowania państwa i jego obywateli. Zdecydowanie trudniejsze, a niejednokrotnie niemożliwe jest również wykrycie ze stuprocentową pewnością sprawcy ataku. W związku z powyższym, w przypadku ewentualnych konfliktów lub sytuacji kryzysowych, cyberataki będą stanowiły coraz większe zagrożenie.

W literaturze wskazuje się na następujące czynniki wpływające na podatność IK na cyberataki:

1) Brak świadomości w zakresie bezpieczeństwa systemów teleinformatycznych,
2) Wysokie koszty bezpieczeństwa,
3) Korzystanie z podwykonawców,
4) Upowszechnienie się technologii i jej dostępność,
5) Brak edukacji na wszystkich poziomach ochrony,
6) Brak analizy potencjalnych ryzyk,
7) Brak opracowanych wdrażanych równolegle (alternatywnych) metod działania,
8) Element ludzki.

Najistotniejsze zagrożenie dla cyberbezpieczeństwa IK stanowi brak świadomości właścicieli, operatorów obiektów IK i użytkowników cyberprzestrzeni w zakresie zagrożeń, ryzyka i konsekwencji ewentualnych cyberataków dla prawidłowego funkcjonowania IK. Brak zainteresowania osób zarządzających obszarami IK w temacie zapewnienia cyberbezpieczeństwa prowadzi do ograniczania kosztów przeznaczonych na ten cel. Panujące przeświadczenie, iż wprowadzenie drogich oprogramowań lub zatrudnianie specjalistów jako działań profilaktycznych jest nieopłacalne i bardziej kosztowne niż naprawa ewentualnych zniszczeń prowadzi do osłabienia ochrony systemu. W konsekwencji, może dochodzić do sytuacji, w których właściciele lub operatorzy obiektów wchodzących w skład IK nie będą nawet wiedzieli, iż są celem ataków mających na celu pozyskanie informacji o funkcjonowaniu

22 *Tamże;*

danego obszaru IK. Co więcej, w celu ograniczenia kosztów, coraz częściej do wykonywania wewnętrznych zadań danego przedsiębiorstwa wykorzystuje się zewnętrznych podwykonawców. Często są to małe podmioty, które nie mają finansowych możliwości wprowadzenia odpowiednich zabezpieczeń. Podczas wykonywania prac, system operatora IK jest połączony z systemem podwykonawcy, co może ułatwić dostęp osób trzecich do chronionych informacji.

W literaturze podnosi się, iż z tym zagrożeniem bardzo mocno związany jest również brak systemowej edukacji na wszystkich poziomach ochrony IK, w tym edukacji szkolnej i uniwersyteckiej kształcącej kadry zarządcze, jak również kadry mające zdolność przeciwdziałania zagrożeniom dla IK[23]. Należy zwrócić uwagę, iż o ile w przeszłości rozwiązania teleinformatyczne projektowane były odrębnie dla poszczególnych przedsiębiorstw, a wiedzę w tym zakresie posiadali wyłącznie specjaliści, to dziś, w wyniku unifikacji, technologia teleinformatyczna jest rozpowszechniona i ogólnodostępna. Możliwa jest zatem ingerencja w funkcjonujący system bez obecności przy jego instalacji, jak również bez specjalistycznej wiedzy. Cyberataki na technologie teleinformatyczne wykorzystywane w ramach IK mogą następować z dowolnego miejsca na świecie i być przeprowadzane przez osoby, które nie posiadają szczegółowych informacji o danym obiekcie. Im bardziej powszechne jest rozwiązanie zastosowane w danym przedsiębiorstwie, tym łatwiejszym może być celem ataku.

Warto wskazać tu jako przykład popularne systemy SCADA (Supervisory Control And Data Acquisition) nadzorujące przebieg procesu technologicznego i produkcyjnego i wykorzystywane do kontroli i sterowania automatyką przemysłową. W powszechnej opinii są one podatne na ataki hakerów, co potwierdza atak na systemy SCADA kanadyjskiej spółki Telvent (obecnie należącej do grupy Schneider Electric) – operatora gazociągów w Ameryce Północnej i Łacińskiej w 2012 roku[24]. Ponadto, nie bez znaczenia dla cyberbezpieczeństwa jest rosnąca popularność powszechnie dostępnych i niedrogich usług cloud–computingu i wirtualizacji. Bezpieczeństwo przechowywania danych w tzw. „chmurze" w kontekście zagrożenia cyberatakami jest jednak wątpliwe.

Za największe zagrożenie dla zasobów informacyjnych uważa się jednak czynnik ludzki, to jest pracowników danego podmiotu i osoby cieszące się zaufaniem zarządzających. Przede wszystkim osoby te mają najszerszy dostęp do informacji, które mogą wykorzystać dla celów osobistych lub zarobkowych, czy też przekazać dane osobom z zewnątrz. Należy podkreślić również, iż na poziom cyberbezpieczeństwa IK ma wpływ poziom skomplikowania haseł używanych przez pracowników, fakt korzystania przez nich z personalnych urządzeń mobilnych i przechowywania na nich danych oraz korzystanie z własnego niezabezpieczonego oprogramowania.

Ochrona teleinformatycznych elementów infrastruktury krytycznej w aktualnym stanie prawnym

Zagadnienie ochrony IK zostało określone w licznych aktach prawnych, zarówno rangi ustawowej, jak i podustawowej, w zależności od dziedziny funkcjonowania państwa, której dotyczą. Podstawowym aktem prawnym regulującym ochronę IK jest **ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym**. Ustawa definiuje pojęcie infrastruktury krytycznej oraz ochrony infrastruktury krytycznej. Zgodnie z art. 3 pkt 3 ustawy, przez ochronę IK należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Ustawa o zarządzaniu kryzysowym nakłada bezpośrednio na właścicieli oraz posiadaczy obiektów, instalacji lub urządzeń IK obowiązek ich ochrony, w tym poprzez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. To również operatorzy IK zostali obciążeni obowiązkiem finansowania

23 A. Poniewierski, *Zagrożenia dla bezpieczeństwa infrastruktury krytycznej w kontekście zaawansowanego zastosowania rozwiązań teleinformatycznych – wyzwania dla państwa*; [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, G. Abgarowicz, R. Antkiewicz, P. Ciepiela, M. Dyk, D. Dziwisz, Z. Fałek, P. Gajek, R. Kasprzyk, W. Kotłowski, M. Maj, A. Najgebauer, D. Pierzchała, A. Poniewierski, M. Pyznar, M. Ryba, K. Rzecki, J. Świątkowska, Z. Tarapata, A. Wiercińska-Krużewska;

24 D. Łydziński, *Cyberbezpieczeństwo i ochrona infrastruktury krytycznej*, http://www.safetyandsecurity.pl/index.php/archiwum/27-bezpieczenstwo-it/254-cyberbezpieczenstwo-i-ochrona-infrastruktury-krytycznej, dostęp: 2.04.2015 r.

działań z zakresu ochrony IK z własnych środków. Po stronie organów państwa (to jest Rady Ministrów) pozostaje przyjęcie „Narodowego Planu Ochrony Infrastruktury Krytycznej", który przede wszystkim określa ramy współpracy sektora publicznego (administracji publicznej) z sektorem prywatnym (operatorami IK).

Obecny kształt ustawy wynika po części z implementacji **Dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony** (Dz.Urz. UE z 23.12.2008r., L 345/75), która w założeniu ma stanowić pierwszy krok w etapowym podejściu do rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz do oceny potrzeb w zakresie poprawy jej ochrony. Dyrektywa jednoznacznie powierza zasadniczą i ostateczną odpowiedzialność za ochronę europejskiej IK państwom członkowskim i właścicielom/operatorom tych infrastruktur. Dyrektywa nie zawiera jednak szczegółowych regulacji dotyczących instrumentów prawnych lub procedur, które powinny być zastosowane w celu ochrony IK.

Odnośnie elementów infrastruktury teleinformatycznej (z wyłączeniem jednak infrastruktury wirtualnej) bardziej szczegółowe rozwiązania zawierają przepisy ustawy z dnia 16 lipca 2004 r. **prawo telekomunikacyjne**. Na przedsiębiorców telekomunikacyjnych został między innymi obowiązek informowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach (art. 175a ustawy), posiadania planów działań w sytuacjach szczególnych zagrożeń (art. 176a ust. 2 ustawy), czy też nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej w sytuacjach szczególnych zagrożeń (art. 177 ust. 3 ustawy).

Jednym z bardziej istotnych dokumentów, wyznaczających strategiczne kierunku rozwoju cyberbezpieczeństwa Polski, a w tym także cyberbezpieczeństwa IK jest **Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016**. Przedmiotem Programu są propozycje działań zarówno o charakterze prawno-organizacyjnym, technicznym, jak i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Adresatami Programu są organy władzy publicznej, operatorzy IK, przedsiębiorcy i użytkownicy indywidualni cyberprzestrzeni oraz inne instytucje będące użytkownikami cyberprzestrzeni. W treści Programu zostało podkreślone, iż znacząca część zasobów infrastruktury teleinformatycznej stanowi własność prywatną, zatem przedsiębiorcy, którzy są właścicielami tych zasobów powinni pełnić istotną rolę w realizacji założeń Programu.

Wśród założeń zmian legislacyjnych Program zakłada uregulowanie wszelkich aspektów związanych z zarządzaniem i bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej przez wprowadzenie przepisów dotyczących między innymi zdefiniowania podjęć dotyczących cyberprzestrzeni, cyberprzestępczości i cyberterroryzmu, ustalenia odpowiedzialności za ochronę cyberprzestrzeni RP, wprowadzenia funkcji Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP oraz umocowania prawnego Rządowego Zespołu Reagowania na Incydenty Komputerowe. W zakresie działań technicznych Program przewiduje w szczególności rozbudowę zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego w administracji publicznej, systemu wczesnego ostrzegania oraz testowanie poziomu zabezpieczeń w postaci organizowanych cyklicznie ćwiczeń polegających na przeprowadzaniu kontrolowanych ataków symulujących działania cyberterrorystyczne.

W oparciu o Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 Ministerstwo Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego opracowało **Politykę Ochrony Cyberprzestrzeni**, mieszczącą się w grupie strategicznych dokumentów doprecyzowujących kierunki działań wskazanych w strategiach, programach rozwoju i innych dokumentach programowych. Polityka zwraca uwagę na konieczność zaktywizowania współpracy z przedsiębiorcami w ramach sektorów zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowego i transportowego oraz rekomenduje stworzenie wewnętrznych forów wymiany informacji i doświadczeń, a także zacieśnienie kontaktów z administracją publiczną. Omawiany dokument jest jednak bardzo ogólny i nie zawiera propozycji konkretnych działań, które należałoby podjąć.

Istotniejszym dokumentem, zawierającym bardziej szczegółowe informacje dotyczące spo-

sobów ochrony sieci teleinformatycznych, jest wspomniany już **Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)**. Dokument ten zawiera szereg dobrych praktyk, w konsekwencji których ochrona sieci może zostać wzmocniona. NPOIK zawiera również wiele inicjatyw o charakterze edukacyjnym, zważając na istniejące braki w tym zakresie. Należy w tym miejscu również wskazać na uzupełniające znaczenie krajowego planu zarządzania kryzysowego, wymieniającego zakłócenie funkcjonowania systemów łączności i systemów teleinformatycznych w ramach identyfikacji zagrożeń oraz wskazującego na podmioty odpowiedzialne za koordynację działań w przypadku cyberataków[25].

Finansowanie ochrony IK

Niezwykle istotnym zagadnieniem w kontekście zapewnienia cyberbezpieczeństwa IK, jest fakt, iż zgodnie z NPOIK działania z zakresu ochrony IK są finansowane ze środków własnych uczestników Programu na podstawie art. 6 ustawy o zarządzaniu kryzysowym. Co więcej, zarówno w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, jak i Polityce Ochrony Cyberprzestrzeni wskazuje się, iż koszty realizacji przewidzianych w tych dokumentach działań nie powinny implikować dodatkowych środków z budżetu państwa. Biorąc jednak pod uwagę fakt, iż infrastruktura teleinformatyczna, w tym infrastruktura wirtualna, stanowi infrastrukturę krytyczną kluczową dla bezpieczeństwa państwa i jego obywateli, obciążanie wyłącznie operatorów IK, którzy w przeważającej części należą do sektora prywatnego, kosztami wszystkich nakładów poniesionych w związku z utrzymaniem IK, może przekładać się na zmniejszenie poziomu ochrony IK, w tym cyberbezpieczeństwa IK.

Podkreślenia wymaga bowiem, iż o ile celem podmiotów publicznych będzie zapewnienie bezpieczeństwa państwa i obywateli w jak najwyższym stopniu, to podmioty należące do sektora prywatnego, w tym operatorzy IK będą dążyć przede wszystkim do uzyskania coraz lepszych wyników finansowych oraz obniżania kosztów. W konsekwencji, przedsiębiorcy zarządzający IK mogą ograniczać środki wydatkowane na zapewnienie ochrony infrastruktury teleinformatycznej, co zmniejszy poziom jej ochrony. Słabo zabezpieczona infrastruktura teleinformatyczna będzie łatwym celem wszelkich ataków, zarówno konwencjonalnych, jak i cyberataków.

Należy jednak zwrócić uwagę, iż NPOIK wskazuje instrumenty pośrednio finansujące działania z zakresu ochrony IK, to jest Decyzję Rady z dnia 12 lutego 2007 roku ustanawiającą na lata 2007-2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" – CIPS oraz krajowe programy operacyjne, w ramach których wydatkowane są środki z funduszy europejskich[26].

Wydaje się, iż wskazane w NPOIK środki finansowania nie są jednak wystarczające do zachęcenia operatorów IK z sektora prywatnego do podejmowania aktywnych działań w celu zapewnienia cyberbezpieczeństwa IK znajdującej się w jego posiadaniu.

Zmiany w ustawodawstwie UE

Dotychczasowe ochrona IK oparta była na dobrowolnej współpracy sektora publicznego i prywatnego, jak również została pozostawiona w zakresie szczegółowych regulacji państwom członkowskim UE. Niemniej jednak, w tym również ze względu na wzrost zagrożenia cyberatakami, w przyjętej – na dzień dzisiejszy – w pierwszym czytaniu przez Parlament Europejski Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (COM(2013) 48 final, 2013/0027 (COD) 7.2.2013)[27] można zauważyć dążenie do odgórnej regulacji kwestii bezpieczeństwa sieci i informacji.

Zasadniczym celem proponowanej dyrektywy jest bowiem zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci telekomunikacyjnych i przetwarzanych w nich informacji. W konsekwencji poziom gotowości i współpracy ma zostać ujednolicony we wszystkich państwach członkowskich. Cel ten, w ocenie projektodawcy, zostanie osiągnięty poprzez nałożenie na operatorów infrastruktury krytycznej i organy admi-

25 A. Kozłowski, *Cyberbezpieczeństwo infrastruktury energetycznej*, Policy Paper nr 7/2014

26 za A. Wiercińska-Krużewska, P. Gajek; *Prawne uwarunkowania ochrony infrastruktury krytycznej* [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, G. Abgarowicz, R. Antkiewicz, P. Ciepiela, M. Dyk, D. Dziwisz, Z. Fałek, P. Gajek, R. Kasprzyk, W. Kotłowski, M. Maj, A. Najgebauer, D. Pierzchała, A. Poniewierski, M. Pyznar, M. Ryba, K. Rzecki, J. Świątkowska, Z. Tarapata, A. Wiercińska-Krużewska

27 stan na dzień 2.04.2015 r.

nistracji publicznej obowiązku podjęcia działań mających na celu przeciwdziałanie zagrożeniom bezpieczeństwa oraz obowiązku zgłaszania poważnych incydentów właściwym organom administracji krajowej.

Założeniem dyrektywy jest zobowiązanie wszystkich państw członkowskich do ustanowienia właściwych organów ds. bezpieczeństwa sieci telekomunikacyjnych i informacji, w tym powołanie zespołów reagowania na incydenty komputerowe (CERT) podlegających bezpośrednio ustanowionym organom oraz przyjęcie krajowych strategii i planów współpracy w zakresie bezpieczeństwa sieci telekomunikacyjnych i informacji. Ponadto, dyrektywa ma zobowiązać właściwe organy krajowe do współpracy w oparciu o sieć umożliwiającą bezpieczną i skuteczną koordynację, w tym skoordynowaną wymianę informacji, jak również wykrywanie i reagowanie na poziomie UE. Państwa członkowskie powinny wymieniać się przez tę sieć informacjami i współpracować ze sobą w celu wykrywania i zwalczania zagrożeń oraz incydentów w zakresie bezpieczeństwa sieci telekomunikacyjnych i informacji. Działania miałyby być podejmowane na podstawie uprzednio opracowanego europejskiego planu współpracy w tym zakresie.

Przyszła dyrektywa ma również na celu zapewnienie rozwoju kultury wspierającej przeciwdziałanie zagrożeniom oraz wymiany informacji między sektorem prywatnym i publicznym. W szczególności, adresaci dyrektywy (w tym operatorzy IK) będą zobowiązani do dokonywania oceny zagrożeń, na jakie są narażeni, do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci telekomunikacyjnych i przetwarzanych w nich informacji, jak również do podejmowania środków zapobiegających incydentom dotyczącym infrastruktury teleinformatycznej oraz zmniejszający wpływ tych incydentów na działalność tych przedsiębiorców i zapewniający ciągłość świadczonych usług. Jednocześnie podmioty te zostaną zobowiązane do zgłaszania właściwym organom wszelkich incydentów zagrażających ich infrastrukturze teleinformatycznej oraz zakłócających świadczenie usług lub dostawę towarów o istotnym znaczeniu dla bezpieczeństwa państwa.

W literaturze wyrażana jest jednak wątpliwość, czy ten sposób zaktywizowania prywatnych operatorów IK do działania w zakresie ochrony IK nie przyczyni się do minimalistycznego podejścia ze strony tych podmiotów, tj. wypełniania obowiązków nałożonych przez prawo wyłącznie w wymaganym zakresie i w celu uniknięcia sankcji[28].

Postulaty zmian

Cyberbezpieczeństwo IK jest przedmiotem wielu regulacji zarówno na poziomie krajowym, jak i unijnym. Niemniej jednak, w przeważającej mierze są to regulacje zbyt ogólne, niezawierające propozycji szczegółowych praktycznych rozwiązań.

Wśród postulatów zmian obowiązujących obecnie przepisów prawnych, pojawia się w szczególności uzupełnienie definicji IK zawartej w ustawie o zarządzaniu kryzysowym w taki sposób, aby nie ulegało wątpliwości, iż obejmuje ona tzw. infrastrukturę wirtualną. Istotne może być również wprowadzenie regulacji nakładających szczegółowe obowiązki w zakresie cyberbezpieczeństwa na właścicieli i posiadaczy IK umożliwiające kontrolę poziomu ochrony IK, wdrażanie rozwiązań prewencyjnych oraz zapewnienie mechanizmów szybkiego reagowania na cyberataki przy jednoczesnym zapewnieniu ciągłości świadczonych usług.

W literaturze przedmiotu wskazuje się również na zapewnienie przez państwo sposobu, aby operatorzy IK z sektora prywatnego podejmowaliby aktywne działania w celu zapewnienia cyberbezpieczeństwa IK znajdującej się w ich posiadaniu. Wśród podstawowych bodźców motywujących przedsiębiorców wskazuje się możliwość ubiegania się o dofinansowanie części nakładów poniesionych w związku z utrzymaniem i zapewnieniem bezpieczeństwa IK. Niezwykle istotne jest także nawiązanie tzw. współpracy publiczno-prywatnej pomiędzy operatorami IK a administracją publiczną. W konsekwencji takiej współpracy przedsiębiorcy uzyskaliby dostęp do specjalistycznej wiedzy, mieliby możliwość identyfikacji najlepszych praktyk i standardów w zakresie ochrony IK, jak również wpływ na kształtowanie polityki państwa w zakresie ochrony IK[29].

Ponadto, konieczne jest także zacieśnienie opartej na zaufaniu współpracy zarówno pomiędzy operatorami IK a administracją państwową, jak również pomiędzy samymi przedsiębiorcami z danej branży, w tym również w celu wzmocnienia ochrony sieci komputerowych. Obiekty wchodzące w skład IK wymagają szczególnych standardów bezpieczeństwa, zarówno w zakresie

28 A. Wiercińska-Krużewska, P. Gajek; *Prawne…*

29 *Tamże*

ochrony przed atakami konwencjonalnymi jak i cyberatakami.

Konflikt lub nawet widmo konfliktu na arenie międzynarodowej, jak również rozwój działalności terrorystycznej zwiększa zagrożenie cyberprzestępczością. W obliczu ogromu strat, jakie może ponieść państwo i obywatele przez zaburzenie funkcjonowania IK, konieczne jest zwiększenie świadomości osób odpowiedzialnych, wzmocnienie działań prewencyjnych oraz przygotowanie ewentualnych odpowiednich (zarówno organizacyjno-prawnych jak i technicznych) rozwiązań, pozwalających na minimalizację skutków naruszenia cyberbezpieczeństwa.

II. Pojęcie „disaster recovery" systemów informatycznych dla Instytucji posiadających Infrastrukturę krytyczną

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590 z późn. zm.) definiuje pojęcie infrastruktury krytycznej jako 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 obejmuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych;

Biorąc pod uwagę nieograniczony postęp technologiczny – w praktyce wszystkie ze wskazanych powyżej i zdefiniowanych w ustawie o zarządzaniu kryzysowym obszarów funkcjonują bezpośrednio lub pośrednio w oparciu o zaawansowane rozwiązania technologiczne.

Ocena ryzyka wystąpienia zagrożeń dla infrastruktury krytycznej jest kwestią kluczową dla zapewnienia jej skutecznej ochrony i ciągłości działania. Należy stwierdzić iż, liczba scenariuszy potencjalnych zagrożeń jest nieskończona.

W przypadku zaawansowanych technologicznie systemów informatycznych, stanowiących kluczowy element infrastruktury krytycznej, zagrożenia te mają szczególny charakter. Należy wskazać, iż czasowa niedostępność, awaria krytyczna lub w skrajnym przypadku zniszczenie systemu może spowodować nieodwracalne skutki o charakterze ekonomicznym, organizacyjnym, ale co szczególnie istotne, wywierające bezpośredni wpływ na bezpieczeństwo państwa i obywateli.

Skuteczna ochrona infrastruktury informatycznej, ze szczególnym uwzględnieniem złożonych systemów informatycznych wymaga ścisłej współpracy sektora prywatnego oraz organów władzy publicznej. Podjęcie niezbędnych działań w szczególności w celu szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie wydaje się niemożliwe bez dokonania ścisłego podziału zadań, audytu, transferu wiedzy, opracowania szczegółowych planów ochrony.

W przypadku systemów informatycznych krytycznych z punktu widzenia funkcjonowania państwa, budowanych i rozwijanych na rzecz jednostek administracji publicznej potrzeba współpracy jest szczególnie widoczna. Architektura tych systemów powstaje przy ścisłej współpracy przedsiębiorstw prywatnych. Odpowiedni dobór i konfiguracja sprzętu, oprogramowania, stworzenie kompletnej dokumentacji technicznej i powykonawczej mają bezpośredni wpływ na ich bezpieczeństwo.

Zapewnienie bezpiecznego funkcjonowania infrastruktury krytycznej polega na analizie ryzyka wystąpienia zdarzeń powodujących zakłócenia w jej prawidłowym funkcjonowaniu, w tym w szczególności opracowanie alternatywnych (równoległych) metod działania.

W ramach kluczowych czynności dotyczących opracowania procedur distaster recovery należy wymienić w szczególności:

a) Czynności kontrolne i audyt

Czynności te polegają na weryfikacji zgodności rozwiązań organizacyjnych i technicznych dotyczących bezpiecznego zapewnienia usług ośrodka przetwarzania danych (data center) z wybranymi wymaganiami standardów. Standardami takimi są

- Norma TIA – 942 ”Telecommunications Infrastructure Standard for Data Centers”,
- Wytyczne SANS Institute odnośnie analizy lokalizacji data center,
- Wytyczne wydane przez Uptime Institute,
- Norma PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania,
- Norma ISO/IEC 27002 „Information technology – Security techniques – Code of practice for information security controls”.

b) Analiza dokumentacji

Analiza dokumentacji (w tym procedur IT), pozwalająca na weryfikację stosowanych środków kontroli i bezpieczeństwa. Jest to etap, na którym pojawiają się wstępne rekomendacje dalszych działań.

c) Analiza systemów

W ramach czynności poprzedzających opracowanie procedur niezbędna jest także **weryfikacja faktycznie funkcjonujących zabezpieczeń** w lokalizacjach krytycznych z punktu widzenia organizacji.

Weryfikacja powinna obejmować: główne lokalizacje, serwerownie, potencjalne lokalizacje zapasowe, zabezpieczenie stref chronionych, redundancje krytycznych mediów i zasobów, zabezpieczenie fizyczne pomieszczeń świadomość personelu w zakresie procedur bezpieczeństwa i ciągłości działania, zabezpieczenia technologiczne w obszarze ICT (Information and Communication Technologies).

W ramach przygotowania odpowiednich procedur w ramach disaster recovery niezbędne jest przeprowadzenie formalnej oceny dojrzałości wdrożonych w organizacji rozwiązań w obszarze zarządzania data center, w tym jego bezpieczeństwem i ciągłością działania, w szczególności w oparciu o wymagania norm ISO/IEC 27002, ISO/IEC 24762 oraz dobre praktyki w zakresie zarządzania infrastrukturą teleinformatyczną.

Poniższy wykres wskazuje wybrane obszary poddawane badaniu w ujęciu procentowym.

Wnioski i spostrzeżenia zebrane w trakcie analizy winny być podstawą **przygotowania szczegółowego raportu**. Dokument powinien zawierać ocenę stanu zabezpieczeń fizycznych, technicznych i organizacyjnych funkcjonujących w obszarze zarządzania data center, jego bezpieczeństwa i ciągłości działania. Ponadto, raport musi obejmować plan wdrożenia brakujących rozwiązań w obszarze zarządzania ciągłością działania oparty na liście rekomendacji z audytu. W ramach rekomendacji należy wyróżnić następujące grupy: przeprowadzenie niezbędnych szkoleń, wdrożenie dodatkowych procedur, instrukcji, przeprowadzenie szczegółowych testów bezpieczeństwa, w tym dotyczących systemów IT lub wdrożenia zabezpieczeń technicznych.

Wskazane powyżej obszary stanowią wybrany zbiór czynności w ramach ustalenia procedur disaster recovery w organizacji. W zależności od specyfiki danej jednostki, działania mogą obejmować inny w szczególności szerszy zakres.

Biorąc pod uwagę złożony charakter działań w ramach ustalenia odpowiednich procedur niezbędne jest współdziałanie specjalistów o zróżnicowanym zakresie posiadanych kompetencji, doświadczenia, wiedzy – prawników, informatyków, audytorów, specjalistów ds. ochrony danych osobowych, osób posiadających wiadomości specjalne charakterystyczne dla danej organizacji.

Właściwe podejście do zasygnalizowanych powyżej zagadnień, pozostaje w bezpośrednim związku z poziomem bezpieczeństwa infrastruktury krytycznej.

4. Bezpieczeństwo przestrzeni miejskiej w dobie terroryzmu nowej ery

(Opracowanie: *Krzysztof Mielech*, *Mateusz Kamm*, Kancelaria J. Bójko i Wspólnicy / LSW Leśnodorski Ślusarek i Wspólnicy)

I. Krajowe regulacje prawne, nowa sytuacja międzynarodowa

Polski nie można z całą pewnością nazwać krajem o wysokim stopniu zagrożenia atakiem terrorystycznym – m.in. dlatego, że od wielu lat nie doszło w naszym kraju do skutecznego zamachu terrorystycznego skierowanego przeciwko obiektom cywilnym czy instytucjom państwa. Ostatni taki przypadek miał miejsce 6 października 1971 r., kiedy bracia Jerzy i Ryszard Kowalczykowie wysadzili w powietrze aulę Wyższej Szkoły Pedagogicznej w Opolu – zamach miał podłoże polityczne, dokonano go w noc poprzedzającą uroczystą akademię z okazji święta Milicji Obywatelskiej i Służby Bezpieczeństwa. W wyniku zamachu nikt nie ucierpiał, jednak budynek został poważnie uszkodzony. Zjawisko drobnego terroru bombowego o podłożu kryminalnym jest jednak w Polsce znane, rocznie dochodzi nawet do kilkuset takich zamachów. Można też z całą pewnością stwierdzić, że aktywny udział Polski w zagranicznych misjach wojskowych oraz konflikt na wschodniej Ukrainie sprawiają, że potencjalne zagrożenie terrorystyczne wzrasta, o czym świadczą np. niedawno ujawnione plany przeprowadzenia w 2005 roku zamachów na terytorium Polski przez Al-Kaidę, nakierowanych przede wszystkim na obiekty amerykańskie.

Zadania związane z bezpieczeństwem antyterrorystycznym zostały w Polsce przydzielone do kilku instytucji.

Na poziomie strategicznym za koordynację działań organów państwa i administracji publicznej związanych z reakcją na sytuacje kryzysowe odpowiada powołane w 2007 r. Rządowe Centrum Bezpieczeństwa. Jest to instytucja rządowa o charakterze centrum zarządzania kryzysowego, odpowiedzialna za ograniczanie skutków zdarzeń o charakterze terrorystycznym i zapobieganie im. Do podstawowych zadań Rządowego Centrum Bezpieczeństwa należy m.in. zapewnienie odpowiedniej koordynacji polityki informacyjnej organów administracji publicznej w sytuacjach kryzysowych.

Główną państwową instytucją odpowiedzialną za ochronę antyterrorystyczną państwa na szczeblu operacyjnym jest Agencja Bezpieczeństwa Wewnętrznego. Do zakresu jej podstawowych działań należą działania prewencyjne związane z zabezpieczeniem miejsc szczególnie istotnych dla bezpieczeństwa państwa, w tym infrastruktury krytycznej.

Należy przypomnieć iż, zgodnie z ustawą o zarządzaniu kryzysowym z 26 kwietnia 2007 r., do infrastruktury krytyczne zalicza się m.in. systemy zaopatrzenia w energię i paliwa; łączności i usług teleinformatycznych; finansowe; zaopatrzenia w żywność i wodę; ochrony zdrowia; transportowe i komunikacyjne; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochrona infrastruktury krytycznej definiowana jest jako zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia elementów infrastruktury krytycznej w przypadku zagrożeń, w tym awarii i ataków. Zgodnie z zasadami przyjętymi przez Rządowe Centrum Bezpieczeństwa ochronę infrastruktury krytycznej stanowi suma działań w zakresie ochrony fizycznej, technicznej, osobowej, teleinformatycznej, prawnej i planów odtwarzania. Przez ochronę techniczną należy rozumieć zespół przedsięwzięć związanych z budową i eksploatacją obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony, mające na celu minimalizację ryzyka zakłóceń w funkcjonowaniu infrastruktury krytycznej. Techniczna ochrona infrastruktury krytycznej dotyczy nadzoru nad zgodnością konstrukcji budynków, urządzeń, instalacji i usług z obowiązującymi normami (np. budowlanymi) oraz innymi przepisami (np. przeciwpożarowymi), co ma zagwarantować jej bezpieczne użytkowanie. Ochrona techniczna oznacza

również wymienione w ustawie o ochronie osób i mienia techniczne zabezpieczenie obiektu, tzn. wykorzystanie do ochrony obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych i podobnych środków.

Na świecie, skrajnym przykładem reakcji na konieczność wzmocnienia środków umożliwiających efektywniejsze działanie w stanach kryzysowych był tzw. *Patriot Act*, ustawa podpisana 26 października 2001 r. przez prezydenta George Busha, dająca służbom amerykańskim prawo do podsłuchiwania rozmów telefonicznych, kontrolowania korespondencji, rewizji, wglądu w dane finansowe i medyczne, a także ułatwiająca zatrzymania, aresztowania i deportacje. Uprawnione jest więc stwierdzenie, że w wyniku zamachów na World Trade Center 11.09.2001 r. rozpoczęła się nowa era w walce z terroryzmem, w której zwłaszcza przestrzenie miejskie stały się przedmiotem bezprecedensowej fortyfikacji i militaryzacji. Zachodnie społeczeństwa uświadomiły sobie, że to właśnie infrastruktura (również krytyczna) i technologie przez nich stworzone, mogą zostać wykorzystane przeciwko nim jako najbardziej skuteczna broń. Zgodnie z przewidywaniami francuskiego teoretyka kultury i urbanisty, Paula Virilio, komunikacja masowa stała się bronią masowego rażenia, zdolną do eskalacji przemocy i wywołania chaosu na dużą skalę, zwłaszcza wobec błyskawicznego przesyłu informacji we współczesnym, interaktywnym społeczeństwie[30].

30 W tym kontekście należy szczególnie przywołać zamachy, do których doszło w Madrycie i Londynie. 11 marca 2004 r. w godzinach porannego szczytu w Madrycie doszło do ataku na podmiejskie pociągi kursujące pomiędzy stacjami Alcalá de Henares i Atocha. Zamach przeprowadzono za pomocą ukrytych w plecakach 13 zdalnie sterowanych bomb umieszczonych w bagażu podróżnych – w jego wyniku zginęło 191 osób. Jest to najtragiczniejszy zamach terrorystyczny w historii Hiszpanii. Nie odkryto powiązań sprawców z Al-Kaidą, zamach był zorganizowany przez grupę muzułmanów pochodzących z Maroka, Syrii i Algierii. 7 lipca 2005 r. o godz. 8:50 zaatakowano trzy pociągi londyńskiego metra, a godzinę później wysadzono w powietrze piętrowy autobus pełen ludzi. Łącznie zginęło 56 osób, kolejnych 700 zostało rannych – był to pierwszy w Europie samobójczy atak terrorystyczny, zamachowcami byli islamscy ekstremiści, zamieszkali w Wielkiej Brytanii Arabowie, członkowie komórki w Leeds, mający pośrednie powiązania z Al-Kaidą.

II. Terroryzm nowej ery – szczególna podatność metropolii

Terroryzm nowej ery (*New Age Terrorism*) zdefiniowany został przez Briana Micheala Jenkinsa. Cechuje go zwłaszcza: okrucieństwo i bezwzględność w atakowaniu celów cywilnych; posiadanie własnych, niezależnych od państw źródeł finansowania; sieciowy model organizacji; globalność w skali działania oraz efektywne wykorzystywanie nowych technologii medialnych. Natomiast Łukasz Kamieński w książce *Technologia i wojna przyszłości* (2009) zaproponował podział na terroryzm nowoczesny i ponowoczesny. Motywy terroryzmu ponowoczesnego są raczej religijne i fundamentalistyczne aniżeli polityczne i ideologiczne. *Modus operandi* ponowoczesnego terroryzmu sprawia również, że wybór ofiar jest mniej przemyślany, gdyż terrorystom głównie chodzi o jak najbardziej nieograniczony efekt i szeroko zakrojone skutki zamachu. Obecnie celem przemocy terrorystów stała się przemoc sama w sobie, w większym stopniu zaczęto też wykorzystywać nowoczesne technologie, a finansowania terrorystów wspierane jest w przeważającym stopniu przez międzynarodową siatkę zorganizowanej przestępczości.

Najczęściej przywoływane powody szczególnej wrażliwości i podatności dużych miast[31] (obszarów metropolitalnych, stolic państw rozwiniętych, itp.) na ataki terrorystyczne są następujące:

- skupiają najważniejsze, najbardziej witalne funkcje polityczne i gospodarcze – są ośrodkami władzy i głównymi węzłami w globalnej sieci przepływu informacji i kapitału,
- to w nich znajdują się ikoniczne budynki i obiekty o charakterze symbolicznym (dlatego też stanowią najbardziej atrakcyjne medialnie cele ataku),

31 Wydarzenia ostatnich lat pokazują jednak, że komórki międzynarodowej sieci islamskiego terroryzmu atakują również wybrane cele o charakterze symbolicznym, szczególnie obiekty reprezentujące USA oraz Izrael, a także świątynie i synagogi. Atakowano m.in. ambasady Izraela w Buenos Aires (1992 r.) i Londynie (1994 r.), budynek towarzystwa izraelsko-argentyńskiego w Buenos Aires (1994 r.), synagogę na wyspie Jerba w Tunezji (2002), izraelski hotel Paradise w Kenii (2002 r.), amerykański konsulat w Karaczi (2002). Do preferowanych celów ataków terrorystycznych ze strony islamistów zaczęły się również zaliczać kurorty, w których przebywają zachodni turyści: zamachy w Bali w latach 2002 i 2005 r., ataki na Hotel Mariott w Dżakarcie (2003 r.), hotel Hilton Taba w Egipcie (2004 r.), Sharm El-Sheikh w Egipcie (2005 r.), Dahab w Egipcie (2006 r.). W listopadzie 1997 r. w wyniku tzw. masakry w Luksorze zginęło 62 Turystów – w jego efekcie, doszło do załamania ruchu turystycznego, wieloletniej stagnacji budownictwa i przemysłu turystycznego, który stanowi dla Egiptu jednym z głównych źródeł dochodów. Należy również wspomnieć o ataku terrorystycznym, który miał miejsce 18 marca 2015 roku w Muzeum Bardo w Tunisie – w tym zamachu zginęły 24 osoby (w tym trzech Polaków), ok. 50 osób zostało rannych. Odpowiedzialność za ten zamach wzięło na siebie Państwo Islamskie.

– śródmieścia dużych miast grupują ogromną liczbę budynków i ludzi, skoncentrowanych na niewielkiej powierzchni terenu (atak może skutkować dużymi stratami ludzkimi i materialnymi przy zaangażowaniu stosunkowo niewielkich środków),
– anonimowość, wielokulturowość i wielorasowość mieszkańców zapewniają terrorystom swobodę działania i większą możliwość ukrycia się,
– wysoko rozwinięte sieci transportu, komunikacji i łączności miast ułatwiają przygotowanie, przeprowadzenie ataku oraz sprawną ucieczkę sprawców z miejsca zdarzenia,
– przestrzeń publiczna dużych miast, dworce i środki masowego transportu stanowią obiekty trudne do ochrony i efektywnego zabezpieczenia przed atakiem terrorystycznym,
– ataki na cele cywilne nie wymagają użycia technologii militarnej i mogą być przeprowadzane z użyciem najprostszych środków (np. bomby domowej konstrukcji),
– stała obecność mediów w miastach zapewnia natychmiastowe rozpowszechnienie informacji, a tym samym osiągniecie podstawowego celu terroryzmu, jakim jest natychmiastowy przekaz medialny, która zwielokrotnia psychologiczne, społeczne i polityczne skutki terroryzmu.

Koncepcją miejskiego bezpieczeństwa zajmował się Michel Foucault w jednym z cyklów (1977–78) swoich słynnych wykładów w College de France. Poza szerokimi związkami z wypracowaną przez niego koncepcją biopolityki, model miejskiego bezpieczeństwa okazuje się ustanawiać wyraźne związki z mechanizmami kształtowania bezpieczeństwa w przestrzeniach miejskich: „Dobra organizacja miasta polega właśnie na tym, że bierze się pod uwagę zdarzenia możliwe. Innymi słowy, można tu mówić, jak sądzę, o technice nakierowanej na problem bezpieczeństwa, czyli w gruncie rzeczy, problem serii". Foucault dalej stwierdza: „Bezpieczeństwo urządza otoczenie pod kątem zdarzeń lub elementów możliwych, serii, którym trzeba będzie nadać pewien kształt, uwzględniając złożone i zmienne warunki. Odsyła ono do wymiaru czasu i przypadkowości, które należy wpisać w daną przestrzeń. Jest to chyba właśnie to, co nazywa się środowiskiem: przestrzeń, w której pojawiają się serie przypadkowych elementów"[32].

32 Zob. M. Foucault, Bezpieczeństwo, terytorium, populacja: wykłady w Collège de France 1977-1978, tłum. Michał Herer, Warszawa 2010

III. Miejska architektura jako przestrzeń obronna

Jedna z pierwszych kluczowych idei poprawiania miejskiego bezpieczeństwa przedstawiona została przez amerykańskiego architekta Oscara Newmana w wydanej przez niego w 1972 r. książce *Defensible Space. Crime Prevention through Urban Design*. Autor wskazał m.in. jak określone zabiegi projektowe i manipulacje przestrzenne mogą integrować lokalną społeczność, pozwalać jej kontrolować zamieszkiwane terytorium i tym samym wpływać na poziom bezpieczeństwa. Newman między innymi dowodził, że to ludzie obserwujący przechodniów z okien sowich domów są najlepszym gwarantem bezpieczeństwa. Swoją koncepcję organizacji przestrzeni nazwał *Defensible Space* („przestrzeń obronna"). Według Newmana przestrzeń obronna jest takim modelem środowiska zamieszkania, który ogranicza zagrożenia kryminalne „poprzez stworzenie przestrzeni fizycznej wyrażającej określoną strukturę społeczną, która nad daną przestrzenią panuje, kontroluje ją i zapewnia ochronę". Podstawowym ogniwem tego systemu są mieszkańcy, wzajemnie dbający o swoje bezpieczeństwo. Bezpieczne środowisko zamieszkania jawi się więc jako zjawisko psychofizyczne, w którym dużą role odgrywa dobry projekt, zapewniający mieszkańcom poczucie własności, kontroli, wspólnoty i bezpieczeństwa. Newman zauważył też silny związek pomiędzy postrzeganiem danego terytorium jako własnego i dbałością o nie a stanem bezpieczeństwa okolicy. Tym samym, im model zabudowy jest gęstszy i znajdujący się bliżej centrum miasta, tym trudniej jest wydzielić potencjalnie bezpieczne sąsiedzkie terytorium – w takim przypadku prywatne kończy się już na progu mieszkania, a dalej zaczyna się ziemia niczyja, najczęściej anonimowa lub wroga – mieszkańcy czują się wtedy mniej odpowiedzialni za swoją okolicę i oczekują zwiększonych wysiłków ze strony administracji, władz lokalnych lub publicznych.

Newman zauważył ponadto, że architekt dysponuje środkami, dzięki którym możliwe jest definiowanie granic przestrzeni, w celu przypisania ich określonym grupom mieszkańców. Postulował zwłaszcza, aby w budynkach o dużej liczbie mieszkańców tworzyć halle wejściowe, wspólne tylko dla kilku mieszkań, a także aby

przestrzeń wokół poszczególnych budynków dzielić przy użyciu symbolicznych lub fizycznych przegród, tworząc tym samym obszary łatwiejsze do identyfikacji, zagospodarowania i kontroli potencjalnie sprawowanej przez poszczególne grupy mieszkańców. Ponadto zwrócił uwagę na praktyczność przecinania ulic tranzytowych przez strefy piesze, co może znacznie ułatwiać tworzenie nowych skwerów i ulicznych placów.

Zgodnie z koncepcją Newmana, do większości przestępstw popełnianych w budynkach lub na terenie osiedli dochodzi w miejscach ukrytych przed wzrokiem mieszkańców, takich jak windy, klatki schodowe, nieoświetlone zaułki czy uliczne zakamarki.

Koncepcja przestrzeni obronnej ma więc za zadanie m.in. wzmacnianie poczucia własności i przynależności do lokalnej wspólnoty sąsiedzkiej za pomocą wydzielania i oznaczania granic pomiędzy przestrzenią publiczną i sąsiedzką; dąży też do bardziej efektywnego wykorzystania elementów projektu i cech środowiska w celu zagwarantowania wyższego stopnia naturalnego nadzoru; sprzyjające jest też łączenie zespołów mieszkaniowych z tymi fragmentami miasta, które są uznane za bezpieczne.

Co szczególnie ważne, kwestia kształtowania przestrzeni obronnej rozwijana jest nadal jako jedna ze strategii kryminalnej prewencji sytuacyjnej, gdzie za główny środek przeciwdziałania przestępczości uznaje się kształtowanie odpowiednich warunków środowiskowych i zabezpieczanie przestrzeni poprzez urządzenia kontroli dostępu, bariery i wzmocnienia.

Najprawdopodobniej z teorii Newmana wywodzi się kryminologiczna teoria rozbitego okna (*Broken Window Theory*), spopularyzowana w latach 80. przez burmistrza Nowego Jorku Rudolpha Giulianiego – zakładała ona, iż jedną ze skutecznych metod walki z przestępczością jest dbałość o stan środowiska zabudowanego.

W XXI wieku, to zwłaszcza atak terrorystyczny na WTC doprowadził do ponownego podjęcia tematu przestrzeni obronnej. W artykule opublikowanym wkrótce po zamachu w New York Times pt. *A City Transformed: Designing Defensible Space* autorstwa Anthony'ego Vidlera czytamy: "Atak terrorystyczny na World Trade Center podgrzewa publiczną debatę o tym, czy należy zmienić nasze doświadczenie i sposób budowy przestrzeni publicznych. Czy najbardziej charakterystyczne zasoby miasta, jakimi są jego gęstość, koncentracja i monumentalne budowle – nadal mają sens? Czy pragnienie stworzenia przestrzeni obronnej radykalnie zmieni model miasta, jaki znamy?".

Obecnie, przykładem skrajnej przestrzennej polityki antyterrorystycznej są działania podejmowane przez Izrael – polegają one na parcelacji i izolacji poszczególnych, co jest realizowane przy pomocy systemu barier, murów i wyburzeń zabudowy. Celowo doprowadza się też do blokowania komunikacji pomiędzy poszczególnymi obszarami. Utworzono w ten sposób wielowymiarowy system przestrzennej separacji, kontroli i dominacji, określany jako *securityscape* – pejzaż bezpieczeństwa, w którym polityczna i militarna przemoc oraz różne taktyki obronne i zabezpieczenia obejmują wszystkie sfery życia. Wydaje się, że odpowiedzią na wzrost zagrożenia terrorystycznego współczesnych miasta może być umiejętne stosowanie zasad prewencji sytuacyjnej, podnoszenie zdolności do zapobiegania niebezpieczeństwu i doskonalenie szybkiej reakcji służb ratunkowych na potencjalne zagrożenia i ataki. Kompleksowo implementowane systemy zabezpieczeń antyterrorystycznych, które zostaną zintegrowane z krajobrazem miejskim i będą sprawnie współpracować z innymi systemami miejskiej infrastruktury, mają szansę stać się ważnym ogniwem w systemie bezpieczeństwa publicznego. Wielowymiarowy, lecz stosunkowo mało ingerujący w przestrzeń miejską system zabezpieczeń (np. inteligentny miejski monitoring, sprawne wykorzystanie elementów małej architektury i zabezpieczeń strefowych) może się przyczynić do ograniczenia ryzyka w zakresie bezpieczeństwa publicznego, a nawet doprowadzić do rewitalizacji przestrzeni śródmiejskiej[33].

33 Zob. A. Jasiński, Architektura w czasach terroryzmu: miasto, przestrzeń publiczna, budynek, Warszawa 2013

IV. Polityka bezpieczeństwa w polskim systemie planowania i zagospodarowania przestrzennego

Podstawowym aktem prawnym z zakresu planowania i zagospodarowania przestrzennego jest ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym („u.p.z.p."). Uchwalany przez gminę miejscowy plan zagospodarowania przestrzennego jest jednym z najistotniejszych mechanizmów prawnych umożliwiających skuteczną realizację polityki bezpieczeństwa i obronności państwa. W odróżnieniu od planu zagospodarowania przestrzennego województwa, jak również koncepcji zagospodarowania przestrzennego kraju, jedynie miejscowy plan zagospodarowania przestrzennego uchwalany przez gminę stanowi źródło powszechnie obowiązującego prawa na danym terytorium (art. 14 ust. 8 u.p.z.p.), może więc m.in. wprowadzać ograniczenia w zakresie wykonywania prawa własności nieruchomości, wykluczać bądź ograniczać w możliwości realizacji określonych inwestycji, jak również może przewidywać inne rozwiązania mające na celu zapewnienie bezpieczeństwa i obronności państwa poprzez np. poprzez tworzenie obszarów specjalnych. Sporządzanie miejscowego planu zagospodarowania przestrzennego nie jest, co do zasady, obowiązkowe. Według danych Ministerstwa Infrastruktury i Rozwoju, na koniec 2012 r. jedynie ok. 28% powierzchni kraju zostało objętych miejscowymi planami zagospodarowania przestrzennego. Dlatego też znaczna część inwestycji na terenie Polski w dalszym ciągu jest realizowana na podstawie decyzji o lokalizacji inwestycji celu publicznego oraz decyzji o warunkach zabudowy. Co więcej, w stosunku do niektórych obszarów o szczególnym znaczeniu dla bezpieczeństwa i obronności kraju (tj. w stosunku do terenów zamkniętych), realizacja inwestycji może nastąpić wyłącznie w oparciu o odpowiednie decyzje administracyjne – decyzje o lokalizacji inwestycji celu publicznego lub decyzji o warunkach zabudowy. Z punktu widzenia inwestora, jak również z punktu widzenia podmiotów odpowiedzialnych za zapewnienie ochrony terenów oraz posadowionej na nich infrastruktury kluczowej ze względów obronności i bezpieczeństwa państwa (w tym infrastruktury krytycznej), istotna jest prawidłowa identyfikacja ograniczeń wynikających z przepisów regulujących planowanie i zagospodarowanie przestrzenne, jak również wykorzystywanie możliwości uczestnictwa w procesie kształtowania ładu przestrzennego, w sposób niesprzeczny z wymogami bezpieczeństwa publicznego (np. przewidziany w art. 17 i n. u.p.z.p. tryb składania uwag i wniosków do projektu miejscowego planu).

Miejscowy plan zagospodarowania przestrzennego jako instrument realizacji polityki bezpieczeństwa publicznego

Jako akt prawa miejscowego o charakterze powszechnie obowiązującym, miejscowy plan zagospodarowania przestrzennego powinien dążyć do urzeczywistnienia ładu przestrzennego, którego jednym z istotnych elementów są potrzeby obronności i bezpieczeństwa państwa (art. 1 ust. 2 pkt. 8 u.p.z.p.). Potrzeby obronności i bezpieczeństwa są realizowane w miejscowym planie zagospodarowania przestrzennego m.in. poprzez ustalanie przeznaczenia terenów uznanych za szczególnie ważne dla bezpieczeństwa i obronności państwa; ustalenie linii rozgraniczających tereny o różnym przeznaczeniu; ustalenie zasad kształtowania zabudowy oraz wskaźników zagospodarowania terenu; wprowadzenie zakazu zabudowy i ustalenie szczególnych warunków zagospodarowania terenów oraz wprowadzenie ograniczeń w użytkowaniu terenów.

Najdalej idącym środkiem ingerencji miejscowego planu zagospodarowania przestrzennego w instytucje prawa prywatnego, jakim jest prawo własności nieruchomości, jest zakaz zabudowy (art. 15 ust. 2 pkt. 9 u.p.z.p.). Nie ulega wątpliwości, że wprowadzenie zakazu zabudowy na określonych obszarach może służyć celom zapewnienia bezpieczeństwa oraz obronności państwa – jak bowiem wskazano w Koncepcji Przestrzennego Zagospodarowania Kraju 2030, istotnym kierunkiem rozwoju planowania przestrzennego w Polsce jest dokonywanie „*rezerwacji terenów dla celów strategicznych, zapewniających możliwość budowy lub rozbudowy infrastruktury, obiektów i baz wojskowych.*" Wprowadzenie ograniczenia w formie zakazu zabudowy należy rozumieć szeroko, bowiem zgodnie z definicją zawartą w art. 3 pkt. 6 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane („Prawo budowlane"), budowa oznacza nie tylko wykonanie obiektu budowalnego

w określonym miejscu, ale również zakaz rozbudowy, odbudowy i nadbudowy obiektu.

Kolejnym istotnym z punktu widzenia zapewnienia obronności i bezpieczeństwa państwa instrumentem prawnym, jest określanie w miejscowym planie zagospodarowania przestrzennego zasad modernizacji, rozbudowy i budowy systemów komunikacji i infrastruktury technicznej. Przez pojęcie „infrastruktury technicznej" należy rozumieć drogi, a także wybudowane pod ziemią, na ziemi lub nad ziemią przewody lub urządzenia wodociągowe, kanalizacyjne, ciepłownicze, elektryczne, gazowe i telekomunikacyjne. Te urządzenia i budowle mogą zostać uznane za obiekty szczególnie ważne dla bezpieczeństwa i obronności, co uzasadnia objęcie ich szczególną ochroną, zgodnie z treścią art. 143 ust. 2 ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami („u.g.n."). W rozporządzeniu Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, do przedmiotowych obiektów zaliczono m.in. wszelkie obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, morskiego i wodnego śródlądowego, drogownictwa, kolejnictwa i łączności oraz ośrodki dokumentacji geodezyjnej i kartograficznej, a także inne obiekty znajdujące się we właściwości organów administracji rządowej, organów jednostek samorządu terytorialnego, formacji, instytucji państwowych oraz przedsiębiorców i innych jednostek organizacyjnych, których zniszczenie lub uszkodzenie mogące stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa. Szczególna ochrona obiektów jest przygotowywana przez organy, instytucje, formacje, przedsiębiorców lub jednostki organizacyjne, w których właściwości znajdują się obiekty (§ 4 ust. 4 rozporządzenia).

Decyzja o lokalizacji inwestycji celu publicznego, decyzja o warunkach zabudowy

W związku z nieobowiązywaniem na zdecydowanej większości obszarów kraju postanowień miejscowych planów zagospodarowania przestrzennego, ustalenie warunków zabudowy umożliwiających realizację polityki bezpieczeństwa i obronności państwa odbywa się często na podstawie decyzji administracyjnych, tj. decyzji o ustaleniu lokalizacji inwestycji celu publicznego (art. 50 u.p.z.p.) lub decyzji o warunkach zabudowy (art. 59 u.p.z.p.). W przypadku gdy na danym terenie nie obowiązuje miejscowy plan zagospodarowania przestrzennego, wskazane wyżej decyzje stają się wówczas mechanizmami służącymi do realizacji polityki obronności i bezpieczeństwa publicznego, stąd zostały pokrótce opisane niżej.

Uzyskanie decyzji o lokalizacji inwestycji celu publicznego jest zastrzeżone dla inwestycji celu publicznego, przez co należy rozumieć działania o znaczeniu lokalnym (gminnym) i ponadlokalnym (powiatowym, wojewódzkim i krajowym), a także krajowym (obejmującym również inwestycje międzynarodowe i ponadregionalne), bez względu na status podmiotu podejmującego te działania oraz źródła ich finansowania, stanowiące realizację celów, o których mowa w art. 6 u.g.n. Przepis ten zawiera zamknięty katalog inwestycji uznawanych za cel publiczny i zalicza do nich m.in. budowę i utrzymywanie publicznych urządzeń służących do zaopatrzenia ludności w wodę, gromadzenia, przesyłania, oczyszczania i odprowadzania ścieków oraz odzysku i unieszkodliwiania odpadów, w tym ich składowania, a także budowę oraz utrzymywanie obiektów i urządzeń służących ochronie środowiska, zbiorników i innych urządzeń wodnych służących zaopatrzeniu w wodę regulacji przepływów i ochronie przed powodzią. Wynika z tego, że co do zasady możliwość realizacji inwestycji polegającej na budowie (a także rozbudowie, czy modernizacji) infrastruktury istotnej ze względów bezpieczeństwa i obronności, wymaga wydania decyzji o ustaleniu lokalizacji inwestycji celu publicznego, nawet jeśli inwestorem jest podmiot prywatny. Inwestycje niemające charakteru inwestycji celu publicznego wymagają wydania decyzji o warunkach zabudowy. Uzyskanie tej decyzji wymaga spełnienia bardziej rygorystycznych warunków, co świadczy o przyznaniu prymatu w uzyskiwaniu zezwolenia inwestycjom publicznie użytecznym, w tym też inwestycjom kluczowym ze względów bezpieczeństwa i obronności państwa.

W konsekwencji, w stosunku do niektórych obszarów jedyną możliwością ustalenia warunków zabudowy i realizacji inwestycji jest uzyskanie opisanych wyżej decyzji. Dotyczy to również terenów zamkniętych, ponieważ postanowienia miejscowego planu nie mogą określać przeznaczenia terenu na tych obszarach. Definicję terenu zamkniętego zawiera art. 2 pkt. 9 ustawy z dnia

17 maja 1989 r. Prawo geodezyjne i kartograficzne („u.p.g.k."), zgodnie z którym przez tereny zamknięte rozumie się *„tereny o charakterze zastrzeżonym ze względu na obronność i bezpieczeństwo państwa, określone przez właściwych ministrów i kierowników urzędów centralnych*". Tereny zamknięte są ustalane przez właściwych ministrów i kierowników urzędów centralnych w drodze decyzji. W decyzji tej określane są także granice terenu zamkniętego (art. 4 ust. 2a u.p.g.k.). Jedynym kryterium wydania decyzji ustalającej teren zamknięty jest więc znaczenie tego terenu ze względu na obronność i bezpieczeństwo państwa.

Odnosząc się zaś do kwestii prowadzenia inwestycji na terenach zamkniętych należy wspomnieć o wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 marca 2007 r. IV SA/Wa 256/07, którego teza stanowi: *„Nie ma przepisów prawa, które by wprowadzały wprost zakazy realizacji określonych inwestycji na terenach zamkniętych. Ponieważ tereny takie są tworzone ze względu na obronność i bezpieczeństwo państwa, przy wydawaniu decyzji o warunkach zabudowy organ winien więc dokonać, oceny czy realizacja określonej inwestycji nie będzie godzić w cel, dla którego strefa została ustanowiona*." Co do zasady nie ma więc prawnych ograniczeń w realizacji inwestycji na terenach zamkniętych, o ile nie będzie ona godzić w bezpieczeństwo i obronność państwa. Dokonując więc „zamknięcia" danego obszaru, wprowadza się kryterium dopuszczalności inwestycji, jakim jest nietworzenie zagrożenia dla bezpieczeństwa i obronności państwa. Instytucja terenów zamkniętych jest więc istotnym mechanizmem w realizacji polityki bezpieczeństwa publicznego i ochrony znajdującej się na danym obszarze infrastruktury. W przypadku procesu inwestycyjnego, istotnego znaczenia nabiera więc właściwa identyfikacja uwarunkowań lokalnych z zakresu bezpieczeństwa i obronności, których dokładna analiza powinna nastąpić już na etapie planowania inwestycji.

Kierunki zmian legislacyjnych

Ogólne kierunki zmian i rozwoju w kwestii obronności i bezpieczeństwa w aspekcie organizacji przestrzeni miejskiej przedstawiono w Koncepcji Przestrzennego Zagospodarowania Kraju 2030 – dokumentu przyjętego przez Radę Ministrów 13 grudnia 2011 r. („KPZK"). W dokumencie tym stwierdzono, że polityka przestrzenna powinna tworzyć warunki dla uwzględniania wymagań obronności i bezpieczeństwa państwa we wszystkich opracowaniach planistycznych z zakresu zagospodarowania przestrzennego – dotyczy to w szczególności przestrzeni miejskich. Zwrócono również uwagę na konieczność podejmowania działań z zakresu polityki przestrzennego zagospodarowania kraju w taki sposób, aby umożliwiać zapewnienie odpowiednich zdolności obronnych państwa np. poprzez nadawanie nowym strukturom przestrzennym pożądanych walorów obronnych oraz poprawianie warunków dla realizacji zadań obronnych na pozostałych obszarach, usprawnienie procedury lokalizacji planowanych inwestycji o znaczeniu dla bezpieczeństwa i obronności, a także dokonywanie rezerwacji terenów dla celów strategicznych, zapewniających możliwość budowy lub rozbudowy infrastruktury, obiektów i baz wojskowych. W zakresie pożądanych rozwiązań dla poszczególnych gałęzi infrastruktury w KPZK wskazano, że wymogi obronności powinny być respektowane przy kształtowaniu sieci osadniczej i kształtowaniu rozmieszczenia przemysłu o znaczeniu obronnym, w rozwoju infrastruktury technicznej (rurociągi i magistrale powinny być rozmieszczane bez dysproporcji i z maksymalnym rozśrodkowaniem). W odniesieniu do transportu w KPZK podkreślono, że wskazane jest tworzenie układów obwodnicowych, rozmieszczanie stacji rozrządowych i kontenerowych z dala od ośrodków miejskich, budowanie awaryjnych przepraw przez rzeki, unikanie podwieszania pod dużymi mostami sieci spełniających ważne funkcje gospodarcze. Z powyższego wynika, że znaczna część infrastruktury powinna być lokalizowana z dala od miast i „przenoszona" na obszary peryferyjne, poza aglomeracjami. Ponadto przewidziano, że w łączności i energetyce ważne jest kształtowanie sieci telekomunikacyjnej i energetycznej o konfiguracji gwiaździstej – wielobocznej, tworzenie samodzielnych regionalnych podsystemów energetycznych, wielokrotnie sprzężonych z systemem ogólnokrajowym, zapewnienie ważnym odbiorcom zasilania awaryjnego.

Wobec powyższego, uprawnione jest stwierdzenie, że znaczenie mechanizmów planowania i zagospodarowania przestrzennego wpływających na ład przestrzenny, w tym zabudowę w ośrodkach miejskich, w celu realizacji polityki bezpieczeństwa i obronności państwa, stale wzrasta.

JBW KANCELARIA

Kancelaria J. Bójko i Wspólnicy
www.kancelariajbw.com.pl

ul. Targ Rybny 11a/4, 80-838 Gdańsk
tel.: + (48) 58 305 46 63

+ (48) 664 114 082