DOI:10.17951/k.2023.30.2.85-106

ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. XXX, 2 SECTIO K 2023

Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Wydział Politologii i Dziennikarstwa,
Instytut Nauk o Polityce i Administracji

WOJCIECH ZIĘTARA

ORCID ID: 0000-0002-1990-6342

Wymiar formalnoprawny infrastruktury krytycznej na poziomie krajowym i europejskim

Formal and Legal Dimension of Critical Infrastructure at Polish and European Level

ABSTRAKT

Po rozpoczęciu przez Federację Rosyjską agresji na Ukrainę w 2022 r. zaatakowano ukraiński system infrastruktury krytycznej w celu jego całkowitego lub częściowego zniszczenia. W odpowiedzi na te ataki władze ukraińskie zapowiedziały odbudowę systemu ochrony infrastruktury na podstawie rozwiązań prawnych Unii Europejskiej. W artykule omówiono zagadnienia infrastruktury krytycznej, zarówno na płaszczyźnie europejskiej, jak i polskiej. W polskim systemie prawnym obowiązują przepisy z 2007 r., natomiast w europejskim – dyrektywa z 2008 r., niemniej jednak w 2022 r. dokonano zmiany przepisów prawnych, które zostaną implementowane do krajowych systemów prawnych w 2024 r. W tekście jako cel przyjęto dokonanie analizy treści przepisów aktów prawnych w zakresie infrastruktury krytycznej w Polsce oraz w Unii Europejskiej. Analizie towarzyszą pytania badawcze dotyczące sposobu definiowania podstawowych pojęć i terminów w obu systemach prawnych oraz wzajemnych relacji obu systemów. Nawiązano do metody badania dokumentów pozwalającej na dokonanie analizy aktów prawnych oraz przeprowadzenie analizy porównawczej. Państwa członkowskie uzyskały pozycję nadrzędną wobec organów europejskich, jednak rosnące zagrożenia naturalne i antropologiczne oraz proces pogłębiania europejskiej integracji politycznej wpłynęły na stopniową zmianę sposobu myślenia o infrastrukturze krytycznej. Pozycja organów Unii Europejskiej na podstawie dyrektywy z 2022 r. została zdecydowanie wzmocniona wobec państw członkowskich.

Słowa kluczowe: Polska, Unia Europejska, bezpieczeństwo, infrastruktura krytyczna, systemy infrastruktury krytycznej

WSTĘP

24 lutego 2022 r. Federacja Rosyjska rozpoczęła pełnoskalową agresję na Ukrainę. Przebieg wojny ma swoją dynamikę pozwalającą na wyodrębnienie jej etapów, wśród których można wskazać na rozpoczęcie jesienią 2022 r. zmasowanych ataków na infrastrukturę krytyczną (dalej: ik). Największe ataki za pomocą rakiet i dronów przeprowadzono 15 i 23 listopada 2022 r. i miały bezpośredni związek z sytuacją na froncie, ale także spadkiem temperatur powietrza i wzrostem zapotrzebowania na energię elektryczną w sezonie jesienno-zimowym. Celem działań Rosjan było całkowite zniszczenie lub znaczące ograniczenie funkcjonowania systemu energetycznego Ukrainy. Ataki w dużym stopniu unaoczniły kwestię wpływu systemu infrastruktury krytycznej na system bezpieczeństwa państwa i chociaż zagadnienie to jest już przedmiotem działań państw od wielu lat, to jednak dopiero zakres agresji rosyjskiej wprowadził w szerokim stopniu zagadnienie infrastruktury krytycznej do agendy medialnej i świadomości społecznej Polaków. A wraz z nią pytanie o stopień bezpieczeństwa infrastruktury krytycznej w polskim systemie bezpieczeństwa narodowego. Jednocześnie wraz z rozwojem działań rosyjskich wobec ukraińskiej infrastruktury krytycznej pojawiła się także informacja, że władze Ukrainy zamierzają zbudować system ochrony infrastruktury krytycznej w nawiązaniu do przepisów prawnych i dobrych praktyk Unii Europejskiej. Mając powyższe na uwadze, należy uznać zarówno europejski, jak i polski system infrastruktury krytycznej za istotny element bezpieczeństwa Europy. Dlatego celem niniejszego artykułu jest dokonanie analizy treści przepisów aktów prawnych w obszarze ik w Polsce na poziomie przede wszystkim ustawowym oraz w Unii Europejskiej na poziomie dyrektyw. Analizie towarzyszą pytania badawcze o to, w jaki sposób są definiowane podstawowe pojęcia i terminy w zakresie ik na obu poziomach oraz czy są względem siebie komplementarne, czy jeden system jest nadrzędny względem drugiego systemu prawnego. W artykule nawiązano do metody badania dokumentów pozwalającej na dokonanie analizy aktów prawnych oraz przeprowadzenie analizy porównawczej.

Należy podkreślić, że dotychczasowe analizy podstawy prawnej obu poziomów w polskiej literaturze przedmiotu nawiązywały do aktów prawnych z 2007 i 2008 r. Jest to w pełni zrozumiałe w kontekście dat poszczególnych publikacji na temat infrastruktury krytycznej [Radziejewski 2014: 35–49; Lazari 2014: 1–7; Długosz 2015: 13–18, 35–43, 46–42; Żuber, Smolarek 2016: 12–25; Setola, Luiijf, Theocharidou 2017: 9–12; Jakubiak 2018: 165–175; Sobolewski, Michailiuk 2019: 30–31, 404–409; Molendowska, Ostrowska, Górski 2021: 21–32, 76–86]. Tymczasem niniejszy artykuł obejmuje zmiany wprowadzone w europejskim systemie prawnym w 2022 r., które staną się częścią krajowych systemów prawnych do 2024 r.

INFRASTRUKTURA KRYTYCZNA W KRAJOWYM SYSTEMIE PRAWNYM

Podstawą prawną pozwalającą określić funkcjonowanie infrastruktury krytycznej w polskim systemie bezpieczeństwa są art. 3 pkt 2 i 3 oraz art. 6 Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej: uzk) [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym]. W powyższych artykułach zdefiniowano infrastrukturę krytyczną wraz z wyszczególnieniem jej systemów oraz wskazano na obowiązek jej ochrony w celu zachowania ciągłości funkcjonowania. W myśl powyższych przepisów infrastruktura krytyczna jest rozumiana 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" [art. 3 pkt 2 uzk]. W powyższej definicji można wyodrębnić i podkreślić trzy elementy konstytutywne infrastruktury krytycznej: po pierwsze, infrastruktura jest złożona z systemów tworzących sieć, czyli mamy do czynienia z obiektami, które są ze sobą zespolone, a nie są pojedynczymi punktami niepowiązanymi ze sobą; po drugie, infrastruktura krytyczna ma istotne znaczenie dla bezpieczeństwa narodowego, czyli założono, że pewne obiekty mają znaczenie nadrzędne względem pozostałych i dodatkowo muszą być one powiązane z wymiarem bezpieczeństwa; i po trzecie, infrastruktura krytyczna pozwala funkcjonować administracji publicznej, instytucjom i przedsiębiorcom, czyli w myśl rozumowania *a contrario* każde zakłócenie ciągłości infrastruktury przekłada się na obniżenie dobrego poziomu funkcjonowania administracji publicznej i pozostałych podmiotów wchodzących w skład sektorów państwa. W związku z powyższym, infrastruktura krytyczna powinna być właściwie zabezpieczona i chroniona. Znalazło to rozwinięcie w dalszych przepisach uzk, w których przyjęto, że infrastruktura krytyczna podlega ochronie rozumianej jako „działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizację ich skutków oraz szybkiego odtwarzania tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie" [art. 3 pkt 3 uzk]. W ustawie założono możliwość wystąpienia sytuacji, które wpłyną na ciągłość funkcjonowania infrastruktury, ale w związku z tym istotnym elementem stała się konieczność zdefiniowania ryzyka wystąpienia wszelkich zdarzeń, które mogą tę ciągłość funkcjonowania ograniczyć lub przerwać, a dodatkowo, aby przyjąć rozwiązania, które powyższym incydentom będą zapobiegały, eliminowały je, ograniczały lub szybko usuwały w przypadku przerwania ciągłości działania. Znalazło to rozwinięcie w art. 6 uzk, w którym zdefiniowano zadania z zakresu ochrony infrastruktury krytycznej, do których zaliczono: gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej; opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej; odtwarzanie infrastruktury krytycznej; współpracę między administracją publiczną a właści-

cielami oraz posiadaczami samoistnymi i zależnymi infrastruktury krytycznej. Na powyższe podmioty będące częścią sektorów państwa nałożono obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej, w tym przygotowanie i wdrażanie planów ochrony infrastruktury krytycznej oraz utrzymanie systemów rezerwowych pozwalających na podtrzymanie ik do czasu pełnego odtworzenia. Z kolei na Radę Ministrów nałożono obowiązek określenia w drodze rozporządzenia szczegółów dotyczących wspomnianych wyżej planów ochrony ik.

Dopełnieniem definicji infrastruktury krytycznej jest wskazanie jedenastu systemów, które ją współtworzą. Należą do niej systemy: 1) zaopatrzenia w energię, surowce energetyczne i paliwa; 2) łączności; 3) sieci teleinformatycznych; 4) finansowe; 5) zaopatrzenia w żywność; 6) zaopatrzenia w wodę; 7) ochrony zdrowia; 8) transportowe; 9) ratownicze; 10) zapewniające ciągłość działania administracji publicznej; 11) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[1].

Tabela 1. Systemy infrastruktury krytycznej na poziomach krajowym i europejskim

System infrastruktury krytycznej	Poziom krajowy	Poziom europejski	
		2008	2022
Zaopatrzenia w energię, surowce energetyczne i paliwa	+	+	+
Łączności	+	–	+
Sieci teleinformatycznych	+	–	+
Finansowy	+	–	+
Zaopatrzenia w żywność	+	–	+
Zaopatrzenia w wodę	+	–	+

[1] Art. 3 pkt 2 uzk. Trybunał Konstytucyjny na rozprawie 21 kwietnia 2009 r. wydał wyrok w sprawie art. 3 pkt 2 uzk i orzekł o jego zgodności z art. 2 Konstytucji Rzeczypospolitej Polskiej z 1997 r. (KRP) (demokratyczne państwo prawne urzeczywistniające zasady sprawiedliwości społecznej) oraz, że nie jest niezgodny z art. 22 (ograniczanie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny) w związku z art. 31 ust. 3 KRP (ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw). Wnioskodawca zarzucił, że wprowadzone przepisy naruszają zasadę poprawnej legislacji, ponieważ uniemożliwiają wskazanie podmiotów zaliczanych do infrastruktury krytycznej. Ponadto podniesiono we wniosku, że na właścicieli i samoistnych posiadaczy systemów (obiektów, urządzeń) infrastruktury krytycznej nałożono obowiązek naruszający wolność działalności gospodarczej. Ponadto wskazano, że nałożenie pewnych zadań, a w związku z tym ograniczeń powinno zostać dokonane w formie odrębnej ustawy. Sędziowie nie podzieli powyższych zarzutów i w wyroku wskazali, że definicja infrastruktury krytycznej jest oparta na terminach dosyć powszechnie obowiązujących, jakkolwiek nie do końca precyzyjnych. Wyjaśniono, że definicja ik została poszerzona o enumeratywnie wyliczone systemy, które pozwalają na dokładne określenie zakresu podmiotowego na podstawie ustaw, które wchodzą w skład tychże systemów. Jednocześnie stwierdzono, że przepis nie nakłada ograniczeń wolności działalności gospodarczej w sposób naruszający zasadę proporcjonalności. W uzk nie wprowadzono przepisów, które zawierałyby sankcje wobec podmiotów, które nie zastosują się do dyspozycji zawartych w przepisach i odmówią współpracy z administracją publiczną. Wyrok Trybunału Konstytucyjnego z dnia 21 kwietnia 2009 r. sygn. akt K 50/07 [Dz. U. 2009, Nr 65, poz. 553].

System infrastruktury krytycznej	Poziom krajowy	Poziom europejski	
		2008	2022
Ochrony zdrowia	+	–	+
Transportowy	+	+	+
Ratowniczy	+	–	+
Zapewniający ciągłość działania administracji publicznej	+	–	+
Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	+	–	+
Przestrzeni kosmicznej	–	–	+

+ system infrastruktury krytycznej występuje w systemie prawnym.

– system infrastruktury krytycznej nie został zdefiniowany w systemie prawnym.

Źródło: Opracowanie własne na podstawie art. 3 pkt 2 i 3 oraz art. 6 Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, załącznikiem III Dyrektywy Rady Unii Europejskiej 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony oraz art. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.

Istotnym elementem definiowania ik było wprowadzenie do ustawy terminu europejskiej infrastruktury krytycznej (dalej: eik). W związku z przyjęciem Dyrektywy Rady Unii Europejskiej 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (dalej: deik)[2] znowelizowano uzk. W myśl uzk termin europejskiej infrastruktury krytycznej oznacza: „systemy oraz wchodzące obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie”[3]. Powyższa definicja jest tożsama z definicją infrastruktury krytycznej w zakresie przedmiotowym, natomiast wprowadziła dwie istotne modyfikacje w zakresie podmiotowym i terytorialnym. Europejska infrastruktura krytyczna obejmuje dwa systemy energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportowy, podczas gdy polska infrastruktura krytyczna aż jedenaście systemów (patrz tabela 1). Ponadto infrastrukturę krytyczną uznano za europejską jedynie w przypadku wystąpienia wpływu na co najmniej dwa państwa Unii Europejskiej, natomiast polska infrastruktura krytyczna swoim zasięgiem terytorialnym obejmuje obszar Rzeczypospolitej Polskiej.

[2] [Dz. Urz. UE L 345/75 z 23.12.2008].
[3] [Art. 3 pkt. 2a uzk].

Uzupełnieniem krajowego systemu prawnego w zakresie infrastruktury krytycznej są akty wykonawcze[4] oraz Narodowy Program Ochrony Infrastruktury Krytycznej (dale: NPOIK). Za przygotowanie NPOIK odpowiedzialne jest Rządowe Centrum Bezpieczeństwa (dalej: RCB). Program powstaje we współpracy z ministrami i kierownikami organów centralnych administracji publicznej w zakresie działów bezpieczeństwa narodowego, a jest przyjmowany przez Radę Ministrów.

Pierwszy NPOIK został przyjęty w 2013 r. i składał się z dokumentu głównego oraz dwóch załączników: Charakterystyki systemów infrastruktury krytycznej oraz Standardów służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej w formie dobrych praktyk i rekomendacji. Kryteria pozwalają wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej. Po 2013 r. program przyjęto jeszcze czterokrotnie w latach 2015, 2018, 2020 oraz 2023 r. Należy jednak podkreślić, że wszystkie późniejsze wersje NPOIK były przyjmowane w postaci tekstu jednolitego, stanowiącego nawiązanie do treści programu z 2013 r. i zawierającego jedynie niewielkie zmiany treści (patrz tabela 2) oraz dwóch załączników, z którego tylko jeden dotyczący Standardów był udostępniany, natomiast drugiemu załącznikowi nadawano klauzulę dokumentu zastrzeżonego.

Tabela 2. Wybrane zmiany w dokumencie głównym Narodowego Programu Ochrony Infrastruktury Krytycznej w latach 2013–2023

Rok Programu / Punkt Programu		2013	2015	2018	2020	2023
Dokument główny		X	X	X	X	X
Charakterystyka systemów infrastruktury krytycznej		X	X Zastrzeżone	X Zastrzeżone	X Zastrzeżone	X Zastrzeżone
Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej		X	X	X	X	X
Zakres Zidentyfikowana infrastruktura krytyczna		X	X	X	X	X
Cel Poprawa bezpieczeństwa infrastruktury krytycznej		X	X	X	X	X
Priorytety	Wzrost świadomości, wiedzy i kompetencji uczestników	X	–	–	–	–
	Współpraca uczestników	X	X	X	X	X
	Identyfikacja zależności pomiędzy systemami	–	X	X	X	X
	Ocena ryzyka zakłócająca infrastrukturę krytyczną	–	X	X	X	X

[4] Jako wybrane obowiązujące akty wykonawcze w polskim systemie prawnym w zakresie infrastruktury krytycznej na podkreślenie zasługują Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. 2010 Nr 83 Poz. 542), Rozporządzenie Prezesa Rady Ministrów z dnia 26 kwietnia 2021 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej (Dz. U. 2021 Poz. 793).

Punkt Programu / Rok Programu		2013	2015	2018	2020	2023
Zasady	Współodpowiedzialność	X	X Filar 1	X Filar 1	X Filar 1	X Filar 1
	Współpraca	X	X Filar 2	X Filar 2	X Filar 2	X Filar 2
	Zaufanie	X	X Filar 3	X Filar 3	X Filar 3	X Filar 3
	Proporcjonalność	X	X	X	X	X
	Uznanie różnic między systemami	X	X	X	X	X
	Wiodąca rola ministra odpowiedzialnego za system	X	X	X	X	X
	Równość operatorów	X	X	X	X	X
	Komplementarność	X	X	X	X	X
Adresaci	Administracja publiczna	X	X	X	X	X
	Operatorzy	X	X	X	X	X
	Przedsiębiorcy	X	–	–	–	–
	Pozostałe Podmioty Gospodarcze i Organizacje	–	X	X	X	X
	Środowisko naukowe	X	X	X	X	X
	Społeczeństwo	X	X	X	X	X

NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej. „X" – punkt wystąpił w Programie, „-" – punkt nie wystąpił w Programie.

Źródło: Opracowanie własne na podstawie Narodowych Programów Ochrony Infrastruktury Krytycznej z 2013, 2015, 2018, 2020 i 2023 r. *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, 2013, 2015, 2018, 2020, 2023, http://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (dostęp: 20.07.2023).

Zakres programu obejmuje zidentyfikowaną infrastrukturę krytyczną umieszczoną w wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład systemów infrastruktury krytycznej. Celem NPOIK jest stworzenie warunków poprawy bezpieczeństwa ik, który przełoży się na osiągnięcie celu nadrzędnego, jakim jest podniesienie poziomu bezpieczeństwa Polski. W dokumencie z 2013 r. zdefiniowano dwa działania priorytetowe, do których zaliczono: podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu oraz zainicjowanie skutecznej współpracy między uczestnikami Programu. Programy przyjmowane w późniejszych latach obejmowały już trzy priorytety, wśród których utrzymano jako działanie współpracę między uczestnikami Programu, ale dodatkowo wprowadzono dwa nowe działania obejmujące identyfikację zależności między systemami oraz dokonanie oceny ryzyka zakłócającego ciągłość systemów infrastruktury krytycznej. W dokumencie głównym zdefiniowano także zasady programu. Łącznie wskazano osiem zasad, ale trzy z nich uznano za nadrzędne wobec pozostałych i od 2015 r. nadano im dodatkowe określenie filarów zasad programu. Zaliczono do nich zasady: współodpowiedzialności, współpracy i zaufania. Zasadę współodpowiedzialności zdefiniowano jako wspólne dążenie wszystkich uczestników do

poprawy bezpieczeństwa infrastruktury krytycznej. Zasada współpracy oznacza, że uczestnicy programu wykonują określone, zbieżne i wzajemnie uzupełniające się zadania w celu osiągnięcia celu wynikającego z zasady współodpowiedzialności. Trzecim filarem jest zasada zaufania rozumiana w taki sposób, że motywacją działalności uczestników jest realizacja zasady współodpowiedzialności. Zestaw zasad programu ochrony infrastruktury krytycznej uzupełniono pięcioma dodatkowymi regułami: proporcjonalności i działań opartych na ocenie ryzyka, definiującej działania w programie przez zastosowanie adekwatnego poziomu ryzyka; uznania różnic pomiędzy poszczególnymi systemami infrastruktury krytycznej, rozumianej w ten sposób, że pomimo pewnych podobieństw o specyfice systemów świadczą unikalne cechy, które je definiują i odróżniają od pozostałych systemów; kluczowej roli ministra odpowiedzialnego za dany system infrastruktury krytycznej przyznającą nadrzędną pozycję w systemie organów administracji publicznej oraz pozostałych podmiotów programu ministrowi nadzorującemu dany system; równości operatorów zakładającej, że pomimo występowania zarówno podmiotów państwowych, jak i prywatnych w realizacji programu wszyscy uczestnicy są traktowani równorzędnie i są sobie równi; komplementarności, czyli zastosowania wielu rozwiązań mogących przyczynić się do wzrostu poziomu bezpieczeństwa infrastruktury krytycznej. Zakres podmiotowy NPOIK został określony stosunkowo szeroko, ponieważ uwzględniono w nim przede wszystkim organy administracji publicznej odpowiedzialnej za systemy infrastruktury krytycznej oraz operatorów infrastruktury krytycznej, ale także przedsiębiorców ze względu na wysoki stopień współzależności sektorów gospodarki oraz członków środowiska naukowego realizującego badania naukowe i wdrożeniowe w zakresie bezpieczeństwa infrastruktury krytycznej oraz całego społeczeństwa, ponieważ przyjęto w programie, że każdy obywatel korzysta z poszczególnych systemów w swoim codziennym życiu. Począwszy od programu z 2015 r. kategorię przedsiębiorców zastąpiono grupą Podmiotów gospodarczych i Organizacji, co jeszcze rozszerzyło zakres katalogu podmiotów.

Zapowiedziano, że NPOIK będzie aktualizowany co najmniej co dwa lata, ale cele przyjęte w 2013 r. miały zostać osiągnięte w ciągu sześciu lat, natomiast cele z 2015 r. miały być wdrażane przez okres czterech lat z zachowaniem terminów z 2013 r. Jednocześnie podkreślono, że wzrost poziomu bezpieczeństwa infrastruktury krytycznej jest procesem zakładającym stopniową realizację celów[5].

Nawiązując do jednej z zasad programu określających nadrzędną pozycję ministrów wobec pozostałych uczestników programu, wskazano ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej (patrz tabela 3). W 2013 r. za systemy odpowiadali samodzielnie: Minister Administracji i Cyfryzacji za system łączności, system sieci teleinformatyczny oraz system zapewniający ciągłość działania administracji publicznej; Minister Finansów za system finansowy; Minister

[5] [Rządowe Centrum Bezpieczeństwa 2013: 6–10; 2015: 8–12; 2018: 8–12; 2020: 8–12; 2023: 8–12].

Tabela 3. Ministrowie odpowiedzialni za poszczególne systemy infrastruktury krytycznej w latach 2013–2023

Rok Programu / System infrastruktury krytycznej	2013	2015	2018	2020	2023
	Odpowiedzialny Minister				
Zaopatrzenia w energię, surowce energetyczne i paliwa	Minister Gospodarki Minister Skarbu Państwa	Minister Energii	Minister właściwy ds. energii Minister właściwy ds. gospodarki złożami kopalin	Minister właściwy ds. energii Minister właściwy ds. gospodarki złożami kopalin Minister właściwy ds. aktywów państwowych	Minister właściwy ds. energii Minister właściwy ds. gospodarki złożami kopalin Minister właściwy ds. aktywów państwowych
Łączności	Minister Administracji i Cyfryzacji	Minister Cyfryzacji Minister Infrastruktury i Budownictwa	Minister właściwy ds. informatyzacji Minister właściwy ds. łączności	Minister właściwy ds. informatyzacji Minister właściwy ds. łączności	Minister właściwy ds. informatyzacji Minister właściwy ds. łączności
Sieci teleinformatycznych	Minister Administracji i Cyfryzacji	Minister Cyfryzacji	Minister właściwy ds. informatyzacji	Minister właściwy ds. informatyzacji	Minister właściwy ds. informatyzacji
Finansowy	Minister Finansów	Minister Finansów	Minister właściwy ds. budżetu Minister właściwy ds. finansów publicznych Minister właściwy ds. instrumentów finansowych	Minister właściwy ds. budżetu Minister właściwy ds. finansów publicznych Minister właściwy ds. instrumentów finansowych	Minister właściwy ds. budżetu Minister właściwy ds. finansów publicznych Minister właściwy ds. instrumentów finansowych
Zaopatrzenia w żywność	Minister Rolnictwa i Rozwoju Wsi	Minister Rolnictwa i Rozwoju Wsi	Minister właściwy ds. rolnictwa Minister właściwy ds. rynków rolnych	Minister właściwy ds. rolnictwa Minister właściwy ds. rynków rolnych	Minister właściwy ds. rolnictwa Minister właściwy ds. rynków rolnych
Zaopatrzenia w wodę	Minister Środowiska; Minister Administracji i Cyfryzacji	Minister Środowiska	Minister właściwy ds. gospodarki wodnej	Minister właściwy ds. gospodarki wodnej	Minister właściwy ds. gospodarki wodnej

Rok Programu / System infrastruktury krytycznej	2013	2015	2018	2020	2023
	Odpowiedzialny Minister				
Ochrony zdrowia	Minister Zdrowia	Minister Zdrowia	Minister właściwy ds. zdrowia	Minister właściwy ds. zdrowia	Minister właściwy ds. zdrowia
Transportowy	Minister Transportu, Budownictwa i Gospodarki Morskiej	Minister Infrastruktury i Budownictwa Minister Gospodarki Morskiej i Żeglugi Śródlądowej	Minister właściwy ds. transportu Minister właściwy ds. gospodarki morskiej	Minister właściwy ds. transportu Minister właściwy ds. gospodarki morskiej	Minister właściwy ds. transportu Minister właściwy ds. gospodarki morskiej
Ratowniczy	Minister Spraw Wewnętrznych	Minister Spraw Wewnętrznych i Administracji	Minister właściwy ds. wewnętrznych	Minister właściwy ds. wewnętrznych	Minister właściwy ds. wewnętrznych
Zapewniający ciągłość działania administracji publicznej	Minister Administracji i Cyfryzacji	Minister Cyfryzacji	Minister właściwy ds. informatyzacji	Minister właściwy ds. informatyzacji	Minister właściwy ds. informatyzacji
Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	Minister Środowiska	Minister Środowiska	Minister właściwy ds. środowiska	Minister właściwy ds. klimatu	Minister właściwy ds. klimatu

W Programach w 2013 i 2015 r. wskazano konkretnych Ministrów, podczas gdy począwszy od 2018 r. zaczęto wskazywać Ministrów właściwych ze względu na poszczególne działy administracji publicznej.

Źródło: Opracowanie własne na podstawie Narodowych Programów Ochrony Infrastruktury Krytycznej z 2013, 2015, 2018, 2020 i 2023 r. *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, 2013, 2015, 2018, 2020, 2023, http://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (dostęp: 20.07.2023).

Rolnictwa i Rozwoju Wsi za system zaopatrzenia w żywność; Minister Zdrowia za system ochrony zdrowia; Minister Transportu, Budownictwa i Gospodarki Morskiej za system transportowy; Minister Spraw Wewnętrznych za system ratowniczy; Minister Środowiska za system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych. Wspólną odpowiedzialność nałożono na Ministra Gospodarki i Ministra Skarbu Państwa w zakresie systemu zaopatrzenia w energię, surowce energetyczne i paliwa oraz na Ministra Środowiska z Ministrem Administracji i Cyfryzacji za system zaopatrzenia w wodę[6]. W 2015 r. dokonano pewnych zmian w wykazie ministrów odpowiedzialnych za wybrane systemy infrastruktury krytycznej. W czterech przypadkach zachowano ciągłość nadzoru nad systemami przez Ministrów Finansów; Rolnictwa i Rozwoju Wsi; Zdrowia oraz Środowiska (w zakresie systemu substancji chemicznych i promieniotwórczych). Pozostałe systemy objęto odpowiedzialnością nowych ministerstw. Samodzielny nadzór objęli: Minister Energii w zakresie systemu zaopatrzenia w energię; Minister Cyfryzacji – system sieci teleinformatycznych oraz system administracji publicznej; Minister Środowiska – system zaopatrzenia w wodę; Minister Spraw Wewnętrznych i Administracji – system ratowniczy, natomiast nadzór wspólny sprawowali: Minister Cyfryzacji i Minister Infrastruktury i Budownictwa za system łączności oraz Minister Infrastruktury i Budownictwa z Ministrem Gospodarki Morskiej i Żeglugi Śródlądowej – system transportowy[7]. W 2018 r. zmieniono sposób określania ministrów odpowiedzialnych za nadzór nad systemami infrastruktury krytycznej, wskazując działy administracji publicznej[8]. Za system zaopatrzenia w energię, surowce energetyczne i paliwa odpowiedzialność otrzymał minister właściwy posiadający zakres kompetencyjny ds. energii; ds. gospodarki złożami kopalin. System łączności jest nadzorowany przez ministra właściwego ds. informatyzacji. Za system sieci teleinformatycznych odpowiada minister właściwy ds. informatyzacji, natomiast system finansowy to właściwość rzeczowa ministra właściwego ds. budżetu, ministra właściwego ds. finansów publicznych, ministra właściwego ds. instytucji finansowych. Z kolei system zaopatrzenia w żywność przydzielono ministrowi właściwemu ds. rolnictwa, ministrowi właściwemu ds. rynków rolnych, natomiast nad systemem zaopatrzenia w wodę władztwo rozciąga minister właściwy ds. gospodarki wodnej. Nad systemem ochrony zdrowia odpowiedzialność sprawuje minister właściwy ds. zdrowia. System transportowy to zakres obowiązków ministra właściwego ds. transportu, ministra właściwego ds. gospodarki morskiej. Nad systemem ratowniczym nadzór sprawuje minister właściwy ds. wewnętrznych, natomiast nad systemem zapewniającym ciągłość działalności administracji publicznej nadzorowanie powierzono ministrowi

[6] [Rządowe Centrum Bezpieczeństwa 2013: 17].

[7] [Rządowe Centrum Bezpieczeństwa 2013: 17].

[8] W celu utrzymania trwałości określonych ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej, począwszy od 2018 r. wprowadzono w nazewnictwie działy administracji publicznej określone w art. 5 Ustawy z dnia 4 września 1997 r. o działach administracji publicznej [Dz. U. 1997 Nr 141 poz. 943 z późn. zm.].

właściwemu ds. informatyzacji. I wreszcie nad jedenastym systemem substancji chemicznych i promieniotwórczych nadzór powierzono ministrowi właściwemu ds. środowiska[9]. W 2020 r. w wykazie ministrów odpowiedzialnych za poszczególne systemy ik dokonano tylko dwóch zmian. Za system substancji chemicznych i promieniotwórczych odpowiedzialnym uczyniono ministra właściwego ds. klimatu, natomiast za system zaopatrzenia w energię współodpowiedzialność, obok ministra właściwego ds. energii, ministra właściwego ds. gospodarki złożami kopalin, uzyskał minister właściwy ds. aktywów państwowych[10]. W 2023 r. utrzymano wszystkie dotychczasowe zakresy nadzoru ministrów nad systemami infrastruktury krytycznej[11].

INFRASTRUKTURA KRYTYCZNA W SYSTEMIE PRAWA UNII EUROPEJSKIEJ

Na poziomie europejskim prace nad przyjęciem regulacji prawnych rozpoczęły się w 2004 r. jako przede wszystkim odpowiedź na akty terrorystyczne. W toku prac rozszerzono ryzyka o zagrożenia wywołane działaniami człowieka, zagrożenia technologiczne i katastrofy naturalne.

Rada Unii Europejskiej w art. 2 lit. a i b deik zdefiniowała zarówno infrastrukturę krytyczną, jak i europejską infrastrukturę krytyczną. W myśl powyższego przepisu infrastrukturą krytyczną jest „składnik, system lub część infrastruktury zlokalizowana na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji". Można wskazać, że definicje infrastruktury krytycznej obowiązujące w polskim i europejskim systemie prawnym są zbliżone, niemal tożsame. W obu definicjach podkreślono funkcjonowanie infrastruktury krytycznej jako holistycznego systemu mającego wpływ na państwo i jego obywateli.

Europejska infrastruktura krytyczna, jak już zostało to zasygnalizowane wyżej, to „infrastruktura krytyczna zlokalizowana na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie". Zakres terytorialny został określony stosunkowo wąsko, zważywszy na to, że systemy wpływające tylko na dwa państwa zostały uznane za systemy europejskie. Oznacza to, że poziom europejski mogły już uzyskać systemy obejmujące państwa sąsiedzkie.

Zgodnie z deik na państwa członkowskie nałożono obowiązek rozpoznania europejskiej infrastruktury krytycznej, a Komisja Europejska mogła jedynie pomóc państwom członkowskim w zadaniu rozpoznania. Jednak może się to odbyć do-

[9] [Rządowe Centrum Bezpieczeństwa 2018: 18].
[10] [Rządowe Centrum Bezpieczeństwa 2020: 18].
[11] [Rządowe Centrum Bezpieczeństwa 2023: 18].

piero na wniosek państw członkowskich. Przy wyznaczaniu eik państwa powinny uwzględnić dwa rodzaje kryteriów: przekrojowe i sektorowe. Kryteria przekrojowe dzielą się na trzy kategorie: kryterium ofiar w ludziach oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych; kryterium skutków ekonomicznych oceniane w odniesieniu do wielkości strat ekonomicznych lub pogorszenia towarów lub usług, w tym także potencjalnych skutków ekologicznych oraz kryterium skutków społecznych oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych i zakłóceń codziennego życia. Kryteria sektorowe uwzględniają cechy charakterystyczne dla poszczególnych sektorów i są oceniane według ich specyfiki.

W załączniku III deik w ramach dwóch sektorów wskazano także podsektory. W sektorze energii wyodrębniono trzy podsektory, natomiast w sektorze transportu pięć podsektorów. Są to odpowiednio podsektor energii elektrycznej obejmujący infrastrukturę i urządzenia do wytwarzania i przesyłania energii elektrycznej w odniesieniu do dostaw energii elektrycznej, podsektor ropy naftowej obejmujący produkcję, rafinację, przetwarzanie, magazynowanie i przesyłanie rurociągami ropy naftowej oraz podsektor gazu obejmujący produkcję, rafinację, przetwarzanie, magazynowanie i przesyłanie gazociągami gazu oraz terminale skroplonego gazu ziemnego. W sektorze transportowym zdefiniowano podsektory transportu drogowego, transportu kolejowego, transportu lotniczego, transportu wodnego śródlądowego oraz żeglugę oceaniczną, żeglugę morską bliskiego zasięgu i porty. Jednocześnie podkreślono, że wskazany zakres sektorów może zostać rozszerzony o sektory dodatkowe, a poziom priorytetowy w ewentualnym uzupełnieniu wykazu nadano sektorowi teleinformatycznemu (ICT).

Ponadto na każde państwo członkowskie nałożono obowiązek przygotowania planu ochrony infrastruktury oraz przedstawiania sprawozdań Komisji Europejskiej co dwa lata. Przyjęto także możliwość powołania urzędników łącznikowych ds. ochrony jako pełniących funkcje punktu kontaktowego między właścicielem lub operatorem eik a państwem członkowskim, a jednocześnie zobowiązano państwa członkowskie do wyznaczenia punktów kontaktowych ds. ochrony europejskiej infrastruktury krytycznej.

Dyrektywa zobowiązała państwa członkowskie do implementowania jej przepisów do krajowych systemów prawnych do 2012 r. Należy podkreślić, że przepisy europejskie zachowały zasadę subsydiarności, nakazując państwom członkowskim dokonanie analizy sytuacji w dwóch sektorach i zdefiniowanie europejskiej infrastruktury krytycznej w porozumieniu z drugimi państwami członkowskimi. Wszystkie zadania związane z realizacją deik przyznano państwom członkowskim. Działania Komisji ograniczono do możliwości wspierania właścicieli lub operatorów eik, ale tylko za pośrednictwem państw członkowskich, w wymiarze najlepszych praktyk i metod oraz dodatkowych szkoleń i wymiany informacji w zakresie innowacji technicznych na rzecz ochrony infrastruktury krytycznej.

Dyrektywa z 2008 r. jest dokumentem złożonym z 14 artykułów i trzech załączników, a więc stosunkowo zwięzłym i niedługim. Dodatkowo zwyczajem europejskiego systemu prawnego zapowiedziano dokonanie przeglądu obowiązujących przepisów po 2012 r. Przeprowadzono taką analizę przepisów w 2019 r., nawiązując do nowych zagrożeń i wyzwań w zakresie bezpieczeństwa europejskiego i stwierdzono, że dotychczasowe rozwiązania prawne są niewystarczające i wymagają zmiany sposobu myślenia o europejskiej infrastrukturze krytycznej. Wynikało to z faktu, że przepisy z 2008 r. koncentrowały się na ochronie europejskiej infrastruktury krytycznej, podczas gdy występujące w coraz większym stopniu współzależności gospodarcze w Unii Europejskiej wymuszają podniesienie odporności właścicieli lub operatorów ik. Powinni oni rozwijać zdolności do zapobiegania incydentom zakłócającym ciągłość ich funkcjonowania. Mając na uwadze powyższe założenie, do europejskiego systemu prawnego wprowadzono Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającą dyrektywę Rady 2008/114/WE[12] (dalej: dopk).

Wśród uwarunkowań wprowadzenia nowych przepisów wskazano ewolucję zagrożeń hybrydowych i terrorystycznych oraz zwiększone ryzyko wystąpienia klęsk żywiołowych w związku ze zmianą klimatu. Ponadto uznano, że dotychczasowe rozwiązania prawne nie sprzyjały spójności przepisów o europejskiej infrastrukturze krytycznej w państwach członkowskich i zapowiedziano wprowadzenie rozwiązań określających minimalne standardy w tym zakresie. Podkreślono także rosnące współzależności pomiędzy poszczególnymi sektorami ik i dlatego zapowiedziano rozszerzenie dotychczasowej listy sektorów i podsektorów ik. Jednocześnie wyjaśniono, że nowe przepisy nie obejmą kwestii cyberbezpieczeństwa, ponieważ została ona szczegółowo znormalizowana w ramach Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego poziomu cyberbezpieczeństwa na terytorium Unii[13] (dwpc). Także spod zakresu dopk wyłączono podmioty administracji publicznej, funkcjonujące w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, a także misje dyplomatyczne i konsularne państw członkowskich w państwach trzecich.

Dyrektywa z 2022 r. jest aktem złożonym i bardziej rozbudowanym aniżeli dyrektywa z 2008 r., ponieważ składa się z 29 artykułów, 7 rozdziałów i 1 załącznika. Tymczasem w deik nie było w ogóle wyodrębnionych rozdziałów[14].

[12] [Dz. Urz. UE L 333/164 z 27.12.2022].

[13] [Dz. Urz. UE L 333/80 z 27.12.2022].

[14] W Dyrektywie z 2022 r. rozdziały noszą tytuły: Przepisy ogólne, Krajowe ramy dotyczące odporności podmiotów kluczowych, Odporność podmiotów krytycznych, Podmioty krytyczne o szczególnym znaczeniu europejskim, Współpraca i sprawozdawczość, Nadzór i egzekwowanie przepisów, Akty delegowane i akty wykonawcze, Przepisy końcowe.

Tabela 4. Zestawienie wybranych różnic w przepisach prawa na poziomie dyrektyw z 2008 i 2022 r. w zakresie europejskiej infrastruktury krytycznej

Zakres	Dyrektywa z 2008 r.	Dyrektywa z 2022 r.
Liczba sektorów	2	11
Nazwa podmiotów	Operator	Podmiot krytyczny
Cel wprowadzenia przepisów	Ochrona infrastruktury krytycznej przez państwa członkowskie na poziomie krajowym	Uzyskanie zdolności przez państwa członkowskie do zapobiegania incydentom zakłócającym ciągłość funkcjonowania europejskiej infrastruktury krytycznej
Organ wprowadzany przepisami	Urzędnik łącznikowy ds. ochrony	Grupa ds. Odporności Podmiotów Krytycznych
Pozycja państwa członkowskiego	Nadrzędna	Istotna
Pozycja Komisji Europejskiej	Doradcza	Koordynująco-doradcza
Liczba państw, w których muszą być świadczone usługi przez podmioty krytyczne, aby mogły one zostać uzyskać status podmiotów europejskiej infrastruktury krytycznej	2	6
Sankcje za naruszenie przepisów	Brak	Państwa członkowskie wprowadzają sankcje skuteczne, proporcjonalne i odstraszające

Źródło: Opracowanie własne na podstawie Dyrektywy Rady Unii Europejskiej 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony oraz art. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.

W art. 2 pkt 4 dopk zdefiniowano infrastrukturę krytyczną jako składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu niezbędnego do świadczenia usługi kluczowej. Z kolei za usługę kluczową, w myśl art. 2 pkt. 5 dopk, uznano usługę, która ma decydujące znaczenie dla utrzymywania obligatoryjnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska. W miejsce dotychczasowego właściciela lub operatora wprowadzono nowy termin: podmiot krytyczny na oznaczenie podmiotów odpowiedzialnych za funkcjonowanie infrastruktury krytycznej. Podmiot krytyczny jest rozumiany jako podmiot publiczny lub prywatny zidentyfikowany przez państwo członkowskie zgodnie z przepisami dopk i zaliczony do jednej z kategorii sektorów infrastruktury krytycznej (art. 2 pkt. 1 dopk).

W dopk nałożono obowiązki na państwa członkowskie, do których zaliczono: wprowadzenie przepisów krajowych na podstawie przepisów dopk, przyjęcie strategii zwiększającej odporność podmiotów krytycznych, zidentyfikowanie podmiotów krytycznych, wyznaczenie organu odpowiedzialnego za stosowanie przepisów dyrektywy, współpracy z misjami doradczymi oraz współpracę z państwami członkowskimi i Komisją Europejską w powyższym zakresie. Ponadto część obowiązków nałożono na podmioty krytyczne za pośrednictwem państw członkowskich, wśród których można wymienić: wprowadzenie odpowiednich środków technicznych i bezpieczeństwa infrastruktury oraz terminowe zgłaszanie incydentów zakłócających ciągłość usług kluczowych.

Nawiązując do powyższych obowiązków, można wskazać państwa członkowskie zobligowane w terminie do 17 stycznia 2026 r. do przyjęcia strategii zwiększającej odporność podmiotów krytycznych. Strategia powinna zawierać między innymi: zdefiniowane cele strategiczne i priorytety, które przyczynią się do zwiększenia odporności podmiotów krytycznych, określone ramy zarządzania wraz z opisem zakresów obowiązków organów, podmiotów krytycznych i innych stron uczestniczących w realizację strategii, wypunktowane oceny ryzyka, które może mieć wpływ na poziom odporności podmiotów krytycznych. Oceny ryzyka powinny obejmować ryzyka naturalne oraz spowodowane działalnością ludzką, w tym o charakterze międzysektorowym i transgranicznym, wypadki, klęski żywiołowe, stany zagrożenia publicznego, zagrożenia hybrydowe i zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne[15]. Jednocześnie zobowiązano Komisję Europejską do przyjęcia w terminie do 17 listopada 2023 r. wykazu usług kluczowych w sektorach i podsektorach. Uznano, że taka lista ułatwi państwom członkowskim własne prace nad strategią.

Państwa członkowskie zobligowano także do zidentyfikowania podmiotów krytycznych w sektorach i podsektorach w terminie do 17 lipca 2026 r. Podstawą uznania podmiotu za podmiot krytyczny przez państwa członkowskie w świetle przepisów dopk jest spełnienie poniższych warunków: świadczenie co najmniej jednej usługi kluczowej, prowadzenie działalności na terytorium państwa członkowskiego oraz ustalenie przez państwo członkowskie w ocenie ryzyka możliwości wystąpienia incydentu definiowanego jako każde zdarzenie, które może znacząco zakłócić świadczenie usługi kluczowej. W dopk wskazano 11 sektorów: energii; transportu; bankowości; infrastruktury rynków finansowych; zdrowia; wody pitnej; ścieków; infrastruktury cyfrowej; administracji publicznej; przestrzeni kosmicznej; produkcji, przetwarzania i dystrybucji żywności. Tylko w przypadku dwóch sektorów: energii i transportu, wykazano podsektory będące częścią składową sektorów. W przypadku sektora energii wymieniono podsektory: energii elektrycznej, systemu ciepłowniczego i chłodniczego, ropy naftowej, gazu i wodoru, natomiast w przypadku sektora transportu wskazano na podsektory: transportu lotniczego, transportu kolejowego, transportu wodnego, transportu drogowego oraz transportu publicznego. W przypadku pozostałych sektorów wymieniono kategorie podmiotów zdefiniowanych na podstawie przepisów prawa unijnego. Dzięki temu można podsumować, że zakres podmiotowy nowych 11 sektorów wymienionych w dopk jest niemal tożsamy z polskim rozwiązaniem z jednym wyjątkiem. Nawet jeśli nazwy sektorów nie są

[15] W Dyrektywie dopk z 2022 r. wymieniono przestępstwa terrorystyczne, które zostały zdefiniowane w art. 3 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW służące trzem celom: poważnemu zastraszeniu ludności, bezprawnemu zmuszaniu rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania oraz poważniejszej destabilizacji lub zniszczeniu podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej [Dz. Urz. UE L 88/13 z 31.3.2017].

identyczne z obowiązującymi w Polsce, to jednak ich zakresy się przenikają i obejmują te same kategorie podmiotów. Całkowicie nowym sektorem wprowadzonym w dopk jest sektor przestrzeni kosmicznej (patrz tabela 4).

Ponadto państwa członkowskie zobligowano do wyznaczenia co najmniej jednego właściwego organu odpowiedzialnego za prawidłowe stosowanie i egzekwowanie przepisów dopk, a także jeden pojedynczy punkt kontaktowy, który będzie odpowiedzialny za wykonywanie funkcji łącznikowej z pozostałymi punktami oraz z Grupą ds. Odporności Podmiotów Krytycznych (dalej: GOPK). Celem działalności GOPK jest wspieranie Komisji Europejskiej oraz państw członkowskich w zakresie współpracy i wymiany informacji dotyczących przepisów dopk.

Ważną zmianą wobec wcześniejszych przepisów jest zobowiązanie państw członkowskich do przyjęcia przepisów wprowadzających sankcje w przypadku naruszeń przepisów przyjętych na podstawie dopk. O powyższych przepisach i wprowadzonych sankcjach państwa członkowskie informują Komisję Europejską.

Innego rodzaju zobowiązaniem nałożonym za pośrednictwem państw członkowskich na podmioty krytyczne jest uzyskanie odpowiedniego poziomu środków technicznych, środków bezpieczeństwa i środków organizacyjnych służących zapewnieniu ich odporności. W tym celu powinny otrzymać od państw członkowskich właściwą ocenę ryzyka w celu zapobiegania incydentom, zapewnienia fizycznej ochrony ik, odpowiedzi na incydenty, odtworzenia infrastruktury krytycznej po wystąpieniu incydentów, zapewnienia odpowiedniego poziomu zarządzania bezpieczeństwem pracowników, systematycznego zwiększania świadomości pracowników w zakresie ocen ryzyka przez ich udział w szkoleniach, ćwiczeniach i przez możliwość dostępu do materiałów informacyjnych. Także podmioty krytyczne zostały, za pośrednictwem państw członkowskich, zobowiązane do zgłaszania incydentów zakłócających świadczenie usług kluczowych bez zbędnej zwłoki. Przyjęto, że właściwym terminem do zgłoszenia wstępnego incydentu są 24 godziny od chwili uzyskania wiedzy o wystąpieniu incydentu. Zgłoszenie incydentu powinno obejmować wybrane parametry, do których zaliczono: liczbę i odsetek użytkowników dotkniętych zakłóceniem, czas trwania zakłócenia oraz obszar wystąpienia zakłócenia. Także podmioty krytyczne są zobowiązane do wyznaczenia urzędnika łącznikowego odpowiedzialnego za właściwy kontakt z organami państw członkowskich. Podmioty krytyczne w uzasadnionych przypadkach uzyskują od właściwych służb państw członkowskich możliwość weryfikacji osób pełniących kluczowe role w podmiotach krytycznych lub mających dostęp do podmiotów krytycznych.

W art. 17 dopk zdefiniowano podmioty krytyczne o szczególnym znaczeniu na poziomie europejskim. Przyjęto, że muszą być spełnione trzy kryteria. Po pierwsze, podmiot krytyczny powinien zostać wpisany przez państwo członkowskie w określone sektory i podsektory do 17 lipca 2026 r.; po drugie, podmiot krytyczny musi świadczyć usługi kluczowe na rzecz lub w co najmniej sześciu państwach członkowskich; i wreszcie po trzecie, na podstawie właściwej procedury zgłoszenia Komisja Europejska musi stwierdzić, że dany podmiot spełnia przepisy dopk do uznania

go za podmiot krytyczny na poziomie europejskim. Należy podkreślić zasadniczą zmianę w stosunku do przepisów deik z 2008 r., w której przyjęto zakres terytorialny operatorów europejskich działających tylko na rzecz dwóch państw członkowskich. Aktualne przepisy zdecydowanie ograniczają liczbę podmiotów krytycznych oraz preferują podmioty największe o zasięgu co najmniej regionalnym. Podmioty krytyczne poddano nadzorowi przez właściwe organy, a państwa członkowskie mają zapewnić tymże organom wszelkie uprawnienia i środki w celu wykonywania swoich zadań nadzorczych.

W przepisach dopk wprowadzono instytucję misji doradczych, których celem jest dokonanie oceny kryteriów odporności przez podmioty krytyczne. Misja może być utworzona na wniosek państwa członkowskiego, w którym zidentyfikowano podmiot krytyczny; na wniosek co najmniej jednego państwa członkowskiego na rzecz lub w którym świadczona jest usługa kluczowa przez podmiot kluczowy oraz na wniosek Komisji Europejskiej. W skład misji doradczych wchodzą eksperci z państw członkowskich uprawnionych do ich utworzenia oraz przedstawiciele Komisji. Misje uzyskały pełny dostęp do informacji, systemów i obiektów wykorzystywanych do świadczenia usług kluczowych. Po zakończeniu wizyty w terminie trzech miesięcy misja doradcza jest zobowiązana do przedłożenia sprawozdania wszystkim wymienionym wyżej uprawnionym. Wprowadzenie misji doradczych do europejskiego systemu instytucjonalnego infrastruktury krytycznej oznacza zwiększenie dostępu do podmiotów kluczowych oraz wzmocnienie pozycji Komisji Europejskiej będącej organizatorem i koordynatorem tychże misji. Rolę Komisji można zdefiniować także jako doradczą, ponieważ jej zadaniem jest ułatwienie wymiany informacji między członkami i ekspertami z Unii Europejskiej, przygotowanie najlepszych praktyk, szkoleń, ćwiczeń dla podmiotów krytycznych i państw członkowskich oraz podziału środków finansowych na powyższe cele.

Państwa członkowskie zobowiązano do przyjęcia i opublikowania krajowych przepisów wykonawczych do dopk w terminie do 17 października 2024 r., aby od dnia następnego móc je stosować bezpośrednio. Jednocześnie wraz z wejściem w życie nowych przepisów z dniem 18 października 2024 r. traci moc deik. Zapowiedziano także, że Komisja przedstawi Parlamentowi Europejskiemu i Radzie Unii Europejskiej do 17 lipca 2027 r. sprawozdanie z przygotowania państw członkowskich w zakresie realizacji dopk, natomiast do 17 czerwca 2029 r. w zakresie ochrony dopk i propozycji zmian przepisów włącznie z zakresem sektorów, podsektorów i kategorii podmiotów krytycznych.

ZAKOŃCZENIE

Infrastruktura krytyczna została włączona do systemów prawnych Polski i Unii Europejskiej na początku XX w. jako element bezpieczeństwa narodowego i europejskiego. W aktach prawnych, między innymi w ustawach i dyrektywach, zdefiniowano

podstawowe pojęcia oraz klasyfikacje systemów. Oba systemy są komplementarne, jednak można wskazać na pewną ewolucję i różnicę w podejściu do zagadnienia. W polskim systemie prawnym uwzględniono szeroką koncepcję funkcjonowania infrastruktury krytycznej i zidentyfikowano 11 systemów obejmujących 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. Tymczasem na poziomie europejskim zdefiniowano jedynie dwa systemy: energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportowe. Podkreślono wówczas, że zapewnienie ciągłości funkcjonowania infrastruktury było przede wszystkim związane z sieciami lub łańcuchami dostaw, a nie wyodrębnianiem systemów [Radziejewski 2014: 44]. To ograniczone podejście było także konsekwencją ówczesnego sposobu myślenia o pozycji państw członkowskich i organów unijnych. Wskazano wówczas jednoznacznie na państwa członkowskie jako podmioty nadrzędne, które były odpowiedzialne za zachowanie ciągłości działania systemów zarówno na poziomie krajowym, jak i europejskim. Organy unijne miały pozycję podrzędną i uzupełniającą. Jednak rosnące zagrożenia o charakterze naturalnym i antropologicznym oraz pogłębianie integracji politycznej przyczyniły się także do stopniowej zmiany podejścia do pozycji infrastruktury krytycznej w systemie bezpieczeństwa wewnętrznego Unii Europejskiej. Dyrektywa z 2022 r. w pełni odzwierciedla transformację myślenia o infrastrukturze krytycznej. Nawet jeśli państwa członkowskie pozostały głównymi podmiotami odpowiedzialnymi za prawidłowe zarządzanie ik, to utworzono bardziej rozbudowany system instytucjonalny ze wzmocnioną pozycją Komisji Europejskiej jako koordynatorem systemu. Rozbudowano także liczbę systemów, uznając, że tworzą one całość włącznie z podsystemami. Wprowadzono już 11 systemów: energii; transportu; bankowości; infrastruktury rynków finansowych; zdrowia; wody pitnej; ścieków; infrastruktury cyfrowej; administracji publicznej; przestrzeni kosmicznej; produkcji, przetwarzania i dystrybucji żywności. Zakres przedmiotowy jest zbliżony do rozwiązań obowiązujących aktualnie w Polsce poza systemem przestrzeni kosmicznej. Dlatego ocena rozwiązań prawnych obowiązujących w Polsce może być jedynie pozytywna. Jednak państwa członkowskie zobowiązano do przyjęcia zmian w krajowych ustawodawstwach i implementacji rozwiązań europejskich. Następuje stopniowe przesunięcie pozycji podmiotów kluczowych z państw członkowskich na rzecz instytucji unijnych. Uważam, że możemy wyodrębnić dwa okresy z dużym prawdopodobieństwem wystąpienia w najbliższej przyszłości trzeciego okresu. Pierwszy etap trwał od początku XXI w. do dyrektywy z 2022 r. i określiłbym ten etap jako etap z dominującą pozycją państw członkowskich w zakresie zarządzania infrastrukturą krytyczną. Etap drugi, który rozpoczął się w 2022 r., a będzie wzmocniony wraz z implementacją przepisów europejskich do krajowych systemów prawnych w 2024 r., określam jako etap współpracy i zrównoważonych pozycji państw członkowskich

i organów unijnych. Jednocześnie, mając na uwadze dotychczasowy kierunek zmian przepisów i wzajemnych relacji, za najbardziej prawdopodobny scenariusz rozwoju relacji przyjmuję zmianę wzajemnych relacji i wystąpienie okresu trzeciego, który rozpocznie się po 2029 r., w którym to roku zapowiedziano przegląd przepisów na poziomie unijnym, oznaczający dalsze pogłębienie integracji i wzmocnienie pozycji Komisji Europejskiej i Grupy ds. Odporności Podmiotów Krytycznych. Odbędzie się to kosztem państw członkowskich. Należy przyjąć, że pozycja wspomnianej wyżej Grupy lub innego organu utworzonego w jej miejsce może odzwierciedlić rozwiązania charakterystyczne dla współpracy policyjnej i sądowej w ramach bezpieczeństwa wewnętrznego Unii Europejskiej. Podstawą do formułowania postulatów do przyszłych działań pogłębiających współpracę będą stale rosnące zagrożenia hybrydowe, terrorystyczne, klimatyczne i inne, którym państwa członkowskie nie będą w stanie samodzielnie i skutecznie zapobiegać i na nie właściwie reagować.

BIBLIOGRAFIA

Długosz, T. 2015, *Ochrona infrastruktury krytycznej w sektorach energetyki sieciowej*, Warszawa.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 roku w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW, Dz. Urz. UE L 88/13 z 31.3.2017.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego poziomu cyberbezpieczeństwa na terytorium Unii, Dz. Urz. UE L 333/80 z 27.12.2022.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 roku w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, Dz. Urz. UE L 333/164 z 27.12.2022.

Dyrektywa Rady Unii Europejskiej 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 L 345/75 z 23.12.2008.

Jakubiak, E. 2018. *Ochrona infrastruktury krytycznej w Polsce*, „Zeszyty Naukowe Szkoły Głównej Straży Pożarniczej", nr 66.

Lazari, A. 2014. *European Critical Infrastructure Protection*, Springer International Publishing.

Molendowska, M., Ostrowska, M., Górski, P. 2021. *Infrastruktura krytyczna jako element bezpieczeństwa. Wymiar europejski i krajowy*, Toruń.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2013.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2015.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2018.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2020.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2023.

Radziejewski, R. 2014. *Ochrona infrastruktury krytycznej. Teoria a praktyka*, Warszawa.

Rozporządzenie Prezesa Rady Ministrów z dnia 26 kwietnia 2021 roku w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej, Dz. U. 2021 Poz. 793.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej, Dz. U. 2010 Nr 83 Poz. 542.

Setola, R., Luiijf, E., Theocharidou, M. 2017. *Critical Infrastrucures, Protection and Resilience*, [w:] *Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach*, R. Setola, V. Rosato, E. Kyriakides, E. Rome (eds.), Springer International Publishing.

Sobolewski, G., Michailiuk, B., Denysiuk, I. 2019. *Ochrona infrastruktury bezpieczeństwa państwa*, Warszawa.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, Dz. U. 2007, Nr 89, poz. 590 z późniejszymi zmianami.

Ustawa z dnia 4 września 1997 roku o działach administracji publicznej, Dz. U. 1997 Nr 141 poz. 943 z późniejszymi zmianami.

Wyrok Trybunału Konstytucyjnego z dnia 21 kwietnia 2009 roku sygn. akt K 50/07, Dz. U. 2009, Nr 65, poz. 553.

Żuber, M., Smolarek, M. 2016. *Ochrona infrastruktury krytycznej. Dobre praktyki*, Wrocław.

FORMAL AND LEGAL DIMENSION OF CRITICAL INFRASTRUCTURE AT POLISH AND EUROPEAN LEVEL

Abstract: After the Russian Federation began its aggression against Ukraine in 2022, the Ukrainian critical infrastructure system was attacked with the aim of its complete or partial destruction. In response to these attacks, the Ukrainian authorities announced the reconstruction of the infrastructure protection system based on EU legal solutions. Therefore, the article discusses the issues of critical infrastructure, both at the European and Polish level. The provisions of 2007 are in force in the Polish legal system, and the 2008 directive – in the European legal system. However, legal provisions were amended in 2022 and will be implemented into national legal systems in 2024. The aim of the article was to analyze the content of the provisions of legal acts in the field of critical infrastructure in Poland and the EU. The analysis is accompanied by research questions regarding how to define basic concepts and terms in both legal systems and the mutual relations of both systems. The article refers to the document examination method that allows for the analysis of legal acts and comparative analysis. EU Member States have gained a superior position over European bodies, but growing natural and anthropological threats and the process of deepening European political integration have resulted in a gradual change in the way of thinking about critical infrastructure. The position of EU bodies under 2022 directive has been significantly strengthened *vis-à-vis* member states.

Keywords: Poland, European Union, security, critical infrastructure, critical infrastructure systems

BIOGRAM

Wojciech Ziętara, dr hab. prof. UMCS, Katedra Ruchów Politycznych i Badań Etnicznych, Instytut Nauk o Polityce i Administracji, Uniwersytet Marii Curie-Skłodowskiej w Lublinie. Zainteresowania badawcze: historia i współczesność międzynarodowych organizacji ruchów politycznych, systemy doradztwa politycznego. Kontakt e-mail: wojciech.zietara@mail.umcs.pl