BIBLIOTEKA PRZEGLĄDU BEZPIECZEŃSTWA WEWNĘTRZNEGO

Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego.

Wybrane zagadnienia

PRAWO

bezpieczeństwo narodowe

terroryzm

szpiegostwo

zagrożenia hybrydowe

nadzór nad służbami

bezpieczeństwo teleinformatyczne

retencja danych

asymetria zagrożeń

ochrona danych osobowych

pod redakcją
Piotra Burczaniuka

WARSZAWA 2017

Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia

Praca zbiorowa pod redakcją Piotra Burczaniuka

Zespół redakcyjny Anna Przyborowska (redaktor naczelna)
Marta Kuszner-Dolińska (sekretarz Redakcji)
Grażyna Osuchowska, Anna Przyborowska (korekta)
Izabela Laskus (skład)

Projekt okładki Piotr Chorbot

ISBN: 978-83-938217-4-7

**Deklaracja o wersji pierwotnej:
Wersja drukowana publikacji jest jej wersją pierwotną.**

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia
im. gen. dyw. Stefana Roweckiego „Grota” w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

Redakcja
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 645
e-mail: redakcja.pbw@abw.gov.pl
www.abw.gov.pl

Numer zamknięto i oddano do druku w październiku 2017 r.

Druk: Biuro Logistyki
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
Tel. (+48) 22 58 57 657

SPIS TREŚCI

WSTĘP

Problematyka dotycząca zagrożeń bezpieczeństwa narodowego leży w kręgu zainteresowań służb specjalnych, zarówno polskich, jak i zagranicznych. Obecnie obowiązujące uregulowania prawne w tym zakresie zostały wykreowane przed laty, często w okresie zimnej wojny, na podstawie ówczesnej siatki zagrożeń, w wielu wymiarach stanowiących reakcję na dwubiegunowy podział świata. Pojawienie się nowych rodzajów zagrożeń o charakterze hybrydowym, łączących w sobie działania destabilizacyjne, konwencjonalne, nieregularne, cybernetyczne czy też dezinformacyjne, oraz zagrożeń asymetrycznych, takich jak terroryzm, wreszcie postępująca informatyzacja praktycznie wszystkich dziedzin życia oraz rozwój nowych technologii i miniaturyzacja technologii, stanowią asumpt do podjęcia dyskusji na temat gruntownej redefinicji zadań i narzędzi organów odpowiadających za bezpieczeństwo państwa, w tym służb specjalnych, a zwłaszcza ich organizacji. Znalezienie właściwego remedium na współczesne zagrożenia – przy jednoczesnym zagwarantowaniu konstytucyjnych wolności i praw człowieka i obywatela – jest kwestią niezwykle istotną nie tylko z punktu widzenia organów władzy wszystkich państw na świecie, lecz także społeczeństwa obywatelskiego.

Niniejsza publikacja jest kontynuacją dyskusji zapoczątkowanej w opracowaniu pt. *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach* wydanym w maju 2017 r. przez Agencję Bezpieczeństwa Wewnętrznego w ramach serii wydawniczej Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego. Opracowanie zatytułowane *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* jest poświęcona największym wyzwaniom, przed jakimi stoją obecnie służby specjalne całego świata, w tym polskie.

Służby specjalne wszystkich państw stoją w chwili obecnej przed koniecznością takiego określenia ich uprawnień, aby z jednej strony skutecznie rozpoznawać wszelkie zagrożenia bezpieczeństwa narodowego, zapobiegać i przeciwdziałać im oraz je zwalczać, a z drugiej – aby działania służb nie naruszały praw i wolności obywatelskich. Ma temu służyć m.in. właściwe zdefiniowanie pojęcia bezpieczeństwo narodowe oraz jego zakresu, które jest przedmiotem wielu rozważań oraz dyskusji naukowych. Właściwa interpretacja bezpieczeństwa narodowego jest zasadnicza dla funkcjonowania służb specjalnych na całym świecie, a także dla określenia granic ingerencji organów państwa w wolności i swobody obywatelskie. Szczególnie istotne jest znaczenie wyżej wymienionego pojęcia w prawie europejskim, gdyż stosowanie różnego rodzaju instrumentów prawnych (w kontekście korzystania przez służby z ich kompetencji wywiadowczych i kontrwywiadowczych) podlega wielu rygorom prawnym wynikającym z rozmaitych aktów prawa Unii Europejskiej, ale przede wszystkim ograniczeniom, których źródłem są podstawowe wolności i prawa obywatelskie.

Niniejsze opracowanie zawiera analizę istniejących rozwiązań prawnych w zakresie prawa europejskiego, podejmuje również próbę wskazania ich prawidłowej inter-

pretacji na podstawie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej oraz uwzględnia kontekst bieżących prac legislacyjnych na forum Unii Europejskiej, odnoszących się do bezpieczeństwa narodowego. Ponadto w publikacji podjęto próbę usystematyzowania problemu kontroli i nadzoru nad służbami specjalnymi w Rzeczpospolitej Polskiej, które są przejawem gwarancji przyznanych obywatelom na mocy Konstytucji RP. Jednocześnie ten aspekt został uzupełniony o analizę prawno-porównawczą modeli nadzoru i kontroli nad służbami występujących w wybranych porządkach prawnych państw tożsamych kulturowo.

Sprawą bezsporną dla organów władzy wszystkich państw jest przyznanie służbom takich instrumentów, a także taki podział między nie zadań, aby w sposób efektywny mogły przeciwdziałać wielu zagrożeniom bezpieczeństwa narodowego i społeczeństwa. Przykładem realizacji powyższego w Rzeczpospolitej Polskiej jest niewątpliwie *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, która przyznała polskim służbom różnego rodzaju kompetencje, w tym nowe uprawnienia operacyjno-rozpoznawcze w zakresie zapobiegania zdarzeniom o charakterze terrorystycznym. Z uwagi na to, że wspomniana ustawa jest jednym z najważniejszych aktów prawnych regulujących tak istotne zagadnienie, jakim niewątpliwie jest ochrona przed zamachami terrorystycznymi, zdecydowano o przedstawieniu w niniejszej publikacji etiologii prac nad nią. Przy opracowywaniu tekstu wyżej wymienionej ustawy istotne znaczenie miało właściwe wyważenie adekwatności środków i narzędzi przyznanych służbom, które będą skuteczne w zapobieganiu aktom o charakterze terrorystycznym i jednocześnie nie będą naruszały istoty konstytucyjnych wolności i praw człowieka i obywatela, co, jak się wydaje, udało się osiągnąć. Zasygnalizowano jednocześnie ważne elementy powyższego aktu prawnego, zwłaszcza przez wskazanie pojawiających się poglądów doktryny i sądownictwa w kontekście interesującego nas zagadnienia.

Jednym z najważniejszych czynników negatywnie wpływających na bezpieczeństwo narodowe jest – oprócz ataków terrorystycznych – działalność wywiadowcza obcych służb. Z uwagi na mnogość działań, które wpisują się w taką działalność, a które często mogą się łączyć z zamiarem zdestabilizowania sytuacji wewnętrznej kraju, wydaje się, że sprawą niezwykle istotną dla polskiej racji stanu, bezpieczeństwa narodowego oraz ochrony konstytucyjnych wolności i praw człowieka i obywatela winno być właściwe przedefiniowanie pojęć p r z e s t ę p s t w o s z p i e g o s t w a i samego pojęcia w y w i a d. Niniejsza publikacja ma na celu wywołanie dyskusji dotyczącej koniecznych zmian regulacyjnych obejmujących ten czyn zabroniony, ukierunkowanych z jednej strony na rozwiązanie praktycznych problemów pojawiających się na tym gruncie w praktyce funkcjonowania służb w Polsce, a z drugiej – na aktualizację tej normy prawnej w celu jej dostosowania do zmieniającej się siatki zagrożeń bezpieczeństwa Rzeczpospolitej Polskiej, oscylujących wokół zagrożeń o charakterze hybrydowym i asymetrycznym.

Opisując zagrożenia bezpieczeństwa narodowego, nie należy zapominać także o sieciach teleinformatycznych, które mogą stać się celem ataku zarówno dla terrorystów, jak i obcych służb specjalnych. Właściwe zorganizowanie porządku instytucjonalnego w zakresie cyberobrony zaprząta obecnie uwagę rządów w wielu krajach, ale odpowiedzi na pytanie, jak powinien wyglądać model właściwy, bywają różne. Publikacja, którą trzymają Państwo w ręku, zawiera również charakterystykę modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia funkcjonowania wybranych służb specjalnych na świecie. To zagadnienie jest o tyle istotne, że potencjalne ataki w cyberprzestrzeni mogą godzić w sektory strate-

giczne z punktu widzenia bezpieczeństwa narodowego (jak np. w energetykę, system finansowy czy obronny), ale także – z uwagi na powszechny dostęp do Internetu – w zwykłych użytkowników tej sieci. Nie należy zapominać o tym, że informacje, które są niejednokrotnie przechowywane przez użytkowników na twardych dyskach komputerowych, oraz przesyłane przez nich dane, często zawierają dane osobowe lub inne dane wrażliwe. Kradzież danych osobowych i innych tego typu informacji stanowi niewątpliwie poważne zagrożenie obywateli, ich wolności i praw odnoszących się m.in. do prawa do prywatności, ochrony wizerunku czy tajemnicy korespondencji.

W publikacji zdecydowano się przedstawić także charakterystykę rozwiązań legislacyjnych i najważniejszych problemów związanych z – budzącą spory natury prawnej i etycznej w większości państw Unii Europejskiej i NATO – praktyką wykorzystywania przez służby specjalne instrumentów pozwalających na pozyskiwanie danych za pośrednictwem systemów i sieci informatycznych. Dane dotyczące prowadzenia tego typu działań na masową skalę przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA) zostały ujawnione w 2013 r. przez byłego analityka tej Agencji, Edwarda Snowdena. Wywołało to duże kontrowersje nie tylko w Stanach Zjednoczonych, lecz także w państwach europejskich i było katalizatorem trwającej do dziś debaty publicznej nad rolą służb specjalnych i granicami ich kompetencji w systemie demokratycznym, zwłaszcza w kontekście przestrzegania praw i wolności człowieka i obywatela.

Istotnym zagadnieniem wchodzącym w zakres bezpieczeństwa narodowego jest także problem ochrony informacji niejawnych. Obecnie obowiązująca *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* zawiera rozwiązania, które sprawiają, że system ochrony tego typu informacji w Rzeczpospolitej Polskiej nie działa w pełni efektywnie. W związku z powyższym w niniejszej publikacji podjęto próbę sformułowania propozycji zmian legislacyjnych, które wzmocnią skuteczność działania systemu ochrony informacji niejawnych przez uwzględnienie wieloletniego doświadczenia nabytego przez organy sprawujące nadzór nad tym systemem oraz inne właściwe podmioty. Jednocześnie zdecydowano się na wskazanie rozwiązań, których celem miałoby być dostosowanie przepisów wyżej wymienionej ustawy do planowanych zmian w całym systemie bezpieczeństwa państwa.

Należy podkreślić, że przyznanie odpowiedniego zakresu uprawnień i instrumentów (odpowiedzialności) służbom specjalnym jest zagadnieniem niezwykle złożonym. Nie należy zapominać, iż kompetencje przysługujące służbom często stoją w pozornej sprzeczności z zagwarantowanymi konstytucyjnie wolnościami i prawami obywatelskimi. Zadaniem organów władzy jest pogodzenie obu tych wartości, co stanowi poważne wyzwanie ustawodawcze. Jednym z podstawowych praw człowieka i obywatela jest prawo do ochrony danych osobowych. Ochrona tego typu danych jest stosunkowo nową gałęzią ochrony praw jednostki, która jednak w ostatnim czasie, na skutek przemian społecznych i gospodarczych wywołanych powszechną w skali globalnej informatyzacją, zyskuje w szybkim tempie na znaczeniu. W chwili obecnej trwa wielka reforma systemu danych osobowych w Unii Europejskiej zwiększająca m.in. uprawnienia podmiotu danych. Takie ukształtowanie ustawodawstwa unijnego będzie oddziaływało na prawa i obowiązki służb specjalnych, dla których niejawne przetwarzanie informacji o osobach jest nieodzownym elementem działalności służącej ochronie innych fundamentalnych wartości, wśród których poczesne miejsce zajmuje prawo obywateli do życia.

Z gwarancją ochrony danych osobowych nierozerwalnie łączy się problem retencji danych. W ostatnim czasie stał się on niezwykle istotny dla działalności europejskich

organów ścigania i służb specjalnych z uwagi na wyrok Trybunału Sprawiedliwości Unii Europejskiej z 21 grudnia 2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB/Post-ochtelestyrelsen i C-698/15 Secretary of State for the Home Departament/Tom Watson i inni, znany powszechnie jako „wyrok w sprawie Tele2". Najważniejszą tezą tego wyroku jest stwierdzenie przez TSUE, że państwa członkowskie nie mogą nakładać na dostawców usług komunikacji elektronicznej ogólnego obowiązku retencji danych.

W publikacji przedstawiono także analizę międzynarodowych i krajowych podstaw prawnych reagowania na zdarzenia CBRN. Została ona sporządzona w celu weryfikacji stopnia zgodności polskich przepisów prawnych z przepisami prawa międzynarodowego oraz identyfikacji obszarów, w których system prawa polskiego w zakresie reagowania na zdarzenia CBRN winien zostać zmodyfikowany.

Szef
Agencji Bezpieczeństwa Wewnętrznego
prof. dr hab. Piotr Pogonowski

Marcin Nowiński

Pojęcie bezpieczeństwo narodowe w prawie europejskim i międzynarodowym w kontekście uprawnień służb specjalnych

Bezpieczeństwo narodowe[1] jest pojęciem, którego znaczenie i zakres jest wciąż przedmiotem wielu rozważań oraz dyskusji naukowych. Jego właściwa interpretacja na płaszczyźnie prawnej jest niezwykle istotna dla funkcjonowania zarówno służb specjalnych na całym świecie, jak i określenia granic ingerencji organów państwa w wolności oraz swobody obywatelskie. Od właściwej interpretacji tego pojęcia zależy, jaki zakres kompetencji przysługuje służbom specjalnym oraz jakim rygorom i obowiązkom one podlegają w świetle obowiązującego prawa. Pojęcie bezpieczeństwo państwa, w jego szerokim rozumieniu uwzględniającym wymiar wewnętrzny oraz zewnętrzny, jest na tyle istotnym zagadnieniem, że występuje poza porządkami krajowymi poszczególnych państw w prawie europejskim i międzynarodowym.

W prawie wewnętrznym Rzeczpospolitej Polskiej brakuje definicji legalnej bezpieczeństwa narodowego. Należy wskazać, że Konstytucja RP z 2 kwietnia 1997 r.[2] nie posługuje się tym terminem. Pojęciem stosowanym w Konstytucji jest za to bezpieczeństwo państwa. Na gruncie krajowym można przyjąć, że bezpieczeństwo narodowe jest pojęciem o najszerszym zakresie przedmiotowym, które obejmuje również inne rodzaje bezpieczeństwa, jak: bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne oraz bezpieczeństwo zewnętrzne.

Kwestią zasadniczą dla działań podejmowanych przez służby specjalne (mających uprawnienia zarówno o charakterze wywiadowczym, jak i kontrwywiadowczym) państw członkowskich Unii Europejskiej jest właściwa interpretacja pojęcia bezpieczeństwo narodowe, gdyż stosowanie różnego rodzaju instrumentów prawnych przez wymienione służby bądź korzystanie z kompetencji im przysługujących podlega wielu rygorom prawnym, wynikającym z różnego rodzaju aktów prawa Unii Europejskiej. Unia Europejska jest zobowiązana szanować tożsamość państw członkowskich – polityczną lub konstytucyjną. Traktaty wyraźnie wskazują na te zobowiązania. Klauzula bezpieczeństwa narodowego pojawiła się po raz pierwszy w traktacie z Maastricht[3]. W art. F ust. 1 znalazł się zapis, że *Unia szanuje tożsamość narodową państw członkowskich*. W późniejszym okresie art. F ust. 1 traktatu z Maastricht został zmieniony przez traktat z Amsterdamu[4], w związku z czym art. F ust. 1 traktatu z Maastricht został zastąpiony przez art. 6 ust. 3 traktatu z Amsterdamu, który stanowił, że *Unia szanuje tożsamość narodową państw członkowskich*

[1] Ang. *national security*.

[2] Dz.U. nr 78 poz. 483, ze zm.

[3] *Traktat o Unii Europejskiej* został podpisany w Maastricht 7 lutego 1992 r. i wszedł w życie 1 listopada 1993 r. (Dz. Urz. UE C 326 z 6 X 2012 r.).

[4] *Traktat z Amsterdamu, zmieniający Traktat o Unii Europejskiej, traktaty ustanawiające Wspólnoty Europejskie i niektóre związane z nimi akty*, został podpisany w Amsterdamie 2 X 1997 r. i wszedł w życie 1 V 1999 r. (Dz.U. z 2004 r. nr 90 poz. 864/32), http://oide.sejm.gov.pl/oide/images/files/dokumenty/traktaty/Traktat_amsterdamski_PL_1.pdf [dostęp: 31 VIII 2017].

(analogiczne brzmienie do poprzedniego zapisu). Postanowienia dwóch przywołanych powyżej traktatów utorowały ścieżkę do obecnego brzmienia art. 4 ust. 2 traktatu o Unii Europejskiej[5] (dalej: TUE), że:

> Unia szanuje równość Państw Członkowskich wobec traktatów, jak również ich tożsamość narodową, nierozerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym w odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. **W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego**[6]**.**

Powyższe wyłączenie występuje także w wielu aktach prawa pochodnego Unii Europejskiej, które – co do zasady – wykluczają określone czynności o charakterze wywiadowczym[7] w obszarze bezpieczeństwa narodowego z wymogów odnoszących się do typowych działań ochrony bezpieczeństwa i porządku publicznego – będących działaniami o charakterze „policyjnym". Ograniczenia w rozumieniu pojęcia bezpieczeństwo narodowe są przedmiotem szerokiej debaty na poziomie Unii Europejskiej oraz na szczeblu krajowym. Powyższa sytuacja jest spowodowana brakiem definicji legalnej tego pojęcia w prawodawstwie UE. Pomocne w tym zakresie jest z pewnością orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE), który niejednokrotnie odnosił się do przedmiotowej kwestii w jej różnych aspektach. Brak precyzyjnego i jasnego określenia znaczenia pojęcia bezpieczeństwo narodowe wiąże się także z problematycznym rozdziałem kompetencyjnym w obszarze ochrony bezpieczeństwa i porządku publicznego[8], czyli – innymi słowy – kompetencjami o charakterze policyjnym oraz w obszarze dedykowanym służbom specjalnym, czyli prowadzeniu czynności o charakterze wywiadowczym[9] (oraz kontrwywiadowczym). W niektórych państwach członkowskich omawiane kompetencje nie są rozdzielone i mają charakter „mieszany", czyli np. służba specjalna poza kompetencjami wywiadowczymi i kontrwywiadowczymi ma również uprawnienia o charakterze policyjnym. Przykładem tego mogą być służby specjalne, które zostały wyposażone w kompetencje dochodzeniowo-śledcze.

Jest to również istotne w odniesieniu do zadań Unii Europejskiej w obszarze zapewniania bezpieczeństwa wewnętrznego, gdyż zgodnie z art. 4 ust. 2 lit. j *Traktatu o funkcjonowaniu Unii Europejskiej*[10] (dalej: TFUE) kompetencje dzielone między Unię Europejską a państwa członkowskie w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Uwagę zwraca także brak precyzyjnego rozgraniczenia między pojęciami porządek publiczny[11] a bezpieczeństwo narodowe. Z dotychczasowej praktyki wynika, że ochronę tego drugiego dobra Unia Europejska

[5] Wersja skonsolidowana Dz. Urz. UE C 83 z 30 III 2010, s. 13–45.

[6] Dz. Urz. UE C 202/47 z 7 VI 2016 r. Wyróżnienie w tekście pochodzi od autora – przyp. red.

[7] Ang. *intelligence activities*. Pod tym pojęciem należy rozumieć zarówno działania o charakterze wywiadowczym, jak i kontrwywiadowczym.

[8] Ang. *law enforcement*.

[9] Ang. *intelligence activities*.

[10] Wersja skonsolidowana Dz. Urz. UE C 83 z 30 III 2010, s. 47–403.

[11] Ang. *public order*.

pozostawiła państwom członkowskim[12]. W niektórych aspektach funkcjonowania organów odpowiedzialnych za bezpieczeństwo, pojęcie bezpieczeństwo narodowe jest wyzwaniem w sensie metodologicznym, chociażby z uwagi na działania w sensie „inwigilacyjnym", które mogą być prowadzone zarówno na podstawie działań o charakterze policyjnym (przez organy ochrony bezpieczeństwa i porządku publicznego), jak i wywiadowczym (przez służby specjalne).

W związku z brakiem precyzyjnej definicji omawianego terminu należy dążyć do przyjęcia jego właściwej interpretacji, zwłaszcza w przypadku, gdy różnica między ochroną bezpieczeństwa i porządku publicznego a bezpieczeństwem narodowym staje się mało widoczna. W każdym razie bezpieczeństwa narodowego nie powinno się utożsamiać z bezpieczeństwem Unii Europejskiej, bezpieczeństwem państwa, bezpieczeństwem publicznym ani obronnością. Trzeba również podkreślić, że – co do zasady – czynności podejmowane przez służby wywiadowcze są akceptowane jako podlegające klauzuli bezpieczeństwa narodowego, jednak w przypadku organów odpowiedzialnych za ochronę bezpieczeństwa i porządku publicznego, które realizują analogiczne w pewnym stopniu zadania, taka interpretacja nie jest już powszechna[13].

Warte postawienia jest również pytanie, czy interes bezpieczeństwa narodowego państwa trzeciego może być podstawą powołania się na klauzulę bezpieczeństwa narodowego. Z literalnego brzmienia traktatów można wnioskować, że klauzula bezpieczeństwa narodowego przewidziana w TUE nie wskazuje na możliwość powoływania się na bezpieczeństwo narodowe państwa trzeciego jako samodzielną podstawę prawną stosowaną w celu uniknięcia zastosowania prawa Unii Europejskiej. Należy również pamiętać o wyjątkach od powyższej zasady, czyli że mogą istnieć pewne obszary, w których interes bezpieczeństwa narodowego państwa członkowskiego Unii Europejskiej i państwa trzeciego się pokrywają[14]. Każdą z tego typu sytuacji trzeba traktować na zasadzie *case-by-case*[15].

Wracając do art. 4 ust. 2 TUE oraz zawartej tam klauzuli bezpieczeństwa narodowego, należy wskazać, że zgodnie z tym przepisem Unia Europejska nie może przyjmować rozwiązań prawnych odnoszących się do bezpieczeństwa narodowego państw członkowskich. Jak już zaznaczono, nie ma definicji legalnej pojęcia bezpieczeństwo narodowe w prawie Unii Europejskiej, chociaż traktaty unijne zawierają odesłania i odnoszą się do wielu aspektów, które trudno odróżnić od bezpieczeństwa narodowego lub które są z nim bezpośrednio związane i w których zakresie regulacji Unia Europejska ma kompetencje do stanowienia prawa.

Warto podkreślić, że w myśl art. 73 TFUE *Państwa Członkowskie mogą organizować między sobą i na swoją odpowiedzialność uznane przez nie za stosowne formy współpracy i koordynacji między właściwymi służbami ich administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego*. Jak wskazuje A. Grzelak w komentarzu do przedmiotowej regulacji[16],

---

[12] *Mapping EU Member States' legal frameworks*, w: *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, FRA (European Union Agency for Fundamental Rights), *fra.europa.eu/.../fra.../fra-2015-surveillance-intelligence-services-summary-0_en-3.pdf*, s. 11 [dostęp: 31 VIII 2017].

[13] *Working Document on surveillance of electronic communications for intelligence and national security purposes. Adopted on 5 December 2014*, 14/EN WP 228, s. 2.

[14] Tamże, s. 22.

[15] W indywidualny sposób.

[16] A. Grzelak, *Komentarz do art. 72 i komentarz do art. 73*, w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, A. Wróbel, N. Półtorak, D. Miąsik (red.), Warszawa 2012.

> (…) bezpieczeństwo narodowe (ang. *national security*) najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa, która obejmuje problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa. Państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór wartości wewnętrznych, które jego zdaniem powinny być chronione przed zagrożeniami. Bezpieczeństwo narodowe postrzegane jest zatem jako zdolność narodu (państwa) do obrony terytorium i wartości. Termin „bezpieczeństwo narodowe" zawiera w sobie zatem te aspekty, które w kontekście art. 72 nazywane są „bezpieczeństwem wewnętrznym", chociaż intuicyjnie wydaje się pojęciem szerszym, i dotyczy również kwestii bezpieczeństwa w aspekcie militarnym

Dalej A. Grzelak stwierdza również, że w (…) *kontekście współpracy w ramach PWBiS*[17] *pojęcie bezpieczeństwa narodowego powinno być rozumiane możliwie wąsko i ograniczone wyłącznie do tych aspektów, które nie zawierają w sobie elementu transgranicznego, w kontekście czysto wewnętrznym, gdyż inaczej trudno byłoby kontynuować współpracę w ramach PWBiS.*

Powyższa interpretacja art. 73 TFUE ma charakter zawężający i trudno zgodzić się z tezą, że pojęcie b e z p i e c z e ń s t w o n a r o d o w e powinno ograniczać się wyłącznie do tych aspektów, które nie zawierają w sobie elementu transgranicznego. W obecnych czasach, kiedy prawie każda (jeśli nie każda) sfera działalności służb ma w sobie element transgraniczny i jest prowadzona w zakresie współpracy międzynarodowej z innymi organami o analogicznych kompetencjach, trudno byłoby zaakceptować pogląd, że mogą to być tylko działania „czysto wewnętrzne". Takie podejście wcale nie oznacza automatycznego wystąpienia reguł kolizyjnych w odniesieniu do współpracy prowadzonej w ramach PWBiS, gdyż istnieją zagrożenia w sferze bezpieczeństwa narodowego, które z jednej strony wymuszają współpracę w ramach PWBiS poszczególnych organów państw członkowskich w pewnych aspektach, chociaż nie jest to tożsame z tym, że państwa członkowskie, współpracując w tym zakresie, pozbywają się swoich wyłącznych kompetencji dotyczących bezpieczeństwa międzynarodowego.

Warto w kontekście analizy bezpieczeństwa narodowego zwrócić uwagę na art. 75 TFUE, umieszczony w Tytule V – *Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości*, który stanowi:

> Jeżeli wymaga tego realizacja celów, o których mowa w artykule 67, w odniesieniu do zapobiegania terroryzmowi i działalności powiązanej oraz zwalczania tych zjawisk, Parlament Europejski i Rada, stanowiąc w drodze rozporządzeń zgodnie ze zwykłą procedurą ustawodawczą, określają ramy środków administracyjnych dotyczących przepływu kapitału i płatności, takich jak zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej, które należą do osób fizycznych lub prawnych, grup lub innych podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji. Rada, na wniosek Komisji, przyjmuje środki w celu wdrożenia ram, o których mowa w akapicie pierwszym. Akty, o których mowa w niniejszym artykule, zawierają niezbędne przepisy w zakresie gwarancji prawnych.

Mając na uwadze brzmienie powyższego artykułu, należy zadać pytanie, w jaki sposób – ustanawiając właściwość Unii Europejskiej w zapobieganiu terroryzmowi i działaniom powiązanym oraz ich zwalczaniu – odróżnić zakres tych działań od ochrony bez-

[17] Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości.

pieczeństwa narodowego. Ponadto warto wskazać, że większość państw członkowskich jednoznacznie uznaje, że działania antyterrorystyczne bezsprzecznie mieszczą się w sferze bezpieczeństwa narodowego, a tym samym są prerogatywą państw członkowskich Unii Europejskiej. Trzeba także pamiętać, że jest to przykład tego, jak działania Unii Europejskiej w obszarze stanowienia prawa mogą w widoczny sposób być podejmowane na granicy sfery będącej domeną państw członkowskich, czyli bezpieczeństwa narodowego[18].

Na uwagę w rozważaniach dotyczących pojęcia bezpieczeństwo narodowe zasługuje również art. 346 ust. 1 lit. a TFUE, zgodnie z którym (…) *żadne Państwo Członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa*. Ten przepis nie odnosi się wprost do bezpieczeństwa narodowego, chociaż – z uwagi na derogacyjny charakter – ma istotne znaczenie przy właściwej interpretacji omawianego pojęcia. W świetle omawianej normy traktatowej państwa członkowskie mogą podejmować środki, które w innej sytuacji mogłyby być uznane za niezgodne z przepisami traktatów[19]. Jest to możliwe z uwagi na podstawowe interesy bezpieczeństwa państwa, które wiążą się z ochroną informacji strategicznych dla państwa. Warto zaznaczyć, że art. 346 jest klauzulą derogacyjną o charakterze ogólnym i – jak podkreśla W. Sadowski – (…) *wskazane w art. 346 podstawowe interesy bezpieczeństwa definiowane są jako bezpieczeństwo narodowe lub zewnętrze bezpieczeństwo wojskowe*[20].

Należy także nadmienić, że w art. 24 ust.1 TUE[21] oraz art. 2 ust. 4 TFUE[22] przewidziano kompetencje Unii Europejskiej w sferze wspólnej polityki zagranicznej i bez-

[18] W tym przypadku ma się do czynienia z tzw. doktryną zajętego pola. Do powyższej sytuacji dochodzi wówczas, gdy dana dziedzina czy obszar zostaną poddane regulacji prawa Unii Europejskiej za pomocą instrumentu harmonizującego, państwa członkowskie zaś tracą swobodę regulacyjną w odniesieniu do tej dziedziny. Następuje wtedy przejęcie kompetencji przez tzw. zajęcie pola. Aktywne działania państwa członkowskiego w dziedzinie podlegającej regulacji nie są już wówczas możliwe. Powyższy przykład ilustruje sytuację, kiedy niezwykle istotna oraz wrażliwa sfera bezpieczeństwa narodowego może zostać z niego „wyjęta" wskutek podejmowania działań legislacyjnych na forum Unii Europejskiej przez jej organy.

[19] Zob. W. Sadowski, *Art. 346*, w: *Traktat o funkcjonowaniu Unii*…, t. 3 (art. 223–358).

[20] Tamże. Por. z opinią rzecznika generalnego Slynna do sprawy 72/83 Campus Oil, s. 2764.

[21] Artykuł 24 TUE 1 – „Kompetencje Unii w zakresie wspólnej polityki zagranicznej i bezpieczeństwa obejmują wszelkie dziedziny polityki zagranicznej i ogół kwestii dotyczących bezpieczeństwa Unii, w tym stopniowe określanie wspólnej polityki obronnej, która może prowadzić do wspólnej obrony.

Wspólna polityka zagraniczna i bezpieczeństwa podlega szczególnym zasadom i procedurom. Jest określana i realizowana przez Radę Europejską i Radę stanowiące jednomyślnie, chyba że Traktaty przewidują inaczej. Wyklucza się przyjmowanie aktów prawodawczych. Wspólną politykę zagraniczną i bezpieczeństwa wykonuje wysoki przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa oraz Państwa Członkowskie, zgodnie z Traktatami. Szczególną rolę Parlamentu Europejskiego i Komisji w tej dziedzinie określają Traktaty. Trybunał Sprawiedliwości Unii Europejskiej nie jest właściwy w zakresie tych postanowień, z wyjątkiem właściwości do kontrolowania przestrzegania artykułu 40 niniejszego Traktatu i do kontroli legalności niektórych decyzji przewidzianych w artykule 275 akapit drugi Traktatu o funkcjonowaniu Unii Europejskiej.

2. W ramach zasad i celów swoich działań zewnętrznych Unia Europejska prowadzi, określa i realizuje wspólną politykę zagraniczną i bezpieczeństwa, opartą na rozwoju wzajemnej solidarności politycznej między Państwami Członkowskimi, określaniu kwestii stanowiących przedmiot ogólnego zainteresowania i osiąganiu coraz większego stopnia zbieżności działań Państw Członkowskich.

3. Państwa Członkowskie popierają, aktywnie i bez zastrzeżeń, politykę zewnętrzną i bezpieczeństwa Unii w duchu lojalności i wzajemnej solidarności i szanują działania Unii w tej dziedzinie.

Państwa Członkowskie działają zgodnie na rzecz umacniania i rozwijania wzajemnej solidarności politycznej. Powstrzymują się od wszelkich działań, które byłyby sprzeczne z interesami Unii lub mogłyby zaszkodzić jej skuteczności jako spójnej sile w stosunkach międzynarodowych.

Rada i wysoki przedstawiciel czuwają nad poszanowaniem tych zasad".

[22] Art. 2 ust. 4 TFUE 4 – „Zgodnie z postanowieniami Traktatu o Unii Europejskiej Unia ma kompetencję w zakresie określania i realizowania wspólnej polityki zagranicznej i bezpieczeństwa, w tym stopniowego określania wspólnej polityki obronnej".

pieczeństwa, przez odniesienie się do „bezpieczeństwa Unii Europejskiej". Z tego też względu sfera bezpieczeństwa UE pozostaje w zakresie właściwości Unii, chociaż trzeba ją odróżnić od sfery bezpieczeństwa narodowego państw członkowskich, która zgodnie z art. 4 ust. 2 TUE pozostaje poza zakresem właściwości Unii Europejskiej[23].

Karta Praw Podstawowych UE[24] także w swej preambule zawiera zapis, że Unia Europejska szanuje tożsamość narodową państw członkowskich. Jak wynika z tego zapisu, bezsprzecznie uznaje się, że wyżej wymieniona zasada ma powszechne zastosowanie w dorobku prawa europejskiego, czego przykładem jest jej zastosowanie zarówno w traktacie o Unii Europejskiej, Karcie Praw Podstawowych UE, jak i w innych aktach prawnych Unii.

Także *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*[25] stosuje pojęcie b e z p i e c z e ń s t w o n a r o d o w e[26] w art. 6 ust. 1 (*Prawo do rzetelnego procesu sądowego*), wskazując, że:

> (…) postępowanie przed sądem jest jawne, jednak prasa i publiczność mogą być wyłączone z uwagi na porządek publiczny lub bezpieczeństwo narodowe w społeczeństwie demokratycznym;

w art. 8 ust. 2 (*Prawo do poszanowania życia prywatnego i rodzinnego*) stanowiąc, że:

> (…) niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo narodowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób;

w art. 10 ust. 2 (*Wolność wyrażania opinii*), wskazując, że:

> (…) korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa narodowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych (…)

w art. 11 ust. 2 (*Wolność zgromadzeń i stowarzyszania się*), stanowiąc, że:

> (…) wykonywanie tych praw nie może podlegać innym ograniczeniom niż te, które określa ustawa i które są konieczne w społeczeństwie demokratycznym z uwagi na in-

[23] Por. z *Working Document on surveillance of electronic communications*…, s. 22.

[24] *Karta Praw Podstawowych Unii Europejskiej* oide.sejm.gov.pl/oide/?option=com_content&view=article&id=14428...422 [dostęp: 31 VIII 2017].

[25] *Konwencja o ochronie praw człowieka i podstawowych wolności* została otwarta do podpisu 4 XI 1950 r., a weszła w życie 3 IX 1953 r.

[26] W polskiej wersji językowej *Konwencji* jest stosowane pojęcie b e z p i e c z e ń s t w o p a ń s t w o w e, przy czym należy zauważyć, że jest to nieprecyzyjne tłumaczenie angielskiego terminu *n a t i o n a l s e c u r i t y*, który jest stosowany w angielskiej wersji językowej.

teresy bezpieczeństwa narodowego lub bezpieczeństwa publicznego, ochronę porządku i zapobieganie przestępstwu, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Niniejszy przepis nie stanowi przeszkody w nakładaniu zgodnych z prawem ograniczeń korzystania z tych praw przez członków sił zbrojnych, Policji lub administracji państwowej.

Jak wynika z tych zapisów, klauzula bezpieczeństwa narodowego jest jedną z zasadniczych przesłanek konwencyjnych, które uzasadniają pewne (sprecyzowane) ograniczenia w korzystaniu z praw gwarantowanych na podstawie *Konwencji*. Te wyłączenia z uwagi na przesłankę interesu bezpieczeństwa narodowego wskazują, że prawa, które ustanawia *Konwencja*, nie mają charakteru absolutnego, a państwa strony, zachowując standardy społeczeństwa demokratycznego, mogą korzystać z możliwości ograniczenia poszczególnych praw – o ile jest to uzasadnione zaistniałą sytuacją. Istotne – w kontekście powyższych rozważań – jest to, że Europejska Komisja Praw Człowieka (w sprawie Esbester przeciw Wielkiej Brytanii) rozważała możliwość wprowadzenia definicji pojęcia interesy bezpieczeństwa narodowego, dochodząc do wniosku, że nie jest konieczne jej wyczerpujące zdefiniowanie. W opinii Komisji wiele przepisów prawa z uwagi na zakres regulacji powinno mieć elastyczny charakter, tym bardziej, że wiele regulacji prawnych w mniejszym lub większym stopniu jest niejednoznacznych, a ich interpretacja powinna być ukształtowana w praktyce[27]. Orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: ETPC) z pewnością wniosło istotny wkład w określenie pewnych immanentnych części składowych koncepcji omawianego pojęcia. Można zatem wskazać, że ochrona bezpieczeństwa państwa i porządku konstytucyjnego oraz demokratycznego przed zagrożeniem szpiegostwem, terroryzmem, wspieraniem terroryzmu, separatyzmem i podżeganiem do łamania dyscypliny służbowej w sferze wojskowej, z pewnością *per se* stanowią działania w sferze bezpieczeństwa narodowego. Również w orzeczeniu w sprawie 1365/07 (C.G. i inni przeciw Bułgarii)[28] Trybunał wskazał, że pojęcie bezpieczeństwo narodowe może być znaczeniowo szerokie, z dużym marginesem uznaniowości pozostawionym władzy wykonawczej w celu określenia, co jest w interesie bezpieczeństwa danego państwa. Nie oznacza to jednak, że granice mogą zostać rozciągnięte poza naturalne znaczenie omawianego pojęcia. Warto zwrócić uwagę na to, że orzecznictwo TSUE również nie zdołało ukształtować precyzyjnej definicji omawianego pojęcia. W sprawie C-275/06 (Promisucae)[29] Trybunał, odnosząc się w tym orzeczeniu do art. 15 ust. 1 *Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej*[30] oraz wskazując na podstawie wyżej wymienionego przepisu na przysługującą państwom członkowskim możliwość ustanowienia wyjątków od zasadniczego obowiązku zapewnienia poufności danych osobowych, ciążącego na mocy art. 5 tej dyrektywy, wskazał, że żaden z tych wyjątków nie

[27] Sprawa Esbester vs United Kingdom (18601/91) (1994), decyzja Komisji z 2 IV 1993 r., www.echr.ketse.com/doc/18601.91-en-19930402/view/ [dostęp: 31 VIII 2017].

[28] Sprawa C.G. and Others vs Bulgaria (1365/07), 24 April 2008, www.echr.ketse.com/doc/1365.07-en-20080424/view/ [dostęp: 31 VIII 2017].

[29] Wyrok TUSE z 29 I 2008 r. mającej za przedmiot wniosek o wydanie, na podstawie art. 234 WE, orzeczenia w trybie prejudycjalnym złożony przez Juzgado de lo Mercantil nº5 de Madrid (Hiszpania).

[30] Dz. Urz. WE L 201 z 31 VII 2002, s. 37; Dz. Urz. UE, polskie wydanie specjalne, rozdz. 13, t. 29, s. 514, ze zm.

wydaje się jednak odnosić do sytuacji, w których chodzi o wszczęcie postępowania cywilnego. Z jednej strony dotyczą one bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego, które stanowią działania właściwe państwom lub władzom państwowym, obcych dziedzinom działalności osób prywatnych, i z drugiej – ścigania przestępstw kryminalnych[31]. Z powyższego orzeczenia można wysunąć wniosek, że Trybunał, po pierwsze, wskazał jasno, że należy rozróżnić sferę bezpieczeństwa narodowego od sfery obronności i bezpieczeństwa publicznego, i po drugie – że działania w wymienionych obszarach są właściwe dla państwa lub władz państwowych, tym samym są obce działalności osób prywatnych. TSUE wyraźnie uznaje bezpieczeństwo narodowe za właściwość państwa członkowskiego, a działania w tej sferze należą do kompetencji władz tego państwa. Co prawda powyższy wyrok nie wskazuje definicji bezpieczeństwa narodowego, ale wskazuje na dwa ważne atrybuty tego pojęcia, o których jest mowa powyżej[32].

Interesujący pogląd w tej materii prezentuje również rzecznik generalny TSUE Francis Jacobs w opinii przedstawionej 6 kwietnia 1995 r.[33] w sprawie C-120/94 (Komisja przeciw Grecji). Stwierdził on, że zagadnienie bezpieczeństwa narodowego należy w zasadzie do oceny państwa[34], co zostało podkreślone w orzecznictwie ETPC w odniesieniu od art. 15 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Zgodnie z regulacją konwencyjną umawiające się strony *Konwencji* mogą podjąć środki uchylające stosowanie zobowiązań wynikających z niniejszej *Konwencji*, w zakresie ściśle odpowiadającym wymogom sytuacji, pod warunkiem że środki te nie są sprzeczne z innymi zobowiązaniami wynikającymi z prawa międzynarodowego,w przypadku wojny lub innego niebezpieczeństwa publicznego zagrażającego życiu narodu. W orzeczeniu ETPC z 18 stycznia 1978 r. w sprawie Irlandia przeciw Wielkiej Brytanii Trybunał uznał, że do umawiających się stron należą kompetencje, w których zakresie pozostaje odpowiedzialność za życie ich narodów, stwierdzenie czy występuje zagrożenie życia obywateli w wyniku sytuacji kryzysowej i jeśli tak, to jak dalece mają sięgać podejmowane przez państwo działania służące przezwyciężaniu sytuacji kryzysowej. Władze państwowe, zdaniem Trybunału, są w lepszej sytuacji niż sąd międzynarodowy, aby decydować, czy występuje sytuacja kryzysowa i jaki jest charakter oraz zakres ingerencji niezbędnej do uniknięcia zagrożenia[35]. Zarówno opinia rzecznika generalnego TSUE, jak i wyrok ETPC dowodzą jednej rzeczy, że bezpieczeństwo narodowe jako sfera, której zakres nie jest sztywno uregulowany, pozostawia się swobodnej ocenie państw i ich władz, gdyż to one są odpowiednimi podmiotami do podejmowania działań w tej sferze i to one ponoszą ich skutki.

Warto również poświęcić uwagę nieco odmiennemu spojrzeniu na tematykę związaną ze sferą bezpieczeństwa narodowego. Podstawowe zasady odnoszące się do tej tematyki zostały opracowane i omówione w *Globalnych zasadach dotyczących bezpieczeństwa narodowego i prawa do informacji (Zasady z Tshwane)*[36] i stanowią zbiór

[31] Pkt 50 i 51 sprawy C-275/06 (Promisucae).

[32] Analogiczne tezy znalazły się w wyroku TSUE 101/01 (Lindqvist, pkt 43) z 6 XI 2003 r.

[33] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61994CC0120 [dostęp: 30 VIII 2017].

[34] Pkt 55 opinii rzecznika generalnego.

[35] https://www.cvce.eu/en/obj/judgement_of_the_european_court_of_human_rights_ireland_v_the_united_kingdom_18_january_1978-en-e07eaf5f-6d09-4207-8822-0add3176f8e6.html [dostęp: 30 VIII 2017].

[36] *Globalne zasady dotyczące bezpieczeństwa narodowego i prawa do informacji (Zasady z Tshwane)* zostały ogłoszone 12 VI 2013 r. i są wynikiem ponad rocznej pracy 22 grup, obejmującej konsultacje z przeszło 500 ekspertami z ponad 70 krajów świata. Najistotniejszym wydarzeniem podczas opracowywania zasad było spotkanie, do którego doszło w mieście Tshwane (Republika Południowej Afryki).

wskazań dla podmiotów uczestniczących w tworzeniu, weryfikowaniu bądź implementowaniu przepisów prawnych przysługujących państwu, dotyczących kompetencji do odmowy ujawnienia informacji ze względów bezpieczeństwa narodowego oraz ewentualnej odpowiedzialności za ujawnienie takich informacji. Te zasady zostały opracowane przez organizacje pozarządowe, ośrodki akademickie oraz współpracujących z nimi ekspertów[37].

Jak wskazują autorzy opracowania, bezpieczeństwo narodowe i przysługujące każdej osobie prawo poznania prawdy są często postrzegane jako wartości przeciwstawne. Z tego powodu występują sporne interesy między władzą publiczną dążącą do utrzymywania poufności informacji ze względu na konieczność ochrony bezpieczeństwa narodowego a przysługującym każdej osobie prawem do informacji, które pozostają w dyspozycji organów publicznych. W praktyce, zdaniem autorów, uzasadnione interesy bezpieczeństwa narodowego są najlepiej chronione wówczas, gdy opinia publiczna jest dobrze poinformowana o działaniach państwa, w tym podejmowanych w celu ochrony bezpieczeństwa narodowego. Już w preambule tego dokumentu podkreślono, że podstawowym celem jest dostęp do informacji jako prawo każdej osoby i jako takie powinno podlegać ochronie prawnej. Jednocześnie wskazano przesłankę uzasadnionego interesu państwa w odmowie ujawnienia pewnych informacji, w tym ze względów bezpieczeństwa narodowego. Ponadto podkreślono istotne znaczenie równowagi między ujawnieniem a odmową ujawnienia informacji, co w społeczeństwie demokratycznym ma zasadnicze znaczenie i decyduje o bezpieczeństwie. Autorzy zasad wskazują w preambule także na to, że pewne informacje, których ujawnienia nie powinno się odmawiać ze względów bezpieczeństwa narodowego, mogą mimo wszystko nie zostać ujawnione z różnych innych powodów uznawanych w prawie międzynarodowym, którymi mogą być: stosunki międzynarodowe, rzetelność postępowania sądowego, prawa stron sporu oraz prawo do prywatności jednostki, z zastrzeżeniem zawsze obowiązującej zasady, że odmowa ujawnienia informacji jest możliwa jedynie w sytuacji, gdy interes publiczny w zachowaniu w tajemnicy takiej informacji znacznie przeważa nad interesem publicznym związanym z dostępem do niej.

W *Globalnych zasadach* zostały sprecyzowane także poszczególne definicje, takie jak przedsiębiorstwo sektora bezpieczeństwa narodowego oraz uzasadniony interes bezpieczeństwa narodowego, zdefiniowany jako interes, którego rzeczywistym przedmiotem i głównym skutkiem jest ochrona bezpieczeństwa narodowego i który jest zgodny z prawem krajowym i międzynarodowym. Interes bezpieczeństwa narodowego nie jest uznawany za uzasadniony, jeżeli jego prawdziwym przedmiotem bądź głównym skutkiem jest ochrona interesu niezwiązanego z bezpieczeństwem narodowym, na przykład ochrona władzy publicznej albo jej urzędników przed kompromitacją bądź ujawnieniem szkodliwego postępowania, zatajenie informacji o naruszeniach prawa człowieka, innego rodzaju naruszeniach prawa albo funkcjonowania instytucji publicznych, wzmacnianie bądź zachowanie partykularnego interesu politycznego, partyjnego bądź ideologicznego, a także tłumienie protestów zgodnych z prawem. Co interesujące – w zasadach nie zdefiniowano terminu bezpieczeństwo narodowe. Zawarto w nich jedynie rekomendacje w tym zakresie, zgodnie z którymi ten termin powinien zostać precyzyjnie zdefiniowany w prawie krajowym, w sposób odpowiadający potrzebom społeczeństwa demokratycznego.

[37] http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/03/Zasady-z-Tshwane.pdf [dostęp: 31 VIII 2017].

Jeśli chodzi o same zasady, to odnoszą się one do określenia różnych aspektów prawa do informacji w kontekście wymogów dotyczących ograniczenia ww. prawa z uwagi na konieczność ochrony bezpieczeństwa narodowego. Ciekawa konkluzja znajduje się w ramach zasady nr 2, która w pkt b stanowi, że:

> (…) bezpieczeństwo narodowe stanowi jedną z najpoważniejszych publicznych przesłanek ograniczania dostępu do informacji, jeżeli organy publiczne powołują się na inne tego typu przesłanki – w tym dotyczące stosunków międzynarodowych, porządku, zdrowia i bezpieczeństwa publicznego, egzekwowania prawa, możliwości nieskrępowanego przekazywania niezależnych porad w przyszłości, skutecznego formułowania zasad polityki oraz interesów gospodarczych państwa – muszą one co najmniej spełnić te standardy dotyczące nakładania ograniczeń prawa dostępu do informacji, które uznane zostały na mocy niniejszych Zasad za istotne.

Mając na uwadze powyższe twierdzenie, należy uznać, że także podmioty pozarządowe traktują przesłankę ochrony bezpieczeństwa jako najpoważniejszą oraz mającą największy „ciężar gatunkowy" z wymienionych przesłanek. Świadczy to też o tym, że bezpieczeństwo narodowe jest uznawane za materię, która skupia w swoim zakresie najistotniejsze zagrożenia państwa. W omawianym opracowaniu jako dobrą praktykę postuluje się również precyzyjne zdefiniowanie pojęcia b e z p i e c z e ń s t w o n a r o d o w e w systemach prawa krajowego, w sposób odpowiadający zasadom społeczeństwa demokratycznego.

Globalne zasady – jakkolwiek prezentują stanowisko podmiotów pozarządowych, których spojrzenie na problematykę związaną z pojęciem b e z p i e c z e ń s t w o n a r o d o w e jest nieco odmienne niż punkt widzenia organów państwa odpowiedzialnych za bezpieczeństwo narodowe – są z pewnością cennym wkładem w dyskusję oraz głosem dużej części obywateli, w tym przedstawicieli środowisk naukowych. Te środowiska poza nadrzędnym celem, jakim było zapewnienie możliwie szerokiego dostępu do informacji, wskazują także na znaczenie oraz istotę sfery bezpieczeństwa narodowego i kolizję *sui generis*, jaka występuje między tymi dwoma dobrami. Warto również uwzględnić ich dorobek naukowy, gdyż jest on cennym wkładem w dyskusję nad definicjami odnoszącymi się do sfery bezpieczeństwa narodowego (…).

Pojęcie b e z p i e c z e ń s t w o n a r o d o w e oraz jego zakres, a także związane z nim zagadnienia są szczególnie istotne w świetle reformy systemu ochrony danych osobowych na forum Unii Europejskiej oraz z powodu przyjęcia dwóch niezwykle istotnych aktów prawnych w tej materii, tj. *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[38] i *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW*[39]. Drugi z wyżej wymienionych aktów prawnych w swej preambule, w motywie 14 stanowi, że:

[38] Dz. Urz. UE L 119 z 4 V 2016, s. 1–88.

[39] Tamże, s. 89–131.

> (…) niniejsza dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej (TUE), nie należy uznawać za czynności wchodzące w zakres niniejszej dyrektywy.

Przywołana powyżej regulacja dyrektywy 2016/680 precyzyjnie odnosi się do (…) *działalności wykraczającej poza zakres prawa Unii*, odnosząc po stwierdzenie w kolejnej części tej samej sentencji do bezpieczeństwa narodowego, a także do działań (…) *agencji lub jednostek zajmujących się bezpieczeństwem narodowym*. Jednocześnie art. 2 ust. 3 dyrektywy 2016/680 wskazuje, że ta dyrektywa nie ma zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa Unii. Na podstawie cytowanych przepisów można stwierdzić, że prawodawca unijny potwierdził, na przykładzie niniejszego aktu prawnego, że sfera bezpieczeństwa narodowego jest domeną państw członkowskich i to do nich należy regulacja działań w tym zakresie.

Warto wskazać, że ani w przepisach prawa Unii Europejskiej, ani w dotychczasowym orzecznictwie TSUE dotychczas nie wypracowano spójnej, precyzyjnej i jednoznacznej definicji pojęcia bezpieczeństwo narodowe. Ponadto – pomimo braku definicji tego pojęcia, trzeba pamiętać, że zarówno na forum Unii Europejskiej, jak i państw członkowskich pojawiają się również inne pojęcia, znaczeniowo zbliżone do „bezpieczeństwa narodowego", które również nie są precyzyjne zdefiniowane na płaszczyźnie prawa Unii Europejskiej. Są to pojęcia zasadniczo powiązane z szeroko rozumianym bezpieczeństwem: bezpieczeństwo wewnętrzne, bezpieczeństwo państwa, bezpieczeństwo publiczne i bezpieczeństwo obronne. Z uwagi na to, że wszystkie wymienione terminy w większym lub mniejszym stopniu odnoszą się do sfery bezpieczeństwa, pozostają z nią w ścisłej korelacji. Ważny jest też aspekt odnoszący się do bezpieczeństwa narodowego. O tym, czy dana dziedzina lub obszar powinny podlegać sferze tego bezpieczeństwa, nie mogą decydować w sposób kategoryczny wyłącznie argumenty prawne. W rzeczywistości bowiem konieczne jest uwzględnienie bieżącej sytuacji geopolitycznej oraz pozostałych, aktualnych czynników istotnych dla przedmiotowego zagadnienia. Należy zatem przyjąć, że generalnie na forum Unii Europejskiej powszechnie jest akceptowany pogląd, że służby mające ustawowe kompetencje w sferze wywiadowczej oraz kontrwywiadowczej podlegają klauzuli bezpieczeństwa narodowego (co istotne – z uwagi na kryterium podmiotowe, czyli występowanie jako służba odpowiedzialna za tę sferę działań, a nie z uwagi na kryterium przedmiotowe, czyli uznanie, że całe spektrum posiadanych kompetencji odpowiada ściśle określonemu zakresowi). Powinno się tutaj również wskazać na różnice wynikające z odrębności wyżej wymienionych kategorii służb od służb ochrony bezpieczeństwa i porządku publicznego[40], które mogą wykonywać podobne działania, co jednak nie oznacza, że podlegają klauzuli bezpieczeństwa narodowego[41].

[40] Ang. *law enforcement authorities*.

[41] Powyższy pogląd został przedstawiony w: *Working Document on surveillance of electronic communications*…, s. 24.

Reasumując, można stwierdzić, że jedynym organem, który może wprowadzić więcej precyzji do interpretacji pojęcia b e z p i e c z e ń s t w o n a r o d o w e, jest TSUE. Orzecznictwo TSUE w tym zakresie może być pomocne także w związku z oceną stosowania klauzuli bezpieczeństwa narodowego, szczególnie jeśli chodzi o zasadność całkowitego wyłączenia zastosowania poszczególnych przepisów prawa Unii Europejskiej do sfery działalności służb specjalnych w obszarze bezpieczeństwa narodowego oraz ewentualność cząstkowego wyłączenia (rozumianego jako ograniczenie w zakresie stosowania jedynie pewnych aspektów – poszczególnych przepisów prawa Unii Europejskiej z uwagi na bezpieczeństwo narodowe). Powyższe ograniczenie musi wynikać jednakże *explicite* z przepisów danego aktu prawnego[42].

Należy również zwrócić uwagę na to, że ujednolicenie interpretacji pojęcia b e z p i e c z e ń s t w o n a r o d o w e na płaszczyźnie prawa Unii Europejskiej znacząco wpłynęłoby także na stosowanie analogicznej interpretacji tego pojęcia w porządkach krajowych poszczególnych państw członkowskich Unii Europejskiej, co w konsekwencji miałoby istotne znaczenie dla precyzyjnego określenia kompetencji podlegających sferze bezpieczeństwa narodowego na płaszczyźnie krajowej oraz ułatwiłoby dokładne wskazanie, które kompetencje mieszczą się w przedmiotowym zakresie, a które pozostają poza nim.

Sfera bezpieczeństwa narodowego jest najważniejszym aspektem funkcjonowania służb specjalnych mających kompetencje wywiadowcze i kontrwywiadowcze. Dlatego też pozostaje w zakresie wyłącznej kompetencji państw członkowskich Unii Europejskiej, aczkolwiek równie istotne jest dookreślenie zarówno zakresu znaczeniowego przedmiotowego pojęcia, jak i granic jego stosowania w taki sposób, aby nie budziło ono wątpliwości zarówno organów państwa, jak i jego obywateli.

[42] Przykładem może być tutaj *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz. Urz. WE L 281 z 23 XI 1995, s. 31, ze zm.). W art. 3 ust. 2 tej dyrektywy wskazano, że nie ma ona zastosowania do przetwarzania danych osobowych w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy ta działalność dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego. Jednocześnie art. 13 ust. 1 stanowi, że państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianego w art. 6 ust. 1, art. 10, art. 11 ust. 1, art. 12 oraz 21, kiedy takie ograniczenie jest środkiem koniecznym dla zabezpieczenia: a) bezpieczeństwa narodowego; b) obronności; c) bezpieczeństwa publicznego; d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji; e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi; f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c)–e); g) ochrony osoby, której dane dotyczą, oraz praw i wolności innych osób.

Piotr Burczaniuk

System nadzoru i kontroli nad służbami specjalnymi w Polsce – stan obecny na tle analizy prawno-porównawczej wybranych państw. Postulaty *de lege ferenda*

1. Wstęp

Celem niniejszego opracowania jest analiza wybranych aspektów kontroli i nadzoru nad służbami specjalnymi, jakie są wykonywane zarówno przez organy trójpodziału władzy (ustawodawczej, wykonawczej i sądowniczej), jak i w ramach działań prowadzonych przez instytucje autonomiczne, takie jak Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich oraz społeczeństwo obywatelskie. Należy wskazać, że omawiane zagadnienie było i jest poruszane, na gruncie rozważań doktrynalnych, w bogatym dorobku naukowym[1]. Autor ma na celu ujęcie przedmiotowego tematu z perspektywy aktualnego stanu prawnego, w tym *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[2], oraz jego uzupełnienie o analizę prawno-porównawczą modeli nadzoru i kontroli nad służbami, które występują w wybranych porządkach prawnych państw tożsamych kulturowo. Autor pokusił się także o wyprowadzenie postulatów *de lege ferenda*.

Przechodząc do rozważań merytorycznych, za punkt wyjścia należy przyjąć analizę najważniejszych pojęć: k o n t r o l a, n a d z ó r i s ł u ż b y s p e c j a l n e.

W doktrynie prawniczej przez k o n t r o l ę rozumie się porównywanie stanu faktycznego ze stanem wymaganym, wyznaczonym przez normy prawne, techniczne, ekonomiczne itd. K o n t r o l a a d m i n i s t r a c j i polega więc na badaniu jej stanu organizacyjnego oraz zachowania (działania lub niedziałania) ze względu na określone kryteria. Przedmiotem kontroli może więc być zarówno struktura organizacyjna administracji, jak i jej działalność. Z kolei n a d z ó r to stałe i bieżące kontrolowanie podległej lub podporządkowanej jednostki z równoczesnym wydawaniem stosownych decyzji, mających na celu usprawnienie i udoskonalenie działalności nadzorowanej jednostki. Uprawnienia nadzorcze oznaczają tyle, co prawo do kontroli wraz z możliwością wiążącego wpływania na organy czy instytucje nadzorowane[3]. Jak wskazuje Sławomir Zalewski,

> (…) kontrola polityczna oznacza rozciągnięcie pełnej władzy nad instytucjami, które służą ochronie państwa, ochronie jego ważnych interesów oraz zapewnienia bezpieczeństwa jego obywateli. Jak ważna jest rola cywilnej kontroli, obrazuje obecność treści związanych

[1] Szeroko na ten temat pisali m.in. S. Zalewski, *Służby specjalne w państwie demokratycznym*, wyd. 2, Warszawa 2005; M. Bożek, *Nadzór Prezesa Rady Ministrów nad służbami specjalnymi i sposoby jego realizacji w świetle obowiązującego ustawodawstwa*, „Przegląd Sejmowy" 2010, nr 3; P. Pogonowski, *Nadzór nad służbami specjalnymi a bezpieczeństwo państwa na tle doświadczeń krajów demokratycznych*, w: *Interdyscyplinarność nauk o bezpieczeństwie. Paradygmat, wiedza, demarkacja*, K. Raczkowski, K. Żukrowska, M. Żuber (red.), Warszawa 2013; T. Kuć, *Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 190–214.

[2] Dz.U. z 2016 r. poz. 904, ze zm.

[3] M. Wierzbowski, *Prawo administracyjne*, wyd. 4, Warszawa 2001.

> z tym zagadnieniem w ustawach zasadniczych demokratycznych państw, aktach prawa powszechnie obowiązującego, dokumentach politycznych rządów oraz porozumieniach sojuszniczych. Cywilna kontrola nad wojskiem, policją i siłami bezpieczeństwa wyznacza standard demokracji. (…) O ile o kontroli służb specjalnych mówimy w sensie szerszym – obejmującym oddziaływanie polityczne i społeczne, o tyle nadzór nad służbami to instrument państwa demokratycznego, wynikający z ich podporządkowania organom władzy cywilnej. Celem nadzorcy jest zapewnienie efektywnego funkcjonowania służb w określonych warunkach politycznych i prawnych tak, aby zapewniały wsparcie polityki państwa[4].

Zasady wyznaczania linii podziału instytucji sprawujących kontrolę i nadzór nad służbami specjalnymi w Polsce nie są w piśmiennictwie jednolite. Andrzej Żebrowski wyróżnia następujące rodzaje kontroli i nadzoru: polityczny (wykonywany przez parlament oraz podmioty wskazane w konstytucji), administracyjny (realizowany przez Radę Ministrów i podlegle jej organy) oraz prawny (wykonywany przez konstytucyjne organy ochrony prawnej)[5]. Z kolei S. Zalewski przeprowadza linię podziału na podstawie monteskiuszowskiego trójpodziału władzy, wydzielając kontrolę i nadzór sprawowane przez organy władzy ustawodawczej, organy władzy wykonawczej, a także organy władzy sądowniczej[6].

Według autora przyjętą przez S. Zalewkiego linię podziału należy uznać i zaakceptować. W celu pełnego wykazania organów sprawujących nadzór i kontrolę nad służbami specjalnymi należy wyszczególnić również organy ochrony i kontroli prawa[7] jako odrębną kategorię podmiotów, na czele z Najwyższą Izbą Kontroli oraz Rzecznikiem Praw Obywatelskich. Uwagi wymagają również pozycja i znaczenie społeczeństwa obywatelskiego oraz funkcjonalnie z nim sprzężonych mediów.

Pomimo wskazanych powyżej różnic podziałowych, jednolite wydaje się być patrzenie na poszczególne, wymienione instytucje przez pryzmat roli, jaką odgrywają one w tym systemie. Rola władzy wykonawczej koncentruje się na efektywności – służba specjalna jako element egzekutywy sprzężony z nią m.in. administracyjno-prawnym stosunkiem zależności jest rozliczana przez pryzmat celów i zadań stawianych przed nią przez rząd (premiera). Rola władzy sądowniczej jest oparta na elemencie legalistycznym, nakierowanym na nadzór i kontrolę czynności, szczególnie operacyjno-rozpoznawczych, wykonywanych przez służby oraz wyciąganiu konsekwencji w przypadku ich nadużycia (identyfikacji bezprawności działania). Rola ustawodawcy wydaje się nakierowana na trzy elementy: pierwszy – legislacyjny, skoncentrowany na właściwym określeniu zadań i uprawnień służb z uwzględnieniem zasady proporcjonalności przy ograniczaniu konstytucyjnych praw i wolności obywatelskich; drugi – efektywności, nakierowany na realizację celów zidentyfikowanych w drodze demokracji pośredniej przez suwerena; trzeci – legalistyczny, związany z kontrolą przestrzegania obowiązującego prawa, głównie przez zagwarantowanie właściwych narzędzi kontrolnych opozycji parlamentarnej[8].

---

[4] A. Zalewski, *Służby specjalne w państwie*…, s. 105–106.

[5] Zob. A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej*, Kraków 2005, s. 196– 221.

[6] Zob. A. Zalewski, *Służby specjalne w państwie*…, s. 105.

[7] Zgodnie z art. 175 Konstytucji RP wymiar sprawiedliwości w Rzeczpospolitej Polskiej sprawują Sąd Najwyższy, sądy powszechne, sądy administracyjne oraz sądy wojskowe. Wobec tak przyjętego przez ustawę zasadniczą podziału władzy sądowniczej, nie jest możliwe zaliczenie organów ochrony prawa do tej kategorii. Grupa tych podmiotów powinna stanowić odrębny filar wyszczególniony w ramach organów odpowiedzialnych za kontrolę i nadzór nad służbami specjalnymi.

[8] Por. M. Caparini, *Controlling and overseeing intelligence services In democratic states*, w: *Democratic*

Trzecim najważniejszym dla powyższego zagadnienia pojęciem, jest pojęcie służby specjalne. Aktualne akty normatywne wprowadzają w tym zakresie definicję legalną tego pojęcia, ujętą od strony podmiotowej, przez wymienienie enumeratywne podmiotów zaliczanych do służb specjalnych. Zgodnie z art. 11 ustawy o ABW oraz AW – Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne są zwane – na potrzeby tej ustawy – służbami specjalnymi. Ustawa o SKW oraz SWW w art. 4 ust. 2 pkt 3 przyjmuje rozumienie tego pojęcia zgodne z ustawą o ABW oraz AW, natomiast w art. 1 ust. 1 ustawy o CBA wskazano, że tworzy się CBA jako służbę specjalną.

Analogiczną definicję wprowadza też art. 142 ust. 2 *Regulaminu Sejmu RP*, wskazując, że służbami specjalnymi w rozumieniu tego *Regulaminu* są: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne.

2. Kontrola i nadzór nad służbami specjalnymi sprawowane przez organy władzy ustawodawczej

Sejm Rzeczpospolitej Polskiej

Podstawy prawnej uprawnień kontrolnych Sejmu RP wobec służb specjalnych należy poszukiwać w samej Konstytucji Rzeczypospolitej Polskiej. Zgodnie z jej art. 95 ust. 1 władzę ustawodawczą w RP sprawują sejm i senat. W ten sposób oba te konstytucyjne organy władzy, jako elementy demokracji pośredniej, realizują wyrażone przez naród w akcie głosowania oczekiwania, w tym stawiane wobec służb specjalnych, zarówno w wymiarze ich zadań, jak i modelowania narzędzi oraz środków, które są im w drodze ustawy przyznawane. W tej jednej zasadzie ustrojowej są wyrażone więc dwa zadania stawiane przed tym organem władzy w odniesieniu do służb specjalnych, tj. rola legislacyjna (kreator zadań i narzędzi) oraz kontrola efektywności (rozliczanie z jakości wykonanych zadań). Jak wskazuje Tomasz Kuć

> (…) rola władzy ustawodawczej w tworzeniu mechanizmów skutecznego nadzorowania tajnych służb i kontroli nad nimi zarysowuje się już na etapie procesu legislacji. Jest ona pochodną funkcji ustawodawczej parlamentu i chociaż nie można jej traktować jako kontroli sensu stricto, prawne podstawy funkcjonowania służb specjalnych ustanawiane przez Sejm RP określają jednocześnie ramy systemu nadzoru i kontroli nad nimi. Nie mogą one jednak być sprzeczne z ustawą zasadniczą lub odbiegać od międzynarodowych standardów w zakresie ochrony praw i wolności obywatelskich[9].

W tym zakresie ustawy kompetencyjne służb specjalnych podlegają, na zasadach ogólnych, badaniu konstytucyjności, prowadzonej przez Trybunał Konstytucyjny, który dokonuje ich oceny przede wszystkim z punktu widzenia ważenia zasad konstytucyjnych, zwłaszcza zasady bezpieczeństwa, z prawami i wolnościami osobistymi.

Zgodnie z ust. 2 art. 95 Konstytucji RP Sejm RP sprawuje kontrolę nad działalnością Rady Ministrów w zakresie określonym przepisami Konstytucji RP i ustaw.

Control of Intelligence Services, H. Born, M. Caparini (red.), London 2007.

[9] T. Kuć, *Analiza funkcjonalności systemu kontroli*..., s. 201.

> Z treści art. 95 ust. 2 wynika, że Konstytucja RP ustaliła kontrolę reprezentacji Narodu nad działalnością Rady Ministrów. Podkreślić jednak należy, że w zakresie realizacji funkcji kontrolnej uczestniczy tylko Sejm RP, natomiast Senat RP w działaniach tego rodzaju nie bierze udziału, został z nich całkowicie wyłączony. Tezę powyższą uzasadnia fakt, że w ust. 2 wymieniony został tylko Sejm RP, czyli podmiotowy zakres treści ust. 1 i 2 różni się w sposób zasadniczy[10].

Mowa tu oczywiście m.in. o elemencie legalistycznym kontroli. Jej zasady zostały sprecyzowane w trzech aktach ustawodawczych, tj. *Ustawie z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora*[11], *Ustawie z dnia 21 stycznia 1999 r. o sejmowej komisji śledczej*[12] oraz *Uchwale Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. – Regulamin Sejmu Rzeczypospolitej Polskiej*[13]. Również analiza ustaw kompetencyjnych służb specjalnych determinuje ich podległość w zakresie kontroli Sejmowi RP (art. 3 ust. 1 ustawy o ABW oraz AW; art. 5 ust. 2a ustawy o CBA i art. 3 ust. 3 ustawy o SKW oraz SWW).

Kontrola nad służbami specjalnymi sprawowana przez sejm i posłów na podstawie wskazanych aktów prawnych przybiera różne formy. Polega ona głównie na ocenie i prognozowaniu politycznym, prawnym, praksеologicznym i społecznym służb specjalnych. *Ocena ta jest wyrażeniem opinii, poglądów i sugestii o ich faktycznej działalności i obejmuje porównanie osiągniętych wyników z przyjętymi kierunkami działania, wykorzystywania budżetu i przestrzegania norm prawnych*[14].

Posłowie w sprawach dotyczących służb specjalnych mogą kierować do Prezesa Rady Ministrów: interpelacje (za pośrednictwem Marszałka Sejmu), wnioski o przedstawienie informacji bieżących, zapytania poselskie i pytania w sprawach bieżących. W tym zakresie posłowie mogą uzyskiwać od Prezesa Rady Ministrów oraz szefów poszczególnych służb informacje i wyjaśnienia w sprawach wynikających z wykonywania obowiązków poselskich. Co więcej – klubowi poselskiemu oraz grupie co najmniej 15 posłów przysługuje prawo złożenia wniosku o przedstawienie na posiedzeniu Sejmu RP przez członka Rady Ministrów informacji bieżącej. Rozpatrzenie informacji na posiedzeniu Sejmu RP obejmuje przedstawienie uzasadnienia wniosku przez posła wyznaczonego przez podmiot uprawniony do jego złożenia oraz udzielenie odpowiedzi przez przedstawiciela Rady Ministrów. Prezes Rady Ministrów oraz szef danej służby są obowiązani przedstawiać informacje i wyjaśnienia na żądanie stałych i nadzwyczajnych komisji sejmowych, w sprawach będących przedmiotem ich zakresu działania.

Komisja do Spraw Służb Specjalnych

Najważniejszym sejmowym elementem nadzoru nad służbami specjalnymi jest funkcjonująca od 1995 r. Komisja do Spraw Służb Specjalnych. Zgodnie z art. 18 *Regulaminu Sejmu RP* jest ona jedną z 28 komisji stałych działających w Sejmie RP. Zasady i tryb jej pracy zostały określone w osobnym, 12 rozdziale działu II tego aktu prawnego, jej przedmiotowy zakres działania został zaś wyliczony w załączniku do *Regulaminu Sejmu RP*. Zgodnie z nim do zadań Komisji należy:

---

[10] W. Skrzydło, *Komentarz do art. 95 Konstytucji Rzeczypospolitej Polskiej*, LEX/el.
[11] Dz.U. z 2016 r. poz. 1510.
[12] Dz.U. z 2016 r. poz. 1024.
[13] M.P. z 2012 r. poz. 32, ze zm.
[14] A. Żebrowski, *Ewolucja polskich służb specjalnych*…, s. 199.

a) w zakresie legislacji:
   – opiniowanie projektów ustaw, rozporządzeń, zarządzeń oraz innych aktów normatywnych dotyczących służb specjalnych, w tym regulujących działalność tych służb,
   – opiniowanie projektu budżetu w zakresie dotyczącym służb specjalnych;
b) w zakresie opiniodawczym:
   – opiniowanie kierunków działań szefów służb specjalnych,
   – opiniowanie wniosków w sprawie powołania i odwołania poszczególnych osób na stanowiska szefów służb specjalnych i ich zastępców;
c) w zakresie kontrolnym:
   – rozpatrywanie corocznego sprawozdania z wykonania budżetu oraz innych informacji finansowych służb specjalnych,
   – rozpatrywanie corocznych sprawozdań szefów służb specjalnych,
   – zapoznawanie się z informacjami służb specjalnych o szczególnie istotnych wydarzeniach z ich działalności, w tym dotyczących podejrzeń występowania nieprawidłowości w działalności służb specjalnych oraz podejrzeń naruszenia prawa przez te służby, przez dostęp i wgląd do informacji, dokumentów i materiałów uzyskanych w wyniku wykonania zadań ustawowych, zgodnie z przepisami ustawy o ochronie informacji niejawnych[15] oraz ustaw regulujących działalność służb specjalnych (w tym zakresie należy pamiętać o ograniczeniach wynikających z art. 39 ustawy o ABW oraz AW oraz art. 43 ustawy o SKW oraz SWW dotyczących zakazów informacyjnych obejmujących określone w nich: osoby oraz formy i metody pracy operacyjnej tych służb),
   – ocena współdziałania służb specjalnych z innymi organami, służbami i instytucjami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych w zakresie podejmowanych przez nie działań dla ochrony bezpieczeństwa państwa,
   – ocena współdziałania służb specjalnych z siłami zbrojnymi, organami administracji rządowej, organami ścigania i innymi instytucjami państwowymi oraz organami jednostek samorządu terytorialnego, właściwymi organami i służbami specjalnymi innych państw,
   – ocena ochrony informacji niejawnych,
   – badanie skarg dotyczących działalności służb specjalnych.

Ocena służb specjalnych odbywa się w ramach powyższego katalogu na podstawie informacji i sprawozdania szefów służb specjalnych, a także innych uprawnionych osób – w tym m.in. prezesa NIK, rzecznika praw obywatelskich, prokuratora generalnego. W skład Komisji wchodzi nie więcej niż siedmiu posłów. Dostęp członków Komisji do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" określają przepisy ustawy o ochronie informacji niejawnych. Należy wskazać, że Sejmowa Komisja ds. Służb Specjalnych to jedyna komisja sejmowa, w której przypadku regulaminowo posiedzenia odbywają się z wyłączeniem jawności, bez sporządzania biuletynu. Niepisaną zasadą jest również powierzanie naprzemiennie funkcji przewodniczącego Komisji przedstawicielom klubów opozycji parlamentarnej. Warto dodać, że zgodnie z art. 12 ust. 2 ustawy o CBA jej szef przedstawia corocznie, do 31 marca, Sejmowej Komisji do Spraw Służb Specjalnych (oraz Prezesowi Rady Ministrów) sprawozdanie z działalności

[15] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2016 r. poz. 1167, ze zm.).

CBA za poprzedni rok kalendarzowy. Takiego obowiązku sprawozdawczego nie ma żadna z pozostałych służb specjalnych. Ponadto, w odróżnieniu od ABW i AW oraz SKW i SWW szef CBA przedstawia corocznie, do 31 marca, Sejmowi RP oraz Senatowi RP informację o wynikach działalności CBA, z wyjątkiem informacji, do których stosuje się przepisy o ochronie informacji niejawnych.

Senat Rzeczpospolitej Polskiej

W odróżnieniu od uprawnień przysługujących Sejmowi RP, uprawnienia Senatu RP i senatorów w zakresie kontroli nad służbami specjalnymi są niewielkie i ograniczone. W sprawach dotyczących służb specjalnych senatorowie mogą bowiem uzyskiwać od Prezesa Rady Ministrów oraz szefów poszczególnych służb informacje i wyjaśnienia w zakresie wynikającym z wykonywania obowiązków senatorskich. Prezes Rady Ministrów oraz szefowie służb są obowiązani przedstawiać informacje i wyjaśnienia na żądanie stałych i nadzwyczajnych komisji senackich, w sprawach będących przedmiotem zakresu ich działania**.**

3. Kontrola i nadzór nad służbami specjalnymi sprawowane przez organy kontroli państwowej i ochrony prawa

Najwyższa Izba Kontroli

Zgodnie z art. 203 ust. 1 Konstytucji RP Najwyższa Izba Kontroli nadzoruje działalność organów administracji rządowej, w tym szefów służb specjalnych, z punktu widzenia legalności, gospodarności, celowości i rzetelności.

> Należy zauważyć, że NIK jako naczelny organ kontroli państwowej (por. art. 202 ust. 1 Konstytucji RP) jest od strony podmiotowej nie tylko jednym z elementów kontroli sprawowanej przez Sejm RP nad działalnością Rady Ministrów (por. art. 95 ust. 2 Konstytucji RP), lecz także wykonuje kontrolę podmiotów sektora finansów publicznych oraz podmiotów korzystających z funduszy publicznych, które mają niewątpliwie stanowić materiał do prac legislacyjnych w zakresie zmiany obowiązującego prawodawstwa (por. art. 203 Konstytucji RP)[16].

W pierwszej kolejności kontrola NIK jest kontrolą wykonania budżetu i w tym zakresie Izba sprawdza rocznie około 400 jednostek, w tym też służby specjalne. W pozostałym obszarze kontrole są uwzględnione w planie pracy Izby i są wynikiem własnych propozycji oraz sugestii przedstawianych przez organy Sejmu RP i Senatu RP, a także Prezydenta RP i Prezesa Rady Ministrów. Tematyka kontroli na dany rok jest ustalana na podstawie priorytetowych kierunków kontroli uchwalanych przez Kolegium NIK, w których ramach są wyznaczane najważniejsze obszary funkcjonowania państwa, przewidziane do badań w danym roku[17]. Sama kontrola jest przeprowadzana w siedzibie kontrolowanego podmiotu oraz w miejscach wykonywania jego zadań i w godzinach jego pracy. Co istotne – kontroler NIK ma prawo do swobodnego poruszania się po sprawdzanym obiekcie, bez konieczności posiadania przepustki oraz bez rewizji oso-

[16] J. Kulicki, *Kontrola skarbowa w systemie kontroli państwowej*, LEX/el.

[17] *Kontrole NIK*, www.nik.gov.pl/kontrole/informacje-podstawowe-kontrole/ [dostęp: 25 IX 2017].

bistej. Kierownik kontrolowanej jednostki ma obowiązek udostępnić kontrolerowi NIK wszelkie dokumenty i materiały niezbędne do przygotowania i przeprowadzenia kontroli, oczywiście z zachowaniem właściwych przepisów o tajemnicach prawnie chronionych, na czele z przepisami dotyczącymi ochrony informacji niejawnych.

Wyniki przeprowadzonej kontroli kontroler przedstawia w wystąpieniu pokontrolnym, zawierającym opis stanu faktycznego i ocenę kontrolowanej działalności, w tym ustalone nieprawidłowości, ich przyczyny, zakres, skutki, ze wskazaniem osób za nie odpowiedzialnych, a także uwagi i wnioski w sprawie usunięcia stwierdzonych nieprawidłowości. Wystąpienie pokontrolne i zgromadzone materiały dowodowe są podstawą do sporządzenia dokumentu końcowego, tj. informacji o wynikach kontroli, która jest przedkładana m.in. Sejmowi RP, Prezydentowi RP i Prezesowi Rady Ministrów[18].

Rzecznik Praw Obywatelskich

Drugim z wymienionych przez Konstytucję RP organów kontroli państwowej i ochrony prawa jest Rzecznik Praw Obywatelskich. Do jego zadań należy stanie na straży wolności i praw człowieka i obywatela, określonych w Konstytucji oraz w innych aktach normatywnych.

> Obserwując praktykę działania Rzecznika Praw Obywatelskich, można stwierdzić, że nie da się go umieścić w tradycyjnej klasyfikacji trójpodziału władz. Powinien on być raczej rozpatrywany jako podmiot funkcjonujący na linii władza wykonawcza – władza ustawodawcza. Nietrudno bowiem zauważyć, że przedmiotem jego zainteresowań jest obszar działania władzy wykonawczej, a z drugiej strony pozostaje w znacznym powiązaniu z władzą ustawodawczą. Przy omawianiu powyższego zagadnienia nie można oczywiście nie wspomnieć o stosunku urzędu Rzecznika do władzy sądowniczej. Jest to o tyle znaczące, że formy działania Rzecznika Praw Obywatelskich nasuwają pewne analogie z działalnością organów wymiaru sprawiedliwości, a jego kompetencje orientowane są w dużej mierze na ochronę obywatela, co zbliża je do zadań władzy sądowniczej. Stwierdzić jednak trzeba, że zdecydowanie więcej jest różnic niż podobieństw między RPO a sądami[19].

Podjęcie czynności przez Rzecznika następuje na wniosek obywateli lub ich organizacji, na wniosek organów samorządów, Rzecznika Praw Dziecka lub z własnej inicjatywy. Na podstawie skierowanego wniosku Rzecznik może podjąć sprawę i samodzielnie prowadzić postępowanie wyjaśniające lub zwrócić się o zbadanie sprawy lub jej części do właściwych organów, szczególnie organów nadzoru, prokuratury, kontroli państwowej, zawodowej lub społecznej, a także do Sejmu RP o zlecenie Najwyższej Izbie Kontroli przeprowadzenia kontroli w celu zbadania określonej sprawy lub jej części. W ramach tak prowadzonego postępowania RPO może zbadać, nawet bez uprzedzenia, każdą sprawę na miejscu oraz żądać złożenia wyjaśnień, przedstawienia akt każdej sprawy prowadzonej m.in. przez naczelne i centralne organy administracji państwowej, organy administracji rządowej, a więc też przez służby specjalne. Może także żądać przedłożenia informacji o stanie sprawy prowadzonej przez sądy, prokuraturę oraz inne organy ścigania i żądać do wglądu w Biurze Rzecznika Praw Obywatelskich

[18] *Poradnik kontrolowanego*, www.nik.gov.pl/kontrole/poradnik-kontrolowanego/ [dostęp: 25 IX 2017].

[19] Por. A. Deryng, *Rzecznik Praw Obywatelskich jako wnioskodawca w postępowaniu przed Trybunałem Konstytucyjnym*, LEX/el.

akt sądowych i prokuratorskich, a także akt innych organów ścigania – po zakończeniu postępowania i zapadnięciu rozstrzygnięcia. Po zbadaniu sprawy Rzecznikowi przysługuje m.in. prawo do skierowania wystąpienia do organu, organizacji lub instytucji, w których działalności stwierdził naruszenie wolności i praw człowieka oraz obywatela, lub zwrócenie się do organu nadrzędnego nad tą jednostką z wnioskiem o zastosowanie środków przewidzianych w przepisach prawa. Rzecznik Praw Obywatelskich wykonuje swoje zadania przy pomocy podległego mu Biura Rzecznika Praw Obywatelskich, które znajduje się w Warszawie. Zadania i organizację Biura określa statut Biura Rzecznika Praw Obywatelskich.

4. Kontrola i nadzór nad służbami specjalnymi sprawowane przez organy władzy wykonawczej

Prezes Rady Ministrów

Rola władzy wykonawczej w zakresie nadzoru nad służbami specjalnymi koncentruje się na elemencie efektywności – służba specjalna jako cześć egzekutywy opartej na administracyjnym sprzężeniu jest rozliczana przez pryzmat celów i zadań stawianych przed nią m.in. przez rząd (premiera). Zgodnie z art. 146 ustawy zasadniczej Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczpospolitej Polskiej oraz kieruje administracją rządową. Do konstytucyjnych zadań Rady Ministrów należy m.in. zapewnianie bezpieczeństwa wewnętrznego i zewnętrznego państwa oraz porządku publicznego. W tym zakresie część z tych zadań Rada Ministrów realizuje za pośrednictwem wyspecjalizowanych służb, na czele ze służbami specjalnymi, które są zależne administracyjnie od Rady Ministrów. Szef każdej ze służb specjalnych w Polsce odgrywa rolę centralnego organu administracji rządowej (art. 3 ust. 1 ustawy o ABW oraz AW; art. 3 ust. 1 ustawy o SKW oraz SWW; art. 5 ust. 2 ustawy o CBA), sama zaś służba jest urzędem obsługującym ten organ. W ten sposób służba specjalna jest elementem administracji publicznej, wobec której zastosowanie znajdują przepisy prawa administracyjnego, na czele z *Ustawą z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego*[20]. Przekłada się to na sposób działania służby. Jej szef realizuje zadania przez akty prawne o charakterze wewnętrznym, decyzje i zarządzenia, będąc podporządkowanym naczelnemu organowi administracji rządowej. Zgodnie z art. 18 kpa organem naczelnym w stosunku do organów administracji rządowej są: Prezes Rady Ministrów lub właściwi ministrowie. Zasady tego podporządkowania precyzuje art. 33a *Ustawy z dnia 4 września 1999 r. o działach administracji rządowej*[21], zgodnie z którym Prezes Rady Ministrów sprawuje nadzór nad działalnością administracji rządowej nieobjętą zakresem działów tej administracji, wykonywaną m.in. przez: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu i Centralne Biuro Antykorupcyjne. Zakres nadzoru sprawowanego przez Prezesa Rady Ministrów określają ustawy; w tym wypadku są to ustawy kompetencyjne służb specjalnych – w art. 5 ust. 2 ustawy o CBA jest mowa wprost o nadzorze Prezesa Rady Ministrów nad szefem CBA, z kolei w art. 3 ust. 2 ustawy o ABW oraz AW jest mowa o podległości szefów ABW i AW Prezesowi Rady Ministrów[22].

[20] Dz.U. z 2017 r. poz. 1257.

[21] Dz.U. z 2017 r. poz. 888, ze zm.

[22] W podległości wyraża się nie tylko nadzór, lecz przede wszystkim stosunek podporządkowania szefa ABW i AW Prezesowi Rady Ministrów (hierarchicznej podległości). W przypadku szefa CBA mowa jest wyłącznie o nadzorze, jednak z uwagi na przysługujące Prezesowi Rady Ministrów uprawnienia w zakresie

Nieco inaczej ta podległość wygląda w sytuacji szefów Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego, zgodnie bowiem z art. 3 ust. 2 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[23] podlegają oni ministrowi obrony narodowej, z zastrzeżeniem określonych w ustawie uprawnień Prezesa Rady Ministrów lub ministra koordynatora służb specjalnych, w przypadku jego powołania. Co więcej – art. 5 ust. 1 ustawy o CBA wskazuje, że Prezes Rady Ministrów lub wyznaczony przez niego członek Rady Ministrów koordynuje działalność Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego.

> Na płaszczyźnie administracyjnej kontrola cywilnych i wojskowych służb specjalnych, realizowana jest przede wszystkim przez Radę Ministrów i jej uprawnione organy. (…) Kompetencje kontrolne Rady Ministrów podejmowane wobec służb specjalnych mają charakter ogólny i odnoszą się do całego rządu. Szczególne kompetencje w zakresie kierowania, koordynowania i kontrolowania służb specjalnych ustawodawca powierzył Prezesowi Rady Ministrów[24].

Uprawnienia Prezesa Rady Ministrów są elementem jego konstytucyjnych prerogatyw, do których, zgodnie z art. 148, należą m.in.: zapewnienie wykonywania polityki Rady Ministrów i określanie sposobów jej wykonywania, a także koordynacja i kontrola pracy członków Rady Ministrów. Zgodnie z art. 13 ustawy o ABW oraz AW Prezes Rady Ministrów, w celu koordynacji działań w dziedzinie ochrony bezpieczeństwa i obronności państwa, wydaje wiążące wytyczne oraz żąda informacji i opinii m.in. od szefów ABW, AW i CBA – w odniesieniu do ich działalności, oraz od ministra obrony narodowej – w odniesieniu do działalności Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego. Co więcej – Prezes Rady Ministrów w celu zapewnienia wymaganego współdziałania służb specjalnych może żądać od szefów tych służb informacji związanych z planowaniem i wykonywaniem powierzonych zadań (art. 13 ust. 6 ustawy o ABW oraz AW). Uprawnienia Prezesa Rady Ministrów w odniesieniu do poszczególnych służb specjalnych są sprawowane w następujący sposób:

1) wobec Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu:
   - określa kierunki działania Agencji w drodze wytycznych (art. 7 ust. 1 ustawy o ABW oraz AW),
   - wyraża zgodę na podjęcie współdziałania z właściwymi organami i służbami innych państw (art. 8 ust. 1 ustawy o ABW oraz AW),
   - powołuje i odwołuje szefów ABW i AW oraz powierza obowiązki szefów, a także jest właściwy w sprawach wynikających z ich stosunku służbowego (art. 14 ust. 1 i 17 ust. 1 ustawy o ABW oraz AW),
   - nadaje ABW i AW statut, który określa ich organizację wewnętrzną (art. 20 ust. 1 ustawy o ABW oraz AW),
   - wyraża zgodę na kontynuowanie sprawy niepozostającej w kompetencji ABW albo AW (art. 22a ust. 6 ustawy o ABW oraz AW),

---

wydawania wiążących wytycznych i poleceń nie ma wątpliwości, że również w tym wypadku mamy do czynienia z podporządkowaniem.

[23] Dz.U. z 2016 r. poz. 1318, ze zm.

[24] Por. A. Żebrowski, *Ewolucja polskich służb specjalnych*…, s. 210.

- wyraża zgodę na korzystanie przez ABW lub AW z tajnej współpracy z nadawcami lub redaktorami naczelnymi, dziennikarzami lub osobami prowadzącymi działalność wydawniczą (art. 37 ust. 2 ustawy o ABW oraz AW),
- bierze udział w procedurach dotyczących stopni oficerskich: składa wniosek o mianowanie na pierwszy stopień w korpusie oficerskim i na stopień generała brygady oraz mianuje na pozostałe stopnie w korpusie oficerskim, a także decyduje o ich pozbawieniu i przywróceniu (art. 67 ust. 4, art. 75 i art. 76 ustawy o ABW oraz AW),
- wyraża zgodę na sprawowanie przez funkcjonariuszy ABW lub AW funkcji związanych z byciem członkami zarządu, rady nadzorczej lub komisji rewizyjnej spółek prawa handlowego, spółdzielni, z wyjątkiem rad nadzorczych spółdzielni mieszkaniowej, fundacji prowadzących działalność gospodarczą oraz posiadanie w spółkach prawa handlowego więcej niż 10 proc. akcji lub udziały przedstawiające więcej niż 10 proc. kapitału zakładowego, w każdej z tych spółek, a także prowadzenie działalności gospodarczej na własny rachunek lub wspólnie z innymi osobami, a także zarządzanie taką działalnością lub bycie przedstawicielem czy pełnomocnikiem w prowadzeniu takiej działalności (art. 79a ust. 2 ustawy o ABW oraz AW);

2) wobec Centralnego Biura Antykorupcyjnego:
   - wyraża zgodę na podjęcie przez CBA współpracy z właściwymi organami i służbami innych państw oraz z organizacjami międzynarodowymi (art. 2 ust. 2a ustawy o CBA),
   - powołuje na czteroletnią kadencję i odwołuje szefa CBA oraz powierza obowiązki szefowi, a także jest właściwy w sprawach wynikających z ich stosunku służbowego (art. 6 ust. 1, art. 9, art. 54a ustawy o CBA),
   - powołuje i odwołuje zastępców szefa CBA (art. 6 ust. 4 ustawy o CBA),
   - nadaje CBA statut, w którym określa jego organizację wewnętrzną (art. 11 ust. 1 ustawy o CBA),
   - określa kierunki działania CBA w drodze wytycznych (art. 12 ust. 1 ustawy o CBA),
   - wyraża zgodę na zwolnienie ze służby lub odwołanie pełnomocnika do spraw kontroli przetwarzania przez CBA danych osobowych (art. 22b ust. 1 ustawy o CBA),
   - wyraża zgodę na korzystanie przez CBA z tajnej współpracy z nadawcami oraz redaktorami naczelnymi, dziennikarzami lub osobami prowadzącymi działalność wydawniczą (art. 26 ust. 2 ustawy o CBA),
   - dokonuje uzgodnień odpowiednio z Marszałkiem Sejmu RP lub Marszałkiem Senatu RP dotyczących kontroli lub poszczególnych jej czynności przeprowadzanych w obiektach pozostających w zarządzie Kancelarii Sejmu RP i Kancelarii Senatu RP (art. 36 ust. 3 ustawy o CBA),
   - przyjmuje oświadczenia majątkowe szefa CBA i zastępców szefa CBA oraz dokonuje analizy danych w nich zawartych (art. 72 ust. 3 ustawy o CBA);
3) wobec Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego:
   - zatwierdza wytyczne określające kierunki działania SKW oraz SWW określone przez ministra obrony narodowej, w uzgodnieniu z ministrem koordynatorem służb specjalnych (art. 7 ust. 1 ustawy o SKW oraz SWW),
   - wyraża zgodę (po zasięgnięciu opinii ministra obrony narodowej) na podjęcie współdziałania z właściwymi organami i służbami innych państw (art. 9 ust. 2 ustawy o SKW oraz SWW),

- powołuje i odwołuje szefów SKW oraz SWW na wniosek ministra obrony narodowej oraz powierza obowiązki szefa, a także jest właściwy w sprawach wynikających z ich stosunku służbowego (art. 13 ust. 1, art. 18 ustawy o SKW oraz SWW),
- wyraża zgodę na nadanie przez ministra obrony narodowej statutu SKW oraz SWW (art. 21 ust. 1 ustawy o SKW oraz SWW),
- wyraża zgodę na kontynuowanie sprawy niepozostającej w kompetencji SKW lub SWW (art. 27 ust. 6 ustawy o SKW oraz SWW),
- wyraża zgodę na sprawowanie przez funkcjonariuszy SKW lub SWW funkcji związanych z byciem członkami zarządu, rady nadzorczej lub komisji rewizyjnej spółek prawa handlowego, spółdzielni, z wyjątkiem rad nadzorczych spółdzielni mieszkaniowej, fundacji prowadzących działalność gospodarczą oraz posiadanie w spółkach prawa handlowego więcej niż 10 proc. akcji lub udziały przedstawiające więcej niż 10 proc. kapitału zakładowego – w każdej z tych spółek, a także prowadzenie działalności gospodarczej na własny rachunek lub wspólnie z innymi osobami oraz zarządzanie taką działalnością lub bycie przedstawicielem czy pełnomocnikiem w prowadzeniu takiej działalności (art. 41 ust. 3 ustawy o SKW oraz SWW).

Zgodnie z ustawami kompetencyjnymi służb specjalnych na ich szefach ciążą określone obowiązki planistyczne oraz sprawozdawcze. I tak – zgodnie z art. 7 ust. 2 ustawy o ABW oraz AW szefowie tych służb najpóźniej na trzy miesiące przed końcem roku kalendarzowego przedstawiają Prezesowi Rady Ministrów, każdy w zakresie swojej właściwości, roczne plany działania na rok następny, a także przedstawiają mu corocznie do 31 stycznia sprawozdania z działalności obydwu Agencji za poprzedni rok kalendarzowy. Analogicznie, zgodnie z art. 12 ust. 2 ustawy o CBA, jej szef, najpóźniej na dwa miesiące przed końcem roku kalendarzowego przedstawia Prezesowi Rady Ministrów do zatwierdzenia roczny plan działania CBA na rok następny, a także przedstawia corocznie do 31 marca Prezesowi Rady Ministrów oraz – w odróżnieniu od ABW i AW – Sejmowej Komisji do Spraw Służb Specjalnych sprawozdanie z działalności CBA za poprzedni rok kalendarzowy. Pełnomocnik do spraw kontroli przetwarzania danych osobowych przez CBA, działający wyłącznie w tej strukturze (w innych służbach specjalnych tego typu pełnomocnik nie działa), przedstawia corocznie do 31 marca Prezesowi Rady Ministrów, Sejmowej Komisji do Spraw Służb Specjalnych oraz Generalnemu Inspektorowi Ochrony Danych Osobowych – za pośrednictwem szefa CBA – sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym oraz wszystkie przypadki naruszenia przepisów w tym zakresie.

W przypadku wojskowych służb specjalnych obowiązki planistyczne szefów SKW oraz SWW są nakierowane na ministra obrony narodowej. Corocznie sprawozdania z działalności i wykonania budżetu SKW oraz SWW za poprzedni rok kalendarzowy szefowie tych służb przedstawiają do 31 marca Prezesowi Rady Ministrów i ministrowi obrony narodowej. Te plany i sprawozdania oraz wspomniane wytyczne zatwierdza minister obrony narodowej i przekazuje je niezwłocznie Prezydentowi Rzeczpospolitej Polskiej.

Prezes Rady Ministrów oraz Rada Ministrów w sposób istotny kształtują funkcjonowanie służb specjalnych przez tworzenie na poziomie aktów wykonawczych podstaw prawnych ich działania. Wobec Prezesa Rady Ministrów jest skierowanych 46 delegacji

ustawowych zawartych w ustawie o ABW oraz AW, 24 delegacje są zawarte w ustawie o CBA oraz 3 delegacje są zawarte w ustawie o SKW oraz SWW. Rada Ministrów ma upoważnienie do stanowienia prawa w ramach: czterech delegacji ustawowych zawartych w ustawie o ABW oraz AW i czterech zawartych w ustawie o CBA. Brakuje natomiast podstaw do takiego działania określonych w ustawie o SKW oraz SWW. Z kolei w zakresie dotyczącym aktów prawnych o charakterze wewnętrznym Prezesowi Rady Ministrów powierzono wydanie zarządzeń wobec ABW oraz AW w pięciu zakresach spraw, w przypadku CBA zaś – w trzech zakresach spraw. Do kompetencji Prezesa RM należy określenie:

1) statutu (ABW, AW, CBA),
2) sposobu i trybu realizacji przez szefów służb obowiązków związanych z przekazywaniem spraw zgodnie z właściwością (ABW, AW, CBA),
3) sposobu współdziałania właściwych organów, służb i instytucji państwowych z szefem ABW – przy prowadzeniu rejestru sporządzonych i wydanych dokumentów uniemożliwiających ustalenie danych identyfikujących funkcjonariuszy i pracowników tych organów, służb lub instytucji oraz osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych,
4) sposobu współdziałania służb specjalnych z szefem ABW w zakresie prowadzenia ewidencji zainteresowań operacyjnych służb specjalnych,
5) zakresu i trybu współdziałania oraz szczegółowego rozdziału kompetencji między ABW, AW, SKW, SWW i CBA,
6) warunków, zakresu i trybu współdziałania szefów: CBA, ABW, SKW oraz komendanta głównego Policji, komendanta głównego Straży Granicznej, komendanta głównego Żandarmerii Wojskowej i szefa Krajowej Administracji Skarbowej w zakresie zwalczania korupcji w instytucjach państwowych i samorządzie terytorialnym oraz w życiu publicznym i gospodarczym, a także działalności godzącej w interesy ekonomiczne państwa oraz koordynacji dokonywanej przez szefa CBA w zakresie działań o charakterze operacyjno-rozpoznawczym i informacyjno-analitycznym, podejmowanych przez te organy, które mogą mieć wpływ na realizację zadań CBA.

Z kolei w odniesieniu do służb wojskowych stanowienie aktów o charakterze wewnętrznym zostało powierzone ministrowi obrony narodowej, który posiada w tym zakresie kompetencję w pięciu kategoriach spraw. Szczegółowy zakres delegacji ustawowych zawartych w ustawach kompetencyjnych służb specjalnych obrazuje tabela.

Tabela. Liczba upoważnień ustawowych zawartych w ustawach kompetencyjnych służb specjalnych.

Rodzaj aktu prawnego i organ uprawniony do stanowienia	**Ustawa o ABW oraz AW**	**Ustawa o SKW oraz SWW**	**Ustawia o CBA**
	46	**3**	**24**
Rozporządzenia Prezesa Rady Ministrów	tj. art. 23 ust. 9, art. 27 ust. 18, art. 29 ust. 5, art. 30 ust. 5, art. 32a ust. 13, art. 32c ust. 14, art. 34 ust. 3, art. 34 ust. 4, art. 34a ust. 15, art. 36 ust. 5, art. 45 ust. 2, art. 46 ust. 3, art. 48 ust. 5, art. 51 ust. 2, art. 53 ust. 3, art. 54 ust. 4, art. 56 ust. 3, art. 59a ust. 12, art. 65 ust. 3, art. 71 ust. 1, art. 78, art. 86 ust. 2, art. 87 ust. 1, art. 88 ust. 2, art. 89 ust. 2, art. 90 ust. 4, art. 90 ust. 6, art. 92a ust. 9, art. 94, art. 96 ust. 2, art. 97 ust. 4, art. 100, art. 106 ust. 2, art. 107 ust. 3, art. 108 ust. 5, art. 111, art. 116 ust. 1, art. 116 ust. 2, art. 119 ust. 3, art. 125 ust. 2, art. 126 ust. 2, art. 127, art. 134a ust. 3, art. 137, art. 142 ust. 3, art. 152 ust. 1	tj. art. 10 ust. 4, art. 31 ust. 16, art. 38 ust. 4	tj. art. 14 ust. 9, art. 17 ust. 18, art. 19 ust. 6, art. 23 ust. 15, art. 25 ust. 5, art. 33 ust. 8, art. 50 ust. 4, art. 52 ust. 3, art. 54 ust. 5, art. 55 ust. 2, art. 57 ust. 4, art. 58 ust. 4, art. 60 ust. 3, art. 69 ust. 3, art. 72 ust. 6, art. 80 ust. 9, art. 83, art. 85 ust. 5, art. 87 ust. 1, art. 90 ust. 1, art. 90 ust. 3, art. 94 ust. 2, art. 95 ust. 2, art. 140

Źródło: Opracowanie własne.

Rozporządzenia Rady Ministrów	**4** tj. art. 12 ust. 9, art. 24 ust. 2, art. 32a ust. 14, art. 114 ust. 4	–	**4** tj. art. 14 ust. 10, art. 14 ust. 11, art. 47, art. 89 ust. 6
Zarządzenia Prezesa Rady Ministrów	**5** tj. art. 20 ust. 1; art. 22a ust. 9 – nie podlega ogłoszeniu, art. 35 ust. 7, art. 40 ust. 3, art. 42 ust. 2	–	**3** tj. art. 11 ust. 1, art. 24 ust. 5, art. 29 ust. 3
Zarządzenia Rady Ministrów	**1** tj. art. 23 ust. 10	–	–
Zarządzenia ministra obrony narodowej po uzyskaniu zgody PRM	–	**3** art. 21 ust. 1, art. 27 ust. 9	–
Zarządzenia ministra obrony narodowej	–	**5** art. 8 – nie podlega ogłoszeniu, art. 10 ust. 2 – nie podlega ogłoszeniu, art. 10 ust. 2a – nie podlega ogłoszeniu, art. 10 ust. 3 (z MSZ) – nie podlega ogłoszeniu, art. 22 ust. 4	–
Rozporządzenia ministra obrony narodowej	–	**8** art. 28 ust. 2, art. 29 ust. 4, art. 33 ust. 5, art. 34 ust. 5, art. 38 ust. 3, art. 47 ust. 2, art. 48 ust. 2, art. 50 ust. 3	–

Minister koordynator służb specjalnych

Jednym z najistotniejszych elementów związanych z nadzorem i kontrolą nad służbami specjalnymi w Polsce, umiejscowionym w ramach egzekutywy, jest stanowisko ministra koordynatora służb specjalnych. W przypadku tego podmiotu mamy do czynienia z wysokim poziomem skomplikowania jego pozycji prawno-ustrojowej, zarówno w odniesieniu do podległych mu służb, jak i związanych z jego pozycją w ramach struktury Rady Ministrów. Wskazać bowiem należy, że jest to stanowisko niestałe, w pełni uzależnione od woli Prezesa Rady Ministrów, który na podstawie art. 148 Konstytucji RP powierza mu wykonywanie zadań delegowanych z pierwotnych uprawnień samego szefa rządu, w sposób określony w art. 33 ust. 1 *Ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów*[25], tj. przez wydanie rozporządzenia określającego zakres jego działania, co czyni go tzw. ministrem bez teki. Tę sytuację komplikuje ponadto jego pozycjonowanie ustrojowe w odniesieniu do wojskowych służb specjalnych, w których te uprawnienia są rozdzielane w specyficzny sposób pomiędzy ministra koordynatora a ministra obrony narodowej.

Obsługę ministra ma zapewniać wyznaczone przez Prezesa Rady Ministrów ministerstwo bądź inny urząd centralny – w dotychczasowej praktyce zawsze była to Kancelaria Prezesa Rady Ministrów. Pomimo że zadania realizowane przez ministra koordynatora są uzależnione od zakresu upoważnienia udzielonego mu przez Prezesa Rady Ministrów we wskazanym powyżej rozporządzeniu, ustawy kompetencyjne służb specjalnych jednocześnie wiążą z jego powołaniem określone prerogatywy, automatycznie przechodzące spod Prezesa Rady Ministrów na jego osobę bądź włączają go wraz z powołaniem w istniejące procedury nadzorcze. W tym zakresie minister koordynator ma następujące uprawnienia:

1) wynikające z ustawy o ABW oraz AW:
   - wnioskuje do Prezesa Rady Ministrów o wydanie wiążących wytycznych w celu koordynowania działań w dziedzinie ochrony bezpieczeństwa i obronności państwa – jednak wyłącznie w zakresie dotyczącym działalności ABW, AW, SKW oraz SWW (art. 13 ust. 2),
   - w razie konieczności współpracy służb specjalnych w celu realizacji ustawowych zadań Prezes Rady Ministrów powierza obowiązek koordynacji działań w tym zakresie ministrowi powołanemu w celu koordynowania działalności tych służb albo szefowi jednej ze służb (art. 13 ust. 8),
   - wyraża zgodę na kontynuowanie sprawy niepozostającej w kompetencji ABW albo AW (art. 22a ust. 6),
   - wyraża opinię w sprawie decyzji szefa ABW dotyczącej odstąpienia od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa szpiegostwa albo uprawdopodobnienia działalności zmierzającej do popełnienia przestępstwa o charakterze terrorystycznym oraz osobie, która według uzyskanych przez ABW informacji lub materiałów może być jego sprawcą – gdy jest to uzasadnione względami bezpieczeństwa państwa (art. 22b ust. 3),
   - wyraża zgodę na korzystanie przez ABW lub AW z tajnej współpracy z nadawcami lub redaktorami naczelnymi, dziennikarzami lub osobami prowadzącymi działalność wydawniczą (art. 37 ust. 3),

[25] Dz.U. z 2012 r. poz. 392, ze zm.

- jest właściwy w sprawach wynikających ze stosunku służbowego szefa ABW oraz szefa AW (art. 50a),
- wyraża zgodę na sprawowanie przez funkcjonariuszy ABW lub AW funkcji związanych z byciem członkami zarządu, rady nadzorczej lub komisji rewizyjnej spółek prawa handlowego, spółdzielni, z wyjątkiem rad nadzorczych spółdzielni mieszkaniowej, fundacji prowadzących działalność gospodarczą oraz posiadanie w spółkach prawa handlowego więcej niż 10 proc. akcji lub udziałów przedstawiających więcej niż 10 proc. kapitału zakładowego, w każdej z tych spółek, a także prowadzenie działalności gospodarczej na własny rachunek lub wspólnie z innymi osobami oraz zarządzanie taką działalnością lub bycie przedstawicielem czy pełnomocnikiem w prowadzeniu takiej działalności (art. 79a ust. 3);

2) wynikające z ustawy o CBA:
   - koordynuje działalność CBA, ABW, AW, SKW oraz SWW (art. 5 ust. 3),
   - wyraża zgodę na korzystanie przez CBA z tajnej współpracy z nadawcami oraz redaktorami naczelnymi, dziennikarzami lub osobami prowadzącymi działalność wydawniczą (art. 26 ust. 3),
   - jest właściwy w sprawach wynikających ze stosunku służbowego szefa CBA (art. 54a);
3) wynikające z ustawy o SKW oraz SWW:
   - uzgadnia wytyczne określające kierunki działania SKW oraz SWW określone przez ministra obrony narodowej (art. 7 ust. 1),
   - wyraża zgodę na kontynuowanie sprawy niepozostającej w kompetencji SKW lub SWW (art. 27 ust. 7),
   - wyraża opinię w sprawie decyzji szefa SKW dotyczącej odstąpienia od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa szpiegostwa albo uprawdopodobnienia działalności zmierzającej do popełnienia przestępstwa o charakterze terrorystycznym oraz osobie, która według uzyskanych przez SKW informacji lub materiałów może być jego sprawcą, gdy jest to uzasadnione względami bezpieczeństwa państwa (art. 27a ust. 3),
   - wyraża zgodę na sprawowanie przez funkcjonariuszy SKW lub SWW funkcji związanych z byciem członkami zarządu, rady nadzorczej lub komisji rewizyjnej spółek prawa handlowego, spółdzielni, z wyjątkiem rad nadzorczych spółdzielni mieszkaniowej, fundacji prowadzących działalność gospodarczą oraz posiadanie w spółkach prawa handlowego więcej niż 10 proc. akcji lub udziałów przedstawiających więcej niż 10 proc. kapitału zakładowego, w każdej z tych spółek, a także prowadzenie działalności gospodarczej na własny rachunek lub wspólnie z innymi osobami, jak również zarządzanie taką działalnością lub bycie przedstawicielem czy pełnomocnikiem w prowadzeniu takiej działalności (art. 41 ust. 4).

Należy zwrócić uwagę także na odmienną siatkę terminologiczną określającą osobę ministra koordynatora. Ustawa o ABW oraz AW posługuje się zwrotem „minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych", z kolei ustawa o CBA stanowi o „powoływanym ministrze w celu koordynowania działalności służb specjalnych", ustawa o SKW oraz SWW w art. 4 ust. 2 pkt 3 wprowadza zaś definicję legalną tego pojęcia, określając, że gdy mowa jest o *Ministrze*

Koordynatorze Służb Specjalnych – należy przez to rozumieć *Ministra – członka Rady Ministrów*, którego zakres działania jest wyznaczony na podstawie art. 33 ust. 1 *Ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów*[26] i obejmuje zadania związane z działalnością służb specjalnych w rozumieniu ustawy o ABW oraz AW, w tym koordynację działalności tych służb.

Po raz pierwszy koordynator służb specjalnych został powołany na mocy *Rozporządzenia Prezesa Rady Ministrów z dnia 13 stycznia 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Zbigniewa Siemiątkowskiego*[27] w celu wykonywania zadań wyznaczonych przez Prezesa Rady Ministrów związanych zwłaszcza z inicjowaniem, programowaniem i koordynowaniem działań Urzędu Ochrony Państwa i Wojskowych Służb Informacyjnych oraz podejmowanych w celu ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej, Żandarmerii Wojskowej i innych jednostek. Te jego uprawnienia były skoncentrowane na czterech wyodrębnionych tematycznie zagadnieniach:

1) projektowych – w zakresie polityki bezpieczeństwa państwa realizowanych przez UOP i WSI, w zakresie planów i kierunków ich działania oraz rozwiązań legislacyjnych w tym zakresie, a także dokonywaniu ocen stanu bezpieczeństwa państwa i wykonywanych przez te służby zadań,
2) realizacji części zadań nadzorczych Prezesa Rady Ministrów nad UOP oraz związanych z odpowiedzialnością za działalność obu służb specjalnych,
3) wykonywaniu oraz nadzorowaniu zadań i misji specjalnych w dziedzinie bezpieczeństwa państwa wyznaczonych przez Prezesa Rady Ministrów,
4) reprezentowaniu Prezesa Rady Ministrów w kontaktach międzynarodowych związanych z działalnością służb specjalnych.

Tożsame uprawnienia koordynacyjne miał kolejny koordynator służb specjalnych, Janusz Pałubicki, powołany *Rozporządzeniem Prezesa Rady Ministrów z dnia 7 listopada 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Janusza Pałubickiego*[28]. Istotna zmiana w zakresie zadań i uprawnień, w które został wyposażony koordynator, nastąpiła wraz z powołaniem na to stanowisko Zbigniewa Wassermana *Rozporządzeniem Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie szczegółowego zakresu działania Ministra – członka Rady Ministrów – Koordynatora Służb Specjalnych, Zbigniewa Wassermanna*[29]**.** Powierzono mu wykonywanie wyznaczonych przez Prezesa Rady Ministrów zadań, w tym: realizację czynności wynikających z bezpośredniej podległości szefów ABW oraz AW, wykonywanie czynności wynikających ze sprawowanej przez Prezesa Rady Ministrów funkcji nadzoru nad działalnością ABW, AW oraz CBA, z wyłączeniem nadzoru procesowego, koordynowanie i kontrolowanie działalności służb specjalnych oraz ich współdziałania z innymi służbami i organami ochrony prawa, koordynowanie współdziałania służb specjalnych z właściwymi organami i służbami innych państw oraz wykonywanie i nadzorowanie innych wyznaczonych przez Prezesa Rady Ministrów zadań w dziedzinie bezpieczeństwa państwa, w tym misji specjalnych. Koordynator został wyposażony w wiele uprawnień, w tym tożsamych z poprzednikami, ale uzyskał również prawo żądania informacji i opinii w odniesieniu do działalności ABW, AW i CBA oraz żądania od szefów ABW,

[26] Dz.U. z 2012 r. poz. 392 oraz z 2015 r. poz. 1064.
[27] Dz.U. z 1997 r. poz. 27.
[28] Dz.U. z 1997 r. poz. 924, ze zm.
[29] Dz.U. z 2006 r. poz. 998.

AW, CBA oraz SKW oraz SWW (po zawiadomieniu ministra obrony narodowej) informacji, dokumentów i sprawozdań dotyczących poszczególnej sprawy albo rodzaju spraw. Minister miał także uprawnienie do wnioskowania do Prezesa Rady Ministrów o zastosowanie środków nadzoru, określonych w ustawach, wynikających z odpowiedzialności za działania służb specjalnych i organów oraz do prowadzenia postępowań kontrolnych realizacji zadań służb specjalnych, a także ich współdziałania z organami w dziedzinie ochrony bezpieczeństwa państwa. W latach 2007–2008 zadania związane z koordynacją realizował Paweł Graś w ramach stanowiska pełnomocnika rządu ds. bezpieczeństwa i koordynowania służb specjalnych. *Rozporządzeniem Prezesa Rady Ministrów z dnia 24 listopada 2011 r. w sprawie szczegółowego zakresu działania Jacka Cichockiego-Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych*[30], na stanowisko to został powołany Jacek Cichocki, a na mocy *Rozporządzenia Prezesa Rady Ministrów z dnia 28 lutego 2013 r. w sprawie szczegółowego zakresu działania Bartłomieja Sienkiewicza-Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych*[31] realizację tych zadań przejął Bartłomiej Sienkiewicz. Po analizie obu rozporządzeń można wywnioskować, że realizowane przez obu koordynatorów zadania były tożsame i oscylowały wokół zagadnień legislacyjnych związanych z prowadzeniem procesu legislacyjnego projektów aktów prawnych dotyczących służb specjalnych, prawem żądania od szefów służb specjalnych informacji związanych z planowaniem i wykonywaniem powierzonych im zadań, a także zapewnianiem współdziałania służb specjalnych w celu realizacji ich ustawowych zadań oraz prawem zapoznawania się z informacjami przedstawianymi przez służby specjalne.

> Zmiana rządu spowodowana werdyktem wyborczym z jesieni 2016 r. stała się przyczynkiem do kolejnej zmiany koncepcji prowadzenia nadzoru nad służbami specjalnymi przez egzekutywę. Sprowadza się ona do scedowania zasadniczej części prerogatyw i obowiązków szefa rządu na członka Rady Ministrów zajmującego się jedynie kontrolą i nadzorem nad służbami[32].

Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra-Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych[33] w sposób wyraźny wyróżniło i wydzieliło jego zadania w zakresie nadzoru i kontroli nad służbami specjalnymi oraz koordynowania tych zadań. W ramach zadań nadzorczych Prezes Rady Ministrów powierzył mu:

1) wyznaczanie strategicznych kierunków rozwoju i funkcjonowania służb specjalnych,
2) badanie, ocenianie i monitorowanie poprawności realizacji przez służby specjalne zadań określonych w przepisach prawa, wytycznych, planach i programach,
3) opracowywanie programów działalności służb specjalnych w dziedzinie ochrony bezpieczeństwa państwa, stanowiących podstawę wydawania wytycznych dla tych służb,
4) zatwierdzanie rocznych planów i sprawozdań przygotowywanych przez szefów służb specjalnych,

[30] Dz.U. z 2011 r. poz. 1524.
[31] Dz.U. z 2013 r. poz. 272.
[32] Por. T. Kuć, *Analiza funkcjonalności systemu kontroli…*, s. 198.
[33] Dz.U. z 2015 r. poz. 1921.

5) dokonywanie oceny stopnia realizacji rocznych planów działalności służb specjalnych oraz formułowanie wniosków i rekomendacji wynikających z tej oceny,
6) wyznaczanie celów i kierunków rozwoju współpracy międzynarodowej służb specjalnych oraz dokonywanie oceny efektów tej współpracy,
7) wyznaczanie standardów i minimalnych wymagań w zakresie zarządzania zasobami ludzkimi i mieniem w służbach specjalnych,
8) analizowanie i dokonywanie oceny działań związanych z realizowanymi przez ABW i SKW zadaniami z obszaru ochrony informacji niejawnych, o którym mowa w art. 10 ust. 1 ustawy o ochronie informacji niejawnych,
9) rozpatrywanie skarg na działalność służb specjalnych.

Z kolei w ramach działań kontrolnych zadaniem koordynatora pozostaje:

1) przeprowadzanie kontroli w służbach specjalnych na zasadach i w trybie określonych w przepisach o kontroli w administracji rządowej,
2) przeprowadzanie kontroli prawidłowości realizacji postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego na zasadach i w trybie określonym w przepisach o ochronie informacji niejawnych,
3) analizowanie i dokonywanie oceny stosowania przez służby specjalne uprawnień umożliwiających ingerencję w prawa i wolności człowieka i obywatela.

W ramach uprawnień koordynacyjnych minister koordynator m.in. podejmuje działania służące zapewnieniu współdziałania służb specjalnych w ramach przyznanych im kompetencji i postawionych przed nimi zadań, organizuje współpracę służb specjalnych z innymi służbami i instytucjami realizującymi zadania w zakresie bezpieczeństwa państwa oraz zapewnia optymalne warunki współpracy służb specjalnych ze służbami specjalnymi innych państw i organizacjami międzynarodowymi, rozstrzyga spory kompetencyjne między służbami specjalnymi, a także wykonuje zadania o charakterze legislacyjnym wobec służb specjalnych.

W celu realizacji wskazanych zadań ministrowi przyznano wiele uprawnień związanych z prawem do:

1) żądania informacji, w tym niejawnych, dokumentów, analiz i sprawozdań okresowych lub dotyczących poszczególnej sprawy albo rodzaju spraw od szefów służb specjalnych oraz informacji dotyczących budżetu i polityki kadrowej służb, a także informacji określonych w ustawach kompetencyjnych służb,
2) wydawania szefom służb specjalnych wiążących ich wytycznych i poleceń,
3) wydawania decyzji i zgody sprecyzowanych w ustawach kompetencyjnych służb,
4) występowania do członków Rady Ministrów oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach nadzoru, kontroli nad służbami specjalnymi i koordynacji ich działalności,
5) zapoznawania się z informacjami, w tym mogącymi mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczpospolitej Polskiej.

Kolegium do Spraw Służb Specjalnych

Kolegium do Spraw Służb Specjalnych zostało powołane na mocy art. 34 *Ustawy z dnia 8 sierpnia 1996 r. o zmianie niektórych ustaw normujących funkcjonowanie gospodarki i administracji publicznej*[34], nowelizującego *Ustawę z dnia 6 kwietnia 1990 r.*

[34] Dz.U. z 1996 r. poz. 496, ze zm.

o Urzędzie Ochrony Państwa[35]. Było to ściśle związane ze zmianą koncepcji nadzoru nad służbami specjalnymi, szczególnie Urzędu Ochrony Państwa. W następstwie wejścia w życie wskazanych przepisów od 1 października 1996 r. nadzór nad tą służbą przeszedł spod jurysdykcji ministra spraw wewnętrznych na Prezesa Rady Ministrów. Kolegium zostało ukształtowane jako ciało o charakterze kolegialnym, pod przewodnictwem Prezesa Rady Ministrów. W jego składzie znaleźli się: minister spraw wewnętrznych i administracji, minister spraw zagranicznych, minister obrony narodowej, szef Urzędu Ochrony Państwa, sekretarz Komitetu Obrony Kraju, przewodniczący Stałego Komitetu Rady Ministrów właściwego w sprawach zewnętrznego i wewnętrznego bezpieczeństwa państwa oraz przedstawiciel Prezydenta RP. W pracach Kolegium uczestniczył także sekretarz Kolegium, powoływany i odwoływany przez Prezesa Rady Ministrów. Co istotne – zgodnie z *Rozporządzeniem Rady Ministrów z dnia 10 czerwca 1997 r. w sprawie zadań, szczegółowych zasad i trybu funkcjonowania Kolegium do Spraw Służb Specjalnych przy Radzie Ministrów, zasad udziału w posiedzeniach Kolegium przedstawicieli służb specjalnych i innych właściwych organów, a także zakresu czynności Sekretarza Kolegium*[36] swoje zadania wykonywał on przy pomocy Sekretariatu Kolegium, będącego komórką organizacyjną Kancelarii Prezesa Rady Ministrów, w sprawach należących do jego zakresu działania zaś, – był uprawniony do zwracania się do organów administracji rządowej o przedstawienie, na potrzeby Kolegium, informacji niezbędnych do właściwego rozpatrzenia spraw. Wskazana powyżej sytuacja jest o tyle istotne, że pozycja sekretarza Kolegium, a zwłaszcza tworzonego przy nim sekretariatu, stała się pierwszą namiastką quasi-urzędu związanego z nadzorowaniem, kontrolą i koordynacją służb specjalnych. Omawiane przepisy dotyczące Kolegium właściwie w niezmienionej formie zostały wprowadzone do ustawy o ABW oraz AW jako jej rozdział 2. Wskazano w nim, że Kolegium działa przy Radzie Ministrów jako organ opiniodawczo-doradczy w sprawach programowania, nadzorowania i koordynowania działalności ABW, AW, SKW, SWW i CBA oraz działań Policji, Straży Granicznej, Żandarmerii Wojskowej, Służby Więziennej, Biura Ochrony Rządu, Służby Celnej, urzędów skarbowych, izb skarbowych, organów kontroli skarbowej, organów informacji finansowej oraz służb rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej – podejmowanych w celu ochrony bezpieczeństwa państwa. Do zadań Kolegium należy formułowanie ocen lub wyrażanie opinii m.in. w sprawach:

- powoływania i odwoływania szefów służb,
- ustalania kierunków i planów działania służb specjalnych,
- szczegółowych projektów budżetów służb specjalnych, przed ich rozpatrzeniem przez Radę Ministrów,
- projektów aktów normatywnych i innych dokumentów rządowych dotyczących działalności służb specjalnych,
- wykonywania przez służby specjalne powierzonych im zadań, zgodnie z kierunkami i planami działania tych służb,
- rocznych sprawozdań przedstawianych przez szefów z działalności podległych im służb specjalnych,
- koordynowania działalności służb specjalnych, a także działalności służb specjalnych z Policją, Strażą Graniczną, Żandarmerią Wojskową, Biurem Ochrony Rządu, Służbą Celną, urzędami skarbowymi, izbami skarbowymi,

[35] Dz.U. z 1999 r. poz. 526, ze zm.
[36] Dz.U. z 1997 r. poz. 412, ze zm.

organami kontroli skarbowej, organami informacji finansowej i służbami rozpoznania Sił Zbrojnych Rzeczpospolitej Polskiej oraz ich współdziałania w dziedzinie ochrony bezpieczeństwa państwa,
- współdziałania podmiotów organów administracji rządowej, organów samorządu terytorialnego, instytucji państwowych oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej, ze służbami specjalnymi,
- współdziałania służb specjalnych z właściwymi organami i służbami innych państw,
- organizacji wymiany informacji istotnych dla bezpieczeństwa i międzynarodowej pozycji Rzeczpospolitej Polskiej między organami administracji rządowej.

Szczegółowy tryb i zasady funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakres czynności sekretarza tego Kolegium reguluje *Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r. w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakresu czynności sekretarza tego Kolegium*[37]. Obsługą organizacyjną, prawną oraz kancelaryjno-biurową Kolegium w Kancelarii Prezesa Rady Ministrów zajmuje się Biuro Kolegium ds. Służb Specjalnych.

Prezydent Rzeczpospolitej Polskiej

Uprawnienia Prezydenta Rzeczpospolitej Polskiej w zakresie kontroli i nadzoru nad służbami specjalnymi są w aktualnym stanie prawnym znacznie ograniczone i sprowadzają się w większości przypadków do jego udziału, jako organu opiniującego, w zróżnicowanych procedurach dotyczących służb specjalnych. Jednocześnie, sięgając do konstytucyjnych prerogatyw prezydenta dotyczących zadań związanych z jego funkcjonowaniem jako najwyższego reprezentanta Rzeczpospolitej Polskiej oraz gwaranta ciągłości funkcjonowania wszystkich organów władzy państwowej, a także związanych z jego zadaniami dotyczącymi stania na straży suwerenności i bezpieczeństwa państwa, można wskazać, że zadania prezydenta w omawianym zakresie korespondują z koniecznością posiadania przez niego określonego zasobu wiedzy wrażliwej, którą dysponują służby specjalne. To z kolei przekłada się na prawo do informacji i wysłuchania, które można traktować jako przejaw funkcji kontrolnej oraz zadaniowania i – po części – profilowania kierunków pracy służb specjalnych. Każda z ustaw kompetencyjnych służb specjalnych przewiduje prezydenta jako podstawowego adresata posiadanych informacji. Zgodnie z art. 18 ust. 1 i 2 ustawy o ABW oraz AW szefowie Agencji, każdy w zakresie swojej właściwości, przekazują niezwłocznie prezydentowi informacje mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczpospolitej Polskiej. W odróżnieniu od Prezesa Rady Ministrów, przekazanie tych informacji następuje w każdym przypadku, w którym prezydent tak zdecyduje. Analogiczny przepis, art. 19 ust. 1 i 2, jest zawarty w ustawie o SKW oraz SWW. Zgodnie z art. 2 ust. 1 pkt 7 Prezydent RP, obok innych organów, jest wskazany jako adresat informacji odnoszących się do prowadzonej przez CBA działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości tego Biura. Ustawowe uprawnienia prezydenta w odniesieniu do poszczególnych służb specjalnych są zróżnicowane i kształtują się w sposób następujący:

[37] Dz.U. z 2002 r. poz. 929.

1) wobec Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu Prezydent RP:
   – opiniuje wydawane przez Prezesa Rady Ministrów wytyczne w celu koordynacji działań w dziadzienie ochrony bezpieczeństwa i obronności państwa (art. 13 ust .2) oraz jest informowany o ich wydaniu (art. 13 ust. 5),
   – opiniuje powołanie i odwołanie szefów ABW i AW (art. 14 ust. 1),
   – jest powiadamiany przez szefów ABW i AW o wystąpieniu do Prezesa Rady Ministrów z wnioskiem o udzielenie zgody na prowadzenie czynności w trybie art. 22a ustawy o ABW oraz AW, tj. w sytuacji, gdy sprawa, w której są prowadzone czynności, należy do kompetencji innych służb lub instytucji (art. 22a ust. 6) oraz powiadamiany i wyrażeniu tej zgody (art. 22a ust. 8),
   – mianuje na pierwszy stopień w korpusie oficerów oraz na stopień generała brygady (art. 67 ust. 4) oraz decyduje o utracie lub pozbawieniu stopnia podporucznika oraz stopnia generała brygady (art. 75);
2) w przypadku Centralnego Biura Antykorupcyjnego opiniuje powołanie i odwołanie Szefa CBA (art. 6 ust. 1);
3) wobec Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego:
   – jest informowany przez ministra obrony narodowej o wytycznych określających kierunki działania SKW oraz SWW oraz zatwierdzonych planach działania na rok następny i sprawozdaniach z działalności i wykonania budżetu SKW oraz SWW za poprzedni rok kalendarzowy (art. 7 ust. 6),
   – opiniuje powołanie i odwołanie szefów SKW oraz SWW (art. 13 ust. 1),
   – jest powiadamiany przez szefów ABW i AW o wystąpieniu do Prezesa Rady Ministrów z wnioskiem o udzielenie zgody na prowadzenie czynności w trybie art. 27 ustawy o SKW oraz SWW, tj. w sytuacji, gdy sprawa, w której prowadzone są czynności, należy do kompetencji innych służb lub instytucji (art. 27 ust. 6) oraz powiadamiany i wyrażeniu tej zgody (art. 22a ust. 8),
   – mianuje na pierwszy stopień w korpusie oficerów oraz na stopień generała brygady oraz decyduje o utracie lub pozbawieniu stopnia podporucznika oraz stopnia generała brygady.

Warto też odnotować, że członkiem rządowego Kolegium do Spraw Służb Specjalnych jest podległy Prezydentowi RP szef Biura Bezpieczeństwa Narodowego, co niewątpliwie wzmacnia pozycję prezydenta w zakresie wiedzy o funkcjonowaniu służb specjalnych, przekładając się na rzeczywisty wpływ nadzorczo-kontrolny na te służby.

5. Kontrola i nadzór nad służbami specjalnymi sprawowane przez organy władzy sądowniczej i prokuraturę

Rola władzy sądowniczej w procesie nadzoru i kontroli służb specjalnych jest oparta na elemencie legalistycznym, nakierowanym na legalność działania służb, w tym sposobu wykonywania czynności, zwłaszcza operacyjno-rozpoznawczych, oraz wyciąganiu konsekwencji w przypadku nadużycia zasad lub sposobu ich wykonywania (identyfikacji bezprawności działania). Zgodnie z art. 173 Konstytucji RP elementami władzy sądowniczej w Polsce są trybunały – Konstytucyjny i Stanu oraz sądy – Najwyższy, powszechne, administracyjne oraz wojskowe. Z punktu widzenia tematu niniejszej pracy należy zwrócić szczególna uwagę na rolę trybunałów, zwłaszcza Trybunału Konstytucyjnego, oraz sądów w procesie nadzoru i kontroli nad służbami specjalnymi.

Trybunał Konstytucyjny

Podstawowym zadaniem Trybunału Konstytucyjnego jest orzekanie o zgodności ustaw i umów międzynarodowych z Konstytucją RP (art. 188 pkt 1). To zadanie w bezpośredni sposób jest elementem nadzoru władzy sądowniczej nad służbami specjalnymi. Rolą sądu konstytucyjnego jest dokonanie oceny zgodności m.in. przyjętej przez parlament ustawy kompetencyjnej służby specjalnej, w tym ocena określonych w niej zadań oraz przydzielonych służbom narzędzi i środków, z punktu widzenia konstytucyjnych wolności praw i obowiązków człowieka i obywatela. Podstawowym wzorcem konstytucyjnym stosowanym przez TK w tych sprawach jest art. 31 ust. 3 Konstytucji RP, na którego gruncie zostaje wyznaczana przez Trybunał dopuszczalna granica ingerencji ze strony państwa w gwarantowaną jednostce ochronę m.in. na podstawie zasady proporcjonalności.

> Racjonalny prawodawca wybiera zatem cele służące najpełniej realizacji wyrażonego w Konstytucji systemu wartości, a następnie dobiera środki najbardziej adekwatne do realizacji tych celów. Za środki najbardziej adekwatne należy uznać te, które są po pierwsze skuteczne w realizacji pożądanego stanu faktycznego, a po drugie zgodne z przyjętym systemem wartości[38].

Proporcjonalność jest sumą składową trzech zasad: przydatności, konieczności oraz proporcjonalności sensu stricto, tzn. zakazu nadmiernej ingerencji[39]. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej, bądź wolności i praw innych osób. Podstawową więc przyczyną ograniczania praw jednostki mogą być względy wynikające z potrzeb bezpieczeństwa i obronności kraju.

> Jak wynika z art. 5 Konstytucji, jednym z podstawowych zadań RP jest strzeżenie niepodległości i nienaruszalności terytorium. W świetle tego przepisu, któremu – zważywszy na systematykę Konstytucji – została nadana najwyższa ranga, nie może budzić wątpliwości, że zapewnienie bezpieczeństwa państwa jest celem usprawiedliwiającym ograniczenia wszelkich praw i wolności obywatelskich. (…) Ochrona bezpieczeństwa państwa jest szczególną wartością, w zderzeniu z którą prawa jednostki, nawet prawa podstawowe, mogą być – w niezbędnym zakresie – ograniczane (wyrok z 3 lipca 2001 r., K 3.01)[40].

Warto wskazać, że Trybunał Konstytucyjny już kilkukrotnie dokonywał oceny ustaw kompetencyjnych służb specjalnych:

1) ustawy o ABW oraz AW, w sześciu sprawach, o sygnaturach:
   - K 23/11 (art. 5, 27, 28 i inne) – dotyczącej regulacji określających zasady stosowania kontroli operacyjnej,
   - K 45/02 (art. 14, 23, 41, 230 i inne) – dotyczącej przepisów przejściowych i dostosowujących odnośnie do likwidacji UOP,

[38] Por. K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999, s. 166–167.

[39] Por. wyrok TK z 11 IV 2000 r., K 15/98.

[40] *Proces prawotwórczy w świetle orzecznictwa Trybunału Konstytucyjnego*, wyd. 14, Warszawa 2015, s. 166–167.

- K 10/11 (art. 25 ust. 3) – dotyczącej regulacji określających zasady stosowania środków przymusu bezpośredniego,
- K 18/14 (art. 52) – dotyczącej regulacji określających zasady bezpieczeństwa i higieny służby w służbach mundurowych,
- P 30/05 (art. 93) – dotyczącej zasad stosowania przepisów prawa pracy związanych z macierzyństwem,
- SK 48/13 (art. 128) – dotyczącej pominięcia prawa do ekwiwalentu pieniężnego za urlop wypoczynkowy niewykorzystany w roku zwolnienia ze służby;

2) ustawy o CBA, w trzech sprawach, o sygnaturach:
   - K 54/07 (art. 1, 2, 5 i inne) – w zakresie, w jakim pod pojęciem korupcji w sektorze prywatnym należy uznawać zachowanie jakiejkolwiek osoby niepełniącej funkcji publicznej, nie zawężając tego określenia za pomocą przesłanek szkodliwych społecznie odwzajemnień,
   - K 10/11 (art. 15) – dotyczącej regulacji określających zasady stosowania środków przymusu bezpośredniego,
   - K 23/11 (art. 17, 18) – dotyczącej regulacji określających zasady stosowania kontroli operacyjnej;
3) ustawy o SKW oraz SWW, w dwóch sprawach o sygnaturach:
   - K 52/07 (art. 3, 7, 27 i 41) – związanej z likwidacją WSI,
   - K 23/11 (art. 5, 31, 32) – dotyczącej regulacji określających zasady stosowania kontroli operacyjnej.

Sądy powszechne

Przechodząc na grunt sądownictwa powszechnego, należy wskazać, że:

> (…) w każdym kraju demokratycznym niezawisła władza sądownicza jest powołana do oceny naruszenia, czy zagrożenia naruszenia uprawnień podmiotu, czy realizacji przez ten podmiot (obywatela, przedsiębiorcę, cudzoziemca) nałożonych na niego przez prawo obowiązków. Dotyczy to także sfery działalności służb specjalnych, zarówno w zakresie zbierania informacji, metod i środków przedsiębranych do realizacji zadań, jak i oceny ewentualnego naruszenia przez te działania praw podstawowych przysługujących podmiotom prawa[41].

W tym zakresie działania władzy sądowniczej koncentrują się przede wszystkim na ocenie materiału dowodowego zebranego podczas prowadzonego przez prokuraturę postępowania przygotowawczego, zebranego w akcie oskarżenia przeciwko funkcjonariuszom służb specjalnych. Sąd powszechny jest w wielu przypadkach podmiotem, od którego decyzji uzależniona jest w ogóle możliwość prowadzenia przez służby specjalne czynności, w tym szczególnie czynności operacyjno-rozpoznawczych. W tym zakresie należy zwrócić uwagę, że:

1) kontrolę operacyjną zarządza (oraz przedłuża) Sąd Okręgowy w Warszawie na pisemny wniosek szefa służby, złożony po uzyskaniu pisemnej zgody prokuratora generalnego, a w przypadku wniosku o jej przedłużenie – zapoznaje się z materiała-

[41] Por. P. Pogonowski, *Nadzór nad służbami specjalnymi*…

mi uzasadniającymi wniosek, zwłaszcza zgromadzonymi podczas stosowania kontroli operacyjnej zarządzonej w tej sprawie (art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA; art. 31 ust. 1 ustawy o SKW oraz SWW);

2) sąd, na wniosek prokuratora generalnego, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu; zarządza również niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne (art. 27 ust. 15j ustawy o ABW oraz AW; art. 17 ust. 15h ustawy o CBA; art. 31 ust. 14h ustawy o SKW oraz SWW);
3) Sąd Okręgowy w Warszawie sprawuje kontrolę nad uzyskiwaniem przez służbę danych telekomunikacyjnych, pocztowych lub internetowych, w ramach której otrzymuje od szefów służb półroczne sprawozdania oraz może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych (art. 28a ustawy o ABW oraz AW, art. 18a ust. 1 ustawy o CBA, art. 32a ust. 1 ustawy o SKW oraz SWW);
4) Sąd Okręgowy w Warszawie, na pisemny wniosek szefa ABW złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych, mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym (art. 32c ustawy o ABW oraz AW);
5) Sąd Okręgowy w Warszawie, na pisemny wniosek szefa ABW lub CBA, wydaje w drodze postanowienia zgodę na korzystanie przez ABW i CBA z przetwarzanych przez banki informacji stanowiących tajemnicę bankową oraz informacji dotyczących umów o rachunek papierów wartościowych, umów o rachunek pieniężny, umów ubezpieczenia lub innych umów dotyczących obrotu instrumentami finansowymi, świadczenia usług płatniczych lub zawieranych z uczestnikami funduszy inwestycyjnych, a szczególnie z przetwarzanych przez uprawnione podmioty danych osób, które zawarły takie umowy (art. 34a ust. 4 ustawy o ABW oraz AW; art. 23 ust. 4 ustawy o CBA);
6) Pierwszy Prezes Sądu Najwyższego jest ostatnią instancją, która wydaje ostateczną decyzję w zakresie stwierdzenia zasadności uwzględnienia żądania prokuratora lub sądu o zwolnienie funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych od obowiązku zachowania w tajemnicy informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", zgłoszonego w związku z postępowaniem karnym o przestępstwo określone w art. 105 § 1 Kodeksu karnego lub o zbrodnię godzącą w życie ludzkie albo o występek przeciwko życiu lub zdrowiu, gdy jego następstwem była śmierć człowieka (art. 39 ust. 6 ustawy o ABW oraz AW; art. 28 ust. 15 ustawy o CBA; art. 43 ust. 6 ustawy o SKW oraz SWW).

Prokuratura

Ewentualne działania funkcjonariuszy służb specjalnych powinny być i są oceniane z perspektywy ich legalności przez prokuraturę dysponującą uprawnieniami wynikającymi z *Ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego*[42]. W tym zakresie prokuraturze, na czele z prokuratorem generalnym, przysługuje pełne spektrum narzędzi kontrolnych i nadzorczych wobec czynności dochodzeniowo-śledczych oraz operacyjno-rozpoznawczych, podejmowanych przez służby specjalne.

Zgodnie z art. 311 § 1 i 2 kpk śledztwo prowadzi prokurator. Prokurator może powierzyć Policji przeprowadzenie śledztwa w całości lub w określonym zakresie albo dokonanie poszczególnych czynności śledztwa; w wypadkach określonych w art. 309 pkt 2 i 3 można powierzyć Policji jedynie dokonanie poszczególnych czynności śledztwa. Na podstawie art. 312 kpk te uprawnienia przysługują także ABW, CBA i innym organom przewidzianym w przepisach szczególnych. Zgodnie z art. 21 ust. 2 ustawy o ABW oraz AW Agencja Bezpieczeństwa Wewnętrznego wykonuje również czynności na polecenie sądu lub prokuratora w zakresie określonym w kpk oraz kodeksie karnym wykonawczym[43]. Zgodnie z art. 22 ust. 3 tej ustawy, jeżeli informacje i materiały uzyskane przez ABW albo AW wskazują na uzasadnione podejrzenie popełnienia przestępstwa lub przestępstwa skarbowego albo potwierdzają jego popełnienie, szef właściwej Agencji przedstawia je właściwemu prokuratorowi w celu podjęcia decyzji co do ich dalszego procesowego wykorzystania[44]. Zgodnie z art. 23 ust. 7 ustawy o ABW oraz AW na sposób przeprowadzenia zarówno czynności dochodzeniowo-śledczych, jak i administracyjno-porządkowych będących w kompetencji ABW, przysługuje zażalenie do prokuratora właściwego ze względu na miejsce przeprowadzenia czynności[45]. Prokuratura prowadząc lub nadzorują postępowanie przygotowawcze w sprawach karnych i zlecając przeprowadzenie śledztwa ABW lub CBA w całości bądź powierzając im przeprowadzenie określonych czynności dochodzeniowo-śledczych, czuwa jednocześnie, w ramach nadzoru prokuratorskiego, nad sposobem jego prowadzenia, w tym nad oceną samego legalizmu działania.

Prokurator generalny jest jednym z najważniejszych podmiotów uczestniczących w procedurze uruchamiania ustawowo określonych czynności operacyjno-rozpoznawczych, w tym zakresie, i:

1) wyraża opinię w sprawie decyzji szefa ABW dotyczącej odstąpienia od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa szpiegostwa albo uprawdopodobnienia działalności zmierzającej do popełnienia przestępstwa o charakterze terrorystycznym oraz osobie, która według uzyskanych przez ABW informacji lub materiałów, może być jego sprawcą – gdy jest to uzasadnione względami bezpieczeństwa państwa (art. 22b ust. 3 ustawy o ABW oraz AW, art. 27a ust. 3 ustawy o SKW oraz SWW);
2) podejmuje decyzje w zakresie stosowania kontroli operacyjnej:

[42] Dz.U. z 2016 r. poz. 1749, ze zm.

[43] Podobnie art. 13 ust. 2 ustawy o CBA wskazuje, że CBA wykonuje również czynności na polecenie sądu lub prokuratora w zakresie określonym w *Ustawie z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (Dz.U. poz. 555, ze zm.) oraz *Ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy* (t.j.: Dz.U. z 2017 r. poz. 665).

[44] Podobnie art. 27 ust. 3 ustawy o SKW oraz SWW.

[45] Podobnie art. 14 ust. 7 ustawy o CBA i art. 29 ust. 2 ustawy o SKW oraz SWW.

- wyraża w drodze postanowienia zgodę na zarządzenie kontroli operacyjnej (art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA, art. 31 ust. 1 ustawy o SKW oraz SWW),
- wyraża pisemną zgodę na zarządzenie kontroli operacyjnej w przypadkach niecierpiących zwłoki (art. 27 ust. 3 ustawy o ABW oraz AW, art. 17 ust. 3 ustawy o CBA, art. 31 ust. 3 ustawy o SKW oraz SWW),
- wyraża pisemną zgodę na przedłużenie kontroli operacyjnej (art. 27 ust. 8 ustawy o ABW oraz AW, art. 17 ust. 8 ustawy o CBA, art. 31 ust. 6 ustawy o SKW oraz SWW),
- jest informowany przez szefa ABW o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie – również o przebiegu tej kontroli, przedstawiając zebrane w jej toku materiały (art. 27 ust. 14 ustawy o ABW oraz AW, art. 17 ust. 14 ustawy o CBA, art. 31 ust. 13 ustawy o SKW oraz SWW),
- w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego szef ABW przekazuje mu wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej (art. 27 ust. 15 ustawy o ABW oraz AW, art. 17 ust. 15 ustawy o CBA, art. 31 ust. 14 ustawy o SKW oraz SWW),
- wyraża pisemną zgodę na zachowanie materiałów z kontroli operacyjnej, które są istotne dla bezpieczeństwa państwa (art. 27 ust. 15f ustawy o ABW oraz AW),
- jest informowany o zniszczeniu materiałów z kontroli operacyjnej, które nie są istotne dla bezpieczeństwa państwa lub nie są informacjami potwierdzającymi zaistnienie przestępstwa (art. 27 ust. 15l ustawy o ABW oraz AW, art. 17 ust. 15j ustawy o CBA, art. 31 ust. 15a ustawy o SKW oraz SWW);

3) otrzymuje informację o danych niestanowiących treści odpowiednio – przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, które mają znaczenie dla postępowania karnego, a także podejmuje decyzję o zakresie i sposobie wykorzystania tych danych (art. 28 ustawy o ABW oraz AW, art. 18 ust. 6 ustawy o CBA, art. 32 ust. 8 ustawy o SKW oraz SWW);
4) wyraża zgodę na przeprowadzenie czynności operacyjno-rozpoznawczych zmierzających do sprawdzenia uzyskanych wcześniej wiarygodnych informacji o przestępstwie oraz wykrycia sprawców i zdobycia dowodów; te czynności mogą polegać na dokonaniu w sposób niejawny nabycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej (prokurator generalny jest na bieżąco informowany o ich przebiegu i wynikach). W przypadku potwierdzenia informacji o przestępstwie szef ABW przekazuje prokuratorowi generalnemu wszystkie materiały zgromadzone w wyniku wykonywania czynności (art. 29 ust. 4 ustawy o ABW oraz AW, art. 19 ust. 2 ustawy o CBA, art. 33 ust. 4 ustawy o SKW oraz SWW);
5) jest zawiadamiany o zarządzeniu, przebiegu i wynikach czynności operacyjno-rozpoznawczych niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa. W przypadku potwierdzenia informacji o przestępstwie, szef ABW przekazuje prokuratorowi generalnemu wszystkie materiały zgromadzone w wyniku wykonywania czynności (art. 31 ust. 4 ustawy o ABW oraz AW, art. 34 ust. 2 ustawy o SKW oraz SWW);

6) podejmuje decyzje w zakresie stosowania blokady dostępności danych:
   – wyraża pisemną zgodę na zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym (art. 32c ustawy o ABW oraz AW),
   – wyraża zgodę na blokadę dostępności, w przypadkach niecierpiących zwłoki (art. 32c ust. 4 ustawy o ABW oraz AW),
   – wyraża pisemną zgodę na przedłużenie blokady dostępności (art. 32c ust. 4 ustawy o ABW oraz AW).

6. Kontrola i nadzór nad służbami specjalnymi sprawowane przez społeczeństwo obywatelskie

> Koncepcja nowoczesnego państwa demokratycznego zawiera określony model relacji między państwem a społeczeństwem. Model ten, mówiąc najkrócej, opiera się na założeniu istnienia nieprzekraczalnych granic dla ingerencji państwa w strefę praw i podstawowych swobód obywatelskich, a jednocześnie ustanawia właściwą proporcję pomiędzy interesem grupowym a publicznym[46].

W literaturze pojawia się wiele definicji pojęcia społeczeństwo obywatelskie. Najczęściej podkreśla się dwa jego aspekty: idee przyświecające pewnej grupie ludzi oraz formy organizacyjne, w które te grupy ludzi się samoorganizują w celu realizacji tych idei. W kontekście społeczeństwa obywatelskiego często mówi się, że jest ono tzw. trzecim sektorem, w którym podmioty są prywatne, a cele publiczne, w odróżnieniu od sektorów: prywatnego (gdzie podmiot i cel jest prywatny) oraz publicznego (gdzie podmiot i cel jest publiczny). Zdaniem Karla Poppera społeczeństwo plemienne, kolektywne czy rządzone autorytarnie, to społeczeństwo zamknięte, natomiast społeczeństwo, w którym jednostka ma prawo do osobistych decyzji, a zatem posiada gwarancje dla swojego indywidualizmu – to społeczeństwo otwarte[47]. Działalność społeczeństwa obywatelskiego realizuje się zarówno przez instytucje formalne (np. partie polityczne, związki zawodowe, stowarzyszenia, fundacje), jak i działania niesformalizowane (np. rodziny, mniejszości narodowe i etniczne, mieszkańcy danej wspólnoty). Działania społeczeństwa obywatelskiego przybierają różne formy i cele. Jednym z nich jest stosowanie mechanizmów kontroli organów władzy publicznej, głównie w kontekście ochrony praw człowieka i podstawowych wolności. Podstawą prawną takich działań jest *Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie*[48], w której określono podmiotowe i przedmiotowe ramy działania tego typu podmiotów oraz zawarto m.in. definicje legalne następujących pojęć: działalność pożytku publicznego oraz organizacja pozarządowa. Drugą podstawą jest *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej*[49], która każdej osobie, w tym organizacjom pozarządowym, przyznaje uprawnienie

[46] Zob. A. Krasnowolski, *Społeczeństwo obywatelskie i jego funkcje*, Warszawa 2014.
[47] K. Popper, *Społeczeństwo otwarte i jego wrogowie*, t. 1 i 2, Warszawa 2007.
[48] Dz.U. z 2016 r., poz. 1817, ze zm.
[49] Dz.U. z 2016 r., poz. 1764, ze zm.

do uzyskania informacji publicznej, a także do dostępu do dokumentów urzędowych i prawo wstępu na posiedzenia kolegialne organów władzy publicznej. Ta ustawa, przez wymienione uprawnienia, przyznaje społeczeństwu obywatelskiemu istotne narzędzia nadzorczo-kontrolne nad służbami specjalnymi. Kluczem jednak do jej właściwego rozumienia i stosowania jest wyważenie proporcji między potrzebą dostępu do informacji, podyktowaną m.in. wolą działania w celu ochrony praw i wolności obywatelskich, a prawem odmowy takiego dostępu, wynikającego z ochrony bezpieczeństwa państwa. Problem koncertuje się więc na właściwym wyważeniu proporcji między przejrzystością działalności służb specjalnych, a ograniczeniem dostępności informacji o niej oraz na stosowanych przez nie środkach, formach i metodach pracy. Z uwagi na to, że ustawa o dostępie jest oparta na elemencie decyzyjności przybierającej formę decyzji administracyjnej, do której zastosowanie znajdują reguły postępowania administracyjnego, organem ostatecznie upoważnionym do oceny tej proporcjonalności (ważenia dóbr) jest sąd administracyjny, w ramach kontroli pod względem zgodności z prawem zaskarżonej decyzji o odmowie udostępnienia wnioskowanych informacji. Warto tu przytoczyć elementy uzasadnienia Wojewódzkiego Sądu Administracyjnego w Warszawie w sprawie o sygn. II SA/Wa 291/17 z 29 maja 2017 r., w którym sąd przyznaje rację szefowi ABW w zakresie odmowy przekazania wnioskującej fundacji informacji o liczbie porozumień zawartych między ABW a usługodawcami świadczącymi usługi drogą publiczną. Jak wskazał sąd:

> (…) przedmiot sprawy dotyczy zagadnień związanych z bezpieczeństwem Państwa, a przede wszystkim bezpieczeństwem publicznym. Zatem Szef ABW nie pozostaje w błędzie twierdząc, że ujawnienie żądanej informacji może powodować zagrożenie dla bezpieczeństwa Państwa (…) Udostępnienie żądanej informacji może więc w sposób pośredni (w zestawieniu z innymi danymi powszechnie dostępnymi) ujawnić skalę działań organu w ramach uprawnień nadanych powyższym przepisem, również gdy zostanie ujawniona jako bieżące dane statystyczne. (…) W ocenie Wojewódzkiego Sądu Administracyjnego w Warszawie argumentacja Szefa ABW jest uzasadniona, gdy zważy się stan (niewypowiedzialnej, ale rzeczywistej) wojny z terroryzmem z całym światem demokratycznym, falę zamachów terrorystycznych nękającą państwa zachodnie Unii Europejskiej (nawet pomimo ustanowienia w niektórych z nich od półtora roku stanu wyjątkowego) i otwartą wojnę terrorystyczną tzw. „państwa (…)" z całą cywilizacją demokratyczną. W świetle tych wydarzeń i [w związku z] ich agresywnym charakterem, oczywistym jest zwiększenie działań dyskrecjonalnych państw demokratycznych w zakresie bezpieczeństwa wewnętrznego ich obywateli. (…) Żądanie dostępu do informacji publicznej w trybie ustawy o dostępie do informacji publicznej nie może służyć weryfikacji klauzul tajności. Takie rozumienie instytucji obywatelskiego dostępu do informacji publicznych, czyniłoby ustawę o ochronie informacji niejawnych zbyteczną i nadto naruszałoby zasadę wyrażoną w art. 61 ust. 3 Konstytucji, który zezwala na ustawowe ograniczenie prawa dostępu do informacji. Ograniczenie to ustawodawca urzeczywistnił, wprowadzając do polskiego porządku prawnego, ustawę o ochronie informacji niejawnych oraz odpowiednią normę kolizyjną w ustawie o dostępie do informacji publicznej (art. 5 ust. 1).

Podobne stanowisko wyraził Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 17 sierpnia 2017 r. w sprawie o sygn. II SA/Wa 80/17, wskazując w ustnych motywach wyroku, że sąd, podzielając stanowisko szefa ABW, wskazał, że posiada on uprawnienie do oznaczania określonych informacji klauzulą tajności, jeżeli organ

uzna je za informacje niejawne i stwierdzi, że należy je chronić. Odnosząc się do skargi w zakresie udostępnienia informacji o stosowaniu uprawnień, o których mowa w art. 9–11 ustawy o działaniach antyterrorystycznych, Sąd opowiedział się za linią orzeczniczą sądów administracyjnych, z której wynika, że nie wszystkie dane statystyczne dotyczące funkcjonowania służb specjalnych mogą być upublicznione. Biorąc pod uwagę aktualną sytuację geopolityczną, a zwłaszcza zagrożenie terrorystyczne, Sąd podzielił stanowisko organu, że ujawnienie wnioskowanych informacji, może osłabić efektywność polskich służb specjalnych, a to w konsekwencji może utrudnić organowi wykonywanie jego ustawowych działań, a więc może narazić polskie państwo na uszczerbek.

7. Kontrola i nadzór nad służbami specjalnymi w wybranych państwach

Republika Francuska

Do grona służb wywiadowczych we Francji, zgodnie z art. R 811-1 ustawy kodeks bezpieczeństwa wewnętrznego, zaliczają się następujące podmioty:

1) Generalna Dyrekcja Bezpieczeństwa Zewnętrznego (Direction Générale de la Sécurité Extérieure – DGSE),
2) Dyrekcja Wywiadu i Bezpieczeństwa Sił Zbrojnych (Direction du Renseignement et de la Securité de la Défense – DRSD),
3) Dyrekcja Wywiadu Wojskowego (Direction du Renseignement Militaire – DRM),
4) Generalna Dyrekcja Bezpieczeństwa Wewnętrznego (Direction Générale de la Sécurité Intérieure – DGSI),
5) Narodowa Dyrekcja Wywiadu i Dochodzeń Celnych (Direction Nationale du Renseignement et des Enquêtes Douanières – DNRED),
6) Służba Zwalczania Nielegalnego Obrotu Środkami Finansowymi (Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins – TRACFIN).

Kontrola nad tymi służbami jest sprawowana przede wszystkim przez organy władzy wykonawczej – ministrów obrony, spraw wewnętrznych i finansów. Pomocniczą rolę odgrywa powołana w 2007 r. Delegacja Parlamentarna ds. Wywiadu. Istotną funkcję pełnią także niezależne i wyspecjalizowane organy administracyjne – powołana na mocy ustawy o wywiadzie z 2015 r. (fr. *la loi sur le renseignement*) Narodowa Komisja Kontroli Technik Pozyskiwania Informacji (CNCTR), Międzyresortowa Grupa Kontroli czy Narodowa Komisja ds. Informatyki i Wolności (CNIL).

Francuski system kontroli nad służbami wywiadowczymi ma charakter rozproszony. Jak wskazano powyżej, każda z sześciu wymienionych służb podlega określonemu ministrowi:

1) DGSI – Ministrowi Spraw Wewnętrznych,
2) TRACFIN i DNRED – Ministrowi Finansów,
3) DGSE, DRM i DRSD – Ministrowi Obrony.

Funkcję koordynacyjną w stosunku do wszystkich służb pełni Narodowy Koordynator ds. Wywiadu i Zwalczania Terroryzmu. Nazwa tego organu uległa zmianie na podstawie dekretu nr 2017-1095 z 14 lipca 2017 r. – poprzednio nosił on nazwę Narodowego Koordynatora ds. Wywiadu. Zgodnie z art. 1 dekretu, który zmienił przepisy art. R*1122-8 do R*1122-8-2 ustawy kodeks obrony, Koordynator jest powoływany na podstawie dekretu Rady Ministrów, jego zaś głównym zadaniem jest pełnienie funk-

cji doradczej wobec prezydenta w zakresie wywiadu i zwalczania terroryzmu. Ten organ koordynuje działania służb wywiadowczych wymienionych w art. R 811-1 ustawy kodeks bezpieczeństwa wewnętrznego oraz, jeżeli zachodzi taka potrzeba i tylko w celach związanych z polityką wywiadowczą i zwalczaniem terroryzmu – innych służb wymienionych w art. R 811-2 tej ustawy (m.in. niektóre jednostki organizacyjne Policji).

Dekret nakłada na koordynatora obowiązek zapewnienia efektywnej współpracy między służbami wywiadowczymi przez wspieranie skutecznego przepływu informacji między tymi instytucjami, zwłaszcza w przypadku zagrożenia terrorystycznego. Biorąc pod uwagę opisany powyżej trójpodział kontroli nad służbami wywiadowczymi sprawowany przez trzech ministrów (spraw wewnętrznych, obrony i finansów), koordynator nadzoruje proces tworzenia oraz dąży do zapewnienia skuteczności wewnętrznych mechanizmów koordynacji i wymiany informacji dotyczących zagadnień związanych ze służbami wywiadowczymi w każdym z wyżej wymienionych ministerstw. Wspiera on ponadto, szczególnie w zakresie zwalczania terroryzmu, wykorzystywanie technik pozyskiwania informacji wprowadzonych na mocy ustawy o wywiadzie, opisanych w części VIII ustawy kodeks bezpieczeństwa wewnętrznego, oraz wspólne wykorzystywanie instrumentów technicznych między służbami wywiadowczymi.

Szefowie służb wywiadowczych są zobowiązani do informowania koordynatora o sprawach, które powinny zostać przedstawione prezydentowi i premierowi. Koordynator jest też odpowiedzialny za dokonywanie ogólnych analiz zagrożeń bezpieczeństwa Francji i przedstawianie prezydentowi, na podstawie tych analiz, ogólnych założeń działań wywiadowczych oraz działań dotyczących zwalczania terroryzmu, a także określenie, które z działań służb mają charakter priorytetowy. Wraz z właściwymi ministrami koordynuje działania podejmowane przez Francję w zakresie współpracy w wymiarze europejskim i międzynarodowym.

Istotnym elementem systemu nadzoru nad służbami wywiadowczymi jest utworzony na mocy dekretu nr 2014-833 Inspektorat Służb Wywiadowczych (L'Inspection des services de renseignement). Ten organ podlega bezpośrednio premierowi (art. 1). Realizuje on zadania polegające na dokonywaniu czynności kontrolnych, prowadzeniu audytu, opracowywaniu analiz, studiów oraz oceny poszczególnych aspektów działań służb wywiadowczych oraz Akademii Wywiadu. Te działania są prowadzone na polecenie premiera, ministrów właściwych do spraw obrony, bezpieczeństwa wewnętrznego, gospodarki, budżetu – działającego z inicjatywy własnej lub na wniosek – lub koordynatora (art. 2). Zgodnie z art. 3 dekretu członkowie Inspektoratu są wyznaczani przez premiera, po uzyskaniu opinii koordynatora, na wniosek:

1) ministrów właściwych do spraw obrony, bezpieczeństwa wewnętrznego, gospodarki, budżetu, którzy mogą wskazać osobę mającą dostęp do niejawnych informacji wojskowych na poziomie Très Secret-Défense będącą czynnym pracownikiem Generalnego Inspektoratu Sił Zbrojnych, Generalnego Inspektoratu Administracji, Generalnego Inspektoratu Finansów lub Rady Ogólnej ds. Gospodarki, Przemysłu, Energii i Technologii; te wnioski są opracowywane po uzyskaniu opinii szefa tych organów;
2) ministra właściwego do spraw obrony spośród generalnych inspektorów sił zbrojnych mających dostęp do niejawnych informacji wojskowych na poziomie Très Secret-Défense.

Premier określa mandat oraz skład grupy inspektorów w odniesieniu do każdej realizowanej przez nich misji kontrolnej, wyznacza również szefa tej grupy. W ramach

powierzonych im zadań inspektorzy są upoważnieni do dostępu do wszystkich miejsc, przedmiotów, informacji i dokumentów, które mogą okazać się przydatne w realizowanych przez nich zadaniach. Raport z misji kontrolnej jest przekazywany premierowi, ministrom nadzorującym daną służbę wywiadowczą oraz koordynatorowi (art. 4).

Zakres kontroli parlamentarnej nad służbami wywiadowczymi we Francji należy określić jako ograniczony. Jedynym organem władzy ustawodawczej mogącym realizować zadania kontrolne wobec służb wywiadowczych jest Delegacja Parlamentarna ds. Wywiadu powołana na podstawie ustawy nr 2007-443 z 9 października 2007 r.

Brak formalnoprawnych podstaw sprawowania funkcji kontrolnych przez parlament wobec służb wywiadowczych był do 2007 r. elementem wyróżniającym Francję na tle innych państw europejskich. Do chwili utworzenia Delegacji przyjmowano rozwiązania pośrednie – m.in. utworzenie w 2002 r. Komisji ds. Weryfikacji Funduszy Specjalnych (fr. *commission de vérification des fonds spéciaux*) czy przewidziana w art. 5 bis rozporządzenia nr 58-100 z 27 listopada 1958 r. o działalności zgromadzeń parlamentarnych możliwość wysłuchania przez stałą komisję parlamentarną każdej osoby, jeżeli uznaje to za stosowne – z wyłączeniem spraw zawierających informacje niejawne dotyczących sfery obronności, spraw zagranicznych oraz bezpieczeństwa wewnętrznego i zewnętrznego. W art. 6 tego samego rozporządzenia nadano parlamentarnym komisjom śledczym prawo żądania udostępnienia wszelkich dokumentów dotyczących rozpatrywanej przez nie sprawy, z analogicznym wyłączeniem, jak w przypadku art. 5 bis. Z tego względu uzyskanie przez parlament informacji dotyczących obszaru działalności służb specjalnych było praktycznie niemożliwe. Delegacja jest wspólnym organem Zgromadzenia Narodowego i Senatu; w jej skład wchodzi czterech deputowanych i czterech senatorów, a jej członkami z mocy prawa są przewodniczący komisji bezpieczeństwa wewnętrznego i obrony. Pozostali członkowie zaś są wyznaczani przez przewodniczących obu izb. Zadaniem Delegacji jest ogólne monitorowanie działalności służb wywiadowczych oraz środków pozostających w ich dyspozycji. Jej prace mają charakter niejawny. Delegacja może przedstawiać opinie i rekomendacje prezydentowi i premierowi.

Republika Federalna Niemiec

Podobnie jak wszystkie inne organy władzy wykonawczej, służby specjalne w Niemczech podlegają parlamentarnej kontroli działalności rządu za pośrednictwem plenum niemieckiego parlamentu – Bundestagu, szczególnie za pośrednictwem Parlamentarnego Komitetu Obronności, Parlamentarnego Komitetu Spraw Wewnętrznych, Parlamentarnego Komitetu Budżetowego oraz gremiów politycznych i poszczególnych deputowanych Bundestagu. Parlament ma prawo wnioskować o informacje dotyczące służb specjalnych w formie ustnych i pisemnych zapytań lub interpelacji kierowanych do rządu, a także przez powołanie komisji śledczych. Jednak ze względu na potrzebę ochrony form i metod działania służb, a także konieczność zachowania w tajemnicy informacji niejawnych, Rząd Federalny często odwołuje się do kompetencji specjalnych organów parlamentarnych, którymi są: Komisja Kontroli Parlamentarnej oraz Komisja G-10.

Trzy niemieckie służby specjalne: Federalny Urząd do Spraw Ochrony Konstytucji (Bundesverfassungschutzamt – BfV), Federalna Służba Wywiadowcza (Bundesnachrichtendienst – BND) oraz Federalna Wojskowa Służba Kontrwywiadu (Bundesamt für den Militärischen Abschirmdienst – BAMAD) są nadzorowane na poziomie centralnym przez Parlamentarną Komisję Kontrolną Bundestagu (Parlamentarischen

Kontrollgremium des Bundestags – PKGr). Jest to organ składający się z dziewięciu deputowanych Bundestagu i musi być informowany przez Rząd Federalny o działalności służb. Gremium spotyka się przynajmniej raz na kwartał. Członkowie PKGr mogą wnioskować o raporty dotyczące działalności służb i samodzielnie kontaktować się z personelem służb specjalnych, a także muszą być informowani o szczególnych wydarzeniach dotyczących służb. Ponadto PKGr musi informować Bundestag o swoich pracach, jednak przy zachowaniu przepisów dotyczących ochrony informacji niejawnych.

Komisja G-10 jest uprawniona do szczególnego nadzoru nad niejawnymi metodami, które ograniczają prawa obywatelskie w zakresie prywatności korespondencji, poczty i telekomunikacji. PKGr mianuje czterech członków oraz czterech zastępców do tej Komisji. Komisja jest co miesiąc informowana przez służby o przeprowadzaniu przez nie czynności związanych z kontrolą, która stanowi naruszenie przepisów o tajemnicy korespondencji, poczty i telekomunikacji. Ta niezależna Komisja, której członkowie nie muszą być deputowanymi Bundestagu, może przeprowadzić kontrolę w służbach. W ramach kontroli członkowie Komisji mogą uzyskać dostęp do wszelkich dokumentów oraz danych teleinformatycznych. Ponadto ten organ decyduje o tym, czy służby specjalne mogą przeprowadzać czynności związane z kontrolą, która narusza przepisy o tajemnicy korespondencji, poczty i telekomunikacji. Zatem, gdy zachodzi potrzeba założenia podsłuchu telefonicznego przez jedną ze służb, musi zostać złożony stosowny wniosek do Federalnego Ministerstwa Spraw Wewnętrznych, a Komisja G-10 musi wyrazić zgodę na podjecie takich działań. W przypadku zastosowania metod pozostających pod nadzorem Komisji, decyduje ona, czy osoby podsłuchiwane zostaną o tym poinformowane, gdy już działania operacyjne zostaną zakończone.

Kontrola w służbach odbywa się także za pośrednictwem tzw. Komisji Zaufania (Powierniczej) składającej się z członków Komitetu Budżetowego Bundestagu. Komisja musi zatwierdzić niejawne plany finansowe służb. Kontrolę realizacji budżetu oraz zarządzania finansowego w służbach przeprowadza przewodniczący Federalnego Trybunału Obrachunkowego wraz z dwoma innymi urzędnikami. Federalny Komisarz do Spraw Ochrony Danych i Wolności Informacji kontroluje, czy służby przestrzegają przepisów o ochronie danych. Opinia publiczna jest co roku informowana o działaniach podejmowanych przez służby w jawnym raporcie dotyczącym ochrony porządku konstytucyjnego.

Stany Zjednoczone Ameryki

Obowiązki wykonywania nadzoru nad Wspólnotą Wywiadowczą[50] w USA należą zarówno do władzy wykonawczej, jak i ustawodawczej oraz sądowniczej. Niniejszy nadzór oznacza kontrolę nad służbami specjalnymi (CIA, FBI, NSA[51]) w taki sposób, aby ponosiły one odpowiedzialność za swoje działania. Nadzór obejmuje następujące kwestie: wykonywanie wytycznych decydentów politycznych, jakość sporządzanych dokumentów analitycznych, podjęte czynności i ich zgodność z prawem.

Należy podkreślić, że w systemie amerykańskim nadzór władzy wykonawczej nad działalnością Wspólnoty Wywiadowczej ma charakter priorytetowy (względem władzy wykonawczej oraz sądowniczej) w zakresie bezpieczeństwa narodowego oraz działalności wywiadowczej, w tym wyznaczania zakresu prowadzonych przez nie działań.

[50] Ang. Intelligence Community. Pod tym pojęciem należy rozumieć służby specjalne o kompetencjach wywiadowczych i kontrwywiadowczych.

[51] CIA – Central Intelligence Agency, FBI – Federal Investigation Bureau, NSA – National Security Agency.

Uprawnienia prezydenckie odgrywają zasadniczą rolę w nadzorze władzy wykonawczej (tajne operacje[52] prowadzone przez służby specjalne są zatwierdzane przez prezydenta). Prezydent ma ponadto uprawnienie do powoływania komisji mających oceniać sprawy wywiadowcze oraz kontrwywiadowcze[53]. Należy podkreślić, że w ramach sprawowania funkcji nadzorczej przez władzę wykonawczą działa Prezydencka Rada Doradcza do Spraw Wywiadu[54] (PIAB), w której ramach funkcjonuje Rada Nadzoru Działań Wywiadowczych[55] (IOB) mająca kompetencje do prowadzenia postępowań karnych i działań analitycznych dla prezydenta. Członkowie PIAB są mianowani przez prezydenta; są nimi osoby wyróżniające się doświadczeniem w przedmiotowej dziedzinie. W 2008 r. prezydent George W. Bush pozbawił IOB części uprawnień nadzorczych. Przed tą zmianą IOB po zdobyciu wiedzy o domniemanym bezprawnym działaniu wywiadowczym, niezgodnym z dyrektywą prezydencką, była zobligowana powiadomić prezydenta i prokuratora generalnego, obecnie zaś jest zobligowana powiadomić Departament Sprawiedliwości w celu wszczęcia postępowania karnego[56].

Należy zaznaczyć, że przy każdej z amerykańskich agencji wywiadowczych działa Biuro Inspektora Generalnego[57] (OIG) oraz Radca Generalny[58], którzy mają kompetencje nadzorcze. Biuro Inspektora Generalnego składa raporty sekretarzowi Departamentu lub dyrektorowi Agencji. W kompetencjach OIG jest prowadzenie niezależnych postępowań, audytów, inspekcji i specjalnych przeglądów zarówno personelu, jak i realizowanych zadań, w celu wykrycia oraz zapobiegania marnotrawieniu środków, nadużyciom, defraudacjom oraz promowaniu praworządności, gospodarności, wydajności i skuteczności w działaniu.

W ramach amerykańskiej egzekutywy funkcjonuje również Biuro Programów Wywiadowczych[59] (OIP) i Narodowa Rada Bezpieczeństwa[60] (NSC), które zapewnia prowadzenie rutynowych działań nadzorczych, polityki wywiadowczej dla Wspólnoty Wywiadowczej Stanów Zjednoczonych Ameryki. Działania nadzorcze w zakresie służb specjalnych prowadzi również Dyrektor Wywiadu Narodowego[61] (DNI), który ma kompetencje nadzorcze w zakresie wdrażania Narodowego Programu Wywiadowczego[62] dla służb specjalnych. Organem stricte nadzorczym w Biurze DNI jest Wspólna Rada Wspólnoty Wywiadowczej[63] (JICC), która jest kierowana przez DNI, a pozostałymi członkami ww. Rady są sekretarze: Stanu, Skarbu, Obrony, Energii, Bezpieczeństwa Wewnętrznego i Prokurator Generalny[64].

Podstawową prerogatywą w zakresie władzy ustawodawczej są uprawnienia Kongresu Stanów Zjednoczonych Ameryki o charakterze nadzorczym wobec Wspólnoty Wywiadowczej. Te zadania polegają na nadzorowaniu budżetu, jakości sporządzanych

[52] Ang. *covert operations*.

[53] Przykładem mogą być Narodowa Komisja do Spraw Ataków Terrorystycznych czy Komisja Wywiadowcza w sprawie Iraku.

[54] Ang. President's Foreign Intelligence Advisory Board.

[55] Ang. Intelligence Oversight Board.

[56] https://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/html/int018.html [dostęp: 20 IX 2017].

[57] Ang. The Office of the Inspector General.

[58] Ang. General Counsel.

[59] Ang. Office of Intelligence Programs.

[60] Ang. National Security Council.

[61] Ang. Director of National Intelligence.

[62] Ang. *National Intelligence Program*.

[63] Ang. Joint Intelligence Community Council.

[64] https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23110.htm [dostęp: 21 IX 2017].

analiz, badaniu zgodności z prawem podejmowanych działań i błędach popełnianych w pracy wywiadowczej oraz kontrwywiadowczej. Wymienione zadania są realizowane przez dwie podstawowe komisje mające uprawnienia do prowadzenia nadzoru nad Wspólnotą Wywiadowczą. Pierwszą komisją jest House Permanent Select Committee on Intelligence (HPSCI), drugą zaś – Senate Select Committee on Intelligence: Oversight Subcommittee (SSCI).

W HPSCI zasiada 22 członków, w drugiej Komisji SSCI natomiast – 15 senatorów. Partia, która ma przewagę, posiada ośmiu członków w Komisji. Kongres – poza dwiema wyżej wymienionymi Komisjami – ma również inne możliwości sprawowania nadzoru oraz kontroli nad Wspólnotą Wywiadowczą. Jedną z nich jest proces uchwalania budżetu, a zwłaszcza przyznawanie środków finansowych oraz zatwierdzanie ich wykorzystania. Podmiotem, który ma uprawnienia w powyższym zakresie, jest HPSCI i SSCI.

Istotnym uprawnieniem Kongresu jest również prawo do prowadzenia przesłuchań[65] w celu zwracania się o przekazanie informacji oraz ich uzyskiwanie od urzędników państwowych oraz ekspertów. Przesłuchania mają również aspekt nadzorczy, gdyż w ich toku członkowie Kongresu mogą uzyskać informacje o wydajności, systemie finansowania i skuteczności działań prowadzonych przez służby specjalne. Rezultatem tych przesłuchań jest sporządzanie przez jego członków raportu podsumowującego ustalenia.

Istotne są również uprawnienia senatu w zakresie zatwierdzania lub odrzucania nominacji prezydenckich na stanowiska, które pozostają w gestii prezydenta. To uprawnienie ma niebagatelne znaczenie dla obsady stanowisk we Wspólnocie Wywiadowczej (np. stanowisko Dyrektora DNI)[66].

Najważniejszym organem w ramach władzy sądowniczej, który pełni nadzór nad Wspólnotą Wywiadowczą, jest sąd właściwy w sprawach inwigilacji związanej z działaniami wywiadowczymi[67], który jest sądem federalnym ustanowionym na podstawie ustawy FISA z 1978 r.[68] Głównym zadaniem sądu jest zatwierdzanie wniosków służb specjalnych o stosowanie szeroko pojętej inwigilacji w celu zapobiegania działalności szpiegowskiej w Stanach Zjednoczonych Ameryki[69].

Królestwo Wielkiej Brytanii i Irlandii Północnej

W Wielkiej Brytanii Wspólnota Wywiadowcza, tworzona przez służby specjalne o kompetencjach wywiadowczych oraz kontrwywiadowczych (MI5, SIS, GCHQ), podlega nadzorowi ze strony władzy wykonawczej, ustawodawczej oraz sądowniczej.

Centralnym organem rządowym odpowiedzialnym za sferę wywiadowczą w Wielkiej Brytanii jest Wspólny Komitet Wywiadowczy[70] (JIC), który jest wspierany przez Wspólną Organizację Wywiadowczą[71] (JIO). Zasadniczą rolą JIC jest nadzór nad służbami specjalnymi. Jest on kierowany przez stałego przewodniczącego, który jest członkiem Służby Cywilnej. Członkowie tego organu są powoływani z poszczególnych resortów: spraw zagranicznych, obrony, spraw wewnętrznych, rozwoju międzynarodowego, skarbu, a także sił zbrojnych i gabinetu premiera. Wspólny Komitet Wywiadowczy podlega

[65] Ang. *hearings*.
[66] https://fas.org/sgp/crs/intel/RL32525.pdf [dostęp: 21 IX 2017].
[67] Ang. United States Foreign Intelligence Surveillance Court (FISC).
[68] *Foreign Intelligence Surveillance Act of 1978*.
[69] https://www.justice.gov/nsd/office-intelligence [dostęp: 20 IX 2017].
[70] Ang. Joint Intelligence Committee.
[71] Ang. Joint Intelligence Organisation.

nadzorowi Komitetu Wywiadu i Bezpieczeństwa[72]. JIC odpowiada między innymi za formułowanie priorytetów wywiadowczych i innych zadań, które mają zostać wykonane przez służby wywiadowcze. Ponadto sprawuje nadzór nad Wspólnotą Wywiadowczą i jej działaniami analitycznymi. Warto podkreślić, że JIC zapewnia sporządzane przez swoich członków oceny NSC, która stanowi główne forum dyskusyjne dla rządu w zakresie bezpieczeństwa narodowego. Z kolei JIO ocenia informacje wywiadowcze gromadzone przez poszczególne służby i przedstawia je ministrom w celu umożliwienia prowadzenia skutecznego procesu decyzyjnego na szczeblu politycznym. Ponadto JIO wytwarza niezależne, pochodzące ze wszystkich dostępnych źródeł, oceny w zakresie tematyki bezpieczeństwa narodowego i polityki zagranicznej, wspierając jednocześnie działania Sekretariatu Rady Bezpieczeństwa Narodowego[73].

Należy zaznaczyć, że strategiczne zarządzanie polityką wywiadowczą i agendą rządową w zakresie bezpieczeństwa międzynarodowego jest prowadzone przez Doradcę do Spraw Bezpieczeństwa Narodowego[74] (NSC), który stoi na czele Sekretariatu Rady Bezpieczeństwa Narodowego[75] (SNSC), i który zapewnia koordynację w zakresie bezpieczeństwa i działań wywiadowczych o strategicznym znaczeniu dla rządu. Ponadto Sekretariat Rady wspiera również działalnością doradczą premiera i innych ministrów.

Doradca do Spraw Bezpieczeństwa Narodowego, który stoi na czele SNSC, jest odpowiedzialny za koordynację oraz przedstawianie rządowej agendy w zakresie bezpieczeństwa narodowego, ale przede wszystkim pełni funkcję doradcy premiera[76].

Podstawowym organem o kompetencjach nadzorczych nad działaniami Wspólnoty Wywiadowczej – w ramach władzy ustawodawczej – jest Parlamentarny Komitet Wywiadu i Bezpieczeństwa[77] (ISC), ustanowiony na podstawie ustawy o Służbach Wywiadowczych z 1994 r.[78] Jego celem jest kontrola działań i wydatków MI5, SIS i GCHQ. Na podstawie ustawy o sprawiedliwości i bezpieczeństwie z 2013 r.[79] zreformowano ISC, zapewniając mu większe uprawnienia, w tym nadzór nad działaniami operacyjnymi i szersze uprawnienia w zakresie działań wywiadowczych oraz w sferze bezpieczeństwa prowadzone przez rząd. Poza trzema wyżej wymienionymi służbami specjalnymi ISC nadzoruje również działania związane ze sferą wywiadowczą Biura Premiera, w tym działania JIC oraz SNSC. Ponadto ISC zapewnia również nadzór nad Wywiadem Wojskowym i Biurem do Spraw Zwalczania Terroryzmu i Bezpieczeństwa. Członkowie ISC są mianowani przez Parlament. Komitet odpowiada także bezpośrednio przed Parlamentem. Może on również sporządzać raporty (które są kierowane do premiera) w zakresie zagadnień szczególnie istotnych dla bezpieczeństwa narodowego. Członkowie Komitetu mają dostęp do materiałów niejawnych o najwyższych klauzulach w celu wykonywania swoich obowiązków związanych z pracami tego Komitetu[80].

Nadzór nad służbami specjalnymi w ramach władzy sądowniczej był do 31 sierpnia 2017 r. wykonywany przez Głównego Komisarza do Spraw Uprawnień Operacyjno-

[72] Ang. Intelligence and Security Committee.
[73] https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23110.htm [dostęp: 21 IX 2017].
[74] Ang. National Security Advisor.
[75] Ang. Secretariat for the National Security Council.
[76] https://www.gov.uk/government/groups/joint-intelligence-committee [dostęp: 21 IX 2017].
[77] Ang. The Intelligence and Security Committee of Parliament.
[78] *The Intelligence Services Act 1994*.
[79] *The Justice and Security Act 2013*.
[80] http://isc.independent.gov.uk/ [dostęp: 21 IX 2017].

-Rozpoznawczych[81], Komisarza do Spraw Służb Wywiadowczych[82] i Komisarza do Spraw Przechwytywania Komunikacji[83]. Komisarze byli wybierani spośród byłych sędziów. Zadaniem komisarzy było monitorowanie działań podejmowanych przez służby w kontekście ich zgodności z właściwymi przepisami ustaw regulujących ich działalność. Co istotne – powyższe działania miały charakter następczy, a nie uprzedni. Wyżej wymienione działania monitorujące miały charakter kontrolny w odniesieniu do nakazów i decyzji upoważniających do podejmowania działań, które są przygotowywane i wydawane przez poszczególne służby, nie miały jednak, co do zasady, charakteru kontrolnego co do indywidualnych przypadków. Skargi od podmiotów indywidualnych są bezpośrednio kierowane do Trybunału do Spraw Uprawnień Dochodzeniowo-Śledczych[84]. W Wielkiej Brytanii taki nadzór jest realizowany również przez Trybunał do Spraw Uprawnień Dochodzeniowo-Śledczych[85].

Z dniem 1 września 2017 r. w Wielkiej Brytanii w miejsce dwóch dotychczasowych komisarzy **(**Komisarza do Spraw Służb Wywiadowczych i Komisarza do Spraw Przechwytywania Komunikacji) został powołany jeden nowy organ – Komisarz do Spraw Uprawnień Dochodzeniowo-Śledczych[86], którego zadaniem jest kontrola oraz nadzór nad służbami wywiadowczymi. Ten organ jest niezależnym podmiotem o kompetencjach nadzorczych i kontrolnych. Będzie on dysponował Biurem Komisarza do Spraw Uprawnień Dochodzeniowo-Śledczych[87], które przejmie zadania prowadzone przez poprzednio funkcjonujących komisarzy[88].

8. Zakończenie. Postulaty *de lege ferenda*

W doktrynie prawniczej oraz rozważaniach politologicznych dyskusja nad modelem nadzorczo-kontrolnym służb specjalnych jest żywa i przeważnie sprowadza się do wskazywania na potrzebę wprowadzenia w nim istotnych zmian, często jednak bez dokładnej ich konkretyzacji. Należy zaznaczyć, że polski model nadzoru, w znacznej mierze koresponduje z analogicznymi rozwiązaniami stosowanymi w innych, tożsamych nam prawnie państwach świata, zwłaszcza z modelem francuskim. Co więcej – wydaje się, że dyskusja w tym zakresie powinna uwzględniać zróżnicowanie celowościowe nadzoru i kontroli prowadzonych przez każdą z trójdzielnych władz, uzupełnianych w sposób racjonalny o czynnik obywatelski.

Wydaje się, że jednym z najistotniejszym elementów wymagających obecnie przekształcenia jest pozycja ministra koordynatora służb specjalnych. Funkcja ta, jak autor wykazał wcześniej, jest jednym z najistotniejszych elementów nadzorczo-kontrolnych nad służbami, odgrywając dodatkowo zasadniczą rolę w zakresie koordynowania tych służb. Wydaje się jednak, że pozycja tego ministra – szczególnie wobec innych ministrów konstytucyjnych sprawujących nadzór nad służbami mundurowymi, tj. głównie

[81] Ang. Chief Surveillance Commissioner.
[82] Ang. Intelligence Service Commissioner.
[83] Ang. The Interception of Communications Commissioner.
[84] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november 2010.pdf [dostęp: 21 IX 2017].
[85] Ang. Investigatory Powers Tribunal.
[86] Ang. Investigatory Powers Commissioner.
[87] Ang. Investigatory Powers Commissioner's Office (IPCO).
[88] https://www.gov.uk/government/news/investigatory-powers-commissioner-establishes-oversight-regime [dostęp: 22 IX 2017]; http://ipco.org.uk/ [dostęp: 22 IX 2017].

ministra obrony narodowej i ministra właściwego do spraw wewnętrznych – wymaga wzmocnienia, głównie z uwagi na czynnik jej niestałości, uzależniony od decyzji Prezesa Rady Ministrów delegującego na niego swoje uprawnienia. Zdaniem autora należy przeprowadzić debatę w zakresie zmiany modelu funkcjonowania ministra koordynatora, sprowadzającego się do uczynienia z niego ministra konstytucyjnego, z przypisanym określonym działem administracji rządowej zamiast, jak obecnie, „ministra bez teki". Taki zabieg wymagałby również odpowiednich zmian w strukturze działów administracji rządowej i wymagałby wykreowania nowego działu, systemowo ukształtowanego przez zadania między działem „bezpieczeństwo wewnętrzne" a „obrona narodowa".

Wykreowanie ministra konstytucyjnego po pierwsze rozwiązałoby problem jego niestałości, a po drugie – umożliwiłoby rozbudowanie niezbędnego aparatu urzędniczo-pomocniczego, który byłby go w stanie skutecznie obsługiwać. Wydaje się, że taki aparat urzędniczy (ministerstwo) mógłby pełnić nie tylko główną funkcję w zakresie nadzoru i kontroli nad podległymi mu służbami oraz w zakresie rozliczalności i zadaniowości, lecz także mógłby stanowić centrum analityczne bazujące na informacjach pochodzących z wszystkich podległych ministrowi służb. Odpowiednich zmian legislacyjnych wymaga doprecyzowanie i ukształtowanie na poziomie ustawodawczym zadań i uprawnień tego ministra np. w taki sposób, w jaki uczyniło to obecne rozporządzenie w sprawie szczegółowego zakresu działania ministra koordynatora służb specjalnych, przez wyróżnienie zadań w sferze nadzoru i kontroli nad służbami specjalnymi, koordynacji oraz przyznanych uprawnień, a także ich sprzężenie z ustawami kompetencyjnymi tych służb.

Na zakończenie należy wskazać, że wpływ na służby specjalne ma bez wątpienia ich odbiór społeczny, na który składa się wiele ocen cząstkowych o charakterze politycznym, prawnym, prakseologicznym i emocjonalnym dostarczanych przez organy kontroli i nadzoru nad nimi. Jakość tych ocen i sposób ich prezentowania opinii publicznej przekładają się na odbiór i podejście społeczeństwa do służb specjalnych. Wobec powyższego – organy nadzoru i kontroli powinny skupić się na formułowaniu jasnych i przejrzystych ocen, zapewniając ich prezentację szerokiemu kręgowi odbiorców.

Piotr Chorbot

Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji

1. Wstęp

Jednym z największych zagrożeń społeczności międzynarodowej w XXI w. jest terroryzm. Nie sposób nie zauważyć, że w stosunku do innych przestępstw nawet jedno zdarzenie o charakterze terrorystycznym może wywołać wysoce negatywne skutki społeczne. Wystarczy zwrócić uwagę na ostatnie wydarzenia w Londynie, gdzie furgonetka wjechała w tłum osób pod meczetem w Finsbury[1], oraz wydarzenia w Barcelonie, gdzie zginęło 14 osób, a 130 zostało rannych w wyniku ataku terrorystycznego, w którym pojazd kierowany przez zamachowca wjechał w tłum ludzi w alei Las Ramblas[2].

Współcześnie działalność terrorystyczna stanowi duże zagrożenie życia i zdrowia ludzkiego oraz jawi się jako wyzwanie dla współczesnego świata. Terroryzm jest zjawiskiem, które towarzyszyło niemalże wszystkim cywilizacjom na przestrzeni dziejów. Początkowo ataki terrorystyczne miały na celu zastraszenie pewnych grup społecznych i były związane ze stosowaniem przemocy. Obecnie można zaobserwować ciągły rozwój tego zjawiska na poziomie globalnym oraz zmiany w *modus operandi* działań sprawców, jak również ich motywacji. Przełomowe z pewnością były wydarzenia z 11 września 2001 r. w Nowym Jorku. Ataki terrorystyczne, które wówczas przeprowadzono na dwie bliźniacze wieże World Trade Center oraz Pentagon, jak się później okazało, stanowiły punkt zwrotny w wykorzystywaniu terroryzmu jako narzędzia do celów politycznych. Wprawdzie Polski nie dotknęły dotychczas tego rodzaju działania, niemniej jednak istnieją przesłanki, w związku z którymi nie można wykluczyć, że zainteresowanie organizacji terrorystycznych Polską będzie wzrastać. Zorganizowanie przez nasz kraj wielkich przedsięwzięć, tj. Szczytu NATO w Warszawie czy Światowych Dni Młodzieży w Krakowie, jak również – paradoksalnie – udział w organizacjach ponadnarodowych, tj. członkostwo w NATO oraz w Unii Europejskiej, które z jednej strony sprzyjają rozwojowi kraju, umacniają więzi międzynarodowe, zapewniają bezpieczeństwo zewnętrzne Polski, z drugiej zaś mogą jednak spowodować, że staniemy się krajem wchodzącym w orbitę zainteresowań terrorystów[3].

Brunon Hołyst twierdzi, że (…) *terroryzm jako zjawisko nieustannie ewoluuje, jest pojęciem wieloaspektowym, wielopłaszczyznowym, dynamicznym i tym samym jego jednoznaczna definicja jest praktycznie niemożliwa*[4]. Do pojęcia terroryzm wielokrotnie odnoszono się podczas licznych konferencji naukowych, zarówno na poziomie krajowym, jak i międzynarodowym. Nie opracowano jednak spójnej definicji tego zjawiska

[1] http://natemat.pl/210631,atak-terrorystyczny-na-muzulmanow-w-londynie-furgonetka-wjechala-w-tlum-wiernych-sa-zabici [dostęp: 23 IX 2017].

[2] Deptak w centrum miasta, zob. również: http://www.tvp.info/33633256/atak-terrorystyczny-w-barcelonie-zamachowiec-wjechal-w-tlum-ludzi [dostęp: 23 IX 2017].

[3] *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 8.

[4] B. Hołyst, *Terroryzm*, t. 1, Warszawa 2011, s. 52.

na poziomie międzynarodowym. Przyjmuje się, że obecnie istnieje ponad sto definicji terroryzmu. Zasadniczą przeszkodą w zdefiniowaniu tego pojęcia są bez wątpienia jego szerokie ramy. W *Encyklopedii Popularnej PWN* terroryzm określono jako:

> (…) działalność zwykle małych, ekstremistycznych ugrupowań, które za pomocą zabójstw, zagrożeń śmiercią, mordów politycznych, porwania zakładników, uprowadzeń samolotów i innych podobnych środków potępianych przez społeczność międzynarodową, usiłują zwrócić uwagę opinii publicznej na wysuwane przez siebie hasła, bądź też wymusić na rządach państw, w których działają określone ustępstwa lub świadczenia na swoją korzyść (np. zwolnienie więzionych terrorystów, okup)[5].

Ta definicja, nie stanowiąca materii prawnej, w ocenie autora niezwykle trafnie przedstawia to, z czym w rzeczywistości wiąże się dzisiaj terroryzm *sensu stricto*. Można dodać, że terroryzm stale ewoluuje, sprawcy wykorzystują coraz nowocześniejsze technologie komunikacji, wypracowują nowe metody działania i kreują swoją politykę przez działania propagandowe w Internecie. W ten sposób rozwija się potencjał poszczególnych organizacji terrorystycznych. Brak odpowiednich instrumentów po stronie państwa może skutkować powstaniem różnego rodzaju sytuacji kryzysowych. Należy zasygnalizować, że w ciągu ostatnich dwóch dekad prawodawstwo międzynarodowe (np. Konwencja Rady Europy o zapobieganiu terroryzmowi[6]), europejskie i krajowe wprowadziło liczne akty prawne mające na celu zwalczanie terroryzmu[7].

2. Projekt ustawy

Na wstępie wypada odnotować, że na szczeblu administracji rządowej przez wiele lat debatowano nad potrzebą przyjęcia ustawy antyterrorystycznej. Normalnym zjawiskiem jest bowiem zweryfikowanie przez służby, czy posiadane przez nie uprawnienia i narzędzia są wystarczające do rozpoznawania i wykrywania przez nie zagrożeń. Ewaluacja przepisów w zakresie uprawnień i obowiązków służb jest uzasadniona przy uwzględnieniu potrzeby działania służb na podstawie i w granicach prawa. Przykładowo w Belgii ustawa antyterrorystyczna została przyjęta w 2003 r., a jeszcze wcześniej, bo w 2000 r., przyjęto podobną ustawę w Wielkiej Brytanii. Wydawać by się mogło, że konsekwencją takich zabiegów legislacyjnych ze strony innych państw będą również propozycje krajowych przepisów ukierunkowanych na zwalczanie terroryzmu i – co ważniejsze – doprecyzowujących współpracę organów w tym zakresie. W Polsce jednak po 2001 r., pod wpływem wydarzeń z 11 września 2001 r., nie zdecydowano się na opracowanie jednego kompleksowego aktu prawnego dotyczącego tego zjawiska. Wprowadzono natomiast regulacje (do różnych aktów prawnych) odnoszące się do terroryzmu. Obecnie jako ciekawostkę można uznać to, że zgodnie z pierwotną ustawą z 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz.U. poz. 180) w art. 1 ust. 2 pkt 2 do zadań UOP należało zapobieganie i wykrywanie przestępstwa terroryzmu. Natomiast

[5] Tamże, s. 149.

[6] *Konwencja Rady Europy o zapobieganiu terroryzmowi, sporządzona w Warszawie dnia 16 maja 2005 r.* (Dz. U. z 2008 r. poz. 998).

[7] Szczegółowe zestawienia aktów prawnych dotyczących terroryzmu przedstawił Tomasz Bąk, zob. T. Bąk, *Ustawodawstwo antyterrorystyczne w państwach Unii Europejskiej*, w: *Polska ustawa antyterrorystyczna*…, s. 114 i in.

samo przestępstwo terroryzmu, w jego pierwotnej wersji, zostało wprowadzone do ustawy z 6 czerwca 1997 r. – Kodeks karny w 2004 r., na skutek dodania art. 115 § 20 na mocy noweli tego kodeksu z 16 kwietnia 2004 r. Kodeks karny z 1969 r. nie znał pojęcia terroryzm, a obowiązywał do dnia wejścia w życie kodeksu karnego z 1997 r. Z perspektywy historycznej, w kontekście ustawy antyterrorystycznej, w ocenie autora najistotniejszy był jednak akt wewnętrzny Prezesa Rady Ministrów w postaci zarządzenia nr 162 Prezesa Rady Ministrów z 25 października 2006 r., na którego podstawie został utworzony Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych, jako organ pomocniczy Rady Ministrów. Zadaniem tego gremium, które w dalszym ciągu działa, jest zapewnienie współpracy administracji rządowej w zakresie rozpoznawania terroryzmu, przeciwdziałania mu i jego zwalczania, a zwłaszcza: monitorowanie zagrożeń o charakterze terrorystycznym, przedstawianie opinii i wniosków Radzie Ministrów oraz opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu.

Kontynuując, w dniach 14–15 maja 2008 r. w Centralnym Ośrodku Szkolenia Agencji Bezpieczeństwa Wewnętrznego im. gen. Stefana Roweckiego „Grota" w Emowie odbyła się konferencja pt. *Czy Polsce potrzebna jest ustawa antyterrorystyczna?* Organizatorami tego przedsięwzięcia były ówczesne Ministerstwo Spraw Wewnętrznych i Administracji oraz Agencja Bezpieczeństwa Wewnętrznego (dalej: ABW). Przedstawiając komunikat odnoszący się do tego wydarzenia wskazywano, że kwestia celowości przyjęcia ustawy całościowo regulującej problematykę związaną z przeciwdziałaniem terroryzmowi została podniesiona w lutym 2007 r. na posiedzeniu Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych, powołanego z inicjatywy ministra spraw wewnętrznych i administracji. Przeprowadzona analiza pozwoliła wtedy na wyodrębnienie dwóch zasadniczych modeli rozwiązań legislacyjnych. Pierwszy polegał na istnieniu szczegółowych aktów prawnych (jednego lub kilku) regulujących kompleksowo problematykę związaną z przeciwdziałaniem zagrożeniom (albo: zagrożeniu) terrorystycznym (albo: terrorystycznemu). Taki model obowiązywał wówczas (w niektórych przypadkach w formie zmodyfikowanej) m.in. w USA, Wielkiej Brytanii, we Włoszech i Francji. Natomiast istotą drugiego rozwiązania było rozproszenie przepisów dotyczących powyższego zagadnienia w licznych aktach prawnych, często zróżnicowanej rangi. Tego rodzaju rozwiązania obowiązywały na przykład w Hiszpanii, Niemczech, Belgii oraz na Węgrzech[8]. Kolejno, jak wskazuje W. Zubrzycki[9], 10 czerwca 2008 r., na podstawie decyzji nr 5 przewodniczącego wyżej wymienionego Zespołu, został powołany Zespół Zadaniowy do Spraw Usystematyzowania Krajowych Regulacji i Rozwiązań Prawnych Dotyczących Przeciwdziałania Terroryzmowi. We wnioskach końcowych z prac tego gremium, wśród rekomendacji, pozytywnie oceniono ideę stworzenia ustawy kompleksowo regulującej problematykę dotyczącą terroryzmu. Zaproponowano powołanie zespołu do opracowania projektu ustawy o gromadzeniu i przetwarzaniu informacji w celu rozpoznawania zagrożeń o charakterze terrorystycznym. Proces tworzenia tego aktu prawnego nie został ukończony i skierowany na właściwą ścieżkę procesu legislacyjnego. Przy czym debatowano nad stworzeniem dokumentu o charakterze strategicznym, który początkowo nazywano *Strategią Obrony Przed Terroryzmem*, a który ostatecznie uchwalono jako *Narodowy Program Antyterrorystyczny na lata 2015–2019*[10].

[8] https://mswia.gov.pl/pl/aktualnosci/5605,Czy-Polsce-potrzebna-jest-ustawa-antyterrorystyczna-Konferencja-w-Emowie.pdf [dostęp: 10 IX 2017].

[9] W. Zubrzycki, *Dzieje ustawy antyterrorystycznej w Polsce*, w: *Polska ustawa antyterrorystyczna*…, s. 249.

[10] Zob. załącznik do uchwały nr 252 Rady Ministrów z 9 XII 2014 r. w sprawie *Narodowego Programu*

Pomimo wielu informacji odnoszących się do ustawy antyterrorystycznej, które pojawiały się w mediach, pierwszą oficjalną informację zwiastującą nową ustawę przedstawiono 24 marca 2016 r. na konferencji prasowej Ministerstwa Spraw Wewnętrznych i Administracji. Minister Mariusz Błaszczak poinformował wówczas, że jego zespół przygotował projekt ustawy antyterrorystycznej[11].

W dyskusji medialnej, jak również w środowiskach akademickich, debatowano, czy ustawa antyterrorystyczna, a początkowo jej projekt, zawiera rozwiązania prawne adekwatne do potrzeb służb. Podnoszono, że w Polsce zagrożenie terroryzmem jest znikome i że nie było tu do tej pory bezpośredniego zagrożenia atakiem, które stanowiłoby podstawę do wprowadzania tak daleko idących zmian w krajowym porządku prawnym. Jak słusznie zauważa P. Lubiewski, należy przypomnieć przypadek Brunona Kwietnia, który został skazany na 13 lat (wyrok obniżony do 9 lat przez sąd apelacyjny[12]) pozbawienia wolności za przygotowywanie zamachu na Sejm RP[13]. Podobnie jak P. Lubiewski autor uważa, że nie należy rozważać, czy rozwiązania prawne rozszerzające uprawnienia służb, dotykające tajemnic prawnie chronionych, są uzasadnione, ale czy wprowadzono adekwatne do tych uprawnień przepisy w zakresie kontroli i nadzoru nad służbami, które umożliwiałyby rzetelne i obiektywne zweryfikowanie pojawiających się obaw na tle stosowania danej regulacji[14]. W tym zakresie niewątpliwie rola mediów jako nośnika informacji, w przypadku kształtowania odpowiedniej świadomości społecznej na temat służb, byłaby wysoce pożądana. Zauważono liczne artykuły krytycznie prezentujące nowe regulacje prawne dotyczące przeciwdziałania terroryzmowi w Polsce. Ponadto trzeba wskazać, że ustawa o działaniach antyterrorystycznych została w części zaskarżona przez Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego[15]. Należy też odnotować, że przed sądem administracyjnym toczą się sprawy w zakresie dostępu do informacji publicznej[16], w których skarżący kwestionują odmowę udostępnienia im przez szefa ABW danych dotyczących stosowania przez ABW narzędzi, o których mowa w ustawie z 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. poz. 904, ze zm.), zwanej dalej „ustawą AT".

Głównym celem ustawy AT było wzmocnienie systemu antyterrorystycznego Rzeczpospolitej Polskiej. Realizacja tego zadania nastąpiła dzięki wdrożeniu czterech celów szczegółowych:

1) poprawie zdolności do zapobiegania zagrożeniom i zdarzeniom o charakterze terrorystycznym;
2) przygotowaniu służb i instytucji na możliwość wystąpienia zdarzeń o charakterze terrorystycznym;
3) poprawie zdolności do reagowania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym;

Antyterrorystycznego na lata 2015–2019 (M.P. poz. 1218).

[11] http://fakty.interia.pl/tylko-u-nas/news-czy-ustawa-antyterrorystyczna-jest-polsce-potrzebna,nId,2168354 [dostęp: 10 IX 2017].

[12] http://www.tvn24.pl/krakow,50/sad-apelacyjny-obnizyl-wyrok-dla-brunona-kwietnia-z-13-do-9-lat,732977.html [dostęp: 10 IX 2017].

[13] Zob. P. Lubiewski, *Ustawa antyterrorystyczna wobec służb specjalnych. Rozszerzenie czy aktualizacja uprawnień*, w: *Polska ustawa antyterrorystyczna*…, s. 13–14.

[14] Tamże.

[15] Sprawa jest prowadzona w Trybunale Konstytucyjnym pod sygn. K 35/16. Należy zauważyć, że zostało zakwestionowanych 10 przepisów tej ustawy. Por.: http://trybunal.gov.pl/sprawy-w-trybunale/art/9112-ustawa-antyterrorystyczna/ [dostęp: 24 IX 2017].

[16] Zob. http://di.com.pl/sad-uznal-ze-abw-moze-zataic-informacje-o-wykorzystaniu-nowych-uprawnien-do-inwigilacji-58024 [dostęp: 24 IX 2017].

4) *last but not least* – podniesieniu skuteczności w zakresie odtwarzania wykorzystanych sił i środków oraz udoskonalania obowiązujących procedur postępowania w kontekście zagrożeń o charakterze terrorystycznym.

Należy się zgodzić z T. Michalczykiem, że to właśnie odpowiedzi na pytania: W jaki sposób zapobiegać zdarzeniom? Jak prowadzić skuteczne rozpoznanie środowisk terrorystycznych? Jakie siły i środki są niezbędne w celu zapobiegania zamachom są kluczem do zapewnienia skutecznej polityki antyterrorystycznej gwarantującej bezpieczeństwo Polski i jej obywatelom[17].

Pierwotny projekt ustawy o działaniach antyterrorystycznych został zamieszczony na stronach Rządowego Centrum Legislacji, w zakładce „Rządowy Proces Legislacyjny", 22 kwietnia 2016 r.[18] Został on przedstawiony na etapie Stałego Komitetu Rady Ministrów, z pominięciem etapów uzgodnień międzyresortowych i konsultacji społecznych, z uwagi na wagę oraz pilność przedmiotowego projektu[19]. Następnie 6 maja 2016 r. powyższy projekt ustawy został przyjęty przez Stały Komitet Rady Ministrów i rekomendowany przez niego Radzie Ministrów[20]. Dalej został on przyjęty przez Radę Ministrów i wniesiony do Sejmu RP jako projekt rządowy oznaczony drukiem sejmowym nr 516 z 16 maja 2016 r.[21]

Z uzasadnienia do projektu ustawy o działaniach antyterrorystycznych można wywieść etiologię tej regulacji prawnej[22]. Projektodawca na wstępie wskazuje, że:

> Terroryzm stanowi jedno z największych wyzwań w kontekście zapewnienia bezpieczeństwa zarówno z perspektywy globalnej, jak i regionalnej czy krajowej. Jako zagrożenie międzynarodowe wykracza on poza ramy tradycyjnie rozumianych konfliktów i sytuacji kryzysowych.

Następnie podnosi się, że:

> (…) wzrost poziomu zagrożenia terrorystycznego obserwowany w ostatnim okresie w szczególności w państwach Europy Zachodniej, czego przykład stanowią zamachy we Francji i Belgii, skutkuje podejmowaniem zarówno przez poszczególne państwa, jak i organizacje międzynarodowe czy inne gremia, których członkiem jest Polska, starań zmierzających do zmiany przepisów, w celu wzmocnienia możliwości rozpoznawania, przeciwdziałania i zwalczania ewentualnych zagrożeń o charakterze terrorystycznym.

Powyższe oznacza, że w świetle ówczesnych wydarzeń projektodawca powziął kroki zmierzające do analizy i przeglądu obowiązujących przepisów w celu wzmocnienia poszczególnych organów i służb. Wprawdzie w uzasadnieniu zauważa się, że Polska nie była dotychczas bezpośrednim celem ataku terrorystycznego, jednak stwierdzono, że nie oznacza to, że pozostaje zupełnie wolna od tego zagrożenia. Podkreślono także, iż:

---

[17] T. Michalczyk, *Zamachy terrorystyczne w Europie – jak skutecznie prowadzić działania antyterrorystyczne w Polsce*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*…, s. 67.

[18] http://legislacja.rcl.gov.pl/projekt/12284561/katalog/12348751#12348751 [dostęp: 10 IX 2017].

[19] http://legislacja.rcl.gov.pl/docs//2/12284561/12348751/12348752/dokument218002.pdf [dostęp: 10 IX 2017].

[20] http://legislacja.rcl.gov.pl/docs//2/12284561/12348751/12348755/dokument234948.pdf [dostęp: 10 IX 2017].

[21] http://orka.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/%24File/516.pdf [dostęp: 10 IX 2017].

[22] http://orka.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/%24File/516.pdf [dostęp: 10 IX 2017].

> (…) udział Polski w działaniach międzynarodowej koalicji antyterrorystycznej, jak również fakt, że terytorium Rzeczypospolitej Polskiej jest uznawane w materiałach rozpowszechnianych przez organizacje terrorystyczne jako potencjalny cel ewentualnych zamachów, zasadne jest podjęcie na poziomie prawa krajowego odpowiednich działań legislacyjnych, zmierzających do poprawy bezpieczeństwa w związku z tymi zagrożeniami.

Następnie w uzasadnieniu zwrócono uwagę na zmienność metod wykorzystywanych przez terrorystów. W tym miejscu można nadmienić, że przed 2010 r. większość ataków terrorystycznych była związana z działaniami na wielką skalę (np. ataki terrorystyczne na pociągi w Madrycie z 11 marca 2004 r., do których użyto trzynastu bomb, czy ataki na World Trade Center z 11 września 2001 r. w Nowym Jorku z użyciem samolotów pasażerskich). Obecnie ataki terrorystyczne niejednokrotnie nazywa się „incydentami terrorystycznymi", ponieważ dotykają coraz mniejszych grup społecznych (np. atak na redakcję tygodnika „Charlie Hebdo" czy atak mężczyzny ubiegającego się o azyl na przechodniów przed posterunkiem Policji w Paryżu z 7 stycznia 2016 r.). Nie oznacza to jednak, że są one mniej dotkliwe społecznie, wydaje się wręcz, że wywołują tego samego rodzaju efekt, co zdarzenia realizowane na wielką skalę – co może stanowić przesłankę ich realizacji. Często do przeprowadzania ataków są wykorzystywane pojazdy (jak np. w przypadku zamachu w Westminister Bridge w Londynie z 22 marca 2017 r. oraz zamachu podczas jarmarku bożonarodzeniowego w Berlinie z 19 grudnia 2016 r.). Z powyższego wynika, że terroryzm przyjmuje coraz bardziej zróżnicowane formy – ataków dokonują coraz mniejsze grupy, często pojedyncze osoby niewchodzące w skład żadnych struktur.

Projektodawca wskazał, że;

> Polska musi posiadać odpowiednie instrumenty służące właściwemu rozpoznawaniu i ocenianiu zagrożeń oraz skutecznemu przeciwdziałaniu ewentualnym zdarzeniom. W przypadku ataku terrorystycznego Polska musi być przygotowana do podjęcia natychmiastowych i adekwatnych środków reagowania, a także usuwania jego skutków. Osiągnięcie tych celów wymaga zapewnienia mechanizmów współpracy wszystkich służb, organów i instytucji zaangażowanych w szeroko rozumiane działania antyterrorystyczne, jak również władz lokalnych, sektora prywatnego oraz całego społeczeństwa[23].

W ten sposób projektodawca chciał zaznaczyć, że *modus operandi* sprawców przestępstw o charakterze terrorystycznym jest wysoce zmienne, a przyjęte rozwiązania prawne mają pozwolić poszczególnym organom i służbom na łatwiejsze dostosowanie się do wykrywanych zagrożeń. Autor rozumie to również jako potrzebę integracji sił i środków w przypadku powstania zagrożenia, a to wymaga odpowiedniego poziomu współpracy i jej wypracowanych algorytmów.

W uzasadnieniu do projektu ustawy AT można również odnaleźć kryteria, jakimi kierował się projektodawca, dokonując zmiany poszczególnych przepisów i wprowadzając nowe rozwiązania prawne i organizacyjne, a mianowicie:

- wzmocnienie mechanizmów koordynacji działań,
- doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy między nimi,

[23] Tamże.

- zapewnienie możliwości prowadzenia skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego,
- zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń,
- dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze terrorystycznym;
- koncentracja przepisów w zakresie współpracy organów przy zdarzeniach o charakterze terrorystycznym na poziomie ustawowym (w projekcie wskazano, że przepisy obowiązujące w zakresie dotyczącym zwalczania terroryzmu mają charakter rozproszony i nie gwarantują adekwatnych instrumentów prawno-organizacyjnych względem narastających zagrożeń),
- wprowadzenie rozwiązań prawnych adekwatnych do aktualnych potrzeb służb związanych z wykrywaniem i rozpoznawaniem terroryzmu (stworzenie przepisów umożliwiających wykorzystanie możliwości służb w przypadku powstania sytuacji kryzysowej związanej ze zdarzeniem o charakterze terrorystycznym).

Projektodawca zaznaczył także, że wprowadzone przepisy zmierzają do wzmocnienia możliwości koordynacyjnych i nadzorczych względem realizowanych przez nie zadań. W tym aspekcie można odnieść się do rozmowy z przewodniczącym Sejmowej Komisji do Spraw Służb Specjalnych na łamach „Gazety Polskiej Codziennie". Stwierdził on, że posłowie w ramach prac Komisji sprawdzili, jak funkcjonuje ustawa antyterrorystyczna, i uznano, że jest wiele rzeczy do poprawy, jeśli chodzi o funkcjonowanie służb antyterrorystycznych. Marek Opioła wskazał, że obecnie każdy komendant wojewódzki Policji ma swoje siły antyterrorystyczne. Są one zatem rozproszone i nie mają jednolitego systemu zadań, szkoleń czy odpowiedzialności osobowej[24].

Projekt wpłynął na sejmową ścieżkę legislacyjną 16 maja 2016 r. Tego samego dnia został skierowany do I czytania na posiedzeniu Sejmu RP, które odbyło się 20 maja 2016 r. Następnie (również tego samego dnia) został przekazany do Komisji Administracji i Spraw Wewnętrznych, z zaleceniem zasięgnięcia opinii Komisji do Spraw Służb Specjalnych oraz Komisji Obrony Narodowej. Komisje obradowały, czego efektem było ich sprawozdanie wyrażone w druku sejmowym nr 567. Projekt został przekazany do II czytania na posiedzeniu Sejmu RP 8 czerwca 2016 r., dwa dni później zaś odbyło się III czytanie, w którego ramach odbyło się głosowanie nad całością projektu ustawy. Zgodnie z danymi przedstawionymi na stronach Sejmu RP 249 posłów było „za", 173 „przeciw", a 10 wstrzymało się od głosu, co oznaczało, że Sejm RP uchwalił ustawę o działaniach antyterrorystycznych. Wskazywano, że prace nad tą ustawą były prowadzone pospiesznie, jednak jeśli spojrzeć na krajowy proces legislacyjny, to można odnaleźć wiele regulacji, które zostały wprowadzone szybciej i dotyczyły równie istotnych aspektów życia społecznego oraz które pojawiały się w każdej kolejnej kadencji Sejmu RP[25].

Uchwalona ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych została przekazana Marszałkowi Senatu. Senat nie wniósł poprawek, w związku z czym ustawę przekazano do podpisu Prezydentowi RP, który to 22 czerwca 2016 r. ją podpisał. Regu-

[24] Zob. http://gpcodziennie.pl/62494-specsluzbypotrzebujazmiany.html [dostęp: 24IX 2017].

[25] https://www.money.pl/gospodarka/wiadomosci/artykul/kwota-wolna-pis-najszybsza-ustawa-sejm,184,0,2209464.html [dostęp: 23 IX 2017].

lacja, o której mowa, została ogłoszona w Dzienniku Ustaw z 2016 r. pod pozycją 904. Jednokrotnie ustawę znowelizowano, a zmiany wynikały z powstania Krajowej Administracji Skarbowej (Dz.U. z 2016 r. poz. 1948).

3. Ustawa o działaniach antyterrorystycznych

Statystycznie rzecz ujmując, przedmiotowy akt prawny liczy 65 jednostek redakcyjnych, w tym blisko połowa z nich dotyczy zmian w innych ustawach. Ustawę podzielono na następujące rozdziały:

1) rozdział 1 – ogólny,
2) rozdział 2 – *Działania antyterrorystyczne zapobiegające zdarzeniom o charakterze terrorystycznym*,
3) rozdział 3 – *Stopnie alarmowe*,
4) rozdział 4 – *Działania antyterrorystyczne na miejscu zdarzenia o charakterze terrorystycznym, w tym działania kontrterrorystyczne*,
5) rozdział 5 – *Przepisy szczególne dotyczące postępowania przygotowawczego*,
6) rozdział 6 – *Zmiany w przepisach*,
7) rozdział 7 – *Przepisy przejściowe, dostosowujące i przepis końcowy*.

Ustawa zawiera jeden załącznik w postaci wzoru karty informacyjnej KPP/MCR, o której mowa w art. 58 ustawy AT. Poniżej przedstawiono komentarz do niektórych przepisów tej ustawy.

W myśl art. 1 ustawa AT określa zasady prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań.

Ustawa zawiera także słowniczek podstawowych definicji, który został określony w art. 2 ustawy AT. W tym przepisie definiuje się m.in. takie pojęcia, jak: działania antyterrorystyczne, działania kontrterrorystyczne, miejsce zdarzenia o charakterze terrorystycznym, jak również co się rozumie przez zdarzenie o charakterze terrorystycznym.

Najważniejszym przepisem ustawy jest art. 3 ustawy AT. Rozstrzyga on bowiem o podziale kompetencyjnym w obszarze szeroko ujętej problematyki antyterrorystycznej. Na podstawie art. 3 ust. 1 ustawy AT szef ABW odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym. Natomiast zgodnie z art. 3 ust. 2 minister właściwy do spraw wewnętrznych odpowiada za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia. Do momentu uchwalenia niniejszej ustawy nie było tak jednoznacznego rozdzielenia odpowiedzialności kompetencyjnej w kontekście problematyki antyterrorystycznej. W ocenie P. Lubiewskiego ten rozdział kompetencyjny stanowi odpowiedź na wieloletni postulat, aby dokonać precyzyjnego podziału odpowiedzialności w obszarze zdarzeń o charakterze terrorystycznym[26].

Ponadto D. Pożaroszczyk już w 2013 r. wskazywał, że przydzielenie jednej służbie odpowiedzialności za zapobieganie zdarzeniom o charakterze terrorystycznym stanowiło klucz do sukcesu w Niemczech, gdzie komórki terrorystyczne pojawiały się dość licznie, ale często były likwidowane przez Federalny Urząd Ochrony Konstytucji, zanim jeszcze doszło do zamachów[27].

[26] P. Lubiewski, *Ustawa antyterrorystyczna wobec służb specjalnych*…, s. 314.

[27] D. Pożaroszczyk, *Federalny Urząd Ochrony Konstytucji – zadania i charakterystyka zwalczanych zagro-*

Z kolei art. 4 ustawy AT stanowi powtórzenie regulacji prawnej zawartej dotychczas w art. 12a ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209) ustanawiającej obowiązek współpracy organów administracji publicznej, właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego. Ten obowiązek obejmuje m.in. niezwłoczne przekazywanie szefowi ABW będących w ich posiadaniu informacji dotyczących zagrożeń o charakterze terrorystycznym w odniesieniu do infrastruktury administracji publicznej lub infrastruktury krytycznej, w tym zagrożeń funkcjonowania systemów i sieci energetycznych, wodnokanalizacyjnych, ciepłowniczych oraz teleinformatycznych, istotnych z punktu widzenia bezpieczeństwa państwa. Wskazano także, że szef ABW, w przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze administracji publicznej lub infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, może wydawać polecenia organom i podmiotom zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywać im informacje niezbędne do tego celu. Z kolei wymienione tam organy i podmioty informują szefa ABW o podjętych w tym zakresie działaniach. Szef ABW, z uwagi na potrzebę zapewnienia możliwości nadzoru i koordynacji, został również zobowiązany do niezwłocznego informowania o podjętych działaniach ministra koordynatora służb specjalnych.

Jak wynika z uzasadnienia projektu ustawy AT, w celu zapewnienia możliwości skutecznej realizacji przez szefa ABW zadania polegającego na zapobieganiu zdarzeniom o charakterze terrorystycznym, w art. 5–11 ustawy AT zawarto przepisy prawne odnoszące się do realizowanych przez niego, we współpracy z innymi właściwymi służbami i instytucjami, działań w zakresie:

- koordynacji czynności analityczno-informacyjnych podejmowanych przez służby specjalne oraz wymiany informacji przekazywanych przez Policję, Straż Graniczną, Biuro Ochrony Rządu, Państwową Straż Pożarną, Krajową Administrację Skarbową, Żandarmerię Wojskową i Rządowe Centrum Bezpieczeństwa, dotyczących zdarzeń o charakterze terrorystycznym oraz danych o osobach, o których mowa w art. 6 ust. 1 (wykaz informacji o osobach podejrzewanych o terroryzm), przez ich gromadzenie, przetwarzanie i analizowanie, dotyczących zagrożeń o charakterze terrorystycznym oraz danych o osobach mogących mieć związek ze zdarzeniami o charakterze terrorystycznym (art. 5 ust. 1),
- prowadzenia wykazu osób, które mogą mieć związek ze zdarzeniami o charakterze terrorystycznym (art. 6),
- koordynacji czynności operacyjno-rozpoznawczych podejmowanych przez służby specjalne oraz Policję, Straż Graniczną, Krajową Administrację Skarbową i Żandarmerię Wojskową dotyczących zdarzeń o charakterze terrorystycznym oraz czynności obserwowania i rejestrowania, przy użyciu środków technicznych, obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom, podejmowanych przez funkcjonariuszy celnych, w tym wydawania zaleceń, mających na celu usunięcie lub minimalizację zaistniałego zagrożenia terrorystycznego (art. 7),

żeń, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 165–168.

- możliwości zarządzenia wobec osoby niebędącej obywatelem RP, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, na okres nie dłuższy niż 3 miesiące, niejawnego prowadzenia czynności. Szef ABW przekazuje zarządzenie w tej sprawie wraz z uzasadnieniem ministrowi koordynatorowi służb specjalnych, jeżeli został powołany, oraz prokuratorowi generalnemu (art. 9). Prokurator generalny może nakazać zaprzestanie czynności,
- możliwości pobierania przez funkcjonariuszy ABW, Policji i Straży Granicznej obrazu linii papilarnych lub utrwalania wizerunku twarzy albo nieinwazyjnego pobierania materiału biologicznego w celu oznaczenia profilu DNA osoby niebędącej obywatelem Rzeczypospolitej Polskiej (art. 10),
- możliwości uzyskiwania nieodpłatnie dostępu do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach, a także obrazu zdarzeń rejestrowanego przez urządzenia rejestrujące obraz umieszczone w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych oraz otrzymywania nieodpłatnie kopii zarejestrowanego zapisu tego obrazu (art. 11).

Jeśli zaś spojrzeć na treść art. 8 ustawy AT, stanowiącego podstawę do koordynacji przez szefa ABW czynności operacyjno-rozpoznawczych podejmowanych przez służby specjalne i inne służby, przez pryzmat przepisów prawnych wcześniej obowiązujących w tym zakresie, należałoby zwrócić uwagę, że stanowi on dopełnienie art. 40 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2016 r. poz. 1897, ze zm.), zwanej dalej „ustawą o ABW oraz AW", gdyż zgodnie z tym przepisem, który od 2002 r. (uchwalenie przez Sejm RP ustawy o ABW oraz AW) nie uległ zmianie, szef ABW koordynuje podejmowane przez służby specjalne czynności operacyjno-rozpoznawcze mogące mieć wpływ na bezpieczeństwo państwa. W tym kontekście umożliwiono szerszą wymianę informacji z innymi formacjami niż służby specjalne, takimi jak: Policja, Straż Graniczna, Generalny Inspektor Kontroli Skarbowej i Żandarmeria Wojskową, a także w innym zakresie w stosunku do funkcjonariuszy celnych.

Z kolei w art. 9 ustawy AT wprowadzono możliwość zarządzenia przez szefa ABW wobec osoby niebędącej obywatelem RP, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, na okres nie dłuższy niż trzy miesiące, niejawnego prowadzenia czynności operacyjno-rozpoznawczych. Projektodawca wskazał w uzasadnieniu do projektu ustawy, że w świetle wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11) dopuszczalne jest wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, którzy podlegają polskiemu prawu, o czym przesądza art. 37 ust. 2 Konstytucji RP, z zastrzeżeniem, że w tego rodzaju przypadkach ma zastosowanie także art. 31 ust. 3 Konstytucji RP, zgodnie z którym: *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*. W tym wyroku Trybunał nie wykluczył dopuszczalności odmiennego określenia przesłanek pozyskiwania danych i postępowania z nimi w stosunku do osób niepodlegających polskiemu prawu i zaznaczył, że w każdym wypadku takie działania władz publicznych muszą mieścić się w ramach standardów demokratycznego państwa prawnego.

Pozytywne zdanie na temat tego instrumentu zaprezentował M. Róg, w swoim wykładzie pt. *Kontrola cudzoziemców jako element zapewnienia bezpieczeństwa państwa*. Odnosząc się do kwestii konfliktów zbrojnych (militarnych), wskazał, że (…) *zawsze terytorium państwa w którym miały się odbyć działania zbrojne było infiltrowane przez odpowiednio przeszkolonych, no nazwijmy ich funkcjonariuszami obcego państwa*[28].

O zarządzeniu niejawnego prowadzenia czynności w odniesieniu do cudzoziemców, na podstawie art. 9 ustawy AT, szef ABW będzie niezwłocznie zawiadamiał ministra koordynatora służb specjalnych, jeśli został on powołany, oraz prokuratora generalnego. Szef ABW będzie również informował prokuratora generalnego o wynikach wyżej wymienionych czynności, a także przekazywał mu wszystkie zgromadzone materiały, a prokurator generalny będzie podejmował decyzję o zakresie i sposobie ich wykorzystania oraz zarządzał ich zniszczenie.

W kontekście identyfikacji osób, które mogą mieć związek z przestępstwami o charakterze terrorystycznym istotne pozostają również zapisy art. 10 ustawy AT dotyczące uprawnienia funkcjonariuszy ABW, Policji i Straży Granicznej do pobierania obrazu linii papilarnych lub utrwalania wizerunku twarzy osoby niebędącej obywatelem RP, w uzasadnionych, określonych w ustawie przypadkach. Należy nadmienić, że czynności operacyjno-rozpoznawcze dokonywane na podstawie art. 9 ustawy AT są prowadzone zgodnie ze standardami odnoszącymi się do kontroli operacyjnej, które wynikają z ustaw kompetencyjnych służb uprawnionych w tym zakresie, z tym zastrzeżeniem, że organem kontrolnym jest w tym przypadku nie sąd, a prokurator generalny.

W kontekście art. 11 ustawy AT należy wskazać, że szef ABW uzyskał uprawnienia w zakresie nieodpłatnego dostępu do danych i informacji zgromadzonych w rejestrach publicznych oraz ewidencjach prowadzonych przez inne organy, służby i podmioty, w tym także jednostki samorządu terytorialnego, jak również obrazu z urządzeń monitoringu wizyjnego umieszczonych w miejscach publicznych, z uwzględnieniem zasad i trybu przyjętego w obecnie obowiązującym art. 34 ustawy o ABW oraz AW. Ten przepis został utworzony w celu zapewnienia ABW dostępu do wszelkich przydatnych danych i informacji, w celu zapobiegania zdarzeniom o charakterze terrorystycznym.

Celem ustawy AT było wprowadzenie nowych procedur i obowiązków o charakterze informacyjnym oraz rejestracyjnym zmierzających przede wszystkim do przyspieszenia procesu decyzyjnego w przypadku wystąpienia zamachu terrorystycznego w Polsce.

Ustawa AT wprowadziła także powszechnie obowiązujący i dostosowany do wymogów NATO czterostopniowy system stopni alarmowych (art. 15 ustawy AT i następne) na wypadek zagrożeń terrorystycznych oraz stopni alarmowych w cyberprzestrzeni – stopnie alarmowe CRP (dotychczasowy system, obowiązujący na podstawie zarządzenia nr 18 Prezesa Rady Ministrów z 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego obejmował wyłącznie administrację rządową).

Z systemem stopni alarmowych został powiązany system udzielania w trybie pilnym niezbędnego wsparcia ze strony Sił Zbrojnych RP w przypadku, gdy siły i środki Policji mogłyby okazać się niewystarczające do reagowania w przypadku zamachu terrorystycznego.

Kierownicy służb i instytucji właściwi w sprawach bezpieczeństwa i zarządzania kryzysowego, proporcjonalnie do wprowadzonego stopnia alarmowego są zobligowa-

[28] https://www.interwizja.edu.pl/index.php?option=com_content&task=view&id=7155&Itemid=177 [dostęp: 23 IX 2017].

ni do podnoszenia poziomu przygotowania do reagowania na zagrożenia o charakterze terrorystycznym przez realizację określonych dla poszczególnych przedsięwzięć stopni alarmowych.

W ustawie AT uregulowano cztery rodzaje stopni alarmowych i cztery rodzaje stopni alarmowych CRP (w zależności od skali zagrożenia atakiem terrorystycznym):

1) pierwszy stopień (stopień ALFA), wprowadzany w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia;
2) drugi stopień (stopień BRAVO), wprowadzany w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, jednak gdy konkretny cel zdarzenia nie został zidentyfikowany;
3) trzeci stopień (stopień CHARLIE), wprowadzany w przypadku:
   a) wystąpienia zdarzenia potwierdzającego cel potencjalnego zdarzenia o charakterze terrorystycznym godzącego w: bezpieczeństwo lub porządek publiczny albo bezpieczeństwo Rzeczpospolitej Polskiej albo bezpieczeństwo innego państwa lub organizacji międzynarodowej oraz stwarzającego potencjalne zagrożenie Rzeczpospolitej Polskiej,
   b) uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym na terytorium Rzeczpospolitej Polskiej,
   c) uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym, którego skutki mogą dotyczyć obywateli polskich przebywających za granicą lub instytucji polskich albo polskiej infrastruktury, mieszczących się poza granicami Rzeczpospolitej Polskiej;
4) czwarty stopień (stopień DELTA), wprowadzany w przypadku:
   a) wystąpienia zdarzenia o charakterze terrorystycznym, powodującego zagrożenie bezpieczeństwa lub porządku publicznego albo bezpieczeństwa Rzeczpospolitej Polskiej albo bezpieczeństwa innego państwa lub organizacji międzynarodowej oraz stwarzającego zagrożenie Rzeczpospolitej Polskiej,
   b) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym na terytorium Rzeczpospolitej Polskiej,
   c) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym, które ma być wymierzone w obywateli polskich przebywających za granicą lub instytucje polskie albo polską infrastrukturę mieszczące się poza granicami Rzeczpospolitej Polskiej, a zebrane informacje wskazują jednocześnie na nieuchronność takiego zdarzenia.

Na uwagę zasługuje również mechanizm wprowadzony w art. 17 ustawy AT, dotyczący powoływania przez szefa ABW sztabu koordynacyjnego, w przypadku wprowadzenia stopnia alarmowego odnoszącego się do terytorium RP lub stopnia alarmowego CRP.

Na wyżej wymienionej płaszczyźnie można odnotować działania służb. Przykładowo po wydarzeniach w Manchesterze[29] ABW nie rekomendowała wprowadzenia stopnia alarmowego w Polsce. Rzecznik prasowy ministra koordynatora służb specjalnych S. Żaryn powiedział, że ABW w związku z wydarzeniami w Manchesterze (…) *pozostaje w stałym kontakcie ze wszystkimi podmiotami polskiego systemu antyterrorystycznego*

[29]http://wyborcza.pl/7,75399,21849668,wielu-zabitych-i-rannych-podczas-koncertu-w-manchesterze-doszlo.html [dostęp: 24 IX 2017].

i partnerami zagranicznymi, w tym z brytyjskimi oraz dodał, że (…) *Centrum Antyterrorystyczne ABW w chwili obecnej nie posiada informacji świadczących o tym, że zamach w Manchesterze mógłby bezpośrednio wpłynąć na poziom bezpieczeństwa w Polsce* i poinformował, że Agencja (…) *nie rekomenduje wprowadzenia stopnia alarmowego na terytorium RP*. Należy nadmienić, że w wybuchu, do którego doszło w hali widowiskowo-sportowej w Manchester Arena, tuż po zakończeniu koncertu amerykańskiej piosenkarki Ariany Grande, według podawanych wówczas danych zginęły co najmniej 22 osoby, w tym dzieci, a 59 zostało rannych[30]. Trzeba wspomnieć, że na podstawie ustawy dwukrotnie skorzystano na terenie Polski z możliwości wprowadzenia stopni alarmowych. Podczas szczytu NATO w lipcu 2016 r. w Warszawie wprowadzono pierwszy stopień alarmowy ALFA, który obowiązywał w tym mieście. Ponadto stopień alarmowy ALFA wprowadzono także podczas Światowych Dni Młodzieży w dniach 26–31 lipca 2016 r. – obowiązywał on na terytorium całej RP[31]. Jednocześnie obowiązywał drugi stopień alarmowy CRP (BRAVO)[32]. Ten przepis daje podstawę do wprowadzenia i przećwiczenia odpowiednich algorytmów postępowania służb. Zainicjowanie każdego ze stopni wiąże się z realizacją odpowiednich działań zapobiegawczych. W ocenie autora wszelkie przepisy ustanawiane w celu kreacji właściwych postaw i polegające na ćwiczeniu reakcji na zagrożenie pozwalają lepiej przygotować służby do działania, a tym samym – zwiększyć standard bezpieczeństwa RP.

W rozdziale 4 ustawy AT, w art. 18, określono, kto i w jakich przypadkach wyznacza kierującego działaniami antyterrorystycznymi podejmowanymi przez właściwe służby lub organy w ramach ich ustawowych zadań na miejscu zdarzenia o charakterze terrorystycznym. Co do zasady, zwłaszcza w przypadku obecności na miejscu zdarzenia o charakterze terrorystycznym innych służb i organów, komendant główny Policji, a w sytuacjach niecierpiących zwłoki komendant wojewódzki Policji, wyznacza w tym celu funkcjonariusza Policji. Natomiast w przypadku zdarzenia o charakterze terrorystycznym na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne minister obrony narodowej, a w sytuacjach niecierpiących zwłoki komendant główny Żandarmerii Wojskowej, na kierującego działaniami wyznacza żołnierza Żandarmerii Wojskowej.

Kolejny artykuł – 21 – ustawy AT wprowadza rozwiązanie prawne, zgodnie z którym po wprowadzeniu trzeciego lub czwartego stopnia alarmowego minister właściwy do spraw wewnętrznych, z inicjatywy własnej albo na wniosek szefa ABW lub komendanta głównego Policji, może zarządzić zakaz odbywania zgromadzeń lub imprez masowych na obszarze lub w obiekcie objętym stopniem alarmowym, na czas obowiązywania tego stopnia, jeżeli jest to niezbędne do ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego, o czym niezwłocznie informuje Marszałka Sejmu Rzeczpospolitej Polskiej i Marszałka Senatu Rzeczpospolitej Polskiej, którzy przekazują tę informację odpowiednio posłom i senatorom. Przepis, o którym mowa, budził wiele wątpliwości. Szeroko komentowano sprawy dotyczące (…) *zarządzania zakazu odbywania zgromadzeń*, ale pozostawiono bez komentarza wymóg ustanowiony w przepisie, w postaci

[30] http://www.pap.pl/aktualnosci/news,946000,abw-nie-rekomenduje-wprowadzenia-stopnia-alarmowego-w-polsce.html [dostęp: 24 IX 2017].

[31] http://www.pap.pl/aktualnosci/news,1017974,wiceminister-zielinski-niski-poziom-zagrozenia-terrorystycznego-w-polsce.html [dostęp: 24 IX 2017 r.].

[32] http://rcb.gov.pl/stopien-alarmowy-alfa-i-bravo-crp-na-terenie-calego-kraju/ [dostęp: 24 IX 2017].

wprowadzenia trzeciego lub czwartego stopnia alarmowego. Oznacza to mniej więcej, że nie będą możliwe zgromadzenia wyłącznie w przypadkach wskazanych dla tego stopnia, np. wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym lub chociażby w momencie, gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do takiego zdarzenia. Ważne są w tym względzie także zapisy art. 21 ust. 2 – w części wspólnej, zgodnie z którymi zarządzenie obowiązuje w czasie obowiązywania stopnia alarmowego i na obszarze jego obowiązywania w części objętej właściwością miejscową organu administracji publicznej (który wydał decyzję). P. Lubiewski zauważa, że ustawodawca nie zobowiązał organu gminy zakazującego zgromadzenia do poinformowania o wprowadzonym zakazie Marszałków Sejmu i Senatu, a jedynie właściwy sąd okręgowy[33].

W art. 23 ustawy AT wprowadzono możliwość tzw. specjalnego użycia broni, określanego mianem „strzału ratunkowego" lub „snajperskiego", oznaczającego możliwość użycia broni palnej przeciwko osobie dokonującej zamachu, którego skutkiem może być śmierć lub bezpośrednie zagrożenie życia lub zdrowia tej osoby. Będzie to zgodnie z projektem ustawy dopuszczalne w ramach działań kontrterrorystycznych, jeżeli będzie niezbędne do przeciwdziałania bezpośredniemu, bezprawnemu, gwałtownemu zamachowi na życie lub zdrowie człowieka, a użycie broni palnej w sposób wyrządzający możliwie najmniejszą szkodę jest niewystarczające i przeciwdziałanie takiemu zamachowi w inny sposób nie jest możliwe, z uwzględnieniem wszelkich okoliczności zdarzenia o charakterze terrorystycznym oraz możliwości działań kontrterrorystycznych. Ustawodawca ograniczył podmiotowo niniejszy przepis, ponieważ dotyczy on wyłącznie funkcjonariuszy wykonujących działania kontrterrorystyczne, którzy wchodzą w skład wyspecjalizowanych grup kontrterrorystycznych (art. 23 ust. 4 ustawy AT). P. Lubiewski wskazuje, że to zagadnienie nie budziło większych wątpliwości, gdyż postulat umożliwienia służbom fizycznego wyeliminowania (w ściśle określonych sytuacjach) osób zagrażających życiu lub zdrowiu innych osób, podczas gdy inne prawnie dostępne środki nie przynoszą rezultatu, był podnoszony zarówno w środowisku funkcjonariuszy z tzw. grup AT, jak i polityków[34].

W kolejnym rozdziale, począwszy od art. 25 ustawy AT, uregulowano problem prowadzenia postępowań przygotowawczych. W tym zakresie należy zwrócić uwagę na możliwość wydania przez prokuratora postanowienia o przeprowadzeniu przeszukania pomieszczeń i innych miejsc znajdujących się na wskazanym w postanowieniu terenie lub o zatrzymaniu osoby podejrzewanej – jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzewana lub wymienione rzeczy znajdują się na tym terenie. W celu znalezienia rzeczy, które mogą stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, artykuł ten przewiduje również możliwość dokonania przeszukania osób, ich odzieży i podręcznych przedmiotów znajdujących się na wskazanym w postanowieniu terenie. Te czynności można przeprowadzić o każdej porze doby. W tym miejscu należy wskazać, że Europejski Trybunał Praw Człowieka w orzeczeniu „Sher i inni przeciwko Zjednoczonemu Królestwu" (nr 5201/11) uznał, że w przypadku postępowań odnoszących się do przestępstw o charakterze terrorystycznym znajduje uzasadnienie umożliwienie dokonania przeszukania lub zatrzymania na podstawie

[33] Por. P. Lubiewski, *Ustawa antyterrorystyczna wobec służb specjalnych*…, s. 316.
[34] Por. tamże, s. 317.

przesłanek określonych szerzej niż w innych przypadkach[35]. W szczególności Trybunał wskazał, że nie stanowi naruszenia Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności przeprowadzenie przeszukania w warunkach wskazanych powyżej w sytuacji, gdy przysługuje środek zaskarżenia na dokonanie czynności. Należy wskazać, że art. 221 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 2016 r. poz. 1749, ze zm.), zwany dalej „kpk.", przed wejściem w życie ustawy AT umożliwiał przeszukanie i zatrzymanie określonej osoby w ciągu całej doby[36].

Wśród zmian zakładanych w innych ustawach istotne jest zwłaszcza wprowadzenie w ustawie z 6 czerwca 1997 r. – Kodeks karny (Dz.U. poz. 553, ze zm.), zwanego dalej „kk", przepisów definiujących nowe typy przestępstw stanowiących odpowiedź na działania tzw. zagranicznych bojowników, związane z konfliktem w Syrii i Iraku oraz dostosowanie krajowych rozwiązań do podpisanego przez Polskę protokołu dodatkowego do sporządzonej 16 maja 2005 r. w Warszawie *Konwencji Rady Europy o Zapobieganiu Terroryzmowi* (Dz.U. z 2008 r. poz. 998).

Trzeba także zwrócić uwagę na zmiany w ustawie z 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2014 r. poz. 1099, ze zm.). W art. 7 uregulowano nowy obowiązek konsultacji planów ochrony obszarów, obiektów i urządzeń umieszczonych w tzw. ewidencji obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie z właściwym terytorialnie dyrektorem delegatury ABW, w zakresie zagrożeń terrorystycznych. W tym artykule dodano przepis prawny, zgodnie z którym plan ochrony powinien zawierać analizę stanu potencjalnych zagrożeń o charakterze terrorystycznym. Warto zauważyć, że na stronie internetowej ABW powstała zakładka poświęcona temu zagadnieniu, gdzie można zapoznać się z *Procedurą uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie w zakresie zagrożeń o charakterze terrorystycznym*[37].

Odnotowania wymaga instytucja prawna, pozwalająca (art. 38 ustawy AT – zmiany w ustawie o ABW oraz AW dotyczące wprowadzenia nowego art. 22b tej ustawy) na pozyskanie do współpracy osób działających na rzecz innego państwa lub organizacji (w odniesieniu do przestępstw o charakterze terrorystycznym i szpiegostwa). W przypadku, gdy informacje lub materiały uzyskane przez ABW podczas realizacji zadań wskazują na popełnienie przestępstwa szpiegostwa albo uprawdopodobniają działalność zmierzającą do popełnienia przestępstwa o charakterze terrorystycznym szef ABW otrzymał uprawnienie do odstąpienia – gdy jest to uzasadnione względami bezpieczeństwa państwa – od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa oraz o osobie, która według informacji lub materiałów uzyskanych przez ABW może być jego sprawcą.

Skorzystanie przez szefa ABW z powyższego uprawnienia jest możliwe jedynie pod warunkiem, że sprawca przestępstwa szpiegostwa albo podejrzewany o przestępstwa o charakterze terrorystycznym świadomie i dobrowolnie ujawnił wszelkie okoliczności popełnionego czynu lub prowadzonej działalności oraz zobowiązał się do podjęcia tajnej współpracy z ABW. Odstąpienie przez szefa ABW od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa będzie możliwe po zasięgnięciu opinii prokuratora generalnego oraz ministra koordynatora

[35] http://www.echr.coe.int/Documents/COURTalks_Terr_Talk_POL.PDF [dostęp: 24 IX 2017].

[36] Por. P. Lubiewski, *Ustawa antyterrorystyczna wobec służb specjalnych*…, s. 317.

[37] https://www.abw.gov.pl/pl/procedura-uzgadniania-p/1297,W-zwiazku-z-wejsciem-w-zycie-ustawy-z-dnia-10-czerwca-2016-r-o-dzialaniach-antyt.html [dostęp: 21 IX 2017].

służb specjalnych, jeżeli został powołany. Osobie pozyskanej do współpracy na zasadach wskazanych w ustawie AT przysługują odpowiednie do zagrożenia środki ochronne. W ustawie, o której mowa, przewidziano szereg warunków ograniczających prowadzenie współpracy.

Kolejno w ustawie AT uregulowano problem dostępu do informacji stanowiących tajemnicę bankową (art. 34 ustawy AT oraz zmiany w ustawie o ABW oraz AW – dodany na mocy ustawy AT art. 34a ustawy o ABW oraz AW). Ustawa AT umożliwia szefowi ABW uzyskiwanie dostępu do przetwarzanych przez banki informacji stanowiących tajemnicę bankową osób, ich odzieży i podręcznych przedmiotów oraz informacji dotyczących umów o rachunek papierów wartościowych, umów o rachunek pieniężny, umów ubezpieczenia lub innych umów dotyczących obrotu instrumentami finansowymi, świadczenia usług płatniczych lub zawieranych z uczestnikami funduszy inwestycyjnych, a przede wszystkim danych osób, które zawarły takie umowy, przetwarzanych przez uprawnione podmioty. To rozwiązanie miało na celu usprawnienie działań w zakresie przeciwdziałania finansowaniu terroryzmu oraz innych przestępstw, których rozpoznawanie i wykrywanie oraz którym zapobieganie należy do zadań ABW.

W ustawie AT uwzględniono także odpowiedzialność ABW w zakresie rozpoznawania zagrożeń w cyberprzestrzeni, zapobiegania im oraz ich zwalczania, a w ustawie o ABW oraz AW wprowadzono szczegółowe rozwiązania dotyczące ochrony cyberprzestrzeni (art. 34 ustawy AT – zmiany dot. art. 5 – oraz dodane art. 32a–e ustawy o ABW oraz AW). Agencja Bezpieczeństwa Wewnętrznego stała się właściwa w zakresie rozpoznawania zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, zapobiegania im oraz ich zwalczania, przez uwzględnienie tego problemu wśród zadań ustawowych tej instytucji określonych w art. 5 ust. 1 ustawy o ABW oraz AW. Ponadto ABW powierzono zadanie polegające na przeprowadzaniu oceny bezpieczeństwa wskazanych wyżej systemów teleinformatycznych albo sieci teleinformatycznych (art. 32a dodany do ustawy o ABW oraz AW), a także szef ABW został obowiązany do analizy zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych (nowy art. 32e w ustawie o ABW oraz AW). W tym względzie należy zwrócić uwagę na wypowiedź rzecznika ministra koordynatora służb specjalnych S. Żaryna, który stwierdził, że (…) *walka w cyberprzestrzeni jest coraz ostrzejsza*. Wskazał również, że (…) *nikt nie jest w stanie odpowiedzialnie stwierdzić, że Polska jest bezpieczna i odporna na ataki hakerów*. W kontekście wprowadzonego przepisu wskazał, iż (…) *testy faktycznie mają miejsce* (…) *nie chcemy jednak zdradzać szczegółów, nie będziemy informowali o wykrytych lukach czy błędach*. Właściwe zespoły, zwane CERTami[38], czyli zespoły reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet, działają w całej Europie – w Polsce jest ich kilka (m.in. cert pl, cert.gov.pl czy mil-cert pl). Te działania mają na celu, jak wynika z analizy powyższej wypowiedzi, przede wszystkim niedopuszczenie do sytuacji, która niedawno miała miejsce na Ukrainie, gdzie dokonano ataków hakerskich na banki, telekomunikację i metro[39].

[38] Z ang. *Computer Emergency Response Team*.

[39] https://wpolityce.pl/swiat/346123-zmasowany-atak-hakerski-na-ukrainie-wirus-zaatakowal-system-bankowy-i-telekomunikacyjny [dostęp: 24 IX 2017].

Nowym instrumentem (nowy art. 32c ustawy o ABW oraz AW) odnoszącym się do systemów teleinformatycznych, którego celem nie będzie jednak bezpośrednio ich ochrona, ale zapobieganie przestępstwom o charakterze terrorystycznym, przeciwdziałanie im, wykrywanie ich oraz ściganie ich sprawców, było przyznanie Sądowi Okręgowemu w Warszawie, na pisemny wniosek szefa ABW złożony po uzyskaniu pisemnej zgody prokuratora generalnego, uprawnienia do wydania postanowienia, w którym zarządzi zablokowanie – albo zażąda od administratora systemu teleinformatycznego zablokowania – dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym na czas określony, nie dłuższy niż 30 dni.

Powyższy przepis skłonił organizacje pozarządowe do złożenia wniosku na temat tego, ile i jakie strony ABW zablokowała na podstawie nowych przepisów ustawy AT. Agencja odmówiła udzielenia takich informacji. Sprawa trafiła do Wojewódzkiego Sądu Administracyjnego w Warszawie, który stwierdził, że ABW miała prawo odmówić podania informacji. Zdaniem fundacji, która była wnioskodawcą, ten przepis ustawy stanowi zagrożenie dla wolności słowa. Sąd oddalił skargę. Z informacji medialnych wynika[40], że wniosek nie powinien zostać uwzględniony, przeciwko niemu przemawia bowiem interes dotyczący bezpieczeństwa państwa. Ponadto zgodnie z przedstawianymi w mediach informacjami sędzia sprawozdawca, A. Lipiński, miał powiedzieć, że (…) *taka klauzula w tym momencie jest uzasadniona tym, co aktualnie dzieje się na świecie* i wskazał na coraz częstsze dokonywanie zamachów terrorystycznych. Fundacja zapowiedziała, że zwróci się o sporządzenie pisemnego uzasadnienia i że po jego analizie rozważy złożenie skargi kasacyjnej do Naczelnego Sądu Administracyjnego[41].

Rozwiązanie prawne dotyczące zablokowania danych informatycznych było wielokrotnie komentowane na łamach prasy i w mediach społecznościowych[42]. Zapomina się jednak o tym, że o zastosowaniu tego instrumentu prawnego decyduje Sąd, a nie służby, i że to do decyzji sądu należy uwzględnienie wniosku szefa ABW w zakresie zażądania od administratora systemu teleinformatycznego zablokowania dostępności w tym systemie określonych danych. Nie przykłada się należytej wagi do tego, jakie oblicze ma obecnie sieć Internet w kontekście zagrożeń terrorystycznych – jest ona coraz częściej wykorzystywana do nielegalnej działalności związanej z terroryzmem. Z tego względu powyższe uprawnienie ma w opinii autora szczególne znaczenie w odniesieniu do przeciwdziałania działalności organizacji terrorystycznych, które wykorzystują Internet do promowania swojej ideologii, zamieszczania instruktażu dotyczącego sposobu przeprowadzania zamachów terrorystycznych oraz komunikowania się ze swoimi zwolennikami.

Ponadto przewiduje się deanonimizację osób korzystających z tzw. przedpłaconych kart telefonicznych (pre-paid) przez zobowiązanie ich do podania swoich danych operatorowi telekomunikacyjnemu. Mając na uwadze to, że anonimowość tego typu kart dostarcza – jak pokazują przypadki krajowe i zagraniczne – przestępcom, w tym osobom zaangażowanym w działalność terrorystyczną, dogodnego narzędzia do komunikowania się i kamuflażu, w ustawie przewidziano obowiązek rejestracji

[40] http://prawo.gazetaprawna.pl/artykuly/1034557,terroryzm-zmienia-optyke-sadu-na-informacje-publiczna.html [dostęp: 24 IX 2017].

[41] Wyrok WSA w Warszawie z 11 IV 2017 r., sygn. akt: II SA/Wa 1855/16.

[42] http://www.fakt.pl/pieniadze/prawo/abw-zablokuje-strony-internetowe-kontrowersyjna-ustawa-antyterrorystyczna/d081ec2 [dostęp: 23 IX 2017].

użytkowników tych kart. Wprowadzone rozwiązanie prawne było uzasadniane przy uwzględnieniu przeciwdziałania zjawisku fałszywych powiadomień o podłożeniu ładunków wybuchowych, których celem było i jest wywołanie działań właściwych służb i doprowadzenie do zakłócenia funkcjonowania organów państwa. Z tego względu wprowadzono zmianę w ustawie z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243, ze. zm. – art. 43 ustawy AT przez dodanie art. 60b w *Prawie telekomunikacyjnym*), zgodnie z którą abonenci tzw. przedpłaconych kart telefonicznych będą zobowiązani do podania swoich danych. Zgodnie z informacją przedstawioną 19 lipca 2017 r. przez sekretarza stanu w MSWiA Jarosława Zielińskiego odnoszącą się do maja i czerwca 2016 r., czyli jeszcze przed wejściem w życie ustawy AT – odnotowano 88 powiadomień o podłożeniu bomby. Natomiast w lipcu i sierpniu 2016 r. – 60 (w okresie Szczytu NATO w Warszawie i Światowych Dni Młodzieży w Krakowie), we wrześniu i październiku – 37, w listopadzie i grudniu 32. Dodał on, że w I kwartale 2017 r. takich powiadomień było 61 wobec 127 w analogicznym okresie 2016 r. Autor wnioskuje na tej podstawie, że liczba fałszywych powiadomień o podłożeniu ładunku wybuchowego może się nasilać w przypadku realizacji w Polsce przedsięwzięć rangi międzynarodowej[43]. Ponadto wprowadzony obowiązek rejestrowania kart pre-paid spowodował 31 proc. spadek liczby kart przedpłaconych używanych w Polsce w ciągu roku z ponad 25 mln do 18,4 mln sztuk – według GUS – ponieważ karty niezarejestrowane operatorzy byli obowiązani wyłączyć[44]. W. Łączewski poddaje krytyce[45] m.in. problem związany z kartami pre-paid oraz ich rejestracją, odnosi się do szyfrowania danych i niektórych sposobów komunikacji terrorystów[46], nie podpiera jednak swojego stanowiska wiarygodnymi danymi statystycznymi czy badaniami naukowymi, a jeśli już to czyni, jak w przypadku regulacji obowiązujących w Australii, to nie przywołuje ich źródeł. Co więcej, po dotarciu do źródeł przedstawionych na australijskich stronach internetowych nie stwierdzono, że proceder zakupu kart SIM przez „niewidzialną rękę" jest w Australii niemożliwy[47]. Wręcz przeciwnie – wchodząc na jeden z popularnych serwisów aukcyjnych autor nie miał najmniejszego problemu, aby znaleźć ofertę sprzedaży australijskiej karty SIM[48]. Z kolei A Tyburska i B. Jewartowski wskazują, że przepisy dotyczące rejestracji kart pre-paid stosuje się w wielu krajach Europy i świata. W ich ocenie umożliwia to pracę organów śledczych nawet w przypadku rejestracji takiej karty przy użyciu podstawionych osób oraz podrobionych czy skradzionych dokumentów. Podkreślają, że (…) *pozostawione w ten sposób „ślady" dają potencjalnie większe możliwości na ustalenie i zatrzymanie sprawców, a częstokroć zapobieżenie planowanym zamachom*[49].

[43] http://www.pap.pl/aktualnosci/news,1017974,wiceminister-zielinski-niski-poziom-zagrozenia-terrorystycznego-w-polsce.html [dostęp: 24 IX 2017].

[44] Zob. http://serwisy.gazetaprawna.pl/telekomunikacja/artykuly/1061558,karty-prepaid-8-mln-ustawa-antyterrorystyczna.html [dostęp: 24 IX 2017].

[45] Polemika do artykułu Wojciecha Łączewskiego opublikowanego w czasopiśmie „Polityka" pt. *Terroru jak nie było, tak nie ma*, zob. http://www.polityka.pl/tygodnikpolityka/kraj/1712526,1,dlaczego-ustawa-antyterrorystyczna-jest-niebezpieczna.read [dostęp: 23 IX 2017].

[46] W ocenie autora szczegółowe opisywanie tego typu informacji może stanowić cenne źródło dla rozwijających się grup o charakterze terrorystycznym.

[47] Zob. https://www.acma.gov.au/Industry/Telco/Carriers-and-service-providers/Prepaid-mobiles/new-rules-streamline-identity-checking-for-prepaid-mobiles [dostęp: 24 IX 2017].

[48] https://www.ebay.com/b/Australia-Cell-Phone-SIM-Cards/29778/bn_2877533 [dostęp: 24 IX 2017].

[49] A. Tyburska, B. Jewartowski, *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu*…, s. 265.

Uregulowano także kwestię zniszczenia lub unieruchomienia bezzałogowych statków powietrznych (dronów) w przypadkach, które mogą stanowić zagrożenie (art. 39 ustawy AT – dodanie nowych przepisów, m.in. w ustawie z 3 lipca 2002 r. – Prawo lotnicze – Dz.U. z 2016 r. poz. 605 oraz art. 126a). Wprowadzono rozwiązania rozszerzające wykaz przypadków, w których funkcjonariusze określonych w ustawie AT służb, m.in. Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego (art. 126a ust. 2 pkt 1), jak również pracownicy specjalistycznych uzbrojonych formacji ochronnych, mają prawo do użycia lub wykorzystania broni palnej przez umożliwienie zniszczenia lub unieruchomienia bezzałogowego statku powietrznego w przypadkach, gdy przebieg lotu lub działanie takiego statku: zagraża życiu lub zdrowiu osoby, stwarza zagrożenie chronionych obiektów, urządzeń lub obszarów, zakłóca przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników lub stwarza uzasadnione podejrzenie, że bezzałogowy statek powietrzny może zostać użyty jako środek ataku terrorystycznego. Należy zgodzić się ze zdaniem przedstawionym przez A. Tyburską i B. Jewartowskiego, że nowe technologie dają możliwość wykorzystywania tego typu urządzeń przez terrorystów, umożliwiają bowiem zdalne odpalanie ładunków wybuchowych i tym samym atak na wybrany obiekt, system lub urządzenie. Mogą zatem stanowić realne zagrożenie bezpieczeństwa w ruchu lotniczym[50]. Trzeba przypomnieć zdarzenie w bazie lotniczej w Balicach, gdzie dron zrzucił ładunek, który spowodował niegroźny wybuch[51].

Warto zwrócić uwagę także na zaostrzenie przepisów w zakresie dokonywania wydalenia z terytorium RP osób nieposiadających polskiego obywatelstwa (art. 57 ustawy AT i dodany art. 329a do ustawy o cudzoziemcach). Pierwsze konsekwencje prawne wynikające z tego przepisu zastosowano podczas Światowych Dni Młodzieży – deportowano wówczas obywatela Austrii podejrzewanego o radykalizm islamski[52].

4. Rzecznik Praw Obywatelskich – wniosek o zbadanie konstytucyjności niektórych przepisów ustawy AT

Niektóre przepisy ustawy AT zostały, jak to zasygnalizowano wcześniej, zakwestionowane przez Rzecznika Praw Obywatelskich, zwanego dalej „Rzecznikiem", a dokładnie: art. 2 pkt 7, art. 6, art. 6 ust. 3, art. 9 ust. 1, art. 10, art. 11, art. 26, art. 38, art. 48 oraz art. 58. Poniżej przedstawiono, jakie były generalne podstawy do zaskarżenia tych przepisów przez Rzecznika.

Zakwestionowano zatem 9 przepisów ustawy, w tym jeden przepis dwukrotnie[53]. W uzasadnieniu do swojego wniosku Rzecznik napisał, że (…) *cele ustawy należy uznać za słuszne, a bezpieczeństwo publiczne, jako dobro prawne, może usprawiedliwiać ograniczenie przez ustawodawcę korzystania z wolności i praw człowieka i obywatela* (…). Rzecznik wielokrotnie podkreślał, że efektywność działania właściwych organów państwa w zakresie nie tylko reagowania na już zaistniałe zdarzenia, lecz także prewencja w przypadku zagrożeń, których wystąpienie może wyrządzić nieodwracalne straty

[50] Tamże, s. 265.

[51] http://krakow.wyborcza.pl/krakow/1,90279,18406297,dron-zrzucil-ladunek-na-baze-wojskowa-lotniska-w-balicach.html [dostęp: 24 IX 2017].

[52] http://www.polsatnews.pl/wiadomosc/2016-08-02/wydalono-obywatela-austrii-skorzystano-z-przepiso-w-ustawy-antyterrorystycznej/ [dostęp: 24 IX 2017].

[53] http://trybunal.gov.pl/sprawy-w-trybunale/art/9112-ustawa-antyterrorystyczna/ [dostęp: 24 IX 2017].

w odniesieniu do dóbr prawnie chronionych, są szczególnie istotne w warunkach globalizacji przestępczości. Przyznanie właściwych uprawnień służbom odpowiedzialnym za walkę z terroryzmem jest zatem konstytucyjnym obowiązkiem państwa wynikającym z art. 5 Konstytucji RP.

Odnosząc się do art. 2 pkt 7, czyli definicji zdarzenia o charakterze terrorystycznym, zaznaczono brak precyzji prawodawcy w kontekście tego przepisu, który w ocenie Rzecznika pozwala na szeroką interpretację. W tym kontekście należy stwierdzić, że częścią składową zasady przyzwoitej legislacji jest tzw. zasada dostatecznej określoności, z której można wyprowadzić chociażby nakaz stosowania norm jasnych, zrozumiałych dla adresatów. Trybunał Konstytucyjny w wyroku w sprawie P 13/02 z 3 grudnia 2002 r. wyraził pogląd, zgodnie z którym „poważne wątpliwości interpretacyjne" nie wystarczają do stwierdzenia niezgodności danego przepisu z Konstytucją RP. Trzeba zasygnalizować, że w przypadku niejasności przepisu musi się ona łączyć z dodatkowymi okolicznościami powodującymi rozbieżności interpretacyjne, których nie dałoby się usunąć przez zastosowanie zwyczajnych środków mających na celu wyeliminowanie niejednolitości w stosowaniu prawa. Dotychczas nie stwierdzono rozbieżności interpretacyjnych w tym zakresie, stąd też wskazane przez Rzecznika argumenty nie wydają się zasadne.

Następnie zakwestionowano przepis art. 6 ust. 1 dotyczący uprawnienia szefa ABW do prowadzenia wykazu osób, które mogły mieć związek ze zdarzeniem terrorystycznym. Ze względu na posłużenie się w tym przepisie definicją zdarzenia o charakterze terrorystycznym oraz ze względu na to, że zawiera ona pominięcia ustawodawcze w postaci braku procedur umożliwiających kontrolę zasadności zamieszczenia danej osoby w wykazie, Rzecznik uznał, iż jest on w całości niezgodny z przepisami Konstytucji RP. W przypadku art. 6 ust. 3 dotyczącego delegacji do wydania przez szefa ABW zarządzenia, w którym zostanie uregulowany zakres informacji gromadzonych w wykazie, o którym mowa w ust. l, sposób prowadzenia tego wykazu, a także tryb przekazywania podmiotom oraz służbom specjalnym informacji z tego wykazu, wskazał on, że zarządzenie nie może stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów. W tym aspekcie można zwrócić uwagę na podstawową funkcję tego przepisu, która jest wyrażona w potrzebie integracji przepisów odnoszących się do terroryzmu. Dotychczasowy stan prawny ukształtował się w taki sposób, że wiele z regulacji dotyczących problematyki terrorystycznej była rozproszona w różnych rodzajowo ustawach i aktach prawnych rangi podstawowej. Z tego względu organy zobowiązane do realizacji poszczególnych obowiązków dysponowały jedynie niepełnymi danymi. Ponadto problem niedostatecznej spójności baz danych podniesiono w dokumencie pn. *Stronger and Smarter Information Systems for Borders and Security*, który Komisja Europejska przedstawiła Parlamentowi Europejskiemu oraz Radzie Unii Europejskiej[54]. Zwrócono w nim uwagę na tzw. martwe punkty, które mogą powodować ograniczenie możliwości skutecznego działania organów mających uprawnienia dochodzeniowo-śledcze. W kontekście zarządzenia należy odnotować, że adresatem norm zawartych w tym przepisie są wyłącznie jednostki organizacyjne podległe szefowi ABW. Zarządzenie nie stanowi również samodzielnej podstawy prawnej do podejmowania jakichkolwiek działań wobec osoby, jeżeli jej dane znalazły się w wykazie. Ponadto ABW przed wejściem w życie ustawy AT miała (i nadal ma) uprawnienie do zbierania wszelkich danych osobowych, zwłaszcza jeżeli jest to uzasadnione charakterem realizowanych zadań (art. 34 ustawy o ABW oraz AW).

[54]http://www.eulisa.europa.eu/Newsroom/News/Documents/SB-EES/communication_on_stronger_and_smart_borders_20160406_en.pdf [dostęp: 25 IX 2017]; w piśmie nr COM(2016)205 final.

Zaskarżony został również przepis art. 9 ust. l ustawy AT, który przewiduje możliwość niejawnego prowadzenia czynności wobec osoby niebędącej obywatelem Rzeczpospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej. Mechanizmy przewidziane w zaskarżonym art. 9 ust. l ustawy AT w pierwszej kolejności budzą wątpliwości Rzecznika ze względu na brak jakiejkolwiek – zarówno uprzedniej, jak i następczej – kontroli sądu bądź innego niezależnego organu. Ponadto podziela on stanowisko, że niejawne pozyskiwanie informacji może stanowić środek skuteczny i zarazem konieczny do zwalczania masowych niebezpieczeństw, a zwłaszcza do zwalczania szczególnie niebezpiecznej działalności terrorystycznej. Odnosząc się do tego zagadnienia, należy wskazać, co już wcześniej uczyniono, że przepis zawiera mechanizm kontroli następczej, sprawowanej przez prokuratora generalnego (art. 9 ust. 4 ustawy AT). *Last but not least* nie jest to *novum* w polskim systemie prawnym, tego typu procedura występuje bowiem w przypadku „przesyłki niejawnie nadzorowanej" (art. 30 ustawy o ABW oraz AW). Zarzut ukształtowany w ten sposób wydaje się niezasadny z punktu widzenia zdania wyrażonego przez Rzecznika, że te przepisy są pozbawione kontroli ze strony organu zewnętrznego.

W art. 10 ust. l ustawy AT uregulowano przesłanki uzasadniające dopuszczalność pobierania danych biometrycznych. Rzecznik wskazał, że ten przepis odwołuje się do ogólnych i nieprecyzyjnych pojęć: istnienie podejrzenia oraz istnienie wątpliwości. Zwrócił on także uwagę na inne nieprecyzyjne pojęcia zawarte w dalszych przepisach art. 10. Rzecznik dodał, że w krajowym systemie prawnym istnieją przepisy pozwalające na pobieranie danych biometrycznych i uznał, że przepis, o którym mowa, nie spełnia kryterium niezbędności w demokratycznym państwie prawnym.

Na płaszczyźnie art. 11 ustawy AT, który upoważnia szefa ABW do nieodpłatnego dostępu do danych i informacji zgromadzonych w rejestrach publicznych oraz ewidencjach prowadzonych przez podmioty wymienione w tym przepisie, argumentacja była podobna, jak w przypadku art. 10. Zwrócono również uwagę na nieostre pojęcia rejestry publiczne, ewidencje, bazy danych, systemy informacyjne itd. Ogólnie rzecz ujmując, w ocenie Rzecznika szef ABW otrzymał zbyt szeroki dostęp do rejestrów przez (…) *żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce*. Dodano także, że przepis art. 11 nie daje gwarancji, że przepis będzie stosowany tylko wówczas, gdy będzie to konieczne do realizacji celów określonych w ustawie AT. Jak już wcześniej wskazano, zaburzenia w procesie przepływu informacji najważniejszych dla bezpieczeństwa państwa mogą uniemożliwić prowadzenie efektywnych czynności zapobiegawczych. Skoro powierzono szefowi ABW rolę koordynacyjną, powinien on mieć możliwość realnego wykonywania zadań przez weryfikację gromadzonych informacji. Warto odnieść się w tej materii prawnej do wyroku Trybunału Konstytucyjnego w sprawie K 54/07 z 23 czerwca 2009 r., w którym dokonano oceny konstytucyjności niektórych przepisów ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2016 r. poz. 1310, ze. zm. – art. 22), w zakresie dostępu do danych zawartych w rejestrach publicznych i ewidencjach. Niniejsze przepisy zostały uznane za zgodne z Konstytucją RP.

Kolejno, przewidziana w zaskarżonym przepisie art. 26 ust. 2 ustawy AT możliwość stosowania tymczasowego aresztowania na podstawie jedynie uprawdopodobnienia popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym w ocenie Rzecznika pozostaje w sprzeczności z fundamentalnymi zasadami demokratycznego państwa prawnego. Argumentując, wskazano, że przepis

narusza: zasadę zaufania obywateli do państwa, zasadę dostatecznej określoności i zasadę poprawnej legislacji. W art. 38 pkt 6 ustawy AT wprowadza się zmiany w ustawie o ABW oraz AW polegające m.in. na dodaniu art. 32c dopuszczającego blokadę dostępności w systemie teleinformatycznym danych informatycznych, które mają związek ze zdarzeniem terrorystycznym, lub usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. Podobnie jak uprzednio, podniesiono, że przepis posługuje się niedookreślonymi pojęciami, np. dane informatyczne. Jednocześnie wskazano, że zarządzenie blokady może nie przynieść rezultatu z powodu korzystania przez organizacje terrorystyczne z tzw. darknetu. Według Rzecznika o możliwym braku efektywności przyjętych rozwiązań świadczy to, że najbardziej popularne serwisy internetowe są prowadzone za granicą, a zatem przepisy ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2017 r. poz. 1219) nie będą miały do nich zastosowania. Podsumowując, wskazał on, że (…) *ze względu na zbyt ogólny sposób sformułowania przesłanek, nieprecyzyjne określenie zakresu oraz procedurę, która nie zapewnia wystarczających gwarancji powoduje, że przepis ten stwarza ryzyko arbitralnego korzystania z tego narzędzia przez organy państwa*. Zarzut dotyczy tego, że zaskarżony przepis posługuje się określeniami, które nie mają definicji legalnej i w związku z tym będą powodować trudności z ich interpretacją, np. pojęcia dane informatyczne lub zdarzenie o charakterze terrorystycznym. W odniesieniu do powyższego należy zwrócić uwagę, że pojęcie dane informatyczne jest stosowane w polskim systemie prawnym. Występuje np. w kk (art. 165 § 1 pkt 4 – definicja przestępstwa sprowadzenia niebezpieczeństwa dla życia i zdrowia wielu osób oraz mienia w wielkich rozmiarach) i kpk (art. 143 § 1 pkt 6 – spisanie protokołu z zatrzymania danych informatycznych).

Z kolei na mocy art. 57 ustawy AT, jak już wcześniej wskazano, dodano art. 329a w ustawie o cudzoziemcach. Zgodnie z tym przepisem minister właściwy do spraw wewnętrznych, na wniosek komendanta głównego Policji, szefa ABW albo szefa SKW wydaje decyzję o zobowiązaniu do powrotu cudzoziemca, co do którego istnieje obawa, że może prowadzić działalność terrorystyczną lub szpiegowską albo podejrzewanego o popełnienie jednego z tych przestępstw. Zdaniem Rzecznika, skoro ten przepis nie przewiduje żadnych gwarancji dla wydalanego czy deportowanego cudzoziemca i dopuszcza możliwość złożenia skargi do sądu wyłącznie spoza granic Polski, uniemożliwiając tym samym dostęp do akt (które w praktyce zostaną utajnione), a tym samym uniemożliwiając skuteczną obronę, ograniczenie to nie ma charakteru proporcjonalnego i nie jest niezbędne w demokratycznym państwie prawnym (podobne argumenty przedstawiono w przypadku art. 73c ustawy z 14 lipca 2006 r. o wjeździe na terytorium Rzeczpospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin – Dz.U. z 2017 r. poz. 900). W ocenie autora powyższe przepisy dookreślają jednak podmioty, wobec których są stosowane ograniczenia i są one sformułowane w sposób dostatecznie jasny i precyzyjny, co ma służyć ich jednolitemu stosowaniu, jak też obejmują wyłącznie sytuacje, w których racjonalny ustawodawca zamierzał wprowadzić regulację ograniczającą korzystanie z wolności i praw konstytucyjnych. Ponadto dopuszczalność pojęcia lub zwrotu niedookreślonego zależy również od funkcji, jaką pełni dane pojęcie lub zwrot na tle danego przepisu lub aktu prawnego (wyrok TK w sprawie KP 1/09 z 13 października 2010 r.). W orzecznictwie TK wskazywano nawet, że nie każda ustawa zawierająca błędne rozwiązania prawne niepozwalające na osiągnięcie zamierzonego celu, wychodząca z wadliwych założeń

czy ocen ekonomicznych i społecznych, jest niezgodna z Konstytucją RP. W ramach swobody ustawodawcy pozostaje nawet podjęcie rozwiązań dysfunkcjonalnych, chyba że ich konstrukcja jest tak błędna, że można przewidzieć ich całkowitą nieprzydatność do realizacji założonych celów (pogląd wyrażony w wyroku TK w sprawie K 18/95 z 9 stycznia 1996 r.). Odnosząc się do powyższych twierdzeń, należy wskazać, że w związku z wprowadzeniem art. 72c do ustawy o wjeździe oraz art. 329a do ustawy o cudzoziemcach, decyzję o wydaleniu osoby będzie podejmował minister spraw wewnętrznych i administracji na wniosek komendanta głównego Policji, szefa Agencji Bezpieczeństwa Wewnętrznego albo szefa Służby Kontrwywiadu Wojskowego. Ustawodawca celowo powierzył kompetencje w tym szczególnym trybie organowi wyższego stopnia niż wojewoda, który jest właściwy do podjęcia takiej decyzji w pozostałych przypadkach. Należy również pamiętać, że cudzoziemiec, w stosunku do którego jest podejmowana decyzja, może skorzystać z możliwości zaskarżenia decyzji I instancji, a następnie wniesienia skargi do sądu administracyjnego (dokonywanego również spoza terytorium RP przez pełnomocnika procesowego w kraju). Co istotne, analogiczne rozwiązanie obowiązywało również w stanie prawnym przed wejściem w życie ustawy AT, ponieważ zgodnie z art. 72 ust. 2 ustawy o wjeździe w sytuacji, gdy podstawą wydalenia jest działalność terrorystyczna, nie stosowało się art. 72 ust. 1 tej ustawy, według którego wniesienie skargi do sądu administracyjnego na decyzję o wydaleniu, wraz z wnioskiem o wstrzymanie jej wykonania, przedłuża termin wykonania nakazu opuszczenia terytorium Rzeczpospolitej Polskiej do dnia, w którym postanowienie w sprawie tego wniosku stało się prawomocne (Rzecznik jednak nie zdecydował się na zaskarżenie powyższego przepisu).

Kończąc uzasadnienie swojego wniosku do Trybunału Konstytucyjnego, Rzecznik zwrócił uwagę na to, że:

> Zwalczanie terroryzmu i prawidłowe rozpoznawanie zagrożenia terrorystycznego niewątpliwie stanowi istotne zadanie państwa, którego obowiązkiem jest stanie na straży bezpieczeństwa osób pozostających w jego jurysdykcji. Wobec tego pozytywnie należy ocenić podjęcie inicjatywy ustawodawczej w tym obszarze. Jednak wszelkie środki prawne służące do osiągnięcia tego celu muszą być proporcjonalne i ingerować w prawa człowieka jedynie wówczas i jedynie w takim zakresie, jaki jest niezbędnie konieczny i niezbędny. Regulacje ustawy o działaniach antyterrorystycznych w wielu miejscach budzą istotne wątpliwości co do ich zgodności ze standardem konstytucyjnym oraz wynikającym z EKPCz i KPP UE.

5. Podsumowanie

Terroryzm to zjawisko istotne przede wszystkim jakościowo, a nie ilościowo. Jeden atak terrorystyczny może spowodować zagrożenie kilku, a nawet kilku tysięcy ludzi (przykładem – ataki w Nowym Jorku). Nie zawsze obraz statystyczny może dać wymierną informację na temat działalności służb. Autor niniejszego artykułu jest zdania, że może być wręcz przeciwnie. Można przecież założyć, że skoro mamy w Polsce przykładowo 1000 przestępstw przeciwko mieniu, a 1 przestępstwo przeciwko środowisku, to polityka prewencyjna kreowana przez kierownictwo np. Policji powinna być w 100 proc. ukierunkowana na zwalczanie przestępstw przeciwko mieniu. Nie budziłoby to przecież większych wątpliwości ze strony mediów i społeczności. Problem jednak w tym, że to

jedno przestępstwo przeciwko środowisku mogłoby doprowadzić do zatrucia np. rzeki, z której zaopatrywane jest średniej wielkości miasto. Choć trudno to ocenić, ale można przypuszczać, że więcej będzie ofiar tego jednego przestępstwa przeciwko środowisku niż wspomnianego już tysiąca przestępstw przeciwko mieniu. Podobnie rzecz się ma z terroryzmem, zwłaszcza w zamiarach terrorystów leży wykorzystanie czynników biologicznych, chemicznych, radioaktywnych bądź nuklearnych[55].

Z pewnością Polska, jako jeden z krajów potencjalnie zagrożonych terroryzmem, powinna mieć właściwe możliwości instytucjonalne do rozpoznawania terroryzmu i zapobiegania temu zjawisku. W ocenie autora wypracowanie wysokich standardów pracy służb, szczególnie w ramach współpracy między nimi, daje nadzieję (podstawy) na zminimalizowanie możliwości wystąpienia zdarzenia o charakterze terrorystycznym na terenie Rzeczpospolitej Polskiej. Zasygnalizowana potrzeba zwrócenia uwagi na przestępstwa jakościowo istotne, takie jak terroryzm, ma na celu podkreślenie potencjalnych skutków tych przestępstw i potrzeby dobierania adekwatnych sił i środków do ich rozpoznawania oraz ścigania. Osiągnięcie takich celów wymaga współpracy z organami na szczeblu lokalnym, regionalnym i krajowym, takie właśnie działania mogą bowiem spowodować, że szeroko rozumiane działania prewencyjne będą miały swój pozytywny skutek w postaci zapobieżenia powstaniu zagrożenia terrorystycznego.

Rozważając powyższe, nie należy zapominać, że nawet najlepsza współpraca nie zapewni odpowiedniego efektu, jeśli nie będzie wsparta odpowiednim zapleczem informacyjnym i szybkim reagowaniem w przypadku uzyskania informacji o zagrożeniu. Te obszary wymagają praktyki, opracowania algorytmów postępowania, stworzenia podstaw prawnych modelu wymiany informacji, który zapewniałby wysoki standard działania służb. Tymi właśnie postulatami kierował się prawodawca, który w jednym akcie prawnym rangi ustawowej rozstrzygnął, które z organów oraz w jakim zakresie są obowiązane do zapobiegania zdarzeniom o charakterze terrorystycznym i reagowania na nie. Wiceminister spraw wewnętrznych i administracji w jednym z wywiadów podkreślił, że (…) *wprowadzone ustawą antyterrorystyczną instrumenty koordynacyjne, w tym odnoszące się do prowadzenia operacji kontrterrorystycznych, zostały wykorzystane w trakcie zabezpieczenia Światowych Dni Młodzieży oraz Szczytu NATO, i to wykorzystane w sposób bardzo skuteczny*[56]. Ustawa AT miała na celu ograniczenie możliwości wystąpienia ataków terrorystycznych podczas wymienionych wydarzeń. Należy przypomnieć, że zgodnie z *European Union Terrorism Situation and Trend Report (TE-SAT) 2016* w 2015 r. w państwach członkowskich Unii Europejskiej odnotowano 211 zamachów terrorystycznych, wobec 201 w 2014 r. Pociągnęły one za sobą 151 ofiar śmiertelnych[57].

Należy także spojrzeć przez pryzmat podstawowych, konstytucyjnych praw i wolności bywateli i ważyć dobro tych praw w stosunku do potrzeb służb. Nie ulega bowiem wątpliwości, że każde działanie służb powinno być realizowane na podstawie i w granicach prawa. Prawodawca, uchwalając ustawę o działaniach antyterrorystycznych, miał trudne zadanie – z jednej strony zachowania wysokiego poziomu bezpieczeństwa obywateli, a z drugiej zapewnienia wolności i praw, które są podstawą demo-

[55] M.A. Wasilewska, *Terroryzm CBRN a terroryzm biologiczny. Współczesne zagrożenie*, w: *Oblicza współczesnego terroryzmu*, W. Wróblewski (red.), Toruń 2006, s. 195 i in.

[56] http://www.pap.pl/aktualnosci/news,1017974,wiceminister-zielinski-niski-poziom-zagrozenia-terrorystycznego-w-polsce.html[dostęp: 24 IX 2017].

[57] https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_2016.pdf [dostęp: 23 IX 2017].

kratycznego państwa prawa. W. Zubrzycki twierdzi, że stanowiska różnych środowisk dotyczące celowości wprowadzania takiej ustawy są podzielone. Jedne popierają jednorodny akt prawny, inne opowiadają się za nowelizacją obowiązujących, rozproszonych przepisów, a jeszcze inne twierdzą, że dotychczasowe uregulowania były w Polsce wystarczające[58]. Zwracaon uwagę na jeszcze jeden istotny aspekt: podkreśla, że służby muszą się doskonalić i że należy podnosić efektywność ich działania, tak aby mogły należycie wykonywać swoje obowiązki. Należy zwrócić uwagę na opinie A. Tyburskiej i B. Jewartowskiego, którzy wskazują, że:

> (…) w sytuacji współczesnych, hybrydowych zagrożeń, niemożliwe jest funkcjonowanie demokratycznego państwa prawa bez rezygnacji z określonych praw i wolności na rzecz zwiększenia bezpieczeństwa. Każda sytuacja związana z tego typu ograniczeniami musi być jednak traktowana indywidualnie. Rolą administracji rządowej jest w tym przypadku wypracowanie i wdrożenie mechanizmów gwarantujących wykorzystanie uprawnień nadanych ustawą tylko w celach przeciwdziałania terroryzmowi[59].

W ocenie autora takie właśnie przesłanki były podstawą do stworzenia nowej regulacji prawnej. Obecnie jest jeszcze za wcześnie, aby kompleksowo móc ocenić wymierne efekty, jakie ona przyniosła. Niemniej jednak podstawowe wyzwanie i jednocześnie cel w postaci zapobiegania atakom terrorystycznym są realizowane, a najbardziej wymiernym efektem tego jest brak ataków terrorystycznych w Polsce.

[58] W. Zubrzycki, *Dzieje ustawy antyterrorystycznej w Polsce*…, s. 259.

[59] A. Tyburska, B. Jewartowski, *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu*…, s. 267.

Piotr Burczaniuk

Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw

1. Wstęp

O przestępstwie szpiegostwa, jego zakresach definicyjnych, rysie historycznym, rozwiązaniach przyjmowanych w zbliżonych nam systemach prawnych, napisano dużo z punktu widzenia pragmatyki prawniczej, oraz niewiele, biorąc pod uwagę analizę faktyczną spraw problemowych pojawiających się w toku pracy służb upoważnionych do rozpoznawania i zwalczania tego typu zagrożeń. Co więcej – praktyczne problemy pojawiające się w toku działalności służb nie przekładają się na prowadzenie bieżącej dyskusji na temat potrzeby zmian legislacyjnych w tym zakresie. Celem niniejszego materiału jest pokazanie, dzięki analizie historii polskiego systemu prawnego, rozwiązań stosowanych w wybranych państwach świata oraz wykazanie rozbieżności doktryny co do interpretacji aktualnych rozwiązań spowodowanych codziennymi problemami praktycznymi związanymi ze stosowaniem normy prawnej wynikającej z art. 130 kodeksu karnego. Tym artykułem autor pragnie również wywołać dyskusję na temat wybranych aspektów problemowych tej regulacji, aby spowodować jej dostosowanie do zmieniających się zagrożeń bezpieczeństwa Rzeczpospolitej Polskiej, zwłaszcza zagrożeń o charakterze hybrydowym i asymetrycznym.

2. Analiza historyczna

Rok 1918, który przyniósł Polsce niepodległość, stanowił asumpt do prac nad nowym ukształtowaniem jednolitego systemu prawnego. Jego celem była nie tylko odpowiedź na wyzwania związane z terytorialnym zróżnicowaniem trzech systemów prawnych państw zaborczych, lecz także zmierzenie się z zagrożeniami i wyzwaniami stojącymi przed odradzającym się państwem polskim. Ta sytuacja miała szczególne znaczenie w sferze polityki prawno-karnej, która do 1918 r. była kształtowana na ziemiach Polskich trzema odrębnymi aktami normatywnymi – austriacką ustawą karną z 1852 r., niemieckim kodeksem karnym z 1871 r. i rosyjskim kodeksem karnym z 1903 r. W okresie międzywojennym szpiegostwo po raz pierwszy zostało uregulowane dopiero w *Rozporządzeniu Prezydenta Rzeczypospolitej z dnia 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciw Państwu* (Dz.U. z 1928 r. nr 18 poz. 160). Przedmiotowy akt prawny, normując przestępstwo szpiegostwa, oscylował wokół dwóch typów zachowań, tj. ujawnienia (art. 1) bądź zakomunikowania (art. 3 i 4) wiadomości, dokumentów lub przedmiotów, które należy zachować w tajemnicy przed rządem obcego państwa (lub osobie działającej w jego interesie). W tym zakresie działanie polegające na ujawnieniu było sformułowane w sposób następujący:

Kto umyślnie ujawnia innej osobie wiadomości, dokumenty lub inne przedmioty, które ze względu na dobro Państwa Polskiego należy zachować w tajemnicy przed rządem obcego państwa, ulega karze więzienia do lat pięciu (art. 1 § 1)

oraz w typie kwalifikowanym:

Jeśli sprawca, ujawnił wiadomość, dokument lub inny przedmiot, określony w § 1, obcemu rządowi lub osobie w jego interesie działającej, albo działał w zamiarze narażenia na niebezpieczeństwo wojskowej obrony Państwa lub jego sił zbrojnych, albo też z naruszeniem obowiązków urzędu publicznego lub służby publicznej, ulega karze ciężkiego wiezienia od lat pięciu do lat piętnastu (art. 1 § 3).

Z kolei działanie sprowadzające się do zakomunikowania uregulowano w następujący sposób:

Kto umyślnie i bezprawnie komunikuje obcemu rządowi lub osobie w jego interesie działającej jakiekolwiek wiadomości, dokumenty lub inne przedmioty, dotyczące wojskowej obrony Państwa lub jego sił zbrojnych – o ile czyn nie stanowi przestępstwa, przewidzianego w art. 1 (art. 3 § 1)

oraz:

Kto umyślnie i bezprawnie komunikuje obcemu rządowi lub osobie w jego interesie działającej jakiekolwiek wiadomości, dokumenty lub inne przedmioty, a w szczególności dotyczące stosunków politycznych, dyplomatycznych lub gospodarczych Państwa Polskiego, wiedząc o tem, że udzielone wiadomości, dokumenty lub inne przedmioty mogą być obcemu rządowi użyteczne na wypadek wojny przezeń prowadzonej lub w jego nieprzyjaznych dla Państwa Polskiego działaniach lub zamierzeniach, ulega karze więzienia do lat pięciu (art. 4 § 1).

W orzecznictwie powstałym na gruncie przytoczonych przepisów Sąd Najwyższy wskazywał, że :

(…) większość współczesnych ustawodawstw karnych, a w szczególności rozporządzenie Prezydenta Rzeczypospolitej z dnia 16 lutego 1928 r., hołduje zasadzie subjektywizmu, polegającej na nadaniu przy ocenie winy pierwszorzędnego znaczenia pytaniu, czego pragnął sprawca w przedsięwziętym działaniu i do czego dążył, przyczem subjektywizm ten ze szczególną mocą występuje tam, gdzie chodzi o przestępstwo, objęte pojęciem zdrady kraju, przewidując kary nie tylko za to, co zostało dokonane, lecz również i za to, co było zamierzone, a przeto w sprawach karnych o zdradę kraju nie tyle skutek działania, ile tendencja i zamiar sprawcy rozstrzygają o karalności czynu. Do zasadniczych znamion szpiegostwa, stanowiącego jedną z postaci zdrady kraju, nie należy rzeczywista owocność działania sprawcy, lecz dla ustalenia podmiotowych cech owej zbrodni wystarcza stwierdzenie umyślności czynów, utożsamiającej się ze świadomością ich znaczenia i ich możliwego skutku. Każde tedy działanie, uwidaczniające zamiar szkodzenia własnemu państwu, a wspomożenia obcego państwa, stanowi zdradę kraju, bez względu na realne tego działania następstwa, gdyż punkt ciężkości szpiegostwa leży nie w konkretnem dzia-

łaniu sprawcy, lecz w charakteryzującem jego postępowanie zamiarze, szkodliwym dla bezpieczeństwa zewnętrznego państwa. Okoliczność przeto, czy zakomunikowane wiadomości miały lub nie miały istotnego znaczenia, przyniosły lub nie przyniosły pożytku państwu obcemu, a szkodę Polsce, dotyczyły lub nie dotyczyły tajemnic państwowych, nie ma znaczenia dla istoty przestępstwa szpiegostwa[1].

Podobnie, w innej sprawie Sąd Najwyższy podkreślał, że :

(...) bez znaczenia jest, czy wiadomości mają charakter pozytywny lub negatywny, gdyż zarówno jedne jak i drugie mogą należeć do kategorji tych, które ze względu na dobro państwa należy zachować w tajemnicy[2].

Innym razem Sąd Najwyższy stwierdził, że:

(…) w § 4 ustawodawca, wprowadzając odpowiedzialność za szpiegostwo polityczne, dyplomatyczne i ekonomiczne, ukształtował stronę podmiotową czynu znów w odmienny sposób, nie tworząc, wzorem niektórych ustaw zagranicznych (np. angielskiej z 1916), żadnych objektywnych ograniczeń, lecz uzupełniając ogólną podstawę złego zamiaru ustaleniem świadomości, że udzielane informacje mogą być obcemu rządowi użyteczne na wypadek wojny przezeń prowadzonej lub w jego nieprzyjaznych dla Państwa Polskiego działaniach lub zamierzeniach[3].

Kolejnym aktem normatywnym poruszającym przedmiotową problematykę, było *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. Kodeks karny* (Dz.U. z 1932 r. nr 60 poz. 571), zgodnie z którym (art. 99):

Kto wchodzi w porozumienie z osobą działającą w interesie obcego państwa lub organizacji międzynarodowej w celu wywołania wojennych lub innych wrogich działań przeciw Państwu Polskiemu, podlega karze więzienia na czas nie krótszy od lat 10.

Opis znamion przedmiotowego czynu zabronionego odszedł od konstrukcji zawartej w art. 1–5 wspomnianego rozporządzenia Prezydenta Rzeczpospolitej z 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciw Państwu, koncentrując się nie na ujawnieniu lub zakomunikowaniu wiadomości, dokumentów lub innych przedmiotów, a samym fakcie wejścia w porozumienie z osobą działając w interesie obcego państwa oraz, co ciekawe – organizacji międzynarodowej, przeciw państwu polskiemu. Dla prawodawcy staje się więc istotna sama współpraca – „wejścia w porozumienie", bez konkretyzacji, na czym to porozumienie będzie polegało. Prawodawca dopuszczał więc otwarty katalog zarówno działań, jak i zaniechań sprawcy, mieszczący się w kategorii działalności w ramach porozumienia, np. działanie to mogło obejmować nie tylko samo przekazywanie informacji czy dokumentów, lecz także aktywne wykonywanie określonych zadań, pod kierunkiem bądź na rzecz (…) *osoby działającej w interesie obcego państwa lub organizacji międzynarodowej*. Co ciekawe – wobec takiej osoby lub organizacji międzynarodowej prawodawca nie

[1] Wyrok Sądu Najwyższego z 16 I 1931 r., II K 11401/30, LEX nr 410707.
[2] Wyrok Sądu Najwyższego z 14 V 1934 r., II K 464/34, LEX nr 388169.
[3] Wyrok Sądu Najwyższego z 9 XII 1930 r., II K 1403/30, LEX nr 406481.

dookreślił elementów konkretyzujących sposób bądź formę, w jakiej jej działanie następuje (np. w ramach obcego wywiadu lub obcej służby specjalnej), podkreślając jedynie, że jej działanie musi być nakierowane na (…) *wywołanie wojennych lub innych wrogich działań przeciw Państwu Polskiemu*.

Artykuł 17 § 1 *Rozporządzenia Prezydenta Rzeczypospolitej z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu Państwa* (Dz.U. z 1934 r. nr 94 poz. 851), określał: *Kto udziela pomocy w działalności wywiadowczej osobie, działającej w interesie rządu obcego państwa, podlega, jeżeli czyn nie stanowi pomocy do przestępstwa zagrożonego karą cięższą, karze więzienia do lat 5*. Opis znamion czynu zabronionego jest zbudowany analogicznie do opisu zawartego w art. 99 rozporządzenia Prezydenta Rzeczpospolitej z 11 lipca 1932 r. kodeks karny, z tą różnicą, że użyty tam zwrot „osoba działająca w interesie obcego państwa lub organizacji międzynarodowej" zostaje zastąpiony pojęciem d z i a ł a l n o ś ć w y w i a d o w c z a [prowadzona przez] o s o b ę, d z i a ł a j ą c ą w i n t e r e s i e r z ą d u o b c e g o p a ń s t w a. Popełnienie przestępstwa szpiegostwa nie jest związane z jakąś formą „wejścia w porozumienie", lecz zachodzi przez popełnienie czynu, który zostanie uznany za „działalność wywiadowczą". Przytaczając za Andrzejem Lebiedowiczem *differentia specifica* tejże definicji, w zestawieniu z innymi, późniejszymi, wskazywano na (…) *cel wywołania wojennych działań przeciw Państwu Polskiemu, a więc uwypuklenie ścisłego związku szpiegostwa z aspektem militarnym*[4].

Jak wskazał Sąd Najwyższy,

> Każde działanie, uwidoczniające zamiar szkodzenia własnemu Państwu, a wspomożenia obcego państwa stanowi przestępstwo szpiegostwa bez względu na realne tego działania następstwa, ustawa bowiem kładzie nacisk na stronę podmiotową działania oskarżonego, zmierzającego do wyświadczenia usługi obcemu państwu na szkodę własnego kraju[5].

Dekret Prezydenta Rzeczypospolitej z dnia 22 listopada 1938 r. o ochronie niektórych interesów Państwa (Dz.U. z 1938 r. nr 91 poz. 623) wprowadzał w art. 5–7 kategorię przestępstw przeciwko niezależności życia publicznego, w brzmieniu: (…) *obywatel polski, który w związku z działalnością polityczną w Państwie Polskim przyjmuje od osoby działającej w interesie obcego rządu dla siebie lub innej osoby korzyść majątkową albo jej obietnicę, bądź też korzyści takiej żąda, podlega karze więzienia* oraz *obywatel polski, który wchodzi w porozumienie z osobą działającą w interesie obcego rządu lub organizacji międzynarodowej w celu działania na szkodę Państwa Polskiego, podlega karze więzienia.*

Po drugiej wojnie światowej, w nowej rzeczywistości politycznej i ustrojowej, pierwszą regulacją poruszającą problematykę szpiegostwa, był tzw. mały kodeks karny, tj. *Dekret z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa* (Dz.U. z 1946 r. nr 30 poz. 192), w którym w art. 7 wskazano:

> Kto, działając na szkodę Państwa Polskiego, gromadzi lub przekazuje wiadomości, dokumenty lub inne przedmioty stanowiące tajemnicę państwową lub wojskową, podlega karze więzienia na czas nie krótszy od lat 5 lub dożywotnio albo karze śmierci.

[4] A. Lebiedowicz, *Istota szpiegostwa w polskim prawie karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2017, z. 2, s. 34.

[5] Wyrok Sądu Najwyższego z 8 IV 1935 r., III K 409/35, LEX nr 379867.

Przepis tego artykułu spotkał się z dużą krytyką doktryny prawa karnego, która zarzucała mu stypizowanie wyłącznie jednej formy działalności szpiegowskiej, tj. gromadzenia i przekazywania wiadomości. Ponadto przepis pomijał element współdziałania z wywiadem obcego państwa lub organizacji, przez co poddawano w zastanowienie, czy (…) *chroni on wyłącznie zewnętrzne, czy też wewnętrzne bezpieczeństwo państwa*[6]. Co więcej – znaczne problemy pojawiały się na tle kwantyfikatora w postaci „działania na szkodę Państwa Polskiego", nieprecyzyjnego i niejednoznacznego, dopuszczającego odmienne interpretacje.

Najistotniejszym aktem normatywnym w zakresie prawa karnego materialnego okresu PRL była *Ustawa z dnia 19 kwietnia 1969 r. – Kodeks karny* (Dz.U. z 1969 r. nr 13 poz. 94, ze zm.), który w art. 124 typizował przestępstwo szpiegostwa w następujący sposób:

> § 1. Kto bierze udział w obcym wywiadzie lub działając na rzecz tego wywiadu udziela mu wiadomości, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 lub karze śmierci, a jeżeli sprawca działalność tę organizował lub nią kierował – kara pozbawienia wolności nie może być niższa od lat 8.

Wskazany typ podstawowy przestępstwa był uzupełniony o typy kwalifikowane związane ze zbieraniem lub przechowywaniem wiadomości w celu ich udzielenia obcemu wywiadowi albo podejmowania się działalności na rzecz obcego wywiadu, zagrożony karą pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności, oraz o sytuację związaną z czynnym żalem, gdy sprawca zaniechał dalszej działalności i zawiadomił organ powołany do ścigania przestępstw o wszystkich istotnych okolicznościach popełnionego czynu. Jednocześnie w art. 125 wskazano, że w sytuacji, gdy sprawca przestępstwa szpiegostwa dobrowolnie zaniechał dalszej działalności i ujawnił wobec organu powołanego do ścigania przestępstw wszystkie istotne okoliczności popełnionego czynu, sąd zamiast kary przewidzianej w art. 124 § 1 wymierza karę pozbawienia wolności od roku do lat 10. Kształtując przedmiotową regulację, ustawodawca okresu PRL wyeliminował pojawiające się m.in. w doktrynie prawa francuskiego elementy związane z tajnością działania sprawcy przestępstwa szpiegostwa. Co więcej, ustawodawca nie skoncentrował się wyłącznie na elemencie przekazywania wiadomości, lecz dopuścił różne możliwe sposoby funkcjonowania szpiega związane z podejmowaniem czynności na rzecz obcego wywiadu czy braniem udziału w obcym wywiadzie, o czym szerzej poniżej. Za element czynu sprawcy uznano współdziałanie z wywiadem obcego państwa lub obcej organizacji. Omawiany przepis karny został zawarty w rozdziale XIX kodeksu karnego – *Przestępstwa przeciw podstawowym interesom politycznym i gospodarczym Polskiej Rzeczypospolitej Ludowej*. W tym rozdziale stypizowano, jako pierwsze z grupy w nim określonych, przestępstwo zdrady, nakierowane na obywatela polskiego,

> (…) który uczestniczy w działalności obcego państwa lub zagranicznej organizacji mającej na celu pozbawienie niepodległości, oderwanie części terytorium, obalenie przemocą ustroju lub osłabienie mocy obronnej Polskiej Rzeczypospolitej Ludowej albo działając na rzecz obcego wywiadu, godzi w podstawy bezpieczeństwa lub obronności Polskiej Rzeczypospolitej Ludowej, popełnia zdradę Ojczyzny i podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze śmierci.

[6] Por. T. Taras, *Przestępstwo szpiegostwa w świetle nowego kodeksu karnego z 1969 r.*, „Palestra" 1970, nr 14/3 (147), 7–24, s. 8.

To przestępstwo było uznawane za najcięższe i najniebezpieczniejsze przestępstwo skierowane przeciwko PRL. Na gruncie wykładni językowej odróżnienie przestępstwa zdrady w postaci czynu *obywatela polskiego, który działając na rzecz obcego wywiadu, godzi w podstawy bezpieczeństwa lub obronności* PRL od przestępstwa szpiegostwa było znacznie utrudnione. W doktrynie za kryteria różnicujące uznawano: motyw, elementy obiektywne i narodowość[7]. Należy zauważyć, że takiego przestępstwa brakuje w obecnym kodeksie (z wyjątkiem tzw. zdrady dyplomatycznej), a stanowi ono podstawę regulacyjną w systemach karnych m.in. Francji i Niemiec, w których szpiegostwo jest w dalszym ciągu de facto odmianą przestępstwa zdrady.

Sam przepis art. 124 kodeksu karnego dopuszczał sześć form działalności szpiegowskiej:

1) organizowanie działalności obcego wywiadu – podejmowanie czynów polegających na wejściu w porozumienie z obcym wywiadem, wyrażenie na to zgody, a następnie organizowanie siatki szpiegowskiej, w tym werbowanie osób (które będą brały udział w obcym wywiadzie) czy zakładanie kanałów łączności bądź uruchamianie mechanizmów niejawności działań,
2) kierowanie działalnością obcego wywiadu – czyny następujące wraz bądź po fazie organizowania, związane z bieżącym zarządzaniem daną siatką szpiegowską, zadaniowaniem i zlecaniem działań osobom biorącym udział w wywiadzie, odbieraniem i analizowaniem informacji,
3) branie udziału w obcym wywiadzie – przynależność do obcego wywiadu przez nawiązanie dowolnej formy porozumienia z tym wywiadem i podejmowanie działań, choćby mało istotnych, w postaci np. wykonywania zleconych zadań operacyjnych,
4) działanie na rzecz obcego wywiadu przez udzielania mu wiadomości – czyn wpisujący się w szeroką definicję brania udziału w obcym wywiadzie, jak się jednak wydaje niewymagającym wcześniejszego wejścia w porozumienie, a polegający jedynie na przekazywaniu (nawet jednorazowym) – co bardzo ważne – wszelkich wiadomości, nawet jawnych i publicznie dostępnych,
5) podejmowanie się działalności na rzecz obcego wywiadu – czyn polegający na wejściu sprawcy w porozumienie z obcym wywiadem, jednak niepodjęcie (jeszcze) żadnej aktywnej działalności szpiegowskiej, nie wchodząc w fazę „brania udziału w obcym wywiadzie",
6) zbieranie lub przechowywanie wiadomości w celu ich udzielenia obcemu wywiadowi; sprawca wszedł bądź jeszcze nie w porozumienie z obcym wywiadem, jednak skutek – przekazanie – jeszcze nie nastąpił.[8]

Kluczowe dla przedmiotowej regulacji są pojęcia: o b c y w y w i a d i w y w i a d.

> Przez „obcy wywiad" należy rozumieć wywiad obcego państwa lub obcej organizacji uprawiającej działalność wywiadowczą. Państwo obce to państwo nie będące Państwem Polskim. Państwo obce to nie tylko państwo wrogie czy nieprzyjacielskie, ale także państwo z Polską zaprzyjaźnione, a nawet sprzymierzone. (…) Pojęcie zatem „wywiadu obcego" jest pojęciem szerszym od pojęcia „wywiadu wrogiego" (…). Słowo „wywiad" zawiera w sobie dwa elementy ściśle ze sobą zespolone. Pierwszym elementem jest element osobowy, a więc zorganizowany zespół osób uprawiających działalność wywiadowczą, drugim zaś element rzeczowy, tj. sama działalność wywiadowcza[9].

[7] Szerzej zob. tamże, s. 15; *Kodeks karny z orzecznictwem*, Gdańsk 1996, s. 445.
[8] T. Taras, *Przestępstwo szpiegostwa w świetle*…, s. 13.
[9] Tamże, s. 11.

3. Szpiegostwo w kodeksie karnym z 1997 r.

W obecnie obowiązującej *Ustawie z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. z 2016 r. poz. 1137, ze zm.), który wszedł w życie 1 stycznia 1998 r., przestępstwo szpiegostwa zostało uregulowane w art. 130:

> § 1. Kto bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10.
>
> § 2. Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.
>
> § 3. Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
>
> § 4. Kto działalność obcego wywiadu organizuje lub nią kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności.

W uzasadnieniu do rządowego projektu ustawy – Kodeks karny podkreślono, że:

> (…) przepisy chroniące państwo są w nowym prawie karnym oparte na całkowicie odmiennych, w stosunku do dotychczasowych, założeniach. Prawo karne musi chronić państwo i jego konstytucyjny, a nie jedynie wybrany, związany z określoną ideologią, ustrój. Karane powinny być więc nie takie zachowania, które zmierzają do zmiany panującego ustroju (do tego w mniejszym lub większym stopniu zmierza każde ugrupowanie opozycyjne), lecz tylko takie zachowania, które taki cel chcą osiągnąć w drodze pozakonstytucyjnej przez stosowanie przemocy (…) W stosunku do określeń tradycyjnych zamachów na państwo takich, jak zdrada dyplomatyczna, szpiegostwo, nowy kodeks wprowadza bardziej precyzyjne określenia. Widać to szczególnie przy określeniu szpiegostwa. Nie każde udzielenie wiadomości obcemu wywiadowi musi być karane, a jedynie takie, którego przekazanie może wyrządzić szkodę Państwu Polskiemu. Określenie typu szpiegostwa przewidzianego w art. 124 k.k. z 1969 r. umożliwia bardzo szeroką interpretację, obejmującą także zachowania, które nie zasługują na karanie. Nowy kodeks przewiduje za zorganizowanie siatki szpiegowskiej lub kierowanie nią karę nie niższą niż 5 lat pozbawienia wolności albo karę 25 lat pozbawienia wolności (art. 130 §4 k.k.).

Jak pisze Piotr Kardas w komentarzu do kodeksu karnego:

> Przedmiot ochrony obowiązującego aktualnie art. 130 Kodeksu karnego stanowi generalnie bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej, a w szczególności te wszystkie elementy składające się na bezpieczeństwo zewnętrzne, których przekazanie obcym organizacjom wywiadowczym może prowadzić do zagrożenia bezpieczeństwa państwa. Formułując brzmienie art. 130 Kodeksu karnego ustawodawca założył, że dla wypełnienia znamion przestępstwa szpiegostwa niezbędne jest, aby wszelkie wymienione w nim formy zachowania sprawcy były zwrócone przeciwko Rzeczypospolitej Polskiej. Przedmiotem ochrony są więc zarówno tzw. podstawowe elementy bezpieczeństwa ze-

wnętrznego RP, takie jak niepodległość, integralność terytorialna, konstytucyjny ustrój, konstytucyjne organy, podstawy bezpieczeństwa i obronności, moc obronna, jak i wszelkie inne elementy bezpieczeństwa zewnętrznego, które mogą być przedmiotem zainteresowania obcego wywiadu, a których ujawnienie może wyrządzić szkodę Rzeczypospolitej Polskiej[10].

W aktualnie obowiązującym kodeksie karnym przestępstwo szpiegostwa uregulowano w sposób zbliżony do konstrukcji zawartej w art. 124 kk z 1969 r., z istotnymi jednak zróżnicowaniami wpływającymi na interpretację tego przepisu, o czym mowa poniżej.

Zgodnie z art. 130, przestępstwo szpiegostwa, może przybierać osiem taksatywnie wymienionych form:

1. Kierowanie działalnością obcego wywiadu – typ kwalifikowany przestępstwa określony w art. 130 § 4 przewidujący wyższą odpowiedzialność karną, sprowadzający się do zajmowania przez sprawcę w strukturze organizacyjnej wywiadu określonej pozycji bądź też wypełnianie funkcji, z którymi wiąże się wydawanie poleceń, zwłaszcza wobec osób organizujących działalność tego wywiadu.
2. Organizowanie działalności obcego wywiadu – podobnie jak kierowanie, typ kwalifikowany przestępstwa określony w art. 130 § 4 przewidujący wyższą odpowiedzialność karną.

> Organizowanie działalności obcego wywiadu oznacza wszelkie formy zachowania prowadzące do stworzenia organizacji szpiegowskiej. W szczególności może się ono przejawiać poprzez: tworzenie systemu powiązań informacyjnych między poszczególnymi osobami współpracującymi czy mającymi współpracować z wywiadem, wyznaczenie zadań poszczególnym współpracownikom, oznaczenie sposobów kontaktowania się, zaopatrywanie siatki szpiegowskiej w środki ułatwiające jej działalność, werbowanie nowych agentów, szkolenie agentów, dostarczanie im technicznych środków działalności, zbieranie informacji od agentów itp.[11]

„Organizowanie" w odróżnieniu od „kierowania" sprowadza się do działań w zakresie wprowadzania i bieżącego zarządzania planami szpiegowskimi, przygotowanymi przez inną osobę uznawaną za kierującą tą działalnością. Na tle powyższego można zauważyć, że pojęcia: kierowanie i organizowanie, na gruncie kodeksu karnego z 1997 r., są rozumiane przez doktrynę inaczej, niż tożsame pojęcia zawarte w kodeksie karnym z 1969 r. Obecnie bowiem pojęcie organizowanie zawiera w sobie de facto łączne rozumienie obu pojęć wypracowane na gruncie kodeksu z 1969 r., natomiast pojęcie kierowanie utożsamia w sobie działalność hierarchicznie wyższą, związaną z określoną funkcją w strukturze wywiadu;

3. Branie udziału w działalności obcego wywiadu przeciwko Rzeczpospolitej Polskiej – typ podstawowy przestępstwa określony w art. 130 § 1. Wobec brzmienia § 2, który alternatywnie ujmuje „branie udziału w obcym wywiadzie" oraz „działanie na jego rzecz", typ podstawowy przestępstwa szpiegostwa obejmuje czyny inne niż wypełniające znamiona „działania na jego rzecz". Według Piotra Kardasa

[10] P. Kardas, *Kodeks karny. Część szczególna*, t. 2, A. Zoll (red.), Kraków 1999, s. 82–83.
[11] P. Kardas, *Komentarz do art. 130 Kodeksu karnego*, LEX/el.

mieszczą się tu (…) *wszelkie postaci aktywnej współpracy z obcym wywiadem, polegającej na przynależności do struktur organizacyjnych wywiadu, z wyłączeniem: samego działania na rzecz tego wywiadu*[12]. Z kolei Andrzej Marek wskazuje, że pod pojęciem tym (…) *rozumie się wszelką formę współpracy, przede wszystkim przynależność do jego struktur organizacyjnych bez względu na pełnione funkcje (agenta, informatora, osoby opracowującej zbierane informacje itp.)*[13]. Stanisław Hoc stwierdza zaś: (…) *udział w obcym wywiadzie nie wymaga w zasadzie formalnego przystąpienia do niego, choć może być poprzedzony takim aktem. Istotna jest tu więź między obcym wywiadem a sprawcą, nawet wówczas, gdy nie zobowiązał się on do prowadzenia działalności szpiegowskiej*[14]. Co istotne – spenalizowane jest wyłącznie branie udziału w działalności obcego wywiadu, które jest skierowane przeciwko Rzeczpospolitej Polskiej. Takiego zastrzeżenia kodeks karny z 1969 r. nie przewidywał. Nie stanowi więc przestępstwa przynależność do struktury organizacyjnej obcego wywiadu, którego działalność nie jest skierowana przeciwko państwu polskiemu, np. państwu sojuszniczemu czy neutralnemu, przy czym sojusz ten powinien być stwierdzony na gruncie prawnym w umowie międzynarodowej, a nie stanowić wyłącznie wymiar polityczny. Wyjątkiem od opisanej sytuacji jest wynikająca z art. 138 kk zasada wzajemności, czyli gdy czyn zabroniony popełniono na szkodę państwa sojuszniczego, a państwo to zapewnia wzajemność.

4. Branie udziału w obcym wywiadzie i udzielanie temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej – typ kwalifikowany przestępstwa określony w art. 130 § 2. Znaczenie pojęcia b r a n i e u d z i a ł u jest tożsame z użytym w pkt 3, natomiast pojęcie w i a d o m o ś c i należy utożsamiać z dowolną formą przekazywania informacji obcemu wywiadowi, w tym również informacji jawnych i publicznie dostępnych, z tym jednak zastrzeżeniem, że ich przekazanie może wyrządzić szkodę RP. Tym samym w aktualnym kodeksie odchodzi się od definicji i interpretacji pojęcia w i a d o m o ś c i zbudowanej na gruncie Kodeksu karnego z 1969 r. Jak wskazuje Andrzej Marek,

> (…) nie chodzi więc o każdą wiadomość (informację) interesującą obcy wywiad, lecz o wiadomości tego rodzaju, gdy ich przekazanie obcemu wywiadowi stwarza realne zagrożenie interesów państwa polskiego. Będą to zatem wiadomości dotyczące bezpieczeństwa państwa, sił zbrojnych, ważnych interesów gospodarczych, tajemnic strategicznych, ekonomicznych, technicznych itp., przy czym warunkiem penalizacji nie jest, aby zostały one objęte klauzulą tajemnicy państwowej lub służbowej[15].

   Tym samym przekazanie obcemu wywiadowi informacji irrelewantnych z punktu widzenia interesów RP nie jest przestępstwem szpiegostwa. Samo udzielenie tych wiadomości może być jednorazowe bądź wielokrotne.

5. Działanie na rzecz obcego wywiadu i udzielanie temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej – typ kwa-

[12] P. Kardas, *Kodeks karny. Część*…, s. 86.
[13] A. Marek, *Komentarz do art. 130 Kodeksu karnego*, LEX/el.
[14] S. Hoc, *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Opole 2002, s. 62.
[15] A. Marek, *Komentarz do art. 130*…

lifikowany przestępstwa określony w art. 130 § 2. Jak wskazuje Piotr Kardas, *działanie na rzecz obcego wywiadu oznacza wszelkie formy aktywnej współpracy z obcym wywiadem, która nie przybiera jeszcze postaci funkcjonowania w jego strukturach organizacyjnych*[16]. Pojęcie w i a d o m o ś c i należy rozumieć w sposób wyjaśniony w pkt 4.

6. Wejście do systemu informatycznego w celu uzyskania wiadomości, których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej – typ uprzywilejowany przestępstwa określony w art. 130 § 3, przewidujący niższą odpowiedzialność karną. Czynności te można uznać za działania przygotowawcze do przestępstwa w typie podstawowym bądź kwalifikowanym. Brzmienie sformułowania „wchodzi do systemu informatycznego" zastępujące pierwotnie użyty zwrot „włącza się do sieci komputerowej" jest wynikiem nowelizacji z 18 marca 2004 r., będącej następstwem *Konwencji Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości* (CETS nr 185; Dz.U. z 2015 r. poz. 728), która weszła w życie 1 lipca 2004 r. To sformułowanie oznacza czynności dotarcia przez wykorzystanie systemów i sieci teleinformatycznych do danych cyfrowych zapisanych na nośnikach elektronicznych. Samo „dotarcie" może być dokonane przez osobę, której dostęp do systemu jest zalegalizowany (gdy osoba ma prawny dostęp do zasobów), lub osobę przełamującą zabezpieczenia fizyczne bądź systemowe w celu uzyskania takiego dostępu. Zdaniem Piotra Kardasa uzyskane wiadomości muszą mieć charakter informacji, których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej[17]. Odmiennego zdania jest Andrzej Marek, wskazując, że (…) *nie jest przy tym istotna motywacja, którą kieruje się sprawca: może on działać z motywów wrogich państwu polskiemu albo kierować się chęcią osiągnięcia korzyści majątkowej lub osobistej, albo innym motywem*[18].
7. Gromadzenie lub przechowywanie wiadomości, których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej – typ uprzywilejowany przestępstwa określony w art. 130 § 3 przewidujący niższą odpowiedzialność karną. Te czynności można uznać za działania przygotowawcze do przestępstwa w typie podstawowym bądź kwalifikowanym.

> Gromadzenie oznacza każdą czynność, w następstwie której sprawca uzyskuje wiadomości albo wchodzi w posiadanie dokumentu lub innego przedmiotu zawierającego dane, których przekazanie może wyrządzić szkodę RP (…). Przechowywanie polega na przetrzymywaniu w określonym miejscu przedmiotów, będących nośnikami wiadomości, do czasu zaistnienia możliwości przekazania ich obcemu wywiadowi[19].

Co do charakteru gromadzonych lub przechowywanych wiadomości zob. tezy pkt 6.

8. Zgłoszenie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczpospolitej Polskiej – typ uprzywilejowany przestępstwa określony w art. 130 § 3 przewidujący niższą odpowiedzialność karną. Te czynności można uznać za działania

[16] P. Kardas, *Kodeks karny. Część*…, s. 88.
[17] Tamże, s. 90, 96.
[18] A. Marek, *Komentarz do art. 130*…
[19] Piotr Kardas, *Kodeks karny. Część*…, s. 90.

przygotowawcze do przestępstwa w typie podstawowym bądź kwalifikowanym. Zgłoszenie gotowości realizuje się przez zakomunikowanie obcemu wywiadowi chęci działania na jego rzecz. Dla tego przestępstwa nie ma znaczenia reakcja, z jaką spotkało się w obcym wywiadzie (i czy w ogóle) owo „zakomunikowanie gotowości". Istotne jest jednak dotarcie komunikatu o gotowości do struktur obcego wywiadu lub reprezentującej go osoby[20]. Na gruncie kodeksu karnego z 1969 r. takie zgłoszenie gotowości było traktowane wyłącznie jako usiłowanie, zaistnienie zaś przestępstwa z art. 124 § 2 wymagało jej przyjęcia[21]. Należy również pamiętać, że zakomunikowanie gotowości działania na rzecz obcego wywiadu musi obejmować zamiar działania przeciwko Rzeczpospolitej Polskiej[22].

Dla znamion omawianego czynu zabronionego najważniejszymi pojęciami wymagającym analizy są: w y w i a d i o b c y w y w i a d. Oba pojęcia – występujące też na gruncie kodeksu karnego z 1969 r. – zarówno wówczas, jak i obecnie nie zostały doprecyzowane w drodze definicji legalnej. Słownik języka polskiego podaje, że (…) *wywiad to instytucja mająca na celu zbieranie tajnych informacji dotyczących wojskowości, polityki, gospodarki itp. obcych państw; zbieranie takich informacji; ludzie pracujący w tej instytucji*[23]. Na gruncie doktryny prawniczej co do zakresu definicyjnego pojęcia w y w i a d są prezentowane dwa odmienne poglądy. Po pierwsze, w szerokim ujęciu pod tym pojęciem rozumie się rodzaj działalności mającej na celu zbieranie i opracowywanie przez m.in. wyspecjalizowane służby wiadomości o innych państwach, aby móc je wykorzystywać we własnym interesie. Tadeusz Taras wskazuje, że (…) *słowo wywiad zawiera w sobie dwa elementy ściśle ze sobą zespolone. Pierwszym elementem jest element osobowy, a więc zorganizowany zespół osób uprawiających działalność wywiadowczą, drugim zaś element rzeczowy, tj. sama działalność wywiadowcza*[24]. Takie rozumienie wywiadu koncentruje się na przedmiocie działalności[25]. Z kolei, zgodnie z węższym rozumieniem tego terminu, pod pojęciem o b c y w y w i a d należy rozumieć: (…) *tajną służbę specjalną państwa obcego realizującą za pomocą swoistych form i metod zadania w zakresie zdobywania wiadomości dotyczących innych państw i opracowania ich dla organów własnego państwa*[26]. Zbliżoną definicję podaje Lech Gardocki, rozumiejąc pod tym terminem wyspecjalizowane służby, które zajmują się zbieraniem i opracowywaniem informacji uzyskiwanych w sposób tajny w celu ich wykorzystywania w działalności politycznej, gospodarczej lub wojskowej przez państwo lub organizację międzynarodową[27]. Ma to odróżniać tę formę działalności od m.in. działalności agencji prasowych oraz informacyjnych bądź ośrodków naukowych zbierających informacje z sposób jawny i otwarty. Wymienione wąskie rozumienie tego pojęcia jest następnie dość jednoznacznie przytaczane w doktrynie[28]. W ten sposób węższe rozumienie pojęcia w y w i a d, koncentrujące się po pierwsze na jego aspekcie podmiotowym, tj. określonej strukturze organizacyjnej tworzącej wy-

[20] A. Marek, *Komentarz do art. 130*…

[21] Por. uchwała Sądu Najwyższego z 12 XII 1973 r., OSNKW 1974, z. 3, poz. 37.

[22] P. Kardas, *Kodeks karny. Część*…, s. 91.

[23] *Słownik Języka Polskiego*, M. Szymczak (red.),Warszawa 1999.

[24] T. Taras, *Przestępstwo szpiegostwa w świetle*…, s. 11.

[25] Por. W, Kubala, *Sporne zagadnienia szpiegostwa*, ZNASW 1975, nr 10, s 83–84; J. Broniewski, *Szpiegostwo, wywiad paragrafy*, Warszawa 1974, s. 157–160.

[26] S. Hoc, *Przestępstwa przeciwko Rzeczypospolitej*…, s. 61.

[27] L. Gardocki, *Prawo karne*, Warszawa 2009, s. 221.

[28] A. Marek, *Komentarz do art. 130*…; N. Kłączyńska, *Komentarz do art. 130 Kodeksu karnego*, LEX/el; I. Zwoliński, *Komentarz do art. 130 Kodeksu karnego*, LEX/el.; M. Budyn-Kulik, *Komentarz aktualizowany do art. 130 Kodeksu karnego*, LEX/El.

wiad, po drugie – na wycinkowych aspektach tej działalności, jak polityka, ekonomia, obronność, i po trzecie – opierające się na elemencie tajności działania zostało praktycznie jednolicie przyjęte przez doktrynę prawniczą, co na każdym z tych pól doprowadza w działaniach służb zajmujących się rozpoznawaniem tego typu przestępstw do znacznych problemów praktycznych, o czym szerzej poniżej. Warto jednak zaznaczyć istnienie w doktrynie zdań odrębnych w tym zakresie. Bogusław Zając wskazuje, że

> (…) dbałość o suwerenność RP wymaga, by przez „obcy wywiad" w art. 130 nowego kodeksu karnego rozumieć nie tylko cudzoziemskie państwowe organa nazywane wywiadem, lecz także różnorodne ogniwa i służby ochronne, policyjne etc., które by na rzecz obcego państwa zajmowały się zbieraniem danych – bądź na polskim terytorium, bądź o nim i o jego mieszkańcach, lub po to, by móc użyć tych danych na szkodę polskich interesów, obywateli lub osób pod opieką państwa polskiego[29].

Ten sam autor podkreśla też, że:

> (…) należy sądzić, że faktyczne istnienie wywiadu pracującego dla terrorystów stanowi dostateczną przesłankę, by w kwestiach szpiegostwa zwrócić się do doktryny oraz do orzecznictwa o zrewidowanie utartego poglądu, że „wywiadem obcym", owym kontrahentem szpiega, może być tylko odpowiednia, ściśle ograniczona i dokładnie wskazana służba informacyjna obcego państwa, jako że działalność wywiadu jest immanentną cechą, *ex definitione* przysługującą tylko państwom[30].

Przedstawione tezy należy w pełni podzielić.

W odniesieniu do pojęcia o b c y użytego w kontekście wywiadu aktualne pozostają poglądy wypracowane przez doktrynę na gruncie kodeksu karnego z 1969 r. Należy dodać, że dotyczący szpiegostwa art. 130 (jako taki oznaczany przez redakcję większości wydawnictw kodeksu karnego) ani inne przepisy tego aktu normatywnego nie posługują się pojęciem s z p i e g o s t w o, które jest najważniejsze m.in. z punktu widzenia organów ochrony prawnej uprawnionych do rozpoznawania i zwalczania tego typu przestępstw. W tym kontekście art. 5 ust. 1 pkt 2 lit. a wyraźnie wskazuje, że do zadań Agencji Bezpieczeństwa Wewnętrznego należy rozpoznawanie, zapobieganie i wykrywanie przestępstw m.in. szpiegostwa[31]. Z kolei w sferze wojskowej *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. z 2016 r. poz. 1318, ze zm.), pomimo określenia właściwości SKW w art. 5 ust. 1 pkt 1, przez generalne odesłanie do rozdziału XVII kodeksu karnego (w tym do art. 130), w art. 27a kilkakrotnie posługuje się zwrotem „przestępstwo szpiegostwa". Na gruncie prawa karnego procesowego z tym pojęciem można się spotkać w art. 237 § 3 pkt 10 *Ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego* (Dz.U. z 2016 r. poz. 1749, ze zm.), wymieniającym katalog przestępstw, w których przypadku jest możliwe stosowanie kontroli i utrwalania treści rozmów telefonicznych. Również w art. 38 *Ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu* (Dz.U. z 2016 r. poz. 1575) mamy do czynienia z bezpośrednim odwołaniem do przestępstwa „szpiegostwa".

---

[29] B. Zając, *W masce lub bez*, „Rzeczpospolita" z dnia 21 lutego 2000 r.

[30] B. Zając, *Terroryzm zmusza do rewizji przepisów i poglądów* – Teza nr 1, Lex nr 31614/1.

[31] Pojęcie s z p i e g o s t w o pojawia się jeszcze w art. 22b ustawy, nadane przez przepisy zmieniające zawarte w ustawie z 10 VI 2016 r. o działaniach antyterrorystycznych.

4. Szpiegostwo w systemach prawnych wybranych państw

W kontekście przedstawionych powyżej rozważań istotną wartość ma przedstawienie rozwiązań legislacyjnych w zakresie prawnokarnej definicji szpiegostwa i jego ustawowych znamion, funkcjonujących w wybranych państwach świata. Szczegółowa analiza tych przepisów powinna być też pomocna z punktu widzenia zagrożeń o charakterze strategicznym tam występujących, powiązanych z prowadzoną wobec nich ofensywną działalnością wywiadowczą.

W pierwszej kolejności należy się odnieść do przykładu Francji i funkcjonującego tam kodeksu karnego regulującego zagadnienie szpiegostwa w sposób znacznie bardziej szczegółowy i wielokierunkowy, niż czynią to obecnie analogiczne przepisy polskiego kodeksu karnego. Po pierwsze, należy zaznaczyć, że francuskie przepisy karne uznają szpiegostwo za zdradę, wyraźnie wskazując, że czyny określone w art. od 411-2 do 411-11 stanowią zdradę, jeżeli są popełnione przez obywatela Francji lub żołnierza pełniącego służbę dla Francji, albo szpiegostwo – jeżeli są popełnione przez jakąkolwiek inną osobę. Obywatel francuski współdziałający z obcym państwem jest więc zdrajcą, szpiegiem zaś jest osoba, wykonująca de facto ten zawód, w interesie swojego państwa (państwa pochodzenia, w którym pełni służbę bądź dla którego pracuje). Takie rozróżnienie we wprowadzeniu ma istotny walor edukacyjny, naznaczający pejoratywnie osobę zdrajcy kraju, pozostawiający poza tą oceną działanie szpiega, który w domyśle służy swojemu krajowi. Charakterystycznym elementem francuskiego modelu jest szerokie ujęcie podmiotów, na których rzecz przekazywanie informacji jest uznawane za szpiegostwo. Poza organami obcych państw wyżej wymieniony przepis uwzględnia także podmioty niepubliczne, takie jak np. przedsiębiorstwa czy podmioty prywatne kontrolowane przez te państwa. Art. 411-4 powyższego aktu prawnego stanowi że:

> Udzielanie informacji wywiadowczych obcemu mocarstwu, przedsiębiorstwu, innemu zagranicznemu podmiotowi lub podmiotowi znajdującemu się pod kontrolą innego państwa lub jego agentów, w celu wywołania nieprzyjacielskich działań lub aktów agresji wobec Francji podlega karze pozbawienia wolności 30 lat i grzywnie w wysokości 450 000 euro.
>
> Tej samej karze podlega działanie polegające na dostarczaniu obcemu mocarstwu, przedsiębiorstwu lub innemu zagranicznemu podmiotowi lub podmiotowi znajdującemu się pod kontrolą innego państwa lub jego agentów środków pozwalających na wywołanie nieprzyjacielskich działań lub aktów agresji wobec Francji.

Podczas gdy przywołany przepis koncentruje się na działalności zmierzającej do wywołania nieprzyjacielskich działań lub aktów agresji, art. 411-5 penalizuje czyn polegający na prowadzeniu analogicznej działalności stanowiącej zagrożenie tzw. fundamentalnych interesów państwa, rozumianych jako (art. 410-1):

> (…) niepodległość, integralność terytorialna, bezpieczeństwo, republikańska forma instytucji, obronność, dyplomacja, ochrona obywateli Francji w kraju i za granicą, ochrona środowiska naturalnego oraz kluczowe elementy jego potencjału naukowego, gospodarczego i dziedzictwa kulturowego.

Zgodnie z art. 411-5

> (…) jeżeli działanie polegające na udzielaniu informacji wywiadowczych obcemu mocarstwu, przedsiębiorstwu, innemu zagranicznemu podmiotowi lub podmiotowi znajdującemu się pod kontrolą innego państwa lub jego agentów może zagrozić fundamentalnym interesom państwa, sprawca podlega karze 10 lat pozbawienia wolności lub 150 000 euro grzywny.

Dopełnieniem powyższych regulacji są przepisy art. 411-6 do 411-8 wchodzące w skład sekcji zatytułowanej *Dostarczanie informacji obcemu mocarstwu*:

> Art. 411-6 Dostarczanie lub udostępnianie obcemu mocarstwu, przedsiębiorstwu, podmiotowi zagranicznemu lub znajdującemu się pod kontrolą innego państwa lub jego agentów informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów, których wykorzystanie, rozpowszechnienie lub połączenie w całość stanowi zagrożenie dla fundamentalnych interesów państwa podlega karze 15 lat pozbawienia wolności i 225 000 euro grzywny. Art. 411-7 Pozyskiwanie informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów, których wykorzystanie, rozpowszechnienie lub połączenie w całość stanowi zagrożenie dla fundamentalnych interesów państwa podlega karze 10 lat pozbawienia wolności i 150 000 euro grzywny. Art. 411-8 Prowadzenie, na rachunek obcego mocarstwa, przedsiębiorstwa lub podmiotu zagranicznego lub znajdującego się pod kontrolą innego państwa lub jego agentów, działalności mającej na celu uzyskanie lub dostarczenie instrumentów, informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów, których wykorzystanie, rozpowszechnienie lub połączenie w całość stanowi zagrożenie dla fundamentalnych interesów państwa podlega karze 10 lat pozbawienia wolności lub 150 000 euro grzywny.

Jak wynika z powyższego, czynności sprawcze stypizowane w ramach przestępstwa szpiegostwa we Francji, obejmują:

1) udzielanie informacji wywiadowczych w celu wywołania nieprzyjacielskich działań lub aktów agresji wobec Francji, ze szczegółowym dookreśleniem podmiotów, które przez ustawodawcę są zaliczone to katalogu podmiotów zainteresowanych ich pozyskiwaniem, tj. obce mocarstwo, przedsiębiorstwo, inny zagraniczny podmiot lub podmiot znajdujący się pod kontrolą innego państwa, lub jego agentów. Wyraźnie widać, że francuski prawodawca dopuszcza szeroki krąg podmiotów, które mogą prowadzić tego rodzaju działalność wywiadowczą. W tym zakresie nie koncentruje się, jak czyni to m.in. polski ustawodawca, na pojęciu w y w i a d rozumianego wąsko, jako zależna od państwa hierarchiczna organizacja – służba specjalna. Zgodnie z francuskim kodeksem karnym w rzeczywistości każda działalność wywiadowcza prowadzona przez państwo (jego służbę) bądź też – co niezmiernie istotne – inny podmiot, np. gospodarczy, obcy wobec Francji, może być uznany za prowadzący tego typu działalność. Jak z tego wynika – podmiot ten nie musi mieć wyraźnej linii łączącej go z innym państwem, wystarczy by był „obcy", odrębny od Francji. Znamiona przedmiotowego czynu zabronionego mają wyraźnie określone znamię celu (podobnie jak art. 130 § 3 polskiego kk) wyrażone w działaniu sprawcy, nakierowanym na wywołanie nieprzyjacielskich działań lub aktów agresji wobec Francji;

2) udzielanie informacji wywiadowczych obcemu mocarstwu, przedsiębiorstwu, innemu zagranicznemu podmiotowi lub podmiotowi znajdującemu się pod kontrolą innego państwa lub jego agentów mogące zagrozić fundamentalnym interesom państwa, rozumianym jako niepodległość, integralność terytorialna, bezpieczeństwo, republikańska forma instytucji, obronność, dyplomacja, ochrona obywateli Francji w kraju i za granicą, ochrona środowiska naturalnego oraz kluczowe elementy jego potencjału naukowego, gospodarczego i dziedzictwa kulturowego. W odróżnieniu od czynu charakteryzującego działanie sprawcy, omówionego w pkt 1, nie mamy tu do czynienia z tzw. przestępstwem kierunkowym. Kryminalizacja zachowania dotyczy zachowań mogących zagrozić fundamentalnym interesom państwa. W odróżnieniu od polskiego prawodawcy, w odniesieniu do znamienia „przeciwko Rzeczpospolitej Polskiej", kodeks karny francuski dokładnie precyzuje katalog wartości (interesów) uznanych za fundamentalne;
3) dostarczanie lub udostępnianie obcemu mocarstwu, przedsiębiorstwu, podmiotowi zagranicznemu lub znajdującemu się pod kontrolą innego państwa, lub jego agentów informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów, których wykorzystanie, rozpowszechnienie lub połączenie w całość jest zagrożeniem fundamentalnych interesów państwa. Prawodawca konkretyzuje sposoby działalności wywiadowczej, uzupełniając wskazane w pkt 1 i 2 znamię w postaci udzielania informacji wywiadowczej o działania sprowadzające się do dostarczania lub udostępniania informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów. Co ciekawe – te informacje oraz przedmioty mogą być istotne wyłącznie w kontekście ich przetworzenia (połączenia), czyli pracy analitycznej. Szpiegostwo może się wiec sprowadzać np. do zdobycia materiałów powszechnie dostępnych i wykonania ich analizy, której wykorzystanie przez podmiot zewnętrzny wobec Francji godzi w fundamentalne interesy tego państwa. Realizacja znamienia czynu zabronionego tak naprawdę może się więc sprowadzić do wykorzystania indywidualnych umiejętności analitycznych danej osoby i przekazania ich wyniku ze szkodą dla Francji, w tym np. zewnętrznemu podmiotowi gospodarczemu, co zagrozi gospodarczym interesom Francji;
4) pozyskiwanie informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów, których wykorzystanie, rozpowszechnienie lub połączenie w całość jest zagrożeniem fundamentalnych interesów państwa, czyli przygotowanie do przestępstwa, o którym mowa w pkt 3;
5) prowadzenie działalności mającej na celu uzyskanie lub dostarczenie instrumentów, informacji, technologii, przedmiotów, dokumentów, zinformatyzowanych danych lub rejestrów na rachunek obcego mocarstwa, przedsiębiorstwa lub podmiotu zagranicznego, lub znajdującego się pod kontrolą innego państwa lub jego agentów.

W Republice Federalnej Niemiec penalizacja czynu szpiegostwa jest zawarta w przepisach rozdziału II niemieckiego kodeksu karnego, i – podobnie jak we Francji – została wpisana jako odmiana przestępstwa zdrady. Te przepisy są zawarte w sekcjach 93–99 niemieckiego kodeksu karnego. Sekcja 93 wprowadza definicję tajemnicy państwowej, sekcja 94 zaś typizuje przestępstwo zdrady sprowadzające się do ujawnienia tajemnicy państwowej zagranicznemu mocarstwu (lub jednemu z jego pośredników) lub do pozwolenia, aby tajemnica państwowa została ujawniona nieuprawnionej osobie bądź

została upubliczniona, aby spowodować szkodę Republice Federalnej Niemiec lub przynieść korzyść zagranicznemu mocarstwu – i w wyniku powyższego stwarza niebezpieczeństwo poważnej szkody dla zewnętrznego bezpieczeństwa Republiki Federalnej Niemiec. Sekcja 96 typizuje wprost przestępstwo szpiegostwa, wskazując, że jego głównym znamieniem jest uzyskanie tajemnicy państwowej, tj: (…) *ktokolwiek uzyskuje tajemnicę państwową w celu ujawnienia jej, podlega karze pozbawienia wolności od roku do 10 lat* oraz (…) *ktokolwiek uzyskuje tajemnicę państwową, która była w posiadaniu organu państwowego, za namową ujawniając ją, podlega karze wolności od 6 miesięcy do 5 lat. Usiłowanie jest karalne*. Sekcja 98 odnosi się do działania na rzecz zagranicznego mocarstwa. Skonkretyzowano tu szpiegostwo jako zdradę sprowadzającą się do działania w roli agenta tego mocarstwa (bazując na elemencie podmiotowym), wskazując:

> (…) ktokolwiek uczestniczy w działalności na rzecz zagranicznego mocarstwa, którego działania są wymierzone w kierunku przechwycenia komunikacji lub tajemnic państwowych lub; deklaruje na rzecz zagranicznego mocarstwa lub jego pośredników chęć oraz gotowość do uczestnictwa w takiej działalności, podlega karze pozbawienia wolności nieprzekraczającą 5 lat lub grzywny. W szczególnie poważnych przypadkach odpowiedzialność wynosi od roku do 10 lat.

Sekcja 99 natomiast konkretyzuje branie udziału w tego rodzaju zdradzieckiej wobec państwa działalności ujmując ją od strony przedmiotowej (istoty) tej działalności i podaje:

> (…) ktokolwiek uczestniczy w działalności wywiadowczej na rzecz służby wywiadowczej obcego państwa przeciwko Republice Federalnej Niemiec, która obejmuje: komunikację, przekazywanie informacji, obiektów lub wiedzy, lub deklaruje służbom wywiadowczym zagranicznego mocarstwa lub jednemu jego pośredników chęć oraz gotowość uczestnictwa w takiej działalności, podlega karze pozbawienia wolności nieprzekraczającej 5 lat lub karze grzywny.

W modelu niemieckim istotną rolę w kwalifikacji czynu jako przestępstwa szpiegostwa odgrywa uzyskanie dostępu do tajemnicy państwowej. W odróżnieniu do modelu francuskiego zakres podmiotowy nie obejmuje podmiotów prywatnych, a jedynie organy państwa (sekcja 96 ust. 2). Z kolei w sekcji 98 istotnym elementem jest penalizacja czynów osób pośrednio powiązanych z obcymi strukturami wywiadowczymi, w tym prowadzących działania obejmujące przechwytywanie komunikacji. Model niemiecki zawiera również definicję pojęcia d z i a ł a l n o ś ć w y w i a d o w c z a, określając ją jako komunikację, przekazywanie informacji, obiektów lub wiedzy, lub deklarację wobec służb wywiadowczych zagranicznego mocarstwa lub jednego z jego pośredników, a także chęci oraz gotowości uczestnictwa w takiej działalności.

Warto również przytoczyć rozwiązania legislacyjne przyjęte w Federacji Rosyjskiej, gdzie wprowadzono rozróżnienie na akt zdrady i akt szpiegostwa. Zgodnie z art. 275 z d r a d a polega na dokonaniu przez obywatela Federacji Rosyjskiej jednego z trzech następujących czynów: szpiegostwa, ujawnienia tajemnicy państwowej lub udzielenia jakiejkolwiek pomocy obcemu państwu, zagranicznej organizacji lub jej przedstawicielom w prowadzeniu wrogich działań mających na celu wyrządzenie szkody bezpieczeństwu zewnętrznemu Federacji Rosyjskiej. Charakterystycznym elementem

tego modelu jest ograniczenie potencjalnych negatywnych skutków wyżej wymienionej działalności do bezpieczeństwa zewnętrznego. Definicja szpiegostwa została skonstruowana natomiast w sposób uwzględniający, w głównej mierze, aspekt informacyjny – zbieranie i przekazywanie informacji zagranicznej organizacji wywiadowczej w sposób zagrażający bezpieczeństwu zewnętrznemu Federacji Rosyjskiej, jeżeli zostały popełnione przez obcokrajowca lub bezpaństwowca. Zasadniczą różnicą jest zatem wprowadzenie rozróżnienia między przestępstwami zdrady i szpiegostwa z uwagi na aspekt podmiotowy. Podobnie jak w modelu francuskim, zdrada może być popełniona tylko przez obywatela Federacji Rosyjskiej, podczas gdy szpiegostwo – przez obywatela innego państwa lub bezpaństwowca. W tym zakresie art. 275 rosyjskiego kodeksu karnego, typizujący przestępstwo zdrady, wskazuje że:

> Obywatel Federacji Rosyjskiej, który dopuścił się zdrady, czyli szpiegostwa, tj. ujawnienia obcemu państwu, organizacji międzynarodowej lub zagranicznej lub też ich przedstawicielstwom wiadomości, stanowiących tajemnicę państwową, do której dana osoba została upoważniona lub która stała się jej znana w wyniku pełnienia służby, pracy, odbywania nauki lub w innych przypadkach przewidzianych przez prawodawstwo Federacji Rosyjskiej lub też okazania pomocy finansowej, materialno-technicznej, konsultacji lub pomocy innego rodzaju obcemu państwu, organizacji międzynarodowej lub zagranicznej lub też ich przedstawicielstwom w działalności skierowanej przeciwko bezpieczeństwu Federacji Rosyjskiej, podlega karze pozbawienia wolności od 12 do 20 lat oraz grzywnie w wysokości do pięciu tysięcy rubli lub w wysokości zgromadzonego wynagrodzonego lub innego dochodu za okres do trzech lat lub bez grzywny i z ograniczeniem wolności do dwóch lat. Osoba, dopuściwszy się przestępstwa przewidzianego danym artykułem, a także artykułami 276 oraz 278 KK FR, jest zwolniona z odpowiedzialności karnej, jeśli dobrowolnie i we właściwym czasie powiadomi organy władzy lub jeśli w inny sposób zapobiega dalszemu działaniu na szkodę interesów Federacji Rosyjskiej i jeśli jej działania nie są obciążone znamionami innego rodzaju przestępstw.

Z kolei art. 275 określający przestępstwo szpiegostwa podaje:

> (…) przekazywanie, gromadzenie, kradzież, przechowywanie w celu przekazania obcemu państwu, zagranicznej organizacji lub jej przedstawicielom informacji stanowiącej tajemnicę państwową, a także przekazywanie lub przechowywanie innych informacji na polecenie zagranicznej służby wywiadowczej na szkodę bezpieczeństwa zewnętrznego Federacji Rosyjskiej, jeżeli czyny te zostały popełnione przez obcokrajowca lub bezpaństwowca – podlega karze pozbawienia wolności od 10 do 20 lat.

Innym rozwiązaniem w zakresie penalizacji czynu szpiegostwa są przepisy kodeksu karnego Stanów Zjednoczonych Ameryki, które są uregulowane w sposób całkowicie odmienny od rozwiązań europejskich. Te przepisy zawierają wysoce kazuistyczne ujęcie znamion przestępstwa szpiegostwa przez wskazanie bogatego katalogu ściśle dookreślającego zakres czynów kwalifikowanych jako szpiegostwo. Wadą powyższych rozwiązań ujętych w Kodeksie Stanów Zjednoczonych, w tytule 18 zatytułowanym *Przestępstwa i procedura karna*, w części I – *Przestępstwa*, rozdział 37 – *Szpiegostwo i cenzura*, § 793 (*Gromadzenie, przekazywanie lub utrata informacji dotyczących obrony*) jest możliwość szybkiej dezaktualizacji tego katalogu z uwagi na postęp technologiczny oraz

stale modyfikowane sposoby prowadzenia działalności wywiadowczej bądź też z uwagi na dokonanie czynu niemieszczącego się w wyżej wymienionym katalogu, a stanowiącego akt wypełniający znamiona szpiegostwa i wywołujący analogiczne skutki.

5. Wyzwania regulacyjne przestępstwa szpiegostwa w polskim prawie karnym

Sposób określenia znamion czynu zabronionego zawarty w art. 130 kodeksu karnego, w wielu wymiarach, co pokazała powyższa analiza, jest niezbyt fortunny, często niewystarczający, a przede wszystkim niejasny i mało precyzyjny. Sprzyja to odmiennym interpretacjom tego przestępstwa w doktrynie, co może doprowadzać, i doprowadza, do odmiennej kwalifikacji dokonywanych czynów. Uregulowania zawarte w art. 130 kk korespondują bezpośrednio z zagrożeniami bezpieczeństwa zewnętrznego RP występującymi w latach 90. XX w., bazującymi na wypracowanej jeszcze w okresie zimnej wojny koncepcji dwubiegunowości systemu międzynarodowego, opartego na dwóch przeciwstawnych sobie blokach państw. Z tej perspektywy zakres znamion czynu zabronionego ujętego w tym przepisie nie odpowiada na wyzwania współczesnych zagrożeń bezpieczeństwa zewnętrznego państwa, oscylujących wokół zagrożeń ujmowanych w zbiorczą nazwę zagrożeń asymetrycznych. Pod tym pojęciem należy rozumieć wykorzystywanie środków i technik walki (tzw. walka nie fair) w celu osiągnięcia założonych celów niekonwencjonalnych z punktu widzenia adresata, a także zagrożenia o charakterze hybrydowym nakierowane na destabilizację określonych terytorialnie regionów, państw bądź ich segmentów, w celu realizacji przez inne państwo, organizację bądź podmiot ponadpaństwowy (w tym też korporacje handlowe) własnych celów. Jak pokazują doświadczenia ostatnich miesięcy, adresatami tych działań nie są – jak w XX w. – państwo i jego przedstawiciele, lecz ściśle wyodrębnione segmenty, w tym przede wszystkim gospodarcze i finansowe, same zaś działania są prowadzone z wykorzystaniem nowoczesnych narzędzi i środków teleinformatycznych, często nakierowanych na krytyczną infrastrukturę państwa, jak energetyka, łączność czy transport.

Jak słusznie zauważa Fabiana Fetke,

> (…) w chwili obecnej, gdy minęła już ponad dekada obowiązywania art. 130 w nowej formule, zadać należy pytanie, czy ustawodawcy w rzeczywistości udało się nie tylko dostosować brzmienie przepisu do nowej rzeczywistości i zapotrzebowania społecznego wynikającego ze zmian ustrojowych i demokratyzacji życia ale przede wszystkim, czy aktualne ujęcie kodeksowe przestępstwa szpiegostwa zabezpiecza w sposób wystarczający interesy Rzeczpospolitej Polskiej i realnie chroni je przed działaniami obcych służb? Tym samym, czy w obecnym stanie prawnym, szeroko rozumiane organy ścigania dysponują instrumentami prawnymi, które pozwalają im nie tylko na efektywne rozpoznawanie, ale przede wszystkim na skuteczne ściganie i zwalczanie różnego rodzaju zagrożeń ze strony obcych służb specjalnych?
>
> W związku z pojawieniem się nowych zagrożeń o charakterze wywiadowczym, w szczególności zaś zauważalnej zmiany metod działania obcych służb specjalnych, a przede wszystkim odczuwalnego przewartościowania ich zainteresowań, obecna regulacja [art. 130 kk] wydaje się nie przystawać do współczesnych warunków funkcjonowania państwa polskiego. Aktualne ujęcie kodeksowe przestępstwa szpiegostwa zdaje się również nie zabezpieczać w wystarczający sposób interesów Rzeczpospolitej Polskiej i w rzeczywistości nie chroni ich w należyty sposób przed działaniami obcych służb[32].

[32] F. Fetke, *Szpiegostwo w polskim prawie karnym – czy istnieje potrzeba zmian legislacyjnych?,* „Przegląd Bezpieczeństwa Wewnętrznego” 2010, nr 3, s. 91.

Przechodząc do omawiania konkretnych zagadnień problemowych związanych z normą prawną zbudowaną w art. 130 kodeksu karnego, należy zacząć od omówienia zagadnienia problemowego, którego w przepisach tego kodeksu nie poruszono w ogóle, tj. klasycznego przestępstwa zdrady. Współcześnie w systemach karnych wielu państwa (patrz tezy z pkt 3) to przestępstwo stanowi podstawowy czyn zabroniony, najistotniejszy z punktu widzenia przestępstw godzących w bezpieczeństwo państwa. Podobna sytuacja istniała również na gruncie rozwiązań krajowych zarówno okresu dwudziestolecia międzywojennego, jak i PRL. W nowym kodeksie karnym zabrakło jednak przestępstwa odpowiadającego konstrukcji zawartej w art. 122 kk z 1969 r., co – jak uzasadniano – było podyktowane jego wyraźnie polityczną wykładnią i zastosowaniem w okresie PRL przez elementarne wykorzystywanie do walki z opozycją ustrojową tego okresu. W ten sposób aktualnie zostało spenalizowane wyłącznie zachowanie stanowiące przestępstwo zdrady dyplomatycznej z art. 129 kk (wzorowane na art. 106 kk z 1932 r.) penalizującym odpowiedzialność osoby, która jest upoważniona do występowania w imieniu Rzeczpospolitej Polskiej w stosunkach z rządem obcego państwa lub zagranicznej organizacji. Wydaje się, że systemowa eliminacja tego czynu zabronionego w polskim prawie karnym na tle współczesnych zagrożeń jest dyskusyjna. Ten bowiem rodzaj czynu zabronionego, co pokazują doświadczenia państw zachodnich, obejmowałby czynności sprawcze wpisujące się obecnie w elementy działań związanych z zagrożeniami asymetrycznymi bądź hybrydowymi. Prowadząc rozważania na ten temat, należy się podeprzeć rozwiązaniem francuskim, uznającym obywatela francuskiego prowadzącego m.in. działalność szpiegowską wprost za zdrajcę, natomiast obywatela innego państwa podejmującego tego typu działalność – za szpiega. W tym zakresie wyrażany przeze autora pogląd nie jest odosobniony.[33]

Przechodząc na grunt analizy samego przepisu art. 130 kk, należy wskazać, że jednym z podstawowych problemów związanych z określeniem przez ten artykuł znamion czynu zabronionego jest odwołanie się w jego podstawowej formie wyłącznie do „brania udziału w działalności obcego wywiadu". Jak opisano w tezach pkt 2, prawodawca, tworząc analizowany przepis, nie nawiązał do poprzednich regulacji, w tym zwłaszcza kodeksu karnego z 1932 r. koncentrującego się na „wejściu w porozumienie" (aspekt formalny – element osobowy) oraz kodeksu karnego z 1969 r. rozdzielającego udział w obcym wywiadzie (aspekt formalny – element osobowy) od działań na jego rzecz[34] (aspekt materialny – element rzeczowy). Wprowadził natomiast opis znamion w postaci „udziału w działalności obcego wywiadu (materialno-formalny; element rzeczowo-osobowy). W ten sposób praktyka, orzecznictwo i doktryna wypracowana na gruncie tych historycznych aktów normatywnych nie korespondują z rozwiązaniem wprowadzonym w 1997 r. Kluczem do właściwego zrozumienia przedmiotowych znamion stała się więc definicja w y w i a d u, przyjęta ostatecznie prawie jednolicie przez doktrynę w jej wąskim rozumieniu (tj. struktury organizacyjnej) – patrz. tezy pkt. 2, co wobec jednoczesnego niedookreślenia elementów składowych u d z i a ł u w d z i a ł a l n o ś c i doprowadziło, w ramach wykładni prawniczej, do zawężenia zakresowego tego czynu zabronionego, przez co na gruncie wykładniczym wydaje się on pozostawiać wiele sytuacji faktycznie się pojawiających, które powinny być i – przez praktykę opartą na ustawodawstwach innych państw – są uznawane za działalność szpiegowską.

[33] Podobnie twierdzi Andrzej Lebiedowicz, *Istota szpiegostwa w polskim*…, s. 43.

[34] Rozumiane inaczej niż tożsamy zwrot użyty w art. 130 § 2 kk.

Inny problem wynika z przyjętego w doktrynie stanowiska, że (…) *mianem obcego wywiadu nie można określić obcych agencji telewizyjnych, radiowych i prasowych, placówek badawczych i naukowych, a także zagranicznych przedstawicielstw dyplomatycznych i wchodzących w ich skład służb informacyjnych, ponieważ metoda zbierania przez te podmioty informacji ma charakter jawny*[35]. Biorąc pod uwagę skalę zagrożeń o charakterze asymetrycznym i hybrydowym oraz modus operandi sprawców tych działań, wydaje się, że również ten pogląd wymagałby zrewidowania i przesądzenia na poziomie redakcyjnym przepisu.

Patrząc krytycznie na opisaną powyżej definicję, trzeba uznać, że brakuje w niej zarówno normatywnej, np. w postaci definicji legalnej, jak i jednoznacznie przyjętej przez doktrynę i orzecznictwo – tak krajowe, jak i międzynarodowe – definicji pojęcia s ł u ż b a s p e c j a l n a. Należy wyraźnie wskazać, że na gruncie obecnego art. 130 kk wypełnienie znamion przestępstwa wymaga udowodnienia, objęcia przez sprawcę świadomością działań prowadzonych przez lub na rzecz konkretnie zidentyfikowanego zewnętrznego wobec Polski podmiotu bądź określonej struktury organizacyjnej – domyślnie właśnie służby specjalnej. Biorąc pod uwagę, że prowadzenie tej działalności przez daną służbę czy podmiot z założenia jest utajnione, a jej metody niejawne, to powiązanie z nią osoby działającej w jej imieniu („szpiega") staje się w większości przypadków znacznie utrudnione bądź wręcz niemożliwe. Co więcej – bazując na wykładni językowej przedmiotowej normy, można *ad absurdum* stwierdzić, że elementem dowodowym powiązania osoby będącej przedstawicielem obcego wywiadu (działającego w jej imieniu szpiega), powinny być uzyskane od tej służby (a konkretnie – wywiadu) akta personalne tej osoby, służące stwierdzeniu tego faktu. Na tym przykładzie wyraźnie widać, jak dalece wadliwa jest redakcja obecnego brzmienia tego przepisu, kształtująca normę bazującą na elemencie podmiotowym, oscylującym wokół pojęcia w y w i a d.

Przesłanką zaistnienia przestępstw opisanych w art. 130 kk jest działanie skierowane przeciwko Rzeczpospolitej Polskiej. Znamiona przestępstwa nie zostaną zatem zrealizowane, jeśli działalność danej osoby nie jest wymierzona przeciwko RP, lecz jest prowadzona na szkodę np. innego państwa lub jego władz, pod warunkiem, że nie jest to państwo sojusznicze[36]. W tym kontekście należy się zastanowić, czy przestępstwo szpiegostwa powinno być immanentnie nacechowane działalnością wyłącznie na szkodę polskiego państwa? Czy w ramach typów kwalifikowanych tego przestępstwa nie dokonać penalizacji prowadzenia działalności wywiadowczej lub udziału w wywiadzie, nieopisanego przez pryzmat celu – „przeciw RP", a przez znamię miejsca, np. „na terytorium RP", oczywiście z wyłączeniem sytuacji, gdy takie działania są prowadzone przez służby państw sojuszniczych, choć i w tym wypadku kluczowy powinien pozostać element zgody polskich organów na takie działania.

Warto również wspomnieć o problemie interpretacyjnym pojęcia w i a d o m o ś c i, którego wykładnia jest również obecnie zagadnieniem spornym i – jak się wydaje – wymaga doprecyzowania. Kodeks nie precyzuje bowiem bliżej tego terminu, pozostawiając to doktrynie i orzecznictwu, co w rezultacie powoduje trudności interpretacyjne. Ocena przydatności zdobywanych wiadomości przez obcy wywiad jest kłopotliwa z powodu braku jednoznacznego stwierdzenia, kiedy i w jakich okolicznościach obcy wywiad użyje wiadomości na szkodę RP.

[35] I. Zgoliński, *Komentarz do art. 130 Kodeksu karnego*, Lex/el. 2017.

[36] F. Fetke, *Szpiegostwo w polskim*…, s. 94.

Analiza zachowań sprawców przestępstwa szpiegostwa powinna być rozpatrywana również z punktu widzenia działań o charakterze lobbingowym. Jak autor wskazywał w artykule pt. *Znaczenie lobbingu w kontekście bezpieczeństwa wewnętrznego państwa*[37], naruszenie zasad prowadzenia działalności lobbingowej, uregulowanej w *Ustawie z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa*[38] powinna być rozpatrywana w kontekście odpowiedzialności karnej sprowadzającej się do wypełniania znamion określonego typu czynu zabronionego, szczególnie łapownictwa biernego (art. 228 § 1 kk) i czynnego (art. 229 kk), płatnej protekcji (art. 230 kk), handlu wpływami (art. 230a kk) i nadużycia władzy publicznej (art. 231 kk). Identyfikując jednak zagrożenia bezpieczeństwa państwa stanowiące konsekwencję prowadzenia działalności lobbingowej, istotne wydaje się dostrzeżenie i analiza działań grup interesów, których postulaty zwyciężają w konfrontacji z innymi, i odpowiedź na pytanie o przyczynę tego stanu rzeczy. Czy jest ono podyktowane obiektywnymi kryteriami ekonomiczno-technologicznymi, czy też jest wynikiem niejasnego oddziaływania tej grupy interesu na system prawny bądź politykę, w celu zapewnienia dominującej lub monopolistycznej pozycji. Sytuacja staje się szczególnie niebezpieczna, gdy wśród tak działających podmiotów znajdą się takie, które reprezentują „obcy kapitał". Może to doprowadzić do zależności podmiotu gospodarczego albo całego segmentu od zewnętrznej wobec Polski grupy kapitałowej, która jest postrzegana przez pryzmat realizacji interesów innych państw. Ta sytuacja jest więc szczególnie istotna właśnie w kontekście przestępstwa szpiegostwa. Debata nad kształtem art. 130 kk powinna więc brać pod uwagę to, aby opis znamion tego czynu zabronionego bezsprzecznie obejmował działania prowadzone przez podmiot lobbujący, w swoisty sposób „zlecane" przez przedstawicieli innych państw (bezpośrednio lub pośrednio przez ich służby specjalne – w szerokim rozumieniu tego słowa) jako działanie sprowadzające się do czynności (sporządzania analiz, opinii, ukierunkowanych artykułów prasowych), w celu przyjęcia określonych rozwiązań legislacyjnych zbieżnych z interesami tych mocodawców bądź oddziaływania na kształtowanie zgodnego z tym interesem otoczenia politycznego.

6. Zakończenie

Z perspektywy powyższego, właściwe wydaje się podjęcie poważnej debaty w zakresie zmian regulacyjnych obejmujących przestępstwo szpiegostwa, nakierowanych z jednej strony na rozwiązanie problemów, jakie w tym zakresie można zaobserwować w praktyce funkcjonowania służb w Polsce, a z drugiej – na aktualizację tej normy prawnej w celu dostosowania do zmieniającej się siatki zagrożeń bezpieczeństwa Rzeczpospolitej Polskiej, dotyczącej w głównej mierze zagrożeń o charakterze hybrydowym i asymetrycznym.

Zdaniem autora artykułu należy rozważyć zdefiniowanie w kodeksie karnym elementów, pod którymi należy rozumieć „działalność wywiadowczą" oraz „wywiad". Takie podejście umożliwiłoby wprowadzenie zmian w redakcji art. 130 kk, w którym w ramach znamion czynu zabronionego można będzie oddzielić rzeczywiste prowadzenie działalności wywiadowczej, czyli wykonywanie określonych działań (element przedmiotowy), od pojęcia brania udziału w działalności obcego wywiadu, rozumia-

[37] P. Burczaniuk, *Znaczenie lobbingu w kontekście bezpieczeństwa wewnętrznego państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 156.

[38] Dz.U. z 2017 poz. 248.

nego jako formalna przynależność do struktur tego wywiadu (element podmiotowy). Karalne byłoby więc zarówno samo zachowanie sprowadzające się do wykonywania określonych czynności w interesie obcego państwa lub zagranicznej organizacji, bez potrzeby wiązania ich bezpośrednio z wyodrębnionym strukturalnie podmiotem – służbą wywiadowczą, jak i sama przynależność do takich struktur. Kształtując definicję d z i a ł a l n o ś c i w y w i a d o w c z e j, warto byłoby odwołać się do doświadczeń francuskich, definiując działanie „przeciwko Rzeczpospolitej Polskiej" przez pryzmat kategorii interesów, wobec których to działanie może być skierowane.

Dodatkowo, na co autor wskazywał powyżej, należy się zastanowić, czy przestępstwo szpiegostwa powinno być immanentnie nacechowane działalnością wyłącznie na szkodę polskiego państwa? Czy w ramach typów kwalifikowanych tego przestępstwa nie dokonać penalizacji prowadzenia działalności wywiadowczej lub udziału w wywiadzie, które nie jest opisane przez pryzmat celu – „przeciw RP", a przez znamię miejsca, np. „na terytorium RP", oczywiście z wyłączeniem sytuacji, gdy takie działania są prowadzone przez służby państw sojuszniczych, choć i w tym wypadku najważniejszy powinien pozostać element zgody polskich organów na takie działania.

I na koniec przestępstwo zdrady. Wydaje się że prawie trzydziestoletni okres doświadczeń III Rzeczpospolitej oraz przykład płynący z regulacji karnych państw Zachodu i aktualna siatka zagrożeń bezpieczeństwa Polski, zarówno zewnętrznego, jak i wewnętrznego, powinny stanowić wystarczający asumpt do dyskusji nad zasadnością powrotu do penalizacji tego czynu zabronionego.

Michał Kamiński
Justyna Strużewska-Smirnow
Mateusz Wieczerza

Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych

I. Wprowadzenie

Dynamiczny rozwój technologiczny stwarza nowe wyzwania dla organów odpowiedzialnych za bezpieczeństwo państwa. Pojawiające się cyberzagrożenia stale jednak ewoluują, dlatego też przeciwdziałanie niekorzystnym zjawiskom przez ich badanie i monitorowanie nie zapewni pełnej skuteczności zwalczania tych zagrożeń. Efektywne działania wymagają także przewidywania scenariuszy prawdopodobnych sytuacji kryzysowych oraz opracowywania nowych narzędzi, które skutecznie będą chronić dobra społeczne.

Istotną przeszkodą w stworzeniu odpowiedniego modus operandi w zakresie utworzenia na poziomie państwowym kompleksowej ochrony teleinformatycznej jest trudność w uchwyceniu negatywnych zjawisk, szczególnie na początkowym etapie ich rozwoju. Z tego względu zapewnienie przez agendy rządowe właściwego stopnia bezpieczeństwa teleinformatycznego wymaga ścisłej współpracy wielu podmiotów, które – w zakresie swoich kompetencji – potrafią dostrzec i odpowiednio zdefiniować zagrożenia o niejednolitym charakterze. Warto zaznaczyć, że zdarzenia, które powodują negatywne skutki dla społeczeństwa, wynikają zarówno ze szczegółowo zaplanowanych, nierzadko motywowanych ideologicznie działań w obszarze teleinformatyki, takich jak: cyberprzestępczość, cyberterroryzm czy cyberszpiegostwo, jak też z hackingu realizowanego przez niewielkie grupy lub jednostki działające pod wpływem indywidualnych motywów. Potencjalny atak może być ukierunkowany zarówno na pozyskanie wrażliwych informacji, uszkodzenie infrastruktury krytycznej bądź utrudnienie w innym zakresie funkcjonowania obywateli, np. powodując brak dostępu do określonych serwisów informacyjnych lub e-usług. Działalność ukierunkowana na zapewnienie bezpieczeństwa teleinformatycznego musi być zatem realizowana w formach partnerstwa publiczno-prywatnego i musi uwzględniać i usługodawców, i odbiorców usług teleinformatycznych.

Dodatkowym elementem, który utrudnia walkę z cyberzagrożeniami, jest ich globalny charakter. W dokumencie *Wizja Sił Zbrojnych RP – 2030* dostrzeżono, że w przyszłości ta walka obejmie niemal każdy obszar ludzkiej aktywności, odmienny od klasycznego pola walki charakteryzowanego przez szerokość, głębokość oraz wysokość. Oprócz tradycyjnych, fizycznych geoprzestrzeni, jak ląd, morze, przestrzeń powietrzna (i kosmiczna), do prowadzenia walki będą wykorzystywane sfery pozbawione parametrów geograficznych, niemierzalne i nieograniczone, takie jak wirtualna przestrzeń cybernetyczna i sfera informacyjna. Te obszary będą się na siebie nakładać i wzajemnie uzupełniać, tworząc jednolitą, nieznaną do tej pory przestrzeń walki sił zbrojnych[1].

[1] http://d.wiadomosci24.pl/g2/pdf/250_8a52ebb24514c5ec0a386c8867cef049.pdf [dostęp: 7 VIII 2017].

Przytoczoną uwagę, dotyczącą ponadnarodowego charakteru działań militarnych rozgrywających się w cyberprzestrzeni można przenieść na wszelką aktywność związaną z zapewnianiem bezpieczeństwa narodowego. Ścisła współpraca międzynarodowa będzie zatem jednym z zasadniczych elementów skutecznego modelu efektywnej cyberobrony.

Zaznaczone powyżej aspekty dotyczące zagrożeń cybernetycznych mają wpływ na kształtowanie modeli systemów bezpieczeństwa teleinformatycznego w różnych krajach, jednak wyzwania, jakim muszą sprostać właściwe organy w poszczególnych państwach, są uzależnione także od uwarunkowań geopolitycznych czy modelu ustrojowego. W ramach rozwiązań prawnych, których celem jest ochrona sieci teleinformatycznych, ważną rolę odgrywają służby specjalne, ustawowo zobowiązane do podejmowania kompleksowych lub jedynie cząstkowych działań związanych z cyberobroną.

II. REPUBLIKA CZESKA

1. Stan prawny do lipca 2017 r.

W Republice Czeskiej ustawodawca zdecydował się na uregulowanie zagadnienia cyberbezpieczeństwa w jednym, kompleksowym akcie prawnym, jakim jest ustawa Nr 181 z 23 lipca 2014 r. o cyberbezpieczeństwie i zmianie niektórych innych ustaw, która weszła w życie 1 stycznia 2015 r.[2] (zwana dalej „ustawą").

1.1. Systematyka i zakres ustawy o cyberbezpieczeństwie, najważniejsze definicje

Przedmiotowa ustawa dzieli się na sześć części:

- część pierwsza – *Cyberbezpieczeństwo*,
- część druga – *Zmiany w ustawie o ochronie informacji niejawnych i kompetencjach w dziedzinie bezpieczeństwa*,
- część trzecia – *Zmiany w ustawie o komunikacji elektronicznej*,
- część czwarta – *Zmiany w ustawie o wolności informacji*,
- część piąta – *Zmiany w ustawie o dostarczaniu transmisji radiowej i telewizyjnej*,
- część szósta – *Wejście w życie*.

Część pierwsza, obejmująca większość zawartych w ustawie przepisów, dzieli się na pięć rozdziałów:

I – *Przepisy ogólne*,
II – *System na rzecz zapewnienia cyberbezpieczeństwa*,
III – *Stan zagrożenia cybernetycznego*,
IV – *Wykonywanie administracji państwowej*,
V – *Kontrola, nadzór i wykroczenia administracyjne*,
VI – *Przepisy końcowe*.

W rozdziale I znalazły się unormowania odnośnie do przedmiotu regulacji ustawy oraz definicje podstawowych wykorzystywanych w niej pojęć.

Zakres regulacji ustawy został określony w jej pierwszym paragrafie. Zgodnie z ustępem pierwszym tego przepisu reguluje ona prawa i obowiązki stron oraz zakres kompetencji organów władzy państwowej w dziedzinie bezpieczeństwa cybernetycz-

[2] https://www.govcert.cz/en/legislation/legislation/ [dostęp: 5 X 2017].

nego. Natomiast ustęp drugi omawianego paragrafu wyłącza z zakresu przedmiotowego ustawy systemy informacyjne i komunikacyjne służące do przetwarzania informacji niejawnych.

Następnie, w § 2, zawarto definicje najważniejszych, występujących w ustawie pojęć: cyberprzestrzeń, krytyczna infrastruktura teleinformatyczna, bezpieczeństwo informacji, kluczowy system informacyjny, administrator systemu informacyjnego, administrator systemu komunikacyjnego oraz kluczowa sieć.

Spośród wskazanych definicji należy przytoczyć definicję bezpieczeństwa informacji zawartą w § 2 lit. c, która oznacza: (…) *zapewnienie poufności, integralności i dostępności informacji*.

Z kolei kluczowy system informacyjny, zgodnie z lit. d § 2 oznacza (…) *system informacyjny zarządzany przez organ władzy publicznej, który nie stanowi krytycznej infrastruktury informacyjnej i w przypadku którego naruszenie bezpieczeństwa informacji może ograniczyć lub poważnie zagrozić skuteczności działań władzy publicznej*. Natomiast kluczowa sieć, zdefiniowana w § 2 lit. g, to (…) *sieć komunikacji elektronicznej, zapewniająca bezpośrednie połączenia zagraniczne do publicznej sieci łączności lub zapewniająca bezpośrednie podłączenie do krytycznej infrastruktury informacyjnej*.

Z zakresu powyższych definicji można wysnuć wniosek, że pojęcie bezpieczeństwo cybernetyczne jest odnoszone przez przepisy projektowanej ustawy głównie do domeny publicznej.

1.2. Zagadnienia funkcjonalne systemu cyberbezpieczeństwa

W § 3 zawarto listę podmiotów (władz publicznych oraz osób fizycznych i prawnych) mających obowiązki w sferze cyberbezpieczeństwa. Są to:

- dostawcy usług i sieci komunikacji elektronicznej,
- władze publiczne oraz osoby fizyczne i prawne administrujące sieciami kluczowymi,
- administratorzy krytycznej infrastruktury informatycznej,
- administratorzy krytycznej infrastruktury komunikacyjnej,
- administratorzy kluczowych systemów informacyjnych.

W rozdziale II części pierwszej omawianej ustawy pt. *System na rzecz zapewnienia cyberbezpieczeństwa* znajduje się większość zawartych w jej postanowieniach uregulowań merytorycznych. Przedmiotowy rozdział dzieli się na tytuły obejmujące od jednego do kilku paragrafów:

- *Środki bezpieczeństwa* (§ 4–6),
- *Zdarzenie i incydent w zakresie cyberbezpieczeństwa* (§ 7),
- *Raportowanie incydentów cyberbezpieczeństwa* (§ 8),
- *Przechowywanie dokumentacji* (§ 9–10),
- *Środki* (§ 11),
- *Ostrzeżenia* (§ 12),
- *Środki reagowania i środki ochronne* (§ 13–15),
- *Dane kontaktowe* (§ 16),
- *CERT krajowy* (§ 17),
- *Administrator CERT-u krajowego* (§ 18),

- *Umowa prawa publicznego* (§ 19),
- *CERT rządowy* (§ 20).

Pojęcie ś r o d k i b e z p i e c z e ń s t w a zostało zdefiniowane w ustępie 1 § 4. Oznacza ono: (…) *wszystkie czynności, mające na celu zapewnienie bezpieczeństwa informacji w systemach informacyjnych oraz zapewnienie dostępności i niezawodności usług i sieci elektronicznej komunikacji w cyberprzestrzeni*. Przepis ust. 2 przedmiotowego paragrafu nakłada obowiązki w zakresie ustanowienia i wdrożenia środków bezpieczeństwa dla informacyjnych systemów krytycznej infrastruktury informacyjnej, komunikacyjnego systemu informacyjnej infrastruktury krytycznej lub kluczowego systemu informacyjnego oraz prowadzenia dokumentacji bezpieczeństwa ich dotyczącej na następujące osoby:

- administratorów krytycznej infrastruktury informatycznej,
- administratorów krytycznej infrastruktury komunikacyjnej,
- administratorów kluczowych systemów informacyjnych.

W § 5 zawarto katalog środków bezpieczeństwa. Podstawowy ich podział (zgodnie z ust. 1) to środki organizacyjne i środki techniczne.

Stosownie do ustępu 2 § 5 środki organizacyjne obejmują:

a) system zarządzania bezpieczeństwem informacji,
b) zarządzanie ryzykiem,
c) politykę bezpieczeństwa,
d) bezpieczeństwo organizacyjne,
e) wymogi bezpieczeństwa dla dostawców,
f) zarządzanie kapitałem,
g) bezpieczeństwo zasobów ludzkich,
h) obsługę krytycznej infrastruktury informatycznej lub kluczowego systemu informacyjnego i zarządzanie komunikacją,
i) kontrolę dostępu osób do krytycznej infrastruktury informatycznej lub kluczowego systemu informatycznego,
j) nabywanie, rozwój i utrzymywanie krytycznej infrastruktury informatycznej lub kluczowego systemu informatycznego,
k) zarządzanie zdarzeniami w zakresie cyberbezpieczeństwa i incydentami cyberbezpieczeństwa,
l) zarządzanie ciągłością działania,
m) kontrolę i audyt krytycznej infrastruktury informacyjnej i kluczowych systemów informacyjnych.

Natomiast ustęp 3 zalicza do środków technicznych następujące zagadnienia:

a) bezpieczeństwo fizyczne,
b) narzędzia ochrony integralności sieci łączności,
c) narzędzia weryfikacji tożsamości użytkowników,
d) narzędzia zarządzania prawem dostępu,
e) narzędzia ochrony przed szkodliwym kodem,
f) narzędzia rejestrowania działalności krytycznej infrastruktury informacyjnej i kluczowych systemów informacyjnych, ich użytkowników i administratorów,
g) narzędzia wykrywania zdarzeń w zakresie bezpieczeństwa cybernetycznego,
h) narzędzia zbierania i oszacowania zdarzeń w zakresie bezpieczeństwa cybernetycznego,
i) bezpieczeństwo aplikacji,

j) urządzenia kryptograficzne,
k) narzędzia zabezpieczania poziomu dostępności informacji,
l) bezpieczeństwo systemów przemysłowych i służących do zarządzania.

Przepis § 7 ustawy definiuje pojęcia zdarzenie w zakresie cyberbezpieczeństwa oraz incydent cyberbezpieczeństwa, a także formułuje obowiązki niektórych podmiotów związane z zaistnieniem tego rodzaju zdarzeń.

Zdarzenie w zakresie cyberbezpieczeństwa to zdarzenie, które może powodować naruszenie bezpieczeństwa informacyjnego w systemach informatycznych lub naruszenie bezpieczeństwa lub integralności komunikacji elektronicznej. Incydent cyberbezpieczeństwa oznacza natomiast naruszenie bezpieczeństwa informacyjnego w systemie informatycznym lub naruszenie bezpieczeństwa usług lub integralności sieci komunikacji elektronicznej wynikające ze zdarzenia w zakresie cyberbezpieczeństwa.

Władze publiczne oraz administratorzy krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych są obowiązani wykrywać zdarzenia z zakresu cyberbezpieczeństwa (§ 7 ust. 3). Przepis § 8 ust. 1 nakłada na władze publiczne oraz osoby fizyczne i prawne administrujące kluczowymi sieciami, administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych obowiązek raportowania o incydentach cyberbezpieczeństa natychmiast po ich wykryciu, przy czym raporty od władz publicznych oraz podmiotów administrujących sieciami kluczowymi powinny być kierowane do krajowego CERT-u (ust. 2), a od pozostałych podmiotów – do Krajowej Władzy Bezpieczeństwa (ust. 3).

Krajowy Urząd Bezpieczeństwa jest obowiązany przechowywać dokumentację dotyczącą incydentów cyberbezpieczeństwa, a także udostępniać ją innym władzom publicznym, jeśli jest im potrzebna do wykonywania ustawowych obowiązków. Może też udostępniać tę dokumentację krajowemu CERT-owi oraz innym krajowym i zagranicznym podmiotom wykonującym zadania w obszarze cyberbezpieczeństwa, w zakresie niezbędnym do ochrony cyberprzestrzeni (§ 9).

Przepis § 11 ust. 1 definiuje środki jako działania niezbędne w celu ochrony systemów informacyjnych lub usług i sieci komunikacji elektronicznej przed zagrożeniami na polu cyberbezpieczeństwa lub przed incydentami cyberbezpieczeństwa oraz działania mające na celu neutralizację już występującego incydentu cyberbezpieczeństwa.

Ustęp 2 dzieli środki na ostrzeżenia, środki reakcji i środki ochronne. Stosownie do ust. 3 środki reakcji są obligatoryjnie stosowane przez administratorów systemów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej oraz kluczowej infrastruktury informatycznej. Natomiast dostawcy usług i sieci komunikacji elektronicznej, a także władze publiczne oraz osoby fizyczne i prawne administrujące sieciami kluczowymi, wdrażają je w stanie cyberzagrożenia.

Środki ochronne są obligatoryjnie stosowane przez administratorów systemów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej oraz kluczowej infrastruktury informatycznej.

Ostrzeżenia są wydawane przez Krajową Władzę Bezpieczeństwa w sytuacji zaistnienia zagrożenia cyberbezpieczeństwa. Wiedza o zaistnieniu zagrożenia może pochodzić z ustaleń własnych albo zostać przekazana przez krajowy CERT lub odpowiednie organy innych państw. Ostrzeżenia są publikowane na stronie internetowej i doręczane podmiotom obowiązanym, wskazanym w § 3 ustawy.

Środki reakcji natomiast są wdrażane przez podmioty obowiązane na podstawie decyzji administracyjnej, wydawanej przez Krajową Władzę Bezpieczeństwa, w celu przeciwdziałania skutkom incydentu cyberbezpieczeństwa lub zabezpieczenia systemów informatycznych oraz sieci komunikacji elektronicznej przed incydentem. Taka decyzja jest niezwłocznie doręczana podmiotom obowiązanym i natychmiast wykonalna – ewentualne odwołanie nie powoduje zawieszenia wykonalności. Krajowy Urząd Bezpieczeństwa może również zarządzać wdrożenie środków reakcji o charakterze generalnym – bez wskazywania konkretnych adresatów decyzji. W takim trybie wyżej wymieniony Urząd nakazuje również stosowanie środków ochronnych w celu zwiększenia ochrony systemów informatycznych lub sieci i usług komunikacji elektronicznej, na podstawie analizy zakończonego już incydentu cyberbezpieczeństwa. Środki o charakterze generalnym obowiązują od chwili publikacji przez Krajową Władzę Bezpieczeństwa stosownego ogłoszenia.

1.3. Instytucje systemu cyberbezpieczeństwa

Główną instytucją systemu cyberbezpieczeństwa Republiki Czeskiej, według pierwotnej wersji ustawy Nr 181/2014, był Krajowy Urząd Bezpieczeństwa (Národní bezpečnostní úřad – NBU). O roli tego urzędu w obszarze cyberbezpieczeństwa stanowił rozdział IV – *Wykonywanie administracji państwowej*, zawierający tylko jeden paragraf – 22. Ustęp 1 tego paragrafu tworzył domniemanie kompetencji na rzecz NBU, wskazując, że ten urząd wykonuje zadania administracji państwowej w obszarze cyberbezpieczeństwa, chyba że przepisy odrębne stanowią inaczej. Do zadań administracyjnych NBU w obszarze cyberbezpieczeństwa ustawa w § 22 ust. 2 zaliczała: określanie środków bezpieczeństwa, wydawanie środków zaradczych, zapewnianie działania Narodowego Centrum Cyberbezpieczeństwa, przechowywanie rekordów na temat zdarzeń cyberbezpieczeństwa, nakładanie kar administracyjnych, pełnienie funkcji koordynacyjnych podczas stanu cyberzagrożenia, współpracę z władzami publicznymi oraz osobami fizycznymi i prawnymi działającymi w obszarze cyberbezpieczeństwa, jednostkami badawczo-rozwojowymi, innymi jednostkami typu CERT, zapewnianie współpracy międzynarodowej, w tym negocjowanie i zawieranie porozumień międzynarodowych, zapewnianie prewencji, edukacji i metodycznego wsparcia w obszarze cyberbezpieczeństwa, prowadzenie badań i rozwoju w obszarze cyberbezpieczeństwa, zawieranie kontraktu prawa publicznego z administratorem krajowego CERT-u, przekazywanie ministrowi spraw wewnętrznych propozycji określenia elementów infrastruktury krytycznej w obszarze komunikacji i systemów informacyjnych w zakresie cyberbezpieczeństwa, jeśli ich administrator jest państwową jednostką organizacyjną, oraz uznawanie innych systemów informatycznych i komunikacyjnych za elementy infrastruktury krytycznej zgodnie z ustawą o zarządzaniu kryzysowym, a także wykonywanie innych, przewidzianych prawem zadań.

Rządowy CERT, zgodnie z § 20, stanowił część składową Krajowej Władzy Bezpieczeństwa. W zakresie zadań rządowego CERT-u znalazło się m.in. przyjmowanie raportów na temat incydentów cyberbezpieczeństwa od administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych, dokonywanie oceny zdarzeń i incydentów cyberbezpieczeństwa, które wystąpiły w obszarze krytycznej infrastruktury informatycznej, kluczowych systemów informatycznych oraz innych systemów administracji publicznej,

zapewnianie metodycznego wsparcia dla administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych, współpraca z tymi podmiotami podczas incydentów i zdarzeń cyberbezpieczeństwa, otrzymywanie danych od podmiotów istotnych w obszarze cyberbezpieczeństwa i analiza tych danych oraz prowadzenie analiz podatności w obszarze cyberbezpieczeństwa.

Zadania krajowego CERT-u zostały określone w § 17. Zgodnie z ust. 1 tego przepisu głównym zadaniem CERT-u jest zapewnianie wymiany informacyjnej w zakresie cyberbezpieczeństwa na szczeblu krajowym i zagranicznym.

Zadania przypisane administratorowi CERT-u, określone w ustępie 2 tego przepisu, to m.in.: przyjmowanie raportów na temat incydentów cyberbezpieczeństwa od administratorów sieci kluczowych oraz dokonywanie ich ewaluacji, dostarczanie podmiotom administrującym sieciami kluczowymi oraz dostawcom usług i sieci łączności elektronicznej metodycznego wsparcia, pomocy i współpracy, w sytuacji wystąpienia incydentu cyberbezpieczeństwa, działanie jako punkt kontaktowy dla tych podmiotów, prowadzenie analiz podatności w zakresie cyberbezpieczeństwa, przekazywanie do Krajowej Władzy Bezpieczeństwa danych dotyczących incydentów cyberbezpieczeństwa bez ujawniania osób zgłaszających, w czasie stanu cyberzagrożenia zaś – udostępnianie Krajowej Władzy Bezpieczeństwa danych kontaktowych dostawców usług i sieci łączności elektronicznej i administratorów sieci kluczowych.

Jak wynika z powyższego, CERT krajowy i CERT rządowy wykonują dość podobne zadania administracyjne wobec odmiennych grup podmiotów obowiązanych na podstawie ustawy. CERT krajowy przyjmuje raporty o incydentach od administratorów sieci kluczowych, natomiast CERT rządowy – od administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych. Wykonując swoje zadania, administrator krajowego CERT -u był zobowiązany koordynować swoją działalność z Krajową Władzą Bezpieczeństwa i zachować bezstronność w działaniach. Dopuszczalne jest natomiast prowadzenie przez niego działalności gospodarczej w zakresie cyberbezpieczeństwa, jeśli daje się ona pogodzić z zadaniami statutowymi.

Przepis § 18 określa wymogi wobec administratora krajowego CERT-u. Zgodnie z ust. 1 wskazanego przepisu administratorem CERT-u może zostać wyłącznie osoba prawna, spełniająca warunki określone w ust. 2, która zawarła kontrakt prawa publicznego z Krajową Władzą Bezpieczeństwa. Przepis ust. 2 stanowi, że administratorem krajowego CERT-u może być jedynie osoba prawna, która spełnia wymogi określone w ustawie o ochronie informacji niejawnych odnośnie do nieprowadzenia działalności skierowanej przeciwko Republice Czeskiej, legitymująca się co najmniej pięcioletnim doświadczeniem w zakresie operowania i administrowania systemami lub usługami i sieciami komunikacji elektronicznej, posiadająca bazę techniczną do wykonywania zadań CERT-u, będąca członkiem organizacji międzynarodowej zajmującej się cyberbezpieczeństwem, niemająca zaległości podatkowych oraz spełniająca wymóg niekaralności – w rozumieniu ustawy o odpowiedzialności karnej osób prawnych. Administrator CERT-u nie może być również osobą prawną prawa obcego ani też stworzoną jedynie w celu zdobycia zysku.

Wybór administratora krajowego CERT-u odbywa się w trybie określonym przepisami kodeksu postępowania administracyjnego. Ze zwycięzcą postępowania selekcyjnego Krajowy Urząd Bezpieczeństwa podpisuje kontrakt prawa publicznego (§ 19).

1.4. Stan cyberzagrożenia

Niewątpliwie ciekawą instytucją zawartą w omawianej ustawie jest stan cyberzagrożenia, któremu poświęcono rozdział III części pierwszej, obejmujący tylko jeden paragraf – 21. Zgodnie z zawartą w ust. 1 tego przepisu definicją, jest to stan, w którym bezpieczeństwo informacyjne w systemach informacyjnych lub bezpieczeństwo i integralność usług i sieci komunikacji elektronicznej są poważnie zagrożone oraz występuje ryzyko naruszenia lub zagrożenia interesów Republiki Czeskiej, stosownie do przepisów ustawy o ochronie informacji niejawnych.

Zgodnie z ust. 2 stan cyberzagrożenia wprowadza dyrektor Krajowej Władzy Bezpieczeństwa, ogłaszając publicznie swoją decyzję, również w środkach masowego przekazu. Decyzja o ogłoszeniu stanu cyberzagrożenia wchodzi w życie w momencie wskazanym w jej treści, i obowiązuje przez czas w niej określony, nieprzekraczający siedmiu dni. Istnieje możliwość przedłużania stanu cyberzagrożenia na kolejne okresy, jednak całkowity czas jego trwania nie może przekroczyć 30 dni.

Podczas trwania stanu cyberzagrożenia dyrektor Krajowej Władzy Bezpieczeństwa jest obowiązany informować rząd o wdrożonych procedurach mających na celu neutralizację cyberzagrożeń oraz o aktualnym poziomie zagrożeń, które doprowadziły do ogłoszenia stanu cyberzagrożenia. Krajowy Urząd Bezpieczeństwa mógł wydawać decyzje i stosować środki o charakterze generalnym również w stosunku do dostawców sieci i usług komunikacji elektronicznej oraz administratorów kluczowych sieci (ust. 4). Stan cyberzagrożenia nie powinien być ogłaszany, jeśli NBU byłaby zdolna do neutralizacji zagrożenia bezpieczeństwa informacji w systemach informatycznych oraz bezpieczeństwa usług lub bezpieczeństwa i integralności sieci komunikacji elektronicznej za pomocą swoich zwykłych ustawowych kompetencji (ust. 5).

Jeśli natomiast odwrócenie skutków zagrożenia bezpieczeństwa informacji w systemach informatycznych oraz bezpieczeństwa usług lub bezpieczeństwa i integralności sieci komunikacji elektronicznej przy użyciu oprzyrządowania prawnego, dotyczącego stanu cyberzagrożenia, okazałoby się niemożliwe, to dyrektor NBU jest zobowiązany do niezwłocznego wystąpienia do rządu o ogłoszenie stanu wyjątkowego. W przypadku ogłoszenia stanu wyjątkowego decyzje i środki podjęte uprzednio przez dyrektora NBU pozostają w mocy do momentu zastąpienia ich przez środki zastosowane przez rząd na podstawie przepisów o stanie wyjątkowym (ust. 6).

Zakończenie stanu cyberzagrożenia ma miejsce w terminie określonym w decyzji o jego ogłoszeniu, chyba że dyrektor NBU zadecydował o jego wcześniejszym zakończeniu albo jeśli ogłoszono stan wyjątkowy (ust. 7).

1.5. Systemy teleinformatyczne policji i służb specjalnych

Przytoczenia wymaga jeszcze przepis § 33 omawianej ustawy, zawarty w rozdziale VI jej części pierwszej, w podtytule: *Przepisy wspólne*. Określa on zastosowanie ustawy do systemów informacyjnych i komunikacyjnych służb wywiadowczych i policji. Do systemów służb wywiadowczych spełniających kryteria ustanowienia krytycznej infrastruktury komunikacyjnej stosuje się odpowiednio § 4 ustawy dotyczący środków bezpieczeństwa, jednak te systemy nie są ujmowane w spisie infrastruktury krytycznej. Podobne rozwiązanie ma miejsce w odniesieniu do Systemu Informacji Policji Republiki

Czeskiej, wykorzystywanego do działań analitycznych w ramach postępowania karnego, chyba że ten system stanowi krytyczną infrastrukturę informacyjną[3].

2. Reforma systemu cyberbezpieczeństwa – stan prawny po 1 sierpnia 2017 r.

W ostatnim czasie miała miejsce poważna reforma instytucjonalna systemu cyberbezpieczeństwa Republiki Czeskiej, związana z uchwaleniem ustawy nr 205/2017 z 7 czerwca 2017 r. o zmianie ustawy nr 181/2014 o cyberbezpieczeństwie i o zmianie niektórych innych ustaw (ustawa o cyberbezpieczeństwie), o zmianie ustawy nr 104/2017 i niektórych innych ustaw[4]. Wskazana nowelizacja ustawy o bezpieczeństwie cybernetycznym została wprowadzona przede wszystkim ze względu na konieczność implementacji *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. Urz. UE L z 2016 r. nr 194, s. 1)[5].

Zgodnie z postanowieniami wskazanej ustawy z dniem 1 sierpnia 2017 r. zaczął funkcjonować nowy urząd – Krajowy Urząd ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacji (ang. National Cyber and Information Security, czes.: Národní úřad pro kybernetickou a informační bezpečnost – NUKIB),

Do głównych zadań nowego urzędu zalicza się:

- zapewnienie działania CERT- rządowego (GocCERT.cz),
- współpracę z krajowymi zespołami CERT i zespołami CSIRT,
- współpracę z zagranicznymi zespołami CERT i zespołami CSIRT,
- wypracowywanie standardów dla systemów informatycznych infrastruktury krytycznej i infrastruktury kluczowej,
- wspieranie edukacji w zakresie cyberbezpieczeństwa,
- badania i rozwój w obszarze cyberbezpieczeństwa,
- ochronę informacji niejawnych w obszarze systemów informacyjnych i komunikacyjnych,
- ochronę kryptograficzną[6].

Nowo powołany urząd przejął zatem uprawnienia administracyjne Narodowego Urzędu Bezpieczeństwa (NBU) w odniesieniu do sfery cyberbezpieczeństwa. Ma sprawować nadzór nad ochroną systemów infrastruktury krytycznej, odbierać raporty o incydentach i być koordynatorem działań w przypadku zagrożeń cybernetycznych. Siedzibą nowego urzędu ma być Brno[7].

Najważniejsze pozostałe zmiany wprowadzone do ustawy o cyberbezpieczeństwie ustawą nr 205/2017 to:

- wprowadzenie w § 2 nowych definicji: m.in. usługi podstawowej i usługi cyfrowej,
- wprowadzenie w § 3 nowych podmiotów odpowiedzialnych: administratora i operatora systemu informatycznego usług podstawowych oraz dostawcy usług cyfrowych,

[3] https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf [dostęp: 5 IX 2017].

[4] https://www.govcert.cz/en/ [dostęp: 10 IX 2017].

[5] https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2541-zacatkem-srpna-dojde-u-nckb-k-zasadni-zmene/ [dostęp: 19 IX2017].

[6] https://www.govcert.cz/en/ [dostęp: 10 IX 2017].

[7] https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2541-zacatkem-srpna-dojde-u-nckb-k-zasadni-zmene/ [dostęp: 19 IX 2017].

- wprowadzenie w § 4 nowej regulacji odpowiedzialności stron w ramach zawierania umów między organami władz publicznych a dostawcami tzw. *cloud computing* (przetwarzania danych w chmurze),
- wprowadzenie nowych obowiązków informacyjnych organów i osób odpowiedzialnych (§ 4a),
- rozszerzenie zadań podmiotów obowiązanych przy zdarzeniach i incydentach z zakresu cyberbezpieczeństwa (§ 7 i 8),
- wprowadzenia regulacji udzielania informacji w zakresie bezpieczeństwa publicznego (§ 10a),
- rozszerzenie uprawnień krajowego CERT (§ 17),
- rozszerzenie uprawnień rządowego CERT (§ 20),
- powołanie nowego centralnego organu administracji państwowej – Narodowego Urzędu ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacyjnego oraz określenie jego praw i obowiązków (§ 21a – § 24b),
- nowa regulacja wykroczeń administracyjnych i kar za nie (§ 25 – § 27).

Spośród nowych definicji wprowadzonych ustawą nowelizującą omówienia wymaga pojecie usługa podstawowa (§ 2 lit. i). Zostało ono zdefiniowane jako posiadające trzy cechy konstytutywne:

1) zabezpiecza działalność społeczną lub gospodarczą w jednej z dziedzin wskazanych w ustawie (energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, gospodarka wodna, infrastruktura cyfrowa i przemysł chemiczny),
2) jest udostępniana w sieciach komunikacji elektronicznej lub systemach informatycznych,
3) naruszenie sieci komunikacji elektronicznej lub systemów informatycznych, w których ta usługa jest udostępniana, mogłoby mieć znaczny wpływ na bezpieczeństwo społeczne lub ekonomiczne.

Z tym pojęciem łączą się pojęcia: system informatyczny usług podstawowych (§ 2 lit. j) oraz operator usług podstawowych (§ 2 lit. k)[8].

3. Podsumowanie

Republika Czeska jest przykładem kraju mającego uporządkowany i scentralizowany system cyberbezpieczeństwa. Wyrazem tego jest uregulowanie przedmiotowego zagadnienia jedną, kompleksową ustawą oraz powierzenie kompetencji administracyjnych w tym obszarze jednemu wyspecjalizowanemu organowi państwowemu. W tym systemie nie przewidziano żadnej istotnej roli dla służb specjalnych, natomiast rolę organu odpowiedzialnego za cyberbezpieczeństwo powierzono Krajowej Władzy Bezpieczeństwa (Narodowemu Urzędowi Bezpieczeństwa – NBU), która w Republice Czeskiej jest odrębnym urzędem administracji. Taki rozdział kompetencji miał miejsce do 1 sierpnia 2017 r., kiedy to zaczęła działać wyspecjalizowana agencja – Narodowy Urząd ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacji NUKIB, odpowiedzialna jedynie za bezpieczeństwo informatyczne i telekomunikacyjne.

[8] https://www.psp.cz/sqw/sbirka.sqw?cz=205&r=2017 [dostęp: 15 IV 2017].

III. GRECJA

Republika Grecka najważniejszą rolę w swoim systemie cyberbezpieczeństwa przyznała cywilnej służbie specjalnej – Narodowej Służbie Wywiadu (ang. National Intelligence Service – NIS, gr. EYP), do której zadań, oprócz zadań informacyjnych, prowadzenia wywiadu i kontrwywiadu, zaliczają się sprawy techniczne: pełnienie funkcji Władzy Technicznej w zakresie Bezpieczeństwa Informacyjnego – INFOSEC oraz Krajowej Władzy ds. Przeciwdziałania Atakom Elektronicznym[9].

Przypisanie tych funkcji NIS zostało dokonane w art. 4 ustawy nr 3649 – *Narodowa Służba Wywiadu i inne przepisy* (Dz. Urz. Republiki Greckiej Nr 39 z 3 marca 2008 r.), regulującym kompetencje służby. Przepis art. 4 ust. 7 stanowi, że EYP pełni w kraju funkcję *Władzy Technicznej w zakresie Bezpieczeństwa Informacyjnego – INFOSEC*. W tym zakresie EYP zapewnia bezpieczeństwo krajowych systemów informacyjnych i komunikacyjnych. Prowadzi również certyfikację urządzeń służących do ochrony informacji niejawnych. Za dokonanie certyfikacji pobiera opłatę, której wysokość jest określona we wspólnej uchwale ministrów: spraw wewnętrznych oraz gospodarki i finansów.

Na mocy art. 4 ust. 8 ustawy nr 3649 EYP pełni także funkcję Krajowej Władzy ds. Przeciwdziałania Atakom Elektronicznym (ang.: National Authority Against Electronic Attacks – NAAEA), czyli krajowego CERT-u. Zadaniem EYP w tym zakresie jest zapobieganie, a także pasywne i aktywne przeciwdziałanie atakom elektronicznym, skierowanym przeciwko sieciom komunikacyjnym, infrastrukturze służącej do przechowywania danych i systemom komputerowym[10].

Według dostępnych informacji na temat misji NAAEA obejmuje ona przede wszystkim ochronę przed atakami jednostek sektora publicznego oraz krajowej infrastruktury krytycznej. NAAEA wykorzystuje odpowiedni sprzęt oraz zatrudnia wykwalifikowany personel niezbędny do prowadzenia działań, w tym do implementacji strategicznych rodzajów polityki cyberbezpieczeństwa odnoszących się do przeciwdziałania zagrożeniom i atakom oraz zbierania, przetwarzania i dystrybuowania informacji ich dotyczących. W celu zwiększenia efektywności realizacji swojej misji Krajowa Władza Przeciwdziałania Atakom Elektronicznym współpracuje z zagranicznymi zespołami CERT oraz innymi właściwymi organami i służbami[11].

IV. FRANCJA

Wstęp[12]

Zadania w sferze cyberbezpieczeństwa realizowane są we Francji przez cztery organy: Narodową Agencję Bezpieczeństwa Systemów Informatycznych (Agence nationale de la sècurité des systèmes d'information – ANSSI) podlegającą premierowi, Sztab Generalny

[9] http://www.nis.gr/portal/page/portal/NIS/Competences [dostęp: 4 IX 2017].

[10] http://www.nis.gr/npimages/docs/LAW_NUMBER%203649_en.pdf [dostęp: 4 IX 2017].

[11] http://www.nis.gr/portal/page/portal/NIS/NCERT [dostęp: 19 IX 2017].

[12] Ogólna charakterystyka instytucjonalna została opracowana na podstawie dokumentu *Pour une véritable politique publique du renseignement*, Sebastian-Yves Laurent, Institut Montaigne, juillet 2014, www.institutmontaigne.org/res/files/publications/Etude renseignement juillet 2014.pdf, s. 41–45 [dostęp: 10 VIII 2017].

Sił Zbrojnych (l'État major des armées – EMA), Generalną Dyrekcję Uzbrojenia (Direction Générale de l'armement – DGA) oraz w zakresie wywiadu elektronicznego – Generalną Dyrekcję Bezpieczeństwa Zewnętrznego (Direction Générale de la Sécurité Extérieure – DGSE). System ten ma zatem charakter mieszany, składający się zarówno z instytucji cywilnych, jak i wojskowych. Zadania realizowane przez najistotniejszy z punktu widzenia niniejszego opracowania organ – ANSSI, należy ocenić jako wyłącznie defensywne.

Punktem wspólnym opisanych dalej strategicznych dokumentów dotyczących cyberbezpieczeństwa oraz dokumentów analitycznych, tworzonych przez niezależnych ekspertów, jest podkreślenie znaczenia gospodarczego wymiaru cyberbezpieczeństwa i potencjalnych skutków, jakie mógłby wywołać ewentualny atak informatyczny na systemy wykorzystywane przez najważniejsze przedsiębiorstwa. W raporcie Instytutu Montaigne podkreślono, że francuskie podmioty gospodarcze odgrywają istotną rolę w produkcji i eksportcie technologii związanych ze sferą cyberbezpieczeństwa – m.in. Airbus Defence and Space, Thales, Atos czy Sogeti. W dokumencie podkreślono rosnącą rolę partnerstwa publiczno-prywatnego oraz wskazano na sprzyjające uwarunkowania strukturalne, które mogą przyczynić się do zwiększenia ogólnej skuteczności systemu cyberbezpieczeństwa – wzrost świadomości organów państwa, wysoki poziom szkolnictwa wyższego w matematyce i informatyce, a także szybki rozwój sektora prywatnego w sferze nowych technologii. Należy także zauważyć, że potrzeby Francji dotyczące stworzenia skutecznych instrumentów przeciwdziałania i reagowania na zagrożenia cybernetyczne są większe niż w przypadku pozostałych państw europejskich (z wyjątkiem Wielkiej Brytanii) z uwagi na posiadanie technologii pozwalających na wykorzystywanie energii nuklearnej, zarówno w wymiarze cywilnym, jak i wojskowym.

1. Charakterystyka ewolucji systemu cyberbezpieczeństwa na podstawie najważniejszych aktów normatywnych i dokumentów programowych na przestrzeni lat 2008–2017[13]

Biała Księga Obrony i Bezpieczeństwa Narodowego z 2008 r.[14]

Biała księga z 2008 r. określiła zagrożenia związane z atakami informatycznymi wymierzonymi w najważniejsze elementy infrastruktury państwa jako jedno z najbardziej prawdopodobnych zagrożeń na przestrzeni kolejnych 15 lat. Wskazała równocześnie na wiążące się z tego rodzaju zdarzeniem poważne skutki dla funkcjonowania społeczeństwa i wszystkich aspektów życia publicznego. Dokument określa instrumenty informatyczne i komunikacyjne jako system nerwowy społeczeństwa, bez którego jego prawidłowe funkcjonowanie byłoby niemożliwe. Ponadto, w sposób wykładniczy wzrasta uzależnienie wszystkich elementów składowych społeczeństwa od nowych technologii oraz usług społeczeństwa informacyjnego. Warto podkreślić, że biała księga z 2008 r. była pierwszym oficjalnym dokumentem, w której zagrożenia w cyberprzestrzeni określono mianem „poważnych" i jako ich potencjalne formy wymieniono m.in. działalność polegającą na atakach hakerskich czy zorganizowaną przestępczość.

[13] Opracowano na podstawie informacji zawartych na stronie www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/ [dostęp: 10 VIII 2017].

[14] *Défense et Sècurité nationale. Le Livre Blanc*, 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf [dostęp: 16 VIII 2017].

Autorzy dokumentu zwracają uwagę na różnorodność zagrożeń bezpieczeństwa w cyberprzestrzeni. Należą do nich m.in. blokowanie prawidłowego działania najważniejszych elementów infrastruktury informatycznej, możliwość ich fizycznego zniszczenia (np. satelitów czy newralgicznych elementów sieci informatycznych), kradzież danych, a także wrogie przejęcie kontroli nad określonym urządzeniem. Skalę zagrożeń potęguje sukcesywne tworzenie przez inne państwa ofensywnych strategii walki w cyberprzestrzeni i nabywanie coraz bardziej zaawansowanych instrumentów technologicznych w tym zakresie. Ataki prowadzone z wykorzystaniem tych metod mogą mieć zarówno charakter otwarty, jak i zamaskowany.

Biorąc pod uwagę ewolucję technologiczną i coraz większy stopień powiązań między poszczególnymi sieciami i urządzeniami, strategia cyberbezpieczeństwa – oparta wyłącznie na pasywnych instrumentach ochronnych, mimo że w dalszym ciągu są one ważne – nie może w pełni odpowiadać na nowe rodzaje zagrożeń. Te uwarunkowania sprawiają, że konieczne jest stopniowe przekształcenie strategii defensywnej w strategię aktywnej obrony, łączącej w sobie ochronę systemów i nadzór nad ich funkcjonowaniem z możliwościami szybkiej reakcji i działań ofensywnych, jeżeli zajdzie ku temu potrzeba. Ta ewolucja nie będzie jednak możliwa bez odpowiednich działań w wymiarze politycznym i zmiany w sposobie myślenia o problemach związanych z cyberbezpieczeństwem. Właściwe organy państwa powinny pełnić funkcję katalizatora tych modyfikacji przez wspieranie rozwoju wiedzy eksperckiej i udzielanie niezbędnego wsparcia zarówno podmiotom gospodarczym, jak i operatorom sieci informatycznych.

Charakter zagrożeń związanych z cyberprzestrzenią, ich nieprzewidywalność i szybkość wydarzeń wymagają stworzenia zdolności reagowania kryzysowego, zarówno na etapie faktycznego wystąpienia danego zagrożenia, jak i w fazie usuwania jego skutków, co zagwarantuje ciągłość działań sieci dotkniętych atakiem oraz pomoże wykryć osoby odpowiedzialne za tego typu działania. Te czynniki sprawiają, że cyberprzestrzeń należy uznać za nowe pole działań, w którym mogą być prowadzone czynności o charakterze wojskowym. W konsekwencji, niezbędne jest wypracowanie odpowiednich metod postępowania, które można porównać do funkcjonującego w sferze wojskowej angielskiego terminu „*rules of engagement*" (zasada podejmowania działań przy użyciu siły), obejmującego zbiór zasad określających w sposób szczegółowy okoliczności i sposób prowadzenia działań związanych z użyciem instrumentów wojskowych[15].

Główne tezy białej księgi z 2008 r. sprowadzają się do stwierdzenia, że państwo powinno wypracować instrumenty pozwalające na skuteczne zwalczanie zagrożeń w cyberprzestrzeni – cel ten powinien stać się jednym z priorytetów Francji w sferze bezpieczeństwa narodowego. W dokumencie podkreślono konieczność wypracowania zdolności wczesnego wykrywania ataków informatycznych i reagowania na incydenty mające charakter zarówno ściśle ukierunkowany na określone sieci czy urządzenia, jak i na działania o charakterze masowym. Natomiast w sferze zapobiegania zagrożeniom zaproponowano w białej księdze wykorzystywanie urządzeń i sieci mających wysoki stopień zabezpieczeń i stworzenie katalogu kompetencji oraz instrumentów, którymi w razie zagrożenia mogłyby się posługiwać zarówno organy administracji publicznej, jak i tzw. operatorzy infrastruktury krytycznej (fr. *opérateurs d'infrastructures vitales*).

Jednym z działań wdrażającym założenia przedstawione w białej księdze było powołanie, na podstawie dekretu nr 2008-934 z 7 lipca 2009 r.[16], Narodowej Agencji

[15] Tamże, s. 53.

[16] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service à competence nationale dénommé*

Bezpieczeństwa Systemów Informatycznych – wyspecjalizowanego organu administracji publicznej pełniącego funkcję narodowej władzy bezpieczeństwa systemów informatycznych. Zapisy dekretu o utworzeniu ANSSI były również podstawą do powołania Komitetu Strategicznego ds. Bezpieczeństwa Systemów Informacji (fr. *comité stratégique de la SSI*), którego celem było opracowanie narodowej strategii bezpieczeństwa systemów informacji.

Strategia Francji w zakresie ochrony i bezpieczeństwa systemów informacji (strategia SSI) z 2011 r.[17]

Główne założenia strategii SSI są kontynuacją najważniejszych tez zawartych w białej księdze z 2008 r. W dokumencie wymieniono cztery cele strategiczne, do których osiągnięcia mają zmierzać działania podejmowane w sferze cyberbezpieczeństwa. Są nimi:

1. Uzyskanie statusu mocarstwa w sferze cyberobrony.

Francja powinna dążyć do przynależności do ograniczonej grupy państw mających najbardziej rozwinięte zdolności w sferze cyberobrony, zachowując jednocześnie wysoki stopień autonomii w wymiarze strategicznym. W dokumencie zwraca się uwagę na ścisły związek między tymi kompetencjami a pozycją państwa na arenie międzynarodowej – rozwój społeczeństwa informacyjnego i sieci komunikacji elektronicznej jest elementem istotnie przyczyniającym się do wzrostu gospodarczego i poprawy konkurencyjności francuskich podmiotów gospodarczych. Skuteczna ochrona sieci informatycznych jest niezbędna z uwagi na intensyfikację działań wywiadowczych prowadzonych przez inne państwa, których celem jest uzyskanie dostępu do informacji istotnych dla zachowania suwerenności państwa (m.in. informacji niejawnych dotyczących obronności, badań naukowych, technologii, informacji finansowych czy handlowych).

W przeciwieństwie do tradycyjnych konfliktów zbrojnych działania w cyberprzestrzeni nie są ograniczone granicami uczestniczących w nich państw. W konsekwencji, skuteczny system cyberobrony nie może mieć wymiaru wyłącznie narodowego i musi opierać się na ścisłej współpracy z właściwymi organami innych państw, pozwalającej na prowadzenie w czasie rzeczywistym wymiany informacji o potencjalnych zagrożeniach, atakach i możliwych do zastosowania środkach przeciwdziałania skutkom tych zdarzeń.

2. Zagwarantowanie autonomii decyzyjnej przez ochronę informacji istotnych z punktu widzenia suwerenności Francji.

Ten cel jest ściśle powiązany z dwoma aspektami niezwykle istotnymi dla systemu cyberbezpieczeństwa: ogólnymi celami polityki kontrwywiadowczej państwa oraz rozwojem zdolności technologicznych w zakresie bezpieczeństwa informacji. Informacje mające największe znaczenie strategiczne zostały w dokumencie określone jako informacje istotne dla zachowania suwerenności (fr. *l'information de souveraineté*), których prawidłowa ochrona jest warunkiem zachowania suwerenności i autonomii zarówno w polityce wewnętrznej, jak i zagranicznej. Najbardziej efektywnym środkiem zapobiegania nieuprawnionemu uzyskaniu dostępu do tego rodzaju informacji jest stosowanie

"Agence nationale de la sécurité des systèmes d'information", www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 [dostęp: 10 VIII 2017].

[17] *Défense et sécurité des systèmes d'information – Stratégie de la France*, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [dostęp: 11 VIII 2017].

technik kryptograficznych uniemożliwiających lub opóźniających uzyskanie do nich faktycznego dostępu lub zrozumienie ich treści. Obserwowany na przestrzeni ostatnich lat proces stałego zwiększania mocy obliczeniowej komputerów pociąga za sobą znaczny postęp w dziedzinie kryptoanalizy, co wymaga z kolei wykorzystywania coraz bardziej zaawansowanych i wyrafinowanych narzędzi służących do ochrony informacji. Jednym z warunków utrzymania samodzielności decyzyjnej najważniejszych organów jest posiadanie autonomicznych, niezależnych od jakichkolwiek podmiotów zewnętrznych, zdolności oraz technologii w dziedzinach kryptografii i kryptoanalizy.

3. Poprawa cyberbezpieczeństwa najważniejszych elementów infrastruktury krytycznej.

W ustawie – Kodeks obrony[18] określono sektory wchodzące w skład infrastruktury krytycznej, w ramach których działają operatorzy zapewniający: zaspokojenie najważniejszych dla społeczeństwa potrzeb, możliwość sprawowania władzy publicznej, prawidłowe funkcjonowanie systemu gospodarczego, obronnego czy bezpieczeństwa państwa. Rosnące współzależności między sferami gospodarki i informatyki sprawiają, że bezpieczeństwo sieci informatycznych jest jednym z podstawowych warunków utrzymania rozwoju gospodarczego na odpowiednim poziomie. W razie poważnego zakłócenia funkcjonowania sieci telekomunikacyjnych czy Internetu wypracowanie alternatywnych metod wymiany informacji okazałoby się bardzo utrudnione lub niemożliwe, biorąc pod uwagę stale zwiększający się stopień informatyzacji we wszystkich obszarach gospodarki i przemysłu. Z tego względu rozwój nowoczesnych metod reagowania na zagrożenia w cyberprzestrzeni jest jednym z narodowych priorytetów Francji.

4. Zapewnienie bezpieczeństwa w cyberprzestrzeni.

W tym punkcie autorzy strategii zwracają uwagę na społeczny wymiar cyberbezpieczeństwa. Pomimo że zaawansowane ataki informatyczne mające na celu pozyskanie informacji najistotniejszych dla bezpieczeństwa lub gospodarki są jednym z najpoważniejszych zagrożeń strategicznych interesów państwa, należy zwrócić uwagę również na aspekt społeczny i powszechne korzystanie z sieci komunikacji elektronicznej przez większość obywateli. Do potencjalnych zagrożeń należy zatem zaliczyć również takie elementy, jak kradzież tożsamości, haseł do kont bankowych oraz handel bazami zawierającymi dane osobowe. Ponadto, coraz częstszym zjawiskiem jest zdalne przejmowanie kontroli nad urządzeniami informatycznymi przez tzw. botnety. Zadaniem właściwych organów państwa jest zatem zapewnienie odpowiedniego poziomu zaufania do usług świadczonych drogą elektroniczną oraz innych powszechnie wykorzystywanych instrumentów informatycznych. Jednym z przykładów działań pomocnych przy realizacji tego celu było stworzenie w 2010 r. tzw. ogólnego repozytorium bezpieczeństwa (fr. *référentiel général de securité*) – instrumentu służącego zwiększeniu bezpieczeństwa procesu wymiany danych pomiędzy organami publicznymi a obywatelami za pośrednictwem środków komunikacji elektronicznej[19].

Francja zamierza także wspierać wszelkie działania i inicjatywy mające na celu wypracowanie skutecznych instrumentów prawnych regulujących sposób funkcjonowania Internetu i przyczyniające się do zwiększenia efektywności międzynarodowej współpracy dotyczącej ścigania przestępstw cybernetycznych.

---

[18] *Code de la défense*, www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307 [dostęp: 16 VIII 2017].

[19] www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/ [dostęp: 16 VIII 2017].

Biała księga obrony i bezpieczeństwa narodowego Francji z 2013 r.[20]

Opublikowanie nowej wersji białej księgi w 2013 r. miało na celu charakterystykę możliwych do podjęcia działań służących przeciwdziałaniu zaobserwowanej na przestrzeni lat 2008–2013 intensyfikacji cyberataków wymierzonych w systemy informatyczne, które były używane przez podmioty gospodarcze, wykorzystujących coraz bardziej zaawansowane metody technologiczne. Ten dokument to punkt zwrotny w procesie wypracowania mechanizmów chroniących infrastrukturę informatyczną przed potencjalnymi zagrożeniami. Twórcy dokumentu uznali, że skala rozwoju cyberzagrożeń oraz ich negatywne implikacje sprawiają, że organy administracji publicznej nie mogą w dalszym ciągu koncentrować się wyłącznie na cyberbezpieczeństwie sfery publicznej. Konieczne jest również uwzględnienie potrzeb podmiotów prywatnych zarządzających najważniejszymi dla interesów państwa sieciami informatycznymi. Ponadto, rozwój ofensywnych zdolności cybernetycznych został uznany za integralną część strategii cyberobrony[21].

W tym dokumencie zwraca się uwagę na kontynuację trendów opisywanych w analogicznym dokumencie z 2008 r. Wzrost zagrożeń połączony z rozwojem technologii wykorzystywanych w cyberatakach i rosnącą rolą społeczną systemów informatycznych sprawia, że posiadanie mechanizmów efektywnie neutralizujących tego rodzaju wyzwania jest jednym z warunków zachowania pełnej suwerenności państwa. W tym kontekście istotne znaczenie ma pełna i autonomiczna zdolność wytwarzania instrumentów służących zapewnieniu bezpieczeństwa sieci – zwłaszcza w sferze kryptologii oraz wykrywania ataków. Rozwój autonomicznych kompetencji w tym zakresie jest jednak warunkowany stworzeniem niezbędnej infrastruktury naukowej, technologicznej i finansowej.

W tym dokumencie zapowiedziano podjęcie działań mających na celu stworzenie ambitnej i komplementarnej polityki w odniesieniu do systemów informatycznych, opartej głównie na dalszym wykorzystywaniu sieci, które cechują się wysokim poziomem zabezpieczeń przez organy publiczne, dostosowaniem polityki zamówień publicznych do potrzeb związanych z cyberbezpieczeństwem oraz prawidłowym zarządzaniem urządzeniami ruchomej łączności. Dopełnieniem tej polityki ma być prowadzenie działań informacyjnych mających na celu zwiększenie świadomości kierowniczych organów administracji terenowej, jednostek samorządu terytorialnego oraz użytkowników sieci. Poprawie musi ulec również bezpieczeństwo dostawców produktów i usług informatycznych.

W odniesieniu do operatorów infrastruktury krytycznej w dokumencie zapowiedziano przyjęcie aktów normatywnych służących określeniu odpowiednich standardów bezpieczeństwa w kontekście ewentualnych zagrożeń cybernetycznych, które pozwolą na weryfikację stosowania przez operatorów niezbędnych środków bezpieczeństwa. Ten akt stworzy również precyzyjny katalog obowiązków podmiotów publicznych i prywatnych dotyczących zasad prowadzenia audytów, powiadamiania ANSSI o strukturze zarządzanych przez nie systemów oraz o wystąpieniu incydentów zagrażających ich bezpieczeństwu.

---

[20] *Défense et Sécurité nationale. Le Livre Blanc*, 2013, www.livreblancdedefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, s. 105–107 [dostęp: 10 VIII 2017].

[21] P. Brangetto, *National Cyber Security Organisation*: *France, NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia, www.ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf, s. 8 [dostęp: 14 VIII 2017].

Narodowa doktryna przeciwdziałania atakom cybernetycznym jest oparta na komplementarnych i całościowych działaniach, których podstawą są dwie wzajemnie uzupełniające się części składowe:

1) wypracowanie wydajnych i odpornych na ataki cybernetyczne mechanizmów ochrony systemów informatycznych organów państwowych, operatorów infrastruktury krytycznej oraz strategicznie istotnych przedsiębiorstw, które jest połączone z operacyjną organizacją działań obronnych; te elementy mają być koordynowane przez premiera, wszelkie zaś działania mają być oparte na ścisłej współpracy poszczególnych organów w celu jak najszybszego wykrywania zagrożeń;
2) stworzenie całościowych i dostosowanych do okoliczności zróżnicowanych mechanizmów reagowania działających na zasadzie subsydiarności, które polegają na wykorzystaniu w pierwszej kolejności środków prawnych, dyplomatycznych oraz policyjnych, dopuszczających jednakże możliwość stopniowego stosowania mechanizmów znajdujących się w kompetencji Ministerstwa Obrony, jeżeli będą zagrożone strategiczne interesy państwa.

Biała księga z 2013 r. zwraca również uwagę na konieczność rozwoju zdolności ofensywnych, połączonych z działaniami w sferze wywiadowczej, które wywierają istotny wpływ na możliwości skutecznego reagowania na zagrożenia w cyberprzestrzeni. Te zdolności pozwalają na dokonanie kompleksowej charakterystyki zagrożeń, identyfikację ich źródeł, a także stwarzają możliwości przewidywania wystąpienia zagrożeń cybernetycznych i odpowiedniej konfiguracji metod reagowania. Zdolności o charakterze ofensywnym przyczyniają się do znacznego wzbogacenia katalogu środków pozostających w dyspozycji właściwych organów.

W dokumencie zwraca się również uwagę na istotną rolę współpracy z partnerami zagranicznymi w zakresie cyberbezpieczeństwa (do najważniejszych partnerów zaliczono: Niemcy i Wielką Brytanię). Położono również nacisk na wspieranie procesu wypracowywania wspólnych rozwiązań, mających na celu wzmocnienie ochrony przed zagrożeniami infrastruktury krytycznej i sieci komunikacji elektronicznej na poziomie Unii Europejskiej.

Pakt cyberobrony[22]

W nawiązaniu do ogólnych założeń polityki cyberbezpieczeństwa zawartych w białej księdze z 2013 r. Ministerstwo Obrony przedstawiło zarys analogicznych działań w sektorze wojskowym. Dokument zwraca uwagę na konieczność wypracowania skutecznych mechanizmów ochrony przed atakami cybernetycznymi z uwagi na postępującą informatyzację poszczególnych komponentów sił zbrojnych. Podmioty te wykorzystują zaawansowane i najistotniejsze – pod kątem strategicznym – systemy informatyczne związane m.in. z zarządzaniem instrumentami odstraszania nuklearnego czy zaawansowanymi systemami obronnymi wykorzystywanymi przez wojska lądowe, powietrzne i marynarkę wojenną.

W konsekwencji, bezpieczeństwo cybernetyczne jest jednym z priorytetowych obszarów działań zarówno Ministerstwa Obrony, jak i poszczególnych podmiotów wchodzących w skład francuskich sił zbrojnych. Mimo że ogólna odpowiedzialność

[22] *Pacte Défense Cyber – 50 mesures pour changer d'échelle,* www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%Cyber-1.pdf [dostęp: 14 VIII 2017].

za zagwarantowanie bezpieczeństwa systemów informatycznych spoczywa na ANSSI, w razie ewentualnego konfliktu zbrojnego i zaburzenia ciągłości funkcjonowania instytucji państwa te zadania będą realizowane przez podmioty wojskowe. Z tego powodu Ministerstwo Obrony powinno odgrywać pomocniczą rolę zarówno wobec ANSSI, jak i wobec innych podmiotów, do których kompetencji należy przeciwdziałanie zagrożeniom w systemach i sieciach informatycznych (np. jednostek podlegających Ministerstwu Spraw Wewnętrznych odpowiedzialnych za zwalczanie cyberprzestępczości).

Pakt Cyberobrony stanowił dokument określający wszystkie działania, które miały zostać zrealizowane w latach 2014, 2015 i 2016 zgodnie z ustawą o programowaniu wojskowym na lata 2014–2019[23]. Zawiera on środki, które miały zostać podjęte w Ministerstwie Obrony i podległych mu jednostkach, oraz instrumenty mające oddziaływać na sferę zewnętrzną, m.in. w zakresie wspierania jednostek samorządu terytorialnego. Opisane w dokumencie z działania zostały podzielone na sześć głównych tematów:

1) podniesienie poziomu bezpieczeństwa systemów informatycznych oraz wzmocnienie instrumentów ochrony i reagowania wykorzystywanych przez Ministerstwo Obrony i jego najważniejszych partnerów,
2) intensyfikacja działań w sferze badań i rozwoju,
3) właściwe wykorzystanie potencjału ludzkiego i stworzenie spójnego systemu kształcenia i zatrudnienia wyspecjalizowanych kadr,
4) rozwój centrum eksperckiego cyberobrony w Bretanii,
5) rozwój współpracy z partnerami zagranicznymi,
6) wspieranie procesu tworzenia narodowej wspólnoty cyberobrony.

2. Podstawy prawne i struktura organizacyjna systemu cyberbezpieczeństwa

Zgodnie z art. 21 przywołanej powyżej ustawy o programowaniu wojskowym na lata 2014–2019 premier, zgodnie z założeniami strategii bezpieczeństwa narodowego i polityki obrony, określa główne kierunki polityczne i koordynuje działania rządu w zakresie bezpieczeństwa i obrony systemów informatycznych. W tym celu korzysta ze wsparcia narodowej władzy bezpieczeństwa systemów informacji. Jak wskazano we wstępie, tę funkcję pełni powołana na mocy dekretu nr 2009-834 z 7 lipca 2009[24] Narodowa Agencja Bezpieczeństwa Systemów Informatycznych. Organ ten działa przy Sekretarzu Generalnym Obrony i Bezpieczeństwa Narodowego[25]. Do zadań ANSSI, zgodnie z art. 3 dekretu, należy:

- pełnienie funkcji narodowej władzy bezpieczeństwa systemów informatycznych. W tym celu przedkłada ona premierowi propozycje działań zmierzających do reagowania na sytuacje kryzysowe i zagrożenia bezpieczeństwa systemów wykorzystywanych przez organy publiczne, operatorów infrastruktury krytycznej, a także koordynuje, w ramach określonych przez premiera wytycznych, działania rządu w powyższym zakresie;

[23] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portent diverses dispositions concernant la défense et la sécurité nationale*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id [dostęp: 14 VIII 2017].

[24] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service a competence nationale dénommé "Agence nationale de la sécurité des systèmes d'information"*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 [dostęp: 14 VIII 2017].

[25] Sekretarz Generalny ds. Obrony i Bezpieczeństwa Narodowego wspiera działania premiera w zakresie obrony i bezpieczeństwa narodowego, www.sgdsn.gouv.fr [dostęp: 14 VIII 2017].

- opracowywanie, i wdrażanie międzyresortowych bezpiecznych środków komunikacji elektronicznej wykorzystywanych przez prezydenta i rząd;
- inicjowanie i koordynowanie międzyresortowych działań dotyczących bezpieczeństwa systemów informatycznych;
- opracowywanie środków ochrony systemów informatycznych, które następnie są przedstawiane premierowi, oraz nadzorowanie procesu ich stosowania przyjętych środków;
- prowadzenie inspekcji systemów informatycznych wykorzystywanych przez organy administracji publicznej i operatorów infrastruktury krytycznej;
- opracowywanie systemów wykrywania zdarzeń mogących naruszać bezpieczeństwo państwowych systemów informatycznych oraz koordynacja działań, które mają na celu przeciwdziałanie tym zdarzeniom; zbieranie informacji technicznych o incydentach dotyczących państwowych systemów informatycznych i operatorów infrastruktury krytycznej;
- wydawanie certyfikatów dopuszczających do użytku urządzenia i mechanizmy techniczne chroniące informacje objęte tzw. tajemnicą obrony (fr. *de la défense nationale*);
- udział w negocjacjach międzynarodowych oraz prowadzenie współpracy z zagranicznymi organami pełniącymi analogiczne funkcje;
- prowadzenie działalności szkoleniowej dla osób zajmujących się problematyką bezpieczeństwa systemów informatycznych.

Narodowa Agencja Bezpieczeństwa Systemów Informatycznych dokonuje ponadto oceny poziomu bezpieczeństwa urządzeń i usług niezbędnych do ochrony systemów informatycznych (art. 4). Agencja jest odpowiedzialna przede wszystkim za:

- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania; wydawanie upoważnień podmiotom, o których mowa w dekrecie nr 2010-112 z 2 lutego 2010 r.[26] (podmioty dokonujące kwalifikacji dostawców usług zaufania), po dokonaniu oceny kompetencji technicznych tych podmiotów do oszacowania bezpieczeństwa instrumentów stosowanych przez dostawców usług zaufania;
- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania, a także zatwierdzanie punktów ewaluacji przewidzianych w dekrecie nr 2015-350 z 27 marca 2015 r. o kwalifikacji urządzeń bezpieczeństwa i dostawców usług zaufania na potrzeby bezpieczeństwa narodowego[27];
- certyfikację urządzeń służących do generowania i weryfikacji podpisów elektronicznych przewidzianych w dekrecie z 30 marca 2001 r. wydanym w celu stosowania art. 1316-4 kodeksu cywilnego i dotyczącym podpisu elektronicznego[28];
- zatwierdzanie punktów ewaluacji i certyfikacji poziomu bezpieczeństwa urządzeń i systemów informatycznych, o których mowa w dekrecie z 18 kwietnia

[26] *Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9,10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&categorieLien=cid [dostęp: 14 VIII 2017].

[27] *Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405903&categorieLien=cid [dostęp: 14 VIII 2017].

[28] *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-14 du code civil et relatif à la signature électronique*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000404810&categorieLien=cid [dostęp: 14 VIII 2017].

2002 r. o ewaluacji i certyfikacji poziomu bezpieczeństwa urządzeń i systemów informatycznych[29];

- wydawanie autoryzacji i zarządzanie deklaracjami dotyczącymi środków i dostawców instrumentów kryptologicznych, o których mowa w dekrecie z 2 maja 2007 r. wydanym w celu stosowania art. 30, 31 i 36 ustawy nr 2004-575 z 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej oraz dotyczącym instrumentów kryptologicznych i ich dostarczania[30];
- wydawanie i cofanie zezwoleń, o których mowa w art. 226-3 kodeksu karnego (zezwolenia na produkcję i sprzedaż urządzeń służących do utrwalania treści rozmów i pozyskiwania danych informatycznych).

Dekret nakłada na ANSSI również ogólny obowiązek podejmowania działań mających na celu promocję problematyki związanej z bezpieczeństwem systemów informatycznych w kontekście rozwoju i opracowywania nowych technologii w tej sferze. Agencja bierze ponadto udział w badaniach naukowych mających na celu rozwój potencjału technologii informatycznych (art. 6).

Utworzenie ANSSI oraz opracowanie opisanych powyżej dokumentów strategicznych przyczyniło się do poprawy zdolności skutecznego reagowania na zagrożenia cybernetyczne i uporządkowania kompetencji organów administracji publicznej. Niemniej jednak raport[31] opracowany w 2012 r. pod kierownictwem senatora Jean -Marie'a Bockela wskazuje na występowanie licznych ograniczeń natury systemowej, które są związane zarówno ze sposobem ukształtowania kompetencji i środkami, jakimi dysponuje ANSSI, jak i z innymi aspektami funkcjonowania systemu. Pomimo upływu około pięciu lat od czasu wydania powyższego dokumentu i niewątpliwej poprawy stanu systemu cyberbezpieczeństwa we Francji, zamieszczone w nim zagadnienia oraz problemy natury strukturalnej niewątpliwie zachowują znaczenie do chwili obecnej.

Główna teza raportu Bockela sprowadza się do stwierdzenia, że pomimo niewątpliwych postępów dokonanych od chwili wydania białej księgi w 2008 r., możliwości francuskiego systemu zapobiegania i przeciwdziałania cyberzagrożeniom należy uznać za niesatysfakcjonujące[32]. Z praktycznego punktu widzenia zarówno kompetencje ANSSI, jak i instrumenty pozostające w dyspozycji Agencji są znacznie bardziej ograniczone, niż w przypadku analogicznych instytucji funkcjonujących w innych państwach europejskich, np. w Wielkiej Brytanii czy Niemczech. Zdaniem twórców raportu pomimo że Agencja ma status narodowej władzy bezpieczeństwa w odniesieniu do systemów informatycznych, zakres i sposób uregulowania jej uprawnień nie pozwalają na realne i efektywne zapewnienie jednolitego przestrzegania najważniejszych – z punktu widzenia bezpieczeństwa informatycznego – zasad.

---

[29] *Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412673&categorieLien=cid [dostęp: 14 VIII 2017].

[30] *Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646995&categorieLien=cid [dostęp: 14 VIII 2017].

[31] *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense, par M. Jean-Marie BOCKEL, Sénateur*, 18 juillet 2012, https://www.senat.fr/rap/r11-681/r11-6811.pdf [dostęp: 19 IX 2017].

[32] Tamże, s. 82.

Do najistotniejszych wad systemu skutkujących strukturalnymi ograniczeniami możliwości efektywnego realizowania zadań przez ANSSI raport Bockela zalicza niedostateczne środki, jakimi dysponuje Agencja (niedostateczna liczba pracowników i niewystarczający budżet), niski poziom wrażliwości i świadomości w sferze ochrony systemów informatycznych, zarówno w organach administracji publicznej, jak i wśród najważniejszych przedsiębiorców i operatorów infrastruktury krytycznej.

Zagadnienie ochrony systemów informatycznych wykorzystywanych przez operatorów infrastruktury krytycznej zostało określone jako najważniejszy aspekt systemu cyberbezpieczeństwa[33]. To pojęcie, zgodnie z art. R-1332-1 ustawy – Kodeks obrony, obejmuje operatorów publicznych lub prywatnych wskazanych w art. L 1332-1[34] tej ustawy oraz podmioty zarządzające przedsiębiorstwami, o których mowa w art. L 1332-2[35].

Operatorzy infrastruktury krytycznej wykonują zadania zapisane w art. R 1333-2 oraz zarządzają lub wykorzystują w tym celu przedsiębiorstwa, instalacje lub obiekty, których niedostępność lub zniszczenie w wyniku sabotażu, terroryzmu lub innych form szkodliwego działania mogłoby spowodować, bezpośrednio lub pośrednio, obniżenie potencjału gospodarczego lub wojskowego, bezpieczeństwa lub zdolności zachowania podstawowych funkcji społeczeństwa lub stworzyć poważne zagrożenie zdrowia lub życia ludności (art. R 1332-1 II pkt 2 a i b ustawy – Kodeks obrony).

Zgodnie z art. R 1332-2 tej ustawy sektor infrastruktury krytycznej, o którym mowa w art. R 1332-1, obejmuje działania dotyczące produkcji i dystrybucji dóbr lub usług niezbędnych do zaspokojenia podstawowych potrzeb ludności, wykonywania władzy państwowej, funkcjonowania gospodarki, zachowania potencjału obronnego lub bezpieczeństwa państwa, jeżeli ich zastąpienie byłoby niemożliwe lub poważnie utrudnione lub które same w sobie mogą stwarzać poważne zagrożenie. Listę sektorów infrastruktury krytycznej określa, na mocy zarządzenia, pre-

[33] Tamże, s. 86.

[34] *Code de la defense*…, art. L 1332-1:

„Operatorzy publiczni lub prywatni zarządzający przedsiębiorstwami lub wykorzystujący instalacje lub obiekty, których niedostępność spowodowałaby istotne obniżenie potencjału wojskowego lub gospodarczego, bezpieczeństwa lub zdolności zachowania podstawowych funkcji społeczeństwa, zobowiązani są do współpracy, na własny koszt, na warunkach przewidzianych w niniejszym rozdziale, w celu ochrony tych przedsiębiorstw, instalacji i obiektów przed wszelkimi rodzajami zagrożeń, zwłaszcza przed zagrożeniami o charakterze terrorystycznym. Przedsiębiorstwa, instalacje i obiekty, o których mowa w niniejszym artykule, wyznaczane są przez organ administracji publicznej" (tłum. aut.).

[35] Tamże, art. L 1332-2:

„Obowiązki przewidziane w niniejszym artykule mogą zostać rozciągnięte na przedsiębiorstwa wskazane w art. L 511-1 ustawy – Kodeks środowiska (*Code de l'environnement*) lub na przedsiębiorstwa obejmujące podstawową instalację nuklearną, o której mowa w art. L 593-1 ustawy – Kodeks środowiska, jeżeli ich zniszczenie lub awaria ich niektórych instalacji może stwarzać poważne zagrożenie dla ludności. Przedsiębiorstwa te wyznaczane są przez organ administracji publicznej" (tłum. aut.).

Art. L 511-1 ustawy – Kodeks środowiska:

„Obowiązkom wymienionym w niniejszym tytule podlegają fabryki, zakłady, składy, miejsca budowy lub, w ujęciu ogólnym, instalacje wykorzystywane przez osoby fizyczne lub prawne, publiczne lub prywatne, mogące stwarzać zagrożenie dla zdrowia publicznego, bezpieczeństwa, rolnictwa, ochrony środowiska naturalnego, racjonalnego wykorzystania energii czy dziedzictwa kulturowego" (tłum. aut.), https://www.legifrance.gouv.fr/affichCode.do;jsessionid=73175D5154B5C5F9BB10A189852B30AA.tpdila09v_2?idSectionTA=LEGISCTA000006159272&cidTexte=LEGITEXT000006074220&dateTexte=20170919 [dostęp: 19 IX 2017].

mier, po zasięgnięciu opinii Międzyresortowej Komisji Bezpieczeństwa i Obrony. To zarządzenie wskazuje również ministra koordynatora dla każdego z wyżej wymienionych sektorów, do którego zadań należy nadzór nad stosowaniem wytycznych rządu w danym sektorze.

Raport wskazuje, że systemy informatyczne wykorzystywane przez operatorów infrastruktury krytycznej są szczególnie wrażliwe i podatne na wszelkie formy zagrożeń cybernetycznych. Tej tezy dowodzą przytoczone w dokumencie przykłady ataków na instytucje lub przedsiębiorstwa najważniejsze dla funkcjonowania państwa, np. ataki na systemy informatyczne ministerstw gospodarki i finansów w grudniu 2010 r. czy ingerencja w sieci informatyczne wykorzystywane przez strategiczne przedsiębiorstwo AREVA w 2011 r.[36]

Wnioski

Ewolucja systemu bezpieczeństwa cybernetycznego we Francji, zapoczątkowana opracowaniem w 2008 r. białej księgi określającej podstawowe cele i założenia polityczne w obszarze cyberbezpieczeństwa, doprowadziła do uporządkowania organizacyjnego i legislacyjnego. Za najważniejszy element procesu tworzenia spójnego systemu zapobiegania i przeciwdziałania zagrożeniom w cyberprzestrzeni należy uznać utworzenie w 2009 r. Narodowej Agencji Bezpieczeństwa Systemów Informatycznych – centralnego organu odpowiedzialnego za bezpieczeństwo systemów informatycznych. Zarówno sposób uregulowania kompetencji tego organu, jak i środki, jakimi realnie dysponuje, zostały ocenione w raporcie Bockela jako niewystarczające do efektywnego przeciwdziałania atakom na najważniejsze dla państwa systemy informatyczne. Jedna z rekomendacji zawartych w dokumencie[37] zalecała zmianę zakresu kompetencji ANSSI przez przyznanie jej uprawnień do prowadzenia tzw. inżynierii odwrotnej (tr. *rétroconception*) stosowanej w celach związanych z bezpieczeństwem i do analizy zachowania złośliwych elementów oprogramowania. Agencja powinna także móc wykorzystywać urządzenia umożliwiające śledzenie działań podmiotów odpowiedzialnych za ataki informatyczne oraz identyfikować słabe punkty wykorzystywanych przez te podmioty urządzeń lub oprogramowania w celu podjęcia ewentualnych działań odwetowych. Dokument rekomenduje także nadanie ANSSI kompetencji umożliwiających faktyczne oddziaływanie na politykę organów administracji publicznej i operatorów infrastruktury krytycznej w zakresie bezpieczeństwa wykorzystywanych przez nich systemów informatycznych.

Biorąc pod uwagę kształt ustawowych kompetencji ANSSI, należy uznać, że mają one charakter wyłącznie defensywny. Do najważniejszych z nich zalicza się opracowywanie środków ochrony systemów informatycznych i tworzenie mechanizmów wykrywania zagrożeń w systemach i sieciach. Agencja nie dysponuje jednak instrumentami ofensywnymi pozwalającymi na aktywne zwalczanie incydentów mogących negatywnie wpływać na bezpieczeństwo systemów najistotniejszych – z punktu widzenia funkcjonowania organów państwowych czy operatorów – dla infrastruktury krytycznej.

[36] *Rapport d'information*…, s. 20–25.
[37] Tamże, s. 123.

V. MODEL SYSTEMU BEZPIECZEŃSTWA TELEINFORMATYCZNEGO ORAZ OCHRONY SIECI TELEINFORMATYCZNYCH W REPUBLICE FEDERALNEJ NIEMIEC[38]

Zgodnie z § 1 ustawy z 14 sierpnia 2009 r. o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) jest on odpowiedzialny za bezpieczeństwo informacji na poziomie krajowym. Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik – BSI) powstał na mocy ustawy z 1 stycznia 1991 r., ma siedzibę w Bonn i podlega nadzorowi Federalnego Ministerstwa Spraw Wewnętrznych (Bunderministerium des Innern). Aktualnie w Urzędzie jest zatrudnionych ok. 600 pracowników.

Celem działalności BSI jest umożliwienie bezpiecznego korzystania z technologii informacyjnych i komunikacyjnych. Pod nadzorem i przy wsparciu ze strony BSI bezpieczeństwo teleinformatyczne jest realizowane jako priorytetowe działanie w administracji, gospodarce i społeczeństwie. W tym zakresie BSI opracowuje minimalne normy i zalecenia odnoszące się do bezpieczeństwa w sieciach teleinformatycznych oraz w Internecie, które mają pomóc użytkownikom w unikaniu zagrożeń. Urząd jest również odpowiedzialny za ochronę federalnych systemów IT przed różnego typu zagrożeniami (np. wirusy lub oprogramowanie trojańskie). Co roku BSI składa sprawozdanie ze swej działalności Komisji Spraw Wewnętrznych Bundestagu.

W myśl § 3 ustawy o BSI do najważniejszych zadań tego Urzędu należy:

- ochrona sieci federalnych, wykrywanie i zapobieganie atakom na sieci rządowe;
- udostępnianie organom federalnym produktów związanych z bezpieczeństwem IT;
- testowanie, certyfikacja i akredytacja produktów i usług IT;
- ostrzeganie przed złośliwym oprogramowaniem oraz lukami bezpieczeństwa w oprogramowaniu, produktach i usługach IT;
- doradztwo w zakresie bezpieczeństwa teleinformatycznego dla administracji federalnej oraz innych grup docelowych;
- wspieranie organów federalnych odpowiedzialnych za bezpieczeństwo technologii informacyjnych, zwłaszcza gdy te organy wykonują zadania doradcze lub nadzorcze (w szczególności wspieranie Federalnego Komisarza ds. Ochrony Danych i Wolności Informacji, zgodnie z zakresem jego uprawnień);
- wspieranie:
  - policji i organów ścigania w wykonywaniu ich ustawowych obowiązków,
  - organów odpowiedzialnych za ochronę konstytucji w zakresie analizy i oceny informacji pochodzących z rozpoznawania działalności terrorystycznej lub z działań wywiadowczych zgodnych z prawem federalnym i państwowym,
  - Federalnej Służby Wywiadu w realizacji jej ustawowych zadań.

[38] Zagadnienia związane z działalnością Federalnego Urzędu Bezpieczeństwa Teleinformatycznego oraz architekturą bezpieczeństwa teleinformatycznego uregulowaną w związku z założeniami Strategii Bezpieczeństwa Cybernetycznego dla Niemiec opracowano na podstawie ustawy z 14 sierpnia 2009 r. o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego http://www.gesetze-im-internet.de/bsig_2009/index.html#BJNR282110009BJNE000101116 [dostęp: 1 VIII 2017] oraz materiałów opublikowanych na stronie internetowej Federalnego Ministerstwa Spraw Wewnętrznych www.bmi.bund.de [dostęp: 1 VIII 2017].

To wsparcie może być udzielane tylko w przypadkach, gdy konieczne jest zapobieganie działaniom skierowanym przeciw bezpieczeństwu technologii informacyjnych lub przeprowadzenie w ich sprawie śledztwa lub jeśli działania muszą być zrealizowane przy wykorzystaniu technologii informacyjnych. Urząd prowadzi rejestr takich wniosków;

- zapewnianie wsparcia i doradztwa w sprawach związanych ze środkami technicznymi i organizacyjnymi oraz przeprowadzanie testów technicznych w celu ochrony informacji niejawnych przed nieuprawnionym dostępem w myśl § 4 ustawy z 20 kwietnia 1994 r. o wymogach i zasadach postępowań sprawdzających oraz ochronie informacji niejawnych;
- informowanie i podnoszenie świadomości społecznej w zakresie bezpieczeństwa teleinformatycznego i bezpieczeństwa w Internecie;
- opracowywanie jednolitych i obowiązujących standardów bezpieczeństwa teleinformatycznego;
- tworzenie i rozwijanie systemów kryptograficznych dla teleinformatyki federalnej.

Grupami docelowymi, do których BSI kieruje swoje działania, są:

- publiczna administracja na szczeblu centralnym i lokalnym,
- przedsiębiorstwa handlowe,
- instytucje naukowe i badawcze,
- użytkownicy prywatni.

Podczas wykonywania swoich obowiązków BSI współpracuje z innymi służbami, organami i instytucjami, które dostarczają ekspertyzy oraz służą doradztwem. Współpraca jest prowadzona również na płaszczyźnie międzynarodowej.

Strategia Bezpieczeństwa Cybernetycznego dla Niemiec[39], zatwierdzona 23 lutego 2011 r. przez rząd federalny, uznaje ochronę cyberprzestrzeni za podstawowe wyzwanie XXI w., które jest ściśle związane ze współpracą w Europie oraz na świecie. W *Strategii* stworzono ramy dla międzynarodowego zaangażowania BSI, natomiast konkretne działania międzynarodowe Urzędu są związane z kierunkami jego działania. Przykładowo, w ramach Unii Europejskiej i NATO przedsięwzięcia te są realizowane w postaci standaryzacji oraz normalizacji, zarówno na szczeblu dwustronnym, jak i wielostronnym.

Federalny Urząd Bezpieczeństwa Teleinformatycznego utrzymuje kontakty z najważniejszymi międzynarodowymi firmami telekomunikacyjnymi i producentami technologii informatycznych, jest również reprezentowany w niektórych istotnych konsorcjach przemysłowych. Ponadto Urząd, w ramach realizowanych działań profilaktycznych, wymienia regularnie z innymi organami – zarówno w UE, jak też poza nią – wiedzę na temat zagadnień technicznych dotyczących bezpieczeństwa teleinformatycznego oraz bezpieczeństwa w Internecie. W ramach partnerstwa w NATO, BSI współpracuje z organami odpowiedzialnymi za techniczne zagadnienia dotyczące ochrony systemów komputerowych, m.in. z amerykańską Agencją Bezpieczeństwa Narodowego (National Security Agency – NSA). Ta współpraca dotyczy tylko profilaktycznych aspektów cyberbezpieczeństwa, zgodnie z ustawowymi obowiązkami i uprawnieniami BSI.

Konieczność współpracy międzynarodowej w zakresie bezpieczeństwa teleinformatycznego jest jednym z postulatów wspomnianej *Strategii*. Ten dokument dotyczy też innych aspektów bezpieczeństwa cybernetycznego. Jako cel nadrzędny wskazano

[39] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile [dostęp: 1 VIII 2017].

tu zapewnienie na odpowiednim poziomie ochrony połączonym siecią strukturom informatycznym, bez naruszania możliwości, jakie daje korzystanie z cyberprzestrzeni. Realizacji tej wytycznej służą następujące elementy:

- ochrona systemów informatycznych w Niemczech, szczególnie w dziedzinie infrastruktury krytycznej,
- promowanie podstawowych funkcji zabezpieczających, certyfikowanych przez państwo (np. nowy dowód osobisty, De-Mail[40]),
- podnoszenie świadomości obywateli na temat bezpieczeństwa teleinformatycznego, utworzenie Narodowego Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni (Nationalen Cyber-Abwehrzentrum – NCAZ),
- powołanie Narodowej Rady Cyberbezpieczeństwa (Nationalen Cyber-Sicherheitsrat – NCS).

Za realizację założeń *Strategii* są odpowiedzialne: Narodowe Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni oraz Narodowa Rada Cyberbezpieczeństwa. Z uwagi na rolę tych podmiotów, istotną dla całego niemieckiego systemu bezpieczeństwa teleinformatycznego, należy przybliżyć ich zadania oraz strukturę.

Narodowego Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni to płaszczyzna współpracy wybranych organów, które – zgodnie ze swoją właściwością rzeczową – opracowują i przekazują informacje związane z cyberbezpieczeństwem kraju. Pod przewodnictwem BSI tę platformę współtworzą przedstawiciele:

- Federalnego Urzędu Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV),
- Federalnego Urzędu Ochrony Ludności i Reagowania Kryzysowego (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK),
- Federalnego Urzędu Kryminalnego (Bundeskriminalamt – BKA),
- Policji Federalnej (Bundespolizei – BPol),
- Celnego Urzędu Kryminalnego (Zollkriminalamt – ZKA),
- Federalnej Służby Wywiadu (Bundesnachrichtendienst – BND),
- Bundeswehry.

Podstawą działania służb skupionych w NCAZ jest szybka wymiana informacji, tak aby wiedza pochodząca z obszaru działania poszczególnych służb procentowała w postaci wspólnych oszacowań, które dadzą możliwość dokonania analizy i podjęcia decyzji odnośnie do dalszych działań oraz zaleceń. Przedstawiciele wszystkich skupionych w NCAZ organów pracują wspólnie przy jednoczesnym, ścisłym zachowaniu swoich ustawowych uprawnień i obowiązków. Ocena incydentów cyberbezpieczeństwa jest przeprowadzana zgodnie z obowiązkami poszczególnych służb, np.:

- BSI ocenia atak z technicznego punktu widzenia,
- BfV dokonuje oceny z punktu widzenia zagrożeń wywiadowczych,
- BKA ocenia z punktu widzenia zadań policyjnych,
- BBK ocenia wpływ ataku na infrastrukturę krytyczną.

Wszystkie organy reprezentowane w NCAZ, które stanowi centrum wymiany informacji, wnoszą wkład w rozwój świadomości sytuacyjnej. W celu osiągnięcia satysfakcjonującego poziomu współpracy stworzono skuteczne kanały komunikacyjne. Podstawą pracy są codzienne briefingi oraz praca w grupach, zorganizowana tematycznie. Przedstawiciele wszystkich organów, które są niezbędne do przeciwdziałania incydentom bezpieczeństwa cybernetycznego, wymieniają i uzgadniają swoją wiedzę, a jeśli to

[40] Jest to określenie systemu opartego na technologii poczty elektronicznej.

konieczne – spotykają się także z poszkodowanym podmiotem. Istotnym elementem współpracy jest koordynacja działań.

Należy podkreślić, że powszechnie odnotowywany jest stały wzrost liczby zarówno przypadków cyberprzestępczości, jak i cyberszpiegostwa oraz cybersabotażu. Dlatego też duży wpływ na architekturę bezpieczeństwa IT ma monitorowanie incydentów bezpieczeństwa i wnioskowanie na tej podstawie o możliwych scenariuszach zagrożenia. Obowiązkowa jest również ścisła współpraca między organami bezpieczeństwa. Od początku utworzenia NCAZ przedmiotem codziennych briefingów było ok. 3700 przypadków, z czego wiedza na temat 820 meldunków została pogłębiona[41].

Zgodnie z fikcyjnym scenariuszem przedstawionym dziennikarzom w przededniu otwarcia Centrum, jego zwykły cykl pracy może wyglądać następująco:

- BSI uzyskuje informacje o luce bezpieczeństwa, której producent oprogramowania lub sprzętu nie potrafi skutecznie zabezpieczyć,
- BSI przekazuje otrzymane informacje do NCAZ,
- równocześnie BfV dowiaduje się o podjętej „próbie sabotażu", polegającej na usiłowaniu zainstalowania szkodliwego oprogramowania w placówce zaliczanej do infrastruktury krytycznej przez jej pracownika,
- BSI poddaje przedmiotowe oprogramowanie analizie technicznej,
- BSI stwierdza, że wykorzystuje ono rozpoznaną lukę bezpieczeństwa,
- pracownicy NCAZ wspólnie formułują wniosek o zaistnieniu realnego zagrożenia dla infrastruktury krytycznej,
- NCAZ ostrzega zagrożone jednostki organizacyjne, prosząc jednocześnie o informacje zwrotne.

Powyższa procedura ma zapewnić kontrolę NCAZ nad bezpieczeństwem niemieckiej cyberprzestrzeni[42]. Ten scenariusz uświadamia, że kluczowe znaczenie dla spójnego i skutecznego działania w przypadku zagrożenia ma wczesna wymiana informacji między służbami. W ocenie podmiotów nadzorujących NCAZ praca zespołu jest oceniana jako celowa i efektywna.

Jednym z założeń ujętym w Strategii było zapewnienie współpracy pomiędzy państwem a przedsiębiorcami. W celu realizacji tego postulatu została powołana Narodowa Rada Cyberbezpieczeństwa. Powołanie NCS ma służyć zauważalnej poprawie współpracy w obszarze cyberbezpieczeństwa zarówno w ramach administracji rządowej, jak i z innymi istotnymi podmiotami gospodarczymi.

W skład NCS wchodzą:

- Urząd Policji Kryminalnej,
- Ministerstwo Spraw Zagranicznych,
- Ministerstwo Obrony,
- Ministerstwo Gospodarki i Energii,
- Ministerstwo Sprawiedliwości,
- Ministerstwo Oświaty i Badań,
- Ministerstwo Finansów,
- przedstawiciele krajów związkowych Badenii-Wirtembergii oraz Hesji.

Sektor przedsiębiorczości jest natomiast reprezentowany przez:

- Federalny Związek Przemysłu Niemieckiego,

[41] Dane opublikowane w 2017 r.

[42] K. Sacewicz, *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7, s. 129.

- Stowarzyszenie Cyfrowe,
- Izbę Przemysłowo-Handlową,
- operatora przemysłu przesyłowego Amprion,
- UP-KRITIS – partnerstwo publiczno-prywatne pomiędzy operatorami infrastruktury krytycznej – ich związkiem a odpowiednimi agencjami rządowymi.

Spotkania Rady odbywają się do trzech razy w roku, a przewodzi im Pełnomocnik Rządu ds. Technologii Informacyjnych. Działania NCS przyczyniły się do tej pory do:

- wdrożenia istotnych zmian w zakresie ochrony infrastruktury krytycznej,
- skupienia na wspólnych celach działań i interesów związkowych, krajów i przemysłu,
- utworzenia spójnej cyberpolityki zagranicznej,
- podniesienia świadomości zagadnień oraz wyzwań technologicznych na wyższy szczebel polityczny.

Z uwagi na potrzebę uwzględnienia nowych wyzwań, jakie są konsekwencją stałego postępu technologii cyfrowych, 11 września 2016 r. rząd federalny wprowadził nową *Strategię Bezpieczeństwa Cybernetycznego* dla Niemiec[43]. Jest ona kontynuacją strategii zatwierdzonej w 2011 r. W nowej *Strategii Bezpieczeństwa Cybernetycznego* zostały uwypuklone cztery obszary działań:

- bezpieczne i autonomiczne działanie w przestrzeni cyfrowej (m.in. znak jakości – IT dla obywateli, prace nad nowym dowodem osobistym),
- współpraca na styku państwa i przedsiębiorczości (objęcie kolejnych branż ustawą o bezpieczeństwie IT),
- tworzenie wydajnej i trwałej państwowej architektury bezpieczeństwa cybernetycznego (utworzenie cyfrowych sił reagowania),
- aktywny udział Niemiec w europejskiej i międzynarodowej polityce bezpieczeństwa cybernetycznego.

Wraz z wdrożeniem nowej *Strategii*, Federalne Ministerstwo Gospodarki i Technologii powołało grupę roboczą ds. bezpieczeństwa teleinformatycznego w gospodarce (przedsiębiorczości), która we współpracy ze środowiskiem biznesowym podejmuje działania w ramach istniejących inicjatyw. Grupami docelowymi są przede wszystkim małe i średnie przedsiębiorstwa, które nie mają doświadczenia w zakresie bezpieczeństwa teleinformatycznego.

Udział w realizacji zadań określonych w *Strategii*, sprzyja niewątpliwie ścisłej współpracy także w innych obszarach narodowego cyberbezpieczeństwa, które należą do właściwości BSI. Do głównych zadań Federalnego Urzędu Bezpieczeństwa Teleinformatycznego należy m.in. podejmowanie prewencyjnych działań ochronnych, które mają na celu wzmocnienie bezpieczeństwa teleinformatycznego w administracji publicznej. Zgodnie z § 3 pkt 1 ustawy o BSI podstawowym zadaniem Urzędu jest zapobieganie zagrożeniom teleinformatycznych sieci federalnych. W tym kontekście należy wyróżnić pojęcie s i e c i r z ą d o w e, które oznacza infrastrukturę komunikacyjną dla niezawodnych i bezpiecznych transmisji głosu i danych między najwyższymi organami federalnymi i konstytucyjnymi w Niemczech.

Najważniejszymi stosowanymi środkami bezpieczeństwa sieci rządowych jest stałe szyfrowanie komunikacji oraz efektywna polityka bezpieczeństwa, która zapewnia ciągłe i wiarygodne funkcjonowanie komunikacji. W ramach infrastruktury technicznej wprowadzane są także modyfikacje i ulepszenia, jak również bezpieczne połączenia

[43] https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [dostęp: 2 VIII 2017].

na szczeblu administracji lokalnej. Podejmowane przez BSI działania związane z ochroną sieci rządowych są przedmiotem ciągłego rozwoju i adaptacji do pojawiających się wciąż nowych zagrożeń.

Na co dzień zadaniem BSI jest identyfikacja cyberataków na sieci rządowe oraz reakcja polegająca na: ostrzeżeniu, natychmiastowym działaniu, zapewnieniu konkretnej pomocy oraz przekazywaniu zaleceń dla podmiotów. Głównymi jednostkami odpowiedzialnymi za inicjowanie opisanych powyżej środków są: Centrum Sytuacyjne Bezpieczeństwa Teleinformatycznego (IT-Lagezentrum) oraz umieszczony w wydziale BSI Zespół Reagowania na Incydenty Komputerowe (CERT). Zadaniem Centrum Sytuacyjnego jest bieżące monitorowanie bezpieczeństwa teleinformatycznego, ukierunkowane na zapewnienie właściwej oceny potrzeby reagowania oraz podjęcia działań w odpowiedzi na incydenty związane z bezpieczeństwem teleinformatycznym. Natomiast zadaniem CERT jest ocena informacji dotyczących bezpieczeństwa systemów i sieci teleleinformatycznych, rozpoznawanie incydentów w celu zapobiegania ich rozprzestrzenianiu się oraz minimalizowanie ewentualnych skutków, a także pomoc w przywracaniu normalnego funkcjonowania.

Wykonując zadania określone w § 3 pkt 1 ustawy o BSI, Urząd ten realizuje także projekt „sieci federacji", którego zadaniem jest utworzenie jednolitej i bezpiecznej infrastruktury teleinformatycznej dla podmiotów administracji publicznej. Korzystając ze wspólnej infrastruktury, urzędy będą mogły – w zależności od potrzeb – w bezpieczny sposób połączyć wspólną siecią swoje siedziby, komunikować się drogą ponadurzędową, a także oferować np. usługi IT lub same z nich korzystać.

W zakresie telefonii komórkowej w administracji federalnej BSI jest odpowiedzialny za wskazanie odpowiednich urządzeń oraz odpowiednich wymogów ochrony dla przekazywanych informacji. Jeśli informacje nie są objęte szczególną ochroną, pracownicy administracji federalnej mogą korzystać z urządzeń zgodnie z własnym wyborem. Jednak w zakresie komunikacji mobilnej, która wymaga wyższych środków bezpieczeństwa, zaleca się stosowanie specjalnych rozwiązań zatwierdzonych przez BSI.

Urząd wykonuje ustawowe obowiązki także dzięki wiarygodnym, potwierdzonym doświadczeniem informacjom uzyskiwanym w ramach grup roboczych, komitetów i zespołów. Pośród form współpracy BSI należy wymienić: współpracę publiczno-prywatną między operatorami infrastruktury krytycznej, ich stowarzyszeniami oraz odpowiednimi agencjami rządowymi, wymianę informacji pomiędzy administracją i przedsiębiorcami za pośrednictwem krajowego Centrum Sytuacyjnego (mieszczącego się w strukturach BSI), prewencyjną oraz stanowiącą odpowiedź na ataki współpracę federalnych CERT z innymi krajowymi oraz międzynarodowymi sieciami CERT, a także współpracę z partnerami w ramach Sojuszu dla Cyberbezpieczeństwa[44]. Te informacje są uzupełniane dzięki stałemu monitorowaniu i ocenie powszechnie dostępnych źródeł informacji, takich jak serwisy informacyjne i blogi w internecie.

[44] Sojusz dla Cyberbezpieczeństwa powstał z inicjatywy BSI i został zawiązany w 2012 r. we współpracy z Federalnym Stowarzyszeniem Zarządzania Informacją, Telekomunikacją i Nowymi Mediami. Jest to związek wszystkich kluczowych podmiotów działających w obszarze cyberbezpieczeństwa w Niemczech, którego celem jest dostarczanie aktualnych, istotnych informacji na temat zagrożeń cyberbezpieczeństwa. Ta inicjatywa wspiera również wymianę informacji i doświadczeń między uczestnikami. Sojusz dla Cyberbezpieczeństwa obejmuje obecnie ponad 2000 instytucji, z czego prawie 100 to przedsiębiorstwa partnerskie. Uczestnictwo w Sojuszu jest bezpłatne i można się o nie ubiegać w każdej niemieckiej instytucji. Działania Sojuszu koncentrują się głównie na poprawie cyberbepieczeństwa w małych i średnich przedsiębiorstwach.

W związku z obowiązkiem ochrony sieci rządowych Federalny Urząd Bezpieczeństwa Teleinformatycznego, w myśl § 5 ust. 1 pkt 1 i 2 ustawy o BSI, otrzymał uprawnienie do wykorzystania zautomatyzowanych procesów do gromadzenia i oceny protokołu przesyłania danych generowanych przez operowanie federalnymi technologiami komunikacyjnymi w celu rozpoznawania, zawierania lub usuwania zakłóceń lub problemów albo w związku z atakami na federalne technologie komunikacyjne. W ramach tych uprawnień BSI może także wykorzystywać zautomatyzowane procesy do oceny danych generowanych na federalnych interfejsach w celu rozpoznania i ochrony przed szkodliwym oprogramowaniem. Urząd posiada także uprawnienie do usuwania złośliwych programów lub zapobiegania ich funkcjonowaniu, w związku z czym może uruchomić system przeciwdziałania złośliwym oprogramowaniom, aby zapobiec nieautoryzowanemu dostępowi do sieci rządowych przez zainfekowane strony internetowe, bądź może uruchomić system wykrywania szkodliwego oprogramowania.

Istotne znaczenie dla krajowego bezpieczeństwa teleinformatycznego ma obowiązek informacyjny realizowany przez BSI zgodnie z § 7 ust. 1 ustawy. Do uprawnień tej służby należy bowiem ogłaszanie ostrzeżeń o lukach w zabezpieczeniach informatycznych produktów i usług oraz ostrzeżeń przed szkodliwymi programami lub też rekomendowanie środków bezpieczeństwa albo zaleceń odnośnie do korzystania z niektórych produktów. Ostrzeżenia te mogą być wysyłane do podmiotu, którego dotyczą, lub mogą być upowszechniane, np. za pośrednictwem mediów. Producenci są informowani przed publikacją ostrzeżenia. Uprawnienie to jest realizowane przez BSI bardzo ostrożnie, gdyż publiczne ostrzeżenie BSI dla konkretnych produktów może mieć poważne konsekwencje ekonomiczne dla danego przedsiębiorstwa. Z tego względu, w ramach ustawowych uprawnień, Urząd może podjąć decyzję o nieupublicznieniu ostrzeżenia i ograniczeniu kręgu jego adresatów.

Przy omawianiu ochrony sieci teleinformatycznych, która jest wdrażana i nadzorowana przez powołaną specjalnie w tym celu służbę, nie można pominąć istotnego aspektu działalności BSI, jakim jest zadanie realizowane na podstawie art. 9 ust. 1 ustawy, tj. wykonywanie zadań krajowego organu ds. certyfikacji w zakresie bezpieczeństwa teleinformatycznego. Wraz z szansą, jaką stwarza rozwój technologiczny, wzrasta także ryzyko, stale bowiem powiększa się ilość poufnych danych przetwarzanych za pośrednictwem najnowszych technik informacyjnych. Dlatego też sprawne funkcjonowanie obszarów istotnych dla społeczeństwa zależy od niezawodności i bezpieczeństwa nowoczesnych urządzeń i systemów.

Bezpieczeństwo teleinformatyczne odgrywa zatem główną rolę w zminimalizowaniu pojawiającego się ryzyka. Z technicznego punktu widzenia funkcjonalność produktów oraz systemów teleinformatycznych nie jest jednak zrozumiała dla szerszego kręgu użytkowników. Natomiast zaufanie do technologii informacyjnych może powstać tylko wtedy, gdy użytkownicy mogą polegać na ich stosowaniu. Odnosi się to zwłaszcza do zapewnienia bezpieczeństwa danych. Jednym ze sposobów na stworzenie przejrzystości w odniesieniu do właściwości bezpieczeństwa produktów i systemów IT są badania, ocena i certyfikacja produktów oraz systemów opartych na standardowych kryteriach przez niezależne ośrodki uznane przez BSI. To właśnie ten urząd zapewnia obiektywizm i spójność oraz bezstronność badań.

Realizując to uprawnienie, BSI odgrywa także istotną rolę w rozwoju kryteriów bezpieczeństwa. Ocena techniczna produktu jest przeprowadzana po złożeniu wniosku o certyfikację w BSI, na ogół w laboratoriach akredytowanych i licencjonowanych przez

BSI. Wnioskodawca ma prawo wyboru laboratorium, któremu zostaje powierzona realizacja procedur badawczych. Laboratoria służą również doradztwem w zakresie stosowanej procedury na każdym etapie badań. Dzięki certyfikacji poziomu bezpieczeństwa dostawca produktów i usług IT może prezentować swoją ofertę w przystępny sposób. Użytkownicy certyfikowanych produktów i rozwiązań teleinformatycznych są w stanie ocenić, w jakim zakresie produkty i usługi są odpowiednie i jaki wkład będzie musiał ponieść użytkownik w związku z korzystaniem z urządzenia oraz rozwiązań, aby osiągnąć odpowiedni poziom w zakresie bezpieczeństwa IT.

Przedstawione powyżej najważniejsze zadania realizowane przez Federalny Urząd Bezpieczeństwa Teleinformatycznego zarówno w związku z ustawowymi obowiązkami, jak i w ramach wykonywania założeń *Strategii Bezpieczeństwa Teleinformatycznego*, podlegają kontroli. Stały nadzór techniczny nad Urzędem sprawuje Ministerstwo Spraw Wewnętrznych. Ponadto, zgodnie z § 5 ust. 9 ustawy o BSI, służba ta raz w roku przedkłada sprawozdanie Pełnomocnikowi Rządu Federalnego ds. Ochrony Danych i Wolności Informacji. Analogicznie – co roku Komisja Spraw Wewnętrznych Bundestagu jest informowana o stosowaniu uprawnień określonych w § 5 ustawy o BSI.

VI. REPUBLIKA WŁOSKA

1. Ogólna charakterystyka *Dyrektywy wyznaczającej wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego*

Najważniejszym obecnie aktem prawnym regulującym systemowe kwestie dotyczące obszaru cyberobrony bezpieczeństwa teleinformatycznego w Republice Włoskiej jest *Dekret Prezesa Rady Ministrów z dnia 17 lutego 2017 r. „Dyrektywa wyznaczająca wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego"* (Dz. Urz. Nr 87 z 13 kwietnia 2017 r.)[45], zwany dalej „dekretem". Zastąpił on poprzedni dekret Prezesa Rady Ministrów z 24 stycznia 2013 r., który do tej pory regulował architekturę cyberbezpieczeństwa Republiki Włoskiej[46] Niniejszy dekret został wydany w celu implementacji do krajowego porządku prawnego we Włoszech artykułu 7 ust. 1 *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. Urz. UE z 2016 r. L nr 194, s. 1), który nakazuje państwom członkowskim Unii Europejskiej przyjęcie krajowej strategii w zakresie bezpieczeństwa systemów i sieci teleinformatycznych.

Dekret składa się z 13 artykułów. Artykuł 1 określa przedmiot jego regulacji, artykuł 2 – definicje występujących w nim pojęć, artykuły od 3 do 12 regulują obowiązki poszczególnych podmiotów państwowych i prywatnych, artykuł 13 natomiast zawiera przepisy przejściowe i końcowe.

Zgodnie z art. 1 ust. 1 dekret definiuje w jednolity i zintegrowany sposób architekturę instytucjonalną dedykowaną ochronie bezpieczeństwa narodowego w odniesieniu do materialnych i niematerialnych aspektów infrastruktury krytycznej, ze szczególnym

[45] http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html [dostęp: 2 VIII 2017].

[46] http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-security-approvato-nuovo-decreto.html [dostęp: 2 VIII 2017].

uwzględnieniem narodowej cyberobrony i bezpieczeństwa informatycznego. Wskazuje jednocześnie zadania przypisane wszystkim jej komponentom, a także mechanizmy i procedury wymagające stosowania w celu zmniejszenia podatności, zapobiegania różnego rodzaju ryzyku oraz adekwatnej odpowiedzi na ataki i niezwłocznego przywracania funkcjonalności systemów w sytuacji kryzysowej.

Co ważne – ustęp 2 art. 1 dekretu wskazuje, że podmioty uczestniczące w architekturze instytucjonalnej narodowej cyberobrony i bezpieczeństwa informatycznego działają w ramach kompetencji już przyznanych im w aktach rangi ustawowej. Dekret nie przyznaje samoistnie żadnych nowych kompetencji żadnym podmiotom, stanowi więc w istocie instrument tzw. miękkiego prawa. W preambule wskazano wiele przepisów i aktów prawnych przyznających podmiotom objętym zakresem dekretu kompetencje w zakresie bezpieczeństwa informatycznego i cyberobrony. Wśród przytoczonych aktów prawnych na pierwszym miejscu wymieniono ustawę nr 124 z 3 sierpnia 2007 r. ustanawiającą system informacyjny na rzecz bezpieczeństwa Republiki i nowy reżim ochrony tajemnicy państwowej, zmienioną ustawą nr 133 z 7 sierpnia 2012 r., a zatem kluczowy akt prawny regulujący funkcjonowanie służb specjalnych we Włoszech. Art. 1 ust. 3-bis wymienionej ustawy upoważnia Prezesa Rady Ministrów, po zasięgnięciu opinii Międzyresortowego Komitetu Bezpieczeństwa Republiki, do wydawania Departamentowi Informacji Bezpieczeństwa oraz służbom informacyjnym dyrektyw na rzecz wzmocnienia aktywności informacyjnej w zakresie ochrony materialnej i niematerialnej infrastruktury krytycznej, ze szczególnym uwzględnieniem narodowej obrony cybernetycznej oraz bezpieczeństwa informacyjnego.

Przepis art. 1 ust. 3 dekretu przewiduje, że jego celem jest stworzenie systemu organizacyjno-funkcjonalnego dążącego do pełnej integracji działań podejmowanych w ramach kompetencji różnych podmiotów, takich jak: Ministerstwo Rozwoju Ekonomicznego, Agencja na Rzecz Cyfrowych Włoch oraz Ministerstwo Obrony – w zakresie ochrony systemów i sieci oraz prowadzenia operacji wojskowych w cyberprzestrzeni, Ministerstwo Spraw Wewnętrznych – w zakresie działań nakierowanych na przeciwdziałanie i zwalczanie przestępczości informatycznej, obronę cywilną i ochronę ludności. Innymi słowy – celem dekretu jest stworzenie systemu krajowej cyberobrony, z jasnym podziałem zadań i kompetencji między poszczególnymi organami administracji rządowej a innymi podmiotami. Należy zwrócić uwagę na brak wskazania jednego organu odpowiedzialnego za cyberbezpieczeństwo kraju; zamiast tego wskazano główną rolę kilku instytucji odpowiedzialnych za różne sfery administracji. Można zatem stwierdzić, że Włochy przyjęły model rozproszonej odpowiedzialności za bezpieczeństwo informatyczne kraju.

2. Definicje

Z definicji zawartych w art. 2 dekretu można przytoczyć następujące:

- przestrzeń cybernetyczna – zespół wzajemnie połączonych infrastruktur informatycznych, złożony zarówno z urządzeń, oprogramowania, danych i użytkowników, jak i powiązań logicznych między nimi, niezależnie od ich trwałości (art. 2 ust. 1 lit. h),
- bezpieczeństwo cybernetyczne – stan, w którym przestrzeń cybernetyczna jest chroniona dzięki przyjęciu odpowiednich środków bezpieczeństwa fizycznego, logicznego i proceduralnego, w odniesieniu do zdarzeń natury umyśl-

nej lub przypadkowej, polegających na nieuprawnionym przejęciu lub transferze danych, ich bezprawnej modyfikacji lub zniszczeniu, nieuprawnionym przejęciu kontroli, uszkodzeniu, zniszczeniu lub zablokowaniu normalnego funkcjonowania systemów i sieci informatycznych oraz ich kluczowych elementów (art. 2 ust. 1 lit. f),

- zagrożenie cybernetyczne – zbiór zachowań, które mogą być realizowane w przestrzeni cybernetycznej lub za jej pośrednictwem, lub na jej szkodę, lub konstytuujących ją elementów, czego przejawem są przede wszystkim działania jednostek lub organizacji – państwowych i niepaństwowych, publicznych i prywatnych, nakierowane na nieuprawniony dostęp i transfer danych, ich bezprawną modyfikację lub zniszczenie, lub na nieuprawnione przejęcie kontroli, uszkodzenie, zniszczenie lub wstrzymanie regularnego funkcjonowania systemów i sieci informatycznych oraz ich elementów konstytutywnych (art. 2 ust. 1 lit. l),
- zdarzenie cybernetyczne – istotne wydarzenie natury umyślnej lub przypadkowej, polegające na nieuprawnionym dostępie lub przekazaniu danych, ich nieuprawnionej modyfikacji lub zniszczeniu lub zablokowaniu regularnego funkcjonowania sieci i systemów teleinformatycznych oraz ich elementów konstytutywnych (art. 2 ust. 1 lit. m),
- sytuacja kryzysu cybernetycznego – sytuacja, w której zdarzenie cybernetyczne przyjmuje takie rozmiary, intensywność lub charakter, że oddziałuje na bezpieczeństwo narodowe albo nie może być opanowane po zastosowaniu zwykłych kompetencji działających pojedynczo właściwych organów, lecz wymaga podjęcia decyzji koordynacyjnych na szczeblu międzyministerialnym (art. 2 ust. 1 lit. o).

3. Uprawnienia i obowiązki poszczególnych podmiotów

3.1. Prezes Rady Ministrów

Artykuł 3 dekretu mówiący o kompetencjach Prezesa Rady Ministrów odnosi je do jego roli jako osoby odpowiedzialnej za politykę rządu oraz zwierzchnika Systemu Informacyjnego na rzecz Bezpieczeństwa Republiki. Ten przepis przewiduje, że w celach ochrony bezpieczeństwa narodowego w cyberprzestrzeni premier:

- w sytuacjach kryzysowych dotyczących bezpieczeństwa narodowego zwołuje Komitet Międzyministerialny na rzecz Bezpieczeństwa Republiki (CISR),
- przyjmuje i aktualizuje, na wniosek CISR, Narodowe Ramy Strategiczne Bezpieczeństwa Cybernetycznego, zawierające: wskazanie profili i tendencji ewolucji zagrożeń oraz podatności systemów i sieci o znaczeniu narodowym, zdefiniowanie roli i zadań różnych podmiotów, publicznych i prywatnych, działających zarówno w kraju, jak i za granicą, identyfikację instrumentów i procedur, których stosowanie ma zwiększyć zdolności kraju w zakresie zapobiegania i odpowiedzi w odniesieniu do zdarzeń w cyberprzestrzeni, również pod kątem upowszechniania kultury bezpieczeństwa,
- przyjmuje, na wniosek CISR, Narodowy Plan Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego zawierający cele i czynności wymagające podjęcia w celu realizacji narodowych ram strategicznych bezpieczeństwa informacyjnego,

- wydaje dyrektywy i inne akty niezbędne do wdrożenia Planu Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego,
- wydaje, po zasięgnięciu opinii CISR, dyrektywy dla Departamentu Informacyjnego Bezpieczeństwa i dla agencji informacyjnych.

3.2. Komitet Międzyministerialny na Rzecz Bezpieczeństwa Republiki

Jest to ciało o charakterze doradczo-konsultacyjnym obsługujące funkcje Prezesa Rady Ministrów. Do jego kompetencji zalicza się przedkładanie premierowi projektu Narodowych Ram Strategicznych Bezpieczeństwa Cybernetycznego, Narodowego Planu Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego oraz opracowywanie dla organów wywiadowczych wytycznych w zakresie cyberobrony i bezpieczeństwa informatycznego.

Komitet Międzyministerialny na rzecz Bezpieczeństwa Republiki w wykonywaniu swoich zadań w obszarze cyberbezpieczeństwa jest wspierany przez tzw. Techniczny CISR – organ kolegialny niższego szczebla, któremu przewodniczy dyrektor DIS. Techniczny CISR przygotowuje posiedzenia właściwego CISR poświęcone problematyce bezpieczeństwa cybernetycznego, zapewnia wsparcie eksperckie, weryfikuje wprowadzanie w życie działań przewidzianych przez Narodowy Plan Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego, a także skuteczność procedur mających zapewnić koordynację między działaniami podmiotów publicznych i prywatnych. Ponadto koordynuje – w zakresie zaaprobowanym przez CISR i we współpracy z urzędami administracji, agencjami wywiadowczymi, Centrum Cyberbezpieczeństwa i operatorami prywatnymi – tworzenie zarówno zaleceń mających na celu polepszenie rozpoznawania zagrożeń bezpieczeństwa w cyberprzestrzeni i wykrywania podatności, jak i przyjmowania dobrych praktyk w zakresie bezpieczeństwa.

3.3. Dyrektor generalny Departamentu Informacyjnego Bezpieczeństwa

Artykuł 6 dekretu zawiera dość ogólną regulację, zgodnie z którą dyrektor generalny DIS, w celu osiągnięcia celów tego dekretu w zakresie bezpieczeństwa narodowego, podejmuje inicjatywy konieczne do zdefiniowania kierunków niezbędnych działań w interesie ogólnym, dla osiągnięcia celu polegającego na podniesieniu i polepszeniu poziomów bezpieczeństwa systemów i sieci. Realizując to zadanie ma dążyć przede wszystkim do identyfikacji i udostępniania najbardziej adekwatnych i zaawansowanych technologicznie środków wsparcia dla funkcji przygotowania do działań w zakresie zapobiegania, przeciwdziałania i reakcji w sytuacji kryzysu cybernetycznego ze strony organów administracji, podmiotów publicznych i operatorów prywatnych, o których mowa w art. 11 dekretu.

3.4. Podmioty Systemu Informacyjnego Bezpieczeństwa

Artykuł 7 ust. 1 – *Organizacje informacyjne bezpieczeństwa* – wskazuje, że zarówno DIS, jak i służby specjalne (AISI i AISE) prowadzą działalność w obszarze bezpieczeństwa cybernetycznego, posługując się instrumentami przewidzianymi w ustawie nr 124 z 2007 r. oraz w trybie i zgodnie z procedurami określonymi w przepisach tej ustawy.

W tym zakresie dyrektor generalny DIS, na podstawie dyrektyw premiera wydanych zgodnie z art. 1 ust. 3-bis ustawy nr 124 z 2007 r. oraz w świetle ogólnych kierunków oraz podstawowych celów zidentyfikowanych przez CISR, prowadzi koordynację pozyskiwania informacji, nakierowanych na wzmocnienie narodowej obrony cybernetycznej i bezpieczeństwa informacyjnego. Odpowiednie komórki DIS wspierają dyrektora generalnego w wykonywaniu tych funkcji. DIS opracowuje analizy, ewaluacje i prognozy odnoszące się do zagrożeń cybernetycznych. Zapewnia też przekazywanie organom administracji publicznej oraz innym podmiotom, także prywatnym, informacji istotnych dla bezpieczeństwa cybernetycznego i współdzielenie się tego rodzaju informacjami w obszarze właściwości Centrum Cyberbezpieczeństwa.

Zgodnie z art. 7 ust. 4 dekretu do kompetencji Agencji Informacyjnych Bezpieczeństwa (AISI i AISE) zalicza się poszukiwanie i opracowywanie informacji odnoszących się do narodowej cyberobrony i bezpieczeństwa informatycznego, zgodnie z kierunkami zdefiniowanymi w dyrektywach premiera oraz wytycznych koordynacyjnych w zakresie pozyskiwania informacji, ustalonych przez dyrektora generalnego DIS.

W celu udoskonalania potencjału w zakresie działań na rzecz cyberbezpieczeństwa DIS i agencje wywiadowcze AISI i AISE wymieniają informacje z organami administracji publicznej, upoważnionymi podmiotami służb publicznych, uniwersytetami, ośrodkami badawczymi, zawierając w tym celu stosowne porozumienia (podstawą prawną do zawierania tego rodzaju porozumień jest art. 13 ust. 1 ustawy nr 124 z 2007 r.). W tym samym celu te służby mogą uzyskiwać dostęp do baz danych organów administracji publicznej i służb publicznych. Procedura uzyskiwania takiego dostępu jest określona w art. 13 ust 2 ustawy nr 124 z 2007 r.

Zgodnie z ustępem 6 art. 7 dekretu DIS wdraża wszelkie inicjatywy na rzecz promocji i upowszechniania wiedzy i świadomości co do istoty różnych rodzajów ryzyka pochodzących z zagrożeń cybernetycznych oraz środków ochrony przed nimi.

3.5. Centrum Cyberbezpieczeństwa

Centrum Cyberbezpieczeństwa (Nucleo per la sicurezza cibernetica) jest instytucją wspierającą premiera i CISR w sprawach dotyczących bezpieczeństwa cyberprzestrzeni, w zakresie spraw odnoszących się do zapobiegania i przygotowania do wystąpienia ewentualnych sytuacji kryzysowych i uruchamiania procedur alarmowych. Odnosząc się do umiejscowienia organizacyjnego Centrum Cyberbezpieczeństwa, art. 8 ust. 1 dekretu stanowi, że działa ono przy Departamencie Informacji Bezpieczeństwa. Centrum jest kierowane przez wyznaczonego przez dyrektora generalnego DIS zastępcę dyrektora DIS, a składa się z Doradcy Wojskowego oraz przedstawicieli: DIS, AISI, AISE, Ministerstwa Spraw Zagranicznych, Ministerstwa Spraw Wewnętrznych, Ministerstwa Obrony, Ministerstwa Sprawiedliwości, Ministerstwa Rozwoju Gospodarczego, Ministerstwa Gospodarki i Finansów, Departamentu Obrony Cywilnej i Agencji na Rzecz Cyfrowych Włoch (art. 8 ust. 2). W zakresie spraw odnoszących się do przetwarzania informacji niejawnych w pracach Centrum uczestniczy przedstawiciel Centralnego Urzędu Ochrony Informacji Niejawnych (Ufficio centrale per la segretezza).

Członkom Centrum mogą towarzyszyć w posiedzeniach inni pracownicy delegujących ich urzędów. Dopuszczalne jest również zapraszanie do udziału w posiedzeniach przedstawicieli innych organów administracji, uniwersytetów, ośrodków badawczych, a także prywatnych operatorów, jeśli uzasadnia to tematyka spotkania.

Centrum zbiera się przynajmniej raz w miesiącu na wniosek przewodniczącego, którym jest wicedyrektor DIS, lub co najmniej jednego z członków. Z przeprowadzonych czynności Centrum składa sprawozdanie dyrektorowi generalnemu DIS, a ten przekazuje stosowne informacje premierowi i CISR.

Szczegółowy zakres zadań Centrum został określony w art. 9 dekretu. Najważniejszym zadaniem jest zapewnienie łączności między różnymi komponentami architektury instytucjonalnej cyberbezpieczeństwa, które z różnych tytułów podejmują działania w obszarze cyberbezpieczeństwa. Jako zadania Centrum w zakresie przeciwdziałania i przygotowania do wystąpienia sytuacji kryzysu cybernetycznego w dekrecie wymienia się:

- wspieranie opracowywania planów i programów operacyjnych reagowania w sytuacjach kryzysu cybernetycznego przez urzędy administracji i zainteresowanych operatorów prywatnych oraz wypracowanie niezbędnych procedur koordynacji międzyresortowej,
- utrzymywanie służby dyżurnej działającej 24 godziny na dobę siedem dni w tygodniu, właściwej do alarmowania i reagowania w sytuacji wystąpienia kryzysu cybernetycznego,
- ewaluację i wsparcie, w uzgodnieniu z organami administracji odpowiedzialnymi za poszczególne zagadnienia z obszaru cyberbezpieczeństwa, bez uszczerbku dla procedur wymiany informacji między informacyjnymi organami bezpieczeństwa, procedur dzielenia się informacjami, a także z zainteresowanymi operatorami prywatnymi – w celu rozpowszechniania systemu alertów dotyczących zdarzeń cybernetycznych i zarządzania kryzysowego,
- przyjmowanie zawiadomień o przypadkach naruszenia lub próbach naruszenia bezpieczeństwa oraz o przypadkach utraty integralności systemów i sieci od Ministerstwa Rozwoju Gospodarczego, od organów informacyjnych w zakresie bezpieczeństwa, od służb policyjnych, szczególnie od CNAIPIC[47],
- wsparcie i koordynacja, w uzgodnieniu z Ministerstwem Rozwoju Gospodarczego i Agencją na rzecz Cyfrowych Włoch, w zakresie ich właściwości, prowadzenia ćwiczeń międzyresortowych, a także uczestnictwa Włoch w ćwiczeniach międzynarodowych, odnoszących się do symulacji zdarzeń cybernetycznych,
- utrzymywanie narodowego punktu kontaktowego do spraw wymiany raportów z ONZ, NATO i UE, innymi organizacjami międzynarodowymi i innymi państwami.

Jako kompetencje Centrum w zakresie odpowiedzi i usuwania skutków kryzysu cybernetycznego dekret wymienia:

- przyjmowanie, również z zagranicy, sygnałów na temat zdarzeń cybernetycznych i dystrybucję alertów do organów administracji i operatorów prywatnych, w celu wykonania planów działania,
- dokonywanie oceny, czy zagrożenie przyjmuje rozmiary, intensywność lub naturę, które uniemożliwiają zaradzenie mu przez jeden właściwy organ przy użyciu zwyczajnych środków, czy też wymaga podjęcia decyzji koordynacyjnych na szczeblu międzyministerialnym, zapewniając w takim wypadku wdrożenie przewidzianych prawem środków współdziałania i koordynacji,

[47] CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – Narodowe Centrum Zwalczania Przestępczości Informatycznej w Celu Ochrony Infrastruktury Krytycznej – organ posiadający wyłączną właściwość w zakresie zapobiegania i zwalczania przestępstw informatycznych przeciwko informatycznej infrastrukturze krytycznej, które mają znaczenie ogólnokrajowe, stanowiący część *Polizia Postale* – Policji Pocztowej, https://www.commissariatodips.it/profilo/cnaipic.html [dostęp: 10 VIII 2017].

- informowanie we właściwym czasie premiera, za pośrednictwem dyrektora generalnego DIS, o bieżącej sytuacji.

Centrum opracowuje również raporty na temat stosowania środków koordynacji w zakresie przeciwdziałania i zarządzania sytuacją kryzysową i przekazuje je technicznemu CISR.

3.6. Zarządzanie kryzysem cybernetycznym

Zgodnie z art. 10 w celu zarządzania kryzysem cybernetycznym Centrum zbiera się w składzie dostosowanym do aktualnych potrzeb – jego skład może zostać poszerzony o upoważnionych przedstawicieli: Ministerstwa Zdrowia, Ministerstwa Infrastruktury i Transportu, Departamentu Straży Pożarnej, pogotowia ratunkowego, obrony cywilnej, w tym Międzyministerialnego Komitetu Technicznego Obrony Cywilnej (CIDTC) oraz Biura Doradcy Wojskowego Prezesa Rady Ministrów. Upoważnionym przedstawicielom mogą towarzyszyć inni pracownicy zatrudniających ich organów. Do udziału w posiedzeniach można wzywać również upoważnionych przedstawicieli innych władz i instytucji, także lokalnych, i operatorów prywatnych, do których odnosi się art. 11 dekretu, oraz ewentualnie innych zainteresowanych podmiotów. Centrum może spotykać się także, jeśli istnieje taka potrzeba, w składzie zawężonym do podmiotów zainteresowanych tematyką spotkania.

Zadaniem Centrum działającego w składzie w sytuacji zarządzania kryzysowego, jest zapewnienie, aby zadania w zakresie reakcji i stabilizacji, które pozostają w kompetencjach różnych podmiotów, były wykonywane w sposób skoordynowany, zgodnie z planami i programami opracowanymi przez Centrum, a w zakresie technicznych aspektów reakcji – były oparte na planach informatycznych i telematycznych[48] narodowego CERT-u, działającego przy Ministerstwie Rozwoju Gospodarczego i innych CERT-ów działających na podstawie obowiązujących norm (w tym CERT przy Agencji na rzecz Cyfrowych Włoch).

Centrum przekazuje systematycznie premierowi, za pośrednictwem dyrektora generalnego DIS, bieżące informacje na temat rozwoju sytuacji kryzysowej, zapewnia koordynację wdrażania zarządzeń premiera, które mają na celu przezwyciężenie kryzysu na szczeblu międzyresortowym, zbiera wszelkie dane niezbędne do przezwyciężenia kryzysu, wytwarza raporty i dostarcza informacji na temat kryzysu oraz przekazuje je zainteresowanym podmiotom publicznym i prywatnym. Zapewnia również współdziałanie z odpowiednimi instytucjami innych krajów, NATO, UE i organizacji międzynarodowych, których członkiem są Włochy.

3.7. Obowiązki operatorów prywatnych

Artykuł 11 dekretu reguluje obowiązki operatorów prywatnych na rzecz cyberbezpieczeństwa. Jego zakresem są objęte następujące kategorie operatorów: dostawcy

[48] Telematyka – dyscyplina zajmująca się przekazem cyfrowej informacji multimedialnej (audio, video, grafika, dane) za pośrednictwem sieci teleinformatycznych oraz przygotowaniem, gromadzeniem i udostępnianiem tego rodzaju informacji w formie usług teleinformatycznych; termin w obecnym znaczeniu wylansowany przez Komisję Europejską w latach 1994–1998, gdy w ramach IV Programu Ramowego realizowano program zastosowań telematyki w różnych dziedzinach życia publicznego, gospodarki i nauki jako Telematics Applications Programme; znaczącym obszarem zastosowań telematyki jest sektor środowiska, https://pl.glosbe.com/it/pl/telematica [dostęp: 10 VIII 2017].

publicznych sieci, dostawcy publicznie dostępnych usług, operatorzy kluczowych usług i dostawcy usług cyfrowych wymienionych w załączniku III do dyrektywy 2016/1148 (internetowe platformy handlowe, wyszukiwarki internetowe i usługi przetwarzane w chmurze), gestorzy infrastruktury krytycznej o znaczeniu krajowym i europejskim, której działanie jest uzależnione od działania systemów informatycznych i telematycznych.

Do ich obowiązków zaliczono w dekrecie:

- przekazywanie do Centrum Cyberbezpieczeństwa, z wykorzystaniem chronionych kanałów łączności, informacji o każdym istotnym naruszeniu bezpieczeństwa lub integralności systemów informatycznych,
- przyjęcie najlepszych praktyk i środków nakierowanych na ochronę cyberbezpieczeństwa, opracowanych przez techniczny CISR,
- dostarczanie informacji służbom bezpieczeństwa informacyjnego, a także umożliwianie im dostępu do Centrów Operacji Bezpieczeństwa (Security Operations Center) oraz innych archiwów informatycznych – w celu ochrony cyberbezpieczeństwa,
- współpracę w zarządzaniu kryzysami cybernetycznymi, co przyczynia się do przywracania funkcjonalności systemów i sieci pozostających w ich gestii.

W art. 11 ustęp 2 zawarto zapis, że minister rozwoju gospodarczego powołuje narodowe centrum ewaluacji i certyfikacji, które bada warunki bezpieczeństwa oraz podatność produktów, urządzeń i systemów używanych do zapewnienia funkcjonowania sieci, systemów i infrastruktury krytycznej, z zastrzeżeniem przepisów o ochronie informacji niejawnych[49].

4. Podsumowanie

Włoski system cyberbezpieczeństwa opisany w *Dyrektywie wyznaczającej wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego* jest przykładem systemu rozproszonej odpowiedzialności. Włochy nie zdecydowały się na powołanie centralnego urzędu odpowiedzialnego za bezpieczeństwo cybernetyczne kraju, obarczając odpowiedzialnością za to zagadnienie różne urzędy administracji. Centralnym punktem systemu jest automatycznie Prezes Rady Ministrów, który jest odpowiedzialny za całość administracji rządowej. Premiera wspierają ciała kolegialne złożone z przedstawicieli różnych podmiotów, mające zapewnić koordynację działań administracji w tym obszarze.

W systemie cyberbezpieczeństwa Republiki Włoskiej przewidziano istotną rolę dla podmiotów Systemu Informacyjnego Bezpieczeństwa, który tworzą agencje wywiadowcze AISI i AISE oraz koordynujący ich działalność Departament Informacyjny Bezpieczeństwa. Dotyczy to zwłaszcza DIS, który zapewnia funkcjonowanie Centrum Cyberbezpieczństwa – ciała o charakterze po części koordynacyjnym, po części informacyjnym, a po części opniodawczo-doradczym, posiadającego szczególne kompetencje w zakresie zarządzania sytuacją kryzysu cybernetycznego.

Samym służbom wywiadowczym AISI i AISE poza uczestnictwem w pracach Centrum Cyberbezpieczeństwa przypisano głównie klasyczne funkcje analityczno-informacyjne, nakierowane na wspieranie organów decyzyjnych.

[49] http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html [dostęp: 2 VIII 2017].

VII. CHARAKTERYSTYKA NAJWAŻNIEJSZYCH PROBLEMÓW ZWIĄZANYCH Z WYMIANĄ INFORMACJI O ZAGROŻENIACH CYBERBEZPIECZEŃSTWA W USA NA PRZYKŁADZIE USTAWY *CYBERSECURITY ACT OF 2015*

Dnia 18 grudnia 2015 r. ówczesny Prezydent USA Barack Obama podpisał ustawę *Cybersecurity Act of 2015*[50] określaną jako najważniejszy przyjęty do tej pory w Stanach Zjednoczonych federalny akt normatywny dotyczący cyberberpieczeństwa. Głównym elementem ustawy jest stworzenie dobrowolnego mechanizmu wymiany informacji o zagrożeniach bezpieczeństwa systemów i sieci informatycznych między jednostkami federalnymi, a także podmiotami należącymi do sektora prywatnego a tymi jednostkami. Ustawa wprowadza również przepisy wyłączające odpowiedzialność podmiotów prywatnych za ewentualne szkody związane z przekazaniem informacji w trybie wynikającym z ustawy oraz autoryzuje podejmowanie przez jednostki – zarówno publiczne, jak i prywatne – działań związanych z monitorowaniem niektórych systemów informatycznych i stosowaniem instrumentów defensywnych do celów zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Ten akt wprowadza również przepisy mające na celu osiągnięcie wyższego poziomu skuteczności środków ochronnych wykorzystywanych przez agencje federalne oraz poprawę gotowości najważniejszych systemów i sieci informatycznych do skutecznego reagowania na ewentualne zagrożenia[51].

Celem ustawodawcy było zatem stworzenie podstaw prawnych dobrowolnego przekazywania informacji mającego zachęcać podmioty publiczne i prywatne do wymiany informacji o zagrożeniach cyberbezpieczeństwa, bez nieuzasadnionych ograniczeń prawnych i perspektywy odpowiedzialności na gruncie cywilnym oraz karnym, za przekazanie tego rodzaju informacji. Jednocześnie ustawa dąży do zapewnienia wysokiego poziomu ochrony danych osobowych i innych informacji niezwiązanych z omawianymi zagrożeniami. Skuteczność przewidzianych w ustawie mechanizmów w dużej mierze będzie zależeć od woli i inicjatywy podmiotów posiadających informacje o zagrożeniach cyberbezpieczeństwa. Hipotetycznie można zakładać, że nadanie przewidzianym w ustawie instrumentom dobrowolnego charakteru miało zwiększyć szanse na realizację jednego z najważniejszych celów *Cybersecurity Act of 2015*, deklarowanego w uzasadnieniu ustawy – osiągnięcia większego poziomu współpracy w sferze cyberbezpieczeństwa pomiędzy organami państwa a podmiotami prywatnymi z uwagi na eskalację zagrożeń w tym zakresie[52].

1. Geneza ustawy

W ciągu ostatnich 20 lat informacje dotyczące potencjalnych zagrożeń i ataków cybernetycznych były wymieniane za pośrednictwem tzw. Centrów Wymiany i Analizy

[50] Tekst ustawy dostępny na stronie https://www.dni.gov/index.php/ic-legal-reference-book/cybersecurity-act-of-2015 [dostęp: 22 IX 2017].

[51] *Congress Passes and President Signs Long Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector*, Sullivan&Cromwell LLP, https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf [dostęp:16 IX 2017].

[52] *Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015*, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf [dostęp: 19 IX 2017].

Informacji (Information Sharing and Analysis Center – ISAC)[53]. Te podmioty zostały utworzone w 1998 r. na podstawie prezydenckiej dyrektywy nr 63 z 22 maja 1998 r. o ochronie infrastruktury krytycznej[54]. W dokumencie podkreślano konieczność opracowania skutecznego systemu ochrony infrastruktury krytycznej, w tym najważniejszych systemów i sieci informatycznych przez stworzenie mechanizmów pozwalających na efektywną neutralizację zarówno fizycznych, jak i cybernetycznych ataków i innych form nielegalnego oddziaływania na te systemy. Centra miały odgrywać rolę mechanizmu umożliwiającego zbieranie, analizowanie i przekazywanie informacji mogących mieć istotne znaczenie dla podmiotów sektora prywatnego oraz dla Narodowego Centrum Ochrony Infrastruktury (National Infrastructure Protection Center – NIPC)[55] – z punktu widzenia cyberbezpieczeństwa. Do zadań ISAC miało również należeć przesyłanie podmiotom sektora prywatnego informacji uzyskanych od NIPC.

Pomimo rosnącego znaczenia centrów ISAC, podmioty zaangażowane w proces wymiany informacji za ich pośrednictwem oraz eksperci z zakresu cyberbezpieczeństwa argumentowali, że potencjalne czynniki ryzyka związane z wymianą informacji za pośrednictwem ISAC, dotyczące np. odpowiedzialności cywilnej za udostępnienie niezgodne z prawem danych czy ochrony własności intelektualnej, powodują, że efektywność wymiany informacji za pośrednictwem wymienionych organów była ograniczona. W celu neutralizacji tych problemów prezydent podpisał tzw. *Executive Order 13691*[56] w celu wzmocnienia i wspierania tej wymiany zarówno w sektorze prywatnym, jak i między podmiotami sektora prywatnego a organami administracji. Dokument przewidywał utworzenie, ISAO (Information Sharing and Analysis Organizations) – podmiotów odpowiedzialnych za tworzenie tzw. dobrych praktyk w omawianym zakresie oraz doprecyzował zakres kompetencji i sposób działania National Cybersecurity and Communications Integration Center – NCICC – agencji wchodzącej w skład Departamentu Bezpieczeństwa Wewnętrznego (Department of Homeland Security), odpowiedzialnej za koordynację i wymianę informacji zarówno między poszczególnymi jednostkami rządu federalnego, jak i między tymi jednostkami a podmiotami niewchodzącymi w skład administracji rządowej[57].

Przyjęcie ustawy *Cybersecurity Act of 2015* było poprzedzone licznymi inicjatywami legislacyjnymi, które miały stanowić odpowiedź organów federalnych na coraz liczniejsze przypadki ataków cybernetycznych czy szpiegostwa przemysłowego, skutkujących kradzieżą informacji handlowych, własności intelektualnej czy nieuprawnionym dostępem do wrażliwych informacji wytwarzanych i przetwarzanych przez poszczególne organy administracji publicznej. Rok 2014 był określany mianem „*cyber breach*" – spadek poziomu bezpieczeństwa informacji przetwarzanych w systemach i sieciach informatycznych postrzegano jako czynnik poważnie zagrażający bezpieczeństwu organów państwa oraz interesom podmiotów prywatnych, kluczowych z punktu widzenia bezpieczeństwa gospodarczego[58].

[53] Tamże.

[54] *Presidential Decision Directive/NSC-63*, May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm [dostęp: 16 IX 2017].

[55] Zgodnie z dyrektywą nr 63 w skład NIPC wchodzili funkcjonariusze FBI, Secret Service i innych organów mających istotne doświadczenie w zakresie zwalczania przestępstw informatycznych, a także przedstawiciele Departamentu Obrony i tzw. wspólnoty wywiadowczej (Intelligence Community). Zadaniem NIPC było przesyłanie innym podmiotom ostrzeżeń o zagrożeniach cyberbezpieczeństwa oraz dokonywanie analiz tego rodzaju zagrożeń.

[56] *Executive Order of February 13*, 2015, https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing [dostęp: 16 IX 2017].

[57] *Congress Passes and President Signs*…, s. 2.

[58] U.*S. House of Representatives Permanent Select Committee on Intelligence*, The Protecting Cyber

Inicjatywa legislacyjna obu izb Kongresu miała w tym wypadku charakter rozłączny: niemal równocześnie, w marcu 2015 r., Senat zainicjował prace nad projektem *Cybersecurity Information Sharing Act* – CISA[59], Izba Reprezentantów zaś – nad *Protecting Cyber Networks Act* – PCNA[60]. Oba wymienione akty tworzyły mechanizm umożliwiający podmiotom prywatnym wymianę informacji o zagrożeniach cybernetycznych, zachodziły między nimi jednak istotne różnice dotyczące sposobu i trybu, w którym ta wymiana ma być prowadzona, oraz nadzoru na tym procesem.

Mając na uwadze powyższe czynniki oraz dążenie ówczesnej administracji do stworzenia skutecznych podstaw prawnych wymiany informacji w zakresie cyberbezpieczeństwa, procedowane w obu izbach Kongresu projekty CISA i PCNA uległy połączeniu, tworząc *Cybersecurity Act of 2015*[61]. Ten akt należy zatem traktować jako projekt o charakterze kompromisowym mający na celu poprawę skuteczności funkcjonującego dotychczas w USA systemu, a także doprowadzenie do znalezienia odpowiedniej równowagi między wymienionymi powyżej pierwotnymi projektami i stworzenie jednego, spójnego aktu regulującego omawianą problematykę.

2. Charakterystyka najważniejszych elementów ustawy

C*ybersecurity Act of 2015* składa się z czterech tytułów:

1. *Cybersecurity Information Sharing* – przepisy tworzące scentralizowany mechanizm wymiany informacji z zakresu cyberbezpieczeństwa pomiędzy podmiotami sektora prywatnego;
2. *National Cybersecurity Advancement* – poprawa poziomu cyberbezpieczeństwa organów administracji;
3. *Federal Cybersecurity Workforce Assessment* – ocena zdolności i zasobów w zakresie cyberbezpieczeństwa;
4. *Other Cyber Matters* – pozostałe przepisy.

Celem niniejszego opracowania jest przedstawienie najważniejszych elementów tytułu I ustawy – *Cybersecurity Information Sharing*.

3. Wybrane definicje

- Cel związany z cyberbezpieczeństwem (*Cybersecurity Purpose* – sekcja 102 pkt 4) – cel związany z ochroną systemów informatycznych lub informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu przed zagrożeniami dla cyberbezpieczeństwa lub podatnością systemów na ataki informatyczne.
- Zagrożenie cyberbezpieczeństwa (*Cybersecurity Threat* – sekcja 102 pkt 5) – działanie niepodlegające ochronie na podstawie Pierwszej Poprawki do Konstytucji Stanów Zjednoczonych, dokonane w systemie informatycznym lub

Networks Act (H.R.1560), s. 1, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf [dostęp: 16 IX 2017].

[59] Projekt H.R. 1560 (114th): *Cybersecurity Information Sharing Act of 2015* został przegłosowany przez obie izby.

[60] Projekt H.R. 1560 (114th): *Protecting Cyber Networks Act* został przegłosowany przez Izbę Reprezentantów 22 IV 2015 r., nie został jednak przegłosowany przez Senat, proces legislacyjny zatem nie został zakończony, https://www.govtrack.us/congress/bills/114/hr1560 [dostęp: 22 IX 2017].

[61] J.L. Tran, *Navigating the Cybersecurity Act of 2015*, Chapman Law Review, http://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1377&context=chapman-law-review [dostęp: 22 IX 2017].

za jego pośrednictwem, mogące skutkować naruszeniem bezpieczeństwa, dostępności, poufności lub integralności systemu informatycznego lub informacji przechowywanych, przetwarzanych lub przesyłanych przez ten system.

- Wskaźnik zagrożenia cybernetycznego (*Cybersecurity Threat Indicator* – sekcja 102 pkt 6) – informacja niezbędna do opisu lub identyfikacji –
  A. Wrogich działań rozpoznawczych, w tym wykazujących anomalie wzorców komunikacji, których celem może być pozyskiwanie informacji technicznych związanych z zagrożeniem dla cyberbezpieczeństwa lub z elementami systemu wykazującymi podatność na ataki,
  B. Metod obejścia systemu kontroli lub wykorzystywania podatności systemu na ataki,
  C. Podatności na ataki, w tym wykazującej anomalie aktywności, która może świadczyć o podatności określonych elementów systemu na atak,
  D. Metod powodujących, że użytkownik uprawniony do dostępu do systemu, do zgromadzonych w nim lub przesyłanych za jego pośrednictwem informacji w sposób nieświadomy umożliwia obejście systemu kontroli lub wykorzystanie podatności systemu na atak,
  E. Złośliwego kierowania i kontroli nad systemem,
  F. Faktycznej lub potencjalnej szkody spowodowanej incydentem, w tym opisu informacji uzyskanej z systemu wskutek wystąpienia określonego zdarzenia dla cyberbezpieczeństwa,
  G. Jakiekogolwiek innego parametru wskazującego na zagrożenie dla cyberbezpieczeństwa, jeżeli jego ujawnienie nie jest zabronione na mocy innych przepisów,
  H. Jakiejkolwiek kombinacji powyższych elementów.
- Środek defensywny (*Defensive Measure* – sekcja 102 pkt 7) –
  A. Z zastrzeżeniem punktu B, pojęcie środek defensywny oznacza działanie, urządzenie, procedurę, sygnaturę, technikę lub inny instrument stosowany w odniesieniu do systemu informatycznego lub do zgromadzonych w nim informacji, który wykrywa, zapobiega lub zmniejsza skutki znanego, lub którego zaistnienie można podejrzewać, zagrożenia dla cyberbezpieczeństwa lub podatności systemu na atak,
  B. Pojęcie środek defensywny nie obejmuje środków, które niszczą, czynią niezdatnymi do użytku, zapewniają nieautoryzowany dostęp lub wywołują poważną szkodę w systemie informatycznym lub w informacjach zgromadzonych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu, który nie jest w posiadaniu –
     i) prywatnego podmiotu zarządzającego tym środkiem; lub
     ii) innej jednostki lub jednostki federalnej, która będąc do tego należycie umocowaną, wyraziła zgodę na wykorzystanie tego rodzaju środka.
- Jednostka federalna (*Federal Entity* – sekcja 102 pkt 8) – departament lub agencja Stanów Zjednoczonych lub jakakolwiek jednostka organizacyjna takiego departamentu lub agencji.
- System informatyczny (*Information System* – sekcja 102 pkt 9) –
  A. Oznacza system opisany w sekcji 3502 tytułu 44 Kodeksu Stanów Zjednoczonych[62],

[62] Zgodnie z sekcją 3502 tytułu 44 Kodeksu Stanów Zjednoczonych pojęcie system informatyczny oznacza indywidualny zbiór zasobów informacyjnych mający na celu zbieranie, przetwarzanie, przecho-

B. Pojęcie to obejmuje przemysłowe systemy kontroli, takie jak systemy nadzoru i systemy pozyskiwania danych, rozproszone systemy sterowania oraz programowalne kontrolery logiczne.

- Złośliwe kierowanie i kontrola systemu (*Malicious Cyber Command and Control* – sekcja 102 pkt 11) – metody służące do nieautoryzowanej zdalnej identyfikacji, uzyskania dostępu lub użycia systemu informatycznego lub informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu.
- Złośliwe rozpoznanie (*Malicious Reconnaissance* – sekcja 102 pkt 12) – metody służące do aktywnego sondowania lub pasywnego monitorowania systemu informatycznego w celu wykrycia jego podatności na ataki, jeżeli są one powiązane ze znanym zagrożeniem cyberbezpieczeństwa lub zagrożeniem, którego wystąpienie można podejrzewać.
- Monitorowanie (*Monitor* – sekcja 102 pkt 13) – pozyskiwanie, identyfikacja, skanowanie lub posiadanie informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem systemu informatycznego.
- Jednostka niefederalna (*Non-Federal Entity* – sekcja 102 pkt 14) –
  A. Z zastrzeżeniem wyjątków przewidzianych w niniejszym paragrafie, pojęcie jednostka niefederalna oznacza jednostkę prywatną, niefederalną agencję rządową lub departament, lub rząd stanowy, lokalny lub plemienny (w tym pododdział polityczny, departament lub ich część składową),
  B. Pojęcie jednostka niefederalna oznacza agencję rządową lub departament Dystryktu Kolumbii, Wspólnoty Puerto Rico, Wysp Dziewiczych Stanów Zjednoczonych, Samoa Amerykańskiego, Marianów Północnych lub jakiegokolwiek innego terytorium znajdującego się w posiadaniu Stanów Zjednoczonych,
  C. Pojęcie jednostka niefederalna nie obejmuje obcego państwa w rozumieniu sekcji 101 ustawy *Foreign Intelligence Surveillance Act of 1978* (50 *United States Code* 1801)[63].
- Jednostka prywatna (*Private Entity* – sekcja 102 pkt 15) –
  A. Z zastrzeżeniem wyjątków przewidzianych w niniejszym paragrafie pojęcie jednostka prywatna oznacza prywatną osobę lub grupę, organizację, współwłasność, partnerstwo, trust, spółdzielnię, korporację lub inną jednostkę handlową lub non-profit, z uwzględnieniem osób pełniących funkcje kierownicze, pracowników lub agentów takiej jednostki,
  B. Pojęcie jednostka prywatna oznacza rząd stanowy, lokalny lub plemienny realizujący zadania użyteczności publicznej związane m.in. z usługami związanymi z elektrycznością, gazem naturalnym i wodą,
  C. Pojęcie jednostka prywatna nie obejmuje obcego państwa w rozumieniu sekcji 101 ustawy *Foreign Intelligence Surveillance Act of 1978*
     i) kontrola bezpieczeństwa (*Security Control* – sekcja 102 pkt 16) – zarządcze, operacyjne i techniczne środki kontrolne wykorzystywane w celu ochrony przed nieuprawnionym działaniem zmierzającym do naruszenia poufności, integralności lub dostępności systemu informatycznego lub zgromadzonych w nim informacji,

wywanie, wykorzystywanie, rozpowszechnianie i zarządzanie informacjami.

[63] *U.S Code* Title 50 Chapter 36 – *Foreign Intelligence Surveillance*, https://www.law.cornell.edu/uscode/text/50/chapter-36 [dostęp: 18 IX 2017].

ii) podatność na ataki (*Security Vulnerability* – sekcja 102 pkt 17) – jakakolwiek cecha sprzętu, oprogramowania, proces lub procedura mogące umożliwić lub ułatwić obejście kontroli bezpieczeństwa.

- Kontrola bezpieczeństwa (*Security Control* – sekcja 102 pkt 16) – zarządzanie, operacyjne i techniczne środki kontroli wykorzystywane w celu ochrony przed nieautoryzowanym działaniem mającym na celu naruszenie poufności, integralności i dostępności systemu informatycznego lub zgromadzonych w nim informacji.
- Podatność systemu na ataki (*Security Vulnerability* – sekcja 102 pkt 17) – jakakolwiek cecha sprzętu, oprogramowania, proces lub procedura mogąca umożliwić lub ułatwić obejście kontroli bezpieczeństwa.

4. Przekazywanie informacji o zagrożeniach cyberbezpieczeństwa przez organy rządu federalnego

Sekcja 103 pkt (a) ustawy zobowiązuje Narodowego Dyrektora ds. Wywiadu, Sekretarza ds. Bezpieczeństwa Wewnętrznego, Sekretarza Obrony i Prokuratora Generalnego do opracowania – po konsultacji z organami kierowniczymi właściwych jednostek federalnych i z poszanowaniem przepisów dotyczących ochrony informacji niejawnych – źródeł i metod wywiadowczych, prawa do prywatności oraz innych praw i wolności obywatelskich, procedur, mających na celu ułatwienie i wspieranie:

1. Szybkiej wymiany danych o wskaźnikach zagrożenia cybernetycznego i środkach defensywnych stanowiących informacje niejawne, będących w posiadaniu rządu federalnego, z przedstawicielami jednostek federalnych i niefederalnych, mających odpowiednie poświadczenie bezpieczeństwa – sekcja 103 (a) (1).

   Zgodnie z dokumentem *Executive Order 13636*[64] organy administracji dążą do szybkiego opracowywania jawnych raportów dotyczących zagrożeń cybernetycznych identyfikujących konkretny podmiot, który został dotknięty określonym atakiem informatycznym lub inną formą niezgodnego z prawem oddziaływania na systemy informatyczne. W przypadku gdy dane o takim zdarzeniu stanowią informacje niejawne, możliwość przekazania podmiotowi dotkniętemu atakiem informacji przez organy rządu federalnego jest uzależniona od posiadania przez ten podmiot poświadczenia bezpieczeństwa. Ponadto muszą być spełnione wymogi związane z ochroną źródeł i metod wywiadowczych. Wszystkie jednostki federalne uczestniczące w procesie wymiany informacji o zagrożeniach dla cyberbezpieczeństwa są zobowiązane do przestrzegania przepisów dotyczących sposobów oznaczania informacji niejawnych czy restrykcji związanych z ograniczeniem ich obiegu, jak np. klauzula ORCON (*Originator Controlled* – zasada przewidująca kontrolę wytwórcy nad sposobem wykorzystania danej informacji). W nagłych sytuacjach będzie możliwe zastosowanie w dalszym ciągu procedury szczególnej przewidzianej w tytule 32 sekcji 2001.52 Kodeksu Stanów Zjednoczonych[65]. Zgodnie z tą procedurą w sytuacjach kryzysowych, w których istnieje poważne zagrożenie życia,

[64] *Executive Order – Improving Critical Infrastructure Cybersecurity*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [dostęp: 19 IX 2017].

[65] *Code of Federal Regulations*, Title 32, Subtitle B, Chapter XX, Part 2001, Subpart E, Section 2001.52, https://www.law.cornell.edu/cfr/text/32/2001.52 [dostęp: 18 IX 2017].

zdrowia lub obronności, szefowie agencji lub osoby przez nich wyznaczone mogą, pod pewnymi warunkami, zezwolić na ujawnienie informacji niejawnych osobie lub osobom nieposiadającym dostępu do informacji niejawnych[66].

2. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi informacji o wskaźnikach zagrożeń cyberbezpieczeństwa, środkach defensywnych oraz informacji dotyczących zagrożeń cyberbezpieczeństwa znajdujących się w posiadaniu rządu federalnego, które mogą być odtajnione i przekazane innym organom jako informacje jawne – sekcja 103 (a) (2).
   Efektywność procesu wymiany informacji dotyczących zagrożeń cyberbezpieczeństwa jest w naturalny sposób ograniczona, w przypadku gdy stanowią one informacje niejawne – znacznemu wydłużeniu ulega proces ich dystrybucji, krąg ich odbiorców zaś zostaje znacznie ograniczony. W związku z tym cytowany dokument S*haring of Cyber Threat Indicators and Defensive Measures under the Cybersecurity Information Act of 2015* zachęca jednostki federalne do ograniczenia korzystania z reżimu prawnego przewidzianego dla ochrony informacji niejawnych w odniesieniu do wymiany omawianych kategorii informacji. Te podmioty powinny, jeżeli nie jest to sprzeczne z charakterem określonych informacji, dążyć do odtajniania, obniżania klauzul tajności oraz usuwania najbardziej wrażliwych elementów. Jednostki federalne należące do tzw. wspólnoty wywiadowczej (Intelligence Community) powinny rozpowszechniać jawne informacje o zagrożeniach cyberbezpieczeństwa przez aplikacje typu „*tearline*"[67].
3. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi, a także przekazywanie – w razie potrzeby – do publicznej wiadomości informacji o wskaźnikach zagrożenia cyberbezpieczeństwa i środkach defensywnych niestanowiących informacji niejawnych, w tym informacji jawnych, których udostępnianie podlega kontroli (ang. *controlled unclassified*), będących w posiadaniu rządu federalnego – sekcja 103 (a) 3.
   Ustawa zakłada szeroką wymianę jawnych informacji dotyczących wskaźników zagrożeń cyberbezpieczeństwa i środków defensywnych zarówno pomiędzy jednostkami federalnymi, jak i tymi jednostkami a jednostkami niefederalnymi, z zastrzeżeniem szczególnych instrukcji w zakresie sposobu dystrybucji określonych informacji. Jeżeli jednostka federalna otrzyma od jednostki niefederalnej dane dotyczące wskaźnika zagrożeń lub środka defensywnego w sposób inny niż przewidziany w sekcji 105 (c) (mechanizm stworzony przez Departament Bezpieczeństwa Wewnętrznego, Departament of Homeland Security – DHS), powinna je przekazać

[66] *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Act of 2015*, February 16, 2016, s. 7, https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf [dostęp: 18 IX 2017].

[67] Ang. *tearline* – rodzaj aplikacji służąca do wymiany jawnych informacji wywiadowczych stworzonych na podstawie dokumentów o wyższym poziomie tajności, z których zostały usunięte najbardziej wrażliwe elementy, np. informacje o źródłach czy sposobach pozyskania danej informacji. Z tego rodzaju aplikacji mogą korzystać wyłącznie upoważnione osoby – pracownicy tzw. wspólnoty wywiadowczej (Intelligence Community). Założeniem leżącym u podstaw stworzenia tego rodzaju aplikacji była możliwość szerokiego rozpowszechniania informacji o ewentualnych zagrożeniach w celu wspierania ogólnie pojmowanych interesów bezpieczeństwa narodowego; Intelligence Community Directive 209, 6 September 2012 – *Tearline Production and Dissemination*, https://fas.org/irp/dni/icd/icd-2IXpdf [dostęp: 19 IX 2017]. Ogólne informacje o aplikacji zawarto w artykule prasowym na stronie https://www.wired.com/2017/04/american-spies-now-smartphone-app/ [dostęp: 19 IX 2017]. Zob. *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government*, s. 9.

wszystkim pozostałym właściwym jednostkom federalnym, biorąc pod uwagę zakres ich zadań. W miarę możliwości powinna też zdjąć z nich klauzulę tajności i usunąć elementy wrażliwe, wykorzystując do tego aplikacje typu „*tearline*"[68].

4. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi informacji będących w posiadaniu rządu federalnego o zagrożeniach cyberbezpieczeństwa dotyczących tych jednostek, w celu zapobiegania lub neutralizacji negatywnych skutków tych zagrożeń – sekcja 103 (a) (4).
   Zgodnie z sekcją 4 (b) dokumentu *Executive Order 13636* sekretarz ds. Bezpieczeństwa Wewnętrznego i prokurator generalny, współdziałając z dyrektorem Wywiadu Narodowego, zostali zobowiązani do stworzenia systemu pozwalającego na szybkie przekazywanie raportów o zagrożeniach cyberbezpieczeństwa podmiotom, których dotyczy konkretne zagrożenie. Ten proces obejmuje również dystrybucję niejawnych raportów do upoważnionych jednostek infrastruktury krytycznej (ang. *critical infrastructure entities*)[69]. Na podstawie sekcji 103 (a) 4 ustawy organu rządu federalnego powinny one w sposób analogiczny przekazywać informacje również jednostkom niefederalnym, które zostały lub mogą zostać dotknięte wrogą działalnością w cyberprzestrzeni – również tym, które nie należą do tzw. *critical infrastructure entities*[70].
5. Okresowej wymiany tzw. dobrych praktyk w zakresie cyberbezpieczeństwa opracowanych na podstawie analiz wskaźników zagrożeń cyberbezpieczeństwa, środków defensywnych i innych informacji dotyczących tego rodzaju zagrożeń będących w posiadaniu rządu federalnego, z uwzględnieniem potrzeb małych przedsiębiorstw – sekcja 103 (a) (5).
   Do grupy podmiotów opracowujących tzw. dobre praktyki w zakresie bezpieczeństwa należą m.in. Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST), Departament Bezpieczeństwa Wewnętrznego Departament Obrony oraz Agencja Bezpieczeństwa Narodowego[71].

W punkcie (b) sekcji 103 zawarto katalog przesłanek, którym powinny odpowiadać procedury wymiany informacji o zagrożeniach cyberbezpieczeństwa. Jako przykład należy wskazać ogólny wymóg, zgodnie z którym te procedury powinny zapewniać, że rząd federalny ma informacje o wskaźnikach zagrożeń i środkach defensywnych w czasie rzeczywistym, spełniające standardy wynikające z ochrony informacji niejawnych, i utrzymuje zdolności umożliwiające ich wymianę. Te procedury powinny przewidywać tryb, w jakim podmioty, których dane osobowe zostały przekazane niezgodnie z przepisami tytułu I ustawy, powinny zostać poinformowane o tym naruszeniu.

5. Monitorowanie systemów informatycznych i zarządzanie środkami defensywnymi przez jednostki prywatne

Sekcja 104 ustawy upoważnia jednostki prywatne do monitorowania systemów informatycznych i stosowania środków defensywnych zarówno w odniesieniu do wła-

[68] Tamże, s. 10.

[69] Pod pojęciem infrastruktura krytyczna (ang. *critical infrastructure*) zgodnie z sekcją 2 *Executive Order 13636* należy rozumieć systemy i środki, zarówno materialne, jak i wirtualne, na tyle istotne dla Stanów Zjednoczonych, że ich niezdolność do działania lub ich zniszczenie będzie negatywnie wpływało na bezpieczeństwo, narodowe bezpieczeństwo gospodarcze, narodową ochronę zdrowia publicznego lub na sprawy łącznie dotyczące tych elementów.

[70] *Sharing of Cyber Threat Indicators*…, s. 13.

[71] Tamże, s. 15–16.

snych systemów informatycznych, jak i systemów wykorzystywanych przez inne podmioty, po uzyskaniu ich pisemnej zgody (przepis ten obejmuje inne jednostki niefederalne oraz jednostki federalne – po uzyskaniu pisemnej zgody posiadającego odpowiednie kompetencje przedstawiciela tej jednostki federalnej). Jednostki, o których mowa, mogą również monitorować informacje przechowywane, przetwarzane lub przesyłane za pośrednictwem określonego systemu informatycznego [sekcja 104 (a) i (b)][72].

Sekcja 104 (c) upoważnia jednostki niefederalne do wymiany i otrzymywania od innych jednostek niefederalnych lub od organów rządu federalnego informacji dotyczących wskaźników zagrożeń cyberbezpieczeństwa i środków defensywnych, wyłącznie w celach związanych z ochroną cyberbezpieczeństwa i zgodnie z zasadami regulującymi ochronę informacji niejawnych. Informacje przekazane organom stanowym, lokalnym i plemiennym mogą zostać wykorzystane, oprócz celów związanych z ochroną cyberbezpieczeństwa, również do rozpoznawania, zapobiegania i ścigania przestępstw wymienionych w sekcji 105(d)(5)(A) – m.in. szpiegostwo i terroryzm.

Podmiot monitorujący system informatyczny, zarządzający środkami defensywnymi oraz dostarczający lub odbierający wskaźniki zagrożeń cyberbezpieczeństwa lub środki defensywne jest zobowiązany do wprowadzenia i wykorzystywania instrumentu kontroli bezpieczeństwa (ang. *security control*) w celu ochrony przed nieuprawnionym ujawnieniem lub pozyskaniem informacji dotyczących ww. wskaźników lub środków (sekcja 104 d). Ponadto sekcja nakłada na podmiot zamierzający dokonać wymiany informacji o wskaźnikach zagrożeń cyberbezpieczeństwa obowiązek weryfikacji, czy dany wskaźnik zawiera informacje niedotyczące bezpośrednio tego rodzaju zagrożeń, które – zgodnie z jego wiedzą – stanowią dane osobowe określonej osoby fizycznej lub informacje pozwalające na jej identyfikację, i usunięcia tego rodzaju danych lub zastosowania w tym celu odpowiednio skonfigurowanych urządzeń technicznych [sekcja 104 (d) (2) (A) i (B)][73].

Przepis sekcji 104 (e) jest jednym z przykładów tzw. *safe harbours* – przepisów wyłączających odpowiedzialność podmiotów prywatnych za wymianę informacji o zagrożeniach cyberbezpieczeństwa, jeżeli ta wymiana jest prowadzona zgodnie z przepisami ustawy. Wymiana informacji między dwiema (lub więcej) jednostkami prywatnymi na temat wskaźników zagrożeń, środków defensywnych lub udzielania wsparcia w zakresie zapobiegania, badania lub minimalizacji skutków wymienionych zagrożeń nie stanowi naruszenia jakichkolwiek przepisów prawa antymonopolowego (ang. *antitrust laws*).

6. Wymiana informacji o wskaźnikach zagrożeń cyberbezpieczeństwa i środków defensywnych z organami rządu federalnego

Prokurator Generalny i Sekretarz ds. Bezpieczeństwa Wewnętrznego zostali zobowiązani, nie później niż 180 dni od daty przyjęcia ustawy oraz w porozumieniu z organami kierowniczymi właściwych jednostek federalnych, do opracowania i opublikowania dokumentów opisujących procedury dotyczące sposobu postępowania organów rządu federalnego na wypadek otrzymania informacji o wskaźnikach zagrożeń i środkach defensywnych [sekcja 105 (a) 2].

[72] *Congress Passes and President Signs*…, s. 6–7.

[73] *Federal Guidance on the Cybersecurity Information Sparing Act of 2015*, Harvard Law School Forum on Corporate Governance and Financial Regulation, posted by Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [dostęp: 18 IX 2017].

Podczas gdy sekcja 104 (c) dotyczyła wymiany wskaźników zagrożeń i środków defensywnych zarówno z jednostkami federalnymi, jak i niefederalnymi, sekcja 105 dotyczy stricte wymiany tego rodzaju informacji z organami rządu federalnego. Wymiana jest prowadzona przez zarządzaną przez DHS platformę wymiany informacji, o której mowa w pkt c sekcji 105. Sekretarz ds. Bezpieczeństwa Wewnętrznego, nie później niż 90 dni od przyjęcia ustawy, w porozumieniu z organami kierowniczymi właściwych jednostek federalnych, opracowuje i implementuje w Departamencie Bezpieczeństwa Wewnętrznego procedury, które:

- umożliwiają przyjmowanie od jednostek niefederalnych w czasie rzeczywistym wskaźników zagrożeń i środków defensywnych,
- po uzyskaniu odpowiedniego certyfikatu potwierdzającego, że wymiana informacji działa w sposób kompletny i efektywny – będą służyły rządowi federalnemu do otrzymywania informacji dotyczących wskaźników zagrożeń oraz środków defensywnych udostępnianych mu przez jednostki niefederalne,
- gwarantują, że wszystkie właściwe jednostki federalne otrzymują w sposób zautomatyzowany informacje dotyczące wskaźników zagrożeń oraz środki defensywne za pośrednictwem wykorzystywanego przez DHS instrumentu działającego w czasie rzeczywistym,
- spełniają wymogi określone w procedurach i wytycznych tworzonych na podstawie niniejszej sekcji,
- nie ograniczają ani nie wyłączają zgodnego z prawem ujawnienia danych dotyczących komunikacji, nagrań lub innych informacji, w tym m.in. przekazywania przez jednostki niefederalne innym jednostkom niefederalnym lub jednostkom federalnym informacji dotyczących podejrzenia popełnienia przestępstwa, z uwzględnieniem wskaźników zagrożeń lub środków defensywnych, udostępnionych jednostce federalnej w ramach śledztwa federalnego.

Jednostki niefederalne mogą przekazywać tego rodzaju informacje DHS, podczas gdy ten organ będzie zobowiązany do przekazania w sposób zautomatyzowany otrzymanych w ten sposób informacji do Departamentu Handlu, Obrony, Energii, Sprawiedliwości, Skarbu oraz do Biura Narodowego Dyrektora Wywiadu zgodnie z sekcją 105 (a) (3) (A)[74].

Przekazane w trybie sekcji 105 organom rządu federalnego wskaźniki zagrożeń cyberbrzpieczeństwa oraz środki defensywne mogą być udostępnione, przechowywane lub wykorzystane przez agencję lub departament federalny, ich jednostkę organizacyjną, funkcjonariusza, pracownika lub przez agenta rządu federalnego wyłącznie:

- dla celów związanych z cyberbezpieczeństwem,
- w celu identyfikacji zagrożenia cyberbezpieczeństwa (w tym jego źródła) lub podatności systemu informatycznego na atak,
- w celu reagowania, zapobiegania lub neutralizacji konsekwencji bezpośredniego ryzyka utraty życia lub zdrowia, wystąpienia poważnej szkody gospodarczej, w tym aktu terrorystycznego lub użycia broni masowego rażenia,
- w celu reagowania, zapobiegania, neutralizacji konsekwencji lub ścigania poważnego zagrożenia dla małoletniego, w tym wykorzystywania seksualnego i zagrożeń jego fizycznego bezpieczeństwa;

[74] *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf, s. 12 [dostęp: 18 IX 2017].

- w celu zapobiegania, rozpoznawania, udaremnienia lub ścigania przestępstw: oszustwa, kradzieży tożsamości, szpiegostwa lub przestępstw związanych z naruszeniem tajemnicy handlowej.

7. Przepisy wyłączające odpowiedzialność podmiotów prywatnych za przekazywanie informacji zgodnie z ustawą

Sekcja 106 (a) stanowi, że przeciwko podmiotowi prywatnemu prowadzącemu działalność polegającą na monitorowaniu systemu informatycznego na podstawie sekcji 104 (a) nie może być wniesiona jakakolwiek skarga, jeżeli ta działalność była prowadzona zgodnie z przepisami ustawy.

Na zasadzie analogii – zgodnie z sekcją 106 (b) podmiot prywatny nie może zostać pociągnięty do odpowiedzialności za wymienianie informacji związanych ze wskaźnikami zagrożeń cyberbezpieczeństwa lub środków defensywnych zgodnie z sekcją 104 (c), jeżeli ta wymiana odbywała się w myśl przepisów ustawy oraz, w przypadku gdy informacje są przekazywane rządowi federalnemu oraz informacje, o których mowa, były przekazywane za pośrednictwem systemu stworzonego przez DHS[75].

Przekazanie rządowi federalnemu informacji o zagrożeniach cyberbezpieczeństwa nie powoduje uchylenia jakichkolwiek przywilejów ani środków ochronnych przewidzianych na podstawie innych ustaw, w tym tajemnicy handlowej [sekcja 105 (d) (1)].

Informacje przekazane rządowi federalnemu nie podlegają ujawnieniu na podstawie ustawy *Freedom of Information Act* ani na podstawie innych przepisów rangi stanowej czy aktów prawa miejscowego, przewidujących swobodny dostęp do informacji i rejestrów [sekcja 105 (d) (3)][76].

Biorąc pod uwagę to, że konstrukcja ustawy została oparta na założeniu dobrowolnego przekazywania informacji dotyczących zagrożeń cyberbezpieczeństwa, żaden z przepisów ustawy nie powinien być interpretowany jako nakładający obowiązek przekazania danych o wskaźniku zagrożeń lub środka defensywnego ani jako tworzący zobowiązanie do ostrzegania innych podmiotów lub do podejmowania innych działań w związku z otrzymaniem wymienionych informacji [sekcja 106 (c)]. Sekcja 108 (i) expressis verbis stanowi, że nieuczestniczenie danego podmiotu w dobrowolnych działaniach przewidzianych w ustawie, nie pociąga za sobą odpowiedzialności z tego tytułu.

Wnioski

Przyjęcie ustawy *Cybersecurity Act of 2015*, mającej na celu stworzenie mechanizmu wymiany informacji o zagrożeniach cyberbezpieczeństwa, było poprzedzone długotrwałymi rozmowami pomiędzy organami administracji a przedstawicielami przemysłu i sektora prywatnego. Motywem przewodnim prac legislacyjnych było wzmocnienie potencjału zarówno podmiotów publicznych, jak i prywatnych w zakresie identyfikacji omawianych zagrożeń i odpowiedzi na nie. Do najważniejszych kontrowersji wywołanych przez ustawę należy zaliczyć przewidziane w niej rozwiązania dotyczące ochrony prywatności oraz sposobu wykorzystywania przez władze publiczne informacji przekazywanych w trybie opisanym w tytule I ustawy (*Cybersecurity Information Sharing*).

[75] Tamże.

[76] *Federal Guidance on the Cybersecurity*…

Krytycy ustawy podnoszą, że w rzeczywistości jest ona zawoalowaną ustawą inwigilacyjną tworzącą kolejne – obok już istniejących – instrumenty przekazywania organom rządowym informacji o cyberzagrożeniach, zezwalając im jednocześnie na szerokie wykorzystywanie tych informacji również dla celów niezwiązanych z cyberbezpieczeństwem. Ustawa nie zawiera także rozważanego w toku prac legislacyjnych zakazu przekazywania informacji Agencji Bezpieczeństwa Narodowego i Pentagonowi[77]. Sekcja 105 (d) 5 A pozwala na przekazywanie przez organy rządu federalnego otrzymanych zgodnie z ustawą informacji wszystkim agencjom federalnym, departamentom, ich jednostkom organizacyjnym, funkcjonariuszom, pracownikom czy agentom rządu federalnego. Ten sposób sformułowania katalogu podmiotowego potencjalnych odbiorców nie świadczy o tym, że ustawodawca dążył do rzeczywistego ograniczenia przepływu tych danych. Przeciwnie – użycie w przywołanym w poprzednim zdaniu artykule słowa „*any*" (jakikolwiek, każdy) powoduje, że będzie on interpretowany rozszerzająco. Wątpliwości może również budzić szerokie ujęcie w art. 105 (d) 5 A katalogu przesłanek umożliwiających przekazanie informacji.

Kolejnym istotnym problemem jest konstrukcja sekcji 104 (d) 2 zobowiązująca jednostki niefederalne do usunięcia ze wskaźnika zagrożenia lub środka defensywnego informacji niezwiązanych bezpośrednio z cyberbezpieczeństwem, o których ta jednostka w momencie przekazania wie, że stanowią dane osobowe określonej osoby fizycznej lub identyfikują taką osobę. Krytycy ustawy podnoszą, że ten przepis pozwala w konsekwencji na przekazywanie danych osobowych praktycznie w każdym wypadku, czyniąc z tego opcję domyślną, usunięcie danych zaś – wyjątkiem. Obowiązek usunięcia informacji zawierających dane osobowe zachodzi zatem tylko wówczas, gdy jednostka niefederalna ma sprawdzoną wiedzę, że te osoby nie są bezpośrednio powiązane z zagrożeniem cyberbezpieczeństwa, Ten warunek będzie możliwy do spełnienia w nielicznych wypadkach[78].

Na uwagę zasługuje również zarzut przekazywania danych w trybie opisanym w ustawie. Tworzy ono – samo w sobie – potencjalne możliwości kradzieży danych, pomijając równocześnie realne problemy związane z cyberbezpieczeństwem, takie jak wykorzystywanie przez liczne podmioty przestarzałego oprogramowania, brak skutecznych środków ochronnych przed złośliwym oprogramowaniem czy sporadyczne korzystanie z szyfrowania plików. Dobrowolność systemu może powodować brak dostatecznego zainteresowania podmiotów sektora prywatnego udziałem w nim, co sprawi, że system nie będzie miał szans przynieść oczekiwanych rezultatów[79].

Za przyjęciem ustawy opowiadały się natomiast w głównej mierze prywatne podmioty działające w sektorze usług finansowych, argumentując, że przewidziane w ustawie kompleksowa i kolektywna wymiana informacji o zagrożeniach cyberbezpieczeń-

[77] *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance In The Name of Cybersecurity*, https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/ [dostęp: 22 IX 2017].

[78] Te argumenty zostały zawarte w liście do prezydenta Baracka Obamy wystosowanym przez organizacje społeczeństwa obywatelskiego i ekspertów w dziedzinie bezpieczeństwa informatycznego; list dostępny na stronie https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition%20Ltr%20Urging%20Pres.%20to%20Veto%20CISA.8b33e2d86dc14780b35c9cde44a41797.pdf [dostęp: 22 IX 2017].

[79] https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition%20Ltr%20Urging%20Pres.%20to%20Veto%20CISA.8b33e2d86dc14780b35c9cde44a41797.pdf [dostęp: 22 IX 2017].

stwa przyczyni się do skutecznego zabezpieczenia interesów ich klientów w obliczu intensyfikacji tych zagrożeń[80].

Dokonanie całościowej oceny wszystkich aspektów funkcjonowania ustawy będzie możliwe dopiero po zbadaniu jej rzeczywistego sposobu działania, wpływu na poziom cyberbezpieczeństwa i ewentualnych naruszeń prawa do prywatności, sygnalizowanych w toku procesu legislacyjnego. Do pozytywnych aspektów tego aktu należy zaliczyć wprowadzenie pewnej spójności legislacyjnej i terminologicznej przez stworzenie definicji takich pojęć, jak: zagrożenie cyberbezpieczeństwa czy cel związany z cyberbezpieczeństwem. Trzeba też się zgodzić z krytyką jej rozwiązań dotyczących ograniczeń w zakresie przekazywania niezwiązanych z zagrożeniem informacji, zawierających dane osobowe lub pozwalających na identyfikację określonej osoby fizycznej, Konstrukcja zawartych w ustawie przepisów nie może być uznana za czynnik przesądzający o tym, że naruszenia prawa do prywatności będą występować w niemożliwej do zaakceptowania skali. Nie jest natomiast przekonujący pogląd, że jest to tak naprawdę kolejna ustawa inwigilacyjna. Biorąc pod uwagę charakter i ilość uprawnień przysługujących organom wchodzącym w skład tzw. Intelligence Community oraz skalę strat spowodowanych atakami cybernetycznymi, jest mało prawdopodobne, że ustawodawca zamierzał po raz kolejny skupić się na rozszerzaniu katalogu tych uprawnień.

[80] http://www.fsroundtable.org/fsr-launches-advertising-campaign-urging-congress-to-pass-cisa/ [dostęp: 22 IX 2017].

Justyna Strużewska-Smirnow
Mateusz Wieczerza

Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych z perspektywy międzynarodowej

I. REPUBLIKA FEDERALNA NIEMIEC

W ramach uprawnień operacyjno-rozpoznawczych i dochodzeniowo-śledczych realizowanych w celu wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych, przeprowadzanych przez niemieckie służby policyjne i informacyjne, należy wymienić następujące instrumenty monitoringu:

- bezpośrednią kontrolę telekomunikacji, tzw. źródła kontroli telekomunikacyjnej,
- przeszukanie online (niem. *Online Durchsuchung*), które umożliwia śledczym dostęp do całościowych systemów komputerowych. To rozwiązanie pozwala na włamanie się za pomocą środków technicznych do systemu informacyjno-technicznego, na przykład do sieci komputerowej lub pojedynczego urządzenia, które są w użytkowaniu osoby podejrzanej, bez jej wiedzy[1]. W tym wypadku komputery mogą być sprawdzone jeden raz (przejrzenie – niem. *Online-Durchsicht*) lub sprawdzone, czy też nadzorowane w jakimś określonym czasie (niem. *Online -Überwachung*), bez wiedzy użytkownika[2].

Zasadniczą różnicą w przypadku obuwymienionych metod jest zasięg gromadzenia danych. W przypadku przeszukania online można – również bez wiedzy osoby zainteresowanej – pozyskać pozostałe dane znajdujące się w komputerze, które wykraczają poza bieżącą komunikację[3].

Najbardziej spektakularnym osiągnięciem tego rozwiązania jest możliwość monitorowania usług programów typu Messenger, takich jak WhatsApp, przed lub po ich zaszyfrowaniu[4]. Służy temu zainstalowanie określonego typu oprogramowania trojańskiego[5]. Takie

[1] www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[2] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[3] www.wiwo.de/technologie/digitale-welt/whatsapp-was-die-ueberwachung-der-messenger-bedeutet/19972834.html [dostęp: 29 VI 2017].

[4] W tym celu musi zostać zainstalowany i będzie używany program monitorowania telekomunikacji źródłowej (również monitorowanie telekomunikacji na komputerze przed jej zaszyfrowaniem), podczas gdy przy klasycznym monitorowaniu telekomunikacji treść pozostaje zaszyfrowana.

[5] Oprogramowanie trojańskie (tzw. trojan) to program przeprowadzający określone funkcje na komputerze w sposób niejawny lub jako program użytkowy w zakamuflowanej formie, na które użytkownik nie wyraził zgody i ich nie kontroluje. Sam trojan nie musi być szkodliwy. Zwykle współdziała z innym wrogim oprogramowaniem lub umożliwia takiemu oprogramowaniu dostać się do komputera. Nie należy utożsamiać trojana z wirusem komputerowym, wirus bowiem usiłuje się rozprzestrzenić na coraz większą liczbę plików i na cały komputer, a ponadto wirus stara się sam siebie kopiować. Trojan sam się nie kopiuje, ale może zostać połączony z wirusem. Zob. także: www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung

działanie może być podjęte za zgodą sądu w celu czynnej obrony lub zbierania informacji wywiadowczych i tym różni się od kontroli telekomunikacji, że nie dotyczy spraw związanych z przesyłem danych, ale z bieżącą komunikacją osoby docelowej, która jest monitorowana przez oprogramowanie szpiegowskie bezpośrednio na urządzeniu końcowym (komputer, telefon komórkowy). To rozwiązanie umożliwia ominięcie szyfrowania transferu danych[6].

Jak już wspomniano, opisywana metoda wymaga zainstalowania szkodliwego oprogramowania zwanego oprogramowaniem trojańskim. W języku potocznym jest ono określane mianem „trojana publicznego" („*Staatstrojaner*", „*Bundestrojaner*"), w branży IT natomiast pojawiają się także inne określenia, m.in. „*Schadsoftware*" (szkodliwe oprogramowanie) lub „*Govware*" (od angielskiego słowa *government* – rząd[7])[8]. Działanie tego specyficznego oprogramowania trojańskiego jest związane z wykorzystaniem urządzenia rejestrującego pracę na komputerze (tzw. Keylogger, który umożliwia śledzenie pracy na klawiaturze i w ten sposób uzyskiwanie np. haseł do skrzynek poczty elektronicznej). Na ogół to narzędzie występuje w wersji programowej, rzadziej w sprzętowej, która musi być zamontowana bezpośrednio na komputerze podejrzanego[9].

Trojan wypełnia rozkazy, które są przekazywane z innego komputera. Te komendy w sposób niezaszyfrowany są wysyłane do programu. Nadawca nie musi ich uwierzytelniać. W ten sposób powstaje pewna luka trybu bezpieczeństwa, gdyż zainfekowany trojanami komputer może zostać przejęty przez osoby trzecie, które mogą wgrać wrogie oprogramowanie[10]. Trojan znajduje się pomiędzy nadawcą a adresatem (w branży IT jest spotykane określenie „*Man in the Middle*").

Przemycanie trojanów na prywatne komputery może być skutkiem załadowania pliku (np. zdjęć, tekstu lub aktualizacji), odwiedzin na zainfekowanej stronie lub otwarcia zmanipulowanego załącznika do maila. Należy zaznaczyć, że jedyną możliwością obrony przed takim atakiem jest korzystanie z komputera, który nie jest podłączony do Internetu. Oprogramowanie typy „*firewall*" oraz programy antywirusowe znajdują przede wszystkim wirusy i wrogie oprogramowanie, które już jest im znane lub które mają typowe sposoby działania, potrzebują zatem uaktualnianych list wirusów. Z uwagi na to, że trojany są „produkcją jednostkową", istnieją niewielkie szanse na ich wykrycie[11].

Organy śledcze mają uprawnienie do niejawnego przegrywania wrogiego oprogramowania na prywatne komputery, laptopy, telefony komórkowe i tablety w celu odczytywania bezpośrednio u źródła, w czasie rzeczywistym, bieżącej komunikacji. Istnieje również możliwość odczytania całego twardego dysku[12]. W ocenie niemieckich prawników kontrowersyjne jest zagadnienie, czy przeszukanie online jest przeszukaniem w prawnym sensie tego słowa oraz w jakim stopniu odpowiada przeszukaniu mieszkania lub domu (tym samym spełniając konstytucyjny wymóg ustawowego uprawnienia do interwencji w podstawowe prawo do mieszkania, np. zgodnie z niemieckim Kodeksem postępowania karnego – Strafprozessordnung)[13].

-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[6] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

[7] Taki skrót wskazuje, że przeszukanie online odbywa się na polecenie rządu.

[8] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VII 2017].

[9] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[10] www.tagesschau.de/inland/faqtrojaner100.html [dostęp:12 X 2011].

[11] www.tagesschau.de/inland/faqtrojaner100.html [dostęp:12 X 2011].

[12] https://deutsche-wirtschafts-nachrichten.de/2017/06/22/bundestag-will-heimlich-weitreichende-ueberwachung-beschliessen/ [dostęp:22 VI 2017].

[13] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

Istotne znaczenie dla opisanych powyżej zastrzeżeń miał wyrok Federalnego Trybunału Sprawiedliwości (Bundesgerichtshof – BGH) z 31 stycznia 2007 r., który podważył dokonywane przez policję przeszukania online ze względu na brak właściwych przepisów prawnych w niemieckim Kodeksie postępowania karnego. Trybunał nie znalazł podstaw do autoryzacji takich działań w § 102[14] oraz § 105[15] kpk. Te paragrafy, w ocenie Trybunału, nie są podstawą do przeprowadzenia takich działań w przypadku braku zezwolenia. Zgodnie z argumentacją Trybunału niejawność przeszukania online nie odpowiada systematyce otwartych przeszukiwań, dla których podstawę stanowi Kodeks postępowania karnego[16].

Federalny Trybunał Sprawiedliwości odrzucił także § 100a[17] niemieckiego kpk jako podstawę prawną do przeszukania online, argumentując, że przy przeszukaniu online (zachowywaniu danych z komputera lub bieżącym śledzeniu pracy osoby podejrzanej) nie dochodzi do monitorowania telekomunikacji, a więc przepływu komunikacyjnego podejrzanego z osobą trzecią. Co istotne – wyrok Trybunału nie dotyczył jednak metod wykorzystywanych przez służby specjalne, których działania są uprawnione na podstawie ustaw. Zgodnie ze stanowiskiem Rządu Federalnego podstawą prawną jest w tym wypadku np. zarządzenie organu stosującego dany środek operacyjno-rozpoznawczy[18].

Doniesienia pojawiające się w niemieckich mediach potwierdzają, że niemieckie służby specjalne, m.in. Federalny Urząd Ochrony Konstytucji (Bundesamt fur Verfassungsschutz – BFV) oraz Federalna Służba Wywiadowcza (Bundesnachrichtendienst – BND) wykorzystują opisane powyżej metody w celu wykonywania ustawowych zadań. Prawdopodobnie początki stosowania wrogich technik teleinformatycznych na potrzeby ochrony bezpieczeństwa państwa sięgają 2005 r.[19] Chociaż służy specjalne nie upubliczniają danych liczbowych związanych ze stosowaniem opisanych powyżej metod, w 2009 r. w mediach niemieckich pojawiła się informacja, że w 2008 r. BND dokonała przeszukania online poza granicami Republiki Federalnej Niemiec przynajmniej

[14] § 102 – „W przypadku osoby podejrzanej o popełnienie przestępstwa lub uczestnika przestępstwa lub zbierania danych, udzielania pomocy sprawcy, utrudniania postępowania karnego lub paserstwa może być przeprowadzone przeszukanie mieszkania i innych pomieszczeń jak również osoby oraz należących do niej rzeczy zarówno w celu zajęcia jak również po tym fakcie, jeżeli zachodzą powody do przypuszczenia, że przeszukanie doprowadzi do odkrycia dowodów" (wszystkie tłum. aut.), https://www.gesetze-im-internet.de/stpo/_102.html [dostęp: 17 VIII 2017].

[15] § 105 ust. 1 – „Przeszukanie może być nakazane tylko przez sędziego, w nagłych przypadkach także przez prokuraturę i śledczych (zgodnie z § 152 ustawy o Sądzie Apelacyjnym). Sędziowie zarządzają przeszukania zgodnie z § 103 ust. 1 zdanie 2. prokuratura jest do tego uprawniona w nagłych wypadkach", https://www.gesetze-im-internet.de/stpo/_105.html [dostęp: 21 VIII 2017].

[16] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

[17] § 100a ust. 1 – „Telekomunikacja może być również monitorowana i rejestrowana bez wiedzy zainteresowanych osób jeżeli:

1) niektóre okoliczności faktyczne uzasadniają podejrzenie, że ktoś jako sprawca lub uczestnik popełnił poważne przestępstwo, o którym mowa w ust. 2, w przypadkach w których karane jest usiłowanie lub przygotowania do przestępstwa poprzez popełnienie przestępstwa,
2) czyn ten jest poważny również w indywidualnych przypadkach,
3) badanie faktów lub określenie miejsca pobytu oskarżonego w inny sposób byłoby znacznie trudniejsze lub daremne", https://www.gesetze-im-internet.de/stpo/__100a.html [dostęp: 21 VIII 2017].

[18] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland)#cite_note-5 [dostęp: 17 VIII 2017].

[19] W marcu 2005 r. ówczesny Federalny Minister Spraw Wewnętrznych Otto Schily (Socjaldemokratyczna Partia Niemiec, Sozialdemokratische Partei Deutschlands – SPD) został poproszony przez Prezydenta Federalnego Urzędu Ochrony Konstytucji Heinza Fromma o opracowanie metody niejawnego szpiegowania komputerów osób podejrzanych. Według Petera Altmeiera (Unia Chrześcijańsko-Demokratyczna, Christlich Demokratische Union – CDU) parlamentarnego Sekretarza Stanu w MSW od 2005 r. było możliwe dokonywanie przeszukania online. Parlamentarna Komisja Kontrolna została o tym poinformowana w lipcu 2005 r. https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

2500 razy. Działania obejmowały zarówno kopiowanie zawartości twardych dysków, jak i montowanie urządzenia Keylogger[20].

Zgodnie z wynikami audytu wewnętrznego w BND przedstawionymi Parlamentarnej Komisji Kontrolnej przez ówczesnego koordynatora służb specjalnych Klausa Dietera Fritschego, BND śledziła m.in. ruch pocztowy pomiędzy afgańskim ministrem Aminem Farhangiem a dziennikarzem tygodnika „ Der Spiegel". Celem działań BND był też pakistański naukowiec atomowy Abdul Quadir Khan oraz sieci komputerowe w Iraku. Śledzono również ruch poczty elektronicznej biura w Afganistanie prowadzonego przez organizację Welthungerhilfe[21].

Ta informacja ponownie wywołała polityczną dyskusję dotyczącą podstaw prawnych takich działań. Była nią bowiem zgoda wydana przez szefa BND. Po ujawnieniu tych informacji eksperci z koalicji rządowej, a także politycy opozycyjni zażądali regulacji ustawowych w tej materii. Ówczesny przewodniczący Parlamentarnej Komisji Kontrolnej Max Stadler (Wolna Partia Demokratyczna, *Freie Demokratische Partei* – FDP) stwierdził, że standardy państwa prawa w tym zakresie powinny być na nowo zdefiniowane w ustawie. Pojawiły się stwierdzenia, że przeszukanie online powinno być stosowane wyłącznie zgodnie z zasadą proporcjonalności, kontrolę zaś nad tymi działaniami powinien sprawować urzędnik mający kompetencje urzędu sądowego. Ogólne pełnomocnictwo ustawowe, na które – zgodnie z przytoczonym wcześniej stanowiskiem Rządu Federalnego – powoływało się BND, nie pozostawiało miejsca na debatę, od czasu wyroku Trybunału Konstytucyjnego w 2007 r.[22]

Federalny Sąd Konstytucyjny ponownie wypowiedział się w sprawie przeszukania online w wyroku z 27 lutego 2008 r. Dopuścił w nim takie działanie w odniesieniu do ochrony dóbr konstytucyjnych tylko pod ściśle określonymi warunkami, tj.: musi istnieć konkretne zagrożenie dla dobra prawnie chronionego, przesłanką może być np.: zabójstwo, atak terrorystyczny lub przetrzymywanie zakładników. Ponadto muszą zostać spełnione także wymogi formalne: wymagana jest zgodna sądu, zagwarantowana musi zostać również szczególna ochrona danych osobowych i integralność systemów informacyjno-technicznych[23].

Wyrok Sądu wpłynął na kształt nowelizacji ustawy o Federalnej Policji Kryminalnej (Bundeskriminalamt – BKA), nad którą prace odbywały się w 2008 r. Federalna Policja Kryminalna otrzymała kolejne uprawnienia, m.in. w treści ustawy zostały uregulowane również kontrowersyjne przeszukania online, jednak – jak wszystkie uprawnienia BKA charakteryzujące się wysokim stopniem ingerencji – podlegają one kontroli sądowej. Nowe przepisy weszły w życie 1 stycznia 2009 r., jednak już 27 stycznia 2009 r. ustawa została zaskarżona do Federalnego Sądu Konstytucyjnego[24]. Wyrokiem z 20 kwietnia

[20] www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[21] Niemiecka organizacja pozarządowa zajmująca się zwalczaniem głodu na świecie. Informację na ten temat zob. www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[22] www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[23] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[24] Nowelizacja ustawy o BKA w 2008 r. była przedmiotem szerokiej dyskusji społecznej, podnoszono m.in. że przez dodanie nowych uprawnień BKA, zarezerwowanych dotychczas dla służb specjalnych, narusza się zasadę separacji tajnych służb od policji. Rząd federalny i władze policyjne uzasadniały natomiast konieczność wprowadzenia nowych metod walki ze szczególnie poważną przestępczością, w związku z korzystaniem przez przestępców z zaawansowanych technik. Podczas wysłuchania przed Komitetem Wewnętrznym Bundestagu, ówczesny prezydent Federalnego Urzędu Policji Kryminalnej stwierdził, że przeszukania online są nieodzownym instrumentem

2016 r. ustawa została uznana za niekonstytucyjną. Sąd sformułował także wiele wytycznych dotyczących przyszłej regulacji związanych z ingerencją w podstawowe prawo do samostanowienia informacyjnego[25], m.in. zakaz prowadzenia stałego monitorowania w ramach przeszukania online oraz zapewnienie szczególnej ochrony osobom wykonującym zawody zaufania publicznego, takim jak np. adwokaci lub lekarze[26].

Stosowne zmiany w niemieckim ustawodawstwie zostały wprowadzone w 2017 r. W dniu 22 czerwca 2017 r.[27] w Bundestagu uchwalono dwie ustawy, które umożliwiają Federalnej Policji Kryminalnej dokonywanie przeszukań online w celu zwalczania najcięższych przestępstw[28], tj. terroryzmu, prania pieniędzy, korupcji osób zajmujących wysokie stanowiska, pornografii dziecięcej, zabójstw oraz przestępczości zorganizowanej, a także wprowadzają odpowiednie zmiany w niemieckim procesie karnym.

Podstawę prawną przeszukania online jest § 20k ustawy z 7 lipca 1997 r. o Federalnej Policji Kryminalnej oraz współpracy pomiędzy Federacją i krajami związkowymi w sprawach karnych (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*) dotyczący ukrytej interwencji w systemach technologii informacyjnych. Zgodnie z § 20k ust. 1:

Federalna Policja Kryminalna może bez wiedzy osoby zainteresowanej interweniować w środki techniczne w systemach informatycznych wykorzystywanych przez tę osobę oraz pozyskiwać z nich dane, jeśli określone fakty uzasadniają przypuszczenie, że istnieje niebezpieczeństwo:

1) dla nietykalności cielesnej, życia lub wolności osoby,
2) dla dóbr powszechnych, których zagrożenie narusza podstawy lub istnienie państwa lub narusza podstawy egzystencji społecznej.

Zastosowanie środków, o których mowa w zdaniu 1, jest również dopuszczalne, jeżeli z wystarczającym prawdopodobieństwem nie daje się ustalić, że bez zastosowania tych środków w niedalekiej przyszłości wystąpi szkoda, pod warunkiem, że określone fakty odnoszą się do określonego przypadku stwarzania przez osobę zagrożenia dla dóbr wskazanych w zdaniu pierwszym. Te środki mogą być wdrożone tylko, gdy jest to konieczne do wykonania zadań, o których mowa w § 4a[29] (ustawy o BKA), a w przeciw-

zapobiegania atakom terrorystycznym https://de.wikipedia.org/wiki/Bundeskriminalamtgesetz [dostęp: 7 IX 2017].

[25] Jest to prawo jednostki do decydowania o udzielaniu i wykorzystaniu danych jej dotyczących.

[26] https://de.wikipedia.org/wiki/Bundeskriminalamtgesetz [dostęp: 7 IX 2017].

[27] https//ddiv.de/download/CY4a139399X15cd3c8b94dX4b0f/Plenarprotokoll 18-240_22.06.2017.pdf [dostęp: 26 VI 2017].

[28] Ustawa z 22 czerwca 2017 r. dotycząca skutecznego i dostosowanego do praktyki wytaczania postępowania karnego (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*) oraz ustawa z 22 czerwca 2017 r. o zmianach Kodeksu karnego, ustawy o sądach dla nieletnich, Kodeksu postępowania karnego oraz innych ustaw (*Gesetz zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze*).

[29] § 4a ust. 1 – "BKA może wykonywać zadania z zakresu obrony przeciwko międzynarodowemu terroryzmowi, w przypadkach gdy:

1) zachodzi niebezpieczeństwo zagrażające terytorium całego kraju,
2) odpowiedzialność nie znajduje się w gestii policji działającej na terytorium kraju związkowego,
3) wyższy organ państwowy żąda przejęcia,
4) w takich przypadkach może również zapobiegać przestępstwom, o których mowa w art. 129a ust. 1 i 2 Kodeksu karnego i do tego celu są przeznaczone, aby zastraszyć ludność w znaczący sposób, organ władzy państwowej lub organizację międzynarodową niezgodnie z prawem przez użycie siły lub groźby użycia siły, albo polityczne, konstytucyjne, ekonomiczne lub społeczne podstawy państwa lub organizacji międzynarodowej wyeliminować lub znacząco zredukować ich wpływ, a przez sposób popełnienia tych czynów lub ich skutków może państwu lub organizacji międzynarodowej poważnie szkodzić", www.gesetze-im-internet.de/bkag_1997/20k.html [dostęp: 29 VI 2017].

nym razie byłoby bezcelowe lub zasadniczo utrudnione[30].

Istotne uprawnienie zawarte zostało w § 20l ust. 2 pkt 2 ustawy o Federalnej Policji Kryminalnej w myśl którego, w razie konieczności monitorowanie i zapisywanie telekomunikacji może również odbywać się w takiej formie, że za pomocą środków technicznych nastąpi ingerencja w informacyjno-techniczne systemy osoby będącej w kręgu podejrzeń, po to aby umożliwić monitorowanie i nagrywanie szczególnie w formie niezaszyfrowanej[31].

Natomiast w § 20l ust. 2 pkt 5 zdanie 1 ustawodawca wskazał, że (...) *na podstawie zarządzenia* (sądu – przyp. aut.) *każdy, kto wykonuje usługi telekomunikacyjne musi umożliwić Federalnej Policji Kryminalnej zastosowanie środków określonych w ust. 1* (związanych z przechwytywaniem komunikacji – przyp. aut.) *i niezwłocznie udzielić wymaganych informacji*[32].

Taki zapis oznacza, że podmioty oferujące usługi telekomunikacyjne nie mogą blokować kontroli zarządzonej przez sąd, prokuraturę lub śledczego funkcjonariusza policji. Wymienionym organom należy umożliwić przeprowadzenie takiej kontroli[33]. Jak stwierdził jeden z komentatorów: *Przedsiębiorstwa działające w przestrzeni cyfrowej muszą zastanowić się, czy chcą prowadzić swoją działalność w Niemczech, gdyż ich procedury handlowe mogą być nadzorowane przez Rząd Federalny*[34].

Rozwiązania w zakresie uprawnień operacyjno-rozpoznawczych realizowanych w celu wykrywania zagrożeń dla bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych nadal jest przedmiotem dyskusji społecznej Co istotne – działania, jakie aktualnie mogą być podejmowane przez organy śledcze, mają bardzo szeroki zasięg i nie są rozpoznawalne przez użytkownika. Zwolennicy uważają nowe rozwiązania ustawowe za konieczne w walce z terroryzmem i innymi poważnymi przejawami przestępczości. Krytycy natomiast mówią o najdalej idącej kontroli w historii Niemiec.

II. SZWAJCARIA

Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych

W obliczu wciąż wzrastającego zagrożenia terroryzmem w niektórych krajach europejskich służby specjalne dopiero teraz uzyskują nowe możliwości, aby skutecznie chronić obywateli przed ewoluującymi przejawami przestępczości. Najbardziej aktualna zmiana prawa, poprzedzona długą debatą społeczną, miała miejsce w Szwajcarii. W dniu 1 września 2017 r. weszła w życie nowa ustawa z 25 września 2015 r. o Federalnej Służbie Informacyjnej Szwajcarii (*Bundesgesetz über den Nachrichtendienst*)[35], która

[30] www.gesetze-im-internet.de/bkag_1997/20k.html [dostęp: 29 VI 2017].

[31] www.gesetze-im-internet.de/bkag_1997/20l.html [dostęp: 29 VI 2017].

[32] www.gesetze-im-internet.de/bkag_1997/20l.html [dostęp: 29 VI 2017.].

[33] www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[34] https://deutsche-wirtschafts-nachrichten.de/2017/06/22/bundestag-will-heimlich-weitreichende-ueberwachung-beschliessen/ [dostęp: 22 VI 2017].

[35] https://www.admin.ch/opc/de/classified-compilation/20120872/index.html [dostęp: 11 IX 2017].

znacznie poszerza kompetencje tej służby w zakresie wykonywania uprawnień operacyjno -rozpoznawczych, także przy wykorzystaniu systemów i sieci teleinformatycznych.

Próby wzmocnienia służb specjalnych przez umożliwienie im stosowania szerokiego spektrum metod o charakterze operacyjnym sięgają 2007 r. Wówczas to Rada Federalna[36] przyjęła projekt zmian w ustawie o bezpieczeństwie wewnętrznym i przekazała do dalszych prac na forum parlamentarnym. Konieczność zmian w prawie była argumentowana przyjęciem odpowiednich metod walki z terroryzmem. Zgodnie z założeniami tego projektu służby specjalne miały uzyskać prawo do instalowania podsłuchów oraz nadzoru wizyjnego w prywatnych pomieszczeniach, a także zapobiegawczego monitorowania poczty, telefonów, korespondencji elektronicznej oraz dysków komputerowych. Służby uzyskałyby także możliwość rejestrowania i analizowania emisji elektromagnetycznych, pochodzących z systemów technicznych oraz telekomunikacyjnych (zwłaszcza znajdujących się za granicą). Te uprawnienia określono zbiorczą nazwą „specjalne środki pozyskiwania informacji". W myśl projektu ustawy ich wykorzystanie miało być ograniczone do walki z wybranymi przejawami przestępczości, takimi jak: terroryzm, szpiegostwo, rozprzestrzenianie broni masowego rażenia oraz materiałów promieniotwórczych, a także walki z nielegalnym transferem technologii[37].

W ramach ofensywnych działań służb przy wykorzystaniu sieci teleinformatycznych pojawił się także szwajcarski wariant przeszukania online[38]. Ta prerogatywa, określona jako „tajne przeglądanie systemu przetwarzania danych", miała być wykorzystana, gdy konkretne i aktualne zdarzenia pozwalałyby przypuszczać, że osoba podejrzewana o stwarzanie zagrożenia używa dostępnego dla niej systemu danych, który jest szczególnie chroniony. W przypadku podejrzenia, że dochodzi do rozprzestrzenienia materiałów propagandowych w Internecie, których treść dotyczy nawoływania do przemocy, szwajcarskie służby miały mieć możliwość usunięcia takiej strony. Jeśli te treści nie znajdowałyby się na szwajcarskim serwerze, wówczas stosowny dokument miał być przedłożony szwajcarskiemu dostawcy usług, po zatwierdzeniu zlecenia dotyczącego blokady strony internetowej[39].

Ówczesny szef Federalnego Departamentu Sprawiedliwości i Policji[40] Christoph Blocher popierał wprowadzenie przedstawionych powyżej zmian. W jego ocenie stanowiły one dopasowanie możliwości działań szwajcarskich służb specjalnych do standardów europejskich i miały poprawić pozyskiwanie informacji niezbędnych do walki z islamskim terroryzmem. Argumentował także, że nowe rozwiązania nie stały w sprzeczności z porządkiem konstytucyjnym. Jednak większość prawicowych i lewicowych deputowanych zagłosowała przeciw projektowi, a plany nowelizacji prawa zostały zawieszone[41].

[36] Jest to najwyższy organ władzy wykonawczej, składający się z siedmiu członków wybieranych na cztery lata przez Zgromadzenie Federalne.

[37] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

[38] Jest to metoda operacyjno-rozpoznawcza polegająca na włamaniu się za pomocą środków technicznych do systemu informacyjno-technicznego, na przykład sieci komputerowej, lub do pojedynczego urządzenia, które są w użytkowaniu osoby podejrzanej, bez jej wiedzy. Szczegółowe informacje na temat tego typu czynności zostały opisane w części artykułu poświęconej rozwiązaniom stosowanym w RFN.

[39] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

[40] Jest to odpowiednik ministerstwa.

[41] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

Ponownie prace nad nowelizacją prawa rozpoczęły się w 2014 r. W poprzednim projekcie z 2007 r. uwzględniono dualizm służb specjalnych, zadania wywiadowcze i kontrwywiadowcze były bowiem realizowane przez osobne urzędy. Od 1 stycznia 2010 r. te urzędy zostały połączone, tworząc Federalną Służbę Informacyjną (Nachrichtendienst des Bundes – NDB). Jednak zarówno działające do 2010 r. służby, jak i NDB nie miały uprawnień do korzystania ze specjalnych środków pozyskiwania informacji. Nawet w przypadku działań związanych z podejrzeniem o aktywność terrorystyczną lub szpiegostwo NDB miała bardzo ograniczone możliwości działania, np. osoba podejrzana mogła być monitorowana jedynie w miejscach publicznych[42].

W ustawie o NDB, która weszła w życie 1 września 2017 r., zostały dopuszczone nowe metody, dostosowane – jak podkreślali zwolennicy ustawy – do aktualnych możliwości technicznych Nowe metody mogą być realizowane nie tylko w przestrzeni publicznej. Są to:

- monitorowanie ruchu pocztowego i telekomunikacyjnego,
- korzystanie z urządzeń monitorujących,
- penetracja systemów komputerowych i sieci komputerowych[43],
- korzystanie z urządzeń pozycjonujących,
- przeszukiwanie pomieszczeń, pojazdów itp.

Zgodnie z art. 27 ustawy nowe metody znajdują zastosowanie w związku z występującymi aktualnie zagrożeniami, jedynie w wyjątkowych sytuacjach. Mają one służyć do wykrywania szpiegów, zwalczania terroryzmu, handlu bronią lub materiałami promieniotwórczymi, ataków na infrastrukturę krytyczną, a także ochrony innych istotnych interesów narodowych[44]. Szczególnie istotne znaczenie, w ocenie projektodawców, ma nowy instrument określony w rozdziale 4 ustawy o NDB, którym jest „monitorowanie komunikacji przez łącza" (niem. *Kabelaufklärung*), ważne bowiem informacje znacznie częściej są rozprzestrzeniane przez Internet niż za pośrednictwem tradycyjnych metod komunikacji.

W myśl art. 39 ust. 1 NDB może zlecić służbie prowadzącej daną sprawę, aby uzyskała informacje dotyczące istotnych spraw odnoszących się do polityki i bezpieczeństwa wewnętrznego za granicą (art. 6 ust. 1 lit.b), bądź też aby zarejestrowała transgraniczne sygnały z sieci telekomunikacyjnych w celu ochrony innych ważnych interesów krajowych wynikających z art. 3[45]. Ten instrument może jednak znaleźć zastosowanie jedynie wtedy, gdy jeden z partnerów komunikacyjnych znajduje się za granicą. Jeżeli natomiast zarówno nadawca, jak i odbiorca znajdują się na terytorium Szwajcarii, to wówczas nie ma możliwości wykorzystania tej metody. Jeśli służba prowadząca sprawę nie jest w stanie takich sygnałów usunąć w trakcie rejestracji, należy zebrane dane zniszczyć, gdy okaże się że pochodzą z krajowych źródeł[46].

---

[42] https://www.heise.de/newsticker/meldung/Schweizer-Staatsschutz-soll-Telefone-und-Datenstroeme-ueberwachen-duerfen-2120228.html [dostęp:21 II 2014].

[43] Art. 26 ust. 1 lit. d ustawy wskazuje dwie formy takich działań:

1) dostarczanie informacji, które są dostępne w systemach lub za ich pośrednictwem przesyłane,
2) zapobieganie, utrudnianie lub spowalnianie dostępu do informacji, gdy atak za pośrednictwem systemów i sieci komputerowych skierowany jest przeciwko infrastrukturze krytycznej.

[44] W ustawie wyłączone jest natomiast stosowanie specjalnych środków pozyskiwania informacji w celu obrony przed tzw. brutalnym ekstremizmem. To wyłączenie ma skutkować uniknięciem stosowania kontroli wobec osób ze względu na ich przekonania polityczne.

[45] Ochrona porządku konstytucyjnego Szwajcarii, wspieranie szwajcarskiej polityki zagranicznej, ochrona szwajcarskich interesów gospodarczych i finansowych.

[46] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwa-

Istotne znaczenie ma jednak to, że na terenie Szwajcarii większość przepływu danych odbywa się za pośrednictwem zagranicznych serwerów i sieci, zatem komunikacja wszystkich krajowych użytkowników Internetu może być potencjalnie obiektem rozpoznania za pośrednictwem łączy. Ponadto, na mocy nowych rozwiązań, dostawcy Internetu i poczty są zobowiązani do przekazywania odpowiednich danych[47] do powiązanego z organami wojskowymi Centrum Operacji Elektronicznych (Zentrum für elektronische Operationen – ZEO), które następnie dokonuje, przy wykorzystaniu licznych haseł, oceny danych dla NDB[48]. W przypadku gdy treść danych pochodzących z zarejestrowania sygnałów odpowiada słowom kluczowym[49], które stanowią kryterium wyszukiwania, wówczas te dane mogą zostać przekazane wyłącznie do NDB. Do NDB przekazane zostają wyłącznie dane, które zawierają informacje dotyczące realizacji zlecenia związanego ze słowami kluczowymi. NDB odpowiada za ich ocenę kontrwywiadowczą[50].

W wyjątkowych sytuacjach do NDB mogą także zostać przekazane informacje dotyczące osób znajdujących się na terenie Szwajcarii. Art. 42 ust. 2 i 3 określa, że jest to dopuszczalne, gdy te dane:

1) są niezbędne do wyjaśnienia postępowania za granicą, a wcześniej zostały one zanonimizowane,
2) zawierają informacje odnoszące się do działań w kraju lub za granicą, które wskazują na konkretne zagrożenie bezpieczeństwa wewnętrznego zgodnie z art. 6 ust. 1 lit a.

Jednocześnie, w art. 42 ust. 4 ustawodawca podkreśla, że dane, które nie zawierają takich informacji, a dotyczą osób znajdujących się na terenie kraju, powinny zostać jak najszybciej zniszczone.

W myśl art. 39 ust. 4 ustawy sprawy związane z: dopuszczalnymi obszarami śledztw, w których przypadku może być stosowana opisana powyżej metoda, organizację czynności związanych z monitorowaniem komunikacji przez łącza, a także maksymalny czas przechowywania przez służbę prowadzącą zarejestrowanych danych określa rząd federalny. Zebrane dane mogą być także wymieniane z zagranicznymi służbami wywiadowczymi i organami bezpieczeństwa[51].

Dopuszczenie szerokiego spektrum środków pozwalających na gromadzenie danych zostało zrównoważone przez ustawodawcę wieloetapową procedurą, pozwalająca na ich zastosowanie. Zezwolenie na podjęcie działań, zgodnie z art. 30 ustawy, ma następujący przebieg: NDB kieruje stosowny wniosek do Federalnego Sądu Administracyjnego, po zatwierdzeniu wniosku przez sąd, zgody na przeprowadzenie działań udziela szef Federalnego Departamentu Obrony, Ochrony Ludności i Sportu[52], po wcześniejszej konsultacji z szefem Federalnego Departamentu Spraw Zagranicznych oraz szefem Federalnego De-

chungsarsenal-3331327.html [dostęp:26 IX 2016].

[47] Zgodnie z art. 43 ust. 3 i 4 operatorzy sieci telekomunikacyjnych są zobowiązania do zachowania tajemnicy. Operatorom są wypłacane rekompensaty, których wysokość ustanawia rząd federalny według kosztów dostarczenia sygnałów służbie prowadzącej.

[48] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[49] Słowa kluczowe należy tak zdefiniować, aby ich wykorzystanie w jak najmniejszym stopniu było związane z naruszeniem sfery prywatnej osób fizycznych. Ustawowo zakazane jest formułowanie słów kluczy w taki sposób, aby zawierały dane osób fizycznych lub prawnych (źródło: art. 39 ust. 3 ustawy o NDB).

[50] Art. 42 ust. 5 ustawy o NDB.

[51] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[52] NDB jest organizacyjnie umiejscowiona w tym Departamencie.

partamentu Sprawiedliwości i Policji. Sprawy o szczególnym znaczeniu mogą być przedkładane Radzie Federalnej. Procedura konsultacji odbywa się w formie pisemnej.

Osoby, w stosunku do których dopuszczone zostało zastosowanie specjalnych środków pozyskiwania informacji, są po zakończeniu operacji informowane o przyczynie, rodzaju i okresie zastosowania danej metody. Można jednak zrezygnować z tego obowiązku informacyjnego, jeśli zagrażałoby to toczącemu się postępowaniu, bezpieczeństwu wewnętrznemu, zewnętrznemu lub stwarzało zagrożenie dla osób trzecich[53].

Z uwagi na stały wzrost cyberzagrożeń[54] w NDB został założony nowy wydział, określany w mediach jako „Cyber-NDB". Utworzeniu nowej jednostki towarzyszyły społeczne obawy, że mogłaby ona podjąć aktywne czynności operacyjne bez podstawy prawnej. Do czasu przyjęcia nowej ustawy były to jedynie działania profilaktyczne ukierunkowane na ochronę. Aktualnie Cyber-NDB może również podejmować metody ofensywne związane z przenikaniem do systemów i sieci komputerowych. W celu realizacji zadań Cyber-NDB ściśle współpracuje z różnymi agencjami federalnymi, takimi jak: MELANI[55]i KOBIK[56], a także z Wojskową Służbą Informacyjną (Militaerischer Nachrichtendienst – MND)[57].

Nowa ustawa o Federalnej Służbie Informacyjnej budzi społeczne kontrowersje[58], jednak w referendum, które odbyło się we wrześniu 2016 r., 65,5 proc. obywateli Szwajcarii opowiedziało się za przyjęciem nowych ustawowych rozwiązań. W okresie poprzedzającym referendum krytyczną opinię na temat niektórych aspektów nowej ustawy wyraził Federalny Inspektor Ochrony Danych i Informacji Adrian Lobsiger. Wykazywał on, że nowe uprawnienia NDB stwarzają ryzyko naruszenia sfery prywatnej obywateli. Jako problematyczną, z punktu widzenia ochrony danych, ocenił m.in. możliwość infiltracji systemów i sieci komputerowych w celu ingerencji, przeszkodzenia lub spowolnienia w dostępie do informacji. Ponadto NDB została zwolniona z obowiązku podawania informacji do publicznej wiadomości, co może spowodować, że dostęp do niektórych dokumentów urzędowych może być niemożliwy. W ocenie Federalnego Inspektora Ochrony Danych i Informacji istnieje ryzyko, że opinia publiczna nie będzie w pełni informowana o zakresie działań służb[59].

---

[53] Art. 33 ustawy o NDB.

[54] W 2013 r. takie zalecenie wydał w raporcie rocznym Federalny Urząd ds. Zarządzania Teleinformatyką. Była to odpowiedź na cele określone przez Radę Federalną w ramach Narodowej Strategii Ochrony Szwajcarii przeciwko Cyberzagrożeniom. W ramach Strategii zidentyfikowano 16 metod, które pozwolą na wzmocnienie działań mających na celu zwalczanie cyberprzestępczości. Tych 16 metod zostało przyporządkowanych do czterech obszarów: zapobieganie, reagowanie, zapewnienie ciągłości pracy, procesy wspomagające, za: https://www.heise.de/newsticker/meldung/Neuer-Cyber-Geheimdienst-fuer-die-Schweiz-2183874.html [dostęp: 6 V 2014].

[55] Melde- und Analysestelle Informationssicherung (Centrum Raportowania i Analizy w zakresie Bezpieczeństwa Informacji). Celem działania MELANI jest identyfikowanie i przezwyciężanie niebezpieczeństw oraz pomoc operatorom infrastruktury krytycznej w kryzysowych sytuacjach, za: https://www.melani.admin.ch/melani/en/home.html [dostęp: 13 IX 2017].

[56] Jednostka Koordynująca do spraw Zwalczania Przestępczości Internetowej (Koordinationsstelle zur Bekampfung der Internetkriminalitat) odpowiedzialna za sektor cywilny, za: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html [dostęp: 13 IX 2017].

[57] https://www.heise.de/newsticker/meldung/Neuer-Cyber-Geheimdienst-fuer-die-Schweiz-2183874.html [dostęp: 6 V 2014].

[58] Podpisy za przeprowadzeniem referendum zbierali przeciwnicy nowych rozwiązań, m.in.: Partia Zielonych, Juso – młodzieżowa sekcja Partii Socjalistycznej, cześć członków Socjaldemokratycznej Partii Szwajcarii, Partia Piratów, a także takie organizacje, jak: Społeczeństwo Cyfrowe oraz Prawa Podstawowe, za: https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[59] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwa-

W obliczu takich wątpliwości istotne znaczenie ma właściwy mechanizm niezależnej kontroli nad działalnością służb, a szczególnie nad wykorzystaniem dyskusyjnych metod operacyjno-rozpoznawczych. Ustawodawca położył szczególny nacisk na niezależną kontrolę instancyjną nad monitorowaniem komunikacji przez łącza oraz rejestrowaniem i analizowaniem emisji elektromagnetycznych[60]. Zadania w tym zakresie wypełnia niezależna, wewnątrzadministracyjna instancja kontrolna, której członkowie są wybierani przez Radę Federalną na cztery lata. Rada wykonuje nadzór nad zgodnością z prawem tych metod oraz nad prawidłowością dopuszczenia zastosowania. Sprawdza także, czy sposób, w jaki informacje są opracowywane i przekazywane do NDB, jest zgodny z ustawą. Jeżeli wyniki tej kontroli okażą się niekorzystne, może zostać wydane zalecenie dla Federalnego Departamentu Obrony, Ochrony Ludności i Sportu dotyczące zakończenia działań związanych z rejestracją i monitoringiem oraz usunięcia zgromadzonych informacji. Wszelkie zalecenia, wnioski i raporty opracowywane przez organ kontrolny są niejawne.

W okresie prac nad ustawą przewidywano, że nowe metody będą wykorzystywane na poziomie około 10 przypadków rocznie. NDB nie zakłada jednak ustalonej liczby czynności, dlatego też możliwy jest wzrost korzystania z nowych uprawnień w obliczu globalnych zagrożeń, powyżej założeń przedstawionych podczas prac parlamentarnych[61]. Istotne znaczenie dla utrzymania wysokiego poziomu zaufania społecznego dla misji realizowanej przez NDB ma właściwy nadzór nad działalnością tej służby[62].

W art. 76 ustawy określono, że Rada Federalna tworzy niezależny organ nadzorujący NDB, jego przewodniczący zaś jest powoływany na sześć lat, na wniosek szefa Federalnego Departamentu Obrony, Ochrony Ludności i Sportu. Niezależny organ sprawuje nadzór nad działalnością NDB, uprawnionymi służbami w kantonach, a także innymi urzędami, które współdziałają z NDB przy wykonywaniu ustawowych uprawnień. Ten organ sprawdza działalność służby pod względem zgodności z prawem, celowości oraz skuteczności.

W celu realizacji uprawnień organ nadzorujący ma dostęp do wszelkich informacji oraz dokumentów, a także posiada dostęp do wszelkich pomieszczeń jednostek nadzoro-

chungsarsenal-3331327.html [dostęp: 26 IX 2016].

[60] Art. 79 ustawy o NDB.

[61] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[62] W ocenie komentatorów na wynik referendum niewątpliwie miały wpływ wydarzenia ostatnich lat – ataki terrorystyczne w Europie oraz liczne gwałtowne działania związane z przemocą. Kilka lat wcześniej wynik referendum prawdopodobnie byłby niepomyślny dla projektodawców nowej ustawy o NDB. Do niedawna szwajcarskie społeczeństwo pozostawało bowiem pod negatywnym wrażeniem dwóch skandali związanych z gromadzeniem informacji o obywatelach.

Pierwszy z nich miał miejsce pod koniec lat 80. XX w., gdy ujawniono, że władze państwowe oraz Policja w kantonach utworzyły w latach 1900–1990 około 900 tys. rejestracji w celu ochrony państwa. Zarejestrowano osoby, organizacje i wydarzenia. Rejestracje osobowe dotyczyły: zagranicznych anarchistów, szwajcarskich socjalistów oraz związkowców, niechcianych uchodźców politycznych oraz cudzoziemców, którzy zostali zgłoszeni. Rejestracje dotyczyły także ruchów nacjonalistycznych i faszystowskich. Wraz z pojawieniem się antykomunizmu obserwowano przede wszystkim polityków lewicowych i członków związków zawodowych. Szacuje się, że co dwudziesty obywatel szwajcarski oraz co trzeci cudzoziemiec został odnotowany w tej kartotece.

Drugi skandal miał miejsce latem 2010 r., gdy Parlamentarna Komisja Kontrolna została poinformowana o kolejnym masowym gromadzeniu danych przez służby specjalne. Około 200 tys. osób zostało zarejestrowanych bezpośrednio lub jako osoby trzecie, w większości bez odpowiedniej podstawy prawnej, za: https://de.wikipedia.org/wiki/Fischenskandal [dostęp: 11 IX 2017].

wanych. W ramach swoich nadzorczych kompetencji może on domagać się informacji oraz wglądu do akt w innych jednostkach organizacyjnych na szczeblu centralnym oraz w kantonach, jeśli tylko przedmiotowe informacje wykazują związek ze współpracą tych komórek z nadzorowanymi jednostkami. W celu wypełnienia swojej działalności organ kontrolny może mieć również dostęp do wszelkich systemów informacyjnych oraz zbiorów baz danych jednostek nadzorowanych[63]. Nad dzielnością NDB i jednostek organizacyjnych działających w poszczególnych kantonach prowadzony jest również zwierzchni nadzór parlamentarny[64].

III. ALGORYTM AUTOMATYCZNEGO PRZETWARZANIA DANYCH (TZW. CZARNE SKRZYNKI) JAKO INSTRUMENT WYKRYWANIA ZAGROŻEŃ W SYSTEMACH I SIECIACH TELEINFORMATYCZNYCH W REPUBLICE FRANCUSKIEJ

System „czarnych skrzynek" (fr. *boîtes noires*) – wprowadzony we Francji na podstawie art. L 851-3 ustawy o wywiadzie[65] – ma na celu pozyskiwanie informacji przez służby wywiadowcze przez nałożenie na operatorów telekomunikacyjnych obowiązku zainstalowania w zarządzanych przez nich sieciach algorytmów umożliwiających zidentyfikowanie połączeń mogących wskazywać na zagrożenie terrorystyczne. Te urządzenia analizują metadane komunikacyjne w celu wykrycia tzw. sygnałów słabych (fr. *signaux bas*), które mogą wykazywać określone cechy typowe dla sposobów komunikacji osób prowadzących działalność o charakterze terrorystycznym. Ten algorytm może być stosowany wyłącznie w celu zapobiegania zagrożeniom terrorystycznym. Przyjęcie ustawy wywołało we Francji liczne kontrowersje. Do najważniejszych argumentów krytycznych należy zagrożenie, jakie ten akt niesie za sobą dla prawa do prywatności, zarzut, że przewidziane mechanizmy kontrolne są niewystarczające, oraz stwierdzenie, że przyjęcie tego rodzaju norm stanowi legalizację niezgodnych z prawem działań służb wywiadowczych i jest kopią amerykańskich programów wykorzystywanych przez Agencję Bezpieczeństwa Narodowego (NSA)[66].

Algorytm stanowi jeden z najbardziej kontrowersyjnych elementów ustawy o wywiadzie. *Ratio legis* wprowadzenia tego przepisu stanowiło stworzenie instrumentu pozwalającego służbom specjalnym na skuteczną identyfikację zagrożeń terrorystycznych będących wynikiem działalności zarówno zorganizowanych komórek, jak i działalności tzw. samotnych wilków – osób nienależących w sensie formalno-organizacyjnym do żadnej struktury o charakterze terrorystycznym, prowadzących działania w sposób autonomiczny i niezależny[67]. Monitorowanie ich działalności jest nie-

[63] Art. 78 ustawy o NDB.

[64] Art. 81 ustawy o NDB.

[65] *Loi n° 2015-912 du 24 juillet relative au renseignement*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id [dostęp: 20 IX 2017].

[66] www.sous-surveillance.fr/#/ [dostęp: 20 IX 2017].

[67] Przykładem wykorzystania tej taktyki były trzy ataki z użyciem broni palnej wymierzone przeciwko francuskim żołnierzom i osobom pochodzenia żydowskiego w miastach Tuluza i Montabaun w marcu 2012 r. przez Mohammeda Meraha – Francuza pochodzenia algierskiego powiązanego z terroryzmem islamskim. Pomimo stosowania wobec Meraha środków kontroli operacyjnej i obserwacji przez służby specjalne (DGSI, DPSD) oraz zgromadzenia o nim znacznej wiedzy (m.in. o pobytach w Afganistanie i Pakistanie),

zwykle utrudnione. W przypadku gdy komórka terrorystyczna jest złożona z jednej lub dwóch osób, jej wykrycie, analiza metodologii działań i identyfikacja jej potencjalnych celów jest procesem skomplikowanym i rozłożonym w czasie. Zdolność właściwych organów do rozpoznawania i zapobiegania zagrożeniom tego typu jest ograniczona również z uwagi na znacznie mniejszy wyciek informacji na zewnątrz komórki, niż ma to miejsce w przypadku grup liczących kilkanaście lub kilkadziesiąt osób.

Przepis ustanawiający algorytm czarnych skrzynek został wprowadzony na czas określony – zgodnie z art. 25 ustawy o wywiadzie jej art. L 851-3 jest stosowany do 31 grudnia 2018 r. Do 30 czerwca 2018 r. rząd został zobowiązany do przedstawienia parlamentowi raportu dotyczącego sposobu działania instrumentu. Na uwagę zasługuje to, że system nie został dotychczas aktywowany we Francji, aktualnie jest stosowany wyłącznie w odniesieniu do danych, które nie mogą być powiązane z jej terytorium[68].

Na wstępie należy zaznaczyć, że ani opinia Rady Państwa (Conseil d'État) o projekcie ustawy o wywiadzie z 12 marca 2015 r.[69], ani decyzja Rady Konstytucyjnej 2015-713 DC z 23 lipca 2015 r. co do zgodności ustawy o wywiadzie z Konstytucją[70] nie uznały przepisów przewidujących system „czarnych skrzynek" za niezgodne z ustawą zasadniczą. Zdaniem obydwu organów istniejące w ustawie mechanizmy zabezpieczające i środki odwoławcze sprawiają, że te przepisy nie naruszają Konstytucji ani zasad demokratycznego państwa prawnego.

1. Podstawy prawne

Zgodnie z art. 851-3 kodeksu bezpieczeństwa wewnętrznego po uzyskaniu zgody premiera, wydanej po uzyskaniu zgody Narodowej Komisji Kontroli Technik Pozyskiwania Informacji (CNCTR), operatorzy telekomunikacyjni oraz osoby zajmujące się dostarczaniem usług komunikacji elektronicznej, wymienione w ustawach kodeks pocztowy i telekomunikacyjny[71] oraz w ustawie o zaufaniu do gospodarki cyfrowej[72], mogą zostać zobowiązani do wprowadzenia w administrowanych przez nich sieciach automatycznego przetwarzania danych[73] tzw. czarnych skrzynek, zgodnie z kryteriami opisanymi w autoryzacji, w celu wykrycia połączeń mogących wskazywać na zagrożenie terrorystyczne. „Czarne skrzynki" analizują w sposób masowy przepływ danych komunikacyjnych przesyłanych za pośrednictwem kabli optycznych w celu wykrycia

zapobieżenie atakowi okazało się niemożliwe.

[68] *Renseignement: des boites noires dèjà activées à l'échelle internationale*, Marc Rees, https://www.nextinpact.com/news/105039-renseignement-des-boites-noires-deja-activees-a-echelle-internationale.htm [dostęp: 20 IX 2017].

[69] *Conseil d'État, Avis sur un projet de loi relatif au renseignement, N°389.754*, www.legifrance.gouv.fr/Media/Droit-framcais/Les-avis-du-Conseil-d Etat-rendus-sur les-projets-de-loi/2015/avis_ce_prmx1504410L_cm_19_03_2015 [dostęp: 15 IX 2017].

[70] *Décision n° 2015-713 DC du 23 juillet 2015*, www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc-du-23-juillet-2015.144138.html [dostęp: 21 IX 2017].

[71] *Code des postes et des communications électroniques*, www.legifrance.gouv.fr/affichCode.do;jsessionid=DC13EAA7D9C8685F8B507A74EE79EF70.tpdila20v_1?cidTexte=LEGITEXT000006070987&dateTexte=20170920 [dostęp: 20 IX 2017].

[72] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000801164&idArticle=LEGIARTI000006421546&dateTexte=&categorieLien=cid [dostęp: 20 IX 2017].

[73] Użyte w ustawie pojęcie automatyczne przetwarzanie (fr. *traitements automatisés*) należy rozumieć jako urządzenia lub algorytmy służące do takiego przetwarzania.

tzw. sygnałów niskich mogących świadczyć o wystąpieniu elementów charakterystycznych dla zagrożeń związanych z terroryzmem.

Omawiana technika może być wykorzystywana wyłącznie w celu przeciwdziałania i zapobiegania terroryzmowi. Zbieranie danych w tym trybie musi spełniać kryteria zawarte w autoryzacji określającej w sposób wyczerpujący dane, które mają być pozyskane oraz ich parametry techniczne. Zgodę na jej zastosowanie wydaje premier, po zasięgnięciu opinii CNCTR.

Do katalogu danych zbieranych przy wykorzystaniu „czarnych skrzynek" ustawodawca zalicza wyłącznie informacje wymienione w art. L 851-1. Powyższy katalog został szerzej opisany dalej, w części poświęconej kontrowersjom związanym z ustawą.

Narodowa Komisja Technik Pozyskiwania Informacji wydaje opinię na temat wniosku o udzielenie autoryzacji wykorzystania tej techniki. Posiada ona stały, bezpośredni i nieograniczony dostęp do systemów automatycznego przetwarzania danych, a także do informacji zebranych i przechowywanych przy wykorzystaniu systemu. Komisja jest informowana o wszelkich modyfikacjach sposobów, w jakich dane są przetwarzane. Może wydawać w tym zakresie rekomendacje (art. L 851-3 II).

W fazie początkowej autoryzacja jest udzielana na dwa miesiące (z możliwością przedłużenia). Wniosek o przedłużenie zawiera wykaz określający wykrytą liczbę identyfikatorów charakterystycznych dla działań terrorystycznych wskazanych przez system wraz z analizą ich znaczenia oraz możliwości realnego występowania ewentualnych powiązań tych elementów z działaniami terrorystycznymi.

W sytuacji gdy mechanizm wykryje elementy wskazujące na zagrożenie terrorystyczne (np. wyszukiwanie słów powiązanych z terroryzmem, działalność na portalach społecznościowych), premier lub upoważniona przez niego osoba może zezwolić, po uprzednim zasięgnięciu opinii Komisji, na identyfikację osoby fizycznej, która w świetle zebranych danych może być uważana za powiązaną z działaniami o charakterze terrorystycznym, i na zgromadzenie innych informacji jej dotyczących. Te dane są przetwarzane przez 60 dni od chwili ich zebrania. Po upływie tego okresu podlegają zniszczeniu, z wyłączeniem sytuacji wystąpienia poważnych przesłanek wskazujących na zagrożenie terrorystyczne związane z jedną lub większą liczbą osób, których dotyczą zgromadzone informacje.

Identyfikacji osoby wskazanej przez system dokonuje Międzyresortowy Zespół Kontroli (Groupement interministériel de contrôle)[74]. Ten organ zwraca się do operatora usług internetowych o dostarczenie informacji o wskazanej osobie fizycznej. Kolejnym etapem, w zależności od specyfiki konkretnej sytuacji, może być prowadzenie dalszych działań operacyjno-rozpoznawczych bądź wszczęcie śledztwa lub dochodzenia.

[74] Groupement interministériel de contrôle – Międzyresortowy Zespół Kontroli, organ podległy premierowi odpowiedzialny m.in. za:

1) rejestrację wniosków o wykorzystanie technik pozyskiwania informacji;
2) rejestrację autoryzacji wykorzystania technik pozyskiwania informacji;
3) zbieranie i przechowywanie informacji i dokumentów związanych z wykorzystywaniem technik pozyskiwania informacji;
4) centralizację przechwytywania informacji ze względów bezpieczeństwa, ich transkrypcję i inne czynności związane z przetwarzaniem przechwyconych informacji;
5) działania związane z centralizacją informacji wywiadowczych.

2. Uzasadnienie stworzenia mechanizmu *boîtes noires* [75]

Do chwili przyjęcia ustawy o wywiadzie sposób wykorzystywania przez służby wywiadowcze instrumentów technicznych pozwalających na przechwytywanie danych (fr. *captation des données*) nie został we Francji uregulowany w żadnym powszechnie obowiązującym akcie normatywnym.

Charakter współczesnych zagrożeń bezpieczeństwa państwa, zarówno w wymiarze wewnętrznym, jak i zewnętrznym, wymaga efektywnych i dostosowanych do ich specyfiki instrumentów pozwalających na jak najszersze pozyskiwanie informacji, dzięki którym możliwe będzie efektywne przeciwdziałanie i zapobieganie tym zagrożeniom. Tego typu działania są dodatkowo utrudnione przez intensywny rozwój środków komunikacji elektronicznej.

Przywołany dokument wskazuje, że w stanie prawnym poprzedzającym przyjęcie ustawy o wywiadzie nie istniały jakiekolwiek podstawy prawne pozwalające na przechwytywanie, transmisję czy rejestrowanie treści rozmów ani na przesyłanie i rejestrowanie danych informatycznych przesyłanych za pośrednictwem zautomatyzowanego systemu przetwarzania danych lub danych przechowywanych w takim systemie. Potwierdza to podnoszone wielokrotnie, zarówno przez organy władzy publicznej, jak i podmioty prywatne, zarzuty, że działalność służb wywiadowczych jest prowadzona we Francji w obszarze „para-legalnym" czy „ekstra-legalnym"[76]. Należy jednak podkreślić, że studium skutków ewentualnego przyjęcia ustawy o wywiadzie odnosi się prawdopodobnie do braku tego rodzaju instrumentów w sferze operacyjno-rozpoznawczej (w dalszej części dokumentu zaznaczono, że od 2011 r. we francuskim porządku prawnym obowiązują przepisy kodeksu karnego pozwalające na przechwytywanie danych informatycznych).

Nadrzędnym celem ustawy było zatem wyposażenie organów właściwych w zakresie ochrony bezpieczeństwa państwa instrumentów pozwalających na skuteczną realizacje ich ustawowych zadań przy jednoczesnym stworzeniu mechanizmów gwarancyjnych, neutralizujących ryzyko związane z ich głęboką ingerencją w prawo do prywatności.

Zgodnie z danymi przedstawionymi w dokumencie przed wejściem w życie ustawy liczbę wniosków o udostępnienie danych o połączeniach szacowano na 350 000 w skali roku. Przyjęcie omawianego aktu normatywnego spowoduje trudny do wyrażenia w wartościach liczbowych wzrost wniosków kierowanych do operatorów telekomunikacyjnych i podmiotów utrzymujących serwery informatyczne.

Kolejnym, wartym podkreślenia argumentem jest to, że analogiczne przepisy prawne funkcjonują w większości państw demokratycznych – jako przykładowy dokument wymienia brytyjską ustawę *Regulation of Investigatory Powers Act 2000*[77] czy włoską ustawę z 2007 r.[78]

---

[75] Opracowano na podstawie dokumentu *Projet de loi relatif au renseignement, Etude d'Impat, 18 Mars 2015* dostępnego na stronie: www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P1241 200428 [dostęp: 19 IX 2017].

[76] *Conseil Constitutionnel, Décisions n° 2015-713 DC et 2015-714 DC du 23 juillet 2015 – Commentaire*, s. 2, www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2015713DC2015713dc_ccc.pdf [dostęp: 21 IX 2017].

[77] *Regulation of Investigatory Powers Act 2000*, www.legislation.gov.uk/ukpga/2000/23 [dostęp: 20 IX 2017].

[78] *Legge 3 agosto 2007, n.124 – Sistema di informazione per la sicurezza della Repubblica e nuova disci-*

Przyjęcie omawianych regulacji ma niezwykle istotne znaczenie w kontekście coraz szerszych możliwości utrzymywania niezwykle trudnych do wykrycia kontaktów przez ugrupowania terrorystyczne czy zorganizowane grupy przestępcze. Wymiana informacji przez tego rodzaju podmioty jest prowadzona za pośrednictwem zaszyfrowanych środków komunikacji elektronicznej, forów internetowych, zapisywania danych na serwerze, do których dostęp jest uzależniony od znajomości hasła czy na urządzeniu USB. Informacje mogą być przekazywane również za pomocą komputerów znajdujących się w kawiarenkach internetowych.

Kolejnym czynnikiem utrudniającym efektywną realizację zadań służb odpowiedzialnych za wywiad czy bezpieczeństwo wewnętrzne jest coraz większa dywersyfikacja środków komunikacji – zarówno telefonów, jak również komunikatorów internetowych takich jak Skype, Telegram, WhatsApp, Signal czy innych – oraz coraz wyższy stopień zaawansowania technologicznego tych urządzeń. Tradycyjne, ukierunkowane metody przechwytywania treści komunikacji określonej osoby nie są dostosowane do współczesnych zagrożeń i nie pozwalają na spójne i nieprzerwane prowadzenie czynności operacyjno-rozpoznawczych, w sytuacji gdy określona osoba posługuje się różnymi środkami komunikacji czy zmienia dane umożliwiające jej identyfikację (np. numer telefonu, adres poczty elektronicznej).

Pozyskiwanie przez służby danych informatycznych ma szczególne znaczenie w zapobieganiu i zwalczaniu zagrożeń o charakterze terrorystycznym. Masowe wykorzystywanie nowych środków komunikacji przez takie podmioty, jak tzw. Państwo Islamskie sprawia, że na przestrzeni kilku ostatnich lat znacznie wzrosła ilość danych (np. zdjęcia, pliki wideo, prywatne wiadomości), których francuskie służby nie mogą zdobyć zarówno ze względu na ograniczenia natury technologicznej, jak i prawnej. Przechwytywanie danych informatycznych dotyczących odwiedzanych stron internetowych, metadanych o komunikacji elektronicznej czy danych dotyczących zakupów dokonywanych za pośrednictwem sklepów internetowych jest, według twórców dokumentu, niezbędne do ustalenia np. zamiaru wyjazdu określonej osoby do stref działania ugrupowań terrorystycznych (Syria, Irak). Pomoże to ujawnić charakterystyczne dla procesu radykalizacji elementy, np. zakup sprzętu paramilitarnego czy utrzymywanie kontaktów z określonymi osobami czy środowiskami.

Kolejnym niezmiernie istotnym zastosowaniem omawianych regulacji będzie zapobieganie i zwalczanie proliferacji broni masowego rażenia przez monitorowanie działalności podmiotów, w większości stworzonych w sposób sztuczny (tzw. *sociétés écrans*) nabywających od podmiotów wysoce zaawansowanych technologicznie, funkcjonujących we Francji czy innych państwach europejskich, przedmioty czy substancje, które mogą służyć do produkcji komponentów takiej broni.

3. Kontrowersje związane z ewentualnym wykorzystywaniem systemu

Sygnalizowane w toku debaty publicznej wątpliwości związane ze zbieraniem przez służby wywiadowcze informacji w trybie opisanym w art. L 851-3, dodanym do ustawy kodeks bezpieczeństwa wewnętrznego przez ustawę o wywiadzie, należy rozpatrywać na dwóch płaszczyznach. Po pierwsze, według osób i podmiotów prezentujących krytyczne wobec ustawy stanowisko, niezależnie od korzyści związanych z możliwością

plina del segreto, angielska wersja językowa ustawy dostępna na stronie: www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html [dostęp: 19 IX 2017].

powzięcia w ten sposób informacji o potencjalnych zagrożeniach terrorystycznych, ten instrument pociąga za sobą ryzyko stworzenia systemu masowej inwigilacji, działającego bez dostatecznych mechanizmów ograniczających, które zmniejszałyby ryzyko naruszenia prywatności osób niezwiązanych w żaden sposób z działalnością zagrażającą bezpieczeństwu państwa. Po drugie, ustalenie katalogu danych, do których dostęp będzie możliwy dzięki wykorzystaniu algorytmu, jest zadaniem skomplikowanym z uwagi na sposób sformułowania właściwych przepisów i liczne odesłania ustawowe.

Jako jedno z zagrożeń związanych z systemem „czarnych skrzynek" wskazuje się na działanie tych urządzeń na podstawie algorytmu wykorzystującego sztuczną inteligencję, którego szczegółowy sposób działania jest objęty tajemnicą. Zadaniem mechanizmu jest wykrycie elementów typowych dla działań o charakterze terrorystycznym przez analizę zachowań w Internecie, co w dalszej kolejności może doprowadzić do identyfikacji konkretnej osoby, która może być powiązana z działalnością terrorystyczną. Wątpliwości opinii publicznej budzi brak możliwości ustalenia, jakie konkretnie aspekty wykorzystywania sieci podlegają badaniu i jakie zachowania mogą doprowadzić do tego, że dana osoba zostanie wskazana przez system jako mogąca stwarzać zagrożenie[79].

Niepewność natury interpretacyjnej jest również związana z określeniem, jakie konkretnie dane będą podlegać analizie dokonywanej przez system. Trzeba tu podkreślić, że jego ustalenie wymaga interpretacji nie tylko przepisów ustawy o wywiadzie i kodeksu bezpieczeństwa wewnętrznego, lecz także innych aktów prawnych, co sprawia, że zrozumienie rzeczywistego charakteru „czarnych skrzynek" przez osobę nieposiadającą specjalistycznej wiedzy z zakresu prawa i nowoczesnych technologii, niezależnie od przyjęcia dekretu ze stycznia 2016 r. wyjaśniającego wiele istotnych aspektów problemu, było zadaniem skomplikowanym. Dekret, o którym mowa, został przedstawiony szerzej w dalszej części artykułu.

Punktem wyjścia dla określenia ww. katalogu jest zdanie drugie art. L 851-3 par. I, zgodnie z którym:

> Automatyczne przetwarzanie wykorzystuje wyłącznie informacje lub dokumenty, o których mowa w art. L 851-1, nie zbierając innych danych niż te, które odpowiadają parametrom wyjściowym i w sposób nie pozwalający na identyfikację osób, których te informacje lub dokumenty dotyczą[80].

Zgodnie z art. L 851:

> Na zasadach opisanych w rozdziale I tytule II niniejszej księgi[81] może zostać autoryzowane, za pośrednictwem operatorów komunikacji elektronicznej i osób wymienionych w art. L 34-1 kodeksu poczty i komunikacji elektronicznej[82] jak również osób wymie-

[79] G. Chapeau, *Que feront les boîtes noires de la Loi Renseignement?*, 3 IV 2015 r., www.numerama.com/magazine/32699-que-feront-les-boites-noires-de-la-loi-renseignement.html [dostęp: 20 IX 2017].

[80] Wszystkie tłumaczenia aut.

[81] Rozdział I tytułu II księgi VII ustawy (*De l'autorisation de mise en oeuvre*); kodeks bezpieczeństwa wewnętrznego dotyczy autoryzacji wykorzystywania technik pozyskiwania informacji.

[82] *Code des postes et des communications électroniques*:

Art. L 34-1.

„I. Niniejszy artykuł stosuje się do przetwarzania danych osobowych w toku dostarczania usług komunikacji elektronicznej; stosuje się również do sieci wykorzystujących urządzenia zbierania danych identyfikacyjnych.

nionych w pkt 1 i 2 art. 6 ustawy n°2004-575 z dnia 21 lipca 2004 roku o zaufaniu do gospodarki cyfrowej[83], zbieranie informacji i dokumentów przetwarzanych lub przechowywanych przez określone sieci lub usługi komunikacji elektronicznej, w tym danych technicznych dotyczących identyfikacji numeru abonenta lub danych o połączeniu z usługą komunikacji elektronicznej, danych dotyczących spisu wszystkich numerów abonamentu lub danych o połączeniu wskazanej osoby, danych o lokalizacji używanych przez nią urządzeń końcowych i danych dotyczących komunikacji abonenta obejmujących listę numerów połączeń wychodzących i przychodzących oraz czas trwania i datę połączeń.

Analiza przepisów art. L 851-1 ustawy kodeks bezpieczeństwa wewnętrznego, art. L 34-1 kodeksu poczty i telekomunikacji i art. 6 ustawy o zaufaniu do gospodarki cyfrowej prowadzi do wniosku, że obowiązkiem wynikającym z art. L 851-3 mogą zostać objęci operatorzy komunikacji elektronicznej, dostawcy Internetu w rozumieniu ogólnym oraz podmioty hostingowe (co powoduje, iż „czarne skrzynki" obejmują usługi, takie jak YouTube, Gmail czy Facebook)[84].

Istotne znaczenie ma również pojęcie informacji i dokumentów, którym posługuje się art. L 851-1 i do którego odsyła art. L 851-3. Art. L 851-1 zawiera z kolei odesłanie do art. 34-1 kodeksu poczty i telekomunikacji, którego par. VI stanowi, że:

Dane przechowywane i przetwarzane na warunkach określonych w par. III, IV i V dotyczą wyłącznie identyfikacji osób korzystających z usług dostarczanych przez operatorów, charakterystyki technicznej komunikacji zapewnianej przez tych operatorów oraz lokalizacji urządzeń końcowych. W żadnym wypadku nie mogą one ujawniać treści korespondencji ani informacji, z którymi zapoznano się w jakiejkolwiek formie w toku tej komunikacji.

Wątpliwości interpretacyjne związane z zakresem wymienionych pojęć zostały wyjaśnione przez stworzenie definicji informacji i dokumentów na podstawie *Dekretu nr 2016-67 z dnia 29 stycznia 2016 roku dotyczącego technik pozyskiwania informacji*[85].

II. Operatorzy komunikacji elektronicznej, zwłaszcza osoby, których działalność polega na oferowaniu dostępu do usług komunikacji online, usuwają lub czynią anonimowymi wszystkie dane o ruchu, z zastrzeżeniem par. III, IV, V i VI.

Osoby dostarczające usługi komunikacji elektronicznej wprowadzają, z zastrzeżeniem poprzedniego akapitu, wewnętrzne procedury pozwalające na realizację żądań właściwych organów.

Osoby, które z tytułu głównej lub dodatkowej działalności zawodowej oferują połączenia umożliwiające komunikację online przez dostęp do sieci, również bez wynagrodzenia, podlegają na mocy niniejszego artykułu przepisom mającym zastosowanie do operatorów komunikacji elektronicznej. (…)"

[83] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*:

Art. 6

„I.1. Osoby, których działalność polega na oferowaniu dostępu do usług komunikacji elektronicznej online informują swoich abonentów o istnieniu środków technicznych pozwalających na ograniczenie dostępności niektórych usług lub ich selekcję i proponują im co najmniej jeden taki środek. (…)

2. Osoby fizyczne lub prawne zapewniające, również nieodpłatnie, udostępnienie usług komunikacji elektronicznej online, przechowywanie sygnałów, treści pisemnych, obrazów, dźwięków lub jakichkolwiek wiadomości wygenerowanych przez odbiorców tych usług, nie podlegają odpowiedzialności cywilnej związanej z działalnością lub informacjami przechowywanymi na żądanie odbiorcy tych usług, jeżeli nie posiadali wiedzy o ich przestępczym charakterze lub o faktach i okolicznościach mogące wskazywać na ten charakter, jeżeli, od chwili, w której powzięli tego rodzaju informacje, podjęli niezwłoczne działania w celu usunięcia tych danych i uniemożliwienia dostępu do nich. (…)".

[84] *Que feront les boîtes noires ...*

[85] *Décret n°2016-67 du 29 janvier 2016 relatif aux techniques de renseignement*, www.legifrance.gouv.

Art. R 851-5, dodany na podstawie art. 2 dekretu do kodeksu bezpieczeństwa wewnętrznego, stanowi:

> Art. R 851-5 – I. Informacje i dokumenty, o których mowa w art. L 851-1 obejmują, z wyłączeniem treści wymienianej korespondencji lub informacji, z którymi się zapoznano:
>
> 1. Informacje wymienione w art. R.10-13 i R 10-14 kodeksu poczty i komunikacji elektronicznej oraz w art. 1 dekretu nr 2011-219 z dnia 25 stycznia 2011 dotyczącego przechowywania i przekazywania danych pozwalających na identyfikację osób biorących udział w tworzeniu treści umieszczonych w Internecie;
>
> 2. Dane techniczne inne niż wymienione w pkt 1, które:
>
> a) pozwalają na identyfikację urządzeń końcowych;
> b) dotyczą dostępu do urządzeń końcowych w sieciach i do usług komunikacji on-line;
> c) dotyczą przesyłu/dostarczania komunikacji elektronicznej przez sieci;
> d) dotyczą identyfikacji lub weryfikacji użytkownika połączenia, sieci lub usługi komunikacji on-line;
> e) dotyczą charakterystyki urządzeń końcowych i danych konfiguracji oprogramowania.
>
> II. Wyłącznie informacje i dokumenty wymienione w pkt 1 par. I mogą być zbierane na podstawie art. L 851-1. Zbieranie to ma odbywa się z opóźnieniem.
>
> Informacje wymienione w pkt 2 par. I mogą być zbierane wyłącznie w toku stosowania art. L 851-2 i L 851-3 na zasadach opisanych w tych artykułach i z zastrzeżeniem art. R 851-9.

Zarówno art. L 851-1, jak i L 851-3, a także przywołany przepis R 851-5 wprowadzony na mocy dekretu z 29 stycznia 2016 r. przewidują wyłącznie możliwość zbierania i przetwarzania określonych kategorii danych technicznych informujących o poszczególnych parametrach połączeń, nie pozwalają jednak na identyfikację treści rozmów czy korespondencji. Należy zatem uznać, że analizowane przepisy pozwalają na zbieranie i przetwarzanie przez algorytm wyłącznie metadanych. Żadna z kategorii informacji wymienionych w art. L 851-1 czy w pozostałych cytowanych przepisach nie wskazuje, aby było możliwe uzyskanie dostępu do treści komunikacji. Przeciwnie – art. R 851-5 wyraźnie wyłącza z katalogu pojęć wchodzących w zakres definicji informacji i dokumentów treść wymienianej korespondencji oraz informacje, z którymi się zapoznano.

Odnosząc się do mechanizmów mających na celu ochronę praw i wolności, w tym prawa do prywatności, trzeba zwrócić uwagę na art. R 851-9, który podobnie jak art. R 851-5 został dodany do kodeksu bezpieczeństwa wewnętrznego na mocy przywołanego powyżej dekretu. Zgodnie z art. R 851-9

> Informacje i dokumenty zebrane na podstawie niniejszego tytułu nie mogą, bez autoryzacji, o której mowa w art. L 852-1 i art. L 853-2, być wykorzystywane w celu uzyskania dostępu do treści wymienianej korespondencji lub informacji, z którymi się zapoznano.

fr/affichTexte.do?cidTexte=JORFTEXT00003194088&dateTexte=&categorieLien=id [dostęp: 20 IX 2017].

Cytowane przepisy rzeczywiście pozwalają na odtworzenie wielu aspektów życia prywatnego danej osoby – m.in. na ustalenie osób, z którymi utrzymuje ona regularne kontakty, usługi komunikacji elektronicznej, z których korzysta czy uzyskanie informacji o miejscach, w jakich przebywała w konkretnym czasie. Na marginesie należy wspomnieć, że zgodnie z interpretacją Trybunału Sprawiedliwości Unii Europejskiej, wyrażoną w orzeczeniu Tele2[86], krajowe uregulowania przewidujące uogólnione i niezróżnicowane (nieselektywne) zatrzymywanie przez operatorów telekomunikacyjnych wszystkich danych o ruchu i danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników dla celów zwalczania przestępczości są niezgodne z Kartą Praw Podstawowych Unii Europejskiej i dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i prywatności w sektorze łączności elektronicznej[87]. Biorąc pod uwagę konstrukcję przepisów dotyczących algorytmu wprowadzonego na mocy ustawy o wywiadzie, nie sposób uznać, że powoduje on „uogólnione" i „niezróżnicowane" czy „nieselektywne" zbieranie danych. Ustawodawca jasno wskazał cel, w jakim instrument ten może być zastosowany (wyłącznie zapobieganie terroryzmowi) oraz ograniczył katalog danych zbieranych przez mechanizm przez odesłanie do art. L 851-1 i do przepisów innych aktów prawnych. Ponadto, stworzył definicję informacji i dokumentów w art. R 851-5. Analiza tych czynników sprawia jednocześnie, że określanie tego mechanizmu mianem środka masowej inwigilacji jest nietrafne, gdyż celem algorytmu nie jest nieselektywne zbieranie wszystkich możliwych informacji, lecz ściśle ukierunkowane zbieranie określonych w ustawie kategorii metadanych i tylko w celu zapobiegania zagrożeniom terrorystycznym.

4. Charakterystyka najważniejszych opinii legislacyjnych i orzeczenia Rady Konstytucyjnej odnośnie do zgodności ustawy o wywiadzie z Konstytucją

4.1. Opinia Narodowej Komisji Informatyki i Wolności (CNIL)

W początkowej fazie procesu legislacyjnego związanego z tworzeniem ustawy o wywiadzie strona rządowa argumentowała, że metadane, które mają być pozyskiwane dzięki stworzeniu systemu, będą anonimowe, przez co nawet ich ewentualna późniejsza analiza nie stwarza zagrożenia dla prywatności. Przeciwny pogląd wyraziła Narodowa Komisja Informatyki i Wolności (CNIL). Zdaniem tego organu analiza metadanych przez opisywany algorytm polega m.in. na przetwarzaniu danych osobowych, w konsekwencji zaś musi być zgodne z zasadą proporcjonalności[88].

Zgodnie z argumentami CNIL przedstawionymi w opinii nr 2015-078 w sprawie projektu ustawy o wywiadzie[89] algorytm przewidziany w ustawie o wywiadzie ma na celu wykrywanie tzw. sygnałów słabych mogących świadczyć o przygotowywaniu aktu

[86] Wyrok Trybunału z 21 XII 2016 r. w połączonych sprawach C-203/15 i C-698/15, www.curia.europa.eu. [dostęp: 20 IX 2017].

[87] *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)* – Dz. Urz. Wspólnot Europejskich L 201 z 31 VII 2002 r.

[88] *Bulk Collection: Systematic Government Access to Private-Sector Data*, F.H. Cate, J.X. Dempsey (red.), s. 55–56, www.books.google.pl [dostęp: 15 IX 2017].

[89] *Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement*, s. 9 www.cnil.fr/sites/default/files/typo/document/D2015-078-PJLRenseignement.pdf [dostęp: 15 IX 2017].

terrorystycznego na podstawie określonych kryteriów technicznych. Pod pojęciem tych sygnałów rozumie się np. dane techniczne mogące świadczyć o zamiarach czy sposobie działania charakterystycznych dla działań terrorystycznych lub pozostawione przez zaangażowane osoby ślady działalności w Internecie, lub informacje o ich komunikacji, których osobna, jednostkowa analiza nie pozwoliłaby na stwierdzenie, że te osoby mogą prowadzić działalność o charakterze terrorystycznym. Na marginesie trzeba zaznaczyć, że opinia CNIL zwraca w tym miejscu uwagę na niezmiernie istotny aspekt zagadnienia wykrywania zagrożeń w systemach i sieciach elektronicznych – w wielu przypadkach wyłącznie pozyskanie określonego zbioru informacji może pozwolić na identyfikację konkretnego zagrożenia, wzorców zachowań czy osób zaangażowanych w działalność terrorystyczną. Informacje określane jako sygnały słabe mogą stworzyć całościowy obraz danego zagrożenia po ich odniesieniu do większej grupy osób, osobno zaś nie będą przedstawiać jakiejkolwiek wartości z punktu widzenia wywiadowczego. Treść raportu CNIL w sposób bardzo precyzyjny ilustruje istotę różnic między instrumentami masowego pozyskiwania danych a tradycyjnymi, zbliżonymi do kontroli operacyjnej narzędziami ukierunkowanymi wykorzystywanymi przez służby. Analogiczne argumenty są podnoszone w przedstawionych w części dotyczącej Wielkiej Brytanii dokumentach charakteryzujących sposób działania tzw. *bulk powers*, wprowadzonych na mocy ustawy *Investigatory Powers Act*.

Komisja CNIL zasugerowała w opinii zwrócenie przez rząd szczególnej uwagi na doniosłe znaczenie prawidłowego i konkretnego sformułowania przepisów wprowadzających omawiany mechanizm, tak aby jego interpretacja miała charakter zawężający, a wykorzystywanie w praktyce ograniczało się do sytuacji rzeczywiście związanych z zagrożeniem terrorystycznym zgodnie z zasadą proporcjonalności. Pomimo że celem algorytmu jest wykrycie elementów wskazujących na możliwość zaistnienia zdarzenia o charakterze terrorystycznym, jego działanie sprowadza się do zbierania i analizy informacji mogących bezpośrednio lub pośrednio identyfikować konkretną osobę. Zdaniem CNIL świadczy o tym przewidziany w ustawie mechanizm wyrażenia przez premiera zgody na identyfikację określonej osoby, po uzyskaniu opinii CNCTR, jeżeli algorytm wykryje czynniki wskazujące na możliwość zagrożenia terrorystycznego. Identyfikacja osoby jest zatem możliwa na podstawie danych zebranych przez „czarne skrzynki". Organ podkreśla, że automatyczne przetwarzanie danych przez opisywany system musi czynić zadość wymogom wynikającym z *Ustawy z dnia 6 stycznia 1978 r. o informatyce, bazach danych i wolnościach obywatelskich*[90]. CNIL nie stwierdza jednak w przywołanej opinii, że wprowadzenie na podstawie aktu prawa powszechnie obowiązującego systemu tzw. czarnych skrzynek stanowi *per se* naruszenie prawa do prywatności, niedające się pogodzić z zasadami demokratycznego państwa prawnego.

4.2. Opinia Rady Państwa

Przywołana opinia Rady Państwa dokonuje na wstępie krótkiej charakterystyki projektu ustawy o wywiadzie. Do jego najważniejszych elementów należy określenie warunków, w jakich służby wywiadowcze mogą posługiwać się – w określonych enumeratywnie celach – technikami pozyskiwania informacji opisanymi w ustawie, oraz wprowadzenie szczególnego trybu autoryzacji ich wykorzystania dokonywanej przez

[90] *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 [dostęp: 15 IX 2017].

premiera po uzyskaniu opinii CNCTR. W opinii podkreślono istotne znaczenie roli Rady Państwa jako organu właściwego do rozpoznawania skarg na zastosowanie technik pozyskiwania informacji wprowadzonych na mocy ustawy o wywiadzie, do których złożenia, zgodnie z art. L 841-1 kodeksu bezpieczeństwa wewnętrznego, uprawnione zarówno osoby fizyczne, jak i CNCTR.

Rada Państwa zaznacza ponadto, że w toku procesu legislacyjnego dążyła do znalezienia odpowiedniej równowagi między względami związanymi z ochroną bezpieczeństwa narodowego a poszanowaniem życia prywatnego, zgodnie z art. 2 *Powszechnej Deklaracji Praw Człowieka i Obywatela* oraz art. 8 *Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Z dokumentu wynika, że głównym założeniem tego organu było dążenie do wzmocnienia i doprecyzowania przepisów o charakterze gwarancyjnym mających na celu ochronę praw i wolności. Rada Państwa szczególną uwagę przywiązywała do zawarcia w ustawie przepisów przewidujących kontrolę niezależnego organu administracyjnego nad wykorzystywaniem technik pozyskiwania informacji, zarówno w momencie autoryzacji, jak i w czasie ich stosowania, oraz jednocześnie upoważniających Radę Państwa do kontroli sądowej nad stosowaniem przewidzianych w ustawie instrumentów.

Zdaniem organu najważniejszą gwarancją poszanowania praw i wolności obywatelskich w toku wykorzystywania przewidzianych w ustawie ingerujących w prawo do prywatności instrumentów służących gromadzeniu informacji jest zawarcie w ustawie precyzyjnego i zamkniętego katalogu celów, dla których te techniki mogą zostać wykorzystane. Zgodnie z art. L 811-3 ustawy kodeks bezpieczeństwa wewnętrznego, wprowadzonym do tego aktu na mocy art. 2 ustawy o wywiadzie, służby wywiadowcze mogą posługiwać się technikami przewidzianymi w tytule V księgi VIII kodeksu w celu zbierania informacji wywiadowczych istotnych z punktu widzenia obronności i wspierania następujących fundamentalnych interesów państwa:

1. Niepodległości, integralności terytorialnej i obrony narodowej.
2. Istotnych interesów polityki zagranicznej, wykonywania zobowiązań europejskich i międzynarodowych Francji oraz zapobiegania wszelkim formom zagranicznej ingerencji.
3. Istotnych interesów gospodarczych, przemysłowych i naukowych Francji.
4. Zapobiegania terroryzmowi.
5. Zapobiegania:
   1) zamachom na republikańską formę rządów,
   2) działaniom zmierzającym do odtworzenia ugrupowań rozwiązanych na podstawie art. L 212-1[91],

[91] Art. L 212-1 ustawy kodeks bezpieczeństwa wewnętrznego:
Ulegają rozwiązaniu, na mocy dekretu Rady Ministrów, stowarzyszenia i ugrupowania:
1. Prowokujące do zbrojnych manifestacji ulicznych;
2. Posiadające charakter grup zbrojnych lub prywatnych milicji, ze względu na ich formę lub militarny sposób działania;
3. Których celem jest dokonanie zamachu na integralność terytorialną lub siłowa zmiana republikańskiej formy rządów;
4. Których działalność dąży do podważenia legalności rządów republikańskich;
5. Których celem jest pozyskiwanie osób skazanych za współpracę z wrogimi państwami lub propagowanie takiej współpracy;
6. Które prowokują do dyskryminacji, nienawiści lub agresji w stosunku do osób lub grup z uwagi na ich pochodzenie, przynależność do określonej grupy etnicznej, narodu, rasy lub religii lub które propagują idee lub teorie usprawiedliwiające lub zachęcające do takiej dyskryminacji, nienawiści lub przemocy;

3) zbiorowym wystąpieniom z użyciem przemocy stwarzających poważne zagrożenie dla bezpieczeństwa publicznego,

6. Zapobiegania działalności zorganizowanych grup przestępczych.
7. Zapobiegania proliferacji broni masowego rażenia.

Kolejną fundamentalną gwarancją w opinii Rady Państwa jest zawarcie w ustawie przepisów regulujących tryb autoryzacji wykorzystywania instrumentów wprowadzonych na mocy ustawy o wywiadzie. Sposób dokonywania autoryzacji ma szczególne znaczenie w przypadku „czarnych skrzynek" z uwagi na to, że ustawodawca zdecydował się na przyjęcie w tym zakresie przepisów szczególnych powodujących, iż tryb autoryzacji tego instrumentu jest nieco odmienny od pozostałych narzędzi gromadzenia informacji.

Jak już wspomniano, zgodnie z zasadą ogólną wykorzystanie technik pozyskiwania informacji autoryzuje premier, po uprzednim zasięgnięciu opinii CNCTR (art. L 821-1 kodeksu bezpieczeństwa wewnętrznego). Szczegółowe uregulowania dotyczące autoryzacji zostały zawarte w art. L 821-2. Autoryzacja jest wydawana na pisemny i uzasadniony wniosek ministra obrony, spraw wewnętrznych, sprawiedliwości lub ministrów właściwych w zakresie gospodarki, budżetu lub ceł. Minister może upoważnić do składania tego rodzaju wniosków wyłącznie swoich bezpośrednich współpracowników upoważnionych do dostępu do informacji stanowiących tajemnicę obrony narodowej (fr. *secret de la défense nationale*). We wniosku muszą być określone następujące elementy:

1. Technika lub techniki, które mają zostać wykorzystane.
2. Służba, w imieniu której składany jest wniosek o udzielenie autoryzacji.
3. Cel lub cele, które mają zostać osiągnięte dzięki zastosowaniu określonej techniki.
4. Motywy przemawiające za zastosowaniem środków opisanych w autoryzacji.
5. Czas trwania autoryzacji.
6. Osoby, miejsca lub pojazdy, w stosunku do których mają zostać zastosowane techniki pozyskiwania informacji.

Wniosek jest przekazywany przewodniczącemu CNCTR lub, w razie jego nieobecności, jednemu z członków organu, którzy przedstawiają swoją opinię premierowi w ciągu 24 godzin. Jeżeli określony wniosek jest rozpatrywany przez zmniejszony skład lub przez pełny skład Komisji, premier jest o tym informowany, opinia zaś wydawana jest w tym przypadku w ciągu 72 godzin i przekazywana niezwłocznie premierowi. Jeżeli opinia nie zostanie przekazana premierowi w czasie, odpowiednio – 24 lub 72 godzin, wymóg jej uprzedniego uzyskania przed udzieleniem autoryzacji jest uważany za spełniony (art. L 821-3). Autoryzacja na zasadach ogólnych jest udzielana maksymalnie na okres 4 miesięcy (art. L 821-4).

Należy wyróżnić dwie zasadnicze różnice występujące w procesie autoryzacji wykorzystania „czarnych skrzynek" i pozostałych technik pozyskiwania informacji:

1) pierwsza autoryzacja w odniesieniu do tzw. *boîtes noires* może być udzielona na okres dwóch miesięcy. W zakresie ewentualnego przedłużenia art. L 851-3 II odsyła do przepisów ogólnych dotyczących przedłużenia stosowania pozostałych technik pozyskiwania informacji – wynika z tego zatem, że stosowanie „czarnych skrzynek" może zostać przedłużone o kolejne cztery miesiące po upływie początkowego, dwumiesięcznego terminu,

7. Które prowadzą, na terytorium Francji lub poza nim, działania mające na celu dokonanie aktów terrorystycznych we Francji lub za granicą.

2) przesłanką uzasadniającą stosowanie mechanizmu „czarnych skrzynek" jest wyłącznie zapobieganie terroryzmowi.

Ustawodawca wprowadził zatem w sposób expressis verbis daleko idące ograniczenie przesłanek uzasadniających stosowanie omawianego instrumentu. Porównanie norm regulujących funkcjonowanie „czarnych skrzynek" i pozostałych technik pozyskiwania informacji prowadzi zatem do wniosku, że ewentualne użycie tego środka podlega szerokim ograniczeniom przedmiotowym i jest możliwe wyłącznie w celu zapobiegania terroryzmowi. Ustawa nie przewiduje natomiast możliwości jego wykorzystania np. w celach kontrwywiadowczych czy ochrony interesów gospodarczych. Nie można zatem zgodzić się z przedstawianą wielokrotnie we francuskich mediach tezą, że „czarne skrzynki" stanowią nieukierunkowany instrument masowej inwigilacji niepodlegający dostatecznej kontroli. Zarówno przepisy ograniczające cele, w jakich algorytm ten może być wykorzystywany i ograniczenie czasu trwania jego autoryzacji w porównaniu z innymi technikami, jak i opisane w części dotyczącej podstaw prawnych rozgraniczenie między samym stosowaniem mechanizmu a identyfikacją konkretnej osoby przez GIC na podstawie danych zebranych przez „czarne skrzynki" powodują, że pozyskanie za jego pomocą informacji przez służby wywiadowcze jest poddane daleko idącym ograniczeniom.

4.3. Decyzja Rady Konstytucyjnej nr 2015-713 z 13 lipca 2015 r. [92]

Rada Konstytucyjna, zgodnie z art. 61 Konstytucji, w decyzji nr 2015-713 dokonała oceny zgodności ustawy o wywiadzie z Konstytucją[93]. Wniosek o zbadanie konstytucyjności tego aktu złożyli przewodniczący Senatu, prezydent oraz grupa 60 posłów.

Rada Konstytucyjna wydała orzeczenie po uprzednim zbadaniu zgodności ustawy z przepisami Konstytucji, kodeksu obrony, kodeksu karnego, kodeksu bezpieczeństwa wewnętrznego, ustawy o zaufaniu do gospodarki cyfrowej, kodeksu poczty i komunikacji elektronicznej i innych aktów prawnych. Wnioskodawcy zwrócili się o zbadanie zgodności przepisów ustawy o wywiadzie z prawem do poszanowania życia prywatnego, swobody komunikacji, swobody wypowiedzi oraz prawa do wniesienia skutecznego środka odwoławczego.

Charakteryzując treść fundamentalnych zasad francuskiego porządku prawnego – „norm referencyjnych"[94] (fr. *normes de référence*) Rada wskazała, że[95]:

- zgodnie z art. 34 Konstytucji na ustawodawcy ciąży obowiązek stworzenia zasad dotyczących fundamentalnych gwarancji przyznanych obywatelom mających na celu umożliwienie pełnego korzystania z ich praw i wolności, zapewnienia niezbędnej równowagi pomiędzy zapobieganiem zamachom na bezpieczeństwo publiczne, co jest niezbędne dla ochrony praw i nadrzędnych zasad konstytucyjnych, a korzystaniem z gwarantowanych na mocy Konstytucji praw i wolności, do których należą prawo do poszanowania życia prywatnego, nienaruszalność miejsca zamieszkania i tajemnica korespondencji chronione na podstawie art. 2 i 4 Deklaracji Praw Człowieka i Obywatela z 1789 r.;

[92] *Décision n° 2015-713 DC du 23 juillet 2015*, www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc-du-23-juillet-2015.144138.html [dostęp: 21 IX 2017].

[93] *Constitution du 4 octobre 1958*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006071194, [dostęp: 22 IX 2017].

[94] www.lexinter.net/JF/normes_juridiques.htm [dostęp: 22 IX 2017].

[95] Pkt 3, 4 i 5 decyzji 2015-713.

- zgodnie z art. 5 Konstytucji Prezydent Republiki jest gwarantem niepodległości i integralności terytorialnej;
- zgodnie z art. 21 Konstytucji premier kieruje pracami rządu i jest odpowiedzialny za sprawy związane z obroną narodową, sekret obrony narodowej zaś stanowi jeden z elementów mających na celu ochronę fundamentalnych interesów państwa, m.in. niepodległość i integralność terytorialna;
- zgodnie z art. 66 Konstytucji nikt nie może być w sposób arbitralny pozbawiony wolności, a władza sądownicza jest strażnikiem wolności osobistej i zapewnia jej poszanowanie na zasadach przewidzianych w ustawie;
- art. 16 *Deklaracji Praw Człowieka i Obywatela* z 1789 r. gwarantuje prawo do wniesienia skutecznego sądowego środka odwoławczego, prawo do rzetelnego procesu, a także zasadę kontradyktoryjności.

Rozważania Rady Konstytucyjnej odnoszące się do zagadnienia zgodności z Konstytucją przepisu przewidującego wprowadzenie mechanizmu „czarnych skrzynek" sprowadzają się do stwierdzenia, że ten przepis spełnia wymogi konstytucyjności i nie stanowi nieproporcjonalnego zagrożenia prawa do prywatności. Poniżej przedstawiono argumenty Rady zawarte w pkt 58-61 decyzji.

> 58. Biorąc pod uwagę, iż:
>
> – art. L 851-3 kodeksu bezpieczeństwa wewnętrznego stanowi, iż na operatorów telekomunikacyjnych i na osoby wymienione w art. L 851-1 może być nałożony obowiązek zainstalowania urządzeń technicznych służących do automatycznego przetwarzania danych mających na celu, w zależności od parametrów wskazanych w autoryzacji, wykrywanie połączeń mogących świadczyć o zagrożeniu terrorystycznym;
>
> – urządzenia te wykorzystywać będą wyłącznie informacje i dokumenty, o których mowa w art. L 851-1 nie zbierając innych danych niż odpowiadające pierwotnym parametrom i nie zezwalając na identyfikację osób, których te informacje lub dokumenty dotyczą;
>
> – podczas gdy urządzenia służące do automatycznego przetwarzania danych wykryją dane, które mogą wskazywać na istnienie zagrożenia terrorystycznego, identyfikacja tej osoby lub osób i zebranie dotyczących ich danych będą mogły zostać autoryzowane przez Premiera lub przez wyznaczoną przez niego osobę;
>
> 59. Biorąc pod uwagę, iż w opinii deputowanych wnioskujących o zbadanie zgodności przepisów ustawy z Konstytucją, biorąc pod uwagę ilość danych, które mogą potencjalnie podlegać kontroli i niedostateczne gwarancje dotyczące tzw. fałszywych trafień (faux positifs), technika przewidziana przez przedmiotowe przepisy stwarza nieproporcjonalne zagrożenie dla prawa do poszanowania życia prywatnego;
>
> 60. Biorąc pod uwagę, iż:
>
> – pozyskiwanie informacji wywiadowczych w trybie opisanym w art. L 851-3 prowadzone jest w warunkach i z poszanowaniem gwarancji opisanych w motywie 51[96];

[96] 51. Biorąc pod uwagę, że techniki pozyskiwania informacji, o których mowa w art. L 851-1 – L 851-6 oraz w art. L 852-1, są wykorzystywane, z zastrzeżeniem przepisów szczególnych, na zasadach opisanych w rozdziale I tytułu II kodeksu bezpieczeństwa wewnętrznego; iż są autoryzowane przez Premiera, na pisemny i uzasadniony wniosek ministra obrony, ministra spraw wewnętrznych, lub ministra właściwego do spraw gospodarki, budżetu lub ceł, po uzyskaniu uprzedniej opinii Narodowej Komisji Kontroli Technik Pozyskiwania Informacji; iż techniki te mogą być stosowane wyłącznie przez indywidualnie wskazanych i upoważnionych funkcjonariuszy; iż stosowane są pod kontrolą Narodowej Komisji Kontroli Technik Pozyskiwania Informa-

– technika ta może być zastosowana wyłącznie w celu zapobiegania terroryzmowi;

– zarówno samo zastosowanie tej techniki, jak również parametry automatycznego przetwarzania danych podlegają autoryzacji po uprzednim wyrażeniu opinii przez Narodową Komisję Kontroli Technik Pozyskiwania Informacji;

– pierwsza autoryzacja przyznawana jest na ograniczony czas dwóch miesięcy, zaś wniosek o przedłużenie zawierać musi opis liczby identyfikatorów wskazanych przez algorytm oraz analizę ważności informacji wskazanych przez system;

– urządzenia służące do automatycznego przetwarzania danych wykorzystują wyłącznie informacje, o których mowa w art. L 851-1, nie zbierając innych danych niż odpowiadające pierwotnym parametrom i nie zezwalając na identyfikację osób, których te informacje lub dokumenty dotyczą;

– gdy dane wykryte przez algorytm wskazywać będą na możliwość istnienia zagrożenia terrorystycznego, niezbędne będzie wydanie nowej autoryzacji przez Premiera, po uzyskaniu uprzedniej zgody Narodowej Komisji Kontroli Technik Pozyskiwania Informacji w celu identyfikacji określonej osoby;

– dane te przetwarzane są przez 60 dni licząc od momentu ich pozyskania i są niszczone po upływie tego terminu z wyjątkiem wystąpienia poważnych przesłanek świadczących o istnieniu zagrożenia terrorystycznego;

– autoryzacja wykorzystania tej techniki nie może być wydana w trybie pilnym przewidzianym w art. L 821-5;

– w konsekwencji, przepisy te nie stanowią ewidentnie nieproporcjonalnego zagrożenia dla prawa do poszanowania życia prywatnego;

– treść art. L 851-3 kodeksu bezpieczeństwa wewnętrznego musi zostać uznana za zgodną z Konstytucją.

Rada uznała zatem za zgodne z Konstytucją najważniejsze elementy ustawy o wywiadzie, podkreślając, że przewidziane w niej mechanizmy ochronne należy uznać za wystarczające w demokratycznym państwie prawnym. Szczególną uwagę trzeba zwrócić na argumentację Rady, która stanowi swego rodzaju odwrócenie logiki zazwyczaj prezentowanej w orzecznictwie TSUE (np. w cytowanym wyroku w sprawie Tele2 czy w orzeczeniu w sprawie *Digital Rights*[97]). Pomimo że, z oczywistych względów, nie wynika to z samej treści decyzji, za największe zagrożenie dla praw i wolności obywatelskich uznano powtarzające się we Francji zamachy terrorystyczne, nie zaś instrumenty mające na celu przeciwdziałanie tego rodzaju zdarzeniom. Niektórzy komenta-

cji; że skład i organizacja tego niezależnego organu administracyjnego są określone w art. L 833-1 – L 832-5 kodeksu bezpieczeństwa wewnętrznego w sposób zapewniający jego niezależność; iż zadania wymienione w art. L 833-1 – L 833-11 tego kodeksu sformułowane są w sposób zapewniający efektywność jego działań kontrolnych; iż, zgodnie z treścią art. L 841-1 tego kodeksu, zarówno Narodowa Komisja Kontroli Technik Pozyskiwania Informacji, jak również każda osoba może wnieść do Rady Państwa wniosek o zweryfikowanie, czy była wobec niego stosowana w sposób niezgodny z prawem technika pozyskiwania informacji; że w ramach stosowania art. L 871-6 tego kodeksu, działania niezbędne dla wprowadzenia technik wskazanych w art. L 851-1 – L 851-4 oraz L 852-1 mogą być wykonywane wyłącznie przez funkcjonariuszy służb lub podmiotów, nad którymi nadzór sprawuje minister właściwy do spraw komunikacji elektronicznej, operatorów sieci i dostawców usług telekomunikacji (…).

[97] Wyrok Trybunału z 8 IV 2014 r. – *Digital Rights Ireland Ltd przeciwko Minister for Communications*, Marine and Natura Resources, Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Siochana, Irlandii i Attorney General (C-293/12); Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i in. (C-594-12); sprawy połączone C-293/12 i C-594/12, www.curia.europa.eu/juris/documents.jsf?num=C-293/12, [dostęp: 21 IX 2017].

torzy wskazują, że uznanie większości przepisów ustawy za konstytucyjne świadczyło o pragmatycznym podejściu Rady do problemu i wynikało z woli uniknięcia późniejszych zarzutów, że swoją decyzją ułatwiła działalność terrorystyczną, a jednocześnie – uniemożliwiła lub znacznie utrudniła podejmowanie odpowiednich działań przez pozostałe organy państwa[98].

Dokonana przez ten organ wykładnia polegająca na ocenie konstytucyjności ustawy o wywiadzie przez pryzmat fundamentalnych dla francuskiego porządku prawnego norm może być jednak uznana za próbę dynamicznej interpretacji przepisów w szczególnym kontekście historycznym. Tak zwane instrumenty inwigilacji zostały uznane nie za naruszenie konstytucyjnych praw i wolności, ale za środek stanowiący z jednej strony ingerencję w prawo do prywatności, z drugiej zaś – mający na celu ich ochronę przed innym, dużo poważniejszym zagrożeniem jaki jest terroryzm.

5. Wnioski

Biorąc pod uwagę, że omawiany system zgodnie z dostępnymi powszechnie informacjami nie został jeszcze aktywowany na terytorium Francji i działa tylko w odniesieniu do danych zewnętrznych, wszelkie rozważania dotyczące celowości jego istnienia, skuteczności czy zgodności z normami rangi konstytucyjnej i prawem do prywatności mają charakter wyłącznie teoretyczny. Analiza przepisów ustawy dokonana przez Radę Konstytucyjną wskazuje, że samo istnienie algorytmu „czarnych skrzynek" nie może być uznane za niezgodne z francuską konstytucją i przepisami innych ustaw, przez których pryzmat badano przepisy wprowadzające ten instrument. Jego działalność w rozumieniu przepisów ogranicza się do tzw. metadanych – informacji technicznych o połączeniach, które nie ujawniają treści komunikatów.

Ustawa wprowadza również kompleksowy system kontroli i autoryzacji, do którego najważniejszych elementów należy opinia CNCTR, autoryzacja premiera czy możliwość wniesienia skargi do Rady Państwa. Trzeba też pamiętać, że stosowanie tego rodzaju środków podlega również wewnętrznym przepisom i procedurom (np. dotyczącym ochrony informacji niejawnych czy odpowiedzialności dyscyplinarnej), które obowiązują funkcjonariuszy konkretnej służby. Należy również rozróżnić samą sferę analizy metadanych niepozwalającą na identyfikację konkretnej osoby od postępowania po ewentualnym wykryciu zagrożenia, zmierzającym do ustalenia danych pozwalających na tą identyfikację,, do którego zastosowanie mają kolejne wymogi w postaci chociażby dodatkowej autoryzacji premiera, wydanej po uzyskaniu opinii CNCTR.

Szczegółowe poznanie zasad działania algorytmu jest niemożliwe z uwagi na objęcie tych informacji tajemnicą obrony (fr. *secret défense*). Kompleksowa ocena przynajmniej jawnych aspektów jego funkcjonowania będzie możliwa po aktywowaniu systemu w odniesieniu do informacji przetwarzanych na terytorium Francji oraz po przedstawieniu przez rząd raportu o stosowaniu algorytmu, do czego jest zobowiązany najpóźniej do 30 czerwca 2018 r. (art. 25 ustawy o wywiadzie).

Pomimo wszelkich wątpliwości i braku dostatecznej ilości informacji o sposobie działania automatycznego przetwarzania danych, przewidzianego w art. L 851-3 kodeksu bezpieczeństwa wewnętrznego, należy uznać, że jest to potencjalnie efektywny in-

[98] M. Verpeaux, *La loi sur le renseignement, entre sécurité et libertés; À propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*, s. 8, http://web.lexisnexis.fr/newsletter/avocats/10_2015/pdf3.pdf [dostęp: 21 IX 2017].

strument reagowania na współczesne zagrożenia o charakterze terrorystycznym. Analiza zarówno francuskiego systemu prawnego, jak i prawodawstwa innych państw pokazuje, że katalog instrumentów operacyjno-rozpoznawczych dotyczących stricte rozpoznawania i zapobiegania zagrożeniom terrorystycznym jest w rzeczywistości ograniczony. Charakter poczynań osób zaangażowanych w tego rodzaju działalność sprawia, że skuteczność tradycyjnych, bazujących na czynniku ludzkim metod, jest ograniczona. Metody opierające się chociażby na pozyskiwaniu informacji od informatorów nie pozwoliły na zapobiegnięcie serii zamachów (np. na teatr Bataclan w listopadzie 2015 r.), pomimo że z dużą dozą prawdopodobieństwa można zakładać, że francuskie służby specjalne powinny dysponować szczegółowym rozpoznaniem środowisk składających się z imigrantów pochodzących z państw Afryki Północnej czy Bliskiego Wschodu, z uwagi a strukturę etniczną społeczeństwa i duży odsetek osób pochodzących z tych regionów w stosunku do ogółu populacji.

Pomimo wszystkich wątpliwości dotyczących rzeczywistego sposobu działania algorytmu automatycznego przetwarzania danych, środek ten należy rozpatrywać w kategoriach niejako wymuszonej okolicznościami reakcji organów państwa na eskalację zagrożeń związanych z międzynarodowym terroryzmem. Obserwowane na przestrzeni kilku ostatnich lat mutacje tego zjawiska sprawiają, że zagrożenia, na które muszą reagować organy odpowiedzialne za bezpieczeństwo narodowe uległy daleko idącej ewolucji. Analogicznemu procesowi modyfikacji i adaptacji muszą zatem ulec również instrumenty wykorzystywane w celu ich zwalczania.

IV. STANY ZJEDNOCZONE AMERYKI

Pozyskiwanie zewnętrznych informacji wywiadowczych na przykładzie sekcji 702 ustawy *Foreign Intelligence Surveillance Amendments Act of 2008*[99]

W 2008 r. w USA została przyjęta ustawa *Foreign Intelligence Surveillance Amendments Act of 2008*[100] (dalej: FISA Amendments Act) wprowadzająca zmiany w obowiązującym od 1978 r. podstawowym akcie normatywnym regulującym problematykę prowadzenia działań wywiadowczych poza terytorium USA oraz nadzór nad tym procesem – *Foreign Intelligence Surveillance Act of 1978* (dalej: FISA). Jedną z najważniejszych zmian wynikających z ustawy zmieniającej FISA było wprowadzenie sekcji 702, upoważniającej prokuratora generalnego (Attorney General) i dyrektora Wywiadu Narodowego (Director of National Intelligence) do autoryzacji pozyskiwania, za pośrednictwem operatorów usług komunikacji elektronicznej, zewnętrznych informacji wywiadowczych dotyczących tzw. *non-US persons*, w stosunku do których można przypuszczać, że przebywają poza terytorium Stanów Zjednoczonych.

Przepisy sekcji 702 stanowią podstawę prawną pozyskiwania informacji o zewnętrznych zagrożeniach dla bezpieczeństwa Stanów Zjednoczonych za po-

[99] *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, https://www.intelligence.senate.gov/laws/fisa-amendments-act-2008 [dostęp: 23 IX 2017].

[100] *50 U.S. Code Chapter 36 – Foreign Intelligence Surveillance*, https://www.law.cornell.edu/uscode/text/50/chapter-36 [dostęp: 23 IX 2017].

średnictwem mechanizmów często mylnie określanych jako tzw. masowe programy inwigilacji (ang. *mass surveillance*)[101] wykorzystujących Internet i sieci telekomunikacyjne. Programy oparte na sekcji 702 pozwalają zarówno na uzyskanie metadanych, jak i treści komunikacji. Nie jest wymagane zdobycie indywidualnego nakazu sądu na gromadzenie informacji w tym trybie – kontrola specjalnego sądu utworzonego na mocy ustawy FISA – Foreign Intelligence Surveillance Court (dalej: FISC) ogranicza się do zatwierdzenia ogólnych procedur (procedur ukierunkowania i minimalizacji opisanych dalej), według których właściwe organy będą pozyskiwać zewnętrzne informacje wywiadowcze na podstawie sekcji 702[102]. Rola sądu FISC w odniesieniu do tych czynności jest zatem znacznie bardziej ograniczona niż w przypadku kontroli programu masowego pozyskiwania danych o połączeniach telefonicznych prowadzonego na podstawie sekcji 215 FISA[103].

Działania podejmowane na podstawie tych przepisów przez podmioty wchodzące w skład tzw. wspólnoty wywiadowczej (Intelligence Community), zwłaszcza Agencję Bezpieczeństwa Narodowego (National Security Agency – NSA), były określane wielokrotnie jako mające kluczowe znaczenie z punktu widzenia bezpieczeństwa narodowego USA, zwłaszcza w kontekście zapobiegania zdarzeniom o charakterze terrorystycznym[104]. Według publicznie dostępnych danych statystycznych ponad 25 proc. raportów NSA dotyczących międzynarodowego terroryzmu jest opartych na informacjach zbieranych na podstawie sekcji 702, ta proporcja zaś wykazuje tendencję rosnącą od chwili przyjęcia w 2008 r. FISA Amendments Act. Tego rodzaju dane w znacznym stopniu przyczyniły się do zrozumienia przez organy odpowiedzialne za ochronę bezpieczeństwa narodowego sposobu działania ugrupowań terrorystycznych, ustalenia ich taktyki, priorytetów czy długofalowych celów strategicznych. Jak wskazywano w rozdziałach poświęconych analogicznym instrumentom prawnym funkcjonującym w Wielkiej Brytanii i we Francji, działania w trybie sekcji 702 pozwalają nie tylko na analizę informacji o już znanych zagrożeniach, lecz także często pozwalają na wykrycie nowych przesłanek świadczących o potencjalnych działaniach terrorystycznych wymierzonych w USA i inne państwa oraz zidentyfikowanie osób zaangażowanych w te działania, nieznanych dotychczas amerykańskim służbom wywiadowczym[105].

Celem niniejszego artykułu jest dokonanie charakterystyki najważniejszych postanowień sekcji 702 i próba odpowiedzi na pytanie, czy działania podejmowane na jej podstawie mogą faktycznie być uznane za tzw. masową inwigilację oraz czy stoją one w sprzeczności z zasadami demokratycznego państwa prawnego. Autor przedstawi również argumenty podnoszone w kontekście ewentualnego przedłużenia obowiązywania sekcji 702.

---

[101] We wnioskach przedstawiono argumenty przemawiające za tym, że określenie masowe programy inwigilacji jest nieprawidłowo używane w kontekście działań prowadzonych na podstawie sekcji 702.

[102] https://cdt.org/insight/section-702-what-it-is-how-it-works/ [dostęp: 24 IX 2017].

[103] *Brennan Center for Justice at New York University School of Law, Are They Allowed To Do That*? A Breakdown of Selected Government Surveillance Programs, https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, [dostęp: 24 IX 2017]; także: https://www.lawfareblog.com/topic/fisa-215-collection [dostęp: 24 IX 2017].

[104] P. Rosenzweig, C. Stimson, D. Shedd, *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, http://www.heritage.org/defense/report/maintaining-americas-ability-collect-foreign-intelligence-the-section-702-program [dostęp: 24 IX 2017].

[105] *Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, https://www.nsa.gov/about/civil-liberties/resources/assets/files/pclob_section_702_report.pdf [dostęp: 23.IX.2017].

Biorąc pod uwagę, że przepisy sekcji wygasają z dniem 31 grudnia 2017 r.[106], dyskusja dotycząca ewentualnego przedłużenia ich obowiązywania, modyfikacji lub całościowej zmiany, prowadzona w Stanach Zjednoczonych, będzie mieć niezmiernie istotne znaczenie w odniesieniu do sposobu uregulowania kompetencji służb specjalnych i ich roli w demokratycznym społeczeństwie, a także do interpretacji wspólnej dla wszystkich państw euroatlantyckich konstytucyjnej zasady prawa do prywatności.

1. Najważniejsze postanowienia sekcji 702

Tryb pozyskiwania zewnętrznych informacji wywiadowczych na podstawie ustawy FISA Amendments Act został przewidziany w sekcji 702 (a). W celu zachowania niezbędnej spójności terminologicznej poniżej zamieszczono tłumaczenie najważniejszych elementów tego przepisu oraz definicji zawartych w ustawach FISA oraz FISA Amendments Act. Mając na względzie stopień szczegółowości omawianego aktu prawnego poniższe tłumaczenie jest jedynie odzwierciedleniem jego najistotniejszych elementów, niezbędnych dla zrozumienia całości procesu.

Sekcja 702

(a) Autoryzacja. (…) Prokurator Generalny i Narodowy Dyrektor Wywiadu mogą wspólnie autoryzować, na okres do jednego roku, licząc od daty autoryzacji, prowadzenie działań wobec osób, wobec których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych, w celu pozyskania zewnętrznych informacji wywiadowczych.

(b) Ograniczenia. Pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) –

(1) nie może być celowo ukierunkowane na osoby, o których wiadomo, że w momencie pozyskiwania informacji znajdują się na terytorium Stanów Zjednoczonych;

(2) nie może być celowo ukierunkowane na osoby, w stosunku których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych, jeżeli cel pozyskiwania informacji jest ukierunkowany na osoby, w stosunku do których można racjonalnie przypuszczać, że znajdują się na terytorium Stanów Zjednoczonych;

(3) nie może być celowo ukierunkowane na podmiot USA[107] przebywający poza terytorium Stanów Zjednoczonych;

(c) Prowadzenie czynności polegających na pozyskiwaniu zewnętrznych informacji wywiadowczych

(1) Pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) może być prowadzone wyłącznie, jeżeli jest to zgodne z –

(A) procedurami ukierunkowania i minimalizacji przyjętymi zgodnie z podsekcjami (d) i (e); oraz

(B) po wydaniu certyfikatu zgodnie z podsekcją (g).

(2) Ustalenie – w rozumieniu niniejszej podsekcji, dla celów podsekcji (a) pojęcie to oznacza ustalenie przez Prokuratora Generalnego i Dyrektora Wywiadu Narodo-

[106] H.R. 5949 An Act. *To extend the FISA Amendments Act of 2008 for five years*, https://www.govtrack.us/congress/bills/112/hr5949/text [dostęp: 24 IX 2017].

[107] Zgodnie z definicją zawartą w § 6010 rozdziału 69 tytułu 22 Kodeksu Stanów Zjednoczonych pojęcie United States person – tłumaczone w niniejszym opracowaniu jako podmiot amerykański – oznacza obywatela Stanów Zjednoczonych, cudzoziemca uprawnionego do stałego pobytu oraz korporację, spółkę lub inną organizację utworzoną zgodnie z prawem Stanów Zjednoczonych.

wego, że istnieją okoliczności powodujące, że brak niezwłocznej autoryzacji na podstawie podsekcji (a) spowoduje, że istotne z punktu widzenia bezpieczeństwa narodowego Stanów Zjednoczonych informacje wywiadowcze zostaną utracone lub nie będą mogły być uzyskane w odpowiednim czasie, a względy czasowe nie pozwalają na wydanie nakazu zgodnie z podsekcją (i) (3) przed implementacją takiej autoryzacji.

(d) Procedury ukierunkowania

(1) Prokurator Generalny, w porozumieniu z Dyrektorem Wywiadu Narodowego, przyjmuje procedury ukierunkowania, których celem jest –

(A) zapewnienie, że pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) jest ograniczone do osób, w stosunku do których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych;

(B) zapobieganie celowemu pozyskaniu komunikacji, których nadawca lub wszyscy zamierzeni odbiorcy zgodnie z posiadaną wiedzą w czasie pozyskiwania informacji przebywają na terytorium Stanów Zjednoczonych.

(2) Kontrola sądowa – Procedury przyjęte zgodnie z paragrafem (1) podlegają kontroli sądowej zgodnie z podsekcją (i).

(e) Procedury minimalizacji

(1) Prokurator Generalny, w porozumieniu z Dyrektorem Wywiadu Narodowego, przyjmuje procedury minimalizacji spełniające kryteria przewidziane dla procedur minimalizacji opisane w sekcji 101 (h) i 301 (4) w stosunku do pozyskiwania informacji zgodnie z podsekcją (a).

(2) Kontrola sądowa – Procedury minimalizacji przyjęte zgodnie z paragrafem (1) podlegają kontroli sądowej zgodnie z podsekcją (i).

(…)

(g) Certyfikacja

(A) Z zastrzeżeniem (B), przed implementacją autoryzacji na podstawie podsekcji (a), Prokurator Generalny i Narodowy Dyrektor Wywiadu dostarczają sądowi Foreign Intelligence Surveillance Court pisemny certyfikat i inne oświadczenia, sporządzone pod przysięgą i opatrzone pieczęcią zgodnie z niniejszą podsekcją.

(B) Jeżeli Prokurator Generalny i Narodowy Dyrektor Wywiadu dokonają ustaleń zgodnie z podsekcją (c) (2), a względy czasowe nie pozwalają na złożenie certyfikatu na podstawie niniejszej podsekcji przed implementacją autoryzacji na podstawie podsekcji (a), Prokurator Generalny i Dyrektor Wywiadu Narodowego przedkładają sądowi certyfikat dla takiej autoryzacji tak szybko, jak to możliwe, jednak nie później niż 7 dni po dokonaniu ustaleń.

(2) Wymagania – Certyfikat wydany zgodnie z niniejszą podsekcją powinien –

(A) zaświadczać, że:

(i) istnieją zatwierdzone przez sąd FISC procedury, procedury złożone w celu zatwierdzenia lub takie, które zostaną złożone w celu zatwierdzenia wraz z certyfikatem, których celem jest:

(I) zapewnienie, że pozyskiwanie danych na podstawie podsekcji (a) jest ograniczone do osób, w stosunku do których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych;

(II) zapobieganie celowemu pozyskiwaniu komunikacji, których nadawca lub wszyscy zamierzeni odbiorcy w czasie pozyskania znajdują się na terytorium Stanów Zjednoczonych;

(ii) procedury minimalizacji, które mają być stosowane w odniesieniu do pozyskiwania zewnętrznych informacji wywiadowczych:

(I)spełniają kryteria określone w definicji procedur minimalizacji określone w sekcji 101 (h) oraz 301 (4) oraz;

(II) zostały zatwierdzone przez sąd FISC, złożone w celu zatwierdzenia lub zostaną złożone w celu zatwierdzenia wraz z certyfikatem;

(iv) procedury i wytyczne są zgodne z wymogami czwartej poprawki do Konstytucji Stanów Zjednoczonych;

(v) istotnym celem pozyskiwania jest uzyskanie zewnętrznych informacji wywiadowczych;

(vi) pozyskiwanie odbywa się poprzez uzyskiwanie zewnętrznych informacji wywiadowczych z pomocą operatora usług komunikacji elektronicznej.

(…)

(h) Nakazy i sądowa kontrola nakazów

(1) W odniesieniu do pozyskiwania informacji autoryzowanego na podstawie podsekcji (a) Prokurator Generalny i Dyrektor Wywiadu Narodowego mogą zobowiązać na piśmie dostawcy usług komunikacji elektronicznej do:

(A) niezwłocznego udostępnienia organom rządowym wszystkich informacji, urządzeń lub udzielenia wsparcia niezbędnego do pozyskania informacji w sposób zapewniający ochronę informacji o tym pozyskiwaniu oraz tworzący możliwie najmniejsze zakłócenia usług dostarczanych przez tego dostawcę osobie, w stosunku do której będą prowadzone te czynności;

(B) przechowywania danych dotyczących pozyskiwania informacji i udzielonej właściwym organom pomocy zgodnie z procedurami bezpieczeństwa zatwierdzonymi przez Prokuratora Generalnego i Dyrektora Wywiadu Narodowego.

Przewidziany w sekcji 702 zasięg podmiotowy pozyskiwania informacji został określony w sposób szeroki. Obejmuje on nie tylko osoby fizyczne, lecz także osoby prawne (zob. przyp. 9) Osoby te muszą zgodnie z dostępną wiedzą przebywać poza terytorium Stanów Zjednoczonych. Ustawa posługuje się pojęciem *reasonably believed to be located outside the United States,* nie wyjaśnia jednak w sposób precyzyjny, co należy rozumieć pod tym pojęciem Niemniej jednak sekcja 702 przewiduje przyjęcie tzw. procedur ukierunkowania, dzięki którym pozyskiwanie informacji w omawianym trybie będzie ograniczone do osób przebywających poza terytorium Stanów Zjednoczonych[108].

Przepis dotyczący tzw. procedur ukierunkowania ma istotne znaczenie w kontekście ochrony prawa do prywatności. Mają one zapewnić, że prowadzenie działań opisanych w sekcji 702 będzie obejmować osoby określone w ustawie jako „*non-US persons*" (przebywające poza granicami USA). Dokumenty te określają, jakie konkretnie działania będą podejmowane w tym celu przez właściwe organy. Procedury minimalizacji określają natomiast, jakie działania będą podejmowane, aby ograniczyć wykorzystywanie i przechowywanie danych pozyskiwanych zgodnie z sekcją 702. Te procedury podlegają zatwierdzeniu przez Federal Intelligence Surveillance Court (FISC)[109].

[108] *Privacy and Civil Liberties Oversight Board: Report*…, s. 21.

[109] P. Rosenzweig, C. Stimson, D. Shedd, *Maintaining America's Ability*…

Celem działań podejmowanych w trybie sekcji 702 jest pozyskiwanie zewnętrznych informacji wywiadowczych, które w rozumieniu ustawy FISA oznaczają:

> (...) (1) informacje odnoszące się, lub jeżeli dotyczą podmiotu USA są niezbędne dla zdolności Stanów Zjednoczonych do ochrony przed –
>
> (A) faktycznym lub potencjalnym atakiem lub innymi wrogimi działaniami innego państwa lub jego agenta;
>
> (B) sabotażem, międzynarodowym terroryzmem lub międzynarodową proliferacją broni masowego rażenia dokonanymi przez obce państwo lub jego agenta;
>
> (C) niejawnymi działaniami wywiadowczymi obcych służb wywiadowczych lub siatki stworzonej przez obce państwo lub jego agenta;
>
> (2) informacje dotyczące obcego państwa lub zagranicznego terytorium odnoszące się do, lub jeżeli dotyczą podmiotu USA – niezbędne do:
>
> (A) bezpieczeństwa narodowego lub obronności Stanów Zjednoczonych;
>
> (B) prowadzenia polityki zagranicznej Stanów Zjednoczonych.

2. Najważniejsze programy pozyskiwania informacji stosowane na podstawie sekcji 702

Raport *Privacy and Civil Liberties Oversight Board* z 2014 r. zawiera dokładny opis programów wykorzystywanych na podstawie sekcji 702. Największym problemem związanym z praktycznym funkcjonowaniem tych mechanizmów jest możliwość uzyskania nieautoryzowanego dostępu do informacji o podmiotach amerykańskich w toku działań ukierunkowanych na zdobycie zagranicznych danych wywiadowczych. Wyjaśnienie przyczyn tego zjawiska jest możliwe dopiero jednak po dokonaniu charakterystyki dwóch najważniejszych instrumentów wykorzystywanych na podstawie sekcji 702 – programów typu PRISM oraz *upstream collection*[110].

Zgodnie z opisem poszczególnych etapów procesu pozyskiwania zewnętrznych informacji wywiadowczych (przedstawionym w cytowanym raporcie), po uzyskaniu autoryzacji zgodnie z sekcją 702 właściwe organy rządowe przesyłają do operatorów usług komunikacji elektronicznej nakazy udzielenia pomocy w celu otrzymania danych dotyczących komunikacji określonych osób. Właściwy organ określa tzw. selektor, dzięki któremu jest możliwe oznaczenie konkretnej osoby znajdującej się w zainteresowaniu amerykańskich służb wywiadowczych. Mianem s e l e k t o r a można określić informacje służące identyfikacji komunikacji określonej osoby, może to być np. numer telefonu czy adres poczty elektronicznej. Selektory są przekazywane określonemu dostawcy usług komunikacji elektronicznej, po czym rozpoczyna on proces zbierania informacji odnoszących się do wskazanej osoby. Dalszy sposób postępowania jest uzależniony od tego, przez który ze wskazanych powyżej dwóch programów informacje mają być zbierane – PRISM czy *upstream collection*.

Zbieranie informacji z wykorzystaniem programu PRISM rozpoczyna się od przesłania przez właściwy organ administracji określonego selektora dostawcy usług komunikacji elektronicznej, mającemu siedzibę na terytorium Stanów Zjednoczonych. Ten podmiot jest zobowiązany, zgodnie z sekcją 702, do udostępnienia informacji o komunikacji wysyłanej i odbieranej przez ten selektor. Program PRISM ogranicza się wyłącznie do danych przesyłanych za pośrednictwem Internetu, nie obejmuje natomiast połączeń

[110] Tamże.

telefonicznych – dlatego można domniemywać, że najczęściej wykorzystywanym w tym przypadku selektorem będzie adres poczty elektronicznej. Wszystkie dane zebrane z wykorzystaniem programu PRISM są przekazywane NSA. Dodatkowo, część zebranych informacji trafia również do innych organów – zwłaszcza do CIA oraz FBI[111].

Upstream collection jest programem znacznie różniącym się od PRISM, zarówno pod względem sposobu zbierania danych, jak i katalogu objętych nim danych. W odróżnieniu od PRISM *upstream collection* polega na pozyskiwaniu danych dotyczących zarówno komunikacji internetowej, jak i telefonicznej. Jest on prowadzony za pośrednictwem operatorów zarządzających, tzw. *telecommunications backbone* – sieci przesyłowych skupiających dane przesyłane przez mniejsze, lokalne sieci[112]. W ten sposób NSA uzyskuje dostęp do danych transferowanych przez największe telekomunikacyjne punkty przesyłowe[113]. Uzyskane w tym trybie informacje są przekazywane wyłącznie NSA. Istotne znaczenie mają dwie kolejne różnice między programem *upstream collection* a PRISM:

1) *upstream collection* pozwala na pozyskiwanie komunikacji typu „*about*", czyli takiej, w której selektor dotyczący konkretnej osoby jest zawarty w treści komunikacji prowadzonej przez inne osoby, ona sama jednak niekoniecznie musi być stroną takiej komunikacji. Treści wymieniane przez inne strony dotyczą selektora wskazanego przez właściwy organ; są to informacje „o selektorze", stąd też nazwa „*about communications*";
2) program ten obejmuje tzw. *multiple communications transaction* (MCT) – połączenia internetowe zawierające określoną liczbę odrębnych, indywidualnych połączeń. Jeżeli jedno z nich jest połączeniem „z selsktorem", „do selektora" lub „o selektorze" (*about*), wskazanym przez właściwe organy, wówczas NSA uzyskuje dane o całym połączeniu MCT, również o pozostałych połączeniach wchodzących w jego skład, niedotyczących konkretnego selektora.

Pozyskiwanie danych o połączeniach MCT stanowiło jeden z głównych powodów kontrowersji dotyczących możliwości nieautoryzowanego monitorowania komunikacji podmiotów amerykańskich i w konsekwencji – zgodności z prawem niektórych aspektów programu *upstream collection*. Dla wyjaśnienia dokładnego charakteru połączeń MCT istotne znaczenie mają informacje znajdujące się na stronie fundacji Electronic Frontier Foundation, które zostały przekazane przez Dyrektora Wywiadu Narodowego w czasie konferencji prasowej we wrześniu 2013 r.[114] Odpowiadając na pytanie, co dokładnie należy rozumieć pod pojęciem MCT, udzielił on następującej odpowiedzi, zastrzegając, że będzie ona miała charakter ogólny, gdyż dokładne wyjaśnienie istoty tego pojęcia może dotyczyć wrażliwych kwestii operacyjnych:

> Jeżeli dana osoba posiada konto poczty elektronicznej, jak Gmail lub Hotmail, po zalogowaniu się na konto widoczny jest *screenshot* pokazujący określoną liczba e-maili znajdujących się w skrzynce odbiorczej. W przypadku mojego serwera widoczna jest data wiadomości, nadawca, temat i rozmiar wiadomości. Mogę jednak otrzymać 15 różnych [wiadomości] naraz.

[111] *Privacy and Civil Liberties Oversight Board: Report*…, s. 7.

[112] http://searchtelecom.techtarget.com/definition/backbone [dostęp: 24 IX 2017].

[113] *Intelligence Attorney on How „Multi-Communication Transactions" Allowed for Domestic Surveillance"*, https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed [dostęp: 24 IX 2017].

[114] Tamże.

> Wszystkie przesyłane są przez Internet jako jedno połączenie, pomimo że po otwarciu konta wymienionych jest 15 oddzielnych wiadomości. Z przyczyn technicznych NSA nie była i w dalszym ciągu nie jest w stanie podzielić takiej informacji na jej indywidualne komponenty.
>
> Jeżeli zatem jeden z tych maili odnosił się w temacie wiadomości do maila, do którego pierwotnie zamierzano uzyskać dostęp, zebrane zostaną dane o wszystkich wiadomościach znajdujących się w skrzynce. Działa to na zasadzie *screenshot'u*. (…)
>
> Niektóre [z tych e-maili] mogą być wyłącznie wiadomościami wewnętrznymi. Na przykład, jeżeli działania ukierunkowane są na podmiot zewnętrzny, a podmiot ten komunikuje się z podmiotem amerykańskim, możliwe jest uzyskanie całego *screenshot'u* podmiotu amerykańskiego. (…)[115].

Wątpliwości dotyczące rzeczywistego sposobu funkcjonowania programu *upstream collection* oraz możliwość naruszenia prawa do prywatności podmiotów amerykańskich, z uwagi na specyfikę technologiczną tego instrumentu, doprowadziły do podjęcia przez NSA decyzji o wstrzymaniu jego wykorzystywania w odniesieniu do komunikacji „*about*". Zgodnie z oświadczeniem z 28 kwietnia 2017 r. ten organ zdecydował, że z uwagi na kilkukrotne przypadki stosowania programu w sposób niezgodny z wymogami ustanowionymi w sekcji 702, które wynikały z trudności natury technologicznej, czynności NSA prowadzone na podstawie sekcji 702 nie będą obejmować komunikacji typu „*about*". Będą natomiast ograniczone wyłącznie do informacji przesyłanych „do" lub „z" określonego selektora wykorzystywanego przez osobę stanowiącą cel zewnętrznych działań wywiadowczych. Ten zabieg ma zmniejszyć ryzyko naruszania prawa do prywatności podmiotów amerykańskich przez ograniczenie czynności operacyjno-rozpoznawczych prowadzonych przez NSA wyłącznie do osób pozostających w bezpośrednim kontakcie z cudzoziemcami przebywającymi poza terytorium USA, znajdującymi się w zainteresowaniu służb wywiadowczych[116].

3. Wnioski

Określanie programu PRISM i *upstream collection* mianem instrumentów masowej inwigilacji elektronicznej jest pewnego rodzaju nadużyciem. Nie jest to program typu „*bulk*" działający na zasadzie pozyskiwania określonego zbioru informacji, z których potem są odfiltrowywane informacje mogące mieć znaczenie dla bezpieczeństwa narodowego[117]. Omawiane programy działają na zasadzie wykorzystywania konkretnych selektorów identyfikujących komunikację określonej osoby fizycznej znajdującej się poza terytorium USA i niebędącej tzw. *US person*. Sekcja 702 zawiera zatem dwie przesłanki negatywne powodujące, że te programy nie mają w rzeczywistości charakteru masowe-

[115] Tamże.

[116] *NSA Stops Certain Section 702 „Upstream" Activities*, April 28, 2017, https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml [dostęp: 24 IX 2017]. Więcej informacji na temat wstrzymania działań typu „*upstream collection"* przez NSA znajduje się w artykułach prasowych na stronach dzienników „New York Times" i „The Washington Post", https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html?mcubz=1 oraz https://www.washingtonpost.com/world/national-security/nsa-halts-controversial-email-collection-practice-to-preserve-larger-surveillance-program/2017/04/28/e2ddf9a0-2c3f-11e7-be51-b3fc6ff7faee_story.html?utm_term=.bf621de0b542 [dostęp: 24 IX 2017].

[117] Więcej na temat instrumentów typu „*bulk*" w części poświęconej Wielkiej Brytanii.

go pozyskiwania danych, lecz są ukierunkowane na ściśle określone osoby spełniające powyższe warunki. Ponadto ustawa zobowiązuje prokuratora generalnego i dyrektora Wywiadu Narodowego do opracowania dokumentów przewidujących konkretne działania, jakie organy administracji będą podejmować w celu wykluczenia pozyskiwania informacji o podmiotach amerykańskich (procedury minimalizacji i ukierunkowania).

Nie powinno budzić wątpliwości, że programy pozyskiwania informacji, prowadzone na podstawie sekcji 702, są nowoczesnymi i wykazującymi niezwykle wysoki stopień zaawansowania technologicznego instrumentami służącymi do wykrywania zewnętrznych zagrożeń bezpieczeństwa narodowego USA. Krytycy ustawy i przedstawiciele środowisk zaangażowanych w ochronę prawa do prywatności argumentują, że przepisy tej sekcji w aktualnym kształcie stwarzają liczne problemy, do których – jako najważniejsze – należy zaliczyć:

- ograniczony nadzór sądowy,
- niezamierzone zbieranie danych o podmiotach amerykańskich, w przypadku gdy komunikują się oni z cudzoziemcami stanowiącymi cel działań amerykańskich służb wywiadowczych, co stoi w sprzeczności z sekcją 702,
- FBI i inne organy mające uprawnienia dochodzeniowo-śledcze są uprawnione do przeszukiwania danych zebranych w sposób niezamierzony dla celów prowadzenia postępowań niemających związku z terroryzmem czy szpiegostwem, co nie odpowiada pierwotnym założeniom ustawy FISA i stanowi naruszenie czwartej poprawki do Konstytucji Stanów Zjednoczonych,
- nieznaną liczbę podmiotów amerykańskich, których dane zostały pozyskane w toku wykorzystywania programów działających na podstawie sekcji 702,
- kontrowersje związane z tzw. komunikacją *about*,
- masową inwigilację obywateli innych państw, co przyczynia się do pogorszenia opinii wspólnoty międzynarodowej o USA, utrudnia prowadzenie bieżącej polityki zagranicznej oraz powoduje straty dla amerykańskich podmiotów gospodarczych.

Zgodnie z oficjalnym stanowiskiem Białego Domu administracja prezydenta Donalda Trumpa będzie dążyć do utrzymania przepisów sekcji 702 w niezmienionym stanie, biorąc pod uwagę istotne znaczenie wykorzystywanych na jej podstawie programów dla bezpieczeństwa narodowego[118]. Prokurator generalny Jeff Sessions oraz dyrektor Wywiadu Narodowego Dan Coats w liście z 7 września 2017 r. skierowanym do liderów Partii Demokratycznej i Partii Republikańskiej określili reautoryzację przez Kongres przepisów sekcji 702 jako najważniejszy cel legislacyjny Departamentu Sprawiedliwości i Wspólnoty Wywiadowczej[119].

Kontrowersje związane z tzw. masową inwigilacją i kierowane głównie pod adresem NSA zarzuty o niezgodne z prawem praktyki, polegające na niczym nieograniczonym pozyskiwaniem danych przesyłanych za pośrednictwem środków komunikacji elektronicznej czy rozmów telefonicznych, w dużej mierze wynikają z niejawności szczegółowych zasad działania tych programów, sama zaś analiza przepisów ustaw FISA czy FISA Amendments Act nie pozwala na ich dokładne zrozumienie. Jak wskazano w części poświęconej programom PRISM czy *upstream collection*, incydenty zwią-

[118] D. Volz, S. Holland, *White House supports renewal of spy law without reforms: official*, https://www.reuters.com/article/us-usa-trump-fisa/white-house-supports-renewal-of-spy-law-without-reforms-official-idUSKBN16855P [dostęp: 24 IX 2017].

[119] K. Bo Williams, *Sessions, Coats push for permanent renewal of controversial surveillance law*, http://thehill.com/policy/national-security/350155-sessions-coats-push-for-permanent-702-renewal [dostęp: 24 IX 2017].

zane z uzyskaniem danych podmiotów amerykańskich w sposób niezgodny z sekcją 702 wynikają z obiektywnych trudności technologicznych, immanentnie związanych ze sposobem funkcjonowania Internetu i międzynarodowych sieci telekomunikacyjnych. Należy zwrócić uwagę na to, że zaprzestanie przez NSA pozyskiwania komunikacji typu „*about*" w ramach programu *upstream collection* pokazuje, że system nadzoru nad rzeczywistym wykorzystywaniem tego rodzaju instrumentów, zarówno w ramach samej NSA, jak i sprawowanego przez inne organy, jest na tyle efektywny, że jest w stanie wykryć zagrażające prawu do prywatności nieprawidłowości i podjąć odpowiednie środki zaradcze. Pomimo wielu wątpliwości co do dalszego istnienia sekcji 702 po 31 grudnia 2017 r., całkowite usunięcie jej przepisów z amerykańskiego systemu prawnego należy uznać za mało prawdopodobne. Ponadto byłoby to zjawisko szkodliwe zarówno z punktu widzenia bezpieczeństwa narodowego, jak i ochrony prywatności.

Brak zgody Kongresu na przedłużenie obowiązywania sekcji 702 skutkowałby, po pierwsze, powstaniem luki prawnej powodującej, że służby wywiadowcze byłyby zmuszone do działania w obszarze nieuregulowanym jakimkolwiek aktem normatywnym, po drugie zaś – przestałyby obowiązywać jakiekolwiek mechanizmy ochronne funkcjonujące na podstawie omawianych ustaw. Najbardziej korzystnym rozwiązaniem z punktu widzenia ochrony obu fundamentalnych wartości – bezpieczeństwa narodowego i prawa do prywatności – byłaby modyfikacja przepisów sekcji 702 w sposób ograniczający ryzyko związane ze stosowaniem programów typu PRISM czy *upstream collection*, np. przez zwiększenie zakresu kontroli sądowej sprawowanej przez sąd FISC czy ograniczenie możliwości korzystania z zebranych w ten sposób informacji przez służby inne niż NSA. Należy też pamiętać, że duża część problemów związanych ze stosowaniem omawianych mechanizmów ma swoje źródło nie w prawie, lecz w aspektach technologicznych związanych zarówno ze sposobem funkcjonowania nowoczesnych środków komunikacji, jak i z ograniczeniami samej NSA. Zorientowane na sferę zewnętrzną działania wywiadowcze, czy szerzej – działania wszystkich służb specjalnych, zmierzające do ochrony bezpieczeństwa narodowego, prowadzą do powstania nieprawidłowości, występujących z różnym nasileniem, naruszających wolności i prawa obywatelskie. Niemniej jednak zgodność przepisów stanowiących ich podstawę normatywną z normami rangi konstytucyjnej należy oceniać przez pryzmat efektywnego systemu nadzoru i kontroli. Trzeba również wziąć pod uwagę, w jakim stopniu te działania przyczyniają się do ochrony innych wartości stanowiących podstawę demokratycznego państwa prawnego – prawa do życia czy prawa do bezpieczeństwa, bez których prawo do prywatności byłoby jedynie teoretyczną, niemożliwą do urzeczywistnienia koncepcją.

V. WIELKA BRYTANIA

Ujawnienie w 2013 r. przez byłego pracownika amerykańskiej Agencji Bezpieczeństwa Narodowego informacji dotyczących istnienia i zasad funkcjonowania programów masowej inwigilacji wykorzystywanych przez USA, Wielką Brytanię i pozostałe państwa tzw. Pięciorga Oczu (*Five Eyes*) dało początek prowadzonej niemal we wszystkich państwach Unii Europejskiej i NATO dyskusji dotyczącej sposobu rozumienia prawa do prywatności, roli służb specjalnych we współczesnym świecie i wykorzystywanych przez nie instrumentów. Sposób realizacji zadań w sferze bezpieczeństwa narodowego przez upraw-

nione do tego organy jest warunkowany dwoma podstawowymi czynnikami: po pierwsze, dogłębną ewolucją charakteru zagrożeń, na jakie muszą reagować tego rodzaju instytucje, oraz – po drugie – bezprecedensowym rozwojem środków komunikacji elektronicznej i stale zwiększającą się rolą Internetu w niemal wszystkich aspektach życia społecznego. Problem charakteru i zakresu uprawnień przyznanych zarówno służbom zorientowanym na zewnętrzne działania wywiadowcze, jak i organów zajmujących się ochroną bezpieczeństwa wewnętrznego państwa jest nierozerwalnie powiązany z koniecznością znalezienia odpowiednich proporcji między bezpieczeństwem a prawem do prywatności.

Pomimo że przepisy prawne zezwalające na wykorzystywanie przez służby tzw. programów masowej inwigilacji (ang. *mass surveillance*) budzą w naturalny sposób liczne wątpliwości co do ich zgodności zarówno ze standardami konstytucyjnymi na gruncie prawa krajowego, jak i z zakresem praw i wolności przyznawanych na mocy aktów prawa międzynarodowego, opinie ograniczające się do uznania tego rodzaju regulacji za z zasady niezgodne z podstawowymi wartościami demokratycznego państwa prawnego byłoby zbyt daleko idącym uproszczeniem. Ocena skutków społecznych tego rodzaju rozwiązań oraz ich implikacji dla funkcjonowania całego porządku prawnego powinna być dokonywana w sposób dynamiczny, uwzględniający ewolucję zagrożeń dla bezpieczeństwa państwa oraz to, że coraz więcej z nich rozwija się w przestrzeni wirtualnej. Istotne znaczenie w tym kontekście ma nie samo istnienie i wykorzystywanie tego rodzaju instrumentów, lecz działający równolegle niezależny od służb sposób nadzoru umożliwiający weryfikację ich faktycznego działania i zapobieganie ewentualnym naruszeniom.

Celem niniejszego artykułu jest dokonanie charakterystyki niektórych aspektów funkcjonowania w Wielkiej Brytanii dwóch instrumentów przewidzianych w ustawie *Investigatory Powers Act 2016,* która została przyjętej w listopadzie 2016 r.[120] – *Bulk Interception* (masowe przechwytywanie komunikacji zagranicznej) oraz *Bulk Equipment Interference* (masowa ingerencja w urządzenia informatyczne). Analiza rozwiązań brytyjskich w zakresie uprawnień operacyjno-rozpoznawczych może mieć istotne znaczenie w kontekście dyskusji nad sposobami przeciwdziałania obserwowanej intensyfikacji zagrożeń o charakterze terrorystycznym. Głównym aspektem przywołanych instrumentów jest to, że stanowią one nowoczesne środki zdobywania informacji umożliwiające służbom dostęp do ogromnych ilości informacji wymienianych za pośrednictwem środków komunikacji elektronicznej. Te instrumenty wykorzystują równocześnie narzędzia filtrowania i segregacji danych, odrzucając elementy nieprzydatne z punktu widzenia bezpieczeństwa państwa. Wykorzystywanie tego rodzaju instrumentów należy postrzegać nie w kategoriach bezprawnego i nieuzasadnionego zamachu na prawa i wolności obywatelskie czy dążenia brytyjskich służb do niekontrolowanego pozyskiwania informacji o obywatelach, lecz jako próbę dostosowania nieprzystających często do rzeczywistych wyzwań narzędzi wykorzystywanych przez te podmioty w toku realizacji ich ustawowych zadań. Zasadne wydaje się uznanie, że przyjęcie tego rodzaju rozwiązań legislacyjnych i nadanie formalnoprawnych ram działaniom operacyjno-rozpoznawczym w sferze informatyki i telekomunikacji jest wyrazem dążenia do zrównania możliwości działania państwa w zestawieniu z osobami bądź ugrupowaniami stwarzającymi zagrożenie dla podstaw jego funkcjonowania.

Analiza przywołanych rozwiązań legislacyjnych i obserwowana na przestrzeni kilku ostatnich lat ewolucja katalogu instrumentów operacyjno-rozpoznawczych[121]

[120] *Investigatory Powers Act 2016*, www.legislation.gov.uk/ukpga/2016/25/contents/enacted [dostęp: 22 VIII 2017].

[121] Oprócz opisywanych rozwiązań brytyjskich dobrym przykładem w kontekście ewolucji rozwiązań

wykorzystywanych przez służby państw UE i NATO wskazuje, że państwa, które są najbardziej narażone na zagrożenia o charakterze terrorystycznym, konsekwentnie wprowadzają środki umożliwiające skuteczne gromadzenie danych za pośrednictwem systemów i sieci informatycznych. Tendencja ta prawdopodobnie będzie prowadzić do stopniowego ograniczania wykorzystywania tradycyjnych metod pozyskiwania informacji, przy jednoczesnym poszerzaniu sposobu i zakresu wykorzystywania inwigilacji elektronicznej.

1. *Bulk interception*

Bulk interception (masowe przechwytywanie) jest instrumentem umożliwiającym zdobywanie zewnętrznych informacji wywiadowczych (ang. *foreign-focused intelligence*) oraz identyfikację osób, grup oraz organizacji mogących stanowić zagrożenie dla bezpieczeństwa Wielkiej Brytanii. Ten mechanizm polega na przechwytywaniu komunikacji (zarówno treści, jak i danych telekomunikacyjnych) osób przebywających poza jej terytorium oraz filtrowaniu i analizie materiału mogącego mieć znaczenie wywiadowcze. Istota masowych instrumentów pozyskiwania informacji, w tym *bulk interception*, polega na gromadzeniu dużych ilości informacji, z których jedynie część będzie dotyczyć osób mogących stwarzać potencjalne zagrożenie dla bezpieczeństwa narodowego.

Opisywany mechanizm to jeden z podstawowych komponentów działań ukierunkowanych na pozyskiwanie informacji o zdarzeniach wykazujących powiązania z osobami lub podmiotami znajdującymi się poza terytorium Wielkiej Brytanii zagrażających bezpieczeństwu Wielkiej Brytanii. W większości przypadków wiedza służb odpowiedzialnych za ochronę bezpieczeństwa narodowego o ewentualnych zagrożeniach zewnętrznych, stwarzanych przez osoby lub ugrupowania znajdujące się poza jej terytorium, ma charakter wysoce fragmentaryczny i nieweryfikowalny. Ponadto – mając na względzie wykorzystywanie coraz bardziej wyrafinowanych metod komunikacji elektronicznej przez osoby powiązane z działalnością terrorystyczną, zagraniczne służby wywiadowcze, członków transgranicznych zorganizowanych grup przestępczych, a także brak możliwości dokładnego ustalenia technicznych aspektów przesyłu określonej wiadomości spowodowany strukturą zależności i powiązań internetowych metod komunikacji – w wielu sytuacjach masowe przechwytywanie jest jedyną metodą pozwalającą na wykrycie i skuteczne przeciwdziałanie określonemu zagrożenia. Masowe pozyskiwanie danych pozwala na dokonanie ich całościowej analizy, identyfikację połączeń pomiędzy osobami stwarzającymi zagrożenie i podjęcie odpowiednich działań zapobiegawczych.

Założeniem masowego przechwytywania nie jest jednak próba uzyskania dostępu do całości ruchu internetowego. Działanie tego rodzaju nie mogłoby w efektywny sposób realizować faktycznych potrzeb wywiadowczych ani też nie spełniałoby kryterium proporcjonalności. Wykorzystywane przez służbę GCHQ[122] systemy masowego przechwytywania komunikacji ograniczają się do bardzo zawężonej części globalnej infrastruktury sieci Internet. Dokonują one filtrowania ruchu internetowego na podstawie szeregu kryteriów

prawnych dotyczących instrumentów operacyjno-rozpoznawczych było przyjęcie we Francji ustawy o wywiadzie z 24 lipca 2015 r. (*Loi n°2015-912 du 24 juillet relative au renseignement*), www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id [dostęp: 22 VIII 2017].

[122] Government Communications Headquarters (Centrala Łączności Rządowej) – zgodnie z ustawą *Investigatory Powers Act* jest jedyną brytyjską służbą uprawnioną do prowadzenia masowego przechwytywania (ang. *bulk interception*).

(tzw. selektorów) pozwalających na ustalenie konkretnych priorytetów odpowiadających najważniejszym celom operacyjnym służby. Przechwycona komunikacja podlega dalszej analizie po spełnieniu warunków wynikających z przepisów wewnętrznych i tylko wtedy, gdy jest to niezbędne i proporcjonalne dla realizacji zadań służby[123].

1.1. Podstawy prawne

Masowe przechwytywanie zostało uregulowane w rozdziale 1 części 6 ustawy *Investigatory Powers Act* 2016 z 29 listopada 2016 r.[124] (dalej: IPA). Omawiany akt utrzymał najistotniejsze postanowienia ustawy *Regulation of Investigatory Powers Act* z 2000 r. (dalej: RIPA), które odnosiły się do omawianego instrumentu, wprowadzając jednocześnie dodatkowe mechanizmy ochronne mające na celu zwiększenie kontroli nad wykorzystywaniem masowego przechwytywania w praktyce i wzmocnienie instrumentów chroniących prawo do prywatności.

Analogicznie do przepisów ustawy RIPA nakazy autoryzujące masowe przechwytywanie będą wydawane w dalszym ciągu przez Sekretarza Stanu; jednak w myśl ustawy IPA będą podlegać zatwierdzeniu przez Komisarza (Judicial Commissioner) – organu oceniającego niezbędność, proporcjonalność i celowość wydania nakazu w konkretnym przypadku. Wprowadzona przez ustawę IPA procedura dwustopniowej autoryzacji nakazów (ang. *double lock*), obowiązująca nie tylko w przypadku masowego przechwytywania, lecz także w odniesieniu do innych instrumentów zdobywania informacji opisanych w ustawie, jest jedną z najbardziej doniosłych zmian w brytyjskim systemie przepisów prawnych regulujących sferę funkcjonowania służb specjalnych i wykorzystywania przez nie środków niejawnego pozyskiwania informacji. Ciężar oceny, czy charakter określonej sytuacji rzeczywiście uzasadnia wykorzystanie mechanizmów charakteryzujących się wysokim stopniem inwazyjności i potencjalnie mogących stwarzać poważne zagrożenia dla konstytucyjnych praw i wolności, został rozłożony pomiędzy organ władzy wykonawczej (Sekretarz Stanu) i organ o charakterze quasi-sądowym (Komisarz). Pomimo iż szczegółowa analiza systemu kontroli sądowej nad procesem stosowania środków przewidzianych w ustawie wspomnieć w tym miejscu należy, że skargi w zakresie ich niezgodnego z prawem stosowania rozpatruje Investigatory Powers Tribunal utworzony na podstawie sekcji 65 ustawy RIPA. Należy podkreślić, że ustawa IPA wprowadziła możliwość odwołania się od orzeczeń Trybunału do innego sądu krajowego (sekcja 242 IPA).

Ustawa stworzyła również instytucję Investigatory Powers Commissioner – organ nadzorczy skupiający w sobie kompetencje realizowane dotychczas przez trzy oddzielne podmioty (Chief Surveillance Commissioner, Interception of Communications Commissioner and Intelligence Services Commissioner). Dnia 1 września 2017 r. na to stanowisko został powołany sir Adrian Fulford[125]. Zgodnie z art. 229 IPA organ ten kontroluje, przez audyt, inspekcje i inne czynności wyjaśniające, wykonywanie przez organy władzy publicznej zadań związanych z przechwytywaniem komunikacji, pozyskiwaniem i retencją danych komunikacyjnych, pozyskiwaniem danych wtórnych lub związanych z nimi danych systemowych oraz ingerencją w urządzenia.

---

[123] *Investigatory Powers Bill: Operational Case for Bulk Powers*, 1 March 2016, par. 7.1–7.3, s. 26, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents; [dostęp: 24 VII 2017].

[124] www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm [dostęp: 24 VII 2014].

[125] https://www.gov.uk/government/news/investigatory-powers-commissioner-establishes-oversight-regime, http://ipco.org.uk/ [dostęp: 22 IX 2017].

Zgodnie z sekcją 136 ustawy IPA nakaz masowego przechwytywania (ang. *bulk interception warrant*) musi spełniać dwa warunki.

Warunek A. Głównym celem nakazu jest przechwycenie zagranicznej łączności lub zdobycie za jej pośrednictwem tzw. danych wtórnych (ang. *secondary data*). Pojęcie zagranicznej łączności (ang. *overseas-related communications*) oznacza komunikację wysyłaną lub odbieraną przez osoby znajdujące się poza terytorium Wysp Brytyjskich (podsekcja 3). Dane wtórne, w kontekście łączności przesyłanej z wykorzystaniem systemu telekomunikacyjnego, oznaczają dane opisane w sekcji 137 (4) i (5), które mają następujące cechy:

1) są to dane systemowe[126] dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób);
2) są to dane identyfikujące[127] posiadające następujące cechy:
   – są dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób),
   – mogą być logicznie odłączone od reszty komunikatu,
   – w razie odłączenia nie ujawniłyby niczego, co może w rozsądny sposób zostać uznane za mające znaczenie dla komunikatu, pomijając znaczenie wynikające z samej komunikacji lub jakichkolwiek danych dotyczących przesyłu komunikatu.

Pozyskiwanie danych wtórnych jest możliwe zarówno w fazie przesyłu komunikatu, jak i w każdym czasie, gdy jest on przechowywany w systemie lub przez ten system, zarówno przed, jak i po dokonaniu przesyłu [sekcja 137 (2)].

Warunek B. Nakaz zobowiązuje osobę, do której jest skierowany, do realizacji czynności w nim opisanych lub autoryzuje ich dokonanie przez podjęcie następujących działań:

1) przechwycenie, w trakcie przesyłu za pośrednictwem systemu telekomunikacyjnego, łączności opisanej w nakazie,
2) uzyskanie opisanych w nakazie danych wtórnych pochodzących z łączności przesyłanej z wykorzystaniem takiego systemu,
3) dokonanie w sposób opisany w nakazie selekcji przechwyconej treści komunikatów lub danych wtórnych uzyskanych na podstawie nakazu,
4) ujawnienie w sposób opisany w nakazie informacji uzyskanych na jego podstawie osobom, do których skierowany jest nakaz lub osobom działającym w ich imieniu.

Nakaz masowego przechwytywania autoryzuje również dokonanie dodatkowych czynności nieprzewidzianych wprost w treści dokumentu, niezbędnych dla realizacji głównego celu wymienionego w nakazie, z uwzględnieniem przechwycenia łączności niewyszczególnionej w nakazie i uzyskania pochodzących z niej danych wtórnych, zobowiązanie innych osób do udzielenia pomocy w realizacji nakazu, a także uzyskanie od operatora telekomunikacyjnego powiązanych danych systemowych[128].

---

[126] Sekcja 263 (4) IPA– „Dane systemowe w rozumieniu ustawy oznaczają jakiekolwiek dane ułatwiające lub umożliwiające identyfikację wszelkich elementów umożliwiających lub ułatwiających funkcjonowanie –

a) usług pocztowych;
b) systemu telekomunikacyjnego (z uwzględnieniem wszystkich urządzeń stanowiących jego cześć);
c) usługi telekomunikacyjnej dostarczanej za pośrednictwem systemu telekomunikacyjnego;
d) systemu przechowującego dane o komunikacji i inne informacje;
e) usług dostarczanych przez system przechowujący dane o komunikacji i inne informacje".

[127] Sekcja 263 (2) – „Dane identyfikujące w rozumieniu ustawy oznaczają dane ułatwiające lub umożliwiające identyfikację osoby, urządzenia, systemu lub usługi, zdarzenia, lokalizacji osoby, zdarzenia lub innego elementu" (wszystkie tłum. aut.).

[128] Powiązane dane systemowe (ang. *related systems data*), zgodnie z sekcją 136 (6), oznaczają dane systemowe dotyczące łączności będącej przedmiotem nakazu, jej nadawcy, odbiorcy lub zamierzonego odbiorcy, niezależnie od tego, czy jest to osoba fizyczna.

1.2. Rodzaje nakazów przechwytywania danych – najważniejsze różnice pomiędzy tzw. nakazami ukierunkowanymi (*targeted interception warrant*) a nakazami *bulk interception*[129]

Ustawa IPA rozróżnia następujące rodzaje nakazów przechwytywania danych: nakazy ukierunkowane, nakazy masowego przechwytywania danych, nakazy selekcji materiału zebranego za pomocą *bulk interception* do dalszej analizy oraz nakazy wydawane w ramach realizacji wniosku o współpracę wydanego przez właściwe organy innych państw (ang. *mutual assistance warrant*). Pomimo że celem niniejszego opracowania jest charakterystyka instrumentów typu „*bulk*", niezbędne jest wskazanie najważniejszych różnic pomiędzy masowymi a ukierunkowanymi nakazami przechwytywania informacji.

- Nakaz ukierunkowany [sekcja 15 (2)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na przechwyceniu komunikacji wskazanej w nakazie lub pozyskania danych wtórnych.
- Nakaz selekcji materiału zebranego za pomocą *bulk interception* do dalszej analizy [sekcja 15 (3)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na wstępnym oszacowaniu materiału zebranego w toku masowego przechwytywania danych i selekcji wybranych elementów do dalszej analizy. Ten nakaz musi być wydany wówczas, gdy treść przechwyconej komunikacji ma zostać poddana analizie na podstawie kryteriów dotyczących osoby, która według dostępnych informacji przebywa na terytorium Wielkiej Brytanii w chwili selekcji materiału do dalszej analizy. Wydanie tego rodzaju nakazu znosi ustanowiony na podstawie sekcji 152 (4) zakaz selekcji do dalszej analizy treści komunikacji, jeżeli kryteria wykorzystane w celu selekcji przechwyconego materiału odnoszą się do osoby znajdującej się według dostępnej wiedzy na terytorium Wysp Brytyjskich lub jeżeli te kryteria zastosowano w celu zidentyfikowania treści komunikacji wysłanej lub odebranej przez taką osobę.
- Nakaz masowego przechwytywania (sekcja 136) – jego głównym celem jest przechwycenie zagranicznej komunikacji lub uzyskanie danych wtórnych pochodzących z tej komunikacji. Autoryzuje on jednorazowe lub wielokrotne przechwycenie komunikacji, uzyskanie danych wtórnych oraz selekcję przechwyconego materiału do dalszej analizy. Może on dotyczyć również wyłącznie danych wtórnych. W odróżnieniu od nakazów o charakterze ukierunkowanym może on dotyczyć komunikacji określonego zbioru osób, nie zaś indywidualnie wskazanego podmiotu. Druga zasadnicza różnica między nakazem ukierunkowanym a masowym polega na odmiennym zakresie przedmiotowym obu nakazów – sekcja 136 dotyczy przechwytywania zagranicznej komunikacji i pozyskiwania związanych z nią danych wtórnych, *a contrario* – należy zatem wnioskować, że nakaz ukierunkowany dotyczy przechwytywania komunikacji prowadzonej na terytorium Wielkiej Brytanii i zdobywania związanych z nią danych wtórnych.

[129] *Interception of Communications – Draft Code of Practice* s. 12–13, www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice [dostęp: 17 VIII 2017].

1.3. Proces wydawania nakazu masowego przechwytywania (sekcja 138)

Jak wskazano na wstępie, proces wydawania nakazu dokonania czynności związanych z masowym przechwytywaniem danych ma charakter dwustopniowy. W celu wzmocnienia standardów ochrony prywatności cała konstrukcja wykorzystywania środków opisanych w ustawie IPA została oparta na modelu *double lock* zakładającym powierzenie autoryzacji wniosków dwóm niezależnym od siebie organom dokonującym autoryzacji wniosków – Sekretarzowi Stanu i Komisarzowi.

Na wstępie należy wskazać, że mechanizm masowego przechwytywania jest ściśle powiązany ze sferą ochrony bezpieczeństwa narodowego. Zgodnie z sekcja 138 (1) (b) Sekretarz Stanu może, na wniosek szefa jednej ze służb wywiadowczych[130], wydać omawiany nakaz, jeżeli jest to niezbędne:

- w celu ochrony interesu bezpieczeństwa narodowego,
- w tym celu i w którymkolwiek z celów opisanych w podsekcji (2).

Przedstawiony powyżej sposób sformułowania sekcji 138 sprawia, że ustawodawca wprowadził bezwzględny wymóg istnienia związku dwóch pozostałych przesłanek, – zapobiegania i wykrywania poważnej przestępczości oraz ochrony interesów ekonomicznych UK – z bezpieczeństwem narodowym.

Ustawodawca wprowadził ponadto dalsze mechanizmy ograniczające możliwość wykorzystania *bulk interception* w praktyce. Wydanie nakazu w celu ochrony interesów ekonomicznych jest możliwe tylko wtedy, gdy informacje, które mają zostać uzyskane dzięki zastosowaniu mechanizmu, dotyczą działań lub zamierzeń osób znajdujących się poza terytorium Wysp Brytyjskich [sekcja 138 (3)]. Ustawa wyklucza możliwość wydania nakazu, jeżeli ma on służyć wyłącznie pozyskiwaniu dowodów dla celów postępowania karnego [sekcja 138 (4)]. Biorąc pod uwagę konstrukcję przepisów sekcji 138 określających przesłanki materialne stosowania masowego przechwytywania w praktyce, należy zwrócić uwagę na to, że ustawodawca znacznie ograniczył możliwość wykorzystywania tego instrumentu w celu ścigania przestępczości. Przepis sekcji 138 (1) (b) w zw. z podsekcją (2) (a) oraz (4) sprawia, że mechanizm *bulk interception* będzie mógł być stosowany wyłącznie w odniesieniu do wąskiej kategorii przestępstw uznawanych za zagrażające bezpieczeństwu narodowemu (np. przestępstwo szpiegostwa, terroryzmu oraz czyny zabronione związane z proliferacją broni masowego rażenia). Wyłączenie możliwości wykorzystania masowego przechwytywania jedynie w celu zbierania dowodów dla celów postępowania karnego sprawia, że ten instrument będzie miał zastosowanie na etapie rozpoznawania i wykrywania przestępstw zagrażających bezpieczeństwu narodowemu, nie zaś na etapie ewentualnego postępowania sądowego. Opisane powyżej elementy sprawiają, że *bulk interception* należy traktować jako środek o charakterze stricte wywiadowczym, jego zaś rolę w procesie zwalczania przestępczości należy uznać za pomocniczą.

Oprócz wymienionych powyżej przesłanek materialnych sekcja 138 przewiduje następujące warunki wydania nakazu masowego przechwytywania, stanowiąc, że jest to możliwe, jeżeli w opinii Sekretarza Stanu:

- głównym celem nakazu jest przechwycenie zagranicznej łączności (ang. *overseas -related communications*) lub uzyskanie pochodzących z niej danych wtórnych,

[130] Sekcja 263 (1) – „Pojęcie *h e a d* , w odniesieniu do służb wywiadowczych, oznacza –
a) w odniesieniu do Security Service – Dyrektora Generalnego,
b) w odniesieniu do Secret Intelligence Service – Szefa,
c) w odniesieniu do GCHQ – Dyrektora".

- działania autoryzowane na podstawie nakazu są proporcjonalne do zakładanego celu,
- wszystkie wskazane we wniosku o wydanie nakazu cele operacyjne[131] są celami, dla których analiza przechwyconej treści komunikatów lub danych wtórnych jest lub może być konieczna,
- analiza przechwyconej treści komunikatów lub danych wtórnych jest niezbędna w kontekście wszystkich celów operacyjnych z jakichkolwiek powodów, dla których Sekretarz Stanu uznaje wydanie nakazu za niezbędne,
- istnieją wystarczające środki zabezpieczające odnoszące się m.in. do procedur związanych z wykorzystywaniem przechwyconego materiału, jego dalszym ujawnieniem i innymi aspektami dotyczącymi jego ochrony,
- wydanie nakazu zostało zatwierdzone przez Komisarza.
- Jeżeli w opinii Sekretarza Stanu jest prawdopodobne, że realizacja nakazu będzie wymagała pomocy operatora telekomunikacyjnego działającego poza Wielką Brytanią, ustawa nakłada na Sekretarza Stanu obligatoryjny wymóg przeprowadzenia konsultacji z tym operatorem oraz dokonania oceny, przed wydaniem nakazu, m.in. liczby użytkowników usług telekomunikacyjnych dostarczanych przez operatora objętych masowym przechwytywaniem, możliwości technicznych operatora co do udzielenia przez niego pomocy w realizacji nakazu, koszt takiej pomocy i inne ewentualne skutki wykonania nakazu dla operatora (sekcja 139).

1.4. Zatwierdzenie nakazu przez Komisarza

Przy dokonywaniu oceny decyzji o wydaniu nakazu (sekcja 140) Komisarz weryfikuje wnioski Sekretarza Stanu dotyczące:

- konieczności wydania nakazu w związku z przesłankami wymienionymi w sekcji 138 (1) (b) – bezpieczeństwem narodowym, zapobieganiem i wykrywaniem poważnej przestępczości oraz ochroną interesów ekonomicznych istotnych z punktu widzenia bezpieczeństwa narodowego,
- proporcjonalności czynności opisanych w nakazie do zakładanego celu,
- sprawdzenia, czy wskazane w nakazie cele operacyjne mogą zostać uznane za cele, dla których realizacji dalsza analiza przechwyconych treści komunikatów lub danych wtórnych jest lub może być niezbędna,
- weryfikacji, czy analiza przechwyconych treści komunikatów lub danych wtórnych jest niezbędna dla realizacji każdego z ww. celów.

W razie odmowy zatwierdzenia decyzji o wydaniu nakazu Komisarz informuje o tym pisemnie Sekretarza Stanu.

1.5. Wymogi formalne nakazu

Zgodnie z sekcją 142 nakaz masowego przechwytywania musi spełniać określone kryteria formalne. Do najważniejszych z nich należą:

- wzmianka identyfikująca dokument jako nakaz masowego przechwytywania,

[131] Sekcja 142 – „Cele operacyjne wskazane w nakazie muszą odpowiadać celom wymienionym na liście prowadzonej przez szefów służb wywiadowczych (lista celów operacyjnych) jako cele, dla których przechwycona treść lub dane wtórne na podstawie nakazu masowego przechwytywania mogą być poddane dalszej analizie".

- nakaz musi być adresowany do szefa służby wywiadowczej, który złożył wniosek o wydanie nakazu lub w którego imieniu taki wniosek został złożony,
- nakaz musi wymieniać cele operacyjne, dla których przechwycone treści komunikatów lub dane wtórne mogą być poddane dalszej analizie,
- cele operacyjne wskazane w nakazie muszą być uwzględnione w prowadzonej przez szefów służb wywiadowczych tzw. liście celów operacyjnych (ang. *list of operational purposes*) jako cele uzasadniające dalszą analizę treści przechwyconych komunikatów lub danych wtórnych uzyskanych na podstawie nakazu *bulk interception*.

1.6. Czas trwania, modyfikacje i unieważnienie nakazu

Nakaz traci moc po upływie sześciu miesięcy, licząc od dnia jego wydania lub, w razie jego przedłużenia, w dniu następującym po dniu, w którym utraciłby moc, gdyby nie został przedłużony (sekcja 143). Możliwe jest przedłużenie nakazu przez Sekretarza Stanu za zgodą Komisarza, jeżeli w dalszym ciągu istnieją przesłanki, które uzasadniały jego pierwotne wydanie. Przedłużenie jest możliwe w czasie trwania tzw. okresu przedłużenia (ang. *renewal period*) obejmującym 30 dni przed upływem ważności nakazu, z czego ostatni dzień obowiązywania nakazu jest równocześnie ostatnim dniem okresu przedłużenia.

Nakaz może również zostać zmodyfikowany na zasadach opisanych w sekcji 145. Zmiana może obejmować dodanie, modyfikację lub usunięcie któregoś z celów operacyjnych, wskazanych w nakazie, uzasadniających poddanie przechwyconej treści komunikatów lub danych wtórnych dalszej analizie lub stwierdzenie, że nakaz nie autoryzuje już przechwytywania treści komunikatów w czasie ich przesyłu za pomocą systemu telekomunikacyjnego lub pozyskania danych wtórnych. Możliwość zmiany treści nakazu należy traktować jako element umożliwiający dynamiczne reagowanie na bieżącą sytuację operacyjną oraz dowodzi, że nie w każdym przypadku treść przechwytywanych komunikatów i dane wtórne są ze sobą nierozerwalnie powiązane. Przeciwnie – pozyskiwanie ww. typów danych może mieć charakter alternatywny, na co wskazuje raport[132] o wykorzystywaniu tzw. *bulk powers* opracowany przez niezależny organ – Niezależnego Sprawozdawcę ds. Prawa Antyterrorystycznego (*Independent Reviewer of Terrorism Legislation*). Wskazuje on, że możliwość ograniczenia nakazu masowego przechwytywania wyłącznie do danych wtórnych jest jednym z instrumentów pozwalających na zdobywanie przez służby informacji w sposób w mniejszym stopniu ingerujący w prawo do prywatności.

Jeżeli prowadzenie czynności opisanych w nakazie przestało być niezbędne dla ochrony bezpieczeństwa narodowego, jeżeli przestały one mieć proporcjonalny charakter w stosunku do zakładanych celów lub jeżeli analiza przechwyconych na podstawie nakazu treści komunikatów lub danych wtórnych nie jest już konieczna dla realizacji celów operacyjnych, Sekretarz Stanu lub działający z jego upoważnienia urzędnik szczebla kierowniczego (ang. *senior official*) może stwierdzić wygaśnięcie nakazu w dowolnym momencie jego obowiązywania (sekcja 148).

[132] *Report of the Bulk Powers Review by David Anderson Q.C Independent Reviewer of Terrorism Legislation*, August 2016, pkt 2.9, s. 22 dostęp na stronie https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf [dostęp: 21 IX 2017].

1.7. Praktyczne aspekty działania *bulk interception*

Masowe przechwytywanie można zdefiniować jako gromadzenie, w trakcie ich przesyłu, informacji o komunikacji (prowadzonej poza granicami UK) za pośrednictwem sieci telekomunikacyjnych w taki sposób, że ich treść staje się dostępna dla osób innych niż nadawca lub odbiorca. Instrument *bulk interception* służy wykrywaniu zagrożeń bezpieczeństwa narodowego w dwóch ściśle określonych przypadkach:

1) monitorowania komunikacji osób, które zostały już wcześniej zidentyfikowane jako stwarzające potencjalne zagrożenie,
2) wyszukiwania informacji prowadzących do wygenerowania nowych tropów wywiadowczych (ang. *intelligence leads*) dotyczących sytuacji nieznanych do tej pory właściwym organom, np. nowych zagrożeń terrorystycznych czy cyberataków[133].

Pomimo licznych doniesień medialnych odnoszących się do tzw. programów masowej inwigilacji wykorzystywanych przez służby wywiadowcze państw tzw. Pięciorga Oczu, argumenty przedstawione zarówno przez rząd, jak i przez właściwe organy parlamentarne Wielkiej Brytanii zdają się zaprzeczać tezie, że te służby (np. GCHQ) prowadziły tak naprawdę działania polegające na nieselektywnym i ogólnym monitorowaniu całości komunikacji internetowej, naruszając tym samym prawo do prywatności nieokreślonej liczby osób niestwarzających żadnego zagrożenia dla bezpieczeństwa narodowego. Raport Komisji ds. Wywiadu i Bezpieczeństwa (dalej: komisja ISC) z 2015 r. wskazuje, że masowe przechwytywanie nie może dotyczyć całości komunikacji internetowej z uwagi na ograniczenia natury prawnej, technologicznej oraz praktycznej. Konieczność dokonywania szczegółowych czynności analitycznych dotyczących tak dużej ilości danych byłoby zadaniem przekraczającym możliwości GCHQ. Twórcy raportu wskazują, że ta służba może teoretycznie uzyskać dostęp do niewielkiej części z ok. 100 000 przekaźników[134], stanowiących podstawowy element składowy infrastruktury globalnej sieci Internet. Służba określa przekaźniki, przez które prawdopodobnie mogą być przesyłane dane o istotnym znaczeniu wywiadowczym. Niemniej jednak, z uwagi na to, że przetwarzanie tak ogromnych ilości danych wymaga znacznego nakładu środków i pracy analitycznej, GCHQ przechwytuje komunikację przesyłaną jedynie przez niewielką część tych przekaźników, do których ma teoretycznie dostęp. Co więcej – nie oznacza to, że GCHQ gromadzi i przechowuje całą komunikację przesyłaną przez te przekaźniki, informacje te są następnie poddawane selekcji znacznie zmniejszającej ilość danych, do których służba ta fizycznie uzyskuje dostęp i poddaje analizie[135]. W tym kontekście niezmiernie istotne znaczenie ma zawarta w cytowanym raporcie komisji ISC uwaga, pomimo pojawiających się w debacie publicznej zarzutów, iż *bulk interception* prowadzi do masowego i nieselektywnego pozyskiwania danych, w istocie rzeczy instrument ten ma charakter ukierunkowany – GCHQ wybiera przekaźniki, do których dostęp, z jej punktu widzenia, jest najbardziej korzystny, następnie zaś stosuje tzw. selektory w celu wyodrębnienia komunikacji konkretnych osób[136]. *Bulk interception* nie zbiera zatem wszystkich informacji, lecz ich ściśle wyselekcjonowaną część, co powoduje, że wskazane powyżej zarzuty

[133] *Privacy and Security: a modern and transparent legal framework*; Intelligence and Security Committee of Parliament, 12 March 2015, s. 28, www.isc.independent.gov.uk/news-archive/12March2015 [dostęp: 22 VIII 2017].

[134] Twórcy omawianych raportów posługują się pojęciem *b e a r e r* (tłum. własne aut.).

[135] *Privacy and Security*…, s. 27.

[136] Tamże, s.28–29.

dotyczące powszechnego i systematycznego łamania prawa do prywatności oparte są na niewłaściwych przesłankach.

Zgodnie z informacjami zawartymi w cytowanych powyżej raportach Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego oraz parlamentarnej komisji ISC proces masowego przechwytywania można – w ujęciu ogólnym – podzielić na trzy zasadnicze fazy: zbierania informacji (ang. *collection*), wstępnej selekcji (ang. *filtering*) oraz wyboru, które z informacji nieodrzuconych na poprzednim etapie zostaną faktycznie poddane dalszej analizie (ang. *selection for examination*).

Faza pierwsza – collection

Proces faktycznego zbierania informacji rozpoczyna się od dokonania oceny przewidywanej wartości wywiadowczej danych przesyłanych przez poszczególne przekaźniki oraz wyboru przekaźników, które GCHQ zamierza w danym momencie wykorzystać. Wybór ma charakter wysoce ocenny, opiera się prawdopodobnie na określonych założeniach wypracowywanych na podstawie, po pierwsze, specjalistycznej wiedzy technicznej dotyczącej sposobu przepływu informacji w Internecie oraz, po drugie, na informacjach uzyskanych z innych rodzajów źródeł, np. źródeł osobowych.

Jak wskazano powyżej, GCHQ nie dysponuje możliwościami technicznymi pozwalającymi na jednoczesne pozyskiwanie informacji ze wszystkich najważniejszych przekaźników tworzących globalną sieć Internet. Służba ta ogranicza zatem zakres swoich działań do tych jej elementów składowych, w stosunku do których istnieją uzasadnione przesłanki, by sądzić, że mogą przynieść rzeczywiste korzyści wywiadowcze. Według publicznie dostępnych informacji zawartych w cytowanych raportach liczba przekaźników, z których w danym momencie GCHQ zdobywa informacje, jest niewielka (jest określana np. jako: *a tiny fraction of all the bearers in the world*[137], czyli: niewielka część wszystkich przekaźników na świecie – tłum. wł. aut.) Informacje o dokładnej liczbie przekaźników, do których służba ma dostęp, zostały zawarte w raporcie ISC, ale zostały usunięte z publicznie dostępnej wersji dokumentu. Są to zatem informacje niejawne[138].

Faza druga – wstępna selekcja (filtering)

Wykorzystywane przez GCHQ systemy przetwarzania danych badają ruch internetowy przepływający przez przekaźniki, do których służba ma dostęp. W dalszej kolejności są wykorzystywane instrumenty tzw. filtrowania danych umożliwiające wyselekcjonowanie danych mogących potencjalnie przynieść korzyści wywiadowcze. Jednocześnie odrzuceniu ulegają informacje, których znaczenie, zgodnie z zastosowanymi kryteriami wyboru, jest niewielkie.

Już na etapie wstępnej selekcji odrzuceniu ulega znaczna część danych przesyłanych przez przekaźniki wybrane przez GCHQ. Proces tzw. filtrowania należy trak-

[137] Tamże.

[138] „GCHQ could theoretically assess a small percentage (***%) of the 100.000 bearers which make up the Internet, but in practice they access only a fraction of these (***) (…) GCHQ do not therefore have „blanket coverage of all internet communications, as has been alleged – they have neither the legal authority, the technical capacity nor the resources to do so". (Działania GCHQ nie obejmują zatem w sposób kompleksowy całej komunikacji internetowej, jak zarzucano – nie ma ona ku temu podstaw prawnych, zdolności ani zasobów – tłum. wł. aut.), za: *Privacy and Security*…, s. 28.

tować z jednej strony jako narzędzie pozwalające na skoncentrowanie późniejszych działań analitycznych na informacjach mogących mieć faktycznie znaczenie z punktu widzenia wywiadowczego, z drugiej zaś jest to jeden z etapów złożonego i wielostopniowego procesu selekcji przyczyniający się w znacznej mierze do ochrony prywatności i zminimalizowania negatywnych skutków masowego przechwytywania dla osób niepowiązanych w żaden sposób z działalnością mogącą stanowić zagrożenie dla bezpieczeństwa narodowego. Jest to również argument przemawiający na niekorzyść tezy, że systemy masowego pozyskiwania danych wykorzystywane m.in. przez GCHQ mają charakter zupełnie nieselektywny, wykorzystujące je służby dążą zaś do totalnej inwigilacji wszystkich użytkowników Internetu czy innych systemów komunikacji.

Faza trzecia – wybór informacji do dalszej analizy (selection for examination)

Dane nieodrzucone na etapie wstępnej selekcji są poddawane kwerendom (prostym i złożonym) w celu wyodrębnienia komunikacji mogącej mieć znaczenie wywiadowcze. Raport Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego wskazuje, że GHCQ wykorzystuje dwa zasadnicze, odrębne mechanizmy mające na celu ocenę informacji zbieranych w toku masowego przechwytywania – proces selektorów silnych (ang. *strong selector process*) i proces kwerend złożonych (ang. *complex query process*).

1.8. Proces selektorów silnych

Proces związany z wykorzystaniem selektorów silnych jest przykładem kwerendy prostej, polegającej na wyszukiwaniu informacji na podstawie elementów dających wysokie prawdopodobieństwo jednoznacznej identyfikacji konkretnej osoby. Przykładem selektora silnego jest np. numer telefonu oraz adres poczty elektronicznej. Kwerendy złożone prowadzone są natomiast na podstawie kryteriów wykorzystujących selektory o mniejszej mocy, których nie można jednoznacznie przyporządkować do konkretnej osoby. W połączeniu pozwalają one jednak na znaczne zredukowanie ryzyka tzw. fałszywych trafień (ang. *false positive*) mogących prowadzić do analizy danych dotyczących osoby przypadkowej, niezwiązanej z zainteresowaniami służby[139].

Można domniemywać, że kwerendy proste, wykorzystujące mechanizm selektorów silnych, mają charakter bardziej ukierunkowany i są stosowane wówczas, gdy służba dysponuje stosunkowo dużą ilością informacji o danej osobie czy o konkretnej sytuacji operacyjnej. Ten proces sprawdza się, jeśli weźmie się pod uwagę linię chronologicznego rozwoju danego zagrożenia, na jego dalszych etapach, gdy posiadane przez służbę informacje pozwalają na określenie zaangażowanych osób, wykorzystywanych przez nie środków komunikacji, miejsca ich pobytu czy innych elementów. Można zatem przyjąć, że efektywność procesu selektorów silnych jest najwyższa, jesli doszło do indywidualizacji elementów składowych konkretnej sytuacji mogącej stanowić zagrożenie dla bezpieczeństwa narodowego.

Z technicznego punktu widzenia ten system porównuje dane przepływające przez konkretny przekaźnik z listą selektorów silnych dotyczących konkretnych celów operacyjnych[140]. Zgodnie z informacjami przedstawionymi w cytowanym raporcie komisji ISC, uzyskanymi od służby GCHQ, wszystkie komunikaty i dane wtórne odpowiadające

[139] *Report of the Bulk Powers Review*…, s. 24.

[140] Liczba aktualnie wykorzystywanych przez GCHQ selektorów i indywidualnych celów operacyjnych została usunięta z raportu komisji ISC, *Privacy and Security: a modern and transparent*…, s. 28.

konkretnym selektorom silnym są automatycznie zbierane w czasie zbliżonym do czasu rzeczywistego, podczas gdy pozostałe informacje są odrzucane. Informacje o ilości oraz proporcjach zbieranych i odrzucanych danych nie zostały uwzględnione w publicznie dostępnej wersji raportu.

Komisja zwraca uwagę, że mechanizm *bulk interception* – pomimo że jest zaliczany przez ustawę IPA do kategorii *bulk powers*, rozumianych jako instrumenty masowego pozyskiwania danych – jak wskazano powyżej, w gruncie rzeczy w praktyce jest on ściśle skoncentrowany na określonych osobach, o czym świadczy stosowanie selektorów pozwalających na odrzucenie danych nieprzedstawiających wartości wywiadowczej.

1.9. Proces kwerend złożonych

W przeciwieństwie do opisanego powyżej procesu wykorzystującego selektory silne wykorzystujące czynniki, takie jak np. adres poczty elektronicznej, kwerendy złożone polegają na zastosowaniu większej liczby (np. trzech lub czterech) znacznie bardziej kompleksowych kryteriów selekcji informacji. Ten proces jest prowadzony na podstawie niewielkiej liczby przekaźników (mniejszej niż w przypadku procesu selektorów silnych), w których przypadku najbardziej jest prawdopodobne, że przesyłają one informacje mogące mieć istotne znaczenie[141].

Systemy przetwarzania danych GCHQ stosują w pierwszej kolejności tzw. zasady selekcji (ang. *selection rules*) zezwalające na odrzucenie większości danych przepływających przez dany przekaźnik. Zbierają one równocześnie informacje, które w opinii służby mogą mieć znaczenie z punktu widzenia wywiadowczego. W dalszej kolejności systemy informatyczne dokonują automatycznych sprawdzeń zgromadzonych w ten sposób danych przy użyciu kompleksowych kryteriów wyszukiwania, co pozwala na odrzucenie znacznej części fałszywych trafień (ang. *false positive*). Pomimo że analitycy mogą dokonywać dodatkowych sprawdzeń, korzystając ze złożonych kryteriów wyszukiwania, wewnętrzne regulacje GCHQ i sposób działania systemów analitycznych nie pozwalają im na dokonywanie dowolnych wyszukiwań, nieopartych na istniejących potrzebach operacyjnych.

Proces masowego przechwytywania z wykorzystaniem kompleksowych kryteriów wyszukiwań jest w istocie bliższy koncepcji *bulk interception*, niż pozyskiwanie informacji na podstawie selektorów silnych z uwagi na to, że specyfika jego funkcjonowania zakłada zbieranie niewyselekcjonowanych danych, zarówno treści komunikatów, jak i danych wtórnych. Niemniej jednak pozwala on na dokonywanie kompleksowych kwerend informacji zgromadzonych dzięki kombinacji kilku selektorów, co w znacznej mierze przyczynia się do oddzielenia informacji mogących mieć znaczenie z punktu widzenia bezpieczeństwa narodowego od tych, które nie mają żadnego związku z celami działań służby[142].

Analiza przedstawionych różnic między masowym przechwytywaniem prowadzonym z wykorzystaniem selektorów silnych a procesem kwerend złożonych prowadzi do wniosku, że są to dwa komplementarne i wzajemnie się uzupełniające instrumenty. Skuteczność jednego bądź drugiego mechanizmu w danym przypadku jest uzależniona od odpowiedniego doboru właściwego procesu do konkretnych uwarunkowań operacyjnych. Mechanizm związany z użyciem selektorów silnych, jak wskazano powyżej, jest

[141] Tamże, s. 29.

[142] *Report of the Bulk Powers Review*…, s. 25.

najskuteczniejszy w sytuacji posiadania przez służby innych informacji wskazujących na istnienie określonego zagrożenia, pozwalających na indywidualizację osób zaangażowanych w działania zagrażające bezpieczeństwu narodowemu i wykorzystywanych przez nie środków komunikacji, jak telefony, komunikatory internetowe czy poczta elektroniczna. Jest to zatem faza następująca po wykryciu określonej sytuacji stanowiącej zagrożenie.

Kwerendy złożone pozwalają natomiast na zdobywanie informacji na wcześniejszym etapie, gdy niemożliwe jest jednoznaczne stwierdzenie, czy daną sytuację należy traktować jako zagrażającą bezpieczeństwu narodowemu. W konsekwencji niemożliwe jest oznaczenie zaangażowanych osób czy określenie innych parametrów sytuacji. Proces analityczny w tym przypadku ma znacznie bardziej dogłębny charakter i pozwala na prześledzenie wzorców komunikacji, jej natężenia czy innych elementów, dzięki którym płynące z niej wnioski i prognozy dotyczące potencjalnych scenariuszy rozwoju sytuacji będą miały charakter komplementarny i będą przedstawiać tło analizowanych wydarzeń, w przeciwieństwie do selektorów silnych skoncentrowanych na ściśle określonych osobach czy parametrach.

1.10. Kryteria decyzji o poddaniu zebranych informacji dalszej analizie

Niezależnie od zastosowanego w danym przypadku mechanizmu, ilość pozyskiwanych danych jest zbyt duża, aby było możliwe dokonanie ich całościowej analizy. W odniesieniu do procesu selektorów silnych, w celu wyselekcjonowania danych mogących mieć największe znaczenie z punktu widzenia realizacji zadań GCHQ, są one poddawane procesowi tzw. segregacji (ang. *triage*). Z informacji przekazanych przez GCHQ komisji ISC wynika, że wskutek tego procesu większość zebranych danych nigdy nie jest poddawana jakimkolwiek czynnościom prowadzonym przez analityków[143].

W przypadku kwerend złożonych służba określa, które z danych przechodzących przez dane przekaźniki mogą mieć istotne znaczenie przez stosowanie zasad selekcji (ang. *selection rules*) oraz kompleksowych wyszukiwań. W rezultacie analitycy otrzymują zestawienie zawierające określoną liczbę spisów (ang. *index*) w formie tabeli przedstawiającej wyniki tych wyszukiwań. Raport komisji ISC powołując się na informacje przekazane przez GCHQ, wskazuje, że (…) *uzyskanie przez analityka pełnego dostępu do zawartości określonej pozycji (item) wymaga jej otwarcia bazując na informacjach zawartych w indeksie*. Ten proces wykazuje pewne zbieżności z mechanizmem działania wyszukiwarek internetowych. Analitycy nie mogą badać wszystkich rezultatów wyszukiwania, muszą polegać na swojej indywidualnej ocenie i doświadczeniu w celu podjęcia decyzji o tym, które informacje są z ich punktu widzenia najbardziej istotne. Służba podała komisji ISC również dokładną liczbę pozycji wybieranych przez analityków w czasie jednego dnia pracy, została jednak usunięta z publicznej wersji omawianego raportu[144].

Zasady dotyczące poddawania przechwyconych danych (zarówno treści, jak i danych wtórnych) zostały określone w sekcji 152 IPA. W celu zapewnienia spójności terminologicznej poniżej przytoczono jej tłumaczenie.

> 152 – Instrumenty zabezpieczające w zakresie analizy przechwyconych informacji
>
> (1) Dla celów sekcji (150), wymogi dotyczące przechwyconej treści komunikatów lub danych wtórnych pozyskanych na podstawie nakazu są spełnione, jeżeli:

[143] *Privacy and Security*…, s. 31.

[144] Tamże.

a) selekcja jakichkolwiek przechwyconych treści lub danych wtórnych do dalszej analizy dokonywana jest wyłącznie dla realizacji ustalonych celów (podsekcja 2);

b) selekcja jakichkolwiek przechwyconych treści lub danych wtórnych do dalszej analizy jest niezbędna i proporcjonalna we wszystkich okolicznościach;

c) selekcja jakichkolwiek przechwyconych treści do dalszej analizy spełnia warunki selekcji (selection conditions) (podsekcja (3)).

(2) Selekcja przechwyconych treści lub danych wtórnych do dalszej analizy dokonywana jest wyłącznie dla ustalonych celów, jeżeli przechwycone treści lub dane wtórne są wybierane do dalszej analizy o tyle, o ile jest to niezbędne dla realizacji celów operacyjnych wyszczególnionych w nakazie, zgodnie z sekcją 142.

„Wyszczególnione w nakazie" oznacza wskazane w nakazie w czasie selekcji przechwyconych treści lub danych wtórnych do dalszej analizy.

(3) Do warunków selekcji, o których mowa w podsekcji (1) (c) zaliczają się następujące elementy:

a) przechwycone dane nie mogą zostać wyselekcjonowane do dalszej analizy, jeżeli naruszają one zakaz, o którym mowa w podsekcji (4), a osoba wykonująca czynności związane z realizacją nakazu sądzi, że wybór określonych danych do dalszej analizy nie narusza zakazu analizy komunikacji osoby znajdującej się na terytorium Wysp Brytyjskich;

b) wybór przechwyconych danych do dalszej analizy z naruszeniem zakazu, o którym mowa powyżej jest uzasadniony na podstawie sekcji 152 (5);

c) wybór przechwyconych danych do dalszej analizy z naruszeniem zakazu, o którym mowa powyżej uzyskał autoryzację w postaci odrębnego nakazu wydawanego na podstawie rozdziału 1 części 2 IPA;

(4) Zakaz, o którym mowa w podsekcji (3)(a) polega na tym, że przechwycona treść nie może w żadnym razie zostać wyselekcjonowana do dalszej analizy, jeżeli:

a) jakiekolwiek kryteria wykorzystane w selekcji dotyczą osoby, o której wiadomo, że znajduje się na terytorium Wysp Brytyjskich;

b) wybór tych kryteriów ma na celu zidentyfikowanie treści komunikacji wysłanej lub skierowanej do tej osoby;

(5) Wybór przechwyconej treści komunikatów do dalszej analizy jest dopuszczalny na podstawie niniejszej podsekcji jeżeli:

a) kryteria odnoszące się do danej osoby są lub były używane w celu selekcji przechwyconej treści komunikatów w okolicznościach, o których mowa w podsekcji (3) (a) i (b);

b) w którymkolwiek momencie osoba realizująca nakaz sądzi, że zaistniała istotna zmiana okoliczności dotyczących określonej osoby (podsekcja 6) sprawiająca, że wybór przechwyconej treści komunikatów do dalszej analizy naruszałby zakaz, o którym mowa w podsekcji (4);

c) wydany został pisemny nakaz analizy przechwyconej treści komunikatów z wykorzystaniem tych kryteriów przez osobę pełniącą funkcje kierownicze (*senior officer*);

d) wybór przechwyconej treści komunikatów został dokonany przed upływem okresu, o którym mowa w podsekcji (7).

(6) Dla celów podsekcji (5)(b) istotna zmiana okoliczności dotyczących określonej osoby ma miejsce, jeżeli:

a) osoba ta znalazła się na terytorium Wysp Brytyjskich lub

b) przeświadczenie osoby realizującej nakaz, że osoba znajduje się poza terytorium Wysp Brytyjskich okazało się błędne.

(7) W podsekcji (5) –

a) „osoba pełniąca funkcje kierownicze", w odniesieniu do nakazu skierowanego do szefa służby wywiadowczej, oznacza funkcjonariusza tej służby, który:

b) jest członkiem Wyższej Służby Cywilnej (Senior Civil Service) lub członkiem Wyższej Struktury Kierowniczej Służby Dyplomatycznej Jej Królewskiej Mości (Senior Management Structure of Her Majesty's Diplomatic Service) lub

c) zajmuje analogiczne stanowisko w służbie wywiadowczej. (…)

1.11. Wnioski

Instrument masowego przechwytywania należy traktować jako jedno z podstawowych narzędzi wykorzystywanych przez brytyjskie służby wywiadowcze. Umożliwia on wykrywanie zagrożeń dla bezpieczeństwa narodowego na wczesnym etapie ich powstawania, odkrywanie powiązań między fragmentarycznymi informacjami dotyczącymi konkretnych zagrożeń oraz badanie wzorców komunikacji osób mogących stwarzać potencjalne zagrożenie bezpieczeństwa narodowego. W odróżnieniu od tzw. ukierunkowanych metod pozyskiwania informacji skupionych na jednej osobie lub grupie osób, o których działalności służby mają duży zasób wiedzy, *bulk interception* ma kluczowe znaczenie dla wykrywania nieznanych wcześniej, dopiero powstających zagrożeń[145]. Z chronologicznego punktu widzenia – im bardziej zaawansowany jest etap rozwoju konkretnej sytuacji mogącej potencjalnie zagrażać bezpieczeństwu narodowemu, tym większe znaczenie mają metody ukierunkowane. Mechanizmy masowego pozyskiwania danych, w tym *bulk interception*, znajdują największe zastosowanie w pierwszych fazach procesu wykrywania zagrożeń, gdy zagrożenie ma charakter mglisty i nie jest potwierdzone przez informacje pochodząc z innych źródeł, np. ze źródeł osobowych.

Zawarty w raporcie Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego skrótowy opis cyklu działań służb wywiadowczych również zdaje się sugerować, że masowe przechwytywanie należy uznać za instrument realnie przyczyniający się do neutralizacji zagrożeń dla bezpieczeństwa narodowego[146]. Ten cykl składa się z trzech zasadniczych etapów: wykrywania zagrożeń, zrozumienia ich natury i podjęcia odpowiednich działań. Opisywany model należy traktować jako uproszczenie, a czynności realizowane na poszczególnych etapach są ze sobą ściśle powiązane. Nie są one również podejmowane w sposób linearny – niekiedy działania wdrażane w fazach wykrywania i zrozumienia ulegają, w zależności od stopnia intensywności danego zagrożenia, ograniczeniu na rzecz działań operacyjnych, które mogą okazać się konieczne nawet w razie braku pełnej wiedzy o charakterystyce określonej sytuacji.

Zgodnie z informacjami zawartymi w przywołanym powyżej raporcie, do najważniejszych typów czynności analitycznych prowadzonych na różnych etapach cyklu działań służb wywiadowczych należą:

- identyfikacja celu – ustalenie osób, które mogą stać się przedmiotem zainteresowania służb,
- pogłębienie informacji o celu – pozyskiwanie dalszych informacji o potencjalnym celu (m.in. kontaktach czy codziennych aktywnościach), aby ocenić, czy

[145] *Privacy and Security*…, s. 32.

[146] *Report of the Bulk Powers Review*…, s. 142.

może on stwarzać zagrożenie lub czy z innych powodów może stać się przedmiotem zainteresowania,
- wykrycie anomalii – proces technologiczny zmierzający do wykrycia określonych wzorców w zbiorach danych, których analiza może przyczynić się do identyfikacji zagrożenia,
- analiza sieci – proces technologiczny, dzięki któremu analiza informacji uzyskanych przez przechwytywanie może dostarczyć istotnych informacji dotyczących struktury najbliższego otoczenia osoby znajdującej się w zainteresowaniu służb oraz umiejscowić pozyskane dane w odpowiednim kontekście,
- segregacja i przyznanie pierwszeństwa (priorytetyzacja) – proces polegający na oddzieleniu informacji istotnych od nieistotnych[147].

Biorąc pod uwagę charakterystykę *bulk interception*, wydaje się, że uzyskiwane za pośrednictwem tego instrumentu dane mogą mieć niezwykle istotne znaczenie w identyfikacji oraz pogłębianiu informacji o celu oraz w wykrywaniu anomalii w zbiorach danych, co może doprowadzić do odkrycia elementów charakterystycznych dla ataków terrorystycznych czy cybernetycznych.

Pomimo licznych wątpliwości natury etycznej i prawnej dotyczących stosowania masowego przechwytywania, informacje przedłożone przez brytyjskie służby specjalne, przedstawicieli władzy ustawodawczej i wykonawczej pozwalają na sformułowanie wniosku, że nie sposób zanegować pozytywnego wpływu tego mechanizmu na możliwości neutralizacji najbardziej kompleksowych zagrożeń dla bezpieczeństwa narodowego (terroryzm i cyberprzestępczość) oraz, w ograniczonym zakresie i w ściśle określonych przypadkach, zwalczania przestępczości. Przedstawione poniżej przykłady hipotetycznych sytuacji związanych z wykorzystaniem *bulk interception* przemawiają za tym, że podjęcie skutecznych działań neutralizujących określone zagrożenie nie byłoby możliwe lub byłoby znacznie utrudnione bez zastosowania tego instrumentu. Te przykłady to ogólne streszczenie trzech spraw prowadzonych przez brytyjskie służby specjalne w najbardziej wrażliwych obszarach – zwalczania terroryzmu, ścigania sprawców przestępstw związanych z pedofilią[148] oraz ochrony przed cyberatakami[149].

Sprawa nr 1. Zwalczanie terroryzmu

Prowadzone przez brytyjskie służby specjalne analizy danych zgromadzonych dzięki *bulk interception* doprowadziły do zidentyfikowania nieznanej im wcześniej osoby podejrzewanej o planowanie ataków terrorystycznych na terenie państw UE i NATO.

[147] *Report of the Bulk Powers Review*…, s. 143.

[148] W poprzednim stanie prawnym (sekcja 5 ustawy *Regulation of Investigatory Powers Act* 2000) przesłanki wydania przez Sekretarza Stanu nakazu przechwycenia komunikacji (ang. *interception warrant*) były określone w sposób szerszy niż w ustawie IPA. Było to możliwe m.in. w celu ochrony interesów bezpieczeństwa narodowego oraz zapobiegania i wykrywania poważnej przestępczości. Ustawa nie wymagała jednak, aby przesłanka związana z zapobieganiem i wykrywaniem poważnej przestępczości była połączona z bezpieczeństwem narodowym. W ustawie RIPA zwalczanie przestępczości mogło zatem stanowić samoistną przesłankę wydania nakazu przechwytywania. Zgodnie z sekcją 138 ustawy IPA Sekretarz Stanu może wydać nakaz masowego przechwytywania, jeżeli jest to niezbędne z punktu widzenia ochrony interesów bezpieczeństwa narodowego oraz zapobiegania lub wykrywania poważnej przestępczości lub w celu ochrony interesów gospodarczych.

[149] Opis przywołanych spraw (ang. *case studies*) znajduje się dokumencie *Operational Case for Bulk Powers*, s. 28–29, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents [dostęp: 3 VIII 2017].

Utrzymywała ona kontakty ze współpracującymi z Państwem Islamskim ugrupowaniami o charakterze ekstremistycznym, działającymi na terenie Syrii. Biorąc pod uwagę, że podejrzewana osoba przebywała poza granicami Wielkiej Brytanii, wykrycie prowadzonej przez nią działalności za pomocą innych instrumentów wywiadowczych było mało prawdopodobne. Pomimo podejmowanych przez nią działań, mających na celu maskowanie działalności terrorystycznej, służby dzięki wykorzystaniu danych pozyskanych przez masowe przechwytywanie, były w stanie wykryć, że podejrzewana osoba znalazła się na terytorium jednego z państw europejskich. Brytyjskie służby poinformowały właściwe organy tego państwa, które następnie przerwały proces przygotowywania ataku terrorystycznego i przejęły kilka tzw. improwizowanych ładunków wybuchowych.

Przytoczona sprawa pokazuje, jak istotne znaczenie dla zagwarantowania bezpieczeństwa wewnętrznego może mieć masowe przechwytywanie komunikacji prowadzonej przez osoby znajdujące się poza granicami danego państwa lub w sytuacji, gdy jedna ze stron (nadawca lub odbiorca) znajduje się poza jego granicami. Ten przykład jest dowodem na jedną z najważniejszych tez przemawiających za stosowaniem *bulk interception* – w wielu przypadkach jest to jedyny instrument realnie pozwalający na wykrycie zagrożenia w sytuacji, w której pozyskanie niezbędnych informacji nie jest możliwe za pośrednictwem jakichkolwiek innych metod wywiadowczych. Brytyjskie służby wskazały, że podejrzany o działalność terrorystyczną przebywał poza granicami Wielkiej Brytanii i nie był im wcześniej znany. Zdobycie wyprzedzających informacji o jego planach nie byłoby możliwe przy użyciu innych metod, np. źródeł osobowych, inwigilacji ukierunkowanej czy informacji uzyskanych od organów innych państw. Omawiany przypadek potwierdza również to, że podstawową funkcją masowego przechwytywania jest wykrywanie zagrożeń na wczesnym etapie ich powstawania, wówczas gdy stopień konkretyzacji informacji posiadanych przez służby jest niewielki lub gdy nie dysponują one w ogóle wiedzą o danej sytuacji.

Sprawa nr 2. Zwalczanie przestępstw związanych z pedofilią i wykorzystywaniem seksualnym małoletnich

W 2013 r. służby specjalne Wielkiej Brytanii prowadziły analizy danych uzyskanych dzięki *bulk interception* w celu określenia wzorców komunikacji i korzystania z Internetu osób dopuszczających się czynów zabronionych, związanych z wykorzystywaniem seksualnym małoletnich. Prace te doprowadziły do identyfikacji brytyjskiego obywatela odwiedzającego stronę sprzedającą zdjęcia przedstawiające wymienione czynności. Ta strona znajdowała się na serwerze państwa, które niechętnie współpracowało z organami brytyjskimi w sferze ścigania przestępczości. Bez analizy tych danych działalność tej osoby nie mogłaby zostać w żaden sposób wykryta i nie mogłaby ona zostać pociągnięta do odpowiedzialności. W toku dalszych czynności ustalono, że miejsce pracy podejrzanego zapewniało mu kontakt z dziećmi i małoletnimi oraz że figurował on w specjalnym rejestrze osób skazanych za ten rodzaj przestępstw (*UK Violent and Sexual Offenders Register*). Dzięki wykorzystaniu danych zdobytych dzięki zastosowaniu *bulk interception*, sprawca został skazany na trzy lata pozbawienia wolności i poddany instrumentowi zakazującemu zbliżania się do dzieci i małoletnich, uniemożliwiające mu wykonywanie pracy związanej z kontaktem z nimi lub przewidującemu inne instrumenty ochronne.

Sprawa nr 3. Ochrona przed cyberatakami

Jednym z najbardziej powszechnych zastosowań masowego przechwytywania w Wielkiej Brytanii jest wykrywanie ataków cybernetycznych, m.in. kradzieży danych, oszustw internetowych, wrogich operacji służb wywiadowczych innych państw i ugrupowań terrorystycznych. Wykorzystując informacje, które można porównać do elektronicznych odcisków palców (ang. *electronic signatures*), służby badają techniczne aspekty komunikacji internetowej w celu wykrycia elementów świadczących o możliwości dokonania ataku cybernetycznego wymierzonego w Wielką Brytanię. Tego rodzaju działania umożliwiają identyfikację złośliwego oprogramowania oraz wykrycie nowych, nieznanych wcześniej służbom, form cyberataków. Jeśli weźmie się pod uwagę tempo ewolucji technologicznej i skalę ilości danych funkcjonujących w cyberprzestrzeni, to instrument *bulk interception* jest jedną z niewielu skutecznych metod pozwalających na monitorowanie tego rodzaju ataków na wszystkich etapach, na co nie pozwala specyfika funkcjonowania instrumentów ukierunkowanych.

2. *Bulk equipment interference*

Pojęcie *bulk equimpent interference* (dalej: *bulk EI)* odnosi się do zbioru działań uprawnionych służb, których celem jest pozyskanie określonych informacji (np. treści komunikatów czy danych o urządzeniu) przez ingerencję w funkcjonowanie określonego urządzenia, np. komputera czy telefonu komórkowego. Te czynności mogą być prowadzone w sposób zdalny lub bezpośredni, np. przez fizyczne wpływanie na działalność danego urządzenia. Opisywane operacje mogą charakteryzować się różnym stopniem złożoności w zależności od zamierzonego celu czy poziomu zabezpieczeń urządzeń. Mniej skomplikowane działania mogą polegać np. na zgraniu określonych danych z urządzenia czy wykorzystaniu hasła lub loginu użytkownika w celu uzyskania dostępu do informacji zapisanych w pamięci urządzenia. Większy stopień złożoności wykazują działania polegające na wykorzystywaniu słabych punktów określonego oprogramowania służące przejęciu kontroli nad urządzeniem lub siecią, co umożliwia zdalne przekazywanie za ich pośrednictwem określonych informacji lub monitorowanie aktywności użytkownika[150]. W najbardziej powszechnym rozumieniu ten mechanizm można określić jako prowadzenie czynności o charakterze hakerskim przez służby specjalne[151].

Sposób funkcjonowania *bulk EI* i korzyści operacyjne dla służb specjalnych płynące z wykorzystywania tego sposobu – w kontekście zwalczania zagrożeń dla bezpieczeństwa narodowego oraz ewentualne naruszenia prawa do prywatności i innych dóbr prawnie chronionych – należy rozważać na płaszczyźnie coraz wyraźniej rysującego się w porządkach prawnych niektórych państw UE i NATO podziału na dwa typy mechanizmów pozyskiwania danych: masowych (*bulk*) oraz ukierunkowanych (*targeted*). Podczas gdy instrumenty ukierunkowane w dalszym ciągu mają kluczowe znaczenie z punktu widzenia reagowania na zagrożenia wpisujące się w sferę działalności służb specjalnych – z uwagi na to, że pozwalają one na zdobycie informacji o planach czy działaniach określo-

[150] *Equipment Interference – Draft Code of Practice*, Home Office, Autumn 2016, s. 8, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf [dostęp: 21 IX 2017].

[151] *Report of the Bulk Powers Review*…, s. 34.

nego, zidentyfikowanego już podmiotu – możliwości ich wykorzystania zawierają immanentne ograniczenia natury strukturalnej, które są spotęgowane bezprecedensowym rozwojem nowoczesnych technologii informatycznych czy telekomunikacyjnych.

Zobrazowanie przedstawionej powyżej tezy wymaga szczegółowych informacji dotyczących, z jednej strony, charakterystyki współczesnych zagrożeń bezpieczeństwa narodowego (cyberataki, terroryzm, zjawisko *foreign fighters* czy niezwykle trudny do zidentyfikowania i przerwania proces tzw. *homegrown radicalisation*[152]), z drugiej zaś – sposobu funkcjonowania i rozwiązań technologicznych wykorzystywanych przez nowoczesne środki komunikacji. Te czynniki sprawiają, że dogłębnej redefinicji muszą ulec również instrumenty wykorzystywane przez służby specjalne. W wielu sytuacjach tradycyjne, wysoce ukierunkowane i zindywidualizowane metody pozyskiwania informacji (źródła osobowe, obserwacja, kontrola operacyjna, sprawdzenia w bazach danych itd.) rozmijają się z rzeczywistymi potrzebami i charakterystyką działań stwarzających zagrożenie dla bezpieczeństwa narodowego. Przykładem jest sytuacja, w której w razie rozwijającego się zagrożenia o charakterze terrorystycznym, funkcjonariusze służb nie mogą zakładać, że osoby zaangażowane w realizację hipotetycznego ataku będą komunikować się wyłącznie przy użyciu określonego numeru telefonu czy komunikatora internetowego. Niemożliwe jest również poczynienie założenia, że dane uzyskane dzięki instrumentom ukierunkowanym będą zawierać wszystkie istotne informacje i że za ich pośrednictwem będzie możliwe całościowe odtworzenie zamierzonych działań. Ponadto profesjonalnie działające podmioty, zarówno państwowe (obce służby specjalne), jak i pozapaństwowe (grupy terrorystyczne), korzystają z zaszyfrowanych metod komunikacji, co uniemożliwia lub znacznie utrudnia proces zdobycia informacji mogących zapobiec eskalacji danego zagrożenia. Organy odpowiedzialne za ochronę bezpieczeństwa narodowego będą zatem dysponować coraz bardzie fragmentarycznymi informacjami, natura zaś samych zagrożeń i związanych z nimi podmiotów będzie coraz bardziej nieprzejrzysta. Próby przeciwdziałania opisanym powyżej trendom wymagają dostosowania zbioru instrumentów operacyjno-rozpoznawczych do zmieniających się warunków oraz stworzenia katalogu komplementarnych i wzajemnie oddziałujących środków pozwalających na pozyskiwanie informacji o zagrożeniach na różnych etapach ich rozwoju – zarówno w fazie ich powstawania, jak i w fazie eskalacji[153].

2.1. Podstawy prawne

Przepisy dotyczące sposobu i zasad wykorzystywania *bulk EI* zostały zawarte w rozdziale 3 części 6 IPA. Regulacje dotyczące tego instrumentu należy określić jako analogiczne w stosunku do mechanizmu *bulk interception*. Proces wydawania nakazu

[152] Pojęcie *homegrown radicalisation* odnosi się do procesu radykalizacji osób na stałe przebywających w państwach tzw. świata zachodniego. Takie osoby zaczęły prezentować radykalne, związane z ultrakonserwatywnymi odłamami islamu poglądy z uwagi na fakt obcowania z tego rodzaju ideologią np. w meczetach, szkołach czy przez różnego rodzaju źródła internetowe. Omawiany proces jest niezwykle trudny do wykrycia z uwagi na to, że te osoby pozornie nie stwarzają jasno zarysowanego zagrożenia z punktu widzenia służb – nie podejmowały działań charakterystycznych dla tzw. *foreign fighters*, nie wyjeżdżały do obozów szkoleniowych Państwa Islamskiego w Syrii czy Iraku, nie utrzymują kontaktów z zagranicznymi bojownikami itd. *Homegrown radicalisation* należy uznać za proces jednostkowy i osobniczy, rozwijający się w oderwaniu od ustalonych struktur, grup czy organizacji. Największą rolę odgrywają w nim indywidualne aspekty psychologiczne określonej osoby.

[153] *Equipment Interference – Draft Code of Practice*…, s. 30.

zastosowania *bulk EI* oraz ewentualnych modyfikacji nakazu został poddany systemowi podwójnego nadzoru (*double lock*) ze strony Sekretarza Stanu i Komisarza.

Zgodnie z sekcją 176 pod pojęciem nakazu zastosowania omawianego instrumentu (ang. *bulk equimpent interference warrant*) rozumie się nakaz wydany na podstawie rozdziału 3 części 6 IPA, autoryzujący lub nakazujący osobie, do której jest skierowany, przeprowadzenie działań polegających na ingerencji w funkcjonowanie jakiegokolwiek urządzenia w celu uzyskania treści komunikatów (ang. *communications*), danych o urządzeniu (ang. *equipment data*) lub jakichkolwiek innych informacji. Sekcja 176(c) wskazuje natomiast, że głównym celem nakazu powinno być pozyskiwanie informacji, jeżeli wykazują one powiązania zagraniczne[154]. Ten warunek sprawia, że niemożliwe jest prowadzenie czynności związanych z ingerencją w urządzenia informatyczne, jeżeli jej głównym celem miałoby być zdobywanie informacji dotyczących osób znajdujących się na terytorium Wysp Brytyjskich[155]. Pomimo wyraźnego zastrzeżenia, że *bulk EI* powinno koncentrować się na sferze zewnętrznej, ustawodawca nie wykluczył możliwości prowadzenia działań polegających na ingerencji w funkcjonowanie urządzeń w wymiarze wewnętrznym. Analiza materiału dotyczącego osób znajdujących się na terytorium Wysp Brytyjskich wymaga jednak odrębnego nakazu wydawanego zgodnie z zasadami *double lock*[156].

Definicja komunikacji zagranicznej (ang. *overseas-related communications*) oznacza, analogicznie jak w przypadku przepisów dotyczących masowego przechwytywania, komunikację wysyłaną lub odbieraną przez osoby znajdujące się poza terytorium Wielkiej Brytanii. Na zasadzie analogii – pojęcie *overseas-related information* oznacza informację o osobach znajdujących się poza terytorium tego kraju.

Zgodnie z sekcją 177 pojęcie danych o urządzeniu (*equipment data*) oznacza dane systemowe lub dane identyfikujące (ang. *identifying data*), które:

- są dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób),
- mogą być logicznie odłączone od reszty komunikatu,
- w razie odłączenia nie ujawniłyby niczego, co może w rozsądny sposób zostać uznane za mające znaczenie dla komunikatu, pomijając znaczenie wynikające z samej komunikacji lub jakichkolwiek danych dotyczących przesyłu komunikatu.

Dane o urządzeniu zostało w ustawie [sekcja 176 (3)] określone jako wykazujące powiązania zagraniczne (ang. *overseas-related equipment data*), jeżeli:

- stanowią część lub są połączone z komunikacją zagraniczną lub informacjami o osobach znajdujących się za granicą (*overseas-related information*);
- mogą pomóc w ustaleniu istnienia lub nieistnienia komunikacji zagranicznej lub informacji o osobach znajdujących się za granicą, lub w ich uzyskaniu;
- mogą pomóc w wypracowaniu metod pozwalających na uzyskanie komunikacji zagranicznej lub informacji o osobach znajdujących się za granicą.

[154] Sekcja 176 (c) – „(…) the main purpose of the warrant is to obtain one or more of the following –
i) overseas-related communications;
ii) overseas-related information;
iii) overseas-related equipment data".

[155] *Draft Equipment Interference Code of Practice*, Home Office, February 2017, s. 65, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593753/IP_Act_-_Draft_EI_code_of_practice_Feb2017_FINAL_WEB.pdf [dostęp: 7 VIII 2017].

[156] Tamże.

Nakaz musi zezwalać osobie, do której jest skierowany, uzyskanie komunikacji, danych o sprzęcie lub innych informacji, lub autoryzować dokonanie przez nią czynności, których nakaz dotyczy. Może również zezwalać lub zobowiązywać do selekcji materiału uzyskanego zgodnie z nakazem do dalszej analizy lub do ujawnienia tego materiału osobie, do której nakaz jest skierowany, lub osobie działającej w jej imieniu [sekcja 176 (4)].

2.2. Rodzaje *equipment interference* – najważniejsze różnice między tzw. nakazami ukierunkowanymi (ang. *targeted equimpent interference*) a nakazami *bulk equipment inteference*

Analogicznie jak w przypadku masowego przechwytywania, ustawa IPA wprowadza rozróżnienie między stosowaniem ingerencji w sprzęt w sposób ukierunkowany (*targeted*) oraz prowadzeniem tych czynności w sposób masowy (*bulk*). Ukierunkowana ingerencja w sprzęt jest regulowana w części 5 ustawy (*Equipment Interference*), podczas gdy podstawą prawną wariantu polegającego na prowadzeniu czynności związanych z masowa ingerencją w sprzęt (*bulk EI*) jest rozdział 3 części 6.

Nakazy *EI* w rozumieniu ustawy dzielą się na następujące typy[157]:

- ukierunkowany nakaz ingerencji w urządzenia (ang. *targeted equipment interference warrant*) [sekcja 99 (2)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na ingerencji w urządzenia w celu uzyskania komunikacji, danych o urządzeniu lub innych informacji. Zezwala on również na podjęcie wszelkich czynności niezbędnych dla wykonania nakazu;
- ukierunkowany nakaz analizy materiału (ang. *targeted examination warrant*) [sekcja 99 (9)] – autoryzuje podjęcie czynności polegających na selekcji materiału uzyskanego na podstawie *bulk EI* do analizy, niezależnie od sekcji 193 (4), zakazującej identyfikacji komunikacji lub informacji o charakterze prywatnym dotyczących osób znajdujących się na terytorium Wysp Brytyjskich. Tego rodzaju nakaz musi być uzyskany wtedy, gdy zebrany w powyższy sposób materiał ma zostać poddany dalszej analizie na podstawie kryteriów odnoszących się do osoby, co do której składający wniosek o wydanie nakazu wie, że w chwili wyboru materiału do analizy znajduje się na terytorium Wysp Brytyjskich;
- nakaz masowej ingerencji w sprzęt (ang. *bulk equipment interference warrant*) (sekcja 176) – nakaz, którego głównym celem jest uzyskanie zagranicznej komunikacji, danych o urządzeniu lub innych informacji. Autoryzuje on zdobycie treści zagranicznej komunikacji, danych o urządzeniu oraz innych informacji oraz wybór zebranego materiału do dalszej analizy.

Analogicznie jak w przypadku przechwytywania danych (ang. *interception*), ukierunkowaną ingerencję w sprzęt można zastosować wówczas, gdy właściwe organy mają dostateczną wiedzę pozwalającą na indywidualizację i stosunkowo dokładne określenie osób stwarzających potencjalne zagrożenie i wykorzystywanych przez nich urządzeń. Ingerencja o charakterze masowym ma z kolei zastosowanie, gdy zagrożenie ma charakter nieokreślony, jego zaś charakter i skala nie mogą być sprecyzowane przed wydaniem nakazu.

[157] Tamże, s. 22.

Nakaz ukierunkowany może zostać wydany, jeżeli organ wnioskujący jest w stanie w dostatecznie precyzyjny sposób określić skalę ingerencji w dane urządzenia, przy uwzględnieniu szacunkowej ilości informacji pobocznych, niemających związku z celem wydania nakazu, do których organ, prowadząc czynności, uzyska w sposób naturalny dostęp oraz dzięki czemu oceni proporcjonalność i niezbędność ingerencji. W tym wypadku nie są zatem konieczne dodatkowe ograniczenia i restrykcje stanowiące immanentną cechę reżimu regulującego sposób wykorzystywania masowych środków gromadzenia informacji. Jeżeli natomiast niemożliwe jest dokonanie oceny niezbędności, proporcjonalności i skali ingerencji w czasie wydawania nakazu lub jeżeli zastosowanie ingerencji ukierunkowanej byłoby w danym wypadku niepraktyczne lub niewystarczające, powinien zostać wydany nakaz typu „*bulk*", w ramach którego są przewidziane dodatkowe środki ochronne, np. wielostopniowe ograniczenia dostępu do pozyskanego materiału[158].

2.3. Proces wydawania nakazu *bulk equipment interference* (sekcja 176 i następne)

Elementy proceduralne związane z wydawaniem nakazu *bulk EI* zostały uregulowane na zasadzie analogicznej, jak w przypadku masowego przechwytywania. Do najważniejszych elementów należy zaliczyć dwuetapowy proces zatwierdzania nakazu przez Sekretarza Stanu i Komisarza (*double lock*) oraz wymóg wykazania proporcjonalności i niezbędności wydania nakazu w danym przypadku (sekcja 178). W ten sam sposób zostały uregulowane również przesłanki przedmiotowe warunkujące możliwość zastosowania tego instrumentu. Sekretarz Stanu może wydać nakaz, jeżeli w jego opinii jest to niezbędne w interesie bezpieczeństwa narodowego oraz w celu zapobiegania lub wykrywania poważnej przestępczości lub ochrony interesów ekonomicznych Wielkiej Brytanii i jeżeli te przesłanki mają związek z bezpieczeństwem narodowym. Przesłanka związana z ochroną interesów ekonomicznych może uzasadniać zastosowanie *bulk EI*, jeśli wydanie nakazu jest niezbędne dla pozyskania informacji dotyczących działań lub zamiarów osób znajdujących się poza terytorium Wysp Brytyjskich. Podobnie jak w przypadku masowego przechwytywania, obie pozostałe przesłanki (zwalczanie poważnej przestępczości i ochrona interesów ekonomicznych) muszą pozostawać w koniunkcji z przesłanką ochrony interesów bezpieczeństwa narodowego. Ten mechanizm należy uznać za jeden z wielu elementów wchodzących w skład katalogu środków ograniczających możliwość stosowania instrumentów masowego gromadzenia danych, zarówno masowego przechwytywania, jak i masowej ingerencji w urządzenia informatyczne, których celem jest ochrona prawa do prywatności i minimalizacja możliwości wyrządzenia szkody osobom, które nie stanowią zagrożenia dla bezpieczeństwa narodowego.

Sekretarz Stanu może wydać nakaz, jeżeli, w jego opinii, wskazane we wniosku o wydanie nakazu cele operacyjne uzasadniają analizę materiału zgromadzonego w czasie realizacji czynności autoryzowanych na podstawie nakazu oraz jeżeli sądzi on, że ta analiza jest niezbędna w związku z którymkolwiek z celów, z których powodu Sekretarz Stanu uważa, że wydanie nakazu jest w danym wypadku niezbędne [sekcja 178 (2)]. Przykładem jest następująca sytuacja – jeśli nakaz został wydany w związku z ochroną bezpieczeństwa narodowego oraz zapobiegania i zwalczania poważnej przestępczości, to wybór danych do dalszej analizy musi być niezbędny w kontekście jednej lub obu wymienionych przesłanek[159].

[158] *Draft Equimpent Interference Code of Practice*…, s. 36.
[159] Tamże, s. 69.

Po wydaniu nakazu przez Sekretarza Stanu Komisarz dokonuje wszechstronnej oceny zasadności wykorzystania *bulk EI* w konkretnej sytuacji. Bada on m.in. niezbędność, proporcjonalność oraz to, czy wskazane we wniosku cele operacyjne uzasadniają późniejszą analizę zebranego materiału (sekcja 179). W razie odmowy zatwierdzenia nakazu Komisarz informuje o tym na piśmie Sekretarza Stanu wraz z podaniem przyczyn uzasadniających odmowę.

Przepisy dotyczące kryteriów formalnych nakazu *bulk EI* zostały skonstruowane w sposób analogiczny, jak w przypadku masowego przechwytywania (patrz wyżej).

2.4. Nakazy *bulk EI* wydawane w trybie pilnym

Mając na uwadze specyfikę zagrożeń cybernetycznych i dynamikę ewentualnych wrogich działań prowadzonych z wykorzystaniem narzędzi informatycznych, ustawodawca przewidział wyjątek od zasady *double lock*. Zgodnie z sekcją 180 Sekretarz Stanu może wydać nakaz zastosowania *bulk EI,* jeżeli w jego opinii zachodzi nagła potrzeba wykorzystania tego instrumentu. Jest on zobowiązany do poinformowania o tym Komisarza.

Ocena, czy w danym przypadku rzeczywiście zachodzi konieczność zastosowania trybu pilnego, musi uwzględnić, czy uzyskanie zgody Komisarza – biorąc pod uwagę okoliczności sprawy i konieczność realizacji określonych celów operacyjnych – byłoby praktycznie możliwe i rozsądne. Co do zasady, nakazy wydawane w trybie pilnym powinny wiązać się z co najmniej jedną z poniższych przesłanek:

- bezpośrednim zagrożeniem dla życia lub zdrowia (np. jeżeli występuje bezpośrednie zagrożenie atakiem terrorystycznym, który może być powstrzymany lub którego skutki mogą zostać zminimalizowane dzięki zastosowaniu *bulk EI*),
- ograniczoną czasowo możliwością użycia masowej ingerencji w urządzenia informatyczne w celu wykorzystania okazji pozyskania informacji wywiadowczych lub mogących mieć istotne znaczenie w toku ewentualnego śledztwa (np. sytuacja, w której służby dysponują wiedzą, że grupa o charakterze terrorystycznym działa w określonym rejonie geograficznym, ale zamierza wkrótce przemieścić się w inne miejsce)[160];

Komisarz podejmuje decyzję o utrzymaniu nakazu w mocy w terminie trzech dni roboczych od czasu wydania nakazu oraz zawiadamia o jej treści Sekretarza Stanu. Nakaz przestaje obowiązywać i nie może zostać przedłużony, jeżeli Komisarz odmówi utrzymania nakazu w mocy.

W razie odmowy utrzymania nakazu w mocy osoby realizujące czynności pierwotnie autoryzowane w trybie nagłym przez Sekretarza Stanu są zobowiązane do zaprzestania, tak szybko jak to możliwe, wszelkich czynności związanych z ingerencją w urządzenia informatyczne. W celu zniwelowania negatywnych skutków tych działań Komisarz może wyrazić zgodę na dalszą ingerencję po to, aby osoba realizująca powyższe czynności była w stanie zapewnić, że wszelkie działania związane z pierwotnym nakazem ustały tak szybko, jak to możliwe. Może on również nakazać zniszczenie materiałów uzyskanych w trakcie realizacji czynności lub określić warunki dotyczące ewentualnego użycia lub retencji tego materiału.

[160] Tamże, s. 71.

Ustawa przyznaje Sekretarzowi Stanu możliwość odwołania się od negatywnej decyzji Komisarza do Investigatory Powers Commissioner[161] – organu mogącego utrzymać decyzję Komisarza lub mogącego wydać samoistną decyzję w tej sprawie [sekcja 181 (7)].

Uchylenie nakazu wydanego w trybie pilnym nie pociąga za sobą bezprawności czynności dokonanych w okresie między wydaniem nakazu przez Sekretarza Stanu a jego ewentualnym uchyleniem [sekcja 181 (8)].

Najważniejsze przepisy dotyczące czasu trwania nakazu, jego ewentualnego przedłużenia lub modyfikacji zostały skonstruowane w sposób analogiczny do regulacji dotyczących masowego przechwytywania. Istotną różnicą jest krótszy ustawowy czas trwania nakazu wydanego w trybie pilnym – wynosi on pięć dni roboczych licząc od dnia, w którym nakaz został wydany [sekcja 184 (2) (a)].

2.5. Aspekty praktyczne i rola *bulk EI* w działalności służb specjalnych

Pozyskiwanie danych dzięki zastosowaniu *bulk EI* może być instrumentem pozwalającym organom odpowiedzialnym za ochronę bezpieczeństwa narodowego na przezwyciężenie zagrożeń związanych z ich zmniejszającą się zdolnością skutecznego reagowania na zagrożenia. Może to być spowodowane coraz wyższym poziomem zabezpieczeń technologicznych i szyfrowania urządzeń końcowych (ang. *end-to-end*), stosowanych w narzędziach komunikacji w celu zwiększenia poziomu bezpieczeństwa i prywatności użytkowników. Były dyrektor Federalnego Biura Śledczego (FBI) James Comey określił ten problem jako „*going dark*"[162]. To zjawisko jest jednym z aspektów poruszanych w ramach toczącej się w wielu krajach UE i NATO debaty publicznej, dotyczącej konieczności określenia nowych paradygmatów w zakresie wzajemnych relacji między sposobem wykorzystywania nowoczesnych instrumentów komunikacji a potrzebą wyposażenia właściwych organów w instrumenty dostosowane do nowych uwarunkowań i pozwalające na rzeczywistą realizację zadań przez te organy.

Obserwowany na przestrzeni ostatnich lat bezprecedensowy rozwój technologiczny wywiera w istocie dwojakiego rodzaju wpływ na proces zwalczania przestępczości i innych zagrożeń bezpieczeństwa. Z jednej strony organy realizujące czynności o charakterze operacyjno-rozpoznawczym czy dochodzeniowo-śledczym mogą, dzięki badaniu poszczególnych aspektów wykorzystywania nowoczesnych metod komunikacji, teoretycznie uzyskać dostęp do rozbudowanego katalogu informacji, które pozwalają na wykrywanie ewentualnych zagrożeń. Z drugiej zaś strony – tempo ewolucji nowych technologii sprawia, że stałe i systematyczne dostosowywanie do nich instrumentów, wykorzystywanych przez wspomniane organy, jest niemożliwe. W konsekwencji może dojść do sytuacji, w której z powodu np. zaawansowanych metod szyfrowania informacji wykorzystywanych przez niektóre komunikatory internetowe dostęp organów o charakterze policyjnym czy innych służb do niezbędnych im informacji, mimo zgodności tych działań z powszechnie obowiązującymi przepisami prawa, będzie niewykonalny

[161] Investigatory Powers Commissioner, zgodnie z sekcją 229, prowadzi nadzór nad wykonywaniem przez inne organy publiczne w ich ustawowych zadań w zakresie przechwytywania komunikacji, pozyskiwania lub retencji danych telekomunikacyjnych, pozyskiwania danych wtórnych lub danych systemowych zgodnie z rozdziałem 1 cześci 2 lub rozdziałem 1 części 6 IPA oraz nad prowadzeniem czynności związanych z ingerencją w urządzenia informatyczne (ang. *equipment interference*).

[162] J.B. Comey, *Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?* Director, Federal Bureau of Investigation, Brookings Institution, Washington, D.C. October 16, 2014, www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [dostęp: 8 VIII 2017].

z technicznego punktu widzenia. Szyfrowanie jest jedynie jednym z aspektów problemu *going dark*, stanowi ono jednak główny element opisanej powyżej debaty z uwagi na to, że w wielu wypadkach pociąga za sobą fizyczne wyłączenie możliwości uzyskania przez podmiot publiczny dostępu do informacji, który przysługuje mu na mocy odpowiednich aktów normatywnych bądź indywidualnego aktu kompetentnego organu (np. sądu), autoryzującego tego rodzaju dostęp[163].

Niektóre z przedsiębiorstw informatycznych wskazują również na to, że nie dysponują możliwościami technicznymi, które umożliwiają uzyskanie dostępu do informacji zgromadzonych w pamięci urządzeń. Ten problem pojawił się w kontekście prowadzenia przez FBI czynności mających na celu wyjaśnienie okoliczności i zebranie materiału dowodowego w sprawie zdarzeń w San Bernardino (Kalifornia) z 2 grudnia 2015 r. W ich wyniku śmierć poniosło 14 osób, a 22 zostały ranne.[164] Departament Sprawiedliwości zamierzał, na podstawie nakazu wydanego przez sąd, uzyskać informacje mogące mieć istotne znaczenie dla toczącego się śledztwa przez uzyskanie dostępu do danych zgromadzonych w pamięci urządzenia iPhone należącego do jednego ze sprawców ataku. Nakaz zobowiązywał przedsiębiorstwo Apple do dezaktywacji właściwości technicznej urządzenia, polegającej na automatycznym usuwaniu wszystkich zgromadzonych w nim danych po 10 nieudanych próbach wpisania hasła dostępu. W ten sposób byłoby możliwe obejście zabezpieczeń urządzenia przez próby wpisania określonej liczby kombinacji haseł, bez ryzyka usunięcia danych mających istotne znaczenie dla śledztwa. Przedstawiciele Apple argumentowali, że parametry techniczne i oprogramowanie telefonu sprawiają, że nie są oni w stanie odblokować urządzenia ani wyłączyć funkcji automatycznie usuwającej dane po nieudanych próbach wpisania hasła. Taką możliwość ma wyłącznie użytkownik lub osoba znająca oryginalne hasło[165].

Spór pomiędzy Apple a FBI i Departamentem Sprawiedliwości pokazuje, jak dalece możliwości organów odpowiadających za zwalczanie przestępczości i zagwarantowanie bezpieczeństwa są ograniczone w konfrontacji z osobami korzystającymi z nowoczesnych metod komunikacji. Przedstawiciele FBI wskazywali, że zaszyfrowane dane znajdujące się w pamięci telefonu jednego ze sprawców ataku, Syeda Rizwana Farooka, oraz zbiór koordynatów GPS wskazujących lokalizacje, w których przebywał on przed dokonaniem ataku, mogą zawierać niezwykle istotne informacje dotyczące kontaktów Farooka i jego żony, Tashfeen Malik, z osobami należącymi do Państwa Islamskiego[166].

Pojawiające się w kontekście sprawy San Bernardino interdyscyplinarne problemy prawne i technologiczne wskazują, że zjawisko *going dark* ma niezwykle istotne znaczenie w zwalczaniu terroryzmu. Niemożność uzyskania dostępu do danych przesyłanych za pośrednictwem środków komunikacji elektronicznej lub znajdujących się w pamięci urządzeń w wielu wypadkach może całkowicie uniemożliwić podejmowanie skutecznych działań zapobiegawczych w tej sferze lub odbywających się na późniejszym etapie czynności śledczych. Naturę problemu ilustrują zacytowane w przywoły-

[163] K. Finklea, *Encryption and the „Going Dark" Debate*, July 20, 2016, www.fas.org/sgp/crs/misc/R44481.pdf [dostęp: 8 VIII 2017].

[164] www.edition.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html [dostęp: 8 VIII 2017].

[165] www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.f0ff02bab120 [dostęp: 8 VIII 2017].

[166] www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html [dostęp: 8 VIII 2017]. Także: www.washingtonpost.com/news/post-nation/wp/2015/12/08/both-san-bernardino-attackers-pledged-allegiance-to-the-islamic-state-officlals-say/?utm_term=.093527772da99 [dostęp: 8 VIII 2017].

wanym wcześniej raporcie Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego (*A Question of Trust – Report of the Investigatory Powers Review*) słowa dyrektora Europolu, który stwierdził, że szyfrowanie jest (…) *największym problemem dla policji i służb bezpieczeństwa w sprawach dotyczących zwalczania terroryzmu* (…) *Zmieniło ono samą naturę działań antyterrorystycznych – w przeszłości czynności te opierały się na skutecznym monitorowaniu komunikacji, podczas gdy obecnie nie jest to już możliwe*[167].

Specyfika funkcjonowania instrumentu *bulk EI* sprawia, że jest on w stanie zneutralizować jedno z najważniejszych obecnie wyzwań, z jakim mierzą się służby specjalne i organy o charakterze policyjnym w większości państw UE i NATO. Tym wyzwaniem jest brak technicznych możliwości uzyskania dostępu do zaszyfrowanych informacji zgromadzonych w pamięci urządzeń lub przesyłanych za pomocą środków komunikacji elektronicznej, mimo że tego rodzaju czynności są zgodne z prawem i mieszczą się w katalogu ustawowych kompetencji tych podmiotów. Zaprezentowane poniżej przykłady[168] hipotetycznych sytuacji, w których jest możliwe wykorzystanie *bulk EI*, wskazują, że potencjalne zastosowania tego instrumentu mają charakter komplementarny i mogą obejmować szerokie spektrum zagrożeń bezpieczeństwa.

Przykład nr 1. Przeciwdziałanie i zapobieganie terroryzmowi

Służby wywiadowcze z powodzeniem zastosowały ukierunkowaną ingerencję w urządzenia telekomunikacyjne wykorzystywane przez członków ugrupowania o charakterze terrorystycznym, przebywających w bazie treningowej poza granicami Wielkiej Brytanii. Zgromadziły tym samym informacje o planowanym przez grupę ataku na pochodzących z państw zachodnich turystów w jednym z głównych miast tego samego państwa, w którym była zlokalizowana baza treningowa, nie wiedziały jednak, kiedy atak ma zostać dokonany. Następnie grupa zaprzestała jakiegokolwiek wykorzystywania urządzeń, wobec których zastosowano *bulk EI*, co prawdopodobnie było spowodowane nabyciem nowych urządzeń i rozpoczęciem przygotowań do przeprowadzenia ataku. Służby nie miały również informacji o tym, jakiego typu urządzenia są obecnie wykorzystywane przez ugrupowanie. Biorąc pod uwagę okoliczności sprawy i realne zagrożenie zamachem terrorystycznym, zastosowano masową ingerencję w celu pozyskania informacji za pośrednictwem wszystkich lub znacznej części urządzeń znajdujących się w docelowym mieście, co miało doprowadzić do zidentyfikowania nowych urządzeń członków grupy. Jeżeli urządzenia te zostaną zidentyfikowane dostatecznie szybko, będzie możliwe zapobieżenie potencjalnemu zamachowi.

Przytoczony przykład w jasny sposób charakteryzuje możliwości związane z poprawnym wykorzystaniem *bulk EI*. Hipotetyczna sytuacja, w której zakłada się stosowanie ukierunkowanej ingerencji w sprzęt znajdujący się w posiadaniu zidentyfikowanej grupy przebywającej poza granicami Wielkiej Brytanii oraz nietypowe przejście od techniki ukierunkowanej do masowej, warunkowane dynamiką sytuacji, pokazuje, że zastosowany instrument może być skutecznie wykorzystany w szybko zmieniającej się sytuacji operacyjnej, charakteryzującej się dużą ilością zmiennych parametrów. Należy zwrócić uwagę, że przewidziany w ustawie IPA ogólny podział technik pozyskiwania informacji na ukierunkowane i masowe trzeba traktować jako

[167] *A Question of Trust*, s. 194-195.

[168] Przykłady te znajdują się dokumencie *Operational Case for Bulk Powers*, s. 35–36, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents [dostęp: 8 VIII 2017].

zestaw komplementarnych instrumentów wykorzystywanych w różnych fazach działań operacyjno-rozpoznawczych, nie zaś jako zbiór niezależnych od siebie i całkowicie odrębnych instrumentów. Te zależności dowodzą również, że nowoczesny system gromadzenia informacji za pomocą narzędzi informatycznych będzie wykazywał się odpowiednią skutecznością, jeżeli wchodzące w jego skład komponenty będą wykazywać niezbędny stopień wewnętrznej harmonii i zgodności. Stosowanie technik wyłącznie masowych lub wyłącznie ukierunkowanych spowoduje, że możliwe będzie ich łatwe obejście, chociażby przez regularne zmiany wykorzystywanych telefonów, laptopów czy innych urządzeń. Brytyjski system – zarówno w odniesieniu do *equimpent interference*, jak i *interception* – pozwala na dynamiczną zmianę stosowania poszczególnych technik zdobywania informacji na różnych etapach danej sytuacji operacyjnej.

Przykład nr 2. Przeciwdziałanie proliferacji broni masowego rażenia

Hipotetyczne państwo o ustroju totalitarnym ma własny system poczty elektronicznej wykorzystywany przez część jego obywateli, w tym przez naukowców zaangażowanych w program rozwoju broni biologicznej i w rozprzestrzenianie technologii wojskowej. Liczba użytkowników systemu jest liczona w tysiącach. Służby wywiadowcze innych państw, w celu zdobycia wiarygodnych informacji o ewentualnym zagrożeniu proliferacją broni biologicznej, są w stanie zdobyć jedynie fragmentaryczne informacje pochodzące z innych źródeł wywiadowczych (np. z przechwytywania komunikacji), co oznacza, że niemożliwe jest zidentyfikowanie indywidualnych kont poczty internetowej należących do osób zaangażowanych w rozwój programu. Technika masowej ingerencji w sprzęt może w tym wypadku pozwolić na zdobycie ograniczonej liczby informacji o większej liczbie lub o wszystkich użytkownikach systemu, pozwalającej na określenie osób, w stosunku do których będzie konieczne prowadzenie dalszych działań wywiadowczych przez wykorzystanie ukierunkowanych technik pozyskiwania informacji.

Sytuacja opisana w przykładzie nr 2 akcentuje kilka niezmiernie istotnych aspektów sposobu działania *bulk EI*. Po pierwsze, w przeciwieństwie do sytuacji opisanej w przykładzie nr 1 ilustruje ona typowy dla tego rodzaju operacji przebieg konwersji techniki masowej w ukierunkowaną. Po identyfikacji, którzy z użytkowników systemu poczty elektronicznej mogą być zaangażowani w prace nad programem rozwoju broni masowego rażenia, będzie możliwe skoncentrowanie działań wywiadowczych wyłącznie na tych osobach i wykorzystywanych przez nich urządzeniach. Po drugie – ten casus pokazuje, że identyfikacja konkretnych osób spośród dużej liczby użytkowników danego systemu (w tym wypadku poczty elektronicznej) wymaga uzyskania dostępu do niewielkiej ilości danych o dużej liczbie urządzeń i ich użytkowników. Ten proces – pomimo że jego zakres podmiotowy (użytkownicy i urządzenia) jest szeroki, jego zasięg przedmiotowy (ilość i charakter informacji, do których należy uzyskać dostęp) jest spłycony i powierzchowny – dotyczy bardzo ograniczonego katalogu danych. Po trzecie – omawiana technika jest skuteczna w stosunku do zamkniętych i hermetycznych środowisk operacyjnych (jak np. krąg osób zaangażowanych w program proliferacji broni masowego rażenia w państwie totalitarnym), w odniesieniu do których inne metody wywiadowcze nie mogłyby przynieść spodziewanego rezultatu.

Przykład nr 3. Cyberbezpieczeństwo

Kontrolowany przez inne państwo podmiot zapewnia infrastrukturę (komputery, oprogramowanie i inne elementy) dla analogicznych do *bulk EI* programów, wymierzonych w organy rządowe i podmioty gospodarcze Wielkiej Brytanii. Brytyjskie organy wywiadowcze dążą do identyfikacji tego podmiotu w celu ustalenia, jakie konkretnie urządzenia czy oprogramowanie dostarcza on użytkownikom. Aby to osiągnąć, służby mogą posłużyć się masową ingerencją w urządzenia w celu monitorowania miejsca, z którego prawdopodobnie jest dostarczany zmanipulowany sprzęt. Zadaniem służb jest odkrycie charakterystycznych parametrów działalności dostawców. Wykrycie osób zaangażowanych w tego rodzaju działania będzie wymagać zgromadzenia dużych ilości danych pozwalających na ich identyfikację, co umożliwi późniejsze zastosowanie ukierunkowanych technik pozyskiwania informacji.

Zapobieganie i przeciwdziałanie atakom cybernetycznym jest jedną z podstawowych funkcji masowej ingerencji w urządzenia. Powyższy przykład opisuje sytuację, w której stan zaawansowania rozwoju sytuacji stwarzającej zagrożenie dla bezpieczeństwa narodowego jest wysoki (podmioty dostarczające sprzęt i oprogramowanie prowadzą już zakrojone na szeroką skalę działania), poziom wiedzy służb jest natomiast stosunkowo niski. Posiadają one informację o samym istnieniu zagrożenia i jego skutkach, a także ograniczoną wiedzę dotyczącą metod wykorzystywanych w toku tego procesu, nie są jednak w stanie dokładnie określić jego sprawców. *Bulk EI* może w tym wypadku przyczynić się do neutralizacji zagrożenia przez monitorowanie sposobu wykorzystywania urządzeń teleinformatycznych we wskazanej w przykładzie lokalizacji, będącej prawdopodobnie głównym miejscem działań grupy. Wykrycie osób zaangażowanych w opisane działania wymaga jednak ingerencji we wszystkie urządzenia znajdujące się w tym obiekcie. Na podstawie informacji podanych w przykładzie można założyć, że jest to prawdopodobnie miejsce dystrybucji sprzętu informatycznego. Złośliwe oprogramowanie będzie zatem zainstalowane nie we wszystkich urządzeniach dystrybuowanych za jego pośrednictwem, lecz w wybranych elementach, które następnie trafią do brytyjskich podmiotów będących przedmiotem zainteresowania obcych służb. Określenie, w których urządzeniach to oprogramowanie zostało faktycznie zainstalowane, wymaga więc ingerencji we wszystkie przedmioty sprzedawane bądź udostępniane przez ten punkt.

Neutralizacja zagrożenia będzie wymagać analizy dużej ilości bardziej szczegółowych niż w przykładzie nr 2 danych. Tamta sytuacja zakładała jedynie identyfikację określonych użytkowników systemu, tutaj zaś wykrycie złośliwego oprogramowania znajdującego się w urządzeniach dostarczanych przez opisany powyżej podmiot będzie prawdopodobnie wymagać bardziej zaawansowanych i dogłębnych czynności. W tej sytuacji, podobnie jak w przykładzie nr 2, zakłada się również przejście od zastosowanej początkowo techniki masowej do techniki ukierunkowanej na identyfikację osób zaangażowanych w wymierzone przeciwko brytyjskim podmiotom działania. Należy zwrócić uwagę na to, że przydatność *bulk EI* wynika w tym przypadku z potencjalnie wysokiej skuteczności tego mechanizmu w sytuacjach dynamicznych, w których uwarunkowania operacyjne podlegają częstym fluktuacjom. Niemożliwe jest bowiem stworzenie wyczerpującej listy podmiotów, do których trafił zainfekowany sprzęt informatyczny lub złośliwe oprogramowanie. Niemożliwe jest również, bez dokładnej znajomości sposobu działania tego oprogramowania, precyzyjne oszacowanie szkód, na jakie są narażone brytyjskie podmioty, i określenia, jakie informacje, trafiły do obcych służb

w wyniku tego rodzaju operacji. Przewaga masowej ingerencji w sprzęt nad innymi, tradycyjnymi technikami zdobywania informacji przejawia się również w szybkości działania tego mechanizmu. Ewentualne zdobycie osobowego źródła wśród pracowników podmiotu prowadzącego wrogą działalność byłoby procesem czasochłonnym i obarczonym wysokim stopniem ryzyka. Tak jak w pozostałych przykładach, zaletami *bulk EI* jest duża elastyczność tego mechanizmu oraz to, że stwarza on możliwość dotarcia do informacji nieosiągalnych innymi metodami.

2.6. Wnioski

Wyróżniającą cechą tzw. *bulk powers* na tle innych metod pozyskiwania informacji wykorzystywanych przez służby bezpieczeństwa i ochrony porządku publicznego jest umożliwienie im zdobywania dużych ilości danych przesyłanych za pośrednictwem Internetu oraz środków komunikacji elektronicznej, w celu wykrycia zagrożeń bezpieczeństwa narodowego. Większość zdobytych w ten sposób informacji nie dotyczy osób mogących stwarzać realne zagrożenie, jednak sposób wykorzystywania tych instrumentów, ograniczenia natury technologicznej i prawnej (ograniczenia dostępu, opisane w poprzednich częściach procesy selekcji informacji) oraz konieczność skupienia działań służb na informacjach mogących mieć istotne znaczenie wywiadowcze prowadzi do wniosku, że stworzony w Wielkiej Brytanii system *bulk powers* jest rozwiązaniem optymalnym z punktu widzenia konieczności przeciwdziałania i zwalczania nowych rodzajów zagrożeń bezpieczeństwa narodowego.

Przywoływane w niniejszym opracowaniu raporty brytyjskiego Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego („*Bulk Powers Review*" oraz „*A Question of Trust*") słusznie wskazują, że na podstawie orzecznictwa Europejskiego Trybunału Praw Człowieka nie sposób uznać, że samo wykorzystywanie instrumentów masowego zdobywania danych, przy założeniu, że spełnia ono określone warunki (m.in. istnienie odpowiedniego systemu nadzoru, ograniczenia dostępu do zdobytych informacji) jest nieproporcjonalne i niedające się uzasadnić w demokratycznym społeczeństwie naruszeniem prawa do prywatności. W wydanym w sprawie Weber vs. Germany[169] orzeczeniu Europejski Trybunał Praw Człowieka uznał, że instrument tzw. strategicznego monitorowania komunikacji (ang. *strategic monitoring*) analizowany w toku postępowania, występujący w prawie niemieckim, nie stanowi *per se* nieproporcjonalnego naruszenia prawa do prywatności z uwagi na to, że ten środek może być wykorzystywany w ściśle określonych przypadkach, mechanizmy zabezpieczające prawo do prywatności i ograniczenia proceduralne są zaś wystarczające dla zagwarantowania przestrzegania praw obywatelskich.

Podobną linię orzeczniczą ETPCz przyjął w sprawie Liberty and others vs. the United Kingdom[170], że przepisy brytyjskiej ustawy *The Interception of Communications Act* z 1985 r., podlegające wykładni Trybunału, nie precyzowały w sposób wystarczająco jasny zakresu i sposobu korzystania z przyznanych właściwym organom kompetencji do przechwytywania i analizowania komunikacji zewnętrznej (gdy adresat, nadawca lub obydwoje znajdują się za granicą). Organy brytyjskie nie udostępniły opinii publicznej informacji o tym, w jaki sposób jest dokonywana selekcja przechwyconych informacji

[169] European Couurt of Human Rights, Decision as to the admissibility of application no. 54394/00 by Gabriele Weber and Cesar Richard Saravia v. Germany, 29 June 2006.

[170] European Court of Human Rights, Case of Liberty and others v. the United Kingdom, application no. 58243/00, Judgment, Strasbourg, 1 July 2008.

do dalszej analizy ani o zasadach dalszego udostępniania, przechowywania czy niszczenia przechwyconego materiału. Pomimo wskazania wad poszczególnych przepisów prawa brytyjskiego Trybunał nie wykazał systemowej niezgodności instrumentów masowego pozyskiwania danych z przepisami *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Należy zatem zgodzić się z postawioną w raporcie *A Question of Trust* tezą, że instrumenty typu „*bulk*" nie są same w sobie nieproporcjonalnym naruszeniem prawa do prywatności, niemniej jednak, z uwagi na ich charakter i inwazyjność, muszą podlegać ocenie według bardziej rygorystycznych standardów, niż ma to miejsce w przypadku instrumentów ukierunkowanych, dotyczących konkretnie wskazanej osoby fizycznej.

Porównując przepisy ustawy *Investigatory Powers Act* z instrumentami o charakterze operacyjno-rozpoznawczym, wymienionymi w *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[171] oraz w *Ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[172] należy wskazać, że polski porządek prawny nie zawiera uregulowań zezwalających służbom specjalnym na wykorzystywanie instrumentów typu „*bulk*", pozwalających na masowe zdobywanie danych w celu rozpoznawania, zapobiegania i zwalczania zagrożeń bezpieczeństwa państwa. Charakter uprawnień Agencji Bezpieczeństwa Wewnętrznego w zakresie rozpoznawania zagrożeń w systemach i sieciach informatycznych należy określić jako defensywny i zorientowany w głównej mierze na zabezpieczenie przed atakami informatycznymi systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa[173].

Tego rodzaju sposób ustawowego uregulowania zakresu kompetencji ABW i pozostających w jej dyspozycji instrumentów, służących realizacji zadań opisanych w art. 5 ustawy, wynika częściowo z ustrojowej roli tej instytucji, polegającej na łącznym wykonywaniu zadań zarówno w sferze informacyjnej (uprawnienia operacyjno-rozpoznawcze), jak i w sferze procesowej (uprawnienia dochodzeniowo-śledcze). Najbardziej charakterystycznym przykładem wskazanej powyżej dychotomii jest sposób, w jaki zostało uregulowane w ustawie o ABW oraz AW zagadnienie kontroli operacyjnej. Zgodnie z art. 27 tej ustawy sąd, na pisemny wniosek szefa ABW, złożony po uzyskaniu pisemnej zgody prokuratora generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez ABW w celu rozpoznawania, zapobiegania i wykrywania określonych przestępstw (m.in. szpiegostwa, terroryzmu oraz przestępstw w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeni strategicznym dla bezpieczeństwa państwa). Kontrola operacyjna pozwala na prowadzenie stosunkowo szerokiego katalogu czynności, m.in. uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 27 ust. 6 pkt 4).

Po pierwsze, należy wskazać, że kontrola operacyjna jest instrumentem ściśle związanym ze sferą zwalczania przestępczości, nie zaś ze sferą informacyjną sprowadzającą się do wykrywania zagrożeń bezpieczeństwa państwa. Analiza przepisu art. 27 ustawy prowadzi do wniosku, że w przeciwieństwie do środków pozyskiwania informacji wprowadzonych na podstawie *Investigatory Powers Act* w Wielkiej Brytanii, za-

[171] T.j.: Dz.U. z 2016 poz. 1897 – przyp. red.
[172] Dz.U. z 2016 r. poz. 904 – przyp. red.
[173] Art. 5 pkt 2a ustawy o ABW oraz AW.

równo masowych, jak i ukierunkowanych, kontrola operacyjna nie może być uznana za środek prospektywny, służący wykrywaniu zagrożeń bezpieczeństwa narodowego na wczesnym etapie ich rozwoju. Przeciwnie, konstrukcja art. 27 ustawy powoduje, że jego zastosowanie jest możliwe na późniejszym etapie. Świadczy o tym chociażby katalog informacji, które powinien zawierać wniosek o zastosowanie kontroli operacyjnej – opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej czy dane osoby lub inne dane pozwalające na jednoznacznie określenie podmiotu lub przedmiotu, wobec którego będzie stosowana kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania (art. 27 ust. 7). Te elementy sprawiają, że kontrola operacyjna może mieć zastosowanie wówczas, gdy ABW ma informacje umożliwiające dokonanie stosunkowo dokładnej rekonstrukcji działań osób, w stosunku do których ma być prowadzona kontrola operacyjna, nie zaś np. na pozyskanie informacji o samym procesie powstawania nowych zagrożeń, co umożliwia chociażby instrument *equipment interference*.

Po drugie, kontrola operacyjna w myśl ustawy o ABW jest środkiem wyłącznie ukierunkowanym, o wysokim stopniu indywidualizacji. Świadczy o tym zawarte w art. 27 ust. 7 pkt 4 ustawy sformułowanie (…) *dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie stosowana kontrola operacyjna*. Porównanie *equipment interference* z uzyskiwaniem i utrwalaniem danych w myśl art. 27 ust. 6 pkt 4 prowadzi do wniosku, że ustawa o ABW nie zezwala na prowadzenie czynności polegających na ingerencji w urządzenia informatyczne, jeżeli w danej sytuacji nie jest możliwe jednoznaczne określenie osoby lub osób prowadzących działania, o których mowa w przywołanym artykule czy podanie kwalifikacji prawnej przestępstwa. Niemożliwe zatem na gruncie aktualnie obowiązujących przepisów byłoby zdobywanie informacji o zagrożeniach za pośrednictwem urządzeń i sieci informatycznych w przypadku, w którym ABW posiadałaby fragmentaryczne informacje o zagrożeniu niepozwalające na dokładne określenie zaangażowanych w nie osób.

Przeanalizowanie powyższych elementów prowadzi do wniosku, że w przeciwieństwie do systemu brytyjskiego, zorientowanego na prowadzenie działań służących wykrywaniu zagrożeń na wczesnym etapie ich powstawania z wykorzystaniem instrumentów informatycznych, kontrola operacyjna – w myśl ustawy o ABW oraz AW – jest instrumentem zbliżonym raczej do sfery czynności procesowych niż działań wywiadowczych służących wykrywaniu zagrożeń bezpieczeństwa państwa. Nie podważając niezbędności istnienia tego rodzaju instrumentu, należy zwrócić uwagę na to, że w porównaniu z analogicznymi regulacjami funkcjonującymi w Wielkiej Brytanii w polskim systemie prawnym brakuje przepisów upoważniających właściwe podmioty do prowadzenia czynności typu „*bulk interception*" czy „*bulk equipment interferencje*", umożliwiających wczesne wykrywanie zagrożeń i podejmowanie odpowiednich działań zapobiegawczych. Pomimo że wykorzystywanie instrumentów masowego pozyskiwania informacji jest poważną ingerencją w prawa i wolności gwarantowane na mocy zarówno prawa międzynarodowego, jak i krajowego, samo ich istnienie nie może być uznane za sprzeczne z zasadami demokratycznego państwa prawnego. Wpływ tego rodzaju sposobów działania służb na prawo do prywatności należy rozpatrywać przez pryzmat mechanizmów zabezpieczających, pozwalających na gromadzenie i analizę tylko tych informacji, które mogą mieć istotne znaczenie z punktu widzenia bezpieczeństwa narodowego oraz dostatecznej precyzji i jasności przepisów normujących sposób i zakres ich praktycznego wykorzystywania.

Przyjęcie w Wielkiej Brytanii ustawy IPA należy rozpatrywać w dwóch kontekstach. Po pierwsze – jako próbę stworzenia rozwiązań legislacyjnych umożliwiających skuteczną realizację jednej z podstawowych funkcji państwa – zagwarantowania prawa do bezpieczeństwa. Po drugie, pomimo że ten akt wprowadza instrumenty pozwalające na daleko idącą ingerencję w prawo do prywatności, zawarte w ustawie szczegółowe przepisy dotyczące sposobu i trybu ich wykorzystywania przyczyniają się do zwiększenia pewności prawa i ograniczenia pojawiających się – chociażby w kontekście sprawy ujawnienia dokumentów NSA przez Edwarda Snowdena – wątpliwości dotyczących realnego zakresu kompetencji służb specjalnych i dopuszczalnego przez prawo stopnia ich ingerencji w prawa i wolności obywatelskie. Biorąc pod uwagę występujące w niektórych państwach UE i NATO (np. w Wielkiej Brytanii czy Francji) kierunki zmian legislacyjnych dotyczących katalogu instrumentów wykorzystywanych przez służby wywiadowcze oraz służby odpowiedzialne za ochronę bezpieczeństwa wewnętrznego państwa, można wyraźnie zaobserwować coraz większą liczbę aktów normatywnych wprowadzających instrumenty pozwalające na pozyskiwanie informacji za pośrednictwem systemów i sieci teleinformatycznych.

Pomimo że Polska nie jest priorytetowym celem działań międzynarodowych grup terrorystycznych, utrzymujące się na wysokim poziomie w większości państw Europy Zachodniej zagrożenie terrorystyczne oraz istotna zmiana paradygmatów bezpieczeństwa państw Unii Europejskiej i NATO, związana m.in. z coraz bardziej agresywnymi działaniami Federacji Rosyjskiej w sferze międzynarodowej, skłaniają do refleksji nad kształtem ustawowego uregulowania zakresu kompetencji i uprawnień polskich służb specjalnych. Katalog instrumentów operacyjno-rozpoznawczych przewidzianych w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu był tworzony z myślą o zwalczaniu rozumianych tradycyjnie zagrożeń bezpieczeństwa państwa, takich jak szpiegostwo, terroryzm (istniejący w ówczesnej postaci) oraz działalność zorganizowanych grup przestępczych o zasięgu międzynarodowym. Nieznane były wówczas zjawiska typu: zagrożenia hybrydowe, ataki terrorystyczne dokonywane w Europie przez *foreign fighters* czy przez osoby przechodzące proces tzw. *homegrown radicalisation*, a także wielowymiarowe zagrożenia związane z nasilonym w ostatnich latach procesem migracji. Mniejsze znaczenie miało również wykorzystywanie zaszyfrowanych środków komunikacji elektronicznej i Internetu.

Nawet pobieżna analiza wzorców ataków terrorystycznych dokonywanych w państwach Europy Zachodniej na przestrzeni lat 2015–2017 prowadzi do wniosku, że utrzymujące się na wysokim poziomie bezpieczeństwo Polski jest odpowiednim momentem na zainicjowanie procesu dostosowywania sposobu działania polskich służb specjalnych do nowych zagrożeń. Opisane w artykule wzorce brytyjskie mogą być punktem odniesienia dla pokazania perspektywy organów legislacyjnych państwa niejednokrotnie dotkniętego w przeszłości zjawiskiem terroryzmu.

Michał Kamiński
Michał Ordyniak

Charakterystyka najważniejszych problemów związanych z ochroną danych osobowych w kontekście realizacji ustawowych zadań służb specjalnych

1. Ochrona danych osobowych w służbach specjalnych w ramach polskiego systemu prawnego

W kontekście konstytucyjnych praw i wolności jednostki ochrona danych osobowych jest nierozerwalnie związana z prawem do prywatności, autonomii informacyjnej oraz wolności komunikowania się.

Tematem niniejszego artykułu nie jest jednak ochrona danych osobowych sama w sobie, tylko relacje tejże materii wobec zadań realizowanych przez służby odpowiedzialne za bezpieczeństwo państwa, przede wszystkim w kontekście zapewniania bezpieczeństwa, które może się przejawiać jako bezpieczeństwo wewnętrzne, zewnętrzne oraz publiczne. Ujęcie tej problematyki w kontekście służb, w tym służb specjalnych, skupia jak w soczewce podstawowe zagadnienie dotyczące konkurencji dwóch konstytucyjnych wartości, jakimi są prawa i wolności obywatelskie oraz bezpieczeństwo państwa. Wynika to z konieczności ograniczania w niektórych sytuacjach tychże konstytucyjnych praw jednostki z uwagi na ochronę bezpieczeństwa państwowego.

Sprawą najważniejszą jest odpowiednie ważenie obu tych wartości i wprowadzanie niezbędnych ograniczeń w taki sposób, aby żadna z nich nie utraciła swego podstawowego znaczenia. Sam Trybunał Konstytucyjny podkreślił, że (…) *graniczenie praw jednostki jest możliwe w sytuacji konfliktu dwóch wartości, z jednej strony ochrony konstytucyjnej wolności lub prawa jednostki, ochrony bezpieczeństwa lub porządku publicznego, ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób z drugiej strony* (wyrok z 29 stycznia 2002 r., sygn. K 19/01). Jednocześnie Trybunał podkreślił wagę zasady proporcjonalności, która winna być punktem wyjścia przy stosowaniu tego typu ograniczeń. W orzeczeniu z 26 kwietnia 1995 r., sygn. K 11/94, stwierdził, że (…) *dla oceny, czy doszło do naruszenia zasady zakazu nadmiernej ingerencji konieczne jest zbadanie, czy wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków, czy jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana oraz czy efekty wprowadzanej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela, bowiem ustawodawca konstytucyjny szczególny nacisk położył na kryterium konieczności*. To stwierdzenie zostało później potwierdzone przez Trybunał, m.in. w wyrokach z 11 kwietnia 2000 r. (sygn. K 15/98) czy z 23 listopada 2009 r. (sygn. K 61/08), w których podkreślił, że proporcjonalność jest składową trzech zasad: zasady przydatności, zasady konieczności oraz zasady proporcjonalności sensu stricto, tzn. zakazu nadmiernej ingerencji.

Celem niniejszych rozważań, nie jest wskazywanie, której z tych wartości należy nadać przymiot pierwszeństwa. Ważniejszą sprawą jest znalezienie tzw. złotego środka, sposobu na realizowanie zarówno jednej, jak i drugiej wartości przez wprowadzanie

niezbędnych ograniczeń na gruncie ustawy. Rzeczą niezbędną jest dokonanie właściwej oceny zadań i uprawnień służb na tle poszanowania i ochrony przez władze publiczne praw i wolności jednostki. Należy pamiętać, że nadanie którejkolwiek z tych konstytucyjnych wartości prymatu może spowodować, iż albo prawa i wolności obywatelskie będą nagminnie łamane, albo organy państwa nie będą mogły skutecznie stać na straży bezpieczeństwa państwa.

Samo zagadnienie bezpieczeństwa można porównać do państwa jako tarczy, której personifikacją są powołane i należycie zadaniowane służby, w tym służby specjalne. Rolą ustawodawcy, ale także Trybunału Konstytucyjnego, jest określenie ram realizowania w tym wymiarze zadań przy uwzględnieniu ochrony praw i wolności jednostki. Jednak przy opracowywaniu właściwych rozwiązań nie można zapominać o stanowisku instytucji pro-wolnościowych, których zadaniem jest wskazywanie zagrożeń wynikających z uprawnień nadanych służbom przez ustawodawcę lub przydzielonych zadań. Należy podkreślić, że wyłącznie przez współdziałanie wszystkich tych podmiotów będzie możliwe wypracowanie stosownych rozwiązań.

Sam Trybunał Konstytucyjny w wyroku z 30 lipca 2015 r. (sygn. K 23/11) wskazał, że:

> (…) ciążący na organach państwa obowiązek zagwarantowania wolności i praw oznacza nie tylko zakaz nadmiernej ingerencji, w tym polegającej na niejawnym pozyskiwaniu przez organy państwa informacji o osobach, ale ma szerszy wymiar. Wynika z niego obowiązek stworzenia przez państwo warunków, w których obywatele z zagwarantowanych im wolności i praw mogą swobodnie korzystać. Warunkiem zapewnienia wolności i praw jest zaś poczucie bezpieczeństwa w państwie i braku zagrożeń obywateli. Osiągnięcie tego stanu możliwe jest m.in. poprzez zwalczanie przestępczości mogącej zagrażać wolności człowieka, korzystanie z własności czy podejmowanie działalności gospodarczej. Z drugiej strony, korelatem konstytucyjnego obowiązku państwa, o którym mowa w art. 5 Konstytucji RP, jest także prawo obywateli do ochrony ich bezpieczeństwa przed zewnętrznymi i wewnętrznymi zagrożeniami, w tym terroryzmem i przestępczością.

W tym samym wyroku Trybunał uznał, że:

> (…) choć czynności operacyjno-rozpoznawcze popadają w konflikt z prawem do ochrony prywatności, wolnością i ochroną tajemnicy komunikowania się czy autonomią informacyjną, mogą być uznane za konieczne w demokratycznym państwie prawa z uwagi na ochronę bezpieczeństwa państwa, porządku publicznego bądź ochronę wolności i praw innych osób.

Tym samym Trybunał wskazał na zależność istniejącą pomiędzy tymi dwiema wartościami, którą skrótowo można określić jako: bezpieczne państwo to bezpieczny obywatel.

Efektem tych rozważań, zarówno w opracowywaniu wniosków krótkofalowych, jak i długofalowych, powinna być świadomość istnienia tych dwóch – w sumie przeciwstawnych – konstytucyjnych wartości obok siebie, a co za tym idzie – konieczność ich stałego ważenia w celu znalezienia najwłaściwszego rozwiązania.

Jak już zwrócono uwagę na wstępie, celem niniejszych rozważań jest ochrona danych osobowych w odniesieniu do działalności służb, w tym służb specjalnych. Dlatego też w dalszej części ta problematyka będzie rozwijana.

W pierwszej kolejności należy zwrócić uwagę, że tę sprawę można interpretować w dwojaki sposób. W ujęciu wąskim pod pojęciem ochrona danych osobowych będziemy rozumieli wyłącznie problem ochrony i przetwarzania tego typu danych zgromadzonych przez poszczególne służby specjalne, bez odnoszenia się do sposobu i trybu ich uzyskiwania. Zastosowanie w tym zakresie będą miały przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Z drugiej strony przedmiot rozważań można rozpatrywać w znaczeniu szerokim, w którego ramach będzie konieczne odniesienie się do właściwości danej służby, jej zadań, a także formy realizacji tych zadań, podczas realizacji których może pojawić się problem dostępu do danych osobowych.

Najważniejsze znaczenie dla wąskiego spojrzenia na ochronę danych osobowych przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego ma wspomniana ustawa o ochronie danych osobowych, która zawiera przepisy ogólne i podstawowe odnoszące się do omawianej kwestii. W art. 3 jest mowa o zakresie stosowania tej ustawy przez organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne. Kolejne istotne przepisy to art. 40 oraz 43. Zgodnie z pierwszym z nich administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Drugi przywołany artykuł zawiera wykaz zbiorów informacji, których zgłoszenie do GIODO jest wyłączone spod tego obowiązku. Przykładowo należy wskazać dane zawierające informacje niejawne (ust. 1 pkt 1), dane które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do wykonywania tych czynności (ust. 1 pkt 1a), przetwarzane przez właściwe organy na potrzeby postępowania sądowego (ust. 1 pkt 2) czy też np. dane przetwarzane przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (ust. 1 pkt 2c), które są najistotniejsze z punktu widzenia ABW.

Należy w tym miejscu zwrócić uwagę, że w 2010 r. te ogólne regulacje zostały uzupełnione o lex specialis regulujący omawiane zagadnienie w kontekście funkcjonowania jednej ze służb, tj. Centralnego Biura Antykorupcyjnego. Przepisy, o których mowa, są zawarte w art. 22b ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, który wprowadza nową instytucję – pełnomocnika do spraw kontroli przetwarzania w CBA danych osobowych. Trzeba nadmienić, że w przepisach prawa powszechnego nie ma wyraźnie wyodrębnionych trybów postępowania z informacjami stanowiącymi dane osobowe, właściwych tylko dla tej grupy informacji i tak rozbudowanego od strony formalnej systemu ochrony, jak ma to miejsce w odniesieniu do CBA. W okresie sprawowania rządów przez sejm poprzedniej kadencji trwały prace legislacyjne mające na celu wprowadzenie tego rodzaju instytucji w Agencji Bezpieczeństwa Wewnętrznego. Jednakże w związku z tym, że zostały one wstrzymane, należy przyjąć, iż w odniesieniu do ABW wyznacznikiem są tylko przepisy ustawy o ochronie danych osobowych. Na tej podstawie prawnej zbudowano w Agencji system zabezpieczania informacji zawierających dane osobowe, który opiera się na aktach prawnych o charakterze wewnętrznym, wydanych przez szefa ABW. Te przepisy w pełni uwzględniają dyrektywy wynikające z art. 36 ustawy o ochronie danych osobowych przez to, że zapewniają zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, przywłaszczeniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Trzeba wskazać, że dane osobowe są jedynie jednym z elementów informacji przetwarzanych w ABW. W większości są to informacje niejawne, w tym dane zdobyte

w wyniku czynności operacyjno-rozpoznawczych i podczas przeprowadzania czynności śledczych, związane z realizacją zadań, o których mowa w art. 5 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W ich ramach mogą być zbierane m.in. dane osobowe. Ochrona tego rodzaju informacji jest jednym z obowiązków ABW wyrażonym w art. 35 ust. 1 tej ustawy, zgodnie z którym ABW w związku z wykonywaniem swoich zadań zapewnia ochronę środków, form i metod służących ich realizacji, a także zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy Agencji. Należy również mieć na względzie przepisy ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Zgodnie z art. 11 tej ustawy szef ABW pełni funkcję krajowej władzy bezpieczeństwa. Z tego powodu systemy ochrony danych i informacji w Agencji muszą spełniać najwyższe standardy bezpieczeństwa, a zatem zbiory, w których zawarte są m.in. dane osobowe, są chronione na najwyższym poziomie. Dane osobowe uzyskane w ten sposób są jedynie elementem innych informacji przetwarzanych w ABW, które w większości są informacjami niejawnymi. Do ochrony tego rodzaju informacji zostały zastosowane środki o najwyższym możliwym poziomie bezpieczeństwa. Z powyższego wynika, że system ochrony informacji niejawnych w ABW obejmuje również ochronę danych osobowych. Należy również stwierdzić, że ten system spełnia wymogi wynikające z ustawy o ochronie danych osobowych oraz z ustawy o ochronie informacji niejawnych. Ponadto charakter danych przetwarzanych w ABW uzasadnia podstawę do odstąpienia od obowiązku zgłaszania prowadzonych zbiorów informacji GIODO i jednocześnie ją stanowi. Na marginesie trzeba dodać, że w ABW nie został powołany administrator bezpieczeństwa informacji, o którym mowa w art. 36a ustawy o ochronie danych osobowych, gdyż ten przepis ma charakter fakultatywny, a w przypadku ABW te zadania szef Agencji realizuje za pośrednictwem struktury wewnętrznej ABW, a obowiązki dla poszczególnych jednostek organizacyjnych określa w aktach prawa wewnętrznego. Zadania w tym zakresie są zatem skorelowane z wymogami dotyczącymi bezpieczeństwa innych informacji, w tym zwłaszcza informacji niejawnych.

Wspomniane akty prawne dotyczą informacji niejawnych i z tego względu nie mogą być przedstawione szczegółowe rozwiązania. W ramach wspomnianego systemu zapewniono:

- mechanizm ewidencjonowania baz danych z jednoczesnym określeniem zakresu gromadzonych w nich informacji i sposobu ich pozyskiwania, wynikający m.in. z zarządzenia nr Pf-15 szefa ABW z 28 marca 2013 r. w sprawie ewidencji operacyjnej i innych zbiorów informacji w Agencji Bezpieczeństwa Wewnętrznego. Ta regulacja koreluje z normą wynikającą z art. 40 ustawy o ochronie danych osobowych;
- system ochrony danych osobowych, który jest skorelowany z pozostałymi systemami bezpieczeństwa działającymi w ABW. Przykładowo można wskazać zarządzenie nr Z-46 szefa ABW z 9 grudnia 2014 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych i jawnych w Agencji Bezpieczeństwa Wewnętrznego;
- system kontroli wewnętrznej, który odnosi się do wszelkich spraw związanych z bezpieczeństwem i przetwarzaniem informacji zawartych zarówno w bazach danych ABW, jak i w bazach danych innych uprawnionych podmiotów, do których dostęp mają funkcjonariusze Agencji. Te zadania są realizowane jako jeden z obowiązków jednostki organizacyjnej uprawnionej do prowadzenia kontroli oraz audytu wewnętrznego.

Mając na uwadze powyższe, a także zakres i sposób pozyskiwania informacji przez poszczególne służby specjalne, należy stwierdzić, że kwestie związane z ochroną danych osobowych muszą, oprócz respektowania wcześniej wskazanych konstytucyjnych praw i wolności obywatelskich, uznawać dyrektywy dotyczące bezpieczeństwa państwa oraz konieczność zapewniania bezpieczeństwa jego obywatelom, wynikające również z Konstytucji RP. Trzeba też wywnioskować, że nie można zbudować jednolitego, wspólnego systemu ochrony danych osobowych dla wszystkich służb i organów państwowych. Dostrzegł to również sam ustawodawca, robiąc wyjątek od obowiązku zgłaszania pewnych zbiorów informacji GIODO. W pełni uzasadnione jest twierdzenie, że zasady ochrony danych osobowych poszczególnych służb powinny być ściśle powiązane z zadaniami i zakresem informacji, które są gromadzone przez te służby. Jak się wydaje, taką właśnie okoliczność miał na uwadze również sam ustawodawca podczas uchwalania ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i ustawy o Centralnym Biurze Antykorupcyjnym. Ustawa o ochronie danych osobowych została uchwalona w 1997 r., pozostałe zaś, wymienione wyżej, w 2002 i 2010 r. (art. 22b ustawy o Centralnym Biurze Antykorupcyjnym). W przypadku, gdyby celem ustawodawcy było ustanowienie takiego systemu ochrony danych osobowych, który byłby wspólny dla wszystkich podmiotów państwowych, nie zawierałby on żadnych wyłączeń w przepisach, zwłaszcza takich, jakie dotyczą art. 43 ustawy o ochronie danych osobowych. Ten przepis bez wątpienia odnosi się do służb odpowiedzialnych za jedną z najważniejszych funkcji państwa, jakim jest zapewnianie bezpieczeństwa, w tym bezpieczeństwa obywateli. Ponadto przy uchwalaniu art. 22b ustawy o Centralnym Biurze Antykorupcyjnym również nie doszło do nowelizacji ustaw pozostałych służb pod kątem uwzględnienia w nich wspomnianego wcześniej pełnomocnika ochrony informacji niejawnych.

Na zakończenie problematyki dotyczącej ochrony danych osobowych należałoby zasygnalizować inne, szerokie spojrzenie na ten temat. Jak wspomniano na wstępie, państwo, realizując obowiązki gwaranta bezpieczeństwa własnego i własnych obywateli, pełni funkcję swoistej tarczy przed zagrożeniami. Uprawnienia odnoszące się do przeciwdziałania zagrożeniom muszą być wyrażone w formie przepisów prawnych odpowiedniego poziomu. Konieczne przy tym jest, aby te przepisy były skorelowane z zadaniami nałożonymi na daną służbę, a także aby nie ingerowały w kompetencje innych podmiotów. Tylko w taki sposób zbudowany system prawny pozwoli na sprawną i skuteczną realizację zadań ustawowych oraz będzie odpowiadał zasadzie legalizmu wynikającej z art. 7 Konstytucji RP.

W tym miejscu trzeba wspomnieć o roli ABW w procesie legislacyjnym. Jak wiadomo inicjatywa ustawodawcza przysługuje posłom, senatowi, Prezydentowi RP, Radzie Ministrów oraz grupie obywateli. W tym zakresie ABW może pełnić jedynie funkcję konsultacyjną. W przypadku, gdy rządowy projekt aktu prawnego dotyczy zadań, uprawnień bądź też w inny sposób odnosi się do działalności ABW, jest on zgodnie z § 35 ust. 3 uchwały nr 190 Rady Ministrów z 29 października 2013 r. – Regulamin pracy Rady Ministrów, przekazywany szefowi ABW do konsultacji. W przypadku zaś, gdy dany projekt ustawy jest na etapie prac parlamentarnych, ABW ma uprawnienie jedynie do wyrażenia opinii na temat projektowanych rozwiązań w trakcie prac nad stanowiskiem rządu opracowywanym wobec pozarządowego projektu ustawy. Ponadto należy zauważyć, że sprawy związane z bezpieczeństwem państwa należą do właściwości Rady Ministrów. Dlatego też podjęcie decyzji o nałożeniu zadań na daną służbę należy do tego właśnie podmiotu, na który ABW praktycznie nie ma żadnego wpływu. Nie może być

bowiem mowy o „samozadaniowaniu się" służb, tylko o wykonywaniu poleceń organów, którym są podległe. Opinie ABW mogą dotyczyć zwłaszcza przepisów określających uprawnienia danej służby, ich skuteczności bądź nieprzydatności w odniesieniu do zadań, które mają być wykonywane.

2. System ochrony danych osobowych w Unii Europejskiej z perspektywy służb specjalnych

2.1. Obecny stan prawny

Omawiając kwestie związane z ochroną danych osobowych, należy zaznaczyć, że kształt polskiego ustawodawstwa w tym zakresie jest w znacznej mierze determinowany przepisami prawa Unii Europejskiej.

Jako najistotniejsze akty prawa regulujące materię związaną z ochroną danych należy wymienić:

- *Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz.Urz. UE L z 1995 r. nr 281, s. 31)
- oraz *Decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 roku w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych* (Dz.Urz. UE L z 2008 r. Nr 350, s. 60).

2.1.1. Dyrektywa 95/46/WE

Celem dyrektywy 95/46/WE było zapewnienie harmonizacji przepisów o ochronie danych osobowych na terenie Wspólnoty Europejskiej wobec zaobserwowania tego, że różnica w stopniu ochrony praw i wolności jednostek w odniesieniu do prawa do prywatności może uniemożliwiać przesyłanie tych danych pomiędzy państwami członkowskimi, utrudniając realizację wielu przedsięwzięć ekonomicznych i zakłócając tym samym funkcjonowanie Wspólnego Rynku[1]. W motywach preambuły znajdują się również odniesienia do aktów prawa międzynarodowego regulujących ochronę prawa do prywatności – artykułu 8 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności[2] oraz Konwencji Rady Europy z 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych[3], jako wyznacznika ram standardów ochrony tego typu danych obowiązujących na terenie Europy, które twórcy wzięli pod uwagę, jednak bez wskazania, że realizacja praw jednostki zapisanych w tych przepisach jest celem wydania dyrektywy. O uchwaleniu omawianej dyrektywy zadecydowały zatem głównie przesłanki ekonomiczne, zgodnie z podstawowym celem Wspólnoty Europejskiej, jakim było ustanowienie i zapewnienie funkcjonowania wspólnego rynku. Motyw 13 preambuły omawianej dyrektywy stanowi, że działania określone w tytułach V i VI (wspólna polityka zagraniczna i bezpieczeństwa oraz współpraca w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych) Traktatu o Unii Europejskiej (dalej: TUE) dotyczące bezpieczeństwa

[1] Motyw 7 preambuły.
[2] Motyw 10 preambuły.
[3] Motyw 11 preambuły.

publicznego, obronności i bezpieczeństwa państwa w dziedzinie prawa karnego nie wchodzą w zakres stosowania prawa wspólnotowego. Również przetwarzanie danych osobowych konieczne do zapewnienia ochrony dobrego stanu gospodarczego państwa nie wchodzi w zakres stosowania niniejszej dyrektywy, o ile takie przetwarzanie dotyczy spraw odnoszących się do bezpieczeństwa państwa. Podobny zapis został zawarty w art. 3 omawianej dyrektywy, określającym zakres jej obowiązywania. Zgodnie z ust. 2 wskazanego artykułu:

> 2. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:
> – w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności w obszarach prawa karnego,
> – przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze.

Warto jednak zauważyć, że wskazane wyłączenie odsyła do traktatu o Unii Europejskiej w wersji sprzed wejścia w życie traktatu lizbońskiego[4]. Obecny Tytuł VI TUE nie reguluje już zagadnienia współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, która to dziedzina, stanowiąca dawny trzeci filar Unii Europejskiej, stała się jedną z rodzajów polityki Unii Europejskiej (Przestrzeń wolności, bezpieczeństwa i sprawiedliwości), objętych zakresem jej kompetencji (w tym wypadku są to kompetencje dzielone między Unię Europejską i państwa członkowskie, stosownie do art. 4 ust. 2 lit. j traktatu o funkcjonowaniu Unii Europejskiej), co może budzić wątpliwości odnośnie do aktualności tego wyłączenia. Jak pisze Agnieszka Grzelak w pracy *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*:

> Wskazanie, iż wyłączona z zakresu zastosowania dyrektywy jest działalność wykraczająca „poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI TUE", straciło w chwili obecnej znaczenie o tyle, że obecnie Unia Europejska zastąpiła Wspólnoty Europejskie, a TUE nie reguluje już kwestii związanych ze współpracą policyjną i sądową w sprawach karnych. Można by było zadać pytanie, czy zatem dyrektywa 95/46 w obecnym stanie prawnym nie reguluje już kwestii związanych z omawianym obszarem, jednak przepis art. 3 ust. 2 tiret pierwsze dyrektywy zawiera dodatkowe wskazanie, stwierdzając, że dyrektywa nie ma zastosowania „w żadnym razie" do działalności na rzecz bezpieczeństwa publicznego czy też działalności państwa w obszarach prawa karnego. Nie ma zatem wątpliwości, że wejście w życie TL nie zmieniło zakresu zastosowania dyrektywy 95/46 (…)[5].

Przepisy omawianej dyrektywy nie odnoszą się zatem w dalszym ciągu do przetwarzania danych osobowych zarówno przez organa ścigania, jak i służby specjalne.

---

[4] Traktat z Lizbony zmieniający traktat o Unii Europejskiej i traktat ustanawiający Wspólnotę Europejską (Dz. Urz. UE C z 2007 r. nr 306, s. 1, ze zm.) wszedł w życie 1 grudnia 2009 r.

[5] A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015, s. 196–197.

Transpozycja dyrektywy 95/46/WE do polskiego porządku prawnego nastąpiła w przepisach ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.

2.1.2. Decyzja ramowa Rady 2008/977/WSiSW

Decyzja ramowa Rady 2008/977/WSiSW została wydana jako instrument III filaru Unii Europejskiej. Powodem jej wydania było ustanowienie wspólnych norm przetwarzania i ochrony danych osobowych w celu zapobiegania i zwalczania przestępczości z zamiarem poprawy współpracy policyjnej i sądowej w sprawach karnych pod kątem jej skuteczności i legalności oraz zgodności z prawami podstawowymi, w szczególności z prawem do prywatności i do ochrony danych osobowych[6].

Celem powyższej decyzji, zgodnie z jej art. 1 ust. 1, jest zapewnienie wysokiego poziomu ochrony praw podstawowych i wolności osób fizycznych, a zwłaszcza ich prawa do prywatności, podczas przetwarzania danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Decyzja ramowa ma stosunkowo wąski zakres regulacji, ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych między państwami członkowskimi Unii Europejskiej w ramach współpracy policyjnej i sądowej w sprawach karnych. Ponadto jej art. 1 ust. 4 stanowi, że *Niniejsza decyzja ramowa nie narusza podstawowych interesów bezpieczeństwa narodowego i określonych działań wywiadowczych w zakresie bezpieczeństwa narodowego*. Nie będzie więc nadużyciem stwierdzenie, że obowiązujące w chwili obecnej przepisy prawa Unii Europejskiej tylko w niewielkim stopniu regulują ochronę danych osobowych przetwarzanych przez organy ścigania, przetwarzanie danych przez organy wywiadowcze (służby specjalne) zaś jest w zasadzie wyłączone z ich regulacji.

Decyzja ramowa nakazuje poddanie przetwarzania danych osobowych przez właściwe organy zasadom legalności, proporcjonalności i celowości (art. 3), nakazuje także korygowanie danych nieścisłych, usuwanie lub anonimizowanie danych, których dalsze przetwarzanie nie jest już potrzebne (art. 4), wprowadza ograniczenia w zakresie przetwarzania kategorii danych szczególnie wrażliwych (art. 6) oraz wprowadza zasadę, zgodnie z którą transfer danych osobowych jest dokonywany wyłącznie do tych krajów trzecich, które zapewniają odpowiedni poziom ochrony (art. 13). Decyzja ramowa nakazuje, aby państwa członkowskie zapewniły podstawowe prawa podmiotu danych: prawo do informacji o gromadzeniu lub przetwarzaniu danych osobowych oraz ich udostępnieniu (art. 16–17), prawo do uzyskania korekty danych, ich usunięcia lub zablokowania do nich dostępu (art. 18), prawo do odszkodowania, w przypadku poniesienia szkody na skutek niezgodnej z prawem operacji przetwarzania danych (art. 19) oraz możliwość skorzystania ze środków odwoławczych (art. 20). Jednocześnie państwa członkowskie uzyskały uprawnienie w zakresie ograniczania wykonywania przez podmiot danych prawa do informacji, jeśli takie ograniczenie stanowiłoby skuteczny i proporcjonalny środek pozwalający na uniknięcie przeszkód w prowadzonych postępowaniach, pozwalałoby uniknąć niekorzystnego wpływu na zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie oraz wykonywanie sankcji karnych, jeśli służyłoby ochronie bezpieczeństwa publicznego, bezpieczeństwa narodowego oraz ochronie osoby, której dotyczą dane, a także praw i wolności innych osób

[6] Tak stanowi motyw 3 preambuły decyzji ramowej Rady 2008/977/WSiSW.

(art. 17 ust. 2). Zgodnie z art. 17 ust. 3 każda odmowa lub ograniczenie dostępu powinno zostać przedstawione na piśmie osobie, której dane dotyczą, wraz z pouczeniem o możliwości wniesienia odwołania.

Decyzja ramowa została zaimplementowana do prawa polskiego w przepisach ustawy z 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz.U. z 2011 r. nr 230 poz. 1371, ze zm.). Ta ustawa wdrożyła jeszcze trzy inne instrumenty z zakresu trzeciego filaru Unii Europejskiej, a mianowicie:

- decyzję Rady 2008/615/WSiSW z 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości zorganizowanej (Dz. Urz. UE L z 2008 r. nr 210, s. 1),
- decyzję Rady 2007/845/WSiSW z 6 grudnia 2007 r. dotyczącą współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem (Dz. Urz. UE L z 2007 r. nr 332, s. 103),
- decyzję ramową Rady 2006/960/WSiSW z 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami państw członkowskich Unii Europejskiej (Dz. Urz.UE L z 2006 r. nr 386, s. 89 oraz z 2007 r. nr 75 poz. 36).

Zgodnie z art. 1 ust. 1 ustawy implementującej: *Ustawa określa zasady i warunki wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej w celu wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości i jej zwalczania oraz przetwarzania informacji, a także podmioty uprawnione w tych sprawach*. Ochrona danych osobowych nie została zatem nawet wymieniona wśród głównych celów ustawy. Natomiast wśród podmiotów uprawnionych do wymiany informacji (na jej podstawie) z organami ścigania państw członkowskich Unii Europejskiej w celu wykrywania i ścigania przestępstw lub przestępstw skarbowych, zapobiegania przestępczości i jej zwalczania oraz przetwarzania informacji przepis art. 1 ust. 2 ustawy wymienia: Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Policję, Krajową Administrację Skarbową[7], Straż Graniczną i Żandarmerię Wojskową. Objęcie zakresem niniejszej ustawy Agencji Bezpieczeństwa Wewnętrznego jest związane z przyznaniem jej roli punktu kontaktowego do wymiany informacji, w tym danych osobowych, służących zapobieganiu przestępstwom terrorystycznym, co uczyniono w jej art. 32, dodającym ustęp 3 do artykułu 5 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Obowiązek ustanowienia przez każde państwo członkowskie Unii Europejskiej takiego punktu kontaktowego został przewidziany w art. 16 ust. 3 Decyzji Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości zorganizowanej, której wdrożeniu do polskiego porządku prawnego służy również omawiana ustawa.

Ochrony danych osobowych dotyczy rozdział 4 omawianej ustawy. Przepisy tego rozdziału nakazują podmiotom uprawnionym dokonanie weryfikacji prawidłowości, aktualności i kompletności danych osobowych przekazywanych organom ścigania państw członkowskich Unii Europejskiej (art. 19), przechowywanie danych osobowych wyłącznie przez okres niezbędny do realizacji celu, w jakim zostały przekazane (art. 20), respektowanie ograniczeń dotyczących czasu przechowywania danych nałożonych przez organy ścigania państw członkowskich Unii Europejskiej (art. 21) i sposobu ich przetwarzania (art. 22)

[7] W pierwotnej wersji ustawy na liście właściwych organów w miejscu KAS znajdowały się: Służba Celna oraz organy kontroli skarbowej.

oraz dokumentowania przekazania lub udostępnienia albo otrzymania danych osobowych (art. 23). Określono warunki dopuszczalności przetwarzania danych osobowych otrzymanych od organu ścigania państwa członkowskiego Unii Europejskiej bez zgody tego organu (art. 24 ust. 1) i przetwarzania tych danych przez inne podmioty (art. 24 ust. 2). Wymiana informacji została poddana kontroli Generalnego Inspektora Ochrony Danych Osobowych (art. 25).

2.2. Reforma europejskiego systemu ochrony danych osobowych

Pod koniec pierwszej dekady XXI w. w prawie pierwotnym Unii Europejskiej zaszły zmiany, które otworzyły drogę wielkiej reformie europejskiego systemu ochrony danych osobowych. Mowa tu o przyjęciu traktatu z Lizbony oraz Karty Praw Podstawowych Unii Europejskiej.

Karta praw podstawowych Unii Europejskiej z 12 grudnia 2007 r. (Dz. Urz. UE C z 2007 r. nr 303 s. 1 oraz z 2010 r. nr 81 s. 9)[8] zawiera artykuł 8 przyznający każdemu mieszkańcowi Unii Europejskiej prawo do ochrony dotyczących go danych osobowych. Ustęp 3 wskazanego artykułu stanowi, iż *Dane te muszą przetwarzane być rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą i prawo do dokonania ich sprostowania*. Sformułowane zostają zatem zasady rzetelności, celowości i legalności przetwarzania danych osobowych oraz prawa podmiotu danych: dostępu do dotyczących go danych i prawo do sprostowania. Ustęp 3 art. 8 stanowi, iż przestrzeganie tych zasad podlega kontroli niezależnego organu.

Jednocześnie w traktacie o funkcjonowaniu Unii Europejskiej, w brzmieniu określonym traktatem z Lizbony znalazł się artykuł 16, również regulujący kwestię ochrony danych osobowych. W ustępie 1 powtarza on zasadę wynikającą już z Karty Praw Podstawowych, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Natomiast ustęp 2 zawiera upoważnienie dla Parlamentu Europejskiego i Rady do określenia zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie zasad ochrony danych osobowych ma podlegać kontroli niezależnych organów. Uregulowanie tych kwestii przez Parlament Europejski i Radę ma nastąpić w ramach zwykłej procedury prawodawczej.

W wyniku wejścia w życie traktatu z Lizbony wraz z Kartą Praw Podstawowych Unia Europejska zyskała samoistną podstawę do uregulowania swoimi przepisami ochrony danych osobowych na swoim obszarze. Jest to zmiana rewolucyjna. Dotychczas obowiązująca dyrektywa 95/46/WE została wydana w celu ochrony wspólnego rynku, w wyniku konstatacji, że zróżnicowanie przepisów o ochronie danych osobowych na terenie Unii Europejskiej zaburza jego funkcjonowanie. Obecnie organy Unii Europejskiej są upoważnione do prawnego uregulowania tej kwestii i nie muszą zasadniczo ograniczać się w swoim podejściu perspektywą rynkową.

Jednocześnie traktat z Lizbony zniósł trzeci filar Unii Europejskiej, włączając w rzeczywistości współpracę policyjną i sądową w sprawach karnych do pierwszego filaru jako element przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Jednocześnie do aktu końcowego konferencji międzyrządowej, która przyjęła traktat z Lizbony podpisany w 13 grudnia 2007 r. dołączono *Deklarację 21* o treści:

[8] Karta Praw Podstawowych weszła w życie 1 grudnia 2009 r.

> Konferencja przyznaje, że konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie artykułu 16 Traktatu o funkcjonowaniu Unii Europejskiej, ze względu na szczególny charakter tych dziedzin[9].

W 2009 r. Komisja Europejska przeprowadziła przegląd istniejących ram prawnych w zakresie ochrony danych osobowych, rozpoczynając od konferencji na wysokim szczeblu w maju tego roku, po której nastąpiły konsultacje publiczne trwające do końce tego roku. Prowadzono również wiele analiz[10]. W opublikowanym 4 listopada 2010 r. Komunikacie Komisji Europejskiej do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów zatytułowanym *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej* stwierdzono, że z perspektywy piętnastu lat obowiązywania dyrektywy 95/46/WE należy zauważyć, iż szybki rozwój technologiczny i globalizacja doprowadziły do głębokich przemian w otaczającym nas świecie i przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Wymieniono tu głównie rozwój usług świadczonych drogą elektroniczną, sieci społecznościowe w internecie oraz problem przetwarzania danych „w chmurze". Jak zauważyła Komisja Europejska:

> Równocześnie metody gromadzenia danych osobowych stały się coraz bardziej wyrafinowane i trudniej wykrywalne. Przykładowo użycie zaawansowanych narzędzi umożliwia podmiotom gospodarczym lepsze dobranie strategii przyjmowanej wobec poszczególnych jednostek dzięki monitorowaniu ich zachowania. (…) Także organy publiczne wykorzystują coraz większą ilość danych osobowych do różnych celów, takich jak ustalanie miejsca pobytu osób fizycznych w przypadku epidemii choroby zakaźnej, zapobieganie terroryzmowi i przestępczości oraz zwalczanie tych zjawisk, zarządzanie systemami zabezpieczenia społecznego do celów podatkowych, posługując się aplikacjami używanymi do administracji elektronicznej itd.[11]

Działania analityczne Komisji doprowadziły do wniosku, że podstawowe zasady zawarte w dyrektywie są nadal aktualne, jednak zidentyfikowano następujące sprawy problematyczne:

- reakcję na oddziaływanie nowych technologii (potrzeba sprecyzowania zasad ochrony danych osobowych w odniesieniu do nowych technologii),
- poprawę sytuacji w zakresie ochrony danych osobowych związanych z rynkiem wewnętrznym (brak dostatecznej harmonizacji przepisów),
- reakcję na globalizację oraz poprawę międzynarodowego przekazywania danych,
- zapewnienie lepszych rozwiązań instytucjonalnych w celu skutecznego egzekwowania przepisów o ochronie danych (wzmocnienie roli organów ochrony danych).

---

[9] http://oide.sejm.gov.pl/oide/index.php?option=com_content&view=article&id=14807&Itemid=948#21 [dostęp: 17 IX 2017].

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów pt. *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, s. 2, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52010DC0609&from=EN [dostęp: 17 X 2017].

[11] Tamże, s. 1–2.

Komisja Europejska stwierdziła, że:

> Powyższe wyzwania wymagają od UE wypracowania kompleksowego i spójnego podejścia gwarantującego pełne poszanowanie podstawowego prawa osób fizycznych do ochrony ich danych osobowych poza nią: Traktat Lizboński zapewnił UE dodatkowe środki umożliwiające UE osiągnięcie tego celu: Kartę praw podstawowych UE, w art. 8 której uznano niezależne prawo do ochrony danych osobowych (…) wprowadzono również nową podstawę prawną umożliwiającą ustanowienie całościowych i spójnych unijnych przepisów o ochronie osób fizycznych w odniesieniu do przetwarzania ich danych osobowych oraz swobodnego przepływu takich danych[12].

Jako zasadnicze cele reformy europejskiego systemu ochrony danych osobowych Komisja Europejska wymieniła:
- wzmocnienie praw osób fizycznych,
- poprawę wymiaru związanego z rynkiem wewnętrznym,
- rewizję przepisów o ochronie danych w zakresie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych,
- globalny wymiar ochrony danych,
- zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych.

Na wzmocnienie praw osób fizycznych miały się składać:
- zagwarantowanie odpowiedniej ochrony osobom fizycznym we wszystkich okolicznościach,
- zwiększenie przejrzystości wobec osób, których dane dotyczą,
- poprawę kontroli podmiotu danych nad własnymi danymi,
- pogłębianie świadomości społeczeństwa,
- zapewnienie osobie fizycznej realizacji prawa do świadomej i dobrowolnej zgody na przetwarzanie dotyczących jej danych osobowych,
- zapewnienie ochrony danych szczególnie chronionych,
- zapewnienie większej skuteczności sankcji i środków zaradczych.

Jako elementy poprawy wymiaru związanego z rynkiem wewnętrznym Komisja wymieniła:
- zwiększenie pewności prawnej oraz zapewnienie równych szans administratorom danych,
- zmniejszenie obciążeń administracyjnych,
- wyjaśnienie przepisów dotyczących prawa właściwego oraz odpowiedzialności państw członkowskich,
- wzmocnienie odpowiedzialności administratorów danych,
- zachęcanie do inicjatyw w dziedzinie samoregulacji oraz analizę unijnych systemów certyfikacji.

W zakresie globalnego wymiaru ochrony danych Komisja dostrzegła potrzebę:
- wyjaśnienia i uproszczenia przepisów dotyczących międzynarodowych transferów danych,
- propagowania uniwersalnych zasad.

[12] Tamże, s. 4–5.

W zakresie rewizji przepisów o ochronie danych osobowych w sferze współpracy policyjnej i sądowej w sprawach karnych Komisja Europejska powołała się na swoje stanowiska dotyczące programu sztokholmskiego (COM(2009)262 z 10 czerwca 2009 r.) oraz sztokholmskiego planu działania (COM(2010)171 z 20 kwietnia 2010 r.), w których podkreślono potrzebę zapewnienia (…) *systemu pełnej ochrony" oraz „wzmocnienia stanowiska UE dotyczącego ochrony danych osobowych w kontekście wszystkich obszarów polityki UE, w tym w dziedzinie egzekwowania prawa i zapobiegania przestępstwom*[13].

Podczas analizy decyzji ramowej Komisja zidentyfikowała następujące wady tego aktu:

- decyzja, o której mowa, dotyczy wyłącznie transgranicznej wymiany danych osobowych w granicach UE, nie mając zastosowania do wewnętrznych operacji przetwarzania danych w państwach członkowskich; w praktyce trudno odróżnić obie sytuacje, co może utrudniać faktyczne wprowadzenie w życie i stosowanie tego dokumentu,
- decyzja zawiera zbyt szerokie wyłączenie zasady celowości,
- w decyzji brakuje przepisów nakazujących rozróżnienie miedzy różnymi kategoriami danych,
- decyzja nie zastąpiła różnych sektorowych aktów legislacyjnych dotyczących współpracy policyjnej i wymiaru sprawiedliwości w sprawach karnych, przyjętych na szczeblu UE.

Komisja doszła do wniosku dotyczącego potrzeby rozważenia rewizji przepisów o ochronie danych w zakresie współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Zapowiedziała też ewentualne rozszerzenie stosowania ogólnych przepisów o ochronie danych na obszar współpracy policyjnej i sądowej w sprawach karnych, w tym na przetwarzanie danych na szczeblu krajowym, przy zapewnieniu harmonizacji ograniczeń praw podmiotów danych w tych sferach. Nie wykluczyła jednak przyjęcia szczególnych przepisów o ochronie danych w sektorze policyjnym i sądowym[14].

Komisja zapowiedziała przedstawienie w 2011 r. projektów przepisów zmierzających do rewizji prawnych ram ochrony danych osobowych w duchu podejścia kompleksowego, w kontekście wszystkich rodzajów polityki UE (w tym egzekwowania prawa i zapobiegania przestępczości), przy uwzględnieniu specyfiki tego obszaru[15].

W dniu 24 lutego 2011 r. Rada Unii Europejskiej przyjęła konkluzję, w której poparła zamiar Komisji dotyczący zreformowania ram ochrony danych[16]. To samo uczynił Parlament Europejski w rezolucji z 6 lipca 2011 r.[17]

W dniu 25 stycznia 2012 r. Unijna Komisarz ds. Sprawiedliwości i Praw Podstawowych Viviane Reding przedstawiła projekt kompleksowej reformy przepisów o ochronie danych osobowych. W uzasadnieniu wskazała, że obecnie obowiązujące przepisy w tym zakresie powstały w połowie lat 90. ubiegłego wieku i całkowicie nie przystają do realiów zinformatyzowanego społeczeństwa XXI wieku. Ochrona danych osobowych stanowi

[13] Tamże, s. 14.

[14] Tamże, s. 5–20

[15] Tamże, s. 20.

[16] *Uzasadnienie Wniosku Komisji Europejskiej – rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), Bruksela dnia 25.1.2012 r. COM(2012) 11 final*, s. 4.

[17] Tamże; *Rezolucja PE z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI))*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL [dostęp: 21 IX 2017].

prawo podstawowe wszystkich Europejczyków, ale obywatele nie zawsze mają poczucie pełnej kontroli nad informacjami, które ich dotyczą. W przekonaniu V. Reding zmiany powinny budować zaufanie do usług internetowych oraz wpływać bezpośrednio na większy dostęp do danych osobowych tych osób, których one dotyczą. Komisja Europejska zaprezentowała projekt pakietu reform mających w sposób kompleksowy regulować problematykę związaną z ochroną danych osobowych w ramach Unii Europejskiej[18].

Pierwszym z projektów należących do przedstawionego pakietu był projekt *Ogólnego rozporządzenia o danych*[19]. Miał on derogować obowiązującą dyrektywę 95/46/WE oraz stworzyć nowe zasady regulujące system ochrony danych osobowych z wyłączeniem obszarów, w których będą obowiązywać regulacje szczególne, takich jak: przetwarzanie danych przez organy UE czy przetwarzanie danych w sferze policyjnej i sądowej w sprawach karnych. Projekt ogólnego rozporządzenia o danych został oparty na założeniu, że w całej Unii Europejskiej będzie obowiązywał jeden kompleksowy akt prawny, którego przepisy będą odnosiły bezpośredni skutek oraz będą bezpośrednio stosowane na płaszczyznach krajowych systemów prawnych.

Nieco inne podejście przyjęto w odniesieniu do sfery policyjnej i sądowej w sprawach karnych. W tym zakresie zdecydowano się na uchwalenie w miejsce obecnie obowiązującej decyzji ramowej Rady dyrektywy o ochronie danych osobowych[20]. Zakresem regulacji dyrektywy miało zostać objęte przetwarzanie danych przez organy policyjne i sądowe państw członkowskich na potrzeby ścigania przestępstw i zapobiegania im. Zniknęła znana z decyzji ramowej przesłanka wymiany danych między państwami członkowskimi.

Po trwającym ponad cztery lata procesie legislacyjnym obie części pakietu reformującego europejski system ochrony danych osobowych zostały ostatecznie przyjęte przez Parlament Europejski i Radę 27 kwietnia 2016 r., w brzmieniu nie odbiegającym zasadniczo od pierwotnych założeń.

W dniu 4 maja 2016 r. zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej teksty następujących aktów prawnych:

1) *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (Dz. Urz. UE L nr 119, s. 1), zwane dalej: „rozporządzeniem odo";
2) *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW* (Dz. Urz. UE L z 2016 r. nr 119, s. 89), zwana dalej: „dyrektywą odo".

[18] http://europa.eu/rapid/press-release_IP-12-46_pl.htm [dostęp: 22 IX 2017]

[19] Wniosek Komisji Europejskiej – rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), Bruksela 25 I 2012 r. COM(2012) 11 final.

[20] Wniosek Komisji Europejskiej – dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, Bruksela 25 I 2012 r. COM(2012) 10 final.

W rzeczywistości reforma europejskiego systemu ochrony danych osobowych zostanie wdrożona w maju 2018 r. Rozporządzenie odo wejdzie w życie 25 maja 2018 r., termin implementacji dyrektywy odo upływa zaś 6 maja tego samego roku.

Uwagę zwraca zasadnicze wzmocnienie czynnika regulacyjnego na poziomie europejskim: w zakresie ochrony danych osobowych w „sferze cywilnej" akt harmonizujący ustawodawstwa krajowe, jakim jest dyrektywa, zastąpiono bezpośrednio skutecznym rozporządzeniem, w „sferze policyjnej" zaś szczątkową, bardzo ograniczoną regulację w postaci decyzji ramowej (regulującej wyłącznie ochronę danych osobowych wymienianych w ramach współpracy międzynarodowej) zastąpiono harmonizacją krajowych porządków prawnych w postaci dyrektywy.

2.2.1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

Po wprowadzeniu w życie projektu ogólnego rozporządzenia o danych w całej Unii Europejskiej będzie obowiązywał jeden kompleksowy akt prawny, którego przepisy będą odnosiły bezpośredni skutek oraz będą bezpośrednio stosowane na płaszczyznach krajowych systemów prawnych. Zgodnie z art. 2 ust. 2 rozporządzenia odo jego przepisy nie mają zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii,
b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakresu tytułu V rozdział 2 TUE (*Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa*),
c) przez osobę fizyczną w ramach czynności o charakterze czysto osobistym lub domowym,
d) przez właściwe organy w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Regulacje rozporządzenia nie dotyczą zatem działalności organów wymiaru sprawiedliwości (lit. d) ani służb specjalnych (lit. a).

2.2.2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680

Inaczej sytuacja będzie wyglądała w sferze współpracy policyjnej i sądowej w sprawach karnych. W tym zakresie zdecydowano się na zastosowanie mechanizmu harmonizacji ustawodawstw krajowych państw członkowskich przez uchwalenie dyrektywy w miejsce obecnie obowiązującej decyzji ramowej Rady.

Przepis art. 1 ust. 1 dyrektywy odo stanowi, że *Niniejsza dyrektywa ustanawia przepisy o ochronie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postepowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*. Art. 2 ust. 2 dyrektywy stanowi, że ma ona zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1. Aby więc właściwie określić zakres podmiotowy dyrektywy odo należy zdekodować pojęcie właściwy organ. Definicja tego pojęcia jest zawarta w art. 3 pkt 7. Zgodnie z treścią wskazanej definicji właściwy organ oznacza: (…) *organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępo-*

wań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, a także (…) *inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*.

Zakresem regulacji dyrektywy ma być zatem objęte przetwarzanie danych przez organy policyjne i sądowe państw członkowskich na potrzeby ścigania przestępstw, jak również zapobiegania im. Zniknęła przesłanka wymiany danych między państwami członkowskimi znana z decyzji ramowej.

Dyrektywa odo wymaga, aby dane osobowe zbierane przez organy egzekwowania prawa były: przetwarzane zgodnie z prawem (zasada legalności) i rzetelnie (zasada rzetelności), w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami (zasada celowości), adekwatne, stosowne i nienadmierne w stosunku do celów, w jakich są przetwarzane (zasada adekwatności), prawidłowe i w razie potrzeby uaktualniane, przechowywane w formie umożliwiającej identyfikację osób przez okres nie dłuższy niż jest to niezbędne do ich przetwarzania, odpowiednio zabezpieczane, w tym przed niedozwolonym lub niezgodnym z prawem przetwarzaniem.

Kraje UE zostały zobowiązane do przyjęcia terminów usuwania danych osobowych lub regularnego przeglądu konieczności ich przechowywania (art. 5).

Ważną nowością w stosunku do dotychczasowych regulacji jest wymóg, aby organy egzekwowania prawa wyraźnie rozróżniły dane osobowe poszczególnych kategorii osób, w tym:

- osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony,
- osób skazanych za czyn zabroniony,
- pokrzywdzonych czynem zabronionym lub w których przypadku można zasadnie uznać, że mogą stać się ofiarą czynu zabronionego,
- osób innych w stosunku do czynu zabronionego, w tym potencjalnych świadków.

Do najważniejszych postanowień dyrektywy odo zaliczają się przepisy dotyczące praw osoby, której dane dotyczą. Artykuły 12–14 przewidują prawo wolnego od opłat dostępu podmiotu danych do informacji, które go dotyczą (to prawo obejmuje m.in. uzyskiwanie informacji na temat: tożsamości i danych administratora, celów przetwarzania danych, odbiorców danych, planowanego okresu przechowywania danych, informacji o prawie złożenia skargi do organu nadzorczego oraz prawie do dostępu do danych osobowych oraz ich poprawienia lub usunięcia albo ograniczenia ich przetwarzania).

Zgodnie z art. 13 ust. 2 dyrektywy odo państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, aby:

- uniemożliwić utrudnianie czynności postepowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur,
- uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar,
- chronić bezpieczeństwo publiczne,
- chronić bezpieczeństwo narodowe,
- chronić prawa i wolności innych osób.

Omawiany przepis zawiera zastrzeżenie, że środki ograniczające w stosunku do realizacji prawa do informacji podmiotu danych stosowane przez państwo członkowskie mogą być stosowane w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, oraz z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Powyższe zastrzeżenie wymusza wąskie traktowanie tego wyłączenia.

Odrębnie od prawa do informacji dyrektywy odo traktuje prawo dostępu przysługujące osobie, której dane dotyczą. Polega ono na zapewnieniu takiej osobie uzyskania odpowiedzi na pytanie, czy przetwarzane są informacje, które jej dotyczą, a jeżeli tak – to prawa dostępu do nich oraz do informacji o:

- celu i podstawie prawnej przetwarzania,
- kategoriach odnośnych danych osobowych,
- odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione,
- planowanym okresie przechowywania danych osobowych lub kryteriach służących określeniu tego okresu,
- prawie do żądania od administratora danych sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych jej dotyczących,
- prawie wniesienia skargi do organu nadzorczego oraz jego danych kontaktowych, a także wskazania, jakie dane osobowe są przetwarzane, oraz wszelkich dostępnych informacji o ich pochodzeniu.

Dopuszczalne ograniczenia w zakresie stosowania prawa dostępu formułuje art. 15 dyrektywy odo. Ten przepis zezwala na przyjęcie przez państwo członkowskie aktów prawnych pozwalających ograniczyć – w całości lub w części – prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim częściowe lub całkowite ograniczenie jest działaniem niezbędnym w społeczeństwie demokratycznym do osiągnięcia celów, których wykaz jest identyczny z wykazem tych celów, dla których można ograniczyć informowanie podmiotu, zgodnie z art. 13 ust. 2. Podobnie jak w odniesieniu do ograniczeń dotyczących informowania podmiotu danych, w art. 15 ust. 2 dopuszczono, aby państwa członkowskie przyjęły akty prawne ustalające kategorie przetwarzania danych w całości albo w części spełniające kryteria odmowy dostępu, zgodnie z kryteriami zawartymi w ust. 1. Zarówno jednak w przypadku, gdy odmowa realizacji prawa dostępu do danych następuje w wyniku indywidualnej oceny administratora, jak i zakwalifikowania danych do kategorii wchodzącej w całości w zakres wyłączenia, administrator danych jest obowiązany, stosownie do ust. 3, do pisemnego poinformowania osoby, której dane dotyczą, o każdej odmowie lub ograniczeniu prawa dostępu i o przyczynach tej odmowy albo ograniczenia. Te informacje można pominąć, jeśli ich ujawnienie godziłoby w którykolwiek z celów wymienionych w ustępie 1, natomiast nie można pominąć poinformowania osoby, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

Administratorzy danych mają ponadto być zobowiązani do dokumentowania rzeczywistych lub prawnych powodów, na jakich jest oparta decyzja, w celu udostępnienia tych informacji organom nadzorczym (ust. 4).

Ostatnim z praw podmiotu danych wprowadzanych przepisami dyrektywy odo jest prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania. Zgodnie z ust. 1 wskazanego przepisu, osoba, której dane dotyczą, ma prawo uzyskiwania od administratora danych ich sprostowania, jeśli są one nieprawidłowe. Ustęp 2 przewiduje nałożenie na administratora danych obowiązku usunięcia bez zbędnej

zwłoki danych osobowych, jeśli ich przetwarzanie narusza zasady przetwarzania danych osobowych ustanowione dyrektywą, jest niezgodne z prawem, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienie obowiązku prawnego ciążącego na administratorze. Zamiast usunięcia, administrator ogranicza przetwarzanie, jeśli nie można stwierdzić, czy dane są prawidłowe, lub gdy są one potrzebne do celów dowodowych (ust. 3). Zgodnie z art. 16 ust. 5 państwa członkowskie są obowiązane zapewnić, aby administrator pisemnie informował osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia dotyczących jej danych osobowych oraz jej przyczynach. Ten obowiązek może zostać ograniczony w ustawodawstwie krajowym na warunkach analogicznych do warunków ograniczenia prawa dostępu i obowiązków informacyjnych administratora danych.

Zgodnie z art. 17 dyrektywy odo państwa członkowskie są zobowiązane zapewnić możliwość, aby podmiot danych mógł realizować swoje uprawnienia również za pośrednictwem organu nadzorczego.

Rozdział IV dyrektywy odo reguluje obowiązki administratora danych i podmiotu przetwarzającego dane.

Na administratorze, zgodnie z dyrektywą, spoczywają obowiązki: stosowania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych odbywało się na podstawie tego właśnie dokumentu (art. 19–20); prowadzenia wykazów czynności przetwarzania danych (art. 24); ewidencjonowania czynności przetwarzania danych (art. 25); dokonywania oceny skutków planowanych operacji przetwarzania danych (art. 27); współpracy z organem nadzorczym (art. 26) i prowadzenia z nim uprzednich konsultacji, w wypadku tworzenia nowego zbioru danych (art. 28).

W zakresie bezpieczeństwa danych osobowych (art. 25–31) organy krajowe są zobowiązane podjąć środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa tych danych odpowiadającego zagrożeniu. Jeśli przetwarzanie danych jest zautomatyzowane, należy zastosować odpowiednie środki, w tym:

- uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania,
- zapobieganie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych,
- zapobieganie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu przeglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych[21].

W przypadku naruszenia ochrony danych osobowych dyrektywa nakłada na administratora obowiązek zawiadomienia o tym organu nadzorczego oraz osoby, której dane dotyczą dane. Obowiązek zawiadomienia organu nadzorczego ma charakter bezwzględny – powinno ono nastąpić w terminie 72 godzin od stwierdzenia naruszenia. W przypadku przekroczenia tego terminu niezbędne jest dołączenie uzasadnienia (art. 30).

Natomiast zawiadomienie osoby, której dotyczą dane (art. 31), powinno nastąpić jedynie wtedy, gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Ponadto zawiadomienie osoby fizycznej nie jest wymagane, jeżeli został spełniony jeden z trzech warunków:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

[21] http://eur-lex.europa.eu/legal-content/PL/LSU/?uri=CELEX:32016L0680 [dostęp: 19 IX 2017].

– administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
– wymagałoby ono zbyt dużego wysiłku – w takim momencie zawiadomienie może zostać zastąpione przez publiczny komunikat.

Ostatecznie więc może się okazać, że omówiona norma wprowadzająca obowiązek informowania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych okaże się regulacją martwą.

Istotnym obowiązkiem nałożonym przez dyrektywy odo na administratora danych jest obowiązek wyznaczenia inspektora ochrony danych, monitorującego przestrzeganie przepisów dyrektywy i współpracującego z organem nadzorczym[22]. Z obowiązku powołania inspektora ochrony danych mogą zostać zwolnione jedynie organy sądowe[23].

Rozdział V dyrektywy odo reguluje przekazywanie danych do państw trzecich lub organizacji międzynarodowych.

Ogólne zasady przekazywania danych osobowych odbiorcom mającym siedzibę w państwach trzecich określa artykuł 35 dyrektywy odo. Zgodnie z treścią ust. 1 tego dokumentu państwa członkowskie mają obowiązek zapewnić, aby przekazanie przez właściwe organy danych osobowych, które są lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, mogło nastąpić pod warunkiem zgodności z przepisami krajowymi przyjętymi na podstawie innych przepisów dyrektywy jedynie, jeśli:

a) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1[24];
b) dane osobowe są przekazywane administratorowi w państwie trzecim albo organizacji międzynarodowej, który jest organem właściwym do realizacji celów, o których mowa w art. 1 ust. 1;
c) w przypadku przesyłania lub udostępniana danych od innego państwa członkowskiego to inne państwo członkowskie wyraziło uprzednią zgodę na przekazanie zgodnie ze swoim prawem krajowym;
d) Komisja wydała decyzję dotyczącą zgodności na podstawie art. 36 lub w razie braku takiej decyzji zostały zapewnione lub istnieją odpowiednie zabezpieczenia zgodnie z art. 37 albo w razie braku decyzji odnośnie do zgodności wydanej na podstawie art. 36 lub zabezpieczeń zgodnie z art. 37 zastosowanie mają wyjątki w szczególnych sytuacjach zgodnie z art. 38; oraz
e) w przypadku dalszego przekazania do innego państwa trzeciego lub organizacji międzynarodowej właściwy organ, który dokonał pierwotnego przekazania, lub inny właściwy organ tego samego państwa członkowskiego zezwala na dalsze przekazanie po należytym uwzględnieniu wszystkich istotnych czynników, w tym powagi czynu zabronionego, celu, w którym dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

Przekazanie danych osobowych bez uprzedniej zgody państwa członkowskiego, które te dane udostępniło, jest dopuszczalne wyłącznie wtedy, gdy jest ono niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu bezpieczeństwa publicznego

[22] Zadania inspektora ochrony danych – art. 34 dyrektywy.

[23] Tak stanowi art. 32 ust. 1 dyrektywy.

[24] Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym ochrona przed zagrożeniami bezpieczeństwa publicznego i zapobieganie takim zagrożeniom.

w państwie członkowskim lub w państwie trzecim bądź też bezpieczeństwa ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie.

Istotną regulację zawiera art. 36 – *Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony*. Ten przepis przyznaje Komisji uprawnienie do oceny, czy dane państwo trzecie, terytorium lub przynajmniej jeden sektor w państwie trzecim lub organizacja międzynarodowa zapewniają adekwatny stopień ochrony. W celu ustalenia, czy stopień ochrony jest odpowiedni, Komisja bada praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo, a także praktyki w zakresie ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego w zakresie ochrony danych osobowych w państwie trzecim lub organu nadzorującego organizację międzynarodową, a także międzynarodowe zobowiązania państwa trzeciego lub organizacji międzynarodowej albo inne obowiązki wynikające z prawnie wiążących konwencji lub aktów prawnych oraz z udziału w systemach wielostronnych lub regionalnych, zwłaszcza w sferze ochrony danych osobowych. Po dokonaniu oceny Komisja może w drodze aktu wykonawczego zdecydować, czy państwo trzecie, terytorium, przynajmniej jeden określony sektor w państwie trzecim albo organizacja międzynarodowa zapewniają adekwatny poziom ochrony. Akt wykonawczy Komisji określa terytorialny i sektorowy zakres jego stosowania, a także mechanizm okresowego przeglądu, odbywającego się przynajmniej raz na cztery lata. Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej i na swojej stronie internetowej wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą określony poziom ochrony lub jego brak[25].

W przypadku, gdy Komisja stwierdzi, że dane państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim albo organizacja międzynarodowa zapewniają adekwatny poziom ochrony, przekazanie danych osobowych nie wymaga specjalnego zezwolenia[26].

Jeśli zaś Komisja nie podjęła stosownej decyzji, państwa członkowskie, zgodnie z art. 37 dyrektywy, mogą przekazywać dane osobowe do państwa trzeciego z zastrzeżeniem odpowiednich zabezpieczeń, tzn. gdy w prawnie wiążącym akcie wprowadzono odpowiednie zabezpieczenia ochrony danych osobowych (należy uznać, że takim aktem będzie umowa międzynarodowa łącząca państwo członkowskie z państwem trzecim albo organizacją międzynarodową), albo też jeśli administrator ocenił wszystkie okoliczności związane z przekazaniem danych osobowych i stwierdził, że istnieją odpowiednie zabezpieczenia ochrony danych osobowych. W tym drugim przypadku przekazanie danych osobowych musi zostać udokumentowane, a dokumentacja (obejmująca datę i godzinę przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe) – udostępniona na żądanie organowi nadzorczemu.

Artykuł 38 dyrektywy odo przewiduje ponadto *Wyjątki w szczególnych sytuacjach*, gdy brakuje zarówno decyzji stwierdzającej odpowiedni poziom ochrony danych, jak też odpowiednich zabezpieczeń, o których mowa w art. 37. W takich przypadkach przekazanie danych do państwa trzeciego lub organizacji międzynarodowej jest dopuszczalne, jeśli jest niezbędne:

[25] Art. 36 ust. 8.
[26] Tamże, ust. 1.

a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;
b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi;
c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego;
d) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1[27]; lub
e) w indywidualnym przypadku, dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1.

Również i w tym przypadku występuje obowiązek odpowiedniego udokumentowania przekazania danych osobowych i przekazania dokumentacji organowi nadzorczemu.

Kolejny wyjątek od zasad przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej zawiera art. 39, w którym zostały określone warunki przekazania danych osobowych bezpośrednio odbiorcy w państwie trzecim, który nie jest administratorem danych osobowych stanowiącym organ właściwy do realizacji celu dyrektywy. Takie przekazanie danych osobowych jest dopuszczalne jeżeli;

Artykuł 57 dyrektywy odo nałożył na państwa członkowskie obowiązek przyjęcia przepisów określających skuteczne, proporcjonalne i odstraszające sankcje za naruszenie jej przepisów.

Zgodnie z art. 63 dyrektywy odo termin jej transpozycji upływa 6 maja 2018 r. Do tego dnia państwa członkowskie są zobowiązane przyjąć i opublikować przepisy ustawowe, wykonawcze i administracyjne, niezbędne do wykonania dyrektywy. Teksty tych przepisów muszą zostać niezwłocznie przekazane Komisji Europejskiej. Wyjątek od tego terminu dotyczy zautomatyzowanych zbiorów danych utworzonych przed 6 maja 2016 r. Zgodnie z ustępem 2 takie systemy mogą zostać dostosowane do art. 25 dyrektywy, przewidującego ewidencjonowanie czynności przetwarzania danych w terminie do 6 maja 2023 r., jeśli ich dostosowanie w terminie wcześniejszym wymagałoby „niewspółmiernie dużego wysiłku". Z kolei ustęp 3 pozwala na dalsze wydłużenie terminu dostosowania do 6 maja 2026 r., (…) *jeżeli inaczej nastąpiłyby poważne problemy w funkcjonowaniu tego systemu*.

3. Wpływ reformy unijnego systemu ochrony danych osobowych na prawa i obowiązki służb specjalnych – wnioski *de lege ferenda* dla krajowego ustawodawcy

W chwili obecnej polski ustawodawca stoi przed wyzwaniem, jakim jest dostosowanie polskiego prawa do rozporządzenia i dyrektywy odo. Termin tego dostosowania upływa w maju 2018 r., wraz z wejściem w życie rozporządzenia odo z dniem 25 maja 2018 r. oraz upływem terminu transpozycji dyrektywy odo 6 maja 2018 r. W zakresie ogólnym przepisy ustawy o ochronie danych osobowych zostaną w większości zastąpione bezpośrednio skutecznymi przepisami rozporządzenia. Natomiast w sferze zwalczania przestępczości istnieje konieczność zbudowania w zasadzie od podstaw regulacji systemu ochrony danych osobowych. Stworzenie odpowiednich przepisów prawnych nie będzie łatwe z uwagi na specyfikę obszaru zwalczania przestępczości, która w odniesieniu do poważnych przestępstw polega nierzadko na prowadzeniu działań niejawnych. Może to spowodować krzyżowanie się zakresu regulacji ustawy implementującej dyrektywę odo z zakresem ustawy o ochronie informacji niejawnych.

[27] Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym ochrona przed zagrożeniami bezpieczeństwa publicznego i zapobieganie takim zagrożeniom.

Do najpoważniejszych kontrowersji wymagających rozstrzygnięcia przy tworzeniu ustawy implementacyjnej będzie należało określenie jej zakresu podmiotowego.

Jak już wspomniano wyżej, omawiając poszczególne przepisy dyrektywy odo, jej zakres, stosownie do art. 1 ust. 1, obejmuje przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Niniejszy przepis wyodrębnia dwa zakresy dyrektywy, które muszą zaistnieć łącznie, aby jej przepisy znalazły zastosowanie do danej sytuacji, tj. zakres podmiotowy i przedmiotowy. Zakres przedmiotowy dyrektywy to przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniem bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zakres podmiotowy zaś jest związany z pojęciem właściwy organ, zdefiniowanym w art. 3 pkt 7 dyrektywy odo. Zgodnie z treścią definicji zawartej w tym przepisie właściwy organ oznacza (…) *organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*, a także: *inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*.

Nie ulega wątpliwości, że ustawa implementująca dyrektywę odo powinna objąć swoim zakresem Policję i inne służby właściwe do ścigania przestępstw, zapobiegania im i ochrony bezpieczeństwa publicznego, takie jak: Straż Graniczna, Żandarmeria Wojskowa czy Krajowa Administracja Skarbowa. Powinna objąć również organy wymiaru sprawiedliwości, a zwłaszcza Prokuraturę (w stosunku do sądów sama dyrektywa formułuje wyjątki).

Największa kontrowersja dotyczy kwestii, czy i w jakim zakresie implementacja dyrektywy powinna objąć służby specjalne. Ten problem raczej nie dotyczy służb wywiadowczych odpowiedzialnych za bezpieczeństwo zewnętrzne państwa, tj. Agencji Wywiadu i Służby Wywiadu Wojskowego, w których ustawowych kompetencjach nie znajduje się zwalczanie przestępczości (ustawodawca, w odniesieniu do służb wywiadowczych, posługuje się konstrukcją rozpoznawania i przeciwdziałania „zagrożeniom", a nie „przestępstwom"[28]). Natomiast Służba Kontrwywiadu Wojskowego ma w zakresie swoich kompetencji rozpoznawanie, zapobieganie i wykrywanie przestępstw[29], Agencja Bezpieczeństwa Wewnętrznego i Centralne Biuro Antykorupcyjne zaś – również ściganie ich sprawców.[30]

[28] Art. 6 ust. 1 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2016 r. poz. 1897, ze zm.) i art. 6 ust. 1 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. z 2016 r. poz. 1318, ze zm.).

[29] Art. 5 ust. 1 pkt 1 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.

[30] Art. 5 ust. 1 pkt 2 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i art. 2 ust. 1 pkt 1 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2016 r. poz. 1310, ze zm.).

Z drugiej jednak strony, zgodnie artykułem 2 lit. a dyrektywy odo, nie ma ona zastosowania do działalności nieobjętej zakresem prawa Unii. W tym miejscu należy przypomnieć, że stosownie do art. 4 ust. 2 traktatu o Unii Europejskiej (…) *bezpieczeństwo narodowe pozostaje w sferze wyłącznej odpowiedzialności każdego państwa członkowskiego*. Istotną wskazówkę co do kierunku interpretacji tego wyłączenia stanowi motyw 14 preambuły dyrektywy odo, zgodnie z którym: (…) *dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym* (…) *nie należy uznawać za czynności wchodzące w zakres niniejszej dyrektywy*. Warto zauważyć, że zgodnie z treścią tego zapisu z zakresu regulacji dyrektywy ODO zostają wyłączone zarówno (…) *czynności w zakresie bezpieczeństwa narodowego*, jak i *czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym* wyodrębnione przez ustawodawcę unijnego do odrębnej kategorii. Według niniejszego zapisu istnieje zatem możliwość wyłączenia z zakresu implementacji przedmiotowej dyrektywy do prawa krajowego sfery bezpieczeństwa narodowego na podstawie kryterium podmiotowego (*czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym*) oraz funkcjonalnego (*czynności w zakresie bezpieczeństwa narodowego*). W przypadku zastosowania wyłączenia podmiotowego wystarcza, jeśli dana agencja lub jednostka „zajmuje się" bezpieczeństwem narodowym, nie jest zaś niezbędne prowadzenie przez dany podmiot działalności wyłącznie w sferze bezpieczeństwa narodowego. Należy uznać, że gdyby racjonalny ustawodawca unijny chciał ograniczyć możliwość wyłączenia z zakresu implementacji dyrektywy jedynie czynności wykonywane w zakresie bezpieczeństwa narodowego, mógłby ograniczyć omawiane wyłączenie do kryterium funkcjonalnego albo też w wyłączeniu podmiotowym dodać słowo „wyłącznie" przed wyrażeniem „bezpieczeństwem narodowym", a przecież żadnej z tych rzeczy nie uczynił.

Przed ustawodawcą krajowym stoi zatem poważne zadanie odpowiedniego sformułowania wyłączenia z zakresu stosowania ustawy implementującej dyrektywę odo organów zajmujących się ochroną bezpieczeństwa narodowego. Wymaga to również stosownego określenia w punkcie wyjścia zakresu pojęcia bezpieczeństwo narodowe, które nie ma przecież legalnej definicji. Należy uznać, że w pojęciu bezpieczeństwo narodowe mieści się występujące w polskim prawie pojęcie bezpieczeństwo państwa. Wobec tego w zakresie bezpieczeństwa narodowego z pewnością mieszczą się zadania służb specjalnych ukierunkowane na ochronę suwerenności państwa i jego podstawowych funkcji, takie jak: ochrona porządku konstytucyjnego, prowadzenie działalności kontrwywiadowczej, ochrona informacji niejawnych czy ściganie przestępstw przeciwko bezpieczeństwu państwa.

Jako przykład obrazujący trudności związane z rozgraniczeniem sfery bezpieczeństwa narodowego, pozostającej w zakresie wyłącznej odpowiedzialności państw członkowskich, od sfery wspólnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której kompetencje ma Unia Europejska, należy wskazać problem przeciwdziałania terroryzmowi oraz zwalczania tego zagrożenia. Z jednej strony działalność służb specjalnych w tym obszarze bywa traktowana jako wchodząca w zakres zapewniania bezpieczeństwa narodowego, z drugiej zaś ten obszar coraz częściej jest poddawany regulacji prawa Unii Europejskiej, zwłaszcza w odniesieniu do współpracy międzynarodowej. Granice sfer kompetencji Unii Europejskiej i jej państw członkowskich stają się w tym zakresie coraz mniej przejrzyste.

Przed polskim ustawodawcą stoi więc w chwili obecnej trudne i delikatne zadanie polegające na właściwym wyważeniu rozbieżnych nieraz interesów w toku implementacji dyrektywy odo do polskiego prawa, w sytuacji gdy do upływu terminu transpozycji prawa pozostały już jedynie miesiące. Ustawodawca powinien wziąć pod uwagę prawnie chroniony interes służb specjalnych do ochrony niejawności swoich działań, która jest ich podstawowym modus operandi odróżniającym je od innych organów powołanych do ochrony bezpieczeństwa publicznego, drugiej zaś strony – prawa jednostki wspierane przez ewolucję prawa międzynarodowego, wśród których poczesne miejsce zajmuje w ostatnich latach prawo do ochrony danych osobowych.

Ochronie niejawności działań służb specjalnych służy wiele przepisów prawnych, spośród których na przytoczenie zasługuje np. art. 7 ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167, ze zm.). Określa on kategorie informacji, które powinny być chronione jako informacje niejawne, bez względu na upływ czasu, a mianowicie: dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych, jako osób wykonujących te czynności, jak również dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy. Należy uznać, że „dane mogące doprowadzić do identyfikacji osób" mieszczą się w pojęciu danych osobowych w rozumieniu dyrektywy odo. Co prawda ten przepis nie odnosi się tylko do służb specjalnych, ale do wszystkich organów uprawnionych do prowadzenia czynności operacyjno-rozpoznawczych, należy jednak mieć na uwadze, że dla służb specjalnych tego rodzaju czynności, inaczej niż dla służb policyjnych, stanowią podstawową formę ich działalności. Istnieją ponadto rygorystyczne przepisy o ochronie określonych informacji zawarte w ustawach pragmatycznych służb specjalnych. W tym kontekście należy wymienić: art. 39 ust. 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i analogiczne do niego: art. 43 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego oraz art. 28 ust. 2 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym. Te przepisy wprowadzają bliski bezwzględnego zakaz ujawniania przez służby specjalne informacji o osobie, jeśli te informacje zostały pozyskane w wyniku czynności operacyjno-rozpoznawczych prowadzonych przez służby, a także o osobach udzielających im pomocy. Ujawnienie tego typu informacji jest możliwe tylko w wąsko określonym zakresie przypadków, tj. w przypadku żądania prokuratora lub sądu, zgłoszonego w celu ścigania karnego za czyn zabroniony stanowiący zbrodnię lub występek, którego skutkiem jest śmierć (w przypadku CBA również uszczerbek na zdrowiu albo szkoda w mieniu), lub postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych (w przypadku SKW i SWW również żądania Rzecznika Interesu Publicznego w ramach toczącego się postępowania lustracyjnego), albo w przypadku żądania prokuratora lub sądu, uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Należy uznać, że „informacje o osobie", o których mowa w tych przepisach, obejmują dane osobowe. Te przepisy kłócą się z uprawnieniami podmiotu danych, takimi jak prawo do informacji o przetwarzaniu dotyczących go danych, dostępu do dotyczących go danych czy uprawnieniami niezależnego organu nadzorczego, w tym prawo dostępu do wszelkich danych osobowych przetwarzanych przez podmiot nadzorowany, formułowanymi w przepisach dyrektywy odo (art. 47 ust. 1).

Wskazane powyżej okoliczności przemawiają za pełnym, podmiotowym wyłączeniem służb specjalnych z zakresu obowiązywania przyszłej ustawy transponującej dyrektywę odo do polskiego porządku prawnego.

Krytycy takiego rozwiązania mogą podnosić, że przepisy dyrektywy odo zawierają mechanizmy pozwalające ograniczyć niektóre uprawnienia podmiotu danych. Na przykład art. 15 ust. 1 dyrektywy odo pozwala na przyjęcie rozwiązań umożliwiających ograniczenie w całości lub w części prawa dostępu osoby, której dane dotyczą, do odnoszących się do niej danych, jeśli jest to niezbędne i proporcjonalne do tego, aby np. uniemożliwić utrudnianie postępowania przygotowawczego albo chronić bezpieczeństwo narodowe. Zamiast więc całkowicie wyłączać służby specjalne z zakresu ustawy transponującej dyrektywę odo, można by stworzyć mechanizm pozwalający im na odmowę realizacji praw podmiotu dotyczących przetwarzanych przez nie danych z uwagi na ochronę bezpieczeństwa narodowego. Gdyby jednak taki mechanizm powstał, to należy sądzić, że byłby powszechnie stosowany przez służby specjalne w celu ochrony ich zainteresowań operacyjnych. Wobec tego korzyść, jaką odniósłby podmiot danych, mogłaby się okazać iluzoryczna.

Inną kwestią są uprawnienia nadzorcze niezależnego organu ochrony danych, ponieważ w tym zakresie dyrektywa nie przewiduje możliwości formułowania wyłączeń.

Wobec powyższego, w odniesieniu do planowanej implementacji dyrektywy odo nasuwa się konkluzja, że w sytuacji, gdy prawo Unii Europejskiej daje państwom członkowskim możliwość ochrony atrybutu swojej suwerenności, jakim jest bezpieczeństwo narodowe, przez stosowne wyłączenia, państwo polskie powinno w interesie swoich organów chroniących je przed najpoważniejszymi zagrożeniami skorzystać z nich w najdalej idącym zakresie.

Michał Kamiński

Zagadnienie retencji danych w Unii Europejskiej z perspektywy orzeczenia Tele2

1. Wprowadzenie

W dniu 21 grudnia 2016 r. Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE) wydał wyrok w sprawach połączonych C-203/15 Tele2 *Sverige AB/Post-ochtelestyrelsen* i C-698/15 *Secretary of State for the Home Departament/Tom Watson i inni*[1].

Wyrok, o którym mowa, został wydany na skutek złożenia wniosków o orzeczenie w trybie prejudycjalnym, na podstawie art. 267 *Traktatu o Funkcjonowaniu Unii Europejskiej* (dalej: TFUE), przez administracyjny sąd apelacyjny w Sztokholmie w Królestwie Szwecji i sąd apelacyjny dla Anglii i Walii (wydział cywilny) Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej. Jest to drugie orzeczenie TSUE dotyczące zagadnienia retencji danych telekomunikacyjnych oraz dostępu do nich organów właściwych do zwalczania przestępczości, po orzeczeniu *Digital Rights Ireland i inni* CV-293/12 i C-594/12 z 8 kwietnia 2014 r.[2], które unieważniło dyrektywę retencyjną[3]. Potencjalne skutki ostatniego orzeczenia dla możliwości korzystania z danych telekomunikacyjnych przez policję i służby specjalne państw członkowskich Unii Europejskiej mogą być jednak poważniejsze.

W tym orzeczeniu TSUE dokonał wykładni art. 15 ust. 1 dyrektywy 2002/58/WE z 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[4], zmienionej dyrektywą 2009/136/WE z 25 listopada 2009 r.[5], w związku z art. 7, 8, 11 i art. 52 Karty praw podstawowych Unii Europejskiej.

Dyrektywa 2002/58/WE (dalej: dyrektywa o e-prywatności) jest aktem wydanym w celu harmonizacji przepisów krajowych państw członkowskich Unii Europejskiej dla zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, szczególnie prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej[6].

---

[1] LEX nr 2202679.

[2] LEX nr 1444266.

[3] *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE*.

[4] *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)* – Dz. Urz. UE L 201 z 31 VIII 2002 r., s. 37–47.

[5] *Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów* **(**Dz. Urz. UE L z 2002 r. nr 201, s. 37, z 2006 r. nr 105, s. 54 oraz z 2009 r. nr 337, s. 11).

[6] Art. 1 ust. 1 dyrektywy 2002/58/WE.

Jednocześnie z zakresu przedmiotowej dyrektywy, zgodnie z jej art. 1 ust. 3, miała być wyłączona działalność pozostająca poza zakresem *Traktatu Ustanawiającego Wspólnotę Europejską* – działalność w zakresie Wspólnej Polityki Zagranicznej i Bezpieczeństwa oraz współpraca policyjna i sądowa w sprawach karnych[7], a także działalność dotycząca bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa i działalność państwa w obszarze prawa karnego.

Przepis art. 15 ust. 1 dyrektywy o e-prywatności stanowi:

> 1. Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej (...). W tym celu Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej.

Spośród przytoczonych przepisów art. 5 dyrektywy o e-prywatności nakazuje państwom członkowskim zapewnienie poufności komunikacji, art. 6 – niezwłoczne usuwanie lub anonimizację danych o ruchu w sieci, art. 8 reguluje oferowanie użytkownikowi wyświetlania i ograniczenie identyfikacji rozmów przychodzących i wychodzących, art. 9 zaś – ograniczenie przetwarzania danych o lokalizacji. Art. 15 ust. 1 pozwala państwom członkowskim na ograniczenie tych zasad w swoim ustawodawstwie w celu ochrony wymienionych w tym przepisie prawnie chronionych wartości związanych z bezpieczeństwem i ściganiem przestępczości. Reasumując, omawiany przepis pozwala państwom członkowskim na uregulowanie przepisami krajowymi kontroli treści przekazów telekomunikacyjnych i retencji danych dotyczących tych przekazów.

Warto zauważyć, że unieważniona przez TSUE dyrektywa retencyjna dodała do art. 15 dyrektywy o e-prywatności ust. 1b, który wskazywał, że ustępu 1 nie stosuje się do danych zatrzymywanych na jej podstawie.

Przepisy Karty Praw Podstawowych Unii Europejskiej, które TSUE wziął pod uwagę w swoim orzeczeniu, to: art. 7 (prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się), art. 8 (prawo każdej osoby do ochrony danych osobowych jej dotyczących), art. 11 (prawo do wolności wypowiedzi) i art. 52 (zakres i wykładnia praw i zasad) przewidujący, że wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą być przewidziane ustawą, szanować istotę tych praw i wolności oraz mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

W orzeczeniu TSUE, które jest tematem niniejszego artykułu, wskazano, że przepis art. 15 dyrektywy o e-prywatności należy interpretować w ten sposób, że:

[7] Dyrektywa o e-prywatności odsyła do traktatów europejskich w brzmieniu sprzed wejścia w życie *Traktatu z Lizbony*.

1) stoi na przeszkodzie uregulowaniom krajowym, w których przewidziano uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej – do celów zwalczania przestępczości,
2) stoi na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a zwłaszcza dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby te dane były przechowywane na obszarze Unii

Najważniejszą tezą wyroku jest stwierdzenie przez TSUE, że państwa członkowskie nie mogą nakładać na dostawców usług komunikacji elektronicznej ogólnego obowiązku retencji danych. Prawo UE nie pozwala na ogólną i nieselektywną retencję danych o ruchu i danych dotyczących lokalizacji. Państwa członkowskie mogą jednak przyjmować przepisy przewidujące ukierunkowaną retencję tego rodzaju danych wyłącznie w celu zwalczania poważnej przestępczości, przy założeniu, że te przepisy ograniczają kategorie danych podlegających retencji, objęte nimi środki komunikacji i osoby oraz okres retencji danych do tego, co jest niezbędne dla osiągnięcia celu tych przepisów. Dostęp właściwych organów narodowych do danych podlegających retencji musi być poddany określonym warunkom, w tym ocenie sądu lub niezależnego organu administracyjnego.

2. Geneza orzeczenia – sprawa *Digital Rights Ireland*

Omawiane orzeczenie należy rozpatrywać w kontekście konsekwencji wynikających z wyroku *Digital Rights Ireland i inni* CV-293/12 i C-594/12 z 2014 r.[8], w którym TSUE orzekł o nieważności dyrektywy retencyjnej z uwagi na to, że dopuszczony przez nią stopień ingerencji w prawa i wolności gwarantowane zarówno przez pierwotne, jak i wtórne źródła prawa UE – związany z ogólnym obowiązkiem retencji danych o ruchu i danych dotyczących lokalizacji – nie był ograniczony do tego, co niezbędnie konieczne do osiągnięcia celu tego rodzaju regulacji. Zasadniczym celem wyżej wymienionego aktu prawnego była harmonizacja przepisów państw członkowskich w dziedzinie zatrzymywania danych wytwarzanych lub przetwarzanych przez dostawców ogólnie dostępnych usług komunikacji elektronicznej lub publicznych sieci łączności. Przepisy dyrektywy nakazywały zapewnienie organom ścigania dostępu do powyższych danych zarówno do celów zapobiegania poważnym przestępstwom, takim jak przestępczość zorganizowana i terroryzm, jak i do celów dochodzenia, wykrywania i ścigania takich przestępstw. Nakazywały również przyjęcie środków nakładających na dostawców usług telekomunikacyjnych na terenie Unii Europejskiej obowiązek zatrzymywania danych o ruchu i lokalizacji oraz powiązanych danych niezbędnych do identyfikacji abonenta lub użytkownika.

W wyniku procesu implementacji dyrektywy do krajowych porządków prawnych wdrożono rozwiązania ustawowe stanowiące podstawę prawną do przechowywania przez operatorów telekomunikacyjnych danych o połączeniach telefonicznych obywa-

[8] LEX nr 1444266.

teli UE (m.in. danych o ruchu w sieci, danych lokalizacyjnych) oraz podstawę dostępu do tych danych przez sądy, organy ścigania i służby specjalne państw członkowskich.

Trybunał przeprowadził badanie przepisów dyrektywy w dwóch aspektach: w zakresie naruszenia praw podstawowych do poszanowania życia prywatnego i ochrony danych podstawowych oraz pod kątem zgodności regulacji prawnych zawartych w dyrektywie z zasadą proporcjonalności.

W omawianym wyroku TSUE uznał, że nakładając obowiązek zatrzymywania danych i umożliwiając dostęp do nich właściwym organom krajowym, dyrektywa zbyt mocno ingerowała w prawa podstawowe do poszanowania życia społecznego i do ochrony danych osobowych. Ponadto, zdaniem Trybunału, okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych było dokonywane bez poinformowania o tym abonenta i zarejestrowanego użytkownika, może wywołać u zainteresowanych osób poczucie, że ich życie prywatne podlega stałemu nadzorowi.

Jednakże biorąc pod uwagę to, że przepisy dyrektywy nie zezwalały na zapoznawanie się z treścią komunikatów elektronicznych jako taką i nakazywały dostawcom usług i sieci przestrzeganie określonych zasad ochrony i bezpieczeństwa danych, Trybunał uznał, że przewidziane przepisami dyrektywy zatrzymywanie danych nie naruszało zasadniczej treści praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych. Ponadto Trybunał przyznał, że zatrzymanie danych w celu ich ewentualnego udostępnienia właściwym organom krajowym rzeczywiście odpowiadało celowi w postaci interesu ogólnego, jakim jest zwalczanie poważnej przestępczości, a w konsekwencji – zapewnienie bezpieczeństwa wewnętrznego.

Zdaniem TSUE prawodawca Unii, przyjmując dyrektywę retencyjną, przekroczył jednak granice, które wyznacza poszanowanie zasady proporcjonalności. Trybunał zauważył, że przy uwzględnieniu znaczącej roli, jaką odgrywa ochrona danych osobowych w odniesieniu do prawa podstawowego do poszanowania życia prywatnego, oraz zakresu i znaczenia ingerencji w to prawo, do której prowadziła dyrektywa, uprawnienia dyskrecjonalne prawodawcy Unii powinny być ograniczone, do tego, co ściśle niezbędne. Powyższy warunek nie został jednak spełniony w przypadku omawianego aktu prawnego.

Trybunał stwierdził ponadto, że zapisy dyrektywy nie przewidywały żadnego kryterium gwarantującego, że właściwe organy krajowe, które miałyby dostęp do danych, będą je wykorzystywać wyłącznie do zapobiegania przestępstwom, uważanym – w świetle zakresu i znaczenia ingerencji w omawiane prawa podstawowe – za wystarczająco poważne, by uzasadnić taką ingerencję. Przeciwnie, dyrektywa ograniczała się do odesłania w sposób ogólny do pojęcia p o w a ż n e p r z e s t ę p s t w a, zdefiniowanych przez każde państwo członkowskie w prawie krajowym, co, zdaniem Trybunału, było niewystarczające.

Dyrektywa nie przewidywała również materialnych i proceduralnych przesłanek dostępu właściwych organów do danych podlegających retencji. Dostęp do danych nie został podporządkowany uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Trybunał uznał, że dyrektywa nie przewidywała wystarczających gwarancji umożliwiających zapewnienie skutecznej ochrony danych przed niebezpieczeństwem nadużycia oraz przed jakimkolwiek dostępem do danych i ich wykorzystywaniem w sposób niedozwolony.

Trybunał wskazał również, że dyrektywa przewidywała okres co najmniej sześciu miesięcy na zatrzymanie danych, przy czym nie przeprowadzała jakiegokolwiek rozróżnienia między kategoriami danych w zależności od zainteresowanych osób lub ewentu-

alnej użyteczności danych w stosunku do zakładanego celu. Ponadto, okres ten wynosił od co najmniej sześciu do dwudziestu czterech miesięcy, przy braku obiektywnych kryteriów, na podstawie których należało ustalić okres zatrzymywania, aby zagwarantować jego ograniczenie do tego, co ściśle niezbędne.

Wydanie przez TSUE wskazanego orzeczenia nie miało bezpośredniego skutku dla obowiązywania przepisów krajowych państw członkowskich przewidujących obowiązek retencji danych, wydanych w celu implementacji unieważnionej dyrektywy. Dlatego pojawiły się wątpliwości co do tego, czy uznanie dyrektywy za nieważną oznacza powrót do możliwości samodzielnego regulowania tych zagadnień przez państwa członkowskie. Państwa członkowskie pozostawały jednak związane Kartą Praw Podstawowych, a łącznikiem uzasadniającym jej stosowanie był art. 15 dyrektywy o e-prywatności określający zakres dopuszczalnych wyjątków od poufności w komunikacji elektronicznej[9].

Określenie przez Trybunał elementów wzorca zgodności z Kartą Praw Podstawowych, który, jego zdaniem, naruszała unieważniona dyrektywa, stworzyło poręczne argumenty do kwestionowania uregulowań krajowych dotyczących retencji danych telekomunikacyjnych.

3. Stan faktyczny

Jedną z konsekwencji powyższego orzeczenia było skierowanie przez sądy Szwecji i Wielkiej Brytanii niezależnych od siebie wniosków o wydanie orzeczenia w trybie prejudycjalnym, w celu ustalenia, czy na dostawcach usług elektronicznych w dalszym ciągu spoczywa obowiązek retencji danych wynikający z unieważnionej dyrektywy.

Po wydaniu orzeczenia *Digital Rights* szwedzkie przedsiębiorstwo telekomunikacyjne Tele2 poinformowało miejscowy Urząd Pocztowy i Telekomunikacyjny, że nie zamierza prowadzić dalej retencji danych oraz że dokona zniszczenia danych uzyskanych w okresie poprzedzającym wydanie wyroku (sprawa C-203/15)[10]. Należy wspomnieć, że szwedzki system prawny nakładał na dostawców usług elektronicznych obowiązek systematycznego i ciągłego zatrzymywania danych o ruchu i danych dotyczących lokalizacji wszystkich abonentów oraz zarejestrowanych użytkowników w odniesieniu do wszelkich środków komunikacji elektronicznej, bez żadnych wyjątków, oraz przechowywania ich przez sześć miesięcy[11].

Pytanie prejudycjalne w sprawie C-689/15 jest konsekwencją rozpatrywanego przez Sąd Najwyższy Anglii i Walii wniosku o ocenę legalności sekcji 1 tzw. ustawy DRIPA[12], w którym podniesiono m.in. że ta ustawa jest niezgodna z art. 7, 8 Karty Praw Podstawowych i z art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Zaskarżone przepisy DRIPA upoważniały sekretarza stanu w Departamencie Spraw Wewnętrznych do żądania od publicznych operatorów telekomunikacyjnych retencji ww. danych, z wyłączeniem treści komunikacji.

---

[9] A. Grzelak, *Glosa do wyroku TS z dnia 21 grudnia 2016 r. C-203/15 oraz C-698/15. Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności*, „Europejski Przegląd Sądowy" 2017, nr 3, s. 31–36, LEX nr 316663.

[10] Teza 44 orzeczenia C-203/15, LEX nr 2202679.

[11] Tezy 15–19 orzeczenia C-203/15.

[12] *The Data Retention and Investigatory Powers Act 2014* – ustawa Parlamentu Zjednoczonego Królestwa, która uzyskała Sankcję Królewską 17 VII 2014 r., po uchwaleniu 14 VII 2014 r. Celem ustawy było zapewnienie służbom bezpieczeństwa dostępu do danych telekomunikacyjnych i internetowych wobec unieważnienia tzw. dyrektywy retencyjnej przez Trybunał Sprawiedliwości Unii Europejskiej, uchylonej i zastąpionej 31 XII 2016 r. przez ustawę I*nvestigatory Powers Act*.

Na podstawie wniosków o wydanie orzeczenia w trybie prejudycjalnym złożonych przez sądy szwedzki i brytyjski, TSUE został zobowiązany do udzielenia odpowiedzi na pytanie, czy przepisy prawa krajowego nakładające na operatorów telekomunikacyjnych ogólny obowiązek nieselektywnej retencji danych – zezwalające na dostęp do tych danych właściwym organom narodowym, jeżeli obowiązek ten nie jest ograniczony wyłącznie do zwalczania poważnej przestępczości – są zgodne z prawem Unii Europejskiej, zwłaszcza z dyrektywą 2002/58 dotyczącą prywatności w sektorze łączności elektronicznej, interpretowaną w świetle Karty Praw Podstawowych UE[13].

4. Główne tezy orzeczenia

Trybunał stwierdził w wyroku, że prawo UE nie pozwala na przyjmowanie przepisów prawa krajowego przewidujących ogólny obowiązek nieselektywnej retencji danych. Zgodnie z argumentacją Trybunału ingerencja w prawa i wolności gwarantowane przez system prawa UE, wynikająca z obowiązywania tego rodzaju przepisów, ma niezwykle poważny charakter. Z tego względu taką ingerencję może uzasadniać wyłącznie cel, jakim jest zwalczanie poważnej przestępczości[14].

Trybunał podkreślił również, że podlegające jego ocenie przepisy krajowe przewidujące powyższy obowiązek nie wymagają, aby istniał jakikolwiek związek między danymi podlegającymi retencji a zagrożeniem bezpieczeństwa publicznego i nie jest on ograniczony do zatrzymywania danych dotyczących określonego okresu, miejsca czy osób, o których można sądzić, że są powiązane z usiłowaniem dokonania, przygotowywaniem lub dokonywaniem poważnego przestępstwa. W konsekwencji, normy tego rodzaju wykraczają poza zakres tego, co jest absolutnie konieczne i może być uznane za uzasadnione w demokratycznym społeczeństwie, jak wymaga tego dyrektywa 2002/58 interpretowana w świetle Karty Praw Podstawowych[15].

W ocenie Trybunału nie powinno budzić wątpliwości to, że dyrektywa o e-prywatności nie stoi na przeszkodzie funkcjonowaniu w krajowych porządkach prawnych przepisów nakładających na operatorów telekomunikacyjnych obowiązek ukierunkowanej retencji dla celów zwalczania poważnej przestępczości, pod warunkiem że zawiera ona odpowiednie ograniczenia powodujące, że zakres zatrzymywania danych jest zawężony do tego, co absolutnie konieczne dla realizacji tego celu[16].

W odniesieniu do dostępu właściwych organów narodowych do danych retencyjnych Trybunał potwierdził, że właściwe przepisy prawa krajowego nie mogą ograniczać się do stwierdzenia, że dostęp jest uzasadniony jednym z celów wskazanych w dyrektywie, nawet gdy tym celem jest zwalczanie poważnej przestępczości. Podstawą tych przepisów muszą być obiektywne kryteria w celu dokładnego określenia, w jakich okolicznościach i na jakich warunkach uprawnione organy mogą uzyskać dostęp do danych podlegających retencji[17].

Dostęp uprawnionych organów do danych, z wyjątkiem szczególnie pilnych przypadków, powinien podlegać uprzedniej kontroli niezależnego organu administracyjnego

[13] Orzeczenie C-203/15, tezy 51 i 59.
[14] Tamże, teza 102.
[15] Tamże, tezy 105–107.
[16] Tamże, teza 108.
[17] Tamże, tezy 109–111.

lub sądu[18]. Właściwe organy narodowe, które uzyskały zgodę na dostęp do danych po weryfikacji przez ww. sąd lub organ, są zobowiązane do poinformowania zainteresowanej osoby o dostępie do danych retencyjnych jej dotyczących[19].

Przepisy narodowe muszą stanowić, że dane mogą być przechowywane wyłącznie na terytorium UE oraz że podlegają nieodwracalnemu zniszczeniu po upływie okresu retencji[20].

5. Skutki wyroku TSUE wydanego w trybie prejudycjalnym dla prawa krajowego państw członkowskich

Zgodnie z art. 19 ust. 3 lit. b *Traktatu o Unii Europejskiej* (dalej: TUE) TSUE orzeka w trybie prejudycjalnym (wydaje tzw. *preliminary ruling*) na wniosek sądów państw członkowskich, w sprawie wykładni prawa Unii lub ważności aktów przyjętych przez instytucje. Wymieniona kompetencja została doprecyzowana w art. 267 *Traktatu o Funkcjonowaniu Unii Europejskiej*, zgodnie z którym TSUE jest właściwy do orzekania w trybie prejudycjalnym o wykładni traktatów oraz o ważności i wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii Europejskiej. Co istotne – postępowanie o wydanie orzeczenia w trybie prejudycjalnym z art. 267 nie jest ani powództwem, ani skargą. Stanowi ono formę współpracy między sądem krajowym państwa członkowskiego, przed którym toczy się postępowanie w sprawie, a TSUE[21]. Powyższe oznacza, że bieg tego postępowania określa zarówno prawo UE, jak i przepisy proceduralne państwa członkowskiego, którego sąd rozstrzyga daną sprawę.

Jednocześnie należy dodać, że w związku z tym, że w świetle art. 267 akapit 1 lit. b TFUE sąd krajowy może zwracać się z wnioskiem o dokonanie wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii, to najczęściej przedmiotem wykładni są akty prawne wymienione w art. 288 TFUE, czyli rozporządzenia, dyrektywy i decyzje, łącznie z niewiążącymi opiniami i zaleceniami, gdyż i one mogą mieć znaczenie dla wykładni i stosowania prawa przez organy krajowe.

Niniejszy wyrok (w sprawach połączonych C-203/15 *Tele2 Sverige AB/Post-ochtelestyrelsen* i C-698/15 *Secretary of State for the Home Departament/Tom Watson i inni*) zapadł na skutek pytań prejudycjalnych skierowanych właśnie w trybie art. 267 TFUE (a nie w trybie art. 263 TFUE, czyli skargi bezpośredniej na nieważność aktu prawa UE).

Nie budzi wątpliwości to, że orzeczenie TSUE o wykładni jest wiążące dla sądu, który zwrócił się z pytaniem prejudycjalnym. To związanie nie wynika, co prawda, z brzmienia art. 267, ale zostało jednoznacznie przesądzone w orzecznictwie TSUE (*Postanowienie Trybunału z dnia 5 marca 1986 r. w sprawie 69/85 Wünsche*, pkt 13)[22]. Obejmuje ono nie tylko sąd, który zwrócił się z pytaniem, lecz także wszystkie sądy krajowe orzekające w danej sprawie (np. w wyższej instancji lub instancji ponownej).

Należy również pamiętać, że orzeczenie TSUE nie ma skutku *erga omnes*. Nie stanowi też formalnego precedensu o skutkach wykraczających poza sprawę, w związku z którą zostało wydane, i wobec osób trzecich. Skuteczność orzeczenia TSUE wynika z doktryny

[18] Tamże, teza120.
[19] Tamże, teza 121.
[20] Tamże, teza 122.
[21] M. Szpunar, *Komentarz do art. 267 Traktatu o funkcjonowaniu Unii Europejskiej,* w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz,* t. 3, A. Wróbel (red.), WKP 2012, pkt 1.
[22] Tamże, pkt 9.1.

acte éclairé, która skutkuje m.in. tym, że sąd krajowy może odstąpić od przedłożenia pytania, jeżeli Trybunał rozstrzygał już w analogicznej sprawie. Jeśli sąd krajowy zada w takiej sprawie pytanie, TSUE może odesłać go do wcześniejszego orzecznictwa[23].

Wyrok w trybie prejudycjalnym TSUE po ogłoszeniu jest ostateczny i skuteczny *erga omnes*. Należy przy tym pamiętać, że orzeczenie wydane w trybie prejudycjalnym na podstawie art. 267 TFUE ma charakter wpadkowy w stosunku do postępowania toczącego się przed sądem krajowym. TSUE nie odnosi się do ważności aktów prawa krajowego (np. polskiego) ani też nie orzeka o sprzeczności prawa krajowego z prawem Unii Europejskiej. Po wyroku w trybie prejudycjalnym to sąd krajowy ustala konsekwencje prawne wynikające z prawa krajowego, mogące wiązać się ze wskazaną przez TSUE interpretacją określonych przepisów aktów prawa pochodnego UE. Powyższe odnosi się także do ustalenia na płaszczyźnie krajowej ewentualnych konsekwencji wynikających z krajowego prawa konstytucyjnego, czego powinny dokonać właściwe organy krajowe, w tym krajowe sądy konstytucyjne.

Należy również zaznaczyć, że – co do zasady – w razie uprzedniej implementacji zakwestionowanego przepisu dyrektywy do prawa krajowego państwa członkowskiego, w tym zakresie prawo krajowe implementujące dyrektywę podlega wciąż regulacjom prawa krajowego wyższego rzędu (np. normom konstytucyjnym) i nie traci *ex officio* mocy obowiązującej.

Istotny jest również aspekt skutków orzeczenia zapadłego w trybie art. 267 TFUE w odniesieniu do obowiązywania zakwestionowanych przepisów na płaszczyźnie prawa UE. Jest to o tyle istotne, że konsekwencje orzeczenia wydanego w trybie prejudycjalnym nie są tak oczywiste i jednoznaczne, jak w przypadku stwierdzenia nieważności w trybie art. 263 TFUE (czyli skargi na nieważność aktu prawa UE). W tym drugim przypadku (art. 263 TFUE) nieważny akt prawa UE przestaje automatycznie obowiązywać w systemie prawnym UE, aczkolwiek w przypadku rozstrzygnięcia na podstawie art. 267 TFUE nie ma już tak jednoznacznej interpretacji skutków prawnych na płaszczyźnie UE. Warto również wskazać, że istotą wyroku prejudycjalnego jest to, że pozostaje on wiążący nie tylko dla tego sądu krajowego, który skierował do TSUE pytanie prejudycjalne, lecz także dla każdego innego sądu krajowego tego państwa członkowskiego. Z tego wynika, że sądy krajowe mają uprawnienia, aby w toczącym się przed nimi postępowaniach uwzględnić skutki orzeczenia, które TSUE wydał w innym postępowaniu między innymi stronami.

Z samej istoty dyrektywy jako aktu prawa UE (zgodnie z art. 288 TFUE) wynika, że wymaga ona implementacji przez ustawodawcę krajowego. Tym samym należy przyjąć, że w prawie krajowym państwa członkowskiego UE istnieje akt prawny, który transponuje postanowienia dyrektywy do prawa krajowego. Wyrok TSUE w trybie prejudycjalnym nie będzie mieć więc bezpośredniego przełożenia w prawie polskim na ważność aktu prawa krajowego (np. ustawy) implementującego postanowienia danej dyrektywy. Tym samym z wyroku TSUE nie wynika bezpośrednio automatyczna nieważność aktu prawa krajowego, który transponował do krajowego porządku prawnego regulacje danej dyrektywy.

Reasumując, polski Trybunał Konstytucyjny, w świetle dotychczasowego orzecznictwa, nie uznaje pierwszeństwa prawa UE przed Konstytucją Rzeczypospolitej Polskiej (szczególnie w zakresie tych przepisów Konstytucji, które odnoszą się do ochrony praw odstawowych jednostki), co również ma znaczenie dla przedmiotowej sprawy.

[23] Tamże.

Przy rozważaniu możliwych skutków prawnych omawianego orzeczenia TSUE należy również rozważyć możliwość skorzystania na jego podstawie z mechanizmów prawnych służących ochronie osób w razie niewłaściwej implementacji dyrektywy. W świetle wyroku C-203/15 Trybunał wskazał, jaka powinna być właściwa interpretacja przepisów art. 15 ust. 1 dyrektywy 2002/58. W związku z zapadłym wyrokiem można uznać, że na płaszczyźnie prawa krajowego pojawił się problem niewłaściwej transpozycji dyrektywy 2002/58 do krajowych porządków prawnych państw członkowskich.

W takiej sytuacji należy rozważyć ewentualne konsekwencje postaci bezpośredniego skutku dyrektywy. Zgodnie z orzeczeniem w sprawie 41/74 van Duyn[24], Trybunał stwierdził wyraźnie, że wykluczenie możliwości powołania się przez jednostkę, której dyrektywa dotyczy, na wynikające z dyrektywy obowiązki państwa byłoby nie do pogodzenia z wiążącym charakterem dyrektywy wynikającym z art. 288 zdanie 3 TFUE.

Co do zasady – dyrektywa wywołuje skutki od momentu jej implementacji do prawa krajowego. W opinii Trybunału dyrektywa, która nie została implementowana do krajowego porządku prawnego może powodować określone skutki, jeżeli:

a) implementacja do prawa krajowego nie została dokonana lub została dokonana w sposób niewłaściwy,
b) przepisy dyrektywy mają charakter bezwarunkowy oraz są dostatecznie jasne i precyzyjne,
c) przepisy dyrektywy nadają określone prawa osobom.

Po spełnieniu tych warunków osoby mogą powoływać się na dyrektywę w postępowaniu przeciwko państwu przed sądem krajowym. Niemożliwe jest dochodzenie roszczeń przeciwko innym osobom w związku z jej bezpośrednią skutecznością, jeżeli dyrektywa nie została implementowana (wyrok C-91/92 Paola Faccini Dori v Recreb Srl z 14 czerwca 1994 r.).

Trybunał dopuszcza, pod pewnymi warunkami, uzyskanie odszkodowania za szkody wynikłe w związku z niewłaściwą lub opóźnioną implementacją dyrektywy (wyrok C-6/90 i C-9/90 Francovich i Bonifaci z 19 listopada 1991 r.).

6. Polskie przepisy o retencji danych telekomunikacyjnych a tezy orzeczenia Tele2

Obowiązujące w Polsce przepisy dotyczące retencji danych telekomunikacyjnych, tj. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*[25] (dalej: „Pt"), zostały do tej ustawy wprowadzone na mocy *Ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*[26], wydanej w celu implementacji do polskiego porządku prawnego postanowień dyrektywy retencyjnej. Siłą rzeczy polskie przepisy zawierają rozwiązania odpowiadające przepisom tej dyrektywy zakwestionowanej przez TSUE w wyroku wydanym przez TSUE w sprawie *Digital Rights Ireland*.

Artykuł 180a ust. 1 pkt 1 Pt nakłada na operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych obowiązek zatrzymywania i przechowywania przez 12 miesięcy – licząc od dnia połączenia lub nieudanej próby połączenia – danych określonych w art. 180c Pt, generowanych w sieci telekomunikacyjnej. Zgodnie natomiast z art. 180c ust. 1 obowiązkiem określo-

[24] LEX nr 84379.
[25] T.j. Dz.U. z 2016 r. poz. 1489, ze zm.
[26] Dz.U. z 2009 r. nr 85 poz. 716.

nym w art. 180a ust. 1 są objęte dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz do którego jest kierowane połączenie, a także dane niezbędne do określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia oraz lokalizacji telekomunikacyjnego urządzenia końcowego. Jednocześnie w ust. 2 art. 180c Pt zawarto upoważnienie dla ministra właściwego do spraw informatyzacji do określenia, w formie rozporządzenia wydanego w porozumieniu z ministrem właściwym do spraw wewnętrznych, szczegółowego wykazu danych określonych w ust. 1 oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych. Czynnikami, które organ wydający rozporządzenie jest zobowiązany wziąć pod uwagę, są: rodzaj wykonywanej działalności telekomunikacyjnej przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych, dane określone w ust. 1, koszty pozyskania i utrzymania danych oraz potrzeba unikania wielokrotnego zatrzymywania i przechowywania tych samych danych. Nie można zatem ustanowić na podstawie rozporządzenia generalnych wyłączeń spod obowiązku retencji danych telekomunikacyjnych. Na podstawie przedmiotowej delegacji ustawowej zostało wydane *Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania*[27]. Niniejsze rozporządzenie wyłączyło z obowiązku retencji jedynie dwie kategorie operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych: prowadzących działalność polegającą wyłącznie na dostarczaniu udogodnień towarzyszących oraz rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych lub telewizyjnych.

Należy zatem stwierdzić, że retencja danych telekomunikacyjnych w Polsce ma charakter ogólny i nieselektywny, a więc przepisy art. 180a i 180c nie spełniają określonych w sentencji omawianego orzeczenia wymogów niezbędności i proporcjonalności.

Zasady dostępu właściwych służb państwowych do danych telekomunikacyjnych wraz z regułami wewnętrznej kontroli zostały ustalone przepisami *Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*[28]. Przedmiotowa ustawa wprowadziła zmiany w następujących przepisach: *Ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*[29] – art. 3–30b, *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[30] – art. 28a–28b, *Ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych* [31] – art. 6a, *Ustawie z dnia 27 sierpnia 2009 r. o Służbie Celnej*[32] – art. 75d–75da, *Ustawie z dnia 28 września 1991 r. o kontroli skarbowej*[33] – art. 36b–36bb, *Ustawie z dnia 6 kwietnia 1990 r. o Policji*[34] – art. 20c–20cb, *Ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych*[35] – art. 16 § 4a pkt 3 i art. 175b, *Ustawie z dnia 9 czerwca 2006 r.*

[27] Dz.U. Nr 226, poz. 1828.
[28] Dz.U. poz. 147.
[29] Dz.U. z 2016 r. poz. 96.
[30] Dz.U. z 2015 r. poz. 1929.
[31] Dz.U. z 2015 r. poz. 1198.
[32] Dz.U. z 2015 r. poz. 990.
[33] Dz.U. z 2015 r. poz. 553.
[34] Dz.U. z 2015 r. poz. 355.
[35] Dz.U. z 2015 r. poz. 133.

o Centralnym Biurze Antykorupcyjnym[36] – art. 18–18b, *Ustawie z dnia 12 października 1990 r. o Straży Granicznej*[37] – art. 10 b–10bb, *Ustawie z dnia 9 czerwca 2009 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[38].

Cel, w jakim jest dopuszczalne pozyskiwanie danych telekomunikacyjnych, został określony w różny sposób w poszczególnych ustawach pragmatycznych. Policja może te dane pozyskiwać, aby zapobiegać lub wykrywać przestępstwa, ratować życie lub zdrowie ludzkie bądź wspierać działania poszukiwawcze lub ratownicze. Dotyczy to również Żandarmerii Wojskowej. Straż Graniczna jest ograniczona do zapobiegania bądź wykrywania przestępstw, Służba Celna natomiast – do zapobiegania lub wykrywania przestępstw skarbowych (podobnie Kontrola skarbowa).

Agencja Bezpieczeństwa Wewnętrznego może te dane uzyskiwać, jeśli są jej niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW. Równie szerokie uprawnienia do pozyskiwania danych telekomunikacyjnych, obejmujące całość zadań ustawowych danej służby, polski ustawodawca przyznał Centralnemu Biuru Antykorupcyjnemu oraz Służbie Kontrwywiadu Wojskowego.

Wykonując wytyczne zawarte w wyroku Trybunału Konstytucyjnego K 23/11, wśród których znalazł się postulat wprowadzenia mechanizmu niezależnej kontroli nad wykorzystaniem przez służby właściwe w zakresie przeciwdziałania i zwalczania przestępczości danych telekomunikacyjnych, polski ustawodawca wprowadził do ustaw pragmatycznych poszczególnych służb, a także do przepisów ustrojowych sądów powszechnych i sądów wojskowych, regulacje dotyczące kontroli wykorzystania danych telekomunikacyjnych przez sądy. Ustawą wprowadzającą te mechanizmy była ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw. Ponieważ Trybunał Konstytucyjny nie przesądził, że mechanizm kontroli nad wykorzystaniem danych telekomunikacyjnych musi mieć charakter uprzedni, polski ustawodawca zdecydował o wprowadzeniu mechanizmu następczej kontroli sądowej. Takie też zapisy znalazły się w wymienionych wyżej ustawach pragmatycznych właściwych służb, w tym Agencji Bezpieczeństwa Wewnętrznego. Kontrola jest sprawowana przez sąd okręgowy, któremu wskazany w ustawie organ przesyła w okresach półrocznych sprawozdania obejmujące liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o te dane.

Według TSUE kontrola sądu lub innego niezależnego organu nad wykorzystaniem przez odpowiednie służby danych retencyjnych powinna mieć jednak charakter uprzedni.

Zgodnie z treścią art. 180a ust. 1 Pt operatorzy publicznych sieci telekomunikacyjnych i dostawcy publicznie dostępnych usług telekomunikacyjnych są obowiązani przechowywać dane telekomunikacyjne, podlegające obowiązkowi retencji na terytorium Rzeczpospolitej Polskiej, a zatem wymóg przechowywania danych wyłącznie na terytorium UE został spełniony.

7. Podsumowanie. Wnioski *de lege ferenda*

Wydając przedmiotowe orzeczenie, TSUE uznał, że mimo wcześniejszego stwierdzenia nieważności tzw. dyrektywy retencyjnej uregulowanie retencji danych telekomunikacyjnych pozostaje objęte kompetencją prawodawczą Unii Europejskiej.

[36] Dz.U. z 2014 r. poz. 1402.
[37] Dz.U. z 2014 r. poz. 1402.
[38] Dz.U. z 2014 r. poz. 253.

Należy podkreślić, że to orzeczenie nie ma bezpośredniego skutku w zakresie obowiązywania polskich przepisów regulujących retencję danych telekomunikacyjnych. Polskie przepisy regulujące retencję danych telekomunikacyjnych oraz dostęp do nich odpowiednich służb będą obowiązywały do momentu ich zmiany. Nie można wykluczyć, że na niniejsze orzeczenie będą się powoływały w postępowaniach sądowych podmioty zobowiązane do retencji danych telekomunikacyjnych, jeśli zechcą kwestionować nałożone na nie obowiązki, bądź też podmioty tych danych uznające, że państwo polskie narusza ich prawa. Jest możliwe, że w takiej sytuacji polski sąd zada pytanie prawne Trybunałowi Konstytucyjnemu w trybie art. 193 Konstytucji, a ten wydając orzeczenie, może wziąć pod uwagę zgodność polskich przepisów o retencji danych telekomunikacyjnych z prawem europejskim, stosownie do art. 9 Konstytucji (*Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego*), biorąc pod uwagę tezy orzeczenia TSUE C-203/15 i C-698/15.

W przypadku gdy polskie przepisy dotyczące retencji danych telekomunikacyjnych nie ulegną zmianie, będzie istniało potencjalnie niebezpieczeństwo pozwania Polski przed TSUE przez Komisję bądź inne państwo członkowskie z powodu naruszenia przez nasz kraj zobowiązań ciążących na nim na mocy traktatów. Należy jednak zważyć, że w chwili obecnej problem niezgodności krajowych przepisów dotyczących retencji danych telekomunikacyjnych z prawem europejskim, w świetle wytycznych zawartych w omawianym orzeczeniu, dotyczy nie tylko Polski, lecz także większości państw członkowskich Unii Europejskiej. Taka perspektywa wydaje się zatem dość odległa.

W swojej glosie do niniejszego orzeczenia Agnieszka Grzelak podnosi jednak, że:

> Ponieważ wyrok TS nie pozostawia wątpliwości, że przepisy ustaw regulujących dostęp organów do danych (telekomunikacyjnych – przyp. aut.) leżą w zakresie zastosowania prawa unijnego w rozumieniu art. 51 Karty, zarówno ustawa inwigilacyjna, jak i inne ustawy regulujące dostęp do danych muszą zostać jak najszybciej zbadane w formalnych procedurach pod kątem zgodności z prawem unijnym, z uwzględnieniem wykładni poczynionej w sprawie Tele2. System retencji i udostępniania danych, uregulowany przepisami prawa telekomunikacyjnego, oraz ustaw regulujących dostęp właściwych organów do tych danych wymaga daleko idących zmian, uwzględniających wnioski płynące z wyroków Trybunału Sprawiedliwości w sprawach *DRI* i *Tele2*. Konieczność analizy, weryfikacji i zmiany regulacji krajowych odnoszących się do przechowywania danych jest konieczna, a długotrwały brak reakcji ze strony danego państwa członkowskiego może skutkować reakcją Komisji Europejskiej, która, jako strażnik Traktatów, ma obowiązek monitorowania zgodności prawa krajowego z prawem UE. W sytuacji wątpliwości, Komisja może wszcząć procedurę zmierzającą do weryfikacji naruszenia na podstawie art. 259 Traktatu o funkcjonowaniu Unii Europejskiej[39].

W chwili obecnej rozważenia wymaga to, czy sytuacja spowodowana orzeczeniem TSUE w sprawie Tele 2 wymaga od polskiego ustawodawcy inicjatywy mającej na celu dostosowanie polskiego prawodawstwa do tez niniejszego orzeczenia czy też Polska powinna czekać na inicjatywę ustawodawczą na szczeblu unijnym. Każde z tych rozwiązań ma pewne wady i zalety.

[39] A. Grzelak, *Glosa do wyroku TS z dnia 21 grudnia 2016 r. C-203/15 oraz C-698/15*…

W dniu 10 stycznia 2017 r. rozpoczęły się prace nad rozporządzeniem w sprawie prywatności i łączności elektronicznej mającym zastąpić dyrektywę 2002/58/WE[40], której interpretacja przepisów stała się podstawą orzeczenia Tele2. W tej sytuacji podejmowanie przez polskiego ustawodawcę inicjatywy legislacyjnej w obszarze retencji danych mogłoby się okazać przedwczesne, ponieważ przyjęte teraz przepisy mogłyby okazać się sprzeczne z nowym rozporządzeniem. Wymaga przy tym podkreślenia, że przedstawiony przez Komisję Europejską projekt zawiera podobne jak dyrektywa o e-prywatności wyłączenie z zakresu przewidzianych jego przepisami gwarancji poufności danych telekomunikacyjnych. Tę rolę odgrywa artykuł 11 ust. 1:

> Zakres zobowiązań i praw przewidzianych w art. 5–8 można ograniczyć w drodze środka legislacyjnego w ramach prawa Unii lub prawa krajowego, w sytuacji gdy takie ograniczenie odbywa się z poszanowaniem istoty podstawowych praw i wolności oraz gdy jest to środek konieczny, właściwy i proporcjonalny w demokratycznym społeczeństwie do zabezpieczenia jednego interesu publicznego lub wielu interesów publicznych, o których mowa w art. 23 ust. 1 lit. a)–e) rozporządzenia (UE) 2016/679 lub realizacji funkcji monitorowania, inspekcji lub regulacji w związku z wykonywaniem władzy publicznej na potrzeby takich interesów.

Powyższy przepis nie definiuje nawet bezpośrednio, tak jak czyniła to dyrektywa e-prywatnosci, prawnie chronionych interesów, które uzasadniają ograniczenie zawartych w danym akcie prawnym gwarancji praw podmiotu danych, lecz odsyła w tym zakresie do stosownego przepisu rozporządzenia ogólnego o ochronie danych osobowych. Należy dodać, że w zakresie interesów uzasadniających ograniczenie praw podmiotu danych, skatalogowanych w art. 23 ust. 1 lit. a)–e) rozporządzenia (UE) 2016/679 uwzględniono bezpieczeństwo narodowe, obronność, bezpiczeństwo publiczne i zapobieganie przestępczości. Trudno jednak oczekiwać, aby TSUE uznał, że tak sformułowane wyłączenie z gwarancji praw podmiotu danych telekomunikacyjnych mogło być interpretowane szerzej, niż to wynikające z art. 15 ust. 1 dyrektywy o e-prywatności.

Należy zatem uznać, że przed polskim ustawodawcą stoi wyzwanie w postaci dostosowania przepisów o retencji danych telekomunikacyjnych i dostępie do nich uprawnionych podmiotów do standardów zgodności z Kartą Praw Podstawowych, określonych przez TSUE w orzeczeniu Tele2.

Niezależnie od sposobu takiego dostosowania jest pewne, że ograniczy ono możliwość pozyskiwania danych telekomunikacyjnych przez uprawnione podmioty i tym samym nie wpłynie korzystnie na efektywność pracy operacyjnej organów policyjnych i służb specjalnych. Działania ustawodawcy muszą być nakierowane na zminimalizowanie ewentualnych szkód dla pracy wykrywczej służb powołanych do zwalczania przestępczości przez takie działania dostosowawcze.

Bez wątpienia dostosowanie polskiego prawa do standarów orzeczania Tele2 oznaczałoby konieczność organiczenie zakresu przedmiotowego możliwości korzystania przez uprawnione podmioty z danych telekomunikacyjnych. Trybunał stoi na stanowisku, że wykorzystywanie tego typu danych powinno być ograniczone do zwalczania

[40] Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 [dostęp: 23 IX 2017].

poważnej przestępczości. Jak wskazano, niektóre z polskich służb mogą występować o przekazanie danych telekomunikacyjnych również w innych celach. Należałoby rozważyć pozostawienie możliwości tego rodzaju danych również w celu rozpoznawania i zwalczania zagrożeń dla bezpieczeństwa państwa, mając na uwadze, że bezpieczeństwo narodowe znajduje się w sferze wyłącznej odpowiedzialności państw członkowskich. Tak więc Unia Europejska, jej prawo i instytucje nie powinny ingerować w działania państwa podejmowane w tym obszarze.

Konieczne byłoby również poddanie wniosków uprawnionych podmiotów o udostępnienie danych telekomunikacyjnych uprzedniej kontroli niezależnego organu. Do decyzji ustawodawcy będzie należało, czy tym organem będzie sąd, prokurator czy inny niezależny organ, być może w tym celu powołany.

W uzasadnieniu do omawianego wyroku TSUE wspomniał również o zasadności wprowadzenia obowiązku notyfikacyjnego: właściwe organy ochrony bezpieczeństwa i proządku publicznego, które korzystały z dostępu do danych podlegajacych retencji, powinny poinformować zainteresowane osoby, zgodnie z właściwymi przepisami krajowymi, gdy tylko udzielenie tego rodzaju informacji nie będzie już stanowiło potencjalnego zagrożenia dla prowadzonych przez nie czynności. To, zdaniem Trybunału, jest niezbędne do umożliwienia tym osobom skorzystania z prawa do wniesienia środka zaskarżenia. Co istotne – TSUE nie odniósl się do istnienia tego obowiazku w sentencji wyroku, a jedynie w jednym z motywów uzasadnienia.

Najtrudniejsze do praktycznej realizacji byłoby wprowadzenie selektywnej w miejsce generalnej retencji danych telekomunikacyjnych. Powyższe wynika między innymi ze wskazania przez TSUE, że krajowe instrumenty prawne dotyczące danych telekomunikacyjnych – obejmujace swym zakresem, w sposób uogólniony, wszystkich abonentów i zarejestrowanych użytkowników oraz wszystkie środki łącznosci elektronicznej, jak również dane o ruchu – powinny przewidywać zróżnicownie oraz ograniczenia w zależności od tego, jakiemu celowi mają służyć[41]. Jednocześnie TSUE wskazuje, że musi istnieć związek między danymi podlegającymi retencji a zagrożeniem bezpieczeństwa publicznego. Ponadto TSUE określa, że retencja danych powinna być ograniczona przez zastosowanie:

- kryterium przedmiotowego,
- kryterium podmiotowego,
- kryterium geograficznego,
- kryterium czasowego[42].

Kryterium przedmiotowe odnosi się do wskazania, że retencja ma istotne znaczenie dla ochrony bezpieczeństwa publicznego lub może mieć istotne znaczenie dla zwalczania poważnych przestępstw.

Kryterium podmiotowe oznacza, że retencja może znaleźć zastosowanie wobec tych osób, co do których istnieją poważne przesłanki mogące sugerować, że ich zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami lub z określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, lub z osobami, których zatrzymane dane mogłyby z innych powodów przyczynić się do zapobiegania, wykrywania lub ścigania poważnych przestępstw.

Kryterium geograficzne wskazuje, że zatrzymywane dane powinny być związane z określonym obszarem geograficznym.

[41] Orzeczenie C-203/15, teza 105.

[42] Tamże, teza 106.

Kryterium czasowe określa, że zatrzywane dane powinny być związane z określonym okresem.

Należy wskazać, ze literalne zastosowanie wskazanych kryteriów w prawie krajowym zbliżyłoby metodologię retencji danych do kontroli operacyjnej. Dotyczyłaby ona tylko danych telekomunikacyjnych wygenerowanych od momentu zarządzenia stosowania retencji. Niemożliwe byłoby sięgnięcie przez uprawniony podmiot do danych historycznych, ponieważ te dane nie byłyby zatrzymywane i nie istniałyby już w momencie złożenia wniosku o ich udostępnienie, chyba że byłyby przechowywane przez operatora telekomunikacyjngo do innych celow. Taka sytuacja przyniosłaby nieoszacowane szkody pracy wykrywczej służb powołanych do zwalczania przestępczości. Dlatego rozważenia wymaga to, czy nie byłoby zgodne z określonymi przez TSUE standardami utrzymanie obowiązku retencji danych telekomunikacyjnych, z jednoczesnym ograniczeniem dostępu do nich uprawnionych podmiotów, na podstawie kryteriów przedmiotowych, podmiotowych i czasowych, z równoczesnym stworzniem mechanizmu uprzedniej kontroli nieznależnego organu nad sięganiem przez nie po te dane.

Ten problem wymaga dalszych pogłębionych analiz. Wypracowane ostateczne rozwiazanie musi uwzgledniać zarówno potrzebę ochrony prawa jednostki do prywatności, gwarantowaną w prawie Unii Europejskiej, jak i możliwość zagwarantowania jednostce innych podstawowych praw. Dotyczy to m.in. praw gwarantowanych przez Kartę Praw Podstawowych Unii Europejskiej, jak prawo do życia (art. 2 ust. 1), integralność fizyczna (art. 3 ust. 1), bezpieczeństwo osobiste (art. 6) i nienaruszalność mienia (art. 17 ust. 1), których nie da zagwaratnować się bez umożliwienia organom odpowiedznialnym za bezpieczeństwo publiczne i bezpieczeństwo państwa skutecznej realizacji ich ustawowych obowiązków.

Piotr Chorbot
Mateusz Wieczerza

Analiza dotycząca prawnomiędzynarodowych i krajowych podstaw reagowania na zdarzenia CBRN

Wprowadzenie

Na podstawie analizy aktów prawa międzynarodowego i krajowego można przyjąć, że pod pojęciem zdarzenie CBRN należy rozumieć przypadki nieuprawnionego wejścia w posiadanie, użycia lub jakiejkolwiek innej formy posłużenia się materiałami chemicznymi, biologicznymi lub jądrowymi stwarzającymi zagrożenie bezpieczeństwa albo niekontrolowane uwolnienie tego rodzaju substancji lub materiałów. Normy prawne dotyczące szczegółowych zasad i trybu reagowania na zdarzenia CBRN są regulowane przez przepisy prawa krajowego. System prawa międzynarodowego nie zawiera aktów prawnych odnoszących się wprost do problemu reagowania na powyższe zdarzenia. Zobowiązania państw na płaszczyźnie prawnomiędzynarodowej dotyczą w głównej mierze następujących elementów:

- zagwarantowania odpowiedniego poziomu bezpieczeństwa materiałów jądrowych, chemicznych lub biologicznych;
- obowiązku wymiany informacji o zdarzeniach, które mogą zagrażać bezpieczeństwu;
- implementacji przepisów dotyczących rozbrojenia i nieproliferacji broni masowego rażenia;
- zobowiązania do penalizacji określonych czynów zagrażających bezpieczeństwu, związanych z bezprawnym posługiwaniem się materiałami jądrowymi, chemicznymi lub biologicznymi, na mocy prawa krajowego.

Należy zatem uznać, że przepisy prawa międzynarodowego skupiają się na funkcji prewencyjnej, czyli na sferze zapobiegania zdarzeniom CBRN, podczas gdy domeną prawa krajowego jest wypracowanie szczegółowych norm prawno-ustrojowych precyzujących kompetencje podmiotów odpowiedzialnych za mechanizm reagowania na tego rodzaju zdarzenia, określenie szczegółowego katalogu czynności, które mają zostać podjęte w określonym wypadku, sposobu ich prowadzenia oraz innych elementów. Za jeden z wyjątków od tej zasady należy uznać przepisy *Międzynarodowej Konwencji w sprawie zwalczania aktów terroryzmu jądrowego, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 13 kwietnia 2005 r.*, zobowiązującej państwo, które posiada materiały jądrowe związane z działaniami o charakterze terrorystycznym, do podjęcia czynności zmierzających do zabezpieczenia tych materiałów oraz ich przechowywania zgodnie ze standardami ustanowionymi przez Międzynarodową Agencję Energii Atomowej – MAEA. Charakterystycznym elementem ukazującym relacje pomiędzy prawem międzynarodowym a krajowym jest opisane powyżej nałożenie na państwo określonego zobowiązania co do rezultatu i pozostawienie w dyskrecjonalnej sferze kompetencji tego państwa szczegółowego określenia sposobu, w jaki ma on zostać osiągnięty.

Zobowiązania wynikające z aktów prawa międzynarodowego opisanych w dalszej części analizy można określić jako w znacznej mierze dotyczące sfery informacyjno-koordynacyjnej. Polegają one na zobowiązaniu państw stron określonej konwencji do powiadamiania o konkretnym zdarzeniu pozostałych państw, jak również właściwych organizacji między-

narodowych (np. Międzynarodowej Agencji Energii Atomowej). Tego rodzaju mechanizmy zostały zawarte m.in. w *Konwencji o pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego* czy w *Konwencji o wczesnym powiadamianiu o wypadkach jądrowych.*

Następnym wartym podkreślenia komponentem międzynarodowych aktów prawnych dotyczących zagadnień CBRN jest ustanowienie na mocy określonej konwencji mechanizmu udzielania pomocy państwu dotkniętemu skutkami określonego zdarzenia przez organizacje międzynarodowe. Szczegółowe unormowania w tym zakresie zawiera *Konwencja o zakazie broni chemicznej*, na której mocy państwa mogą zwrócić się do Organizacji ds. Zakazu Broni Chemicznej z wnioskiem o udzielenie pomocy i wsparcia w razie wystąpienia zdarzenia związanego z czynnikami CBRN.

Biorąc pod uwagę to, że krajowe systemy reagowania na zdarzenia CBRN sprowadzają się w znacznej mierze do określenia podmiotów odpowiedzialnych za podejmowanie czynności w tym zakresie oraz zasad współdziałania tych podmiotów i podległości instytucjonalnej, podejmowanie prób harmonizacji norm prawa krajowego przez prawo międzynarodowe w tej sferze byłoby zadaniem niezwykle trudnym.

Polski system prawny nie wykazuje znaczących luk w zakresie implementacji międzynarodowych aktów prawnych dotyczących zagadnień związanych z poszczególnymi aspektami postępowania z materiałami chemicznymi, biologicznymi i jądrowymi do porządku krajowego. Za wyjątek należy uznać brak przepisów prawa krajowego wprowadzających *Konwencję o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu i bezpieczeństwie biologicznym.* **Trzeba podkreślić, że przyjęcie w tym zakresie aktu rangi ustawowej byłoby korzystne, zważywszy że analogiczna ustawa[1] została przyjęta w celu wykonania postanowień *Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów*[2].**

Należy ponadto mieć na uwadze, że istotne znaczenie z punktu widzenia realizacji ustawowych zadań ABW dotyczących zapobiegania i zwalczania terroryzmu mogą mieć obowiązki wynikające z opisanej w dalszej części analizy Rezolucji 1540 Rady Bezpieczeństwa ONZ zobowiązującej państwa do przeciwdziałania wszelkim formom posługiwania się materiałami chemicznymi, biologicznymi lub jądrowymi albo wejścia w ich posiadanie przez aktorów pozapaństwowych.

CZĘŚĆ I
Prawo międzynarodowe i europejskie

ASPEKTY ATOMOWE

1. Konwencja bezpieczeństwa jądrowego, sporządzona w Wiedniu 20 września 1994 r. (*Convention on Nuclear Safety*)

Konwencja bezpieczeństwa jądrowego stanowi najważniejszy element systemu norm prawa międzynarodowego regulujących zagadnienia związane z bezpieczeństwem

[1] *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów* (Dz.U. nr 76 poz. 812, ze zm.)

[2] Wszystkie wyróżnienia w tekście pochodzą od autora.

jądrowym, zapewnieniem odpowiednich środków technicznych i organizacyjnych mających na celu zagwarantowanie bezpiecznego eksploatowania instalacji jądrowych oraz zapobieganiem wypadkom jądrowym i minimalizacją wywołanych przez nie skutków negatywnych. Ten instrument stanowi historycznie pierwszy wiążący akt prawa międzynarodowego dotyczący bezpieczeństwa instalacji jądrowych.

Zgodnie z art. 1, celem *Konwencji* jest:

a) osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa jądrowego na świecie przez poprawę wykorzystania środków krajowych oraz współpracy międzynarodowej, w tym także współpracy technicznej związanej z bezpieczeństwem, tam gdzie jest to uzasadnione;
b) ustanowienie i utrzymanie w obiektach jądrowych skutecznych zabezpieczeń przed powstaniem potencjalnych zagrożeń radiologicznych, aby chronić poszczególne osoby, społeczeństwo i środowisko naturalne przed szkodliwymi skutkami promieniowania jonizującego pochodzącego z takich obiektów;
c) zapobieganie awariom pociągającym za sobą skutki radiologiczne oraz łagodzenie takich skutków, jeśli już powstały.

1.1. Zakres przedmiotowy

Art. 3 *Konwencji* stanowi, że jej postanowienia mają zastosowanie do bezpieczeństwa obiektów jądrowych oznaczających, zgodnie z definicją zawartą w art. 2(i), każdą położoną na lądzie cywilną siłownię jądrową podlegającą jurysdykcji jej Strony, włącznie ze znajdującymi się na tym samym terenie i bezpośrednio związanymi z eksploatacją siłowni obiektami i urządzeniami służącymi do magazynowania, przemieszczania i obróbki materiałów promieniotwórczych. Taka siłownia przestaje być obiektem jądrowym, gdy wszystkie jądrowe elementy paliwowe są na stałe usunięte z rdzenia reaktora, bezpiecznie zmagazynowane zgodnie z zatwierdzonymi procedurami i gdy organ nadzorujący zaakceptował program jej likwidacji.

1.2. Obowiązki państw stron:

- przyjęcie instrumentów prawnych, nadzorczych i administracyjnych niezbędnych do wypełnienia zobowiązań wynikających z *Konwencji* (art. 4). Ten obowiązek został doprecyzowany przez art. 7 określający zakres przedmiotowy wyżej wymienionych przepisów: mają one określać krajowe wymagania bezpieczeństwa, system udzielania zezwoleń dotyczących obiektów jądrowych, system dozorowanej inspekcji i oceny obiektów jądrowych oraz egzekwowanie stosowania właściwych przepisów i przestrzegania warunków zezwoleń;
- podjęcie odpowiednich działań w celu dokonania przeglądu i oceny bezpieczeństwa obiektów jądrowych istniejących w momencie, w którym *Konwencja* zaczęła obowiązywać w danym państwie;
- ustanowienie niezależnego organu nadzorującego, odpowiedzialnego za proces wdrażania przepisów, o których mowa w art. 7 *Konwencji*;
- podjęcie działań zmierzających do wypracowania planów postępowania w przypadku awarii, uwzględniających zarówno obszar samych obiektów jądrowych, jak i terenów poza nimi oraz określających działania, jakie będą wykonywane w razie wystąpienia awarii – rutynowo testowanych w obiektach jądrowych;

- podjęcie niezbędnych kroków mających na celu zapewnienie, że lokalizacja, sposób zaprojektowania, budowa i sposób funkcjonowania obiektu jądrowego odpowiadają zobowiązaniom wynikającym z *Konwencji*, w celu zapobiegania wypadkom, ochrony przed uwolnieniem materiałów promieniotwórczych oraz neutralizacji skutków radiologicznych ewentualnych wypadków.

Konwencja bezpieczeństwa jądrowego nie zawiera przepisów regulujących w sposób szczegółowy problem reagowania właściwych organów na zdarzenia CBRN odnoszące się do wypadków i nieprawidłowości związanych z funkcjonowaniem obiektów jądrowych. Normy wynikające z *Konwencji* mają charakter ogólny, ich zasadniczym celem jest zobowiązanie państw stron do podjęcia działań o charakterze prewencyjnym, zmierzających do ustanowienia mechanizmów uniemożliwiających wystąpienie wypadków jądrowych lub zmniejszających prawdopodobieństwo ich zaistnienia. Analiza przepisów *Konwencji* wskazuje, że wynikające z niej uregulowania dotyczą przedziału czasowego poprzedzającego zaistnienie wypadku jądrowego lub innych zdarzeń zagrażających bezpieczeństwu, związanych z procesem wytwarzania i wykorzystywania energii atomowej (aspekt prewencyjny). Za najważniejszy element *Konwencji* należy uznać określenie w art. 1 trzech fundamentalnych założeń stanowiących podstawy eksploatacji materiałów jądrowych: celu ogólnego bezpieczeństwa jądrowego (*the general nuclear safety objective*), celu ochrony przed zagrożeniami radiologicznymi (*the radiation protection objective*) oraz celu bezpieczeństwa technicznego (*the technical safety objective*). Szczegółowe zobowiązania państw stron wynikające z *Konwencji* mają na celu umożliwienie realizacji powyższych najważniejszych założeń omawianego instrumentu.

2. Konwencja o wczesnym powiadamianiu o awarii jądrowej z 26 września 1986 r. (*Convention on Early Notification of a Nuclear Accident*)

Przyjęcie *Konwencji* w czasie nadzwyczajnej sesji Konferencji Ogólnej Międzynarodowej Agencji Energii Atomowej stanowiło bezpośrednią konsekwencję awarii reaktora elektrowni atomowej w Czarnobylu w kwietniu 1986 r. Ogólnym założeniem leżącym u podstaw tego instrumentu było dążenie do wypracowania efektywnych mechanizmów prawnomiędzynarodowych pozwalających na szybką wymianę informacji w razie zaistnienia transgranicznych zdarzeń, które mogą wywoływać konsekwencje radiologiczne.

2.1. Zakres przedmiotowy

Zasadniczym elementem *Konwencji* jest wynikające z art. 2a zobowiązanie państw stron do niezwłocznego powiadamiania w razie awarii jądrowej zdefiniowanej w art. 1, bezpośrednio lub za pośrednictwem MAEA, państw, które są lub mogą być fizycznie poddane działaniu rezultatów awarii jądrowej, oraz Agencji o zaistnieniu tego rodzaju zdarzenia, jego charakterze, czasie, w którym nastąpiło, i jego dokładnym miejscu, jeżeli ma to istotne znaczenie. Ponadto art. 2b zobowiązuje do dostarczania państwom, które mogą być dotknięte skutkami awarii, oraz MAEA informacji niezbędnych do zminimalizowania skutków radiologicznych w tych państwach.

Należy zwrócić uwagę na to, że *Konwencja* ma zastosowanie do wypadków jądrowych związanych z szerokim spektrum działalności w zakresie produkcji i wykorzystywania energii atomowej, z uwzględnieniem zarówno celów cywilnych, jak i wojskowych[3].

[3] Sh. McBrayer, *Chernobyl's Legal Fallout – The Convention on Early Notification of a Nuclear Accident*, 17 Georgia Journal of International and Comparative Law 303 (1987), www.digitalcommons.law.uga.edu/cgi/

Zgodnie z art. 1 *Konwencji* jej postanowienia odnoszą się do każdego przypadku awarii związanej z urządzeniami lub działalnością prowadzoną przez państwo stronę, osoby fizyczne lub prawne pozostające pod jego jurysdykcją lub kontrolą, wskazanymi w ustępie 2, w której wyniku nastąpiło lub może nastąpić uwolnienie substancji promieniotwórczej i która spowodowała lub może spowodować uwolnienie ponadgraniczne substancji promieniotwórczej mogącej stanowić istotne zagrożenie radiologiczne dla innego państwa.

Pojęcia urządzenia i działalność oznaczają następujące elementy:

a) wszystkie reaktory jądrowe niezależnie od ich lokalizacji,
b) wszelkie obiekty jądrowe cyklu paliwowego,
c) wszelkie obiekty służące do zagospodarowania odpadów promieniotwórczych,
d) przewożenie i magazynowanie paliw jądrowych i odpadów promieniotwórczych,
e) produkcję, stosowanie, przechowywanie, trwałe składowanie i transport radioizotopów na potrzeby rolnictwa, przemysłu, służby zdrowia i w celu prowadzenia badań naukowych w tych dziedzinach,
f) stosowanie radioizotopów do zasilania w energię obiektów kosmicznych.

Art. 3 przewiduje ponadto możliwość fakultatywnego powiadamiania w razie zaistnienia wypadków jądrowych innych niż przewidziane w art. 1, w celu minimalizacji skutków radiologicznych określonego zdarzenia.

2.2. Zadania MAEA

Główną rolę w ustanowionym przez *Konwencję* mechanizmie powiadamiania o wypadkach jądrowych odgrywa MAEA, do której kompetencji należy niezwłoczne informowanie zarówno państw stron, jak i państw niebędących stronami *Konwencji*, które są lub mogą zostać dotknięte skutkami wypadku jądrowego, oraz właściwych organizacji międzynarodowych o wszystkich notyfikacjach, jakie otrzymała zgodnie z art. 2a (informacje o awarii jądrowej, jej charakterze, czasie i miejscu).

Ponadto na wniosek państwa strony, państwa członkowskiego MAEA lub właściwej organizacji międzynarodowej Agencja może przekazać tym podmiotom informacje, o których mowa w art. 2b, tj. informacje niezbędne do zminimalizowania skutków radiologicznych określonego zdarzenia. Enumeratywny katalog tych informacji został zawarty w art. 5. Obejmuje on następujące elementy:

a) czas, dokładne miejsce, jeśli to istotne, oraz charakter awarii jądrowej,
b) urządzenie lub rodzaj działalności,
c) przypuszczalną lub ustaloną przyczynę oraz przewidywany rozwój awarii jądrowej, związanej z ponadgranicznym uwolnieniem substancji promieniotwórczych,
d) ogólną charakterystykę uwolnienia substancji promieniotwórczych, włączając – jeśli jest to możliwe i celowe – charakter, przypuszczalną postać fizyczną i chemiczną, a także ilość, skład i efektywną wysokość uwalniania substancji promieniotwórczych,
e) informacje o istniejących i przewidywanych warunkach meteorologicznych i hydrologicznych, niezbędne do prognozowania uwolnienia ponadgranicznego substancji promieniotwórczych,
f) wyniki pomiarów kontrolnych środowiska, dotyczące uwolnienia ponadgranicznego substancji promieniotwórczych,

viewcontent.cgi?article=1725&context=gjjcl [dostęp: 8 III 2017].

g) podjęte lub planowane środki ochrony na zewnątrz obiektu awarii,
h) przewidywane zachowanie się substancji promieniotwórczych w czasie ich uwalniania.

MAEA prowadzi zarówno aktualny wykaz organów państwowych i punktów kontaktowych, jak i punktów kontaktowych odpowiednich organizacji międzynarodowych i w razie potrzeby udostępnia go tym państwom lub organizacjom.

Nie powinno budzić wątpliwości, że *Konwencja* w znacznej mierze przyczyniła się do zwiększenia poziomu bezpieczeństwa jądrowego przez kodyfikację norm zwyczajowych obowiązujących do momentu jej przyjęcia. Niemniej jednak istotnym niedostatkiem omawianego instrumentu jest nieprecyzyjne uregulowanie obowiązków państw stron w razie zaistnienia wypadku jądrowego. *Konwencja* nie zawiera przepisów regulujących w sposób szczegółowy, jakie konkretnie państwa powinny zostać powiadomione. Pominięte również zostało określenie czasu, w jakim państwo, na którego terytorium doszło do wypadku jądrowego, jest zobowiązane do poinformowania o tym innych podmiotów. Ponadto *Konwencja* nie zobowiązuje państw stron do informowania o wypadkach wynikających z testowania broni jądrowej[4].

3. Konwencja o pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego z 26 września 1986 r. (*Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency*)

Wraz z omówioną powyżej konwencją dotyczącą wczesnego powiadamiania o wypadkach jądrowych, konwencja o pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego stanowi kolejny element mający na celu wzmocnienie instrumentów umożliwiających prowadzenie działań zmierzających do neutralizacji lub zmniejszenia negatywnych skutków wypadków jądrowych w wymiarze transgranicznym, obowiązujących w sferze prawa międzynarodowego. Należy zwrócić uwagę, że oba wymienione instrumenty mają charakter komplementarny i wzajemnie się uzupełniają – pierwszy z nich reguluje zagadnienie odnośnie do wczesnego powiadamiania o samym zaistnieniu wypadku jądrowego, podczas gdy drugi określa sposób i tryb dalszego postępowania na etapie następującym po powzięciu informacji o zdarzeniu, zmierzającego do udzielenia niezbędnej pomocy państwu zagrożonemu skutkami wypadku jądrowego.

3.1. Zakres przedmiotowy

Konwencja zobowiązuje państwa strony do współpracy zarówno międzypaństwowej, jak i pomiędzy państwami a MAEA, oraz do wspierania przy udzielaniu natychmiastowej pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego w celu zminimalizowania jej skutków i ochrony życia, mienia oraz środowiska przed działaniem uwolnionych substancji promieniotwórczych (art. 1 ust. 1). Ten instrument określa zatem międzynarodowe ramy prawne, których celem jest usprawnienie procesu zwracania się o pomoc w razie zaistnienia awarii jądrowej lub zagrożenia radiologicznego oraz udzielania tego rodzaju pomocy. Mechanizm zwracania się o pomoc został określony w art. 2 ust. 1 i 2. Zgodnie z ust. 1, jeżeli w przypadku awarii jądrowej lub zagrożenia radiologicznego państwo strona potrzebuje pomocy, niezależnie od tego,

[4] Tamże, s. 319.

czy taka awaria lub zagrożenie wystąpiły na jego terytorium, pod jego jurysdykcją lub pod kontrolą, może zwrócić się z prośbą o udzielenie takiej pomocy przez każde inne państwo stronę, bezpośrednio lub za pośrednictwem Agencji i przez Agencję lub w odpowiednich przypadkach przez inne międzynarodowe organizacje międzyrządowe. Państwo zwracające się o pomoc jest zobowiązane do określenia zakresu i rodzaju pomocy oraz – jeżeli jest to możliwe – do przekazania stronie udzielającej tego rodzaju pomocy informacji, które mogą okazać się niezbędne do określenia, w jakim stopniu ta pomoc może zostać udzielona. Jeżeli określenie zakresu i rodzaju pomocy okaże się w danym przypadku niemożliwe, państwo zwracające się o pomoc i państwo udzielające pomocy przeprowadzają konsultacje mające na celu określenie sposobu i trybu dalszego postępowania.

3.2. Obowiązki państw stron:

- współpraca z innymi państwami i z MAEA w celu udzielania pomocy na wypadek awarii jądrowej;
- udzielenie państwu zwracającemu się o pomoc informacji, czy jej udzielenie jest możliwe oraz określenie zakresu i warunków ewentualnej pomocy;
- państwo zwracające się o pomoc jest zobowiązane do udostępnienia środków i usług niezbędnych do udzielenia tej pomocy;
- przekazanie MAEA i pozostałym państwom stronom informacji o swoich właściwych organach, punktach kontaktowych upoważnionych do wystosowywania i przyjmowania próśb o pomoc oraz przyjmowania propozycji udzielenia pomocy (punkty kontaktowe powinny działać w sposób ciągły);
- w razie braku odmiennego uzgodnienia pomiędzy stronami, strona zwracająca się o pomoc zwróci koszty operacji stronie udzielającej pomocy;
- państwo zwracające się o pomoc przyznaje personelowi strony udzielającej pomocy i personelowi działającemu w jego imieniu niezbędne przywileje, immunitety i ułatwienia do wykonywania przezeń funkcji związanych z udzielaniem pomocy.

3.3. Zadania MAEA

Na zasadzie analogii do postanowień *Konwencji* o wczesnym ostrzeganiu o wypadkach jądrowych, MAEA pełni funkcję organu o charakterze koordynacyjnym. Tym samym jest zobowiązana do przekazania wniosku o pomoc pozostałym stronom *Konwencji* lub organizacjom międzynarodowym i koordynacji pomocy udzielanej na poziomie międzynarodowym. Ponadto, zgodnie z art. 5, MAEA działa w charakterze organu doradczego – udziela państwom informacji specjalistycznych dotyczących m.in. ekspertów, materiałów i zasobów, które mogą być wykorzystane w razie zaistnienia zagrożenia radiologicznego lub awarii, metodologii i technologii reagowania na tego rodzaju zdarzenia, opracowywania programów kontroli poziomu promieniowania oraz norm i procedur w tym zakresie czy opracowywania dla personelu obiektów jądrowych programów szkoleniowych mających na celu wypracowanie skutecznych mechanizmów działania na wypadek awarii jądrowej lub zagrożenia radiologicznego.

4. *Konwencja o ochronie fizycznej materiałów jądrowych z 3 marca 1980 r.* wraz z załącznikami I i II, z uwzględnieniem zmian z 2005 r.

Konwencja stanowi jeden z trzynastu prawnomiędzynarodowych instrumentów antyterrorystycznych. Jest jedynym wiążącym – w rozumieniu prawa międzynarodowego – instrumentem dotyczącym sfery ochrony fizycznej materiałów jądrowych. Dnia 8 czerwca 2005 r. państwa strony *Konwencji* przyjęły protokół, który ją zmieniał[5]. Podczas gdy jej pierwotna wersja dotyczyła ochrony materiałów jądrowych w transporcie międzynarodowym, protokół zmieniający zobowiązywał państwa do wprowadzenia określonych w dokumencie środków ochrony fizycznej obiektów i materiałów jądrowych w toku wykorzystywania energii atomowej do celów wewnętrznych o charakterze cywilnym, jak również w odniesieniu do ich składowania i transportu na terytorium państw stron. Ponadto postanowienia protokołu zmierzają do wzmocnienia mechanizmów współpracy w zakresie zastosowania środków szybkiego reagowania na wypadek kradzieży lub zaginięcia materiałów jądrowych, neutralizacji skutków radiologicznych sabotażu nuklearnego oraz usprawnienia mechanizmów zapobiegania i zwalczania przestępstw związanych z nielegalnym obrotem tego rodzaju materiałami oraz ich wykorzystywaniem. Elementem istotnym z punktu widzenia systemu reagowania na zdarzenia CBRN jest dodanie do *Konwencji* dwóch nowych definicji – obiektu jądrowego oraz sabotażu oznaczającego atak na obiekt jądrowy.

Zmiany zostały zawarte w Akcie Końcowym Konferencji. Modyfikacji uległ również tytuł *Konwencji*, który otrzymał następujące brzmienie: *Konwencja o Ochronie Fizycznej Materiałów Jądrowych i Obiektów Jądrowych*. Akt Końcowy został podpisany przez przedstawicieli wszystkich 88 państw stron Konwencji, którzy wzięli udział w konferencji[6].

4.1. Cel Konwencji:

- wypracowanie spójnego i efektywnego systemu ochrony fizycznej obiektów i materiałów jądrowych wykorzystywanych do celów cywilnych;
- zapobieganie przestępstwom odnoszącym się do wykorzystania materiałów i obiektów jądrowych używanych do celów cywilnych oraz ich zwalczanie;
- zwiększenie efektywności współpracy międzynarodowej w zakresie ochrony fizycznej obiektów i materiałów jądrowych.

4.2. Zakres przedmiotowy

Zgodnie z art. 2 *Konwencja* ma zastosowanie do materiałów jądrowych używanych w celach pokojowych podczas ich transportu w przestrzeni międzynarodowej. Z zastrzeżeniem wyjątków określonych w art. 3, 4 i 5 ust. 3 *Konwencja* ma również zastosowanie do materiałów jądrowych używanych w celach pokojowych w trakcie ich użytkowania, składowania lub transportu wewnątrz kraju.

[5] *Amendment to the Convention on the Physical Protection of Nuclear Material*, www.iaea.org/sites/default/files/infcirc274r1m1.pdf [dostęp: 16 III 2017].

[6] www.bip.kprm.gov.pl/ftp/kprm/dokumenty/060830u1uz.pdf.

4.3. Reagowanie na zdarzenia CBRN i zobowiązanie do penalizacji określonych czynów

W celu umożliwienia szybkiej wymiany informacji w przypadku bezprawnego przemieszczenia, użycia lub przetworzenia materiałów jądrowych albo realnej groźby zaistnienia jakiegokolwiek z tych przypadków art. 5 ust. 1 zobowiązuje każde państwo do poinformowania pozostałych stron *Konwencji* o swoim organie centralnym oraz punkcie kontaktowym odpowiedzialnym za ochronę fizyczną materiałów jądrowych oraz za koordynację działań w zakresie odzyskania i innych środków interwencji w razie zaistnienia powyższych zdarzeń.

Art. 5 ust. 2 określa sposób postępowania w razie kradzieży, rabunku lub jakiegokolwiek innego bezprawnego zawładnięcia materiałami jądrowymi, jak również w przypadku realnej groźby popełnienia tego rodzaju przestępstw. Państwa są zobowiązane do zapewnienia, zgodnie z przepisami prawa wewnętrznego, maksymalnej możliwej współpracy i pomocy w celu odzyskania i zabezpieczenia tego rodzaju materiałów każdemu państwu zwracającemu się o udzielenie pomocy w tym zakresie. Ten obowiązek dotyczy zwłaszcza:

- poinformowania innych państw o kradzieży, rabunku lub innym bezprawnym zawładnięciu materiałami jądrowymi lub o realnej groźbie takich czynów oraz – jeżeli okaże się to konieczne – poinformowania o tym organizacji międzynarodowych;
- wymiany informacji z państwami lub organizacjami międzynarodowymi w celu zabezpieczenia zagrożonych materiałów jądrowych, sprawdzenia całości kontenerów przewozowych lub odzyskania materiałów jądrowych, które zostały bezprawnie przejęte; ten obowiązek dotyczy także koordynacji działań drogą dyplomatyczną lub innymi uzgodnionymi kanałami, udzielenia pomocy innym państwom, jeżeli o taką się zwrócą, oraz zapewnienia zwrotu materiałów jądrowych skradzionych lub zagubionych w następstwie zdarzeń opisanych powyżej.

Zgodnie z art. 7 *Konwencji* państwa są zobowiązane do penalizacji następujących czynów, jeżeli zostały one dokonane w sposób umyślny:

a) aktu nielegalnego pozyskania, posiadania, używania, przekazywania, przetwarzania, pozbycia się lub rozproszenia materiałów jądrowych, co powoduje lub może spowodować śmierć lub ciężkie uszkodzenie ciała jakiejkolwiek osoby albo znaczne szkody materialne;
b) kradzieży lub rabunku materiałów jądrowych;
c) przywłaszczenia lub uzyskania materiałów jądrowych przez dokonanie oszustwa;
d) aktu żądania wydania materiałów jądrowych pod groźbą użycia siły lub przy jej użyciu albo z wykorzystaniem jakiejkolwiek innej formy zastraszenia;
e) groźby użycia materiałów jądrowych w celu spowodowania śmierci lub poważnych obrażeń jakiejkolwiek osoby albo znacznej szkody materialnej, popełnienia przestępstwa wymienionego powyżej w punkcie b w celu zmuszenia osób fizycznych lub prawnych, organizacji międzynarodowej lub państwa do podjęcia albo powstrzymania się od podjęcia jakiegokolwiek działania;
f) usiłowania popełnienia jakiegokolwiek przestępstwa wymienionego w punktach a, b lub c;
g) aktu, który stanowi współuczestnictwo w jakimkolwiek z przestępstw wymienionych w pkt a–f.

Państwo, na którego terytorium znajduje się domniemany sprawca przestępstwa, podejmuje zgodnie z własnym ustawodawstwem odpowiednie środki, łącznie z aresztem, w celu zapewnienia jego obecności przy przeprowadzaniu postępowania sądowego lub ekstradycji (art. 9).

Biorąc pod uwagę wnioski płynące z systemowej analizy źródeł prawa międzynarodowego w zakresie nieproliferacji broni masowego rażenia, trzeba przyjąć, że wynikające z konwencji zobowiązanie państw do penalizacji określonych czynów zagrażających bezpieczeństwu materiałów jądrowych należy uznać za jeden ze sposobów reagowania na zdarzenia CBRN. Mimo że nie jest to instrument polegający stricte na określeniu fizycznych działań podejmowanych w celu zapobiegania lub neutralizacji skutków powyższych zdarzeń, prawnokarna reakcja właściwych organów państwa na opisane powyżej działania lub zaniechania powinna być uznana za jedną z metod reagowania na opisywane zdarzenia.

5. *Międzynarodowa Konwencja w sprawie zwalczania aktów terroryzmu jądrowego przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 13 kwietnia 2005 roku* (*International Convention for The Suppression of Acts of Nuclear Terrorism*)

Przepisy *Konwencji*, analogicznie do *Konwencji o ochronie fizycznej materiałów jądrowych*, koncentrują się wokół penalizacji zachowań polegających na wykorzystywaniu materiałów jądrowych w celach terrorystycznych.

Enumeratywny wykaz czynów zabronionych został zawarty w art. 2, zgodnie z którym w rozumieniu *Konwencji* przestępstwo popełnia ten, kto w sposób bezprawny i świadomy:

a) posiada materiał promieniotwórczy[7] lub wytwarza bądź posiada urządzenie[8]:
   i) z zamiarem spowodowania śmierci lub poważnego uszkodzenia ciała, lub
   ii) z zamiarem spowodowania poważnej szkody w mieniu lub środowisku;
b) w jakikolwiek sposób używa materiału promieniotwórczego lub urządzenia, lub używa albo powoduje szkodę w obiekcie jądrowym[9] w sposób, który powoduje uwolnienie lub ryzyko uwolnienia materiału promieniotwórczego:
   i) z zamiarem spowodowania śmierci lub poważnego uszkodzenia ciała, lub
   ii) z zamiarem spowodowania poważnej szkody w mieniu lub środowisku, lub

[7] Termin materiał promieniotwórczy oznacza materiał jądrowy oraz inne substancje promieniotwórcze zawierające nuklidy, które ulegają samorzutnemu rozpadowi promieniotwórczemu (proces, któremu towarzyszy emisja jednego lub kilku typów promieniowania jonizującego mogący mieć postać promieniowania korpuskularnego – cząstki alfa, beta, neutrony – oraz elektromagnetycznego – promieniowanie gamma – i które mogą ze względu na swoje właściwości radiologiczne i rozszczepialne powodować śmierć, ciężkie uszkodzenie ciała lub poważne szkody w mieniu lub środowisku.

[8] Termin urządzenie oznacza:

a) każde jądrowe urządzenie wybuchowe lub

b) każde urządzenie powodujące rozproszenie materiału promieniotwórczego albo emisję promieniowania, które mogą, ze względu na swoje właściwości promieniotwórcze, powodować śmierć, ciężkie uszkodzenie ciała lub poważną szkodę w mieniu lub środowisku (art. 1 ust. 4).

[9] Termin obiekt jądrowy oznacza:

a) każdy reaktor jądrowy, w tym reaktory zainstalowane na statkach wodnych, pojazdach, statkach powietrznych lub obiektach kosmicznych, wykorzystywane jako źródło energii do napędzania statków wodnych, pojazdów, statków powietrznych lub obiektów kosmicznych albo w każdym innym celu;

b) każdy zakład przemysłowy lub środek transportu wykorzystywany do produkcji, przechowywania, przetwarzania lub transportu materiału promieniotwórczego (art. 1 ust. 3).

iii) z zamiarem zmuszenia osoby fizycznej lub prawnej albo organizacji międzynarodowej lub państwa do określonego działania albo zaniechania.

2. Przestępstwo popełnia także ten, kto:

a) grozi, w okolicznościach wskazujących na wiarygodność takiej groźby, popełnieniem przestępstwa określonego w pkt 1 b) niniejszego artykułu, lub

b) domaga się bezprawnie i świadomie materiału promieniotwórczego, urządzenia lub obiektu jądrowego, posługując się groźbą, w okolicznościach wskazujących na wiarygodność takiej groźby lub przy użyciu siły.

3. Przestępstwo popełnia także ten, kto usiłuje popełnić przestępstwo określone w ust. 1 niniejszego artykułu.

4. Przestępstwo popełnia także ten, kto:

a) uczestniczy jako współsprawca w popełnieniu przestępstwa określonego w ust. 1, 2 lub 3 niniejszego artykułu lub

b) organizuje inne osoby w celu popełnienia przestępstwa określonego w ust. 1, 2 lub 3 niniejszego artykułu albo kieruje nimi lub

c) w jakikolwiek inny sposób przyczynia się do popełnienia jednego lub większej liczby przestępstw określonych w ustępie 1, 2 lub 3 niniejszego artykułu przez grupę osób działających we wspólnym celu; takie przyczynienie się winno być umyślne i realizowane w celu udzielenia wsparcia ogólnie rozumianej działalności przestępczej lub przestępczego celu grupy bądź przy świadomości, że celem grupy jest popełnienie wymienionego przestępstwa lub przestępstw.

Wyżej przedstawiony zasięg stosowania *Konwencji* został ograniczony w art. 3, zgodnie z którym nie ma ona zastosowania w sytuacji, gdy przestępstwo jest popełnione na terenie jednego państwa, podejrzany oraz ofiary są jego obywatelami, podejrzany został schwytany na terenie tego państwa i żadne inne państwo nie ma podstaw do sprawowania nad nim jurysdykcji zgodnie z zasadami opisanymi w art. 9 *Konwencji*. To wyłączenie sprawia zatem, że *Konwencja* ma zastosowanie wyłącznie do aktów terroryzmu jądrowego o charakterze międzynarodowym, tj. jeżeli określone zdarzenie o charakterze terrorystycznym dotyczy więcej niż jednego państwa[10].

W tym kontekście należy podkreślić, że najważniejszym elementem pozwalającym na skuteczne stosowanie *Konwencji* w praktyce jest norma dotycząca ekstradycji zawarta w art. 13, zgodnie z którą przestępstwa określone w art. 2 uważa się za włączone, jako podlegające ekstradycji, do wszystkich umów o ekstradycji obowiązujących między dowolnymi państwami stronami przed wejściem w życie niniejszej *Konwencji*. Państwa strony zobowiązują się do włączenia takich przestępstw jako przestępstw podlegających ekstradycji do wszystkich umów o ekstradycji, które zostaną pomiędzy nimi zawarte po wejściu *Konwencji* w życie. W rezultacie, jeżeli pomiędzy określonymi państwami nie została zawarta umowa o ekstradycji, *Konwencja* może stanowić samoistną podstawę prawną ekstradycji (analogiczny przepis został zawarty w *Konwencji o ochronie fizycznej materiałów jądrowych)*[11].

[10] O. Jankowitsch-Prevor, *International Convention for the Suppression of Acts of Nuclear Terrorism,* Nuclear Law Bulletin, vol. 2005.2, dostępny na stronie: www.oecd-library.org/nuclear-energy/international-convention-for-the-suppression-of-acts-of-nuclear-terrorism_nuclear_law-2005-5k9czgt915jkcrawler=true [dostęp: 9 III 2017].

[11] Tamże, s. 19.

5.1. Obowiązek współpracy

Poza normami o charakterze prawnokarnym *Konwencja* zobowiązuje państwa również do prowadzenia współpracy z wykorzystaniem następujących instrumentów (art. 7):

a) stosowanie wszelkich możliwych do wdrożenia rozwiązań, w tym, jeśli to konieczne, działań legislacyjnych, w celu zapobiegania i przeciwdziałania przygotowaniom do popełnienia, na swoim terytorium lub poza nim, przestępstw określonych w art. 2, w tym rozwiązań zmierzających do zakazania prowadzenia na swoim terytorium nielegalnych działań osób, grup i organizacji, które zachęcają do udzielania wsparcia technicznego lub informacji, podżegają, organizują, świadomie finansują lub świadomie udzielają tego typu wsparcia lub informacji albo angażują się w realizację takich przestępstw;
b) wymianę dokładnych i sprawdzonych informacji zgodnie z przepisami prawa wewnętrznego oraz w sposób zgodny z określonymi tutaj warunkami, a także koordynację działań administracyjnych i innych, uznanych za odpowiednie, w celu wykrywania przestępstw określonych w art. 2, zapobiegania i przeciwdziałania im oraz ich wyjaśniania, a także wszczynania postępowań karnych w stosunku do osób podejrzewanych o ich popełnienie; w szczególności państwo strona podejmie stosowne kroki w celu niezwłocznego powiadomienia innych państw wymienionych w art. 9 o popełnieniu przestępstw określonych w art. 2 i przygotowaniach do ich popełnienia, zgodnie z powziętymi informacjami, oraz odpowiedniego poinformowania organizacji międzynarodowych.

Art. 14 *explicite* zobowiązuje państwa do wzajemnej pomocy w związku ze ściganiem, prowadzeniem czynności w ramach postępowania karnego lub ekstradycją w sprawach przestępstw, o których mowa w art. 2, jak również w zakresie uzyskiwania materiału dowodowego mającego znaczenie dla określonego postępowania. Ten obowiązek ma być wypełniany zgodnie z wszelkimi umowami i porozumieniami o wzajemnej pomocy prawnej obowiązującymi w stosunkach pomiędzy określonymi państwami. Niemniej jednak, w razie braku takiej umowy lub porozumienia państwa są zobowiązane do udzielania sobie tego rodzaju pomocy zgodnie z przepisami prawa krajowego (art. 14 ust. 2).

5.2. Reagowanie na zdarzenia CBRN – tryb postępowania po przejęciu przez państwo kontroli nad materiałem jądrowym (art. 18)

Konwencja określa katalog specyficznych obowiązków państwa na etapie następującym po odzyskaniu przez jego właściwe organy kontroli nad materiałami jądrowymi, urządzeniami lub obiektami jądrowymi wykorzystanymi w celu popełnienia jednego z przestępstw określonych w art. 2. Zgodnie z art. 18 ust. 1 państwo, w którego posiadaniu znajdą się tego rodzaju materiały, powinno podjąć następujące działania mające na celu neutralizację zagrożenia wynikającego z przestępnego posługiwania się materiałami, urządzeniami lub obiektami jądrowymi:

a) zmierzające do zabezpieczenia materiału promieniotwórczego, urządzenia lub obiektu jądrowego;
b) zapewniające przechowywanie materiału promieniotwórczego zgodnie ze stosownymi zasadami bezpieczeństwa Międzynarodowej Agencji Energii Atomowej oraz

c) pozwalające na dostosowanie się do zaleceń w zakresie ochrony fizycznej oraz standardów bezpieczeństwa i ochrony radiologicznej publikowanych przez Międzynarodową Agencję Energii Atomowej.

Kolejnym etapem, następującym po realizacji powyższych procedur zabezpieczających, jest przekazanie materiałów promieniotwórczych, urządzeń lub obiektów jądrowych państwu będącemu ich właścicielem, państwu, którego obywatelem lub mieszkańcem jest osoba fizyczna lub prawna będąca właścicielem wyżej wymienionych przedmiotów lub państwu, z którego terytorium te przedmioty zostały skradzione lub w inny sposób bezprawnie uzyskane (art. 18 ust. 2).

Jeżeli przepisy prawa wewnętrznego lub międzynarodowego zakazują zwrotu albo przyjęcia wspomnianych przedmiotów lub jeżeli zachodzi sytuacja, o której mowa w art. 3 ust. 2, państwo będące w ich posiadaniu realizuje czynności, o których mowa w art. 18 ust. 1 pkt a, b z zastrzeżeniem, że będą one wykorzystane wyłącznie w celach pokojowych.

Artykuł 3 ust. 2 normuje sytuację, w której posiadanie materiału promieniotwórczego, urządzeń lub obiektów jądrowych jest niezgodne z prawem wewnętrznym państwa, które weszło w ich posiadanie wskutek czynności związanych ze ściganiem przestępstw określonych w *Konwencji*. To państwo jest wówczas zobowiązane do ich możliwie najszybszego przekazania państwu, którego przepisy prawa krajowego dopuszczają posiadanie tego rodzaju przedmiotów i które zapewni ich odpowiednie zabezpieczenie (również z zastrzeżeniem, że będą one wykorzystane wyłącznie w celach pokojowych).

Jeżeli tego rodzaju przedmioty nie należą do żadnego z państw stron *Konwencji,* ich obywatela lub rezydenta nie zostały skradzione lub uzyskane w inny bezprawny sposób z terytorium państwa strony, lub jeżeli żadne z państw stron nie wyraża woli ich odebrania, sposób dysponowania tymi przedmiotami zostanie określony w drodze odrębnej decyzji podjętej na podstawie konsultacji z udziałem zainteresowanych państw i właściwych organizacji międzynarodowych.

W celu realizacji obowiązków wynikających z art. 18 państwo znajdujące się w posiadaniu materiału promieniotwórczego, urządzenia lub obiektu jądrowego może wystąpić o pomoc lub współpracę ze strony innych państw stron i właściwych organizacji międzynarodowych, w szczególności MAEA. Państwo dysponujące lub zatrzymujące przedmioty, o których mowa, jest zobowiązane do poinformowania dyrektora generalnego MAEA o sposobie ich zadysponowania lub zatrzymania, dyrektor zaś przekazuje tego rodzaju informację pozostałym państwom stronom *Konwencji*. Ponadto państwo strona, w którym domniemany sprawca przestępstwa jest ścigany sądownie, ma obowiązek, zgodnie ze swoim prawem wewnętrznym lub stosownymi procedurami, poinformować o ostatecznym wyniku postępowania sekretarza generalnego Organizacji Narodów Zjednoczonych, który z kolei przekazuje te informacje innym państwom stronom.

ASPEKTY CHEMICZNE

1. *Konwencja o zakazie broni chemicznej z dnia 13 stycznia 1993 r.*[12] (*The Chemical Weapons Convention* – CWC)

Konwencja o zakazie broni chemicznej stanowi jeden z fundamentalnych elementów systemu prawa międzynarodowego w zakresie przeciwdziałania proliferacji

[12] *Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów sporządzona w Paryżu dnia 13 stycznia 1993 r.* (Dz.U. z 1999 r. poz. 703).

broni masowego rażenia. System ustanowiony przez *Konwencji* zakazuje państwom stronom posiadania, używania i rozwijania technologii umożliwiającej pozyskanie broni chemicznej i tworzy z kolei system kontroli zgodności postępowania państw z normami *Konwencji* oraz udzielania pomocy na wypadek zagrożenia bronią chemiczną, który jest nadzorowany przez Organizację ds. Zakazu Broni Chemicznej (Organisation for the Prohibition of Chemical Weapons, OPCW).

1.1. Zobowiązania o charakterze ogólnym

Zgodnie z art. I *Konwencji* państwa strony zobowiązują się w żadnych okolicznościach:

a) nie prowadzić badań dotyczących broni chemicznej, nie produkować jej, w żaden inny sposób jej nie nabywać, nie gromadzić, nie przechowywać ani nie przekazywać tej broni pośrednio lub bezpośrednio komukolwiek;
b) nie używać broni chemicznej;
c) nie podejmować żadnych wojskowych przygotowań do użycia broni chemicznej;
d) nie pomagać, nie zachęcać ani nie skłaniać kogokolwiek w dowolny sposób do podejmowania jakiejkolwiek działalności zabronionej państwu stronie na mocy niniejszej *Konwencj*i.

2. Każde państwo strona zobowiązuje się zniszczyć broń chemiczną będącą jego własnością lub w jego posiadaniu albo znajdującą się w dowolnym miejscu podlegającym jego jurysdykcji lub kontroli, zgodnie z postanowieniami niniejszej *Konwencji*.
3. Każde państwo strona zobowiązuje się zniszczyć wszelką broń chemiczną, którą porzuciło na terytorium innego państwa strony, zgodnie z postanowieniami niniejszej *Konwencji*.
4. Każde państwo strona zobowiązuje się zniszczyć wszelkie obiekty służące do produkcji broni chemicznej, będące jego własnością lub w jego posiadaniu, albo znajdujące się w dowolnym miejscu podlegającym jurysdykcji lub kontroli, zgodnie z postanowieniami niniejszej *Konwencji*.
5. Każde państwo strona zobowiązuje się nie używać chemicznych środków policyjnych jako środków prowadzenia wojny.

Broń chemiczna oznacza niżej wymienione, występujące razem lub oddzielnie:

a) toksyczne związki chemiczne oraz ich prekursory, z wyłączeniem tych przypadków, które są przeznaczone do celów niezabronionych na mocy niniejszej *Konwencji*, pod warunkiem, że ich rodzaje i ilości są zgodne z takimi celami;
b) amunicję i urządzenia, specjalnie zaprojektowane do spowodowania śmierci lub innej szkody przez toksyczne właściwości związków chemicznych wyszczególnionych w ustępie a), wyzwalanych w rezultacie zastosowania takiej amunicji i urządzeń;
c) wszelki sprzęt specjalnie zaprojektowany do użycia w bezpośrednim związku z zastosowaniem amunicji i urządzeń określonych w ustępie b) – art. 2 ust. 1.

1.2. Krajowe środki realizacji konwencji

Artykuł VII zawiera szczegółowe normy wskazujące na to, w jaki sposób państwa strony powinny dostosować wewnętrzny system prawny w celu wypełnienia zobowiązań wynikających z *Konwencji*. W myśl tego artykułu każde państwo strona, zgodnie ze

swoimi wymogami konstytucyjnymi, wprowadza środki konieczne do realizacji zobowiązań wynikających z *Konwencji*, a zwłaszcza:

a) zakazuje osobom fizycznym i prawnym znajdującym się w jakimkolwiek miejscu na jego terytorium lub w każdym innym miejscu podlegającym jego jurysdykcji, uznanej przez prawo międzynarodowe, podejmowania wszelkiej działalności zabronionej państwu stronie przez niniejszą *Konwencję*, a w szczególności wprowadza odpowiednie przepisy karne w tym zakresie;
b) nie zezwala w żadnym miejscu znajdującym się pod jego kontrolą na prowadzenie jakiejkolwiek działalności zabronionej państwu stronie przez niniejszą *Konwencję*;
c) zastosuje przepisy karne przyjęte zgodnie z ustępem a) do wszelkiej działalności zabronionej państwu stronie przez niniejszą *Konwencję*, podejmowanej w jakimkolwiek miejscu przez osoby fizyczne mające jego obywatelstwo, zgodnie z prawem międzynarodowym.

Ponadto art. VII ust. 2 i 3 nakłada na państwa obowiązek współpracy i udzielania sobie wzajemnie w odpowiedniej formie pomocy prawnej w celu ułatwienia wykonywania zobowiązań wynikających z konieczności osiągnięcia poziomu kompatybilności norm prawa krajowego wymaganego przez *Konwencję* z ustanowionymi przez nią wymogami. Ponadto w toku realizacji tych zobowiązań państwa podejmują wszelkie środki w celu zagwarantowania bezpieczeństwa ludności, ochrony środowiska oraz współpracują w tym zakresie z pozostałymi państwami.

1.3. Reagowanie na zdarzenia CBRN

System reagowania na zdarzenia polegające na użyciu przeciwko państwu broni chemicznej, policyjnych środków chemicznych jako sposobu prowadzenia wojny lub zagrożenia działalnością innego państwa niezgodną z art. I *Konwencji* został ustanowiony na mocy art. XI *Konwencji*, zatytułowanego *Pomoc i ochrona przed bronią chemiczną*.

Pod pojęciem p o m o c należy rozumieć koordynację i zapewnianie państwom stronom ochrony przed bronią chemiczną, a w szczególności dostarczanie, w razie wystąpienia zagrożeń, o których mowa powyżej, środków do wykrywania tej broni i systemów alarmowania, sprzętu ochronnego, sprzętu do odkażania oraz środków odkażających, medycznych odtrutek i metod leczenia oraz udzielanie konsultacji w sprawie wyżej wymienionych środków ochronnych.

Procedura udzielania pomocy na wypadek zaistnienia zdarzeń, o których mowa powyżej, została określona w ust. 8–11. Każde państwo ma w takim wypadku prawo do jej otrzymania i ochrony przed użyciem albo groźbą użycia broni chemicznej. Wniosek zawierający niezbędne informacje o zdarzeniu jest kierowany do dyrektora generalnego OPCW, który niezwłocznie przekazuje go Radzie Wykonawczej oraz wszystkim państwom stronom. Początkowy etap procedury polega zatem na równoległym poinformowaniu o złożeniu przez dane państwo wniosku o udzielenie pomocy szerokiemu kręgowi odbiorców – zarówno właściwym organom OPCW, jak i wszystkim państwom stronom.

Kolejny etap polega na prowadzeniu praktycznych działań zabezpieczających i naprawczych przez znacznie zawężony krąg podmiotów ograniczający się do państw,

które na podstawie ust. 7b i 7c[13] zobowiązały się do udzielenia nadzwyczajnej pomocy w przypadku użycia broni chemicznej lub policyjnych środków chemicznych albo poważnej groźby użycia tych środków i są skłonne do udzielenia tego rodzaju pomocy zainteresowanemu państwu nie później niż w ciągu 12 godzin od chwili otrzymania wniosku.

Dyrektor generalny jest zobowiązany do wszczęcia dochodzenia w celu określenia dalszych działań nie później niż w ciągu 24 godzin od chwili otrzymania wniosku o udzielenie pomocy. Dochodzenie musi zostać zakończone w ciągu 72 godzin. Po zamknięciu dochodzenia dyrektor generalny kieruje sprawozdanie do Rady Wykonawczej. Jeżeli okoliczności sprawy nie pozwalają na zamknięcie dochodzenia w wyżej wymienionym czasie, sporządzane jest sprawozdanie tymczasowe pozwalające na określenie ogólnej charakterystyki danego zdarzenia, prezentujące zarys ewentualnych środków naprawczych i zabezpieczających oraz zawierające wstępne oszacowanie stopnia zagrożenia wywołanego przez konkretne zdarzenie.

Dodatkowy termin nie może przekraczać 72 godzin, dochodzenie może być jednak przedłużane na dalsze analogiczne okresy. Na koniec każdego okresu dodatkowego Rada Wykonawcza otrzymuje sprawozdania przedstawiające rozwój sytuacji. W zależności od potrzeb i specyfiki konkretnego zdarzenia, celem dochodzenia jest ustalenie faktów mających znaczenie dla ewentualnego udzielenia pomocy, jak również określenie rodzaju pomocy i ochrony wymaganych przez państwo.

Rada Wykonawcza zbiera się w celu rozpatrzenia sytuacji nie później niż w ciągu 24 godzin od otrzymania sprawozdania podsumowującego rezultaty dochodzenia i w ciągu kolejnych 24 godzin podejmuje decyzję o ewentualnym zobowiązaniu Sekretariatu Technicznego OPCW do udzielenia państwu dodatkowej pomocy. Ten organ z kolei przekazuje sprawozdanie z dochodzenia oraz informuje o decyzji podjętej przez Radę Wykonawczą wszystkie państwa strony i właściwe organizacje międzynarodowe. W razie pozytywnej decyzji Rady Wykonawczej dyrektor generalny niezwłocznie udziela pomocy. Może w tym celu współpracować z państwem, które zwróciło się o pomoc, oraz z pozostałymi państwami i organizacjami międzynarodowymi (art. X ust. 10).

Jeżeli rezultaty dochodzenia lub informacje uzyskane z innych wiarygodnych źródeł stanowią dostateczny dowód potwierdzający istnienie ofiar użycia broni chemicznej oraz wskazania do podjęcia natychmiastowej akcji w celu neutralizacji skutków zdarzenia, dyrektor generalny informuje o tym wszystkie państwa strony i podejmuje nadzwyczajne środki pomocy (art. X ust. 11).

[13] Art. X ust. 7:

„Każde Państwo-Strona zobowiązuje się do udzielania pomocy za pośrednictwem Organizacji i w tym celu wybierze według swego upodobania jeden lub więcej z następujących środków:

(a) wnoszenie wkładu do funduszu pomocy złożonego z dobrowolnych składek, który powinien zostać utworzony przez Konferencję na jej pierwszej sesji;

(b) podpisanie, możliwie nie później niż 180 dni od dnia wejścia dla niego w życie niniejszej Konwencji, umowy z Organizacją w sprawie okazania pomocy na wniosek;

(c) zadeklarowanie, nie później niż 180 dni od dnia wejścia dla niego w życie niniejszej Konwencji, rodzajów pomocy, jaką może ono okazać w odpowiedzi na wniosek Organizacji. Jeśli jednak Państwo-Strona nie jest w stanie okazać pomocy, przewidzianej w jego deklaracji, jest ono nadal zobowiązane do okazania pomocy zgodnie z niniejszym ustępem".

ASPEKTY BIOLOGICZNE

1. Konwencja o zakazie broni biologicznej z dnia 19 kwietnia 1972 roku[14] **(*The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological* [Biological] *and Toxin Weapons and on Their Destruction* – BWC)**

Konwencja o zakazie broni biologicznej stanowi jeden z podstawowych elementów prawnomiędzynarodowego systemu rozbrojenia i zapobiegania proliferacji broni biologicznej i bakteriologicznej. Na uwagę zasługuje to, że *Konwencja* była pierwszym wiążącym aktem prawa międzynarodowego odnoszącym się do całej kategorii broni masowego rażenia.

Konwencja zobowiązuje państwa do tego, że nigdy, w żadnych okolicznościach, nie będą prowadzić badań, produkować, gromadzić, w jakikolwiek sposób nabywać ani przechowywać:

1) mikrobiologicznych lub innych biologicznych środków czy toksyn, bez względu na pochodzenie lub sposób produkcji, takich rodzajów i w takich ilościach, które nie są przeznaczone do wykorzystania w celach profilaktycznych, ochronnych lub w innych celach pokojowych;
2) broni, urządzeń lub środków przenoszenia mających służyć wykorzystaniu takich środków lub toksyn we wrogich zamiarach lub w konfliktach zbrojnych.

Zasadniczym celem *Konwencji* jest zatem wprowadzenie ogólnego zakazu wytwarzania broni biologicznej. Nie zawiera ona natomiast przepisów odnoszących się wprost do reagowania na zdarzenia CBRN.

Rezolucja 1540 (2004) Rady Bezpieczeństwa ONZ z dnia 28 kwietnia 2004 roku

Rada Bezpieczeństwa ONZ, działając na podstawie rozdziału VII Karty Narodów Zjednoczonych, zgodnie z rezolucją 1540 zobowiązała państwa członkowskie ONZ do podjęcia działań zmierzających do ograniczenia ryzyka uzyskania broni chemicznej, biologicznej lub nuklearnej przez podmioty niepaństwowe (*non-state actors*). Do najważniejszych postanowień wyżej wymienionej rezolucji należy zobowiązanie państw do podjęcia następujących działań:

- powstrzymania się od udzielania jakichkolwiek form wsparcia aktorom pozapaństwowym dążącym do rozwijania, pozyskania, wytwarzania, posiadania, transportu, przekazywania lub wykorzystania broni chemicznej, biologicznej lub nuklearnej oraz ich nośników;
- ustanowienia przepisów prawa krajowego zakazujących rozwijania, pozyskiwania, wytwarzania, posiadania, transportu, przekazywania lub wykorzystywania broni chemicznej, biologicznej lub nuklearnej oraz ich nośników, zwłaszcza w celach terrorystycznych, jak również brania udziału w powyższych działaniach na zasadzie pomocnictwa, współudziału oraz ich finansowania;
- prowadzenia efektywnych czynności mających na celu wykrywanie działań zmierzających do niezgodnego z prawem nabycia lub sprzedaży powyższych materiałów, zapobieganie takim działaniom oraz ich zwalczanie, jak również organizowania i ułatwiania takiej sprzedaży, także dzięki współpracy międzynarodowej;

[14] *Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzona w Moskwie, Londynie i Waszyngtonie dnia 10 kwietnia 1927 roku* (Dz.U. z 1976 r. nr 1 poz. 1).

- ustanowienie skutecznego narodowego systemu kontroli eksportu, tranzytu, reeksportu i kontroli wyżej wymienionych materiałów oraz działań pośrednio z nimi związanych (np. finansowania), które mogą przyczynić się do ich proliferacji, a także ustanowienie odpowiednich sankcji za niezgodne z prawem działania w tym zakresie.

Podkreślenia wymaga to, że rezolucja 1540 ma charakter wiążący, gdyż podstawą prawną jej przyjęcia przez Radę Bezpieczeństwa ONZ był rozdział VII Karty NZ (Akcja w razie zagrożenia pokoju, naruszenia pokoju i aktów agresji). Dokument przewiduje także mechanizm kontroli wdrażania jej postanowień przez ustanowienie na podstawie art. 4 tzw. Komitetu 1540, którego zadaniem jest monitorowanie procesu implementacji dokumentu przez państwa członkowskie ONZ.

PRAWO EUROPEJSKIE

1. Unijny Mechanizm Ochrony Ludności

Podstawowym instrumentem europejskiego systemu reagowania na sytuacje kryzysowe, w tym na zdarzenia CBRN, jest Unijny Mechanizm Ochrony Ludności, którego podstawę prawną stanowi *Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 roku w sprawie Unijnego Mechanizmu Ochrony Ludności*[15]**.** Mechanizm został stworzony w 2001 r. Jego głównym celem jest wzmocnienie współpracy właściwych organów narodowych w sytuacjach kryzysowych, których skala i specyfika wykracza poza realne możliwości efektywnego reagowania państw członkowskich. Umożliwia on neutralizację skutków klęsk żywiołowych i katastrof spowodowanych przez człowieka dzięki koordynacji procesu udzielania wsparcia materialnego i organizacyjnego państwu dotkniętemu tego rodzaju zdarzeniami.

Współpraca w zakresie ochrony ludności zgodnie z art. 2 *Decyzji* obejmuje:

- działania zapobiegawcze i przygotowawcze prowadzone na terytorium Unii oraz, w niektórych przypadkach (np. na wniosek państwa spoza UE lub ONZ), także poza jej terytorium;
- działania mające wesprzeć reagowanie na bezpośrednie negatywne następstwa klęski lub katastrofy na terytorium UE lub poza nim[16], jeżeli są one podejmowane w odpowiedzi na wniosek o pomoc, który został złożony za pośrednictwem mechanizmu.

Art. 3 *Decyzji* wymienia ponadto następujące cele szczegółowe Mechanizmu:

- uzyskanie wysokiego poziomu ochrony przed klęskami i katastrofami przez zapobieganie im lub ograniczenie ich potencjalnych skutków, propagowanie działań w zakresie zapobiegania, a także przez zacieśnianie współpracy pomiędzy służbami odpowiedzialnymi za ochronę ludności i innymi odpowiednimi służbami;
- zwiększenie gotowości w zakresie reagowania na klęski i katastrofy na poziomie państw członkowskich;

[15] Dz. Urz. UE L/347/924 z 20 XII 2013 r.

[16] Zgodnie z art. 28, w Unijnym Mechanizmie Ochrony Ludności mogą uczestniczyć także państwa należące do EFTA, które są członkami Europejskiego Obszaru Gospodarczego, a także kraje przystępujące do tego Obszaru, kandydujące do niego i potencjalne kraje kandydujące, zgodnie z ogólnymi zasadami i warunkami udziału tych państw w programach UE.

- ułatwienie szybkiego i skutecznego reagowania w przypadku wystąpienia klęsk lub katastrof albo groźby ich wystąpienia;
- zwiększenie świadomości i stopnia gotowości społeczeństwa w odniesieniu do klęsk lub katastrof.

Realizacji celów Unijnego Mechanizmu Ochrony Ludności służy Centrum Koordynacji Reagowania Kryzysowego (ERCC) zapewniające zdolność operacyjną w systemie 24/7, powołane na podstawie art. 7 *Decyzji*.

2. Reagowanie na sytuacje kryzysowe, w tym na zdarzenia CBRN

Artykuł 14 *Decyzji* wprowadza obowiązek notyfikacji o klęskach i katastrofach na terytorium UE i stanowi, że w przypadku wystąpienia wyżej wymienionego zdarzenia lub groźby jego wystąpienia, mającego lub mogącego mieć skutki wykraczające poza granice jednego państwa członkowskiego, państwo, na którego terytorium zaistniała klęska lub katastrofa lub na którego terytorium przypuszczalnie jedno z tych zdarzeń nastąpi, niezwłocznie zawiadamia o tym państwa członkowskie, które mogą zostać dotknięte ich skutkami oraz – jeżeli te skutki mogą okazać się istotne – Komisję Europejską.

Państwo potencjalnie zagrożone skutkami wyżej wymienionych zdarzeń, jeżeli mogą one spowodować wezwanie o pomoc ze strony przynajmniej jednego państwa członkowskiego, niezwłocznie zawiadamia Komisję o tym, że możliwe jest złożenie za pośrednictwem ERCC wniosku o pomoc, tak aby mogła ona podjąć niezbędne czynności przygotowawcze.

W wyjątkowej sytuacji zwiększonego ryzyka państwo członkowskie może wystąpić również o pomoc w formie tymczasowego wstępnego rozmieszczenia zdolności reagowania (art. 15 ust. 2).

Art. 15 ust. 3 decyzji w sposób szczegółowy określa obowiązki Komisji po otrzymaniu wniosku o pomoc. Obejmują one stosownie do sytuacji i w sposób niezwłoczny:

- przekazanie wniosku do punktów kontaktowych państw członkowskich;
- gromadzenie, we współpracy z państwem dotkniętym katastrofą lub kryzysem, zweryfikowanych informacji o zdarzeniu i przekazywanie ich innym państwom członkowskim;
- formułowanie, w porozumieniu z państwem występującym o pomoc, zaleceń dotyczących świadczenia pomocy za pośrednictwem Unijnego Mechanizmu Ochrony Ludności oraz zwracanie się do państw członkowskich o rozmieszczenie określonych zdolności i koordynację procesu udzielania pomocy;
- podejmowanie dodatkowych działań o charakterze koordynacyjnym.

Państwo, do którego został skierowany wniosek o udzielenie pomocy, niezwłocznie określa, czy jest w stanie jej udzielić i za pośrednictwem systemu CECIS (Wspólny System Łączności i Informacji w Sytuacjach Nadzwyczajnych[17]) informuje o swojej decyzji państwo zwracające się o pomoc. Udziela również informacji na temat zakresu, zasad i kosztów pomocy, jakiej jest w stanie udzielić.

Za kierowanie interwencjami podejmowanymi w celu udzielania pomocy odpowiada państwo występujące o pomoc – ustanawia w tym celu wytyczne, a w razie potrzeby wyznacza granice zadań powierzonych określonym modułom lub innym rodzajom zdolności reagowania[18].

[17] System CECIS ma na celu umożliwienie komunikacji pomiędzy ERCC a punktami kontaktowymi państw członkowskich i wymiany informacji pomiędzy tymi podmiotami.

[18] Na mocy art. 11 *Decyzji* została ustanowiona Europejska Zdolność Reagowania Kryzysowego (EERC).

Zadaniem Komisji, na mocy art. 18 *Decyzji*, jest również wspieranie państw członkowskich w uzyskiwaniu dostępu do sprzętu lub zasobów transportowych przez:

- dostarczanie i wymianę informacji dotyczących sprzętu i zasobów transportowych, które mogą być udostępniane przez państwa członkowskie w celu łatwiejszego łączenia tych zasobów w jedną pulę;
- udzielanie państwom członkowskim pomocy w określaniu zasobów transportowych, które mogą pochodzić z innych źródeł, w tym z rynku komercyjnego, oraz ułatwianie im dostępu do tych zasobów;
- udzielanie pomocy w zakresie określenia sprzętu, który może być dostępny z innych źródeł, z uwzględnieniem rynku komercyjnego.

Ponadto Komisja może uzupełniać zasoby transportowe dostarczone przez państwa członkowskie dodatkowymi zasobami niezbędnymi do zapewnienia możliwości szybkiego reagowania w razie wystąpienia klęski lub katastrofy (art. 18 ust. 2).

3. Pozostałe elementy europejskiego systemu reagowania na zdarzenia CBRN

3.1. System ECURIE – European Community Urgent Radiological Information Exchange

System ECURIE został ustanowiony w celu wykonania *Decyzji Rady 87/600/ Euratom z dnia 14 grudnia 1987 roku w sprawie wspólnotowych warunków wczesnej wymiany informacji w przypadku pogotowia radiologicznego*[19]**.** Najważniejszymi komponentami tego systemu są:

- Convention Information Structure (CIS) – element zawierający szczegółowy opis informacji, które mogą być przekazywane za pośrednictwem systemu ECURIE, oraz formatu, w jakim mają być przesyłane;
- programowanie CoDecS umożliwiające tworzenie, wysyłanie i odbieranie informacji w formacie CIS opracowane stricte na potrzeby systemu ECURIE;
- sieć punktów kontaktowych (CPs) i właściwych organów krajowych (CAs) wyznaczonych przez państwa w celu uczestniczenia w systemie.

Najważniejsze elementy *Decyzji Rady 87/600/Euratom* zawarto w art. 1, który nakłada na państwa wchodzące w skład ECURIE obowiązek notyfikacji Komisji i państwom członkowskim potencjalnie narażonym na skutki zdarzenia, które może stwarzać zagrożenie radiologiczne, podjęcia działań w celu ochrony ogółu społeczeństwa w przypadku pogotowia radiologicznego w następstwie:

- awarii zaistniałej na własnym terytorium obejmującej obiekty lub rodzaje działalności wymienione w ust. 2, przy której nastąpił lub może nastąpić znaczny przeciek materiału radioaktywnego;
- wykrycia na terytorium własnym lub poza nim poziomów radioaktywności odbiegających od normy, które mogą być szkodliwe dla zdrowia publicznego w tym państwie członkowskim;
- awarii innych niż awaria na własnym terytorium, dotyczących obiektów lub rodzajów działalności określonych w ust. 2, przy których nastąpił lub może nastąpić znaczące uwolnienie materiału radioaktywnego.

Ten instrument ma formę dobrowolnej puli wcześniej zgłoszonych zdolności reagowania państw członkowskich; obejmuje moduły, inne zdolności reagowania oraz ekspertów.

[19] Dz. Urz. WE L 371/16 z 30 XII 1987 r.

Zgodnie z ust. 2 obiekty lub rodzaje działalności, o których mowa powyżej, to:

- każdy reaktor jądrowy, bez względu na jego lokalizację;
- każdy inny obiekt związany z jądrowym cyklem paliwowym;
- każdy obiekt służący postępowaniu z odpadami radioaktywnymi;
- transport i przechowywanie paliwa jądrowego lub odpadów promieniotwórczych;
- wytwarzanie, wykorzystywanie, przechowywanie, unieszkodliwienie i transport izotopów promieniotwórczych wykorzystywanych w rolnictwie, przemyśle, medycynie i w pokrewnych celach naukowych lub badawczych;
- wykorzystywanie izotopów promieniotwórczych do wytwarzania energii w pojazdach kosmicznych.

Jeżeli państwo zamierza podjąć działania w celu neutralizacji skutków zdarzenia, jest zobowiązane do:

- niezwłocznego poinformowania Komisji i państw członkowskich, na które takie zdarzenie ma lub może mieć wpływ, o podejmowanych środkach i powodach ich podjęcia;
- szybkiego dostarczenia Komisji i wyżej wymienionym państwom dostępnych informacji istotnych do zminimalizowania przewidywanych skutków radiologicznych zdarzenia, jeżeli występują one w tych państwach.

Informacje, o których mowa powyżej, obejmują – bez wpływu na sprawy bezpieczeństwa narodowego – następujące elementy (art. 3):

- naturę i czas wystąpienia zdarzania, jego dokładną lokalizację oraz obiekt lub rodzaj działalności, którego dotyczy zdarzenie;
- zakładaną lub ustaloną przyczynę oraz przewidywany rozwój awarii, istotny dla przecieku materiału radioaktywnego;
- ogólną charakterystykę przecieku radioaktywnego obejmującą naturę, prawdopodobną postać fizyczną i chemiczną oraz ilość, skład i efektywną wysokość przecieku;
- informacje o bieżących i przewidywanych warunkach meteorologicznych i hydrologicznych niezbędnych do prognozowania rozproszenia przecieku radioaktywnego;
- wyniki monitoringu środowiska przyrodniczego;
- wyniki pomiarów środków spożywczych, pasz i wody pitnej;
- podjęte lub planowane środki ochronne;
- podjęte lub planowane środki informowania społeczeństwa;
- przewidywaną charakterystykę zachowania przecieku wraz z upływem czasu.

Państwa, po otrzymaniu powyższych informacji, niezwłocznie powiadamiają Komisję o podjętych działaniach i zaleceniach wydanych po ich otrzymaniu. We właściwych odstępach czasu przekazują jej również informacje o poziomach promieniotwórczości w środkach spożywczych, paszach, wodzie pitnej i w środowisku (art. 4).

Komisja niezwłocznie przekazuje wszelkie informacje otrzymane na zasadach i w trybie określonym w *Decyzji* właściwym władzom państw członkowskich. Udostępnia im również wszelkie dane dotyczące znaczącego wzrostu poziomów radioaktywności lub awarii jądrowych w państwach nienależących do UE, szczególnie graniczących z jej terytorium.

3.2. Systemy wczesnego ostrzegania o zagrożeniach zdrowia[20]

W celu zapewnienia możliwości efektywnego zapobiegania i zwalczania sytuacji stanowiących zagrożenie zdrowia publicznego Komisja Europejska utworzyła trzy zasadnicze systemy wczesnego ostrzegania i alarmowania: **EWRS** (Early Warning and Response System), **RAS BICHAT** (Rapid Alerting System for Biological and Chemical Agents Attacks) oraz będący w fazie organizacji system RAS CHEM (Rapid Alerting System for Chemicals).

EWRS

Ten system stanowi mechanizm wymiany informacji wykorzystywany na wypadek zagrożenia epidemiologicznego. Z technicznego punktu widzenia jest to instrument umożliwiający komunikację pomiędzy Komisją, właściwymi organami państw członkowskich odpowiedzialnymi za nadzór epidemiologiczny oraz Europejskim Centrum ds. Zapobiegania i Kontroli Chorób (European Centre for Diseases Prevention and Control – ECDC), działający w trybie online. W systemie uczestniczą również państwa Europejskiego Obszaru Gospodarczego – Islandia, Liechtenstein i Norwegia.

EWRS działa na podstawie przepisów zawartych w dwóch aktach normatywnych ustanawiających obowiązki państw w zakresie powiadamiania o zagrożeniach epidemiologicznych oraz określających szczegółowe zasady funkcjonowania systemu, tj.:

- *Decyzji nr 2119/98/WE Parlamentu Europejskiego i Rady z dnia 24 września 1998 roku ustanawiającej sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie*[21];
- *Decyzji Komisji z dnia 22 grudnia 1999 roku w sprawie systemu wczesnego ostrzegania i reagowania w celu zapobiegania i kontroli chorób zakaźnych na mocy decyzji nr 2119/98/WE Parlamentu Europejskiego i Rady*[22].

System był wielokrotnie wykorzystywany w przypadkach zagrożenia epidemiologicznego, np. w kontekście rozprzestrzeniania się takich chorób, jak SARS czy wirus ptasiej grypy. Organem odpowiedzialnym za wsparcie naukowe i szacowanie ryzyka związanego ze zdarzeniami, których dotyczą informacje wymieniane za pośrednictwem systemu, jest Europejskie Centrum ds. Zapobiegania i Kontroli Chorób.

RAS BICHAT

Ten mechanizm służy wymianie informacji w zakresie zagrożenia zdrowia, związanych z umyślnym uwolnieniem substancji chemicznych, biologicznych i materiałów promieniotwórczych. RAS BICHAT stanowi część *Programu współpracy w zakresie przygotowania i reagowania na ataki z wykorzystaniem środków biologicznych i chemicznych* opracowanego przez Komisję[23].

---

[20] European Commission early warning and rapid alert systems in the field of heath threats, www.ec.europa.eu/health/preparedness_response/generic_preparedness/planning/rapid_alert_en {dostęp: 15 III 2017].

[21] Dz. Urz. WE L 268/1 z 3 X 1998 r.

[22] Dz. Urz. WE L 21/32 z 26 I 2000 r.

[23] Programme of Cooperation on Preparedness and Response to Biological and Chemical Agent Attacks, Luxemburg, 17 December 2001, G/FS D (2001) GG.

Zasady działania RAS BICHAT są analogiczne do EWRS – najważniejszymi elementami są tu system notyfikacji o zagrożeniach związanych z potencjalnym wykorzystaniem lub groźba wykorzystania środków biologicznych albo chemicznych oraz wymiana informacji i koordynacja działań właściwych organów państw członkowskich. Głównym celem ustanowienia systemu było wsparcie członków Komitetu Bezpieczeństwa Zdrowotnego mianowanych przez ministrów właściwych ds. zdrowia (Health Security Committee)[24] w celu usprawnienia koordynacji działań zmierzających do osiągnięcia gotowości i opracowania ewentualnych instrumentów reagowania na wypadek ataku z wykorzystaniem środków biologicznych lub chemicznych.

RAS CHEM

Ten system stanowi mechanizm mający na celu ustanowienie sieci szybkiej wymiany informacji i wczesnego ostrzegania pomiędzy właściwymi organami krajowymi w zakresie incydentów transgranicznych polegających na wykorzystaniu środków chemicznych, które mogą być potencjalnie powiązane ze zdarzeniami o charakterze terrorystycznym.

CZĘŚĆ II
Prawo krajowe

1. Rozwiązania systemowe

Akty prawne odnoszące się w swojej treści do reagowania na zdarzenia i zagrożenia chemiczne, biologiczne, radiologiczne i nuklearne są rozproszone w krajowym prawodawstwie w licznych ustawach i aktach wykonawczych, a także w dokumentach rządowych i samorządowych.

Systemowe rozwiązania merytoryczne określa *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (Dz.U. z 2017 r. poz. 1430), dalej zwana „ustawą o powszechnym obowiązku obrony", i wydany na jej podstawie akt wykonawczy.

Na mocy art. 6 ustawy o powszechnym obowiązku obrony do zadań Rady Ministrów wykonywanych w ramach zapewniania zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju należy zwłaszcza:

1) opracowywanie projektów strategii bezpieczeństwa narodowego;
2) planowanie i realizacja przygotowań obronnych państwa zapewniających jego funkcjonowanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny, w tym planowanie przedsięwzięć gospodarczo-obronnych oraz zadań wykonywanych na rzecz sił zbrojnych i wojsk sojuszniczych;
3) przygotowywanie systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, i organów władzy publicznej do funkcjonowania na stanowiskach kierowania;
4) utrzymywanie stałej gotowości obronnej państwa, wnioskowanie do Prezydenta Rzeczypospolitej Polskiej o jej podwyższanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny oraz o jej obniżanie, stosownie do zmniejszania się stopnia zagrożenia;

[24] https://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/rapid_alert_en [dostęp: 26 IX 2017].

5) określanie obiektów szczególnie ważnych dla bezpieczeństwa państwa, w tym obronności, oraz przygotowywanie ich szczególnej ochrony;
6) **przygotowanie na potrzeby obronne państwa i utrzymywanie w stałej gotowości jednolitych systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania**;
7) przygotowanie systemu stałych dyżurów na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny;
8) określanie zasad wykorzystania służby zdrowia i infrastruktury technicznej państwa na potrzeby obronne, w tym sposobu zabezpieczania przestrzeni powietrznej i wód terytorialnych w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny;
9) zapewnianie funkcjonowania systemu szkolenia obronnego w państwie;
10) prowadzenie kontroli stanu przygotowań obronnych w państwie.

Rada Ministrów została zobowiązana do określenia, w drodze rozporządzenia, trybu realizacji zadań, o których mowa powyżej, w szczególności organizacji i warunków przygotowania oraz sposobu funkcjonowania systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach na terytorium Rzeczpospolitej Polskiej, a także o właściwości organów w tych sprawach (art. 6 ust. 2 pkt 5 ustawy o powszechnym obowiązku obrony).

Pierwotny zapis art. 6 ust. 2 pkt 5 powyższej ustawy dotyczył jedynie zagrożeń promieniotwórczych, jednak w 2006 r. został znowelizowany[25] w taki sposób, że wykreślono wyraz „promieniotwórczych", w konsekwencji czego prawodawca był obowiązany do wydania rozporządzenia obejmującego nie tylko kwestie promieniotwórcze, ale *per analogiam* mógł również uregulować zagadnienia chemiczne i biologiczne. Akt wykonawczy, który następnie wydano, tj. *Rozporządzenie Rady Ministrów z dnia 16 października 2006 r. w sprawie wykrywania skażeń i właściwości organów w tych sprawach* (Dz.U. nr 191 poz. 1415) wszedł w życie 31 października 2006 r., co stanowiło pierwotną podstawę prawną do uruchomienia i rozwijania jednolitego **systemu wykrywania skażeń i alarmowania.**

Należy wskazać, że obecnie obowiązuje *Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach* (Dz.U. z 2013 r. poz. 96), dalej zwane „rozporządzeniem KSWSiA". **Treść pierwotnego rozporządzenia dostosowano do przepisów *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. z 2017 r. poz. 209, ze zm.), w związku z czym przepisy w zakresie reagowania na zagrożenia CBRN stały się również przedmiotem krajowego planu zarządzania kryzysowego, a także innych planów, o których mowa w tejże ustawie.** Na płaszczyźnie dokumentu zatytułowanego. *Krajowy Plan Zarządzania Kryzysowego 2013–2015* w części I – *Plan Główny*, w rozdziale *Charakterystyka zagrożeń oraz ocena ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej* wyodrębniono m.in.: epidemie, skażenia chemiczne, skażenia radiacyjne, epizootie oraz zagrożenie terrorystyczne. Przykładowo w *Planie Zarządzania Kryzysowego m.st. Warszawy* w *Planie Głównym*, w części *Charakterystyka zagrożeń* wydzielono m.in. zagrożenia radiacyjne, chemiczne, epidemiczne, epizootyczne, a także terroryzm.

[25] *Ustawa z dnia 29 lipca 2005 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz o zmianie ustawy o służbie zastępczej* (Dz.U. nr 180 poz. 1496).

W rozporządzeniu KSWSiA określono, że przez (...) *systemy wykrywania skażeń i alarmowania o skażeniach* rozumie się powiązany organizacyjno-technicznie zespół elementów przeznaczonych do identyfikacji skażeń, wytwarzania, gromadzenia, przetwarzania i wstępnej analizy informacji o uwolnieniu do środowiska toksycznych środków chemicznych, materiałów promieniotwórczych, zakaźnych czynników biologicznych i powstaniu ognisk zakażeń, a także o powstałych w następstwie takich zdarzeń skażeniach i potencjalnych źródłach tych zagrożeń.

W § 2 pkt 10 rozporządzenia KSWSiA określono, że rozpoznanie skażeń jest rozumiane jako działanie mające na celu stwierdzenie obecności substancji promieniotwórczych, środków biologicznych lub chemicznych, jak również jako uzupełnienie i potwierdzenie wstępnych meldunków. Natomiast skażenie, zgodnie z pkt 11, to: zanieczyszczenie środowiska, zwłaszcza gruntu, wody, powietrza, żywności, pasz oraz powierzchni ciała ludzi lub zwierząt niebezpiecznymi substancjami i mieszaninami chemicznymi, materiałami promieniotwórczymi lub zakaźnymi czynnikami biologicznymi, niezależnie od ich rodzaju i czasu ich oddziaływania.

Na podstawie § 3 rozporządzenia KSWSiA w przypadku wprowadzenia stanu nadzwyczajnego, w celu zapobieżenia skutkom katastrofy naturalnej, awarii technicznej lub działań terrorystycznych, które mogą spowodować wystąpienie skażeń chemicznych, biologicznych lub promieniotwórczych, jak również w przypadku przeprowadzania treningów i ćwiczeń, systemy działają lub są uruchamiane i rozwijane w ramach jednolitego krajowego systemu wykrywania skażeń i alarmowania, zwanego dalej krajowym systemem.

Nadzór nad funkcjonowaniem krajowego systemu i funkcje koordynacyjne sprawuje minister obrony narodowej przy pomocy centrum dyspozycyjnego, którego rolę odgrywa Centralny Ośrodek Analizy Skażeń Sił Zbrojnych. Minister obrony narodowej we współpracy z ministrami właściwymi do spraw: wewnętrznych, zdrowia, administracji publicznej, rolnictwa, rynków rolnych, gospodarki morskiej, środowiska oraz gospodarki wodnej opracowuje, aktualizuje i uruchamia plany i procedury współdziałania organów i jednostek organizacyjnych nadzorowanych przez tych ministrów lub im podległych w realizacji zadań w ramach krajowego systemu (§ 3 ust. 2 i 3 rozporządzenia KSWSiA).

Plany i procedury, o których mowa w ust. 3, stanowią załączniki do planów zarządzania kryzysowego właściwych ministrów (§ 3 ust. 4 rozporządzenia KSWSiA).

W myśl § 4 rozporządzenia KSWSiA w skład krajowego systemu wchodzą:

1) systemy wykrywania skażeń i alarmowania o skażeniach obejmujące:
   a) system wykrywania skażeń sił zbrojnych Rzeczpospolitej Polskiej – nadzorowany przez ministra obrony narodowej,
   b) sieci i systemy nadzoru epidemiologicznego oraz kontroli chorób zakaźnych w kraju, a także krajowe punkty kontaktowe dla międzynarodowych systemów nadzoru nad zagrożeniami zdrowia lub życia dużych grup ludności – nadzorowane przez ministra właściwego do spraw zdrowia,
   c) system stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych, których działania koordynuje Prezes Państwowej Agencji Atomistyki,
   d) nadzorowane przez wojewodów wojewódzkie systemy wykrywania i alarmowania oraz wojewódzkie systemy wczesnego ostrzegania o zagrożeniach, o których mowa w art. 16 ust. 2 pkt 3 ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209, ze zm.) i w § 3 pkt 6

rozporządzenia Rady Ministrów z 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin (Dz.U. poz. 850), w części dotyczącej skażeń,

e) systemy nadzoru epizootycznego, fitosanitarnego, nadzoru nad bezpieczeństwem produktów pochodzenia zwierzęcego i paszami oraz nadzoru nad produktami rolno-spożywczymi, kontrolowane przez ministrów właściwych do spraw rolnictwa i rynków rolnych oraz zdrowia;

2) organy i jednostki organizacyjne, które dokonują analizy skażeń i oceny sytuacji oraz opracowują, ogłaszają i wprowadzają działania interwencyjne, obejmujące:

a) organy i jednostki organizacyjne prowadzące działania interwencyjne w sytuacji wystąpienia skażeń – nadzorowane przez ministra obrony narodowej, ministrów właściwych do spraw wewnętrznych, zdrowia, środowiska i rolnictwa lub im podległe oraz nadzorowane przez wojewodów,

b) formacje obrony cywilnej wykonujące działania w zakresie monitoringu, wykrywania i rozpoznania skażeń oraz alarmowania o skażeniach – tworzone i nadzorowane przez podmioty wymienione w art. 138 ust. 3 i 4 ustawy z 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczpospolitej Polskiej,

c) dyrektorów urzędów morskich w zakresie swoich kompetencji, o których mowa w art. 42 ust. 2 pkt 1, 1a, 5 i 6 ustawy z 21 marca 1991 r. o obszarach morskich Rzeczpospolitej Polskiej i administracji morskiej (Dz.U. z 2016 r. poz. 2145, ze zm.),

d) inne organy i jednostki organizacyjne wykonujące obserwacje skażeń oraz ich pomiary, powiadamiające o skażeniach na terenie kraju, włączone do systemów, o których mowa w § 1, na podstawie umów i porozumień – zgodnie z tymi porozumieniami.

Należy dodać, że na mocy § 6 rozporządzenia KSWSiA jednolitość i interoperacyjność funkcjonowania systemów wchodzących w skład krajowego systemu zapewniają organy, którym te systemy podlegają lub które je nadzorują. Ponadto koordynację w zakresie jednolitości i interoperacyjności funkcjonowania systemów wchodzących w skład krajowego systemu zapewnia minister obrony narodowej we współpracy z ministrami wymienionymi w § 3 ust. 3 rozporządzenia KSWSiA (spraw wewnętrznych, zdrowia, administracji publicznej, rolnictwa, rynków rolnych, gospodarki morskiej, środowiska oraz gospodarki wodnej), a także dyrektorem Rządowego Centrum Bezpieczeństwa.

Organy i jednostki organizacyjne, które dokonują analizy skażeń i oceny sytuacji, w przypadku wykrycia zagrożenia skażeniami lub stwierdzenia skażeń przez podległe im systemy, są obowiązane do niezwłocznego powiadamiania organu administracji publicznej właściwego terytorialnie dla miejsca takiego zdarzenia.

Minister obrony narodowej oraz ministrowie właściwi do: spraw gospodarki morskiej, spraw wewnętrznych oraz spraw administracji publicznej we współpracy z wojewodami prowadzą ogólnokrajowe treningi uruchamiania systemów i ich pracy w ramach krajowego systemu nie rzadziej niż raz w roku, a także ogólnokrajowe ćwiczenia dotyczące systemów – nie rzadziej niż raz na trzy lata. Dyrektor Rządowego Centrum Bezpieczeństwa jest informowany o ogólnokrajowych treningach i ćwiczeniach przez ministra obrony narodowej.

Ponadto zgodnie z § 7 rozporządzenia KSWSiA systemy wchodzące w skład krajowego systemu zapewniają zwłaszcza:

1) realizację sojuszniczych zobowiązań Rzeczpospolitej Polskiej oraz zobowiązań wynikających z ratyfikowanych porozumień międzynarodowych w zakresie obserwacji, pomiarów, analiz prognozowania skażeń i powiadamiania o skażeniach na terytorium Rzeczpospolitej Polskiej;
2) monitorowanie skażeń, ich wykrywanie i rozpoznanie, umożliwiające natychmiastowe stwierdzenie wzrostu poziomu skażeń na podstawie standardów i norm krajowych;
3) ostrzeganie i alarmowanie ludności lub Sił Zbrojnych Rzeczpospolitej Polskiej o skażeniach;
4) opracowywanie ocen eksperckich dotyczących stanu zagrożenia skażeniami i przygotowywanie zaleceń postępowania ochronnego;
5) doradztwo specjalistyczne w zakresie metodyki ograniczania zasięgu i skutków oddziaływania skażeń;
6) uruchamianie systemów wykrywania skażeń i alarmowania o skażeniach ludności lub Sił Zbrojnych Rzeczpospolitej Polskiej oraz uruchamianie działań interwencyjnych.

W myśl § 8 przygotowaniem systemów wchodzących w skład krajowego systemu do wykonywania zadań, o których mowa w § 7 (m.in. realizacja zobowiązań sojuszniczych Rzeczpospolitej Polskiej, monitorowanie i wykrywanie skażeń, ostrzeganie i alarmowanie ludności lub sił zbrojnych) zajmują się w zakresie swoich kompetencji organy i jednostki organizacyjne, o których mowa w § 4 pkt 2 (m.in. organy i jednostki prowadzące działania interwencyjne w sytuacji wystąpienia skażeń – nadzorowane przez właściwych ministrów, np. ministra obrony narodowej czy spraw wewnętrznych), w stosunku do podlegających im systemów.

Trzeba zauważyć, że funkcjonowanie systemu, organu lub jednostki organizacyjnej w krajowym systemie nie zmienia ich podległości organizacyjnej, a zwłaszcza podległości systemu Sił Zbrojnych Rzeczpospolitej Polskiej oraz systemów określonych w przepisach dotyczących prawa atomowego, administracji rządowej w województwie, zwalczania chorób zakaźnych i zakażeń ludzi, zwierząt i roślin oraz zapobiegania zanieczyszczaniu morza przez statki (§ 12 rozporządzenia KSWSiA).

Sygnały alarmowe i komunikaty ostrzegawcze powszechnie obowiązujące na terytorium Rzeczpospolitej Polskiej określa załącznik do rozporządzenia (§ 10 ust. 1 rozporządzenia KSWSiA). Natomiast decyzje o wprowadzeniu lub ogłoszeniu sygnału alarmowego lub komunikatu ostrzegawczego, a także o ich odwołaniu, podejmuje właściwy terytorialnie organ administracji publicznej (§ 10 ust. 4 rozporządzenia KSWSiA).

2. Podmioty prawnie obowiązane do reagowania na zagrożenia CBRN

Najważniejszymi podmiotami reagującymi na zdarzenia i zagrożenia CBRN w Polsce są m.in.:

1) Państwowa Straż Pożarna (zakładowe straże pożarne/zakładowe służby ratownicze):
   – *Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej* (Dz.U. z 2017 r. poz. 1204, ze zm.)
   – *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 września 2008 r. w sprawie szczegółowych warunków bezpieczeństwa i higieny służby strażaków Państwowej Straży Pożarnej* (Dz.U. poz. 1115);

2) Siły Zbrojne Rzeczpospolitej Polskiej:
   – *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (Dz.U. z 2017 r. poz. 1430, ze zm.),
   – *Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach* (Dz.U. z 2013 r. poz. 96),
   – *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu* kryzysowym (Dz.U. z 2017 r. poz. 209, ze zm.);
3) szpitalne oddziały ratunkowe Państwowego Ratownictwa Medycznego:
   – *Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym* (Dz.U. z 2016 r. poz. 1868, ze zm.),
   – *Rozporządzenie Ministra Zdrowia z dnia 3 listopada 2011 r. w sprawie szpitalnego oddziału ratunkowego* (Dz.U. z 2015 r. poz. 178, ze zm.),
   – *Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi* (Dz.U. z 2016 r. poz. 1866, ze zm.);
4) Policja;
   – *ustawa z dnia 6 kwietnia 1990 r. o Policji* (Dz.U. z 2016 r. poz. 1782, z późn. zm.),
   – *zarządzenie nr 1429 Komendanta Głównego Policji z dnia 31 grudnia 2004 r. w sprawie wprowadzenia w Policji procedur reagowania w sytuacjach kryzysowych* (Dz. Urz. KGP nr 3 poz. 8);
5) Państwowa Agencja Atomistyki, Zakład Unieszkodliwiania Odpadów Promieniotwórczych:
   – *Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe* (Dz.U. z 2017 r. poz. 576, ze zm.),
   – *Projekt rozporządzenia Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych* (Dz.U. poz. 169, ze zm.);
6) Państwowa Inspekcja Sanitarna oraz Państwowa Inspekcja Sanitarna Ministerstwa Spraw Wewnętrznych i Administracji:
   – *Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej* (Dz.U. z 2017 r. poz. 1261, ze zm.),
   – *Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi* (Dz.U. z 2016 r. poz. 1866, ze zm.);
7) Inspekcja Ochrony Środowiska, w tym wojewódzkie inspektoraty ochrony środowiska:
   – *Ustawa z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska* (Dz.U. z 2016 r. poz. 1688, ze zm.);
8) Zespoły Zarządzania Kryzysowego (zespół rządowy, zespoły tworzone przez ministrów oraz kierowników) i administracji samorządowej (wojewódzkie, powiatowe i gminne):
   – *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. z 2017 r. poz. 209, ze zm.);
9) Straż Graniczna:
   – *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (Dz.U. z 2016 r. poz. 1643, ze zm.);
10) Morska Służba Poszukiwania i Ratownictwa:
   – *Ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim* (Dz.U. z 2016 r. poz. 281, ze zm.);

- *Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 22 czerwca 2012 r. w sprawie szczegółowej organizacji Morskiej Służby Poszukiwania i Ratownictwa* (Dz.U. poz. 733);

11) Agencja Rezerw Materiałowych:
   - *Ustawa z dnia 29 października 2010 r. o rezerwach strategicznych* (Dz.U. z 2016 r. poz. 1635, ze zm.).

3. Reagowanie na zdarzenia o charakterze terrorystycznym w sferze CBRN

Aktem prawnym ustanawiającym ramy prawne dotyczące reagowania na zdarzenia o charakterze terrorystycznym jest *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. z 2016 r. poz. 904, ze zm.).

Zgodnie z art. 3 ust. 2 wyżej wymienionej ustawy minister właściwy do spraw wewnętrznych odpowiada za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia. To zadanie realizuje Policja, w ramach swoich kompetencji ustawowych.

Ministrowi spraw wewnętrznych i administracji podlega Komendant Główny Policji. W strukturę Komendy Głównej Policji wchodzi Biuro Operacji Antyterrorystycznych Komendy Głównej Policji, dalej zwane „BOA KGP". Zgodnie z treścią *Decyzji nr 6/2016 dyrektora BOA KGP z dnia 18 kwietnia 2016 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Operacji Antyterrorystycznych Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcą oraz katalogu zadań komórek organizacyjnych* w strukturze BOA KGP funkcjonuje Wydział Wsparcia Operacyjnego, w którego skład wchodzi Zespół Zabezpieczenia Operacyjnego. Do zadań tego Zespołu należy m.in.:

1) uczestniczenie w czynnościach prowadzonych przez Biuro w ramach sił wspierających realizację działań bojowych w strefie skażonej CBRN oraz w zakresie wyznaczonym przez dowodzącego;
2) koordynacja współpracy Policji w zakresie ochrony przed zagrożeniami CBRN z najważniejszymi podmiotami państwowymi zajmującymi sie tymi zagadnieniami;
3) koordynacja lokalnego doskonalenia zawodowego związanego z zagrożeniami niekonwencjonalnymi CBRN;
4) współpraca w zakresie zagrożeń CBRN ze specjalnymi jednostkami interwencyjnymi Grupy ATLAS;
5) opracowywanie planów dotyczących zabezpieczeń CBRN;
6) wspieranie działań minersko-pirotechnicznych w przypadkach CBRN;
7) wykonywanie zadań minersko-pirotechnicznych podczas działań prowadzonych w ramach sił wsparcia, w sytuacjach kryzysowych, zagrożenia lub dokonania przestępstwa o charakterze terrorystycznym, z użyciem materiału lub urządzenia wybuchowego lub podobnie działających środków, w zakresie ich lokalizowania, rozpoznawania, usuwania, neutralizowania, transportu i niszczenia;
8) organizowanie i prowadzenie lokalnego doskonalenia zawodowego dla policjantów dotyczącego minerstwa i pirotechniki zagrożeń CBRN oraz psów bojowych.

3.1. Krajowe przepisy wdrażające regulacje międzynarodowe

W Polsce *Ustawą z dnia 22 czerwca 2001 r. o wykonywaniu Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów* (Dz.U. nr 76 poz. 812, ze zm.), zostały uchwalone przepisy dotyczące zasad wykonywania na terytorium Rzeczypospolitej Polskiej zobowiązań wynikających z *Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, sporządzonej w Paryżu dnia 13 stycznia 1993 r.* (Dz.U. z 1999 r. poz. 703).

W poprzednich latach były prowadzone także prace legislacyjne nad *Projektem ustawy o wykonywaniu Konwencji o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu i bezpieczeństwie biologicznym*, jednak do chwili obecnej tej ustawy nie uchwalono. Nie jest ona również przedmiotem uzgodnień międzyresortowych.

3.2. Inne dokumenty rządowe i akty prawne istotne z punktu widzenia problematyki CBRN

W Polsce problematyka CBRN jest poruszana w dokumentach rządowych oraz innych, m.in. w:

1) *Uchwale Nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (M.P. poz. 1218);
2) uchwale nr 11 Komitetu do Spraw Bezpieczeństwa Euro 2012, na której podstawie 7 października 2011 r. przyjęto koncepcję zabezpieczenia z uwagi na możliwość wystąpienia zagrożeń CBRN pn. *Wytyczne w zakresie zabezpieczenia Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 w odniesieniu do zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych (CBRN) oraz dekontaminacji*.

W pierwszym dokumencie w pkt 2.1. pt. *Diagnoza zjawiska terroryzmu na 2014 r.* w ppkt 2.1.1. pt. *Ujęcie krajowe* stwierdzono, że:

Na uwagę zasługuje także zagrożenie terroryzmem związanym z wykorzystaniem broni masowego rażenia (BMR). Wprawdzie w Polsce dotychczas nie ujawniono bezpośrednich działań związanych z próbami pozyskiwania na dużą skalę lub użycia czynników chemicznych, biologicznych, radiacyjnych i nuklearnych (CBRN) do działań terrorystycznych, należy jednak zwrócić uwagę, że organizacje terrorystyczne starają się uzyskać dostęp do substancji i materiałów, które użyte w zamachu zapewniłyby jak największą siłę rażenia i spowodowałyby jak najdotkliwsze straty.

Ponadto w ppkt 2.2.5. pt. *Wyzwania dla systemu antyterrorystycznego RP* stwierdza się, że:

> Mając na uwadze, iż przedsięwzięcia realizowane w ramach systemu antyterrorystycznego RP muszą zapewnić ochronę kraju w odniesieniu nie tylko do tradycyjnych metod działania organizacji terrorystycznych, ale również zagrożeń niekonwencjonalnych, celowe jest rozwijanie współpracy oraz koordynacji działań w zakresie zapobiegania proliferacji broni masowego rażenia i środków jej przenoszenia oraz reagowania na zagrożenia o charakterze terrorystycznym z użyciem czynników CBRN. Stosownie do powyższego, należy również intensyfikować działania właściwych służb i instytucji w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni.

Jednocześnie w załączniku, w części dotyczącej pkt 4. pt. *Mechanizmy realizacji programu*, w pkt 4.1., w tabeli nr 1 pt. *Zadania i obowiązki wybranych uczestników zarządzania kryzysowego w przypadku zagrożenia o charakterze terrorystycznym w oparciu o Krajowy Plan Zarządzania Kryzysowego* w *Fazie Reagowania*, w kolumnie pt. *Zdolność do reagowania na zagrożenia CBRN* wskazano, że:

Elementem warunkującym efektywność systemu antyterrorystycznego RP jest również zdolność do skutecznego reagowania na zdarzenia z użyciem czynników chemicznych, biologicznych, radiacyjnych i nuklearnych. Zagrożenie terroryzmem związanym z wykorzystaniem broni masowego rażenia powoduje konieczność podejmowania przez właściwe służby i instytucje działań ukierunkowanych na zapobieganie proliferacji czynników i elementów do produkcji tego rodzaju broni, jak również przygotowanie do reagowania i usuwania skutków w przypadku ewentualnych ataków z jej użyciem.

W przypadku drugiego dokumentu, tj. *Wytycznych w zakresie zabezpieczenia Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 w odniesieniu do zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych (CBRN) oraz dekontaminacji*, nie uzyskano jego treści.

4. Wnioski

W Polsce istnieje system reagowania na zdarzenia CBRN. Nadzoruje go minister obrony narodowej. System ten został zaimplementowany do planów zarządzania kryzysowego. Zadania i obowiązki podmiotów odpowiedzialnych za reagowanie na zdarzenia CBRN są uregulowane w ustawach, które je ustanawiają. W celu reagowania na zdarzenia CBRN stosowne podmioty realizują zadania zgodnie ze swoją właściwością i podlegają właściwym przełożonym. Przykładowo, w Państwowej Straży Pożarnej działają jednostki ratownictwa chemicznego i ekologicznego w ramach Krajowego Systemu Ratowniczo-Gaśniczego. Do zakresu działania np. Państwowej Inspekcji Sanitarnej w zakresie zapobiegania i zwalczania chorób należy dokonywanie analiz i ocen epidemiologicznych. Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy prowadzi pomiary radioaktywności atmosfery w sieci wczesnego wykrywania skażeń promieniotwórczych. Ministrowi właściwemu do spraw gospodarki morskiej podlega Morska Służba Poszukiwania i Ratownictwa, która może wykrywać skażenia w obszarze Morza Bałtyckiego i reagować na nie (realizuje procedury zawarte w Krajowym Planie Zwalczania Zagrożeń i Zanieczyszczeń Morza).

W doktrynie wskazuje się[26], że w przypadku wykrycia skażeń promieniotwórczych, chemicznych lub biologicznych informacja o nich jest przesyłana przez podmiot, który wykrył skażenie (obserwatora, posterunek, instytucję itd.) do resortowej jednostki wiodącej, odpowiedzialnej za prowadzenie wymiany informacji z Centrum Dyspozycyjnym KSWSiA (komórka organizacyjna). Do takich jednostek zalicza się:

1) Departament Spraw Obronnych Ministerstwa Zdrowia;
2) Punkt Kierowania Systemu Wykrywania Skażeń Sił Zbrojnych RP;
3) Morskie Ratownicze Centrum Koordynacyjne;
4) Centrum ds. Zdarzeń Radiacyjnych Państwowej Agencji Atomistyki;
5) Oficera Operacyjnego MSWiA;
6) Krajowe Centrum Koordynacji Ratownictwa i Ochrony Ludności.

[26] Szerzej na ten temat: www.sgsp.edu.pl, wykład dr. Józefa Łabędzkiego (Szkoła Główna Służby Pożarniczej) dotyczący *Krajowego Systemu Wykrywania Skażeń i Alarmowania*.

Na postawie powyższej informacji Centrum Dyspozycyjne KSWSiA sporządza ocenę sytuacji i projekty komunikatów ostrzegawczych, które przesyła do Rządowego Centrum Bezpieczeństwa. Szczegółowe uregulowania, w tym procedury, w zakresie współdziałania zostały uzgodnione przez przedstawicieli resortów, których podmioty wchodzą w skład KSWSiA, i zawarte w dokumencie pn. *Plan współdziałania jednostek organizacyjnych wchodzących w skład jednolitego krajowego systemu wykrywania skażeń i alarmowania*.

W kontekście reagowania na zdarzenia CBRN o charakterze terrorystycznym główną rolę powierzono Policji, a szczegółowe zadania w zakresie CBRN realizuje Biuro Operacji Antyterrorystycznych KGP. Problematyka dotycząca CBRN została ujęta również w Narodowym Programie Antyterrorystycznym.

Ostatnie ćwiczenia z zakresu reagowania na zdarzenia CBRN zostały przeprowadzone pod kryptonimem „Patrol-2015”[27]. Zorganizowano je w Świerku, w Narodowym Centrum Badań Jądrowych. Jednym z elementów ćwiczeń sprawdzających działanie Krajowego Systemu Wykrywania Skażeń i Alarmowania było hipotetyczne uwolnienie materiału promieniotwórczego z jednego z obiektów instytutu w wyniku ataku terrorystycznego .

Jak wynika z powyższego, KSWSiA jest podstawowym systemem reagowania na zdarzenia CBRN w Polsce. Pomimo wielu podmiotów zaangażowanych w jego funkcjonowanie, wydaje się być spójny i komplementarny. Pozytywnie należy odnieść się do realizacji przez ustawodawcę przepisów dotyczących organizacji ćwiczeń z zakresu CBRN, które umożliwiają sprawdzenie reakcji poszczególnych podmiotów oraz sposobu ich współdziałania, a także opracowanie szczegółowych wytycznych na wypadek powstania sytuacji kryzysowej związanej z użyciem określonego czynnika biologicznego, chemicznego radiologicznego lub nuklearnego.

[27] https://www.ncbj.gov.pl/pl/aktualnosci/podsumowanie-cwiczen-patrol-2015-swierku [dostęp: 26 IX 2017].

Paweł Antosiak
Jakub Pałka

Wybrane aspekty ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Problemy, interpretacje oraz propozycje ewentualnych rozwiązań legislacyjnych

1. Wstęp

Wnioski wynikające z praktycznego stosowania przepisów obowiązującej już od ponad sześciu lat ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[1] (zwanej dalej „ustawą") umożliwiają wskazanie tych obszarów systemu ochrony informacji niejawnych w Rzeczpospolitej Polskiej, w których przypadku przyjęte rozwiązania prawne, organizacyjne i proceduralne nie są w pełni efektywne. Tym samym możliwe jest sformułowanie propozycji takich zmian legislacyjnych w powyższym zakresie, które mogłyby znacznie wzmocnić skuteczność działania systemu ochrony informacji niejawnych przez uwzględnienie wieloletniego doświadczenia nabytego przez organy sprawujące nadzór nad tym systemem oraz pozostałe podmioty ustawy, jak również dostosowałyby tę ustawę do wprowadzanych zmian w systemie bezpieczeństwa państwa, którego częścią jest system ochrony informacji niejawnych. Stwierdzone problemy związane ze stosowaniem przepisów ustawy wskazują przede wszystkim na potrzebę dalszego doprecyzowania i zracjonalizowania rozwiązań przyjętych w 1999 i 2010 r.

W związku z tym warto rozważyć dokonanie zmian o znaczeniu zasadniczym dla prawidłowego i efektywniejszego funkcjonowania systemu ochrony informacji niejawnych, a także wzmocnienie – tam, gdzie nie powoduje to żadnego zagrożenia interesu ochrony informacji niejawnych – pozycji obywatela względem państwa i jego organów, jako głównych podmiotów odpowiedzialnych za prawidłowe funkcjonowanie systemu ochrony tych informacji.

W niniejszym opracowaniu nie zawarto wszystkich problemów i związanych z nimi ewentualnych propozycji zmian, a tylko te zasadnicze, w tym rozwiązania, które – w subiektywnej opinii autorów opracowania – istotnie wzmocniłyby system ochrony informacji niejawnych w RP. Dlatego byłoby wskazane, aby stały się one elementem składowym przepisów regulujących jego funkcjonowanie.

2. Organizacja systemu ochrony informacji niejawnych

System ochrony informacji niejawnych w Rzeczpospolitej Polskiej powinien zapewniać stosowanie jednolitych standardów w zakresie tej ochrony w odniesieniu do wszystkich jednostek organizacyjnych uczestniczących w obiegu takich informacji. Zachowanie pełnej spójności wyżej wymienionego systemu i jednolitości stosowanych rozwiązań wymagałoby zasadniczej zmiany ustawowej mającej na celu ustanowienie jednego organu sprawującego ogólny nadzór nad tym systemem, zarówno w sferze cy-

[1] Dz.U. z 2016 r. poz. 1167, ze zm.

wilnej, jak i wojskowej. Biorąc pod uwagę pozytywne doświadczenia wynikające ze stosowania przepisów dotyczących nadzoru ABW nad informacjami niejawnymi międzynarodowymi (art. 11 ustawy), właściwe wydaje się wprowadzenie analogicznego modelu sprawowania nadzoru nad krajowymi informacjami niejawnymi, tj. przypisanie głównej roli jednemu organowi w sprawowaniu nadzoru nad systemem ochrony tych informacji, co pozwoliłoby uniknąć rozbieżnych interpretacji, a przez to – odmiennego stosowania przepisów ustawy przez ABW i SKW.

Widocznym mankamentem ustawy stało się niedostatecznie precyzyjne uregulowanie działalności osób najważniejszych dla systemu ochrony informacji niejawnych, tj. kierownika jednostki organizacyjnej, pełnomocnika ochrony (i jego zastępcy), kierownika kancelarii tajnej, inspektora bezpieczeństwa teleinformatycznego i administratora systemu. Przy czym nie chodzi tu jedynie o wymogi, jakie te osoby powinny spełniać, aby pełnić funkcje wynikające z ustawy, ale o istotny z punktu widzenia prawidłowości funkcjonowania systemu ochrony informacji niejawnych problem, jakim jest określenie, kogo należy uważać np. za kierownika jednostki w rozumieniu ustawy, co dotychczas jest w różny sposób interpretowane – zwłaszcza w jednostkach administracji publicznej.

W związku z powyższym wskazane byłoby przede wszystkim doprecyzowanie pojęcia kierownik jednostki organizacyjnej pojawiającego się w treści ustawy, przez określenie w sposób jednoznaczny, kto pełni tę funkcję (a tym samym ponosi odpowiedzialność za ochronę informacji niejawnych), tj. przez wprowadzenie jego definicji. W opinii autorów opracowania kierownikiem jednostki organizacyjnej powinna być osoba stojąca na jej czele, która nią zarządza i zapewnia – przy pomocy lub za pośrednictwem podległych pracowników – realizację jej zadań. Taka definicja uniemożliwia przyjęcie rozwiązania (dotychczas często spotykanego) polegającego na wyznaczeniu do pełnienia roli kierownika jednostki organizacyjnej innej osoby, niż kierująca daną jednostką. Oczywiście ta propozycja musiałaby uwzględniać odmienność traktowania osoby pełniącej funkcję kierownika przedsiębiorcy z uwagi na konieczność uwzględnienia mnogości form reprezentowania podmiotów gospodarczych wynikających z odrębnych przepisów. Tak skonstruowany przepis dodatkowo spowodowałby zaniechanie faktycznego kontestowania przez kierowników jednostek organizacyjnych zasady bezpośredniej podległości pełnomocnika ochrony kierownikowi jednostki organizacyjnej, przejawiającego się w usytuowaniu pionu ochrony i pełnomocnika ochrony w strukturze innych komórek organizacyjnych.

Kolejnym krokiem mającym na celu precyzyjne uregulowanie definicji kierownika jednostki organizacyjnej powinno być wskazanie, że kierownik jednostki organizacyjnej przetwarzającej informacje niejawne musi posiadać poświadczenie bezpieczeństwa upoważniające go do dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli informacji niejawnych przetwarzanych w kierowanej przez niego jednostce, bądź upoważnienie, w przypadku gdy w tej jednostce są przetwarzane informacje niejawne oznaczone wyłącznie klauzulą „zastrzeżone". Właściwe byłoby również, aby w sytuacji, w której osoba pełniąca tę funkcję nie uzyskała poświadczenia bezpieczeństwa (lub upoważnienia – odpowiednio), mogła tę funkcję pełnić osoba ją zastępująca, wskazana przez osobę niespełniającą wspomnianego wymogu lub przez organ uprawniony do obsady stanowiska.

Powyższe propozycje pozostają w korespondencji z odpowiedzialnością, jaką ponosi kierownik jednostki za ochronę informacji niejawnych, gdyż brak wymogu posiadania powyższych uprawnień uniemożliwia skuteczne i realne realizowanie tego obowiązku. Poza

tym taki wymóg ustawodawca określił wobec innych osób realizujących zadania w zakresie ochrony informacji, np. wobec pełnomocnika ochrony, kierownika kancelarii tajnej oraz ich zastępców. Należy podkreślić, że na poziomie jednostki organizacyjnej to funkcja kierownika jednostki jest zasadnicza w zakresie ochrony informacji niejawnych, a tym samym posiadanie przez niego – odpowiednio – poświadczenia bezpieczeństwa lub upoważnienia do dostępu do tych informacji jest naturalną tego konsekwencją. Wymóg posiadania odpowiedniego poświadczenia nie powinien obejmować jedynie kierowników jednostek organizacyjnych, którzy mają dostęp do informacji niejawnych *ipso iure*.

Powyższe jest o tyle istotne, że przepisy ustawy nie precyzują jednoznacznie konieczności poddania się kierownika jednostki organizacyjnej stosownemu postępowaniu sprawdzającemu, co w zestawieniu z odpowiedzialnością spoczywającą na nim w zakresie ochrony informacji niejawnych należy uznać za nielogiczne, czyniące tę odpowiedzialność fikcyjną.

Jeśli natomiast chodzi o wymagania dotyczące pozostałych osób zajmujących najważniejsze stanowiska w sferze ochrony informacji niejawnych, należy je również uznać za niewystarczające, jednakże tylko w odniesieniu do osób zajmujących te stanowiska w podmiotach najważniejszych z punktu widzenia zapewniania bezpieczeństwa państwa[2] i jego strategicznych interesów. W przypadku tych osób, z uwagi na ich szczególną rolę w systemie bezpieczeństwa RP, i w tych podmiotach, właściwym rozwiązaniem byłoby określenie dodatkowych warunków, jakie te osoby powinny spełniać. I tak wydaje się, że pełnomocnik ochrony i jego zastępca poza obywatelstwem polskim, wykształceniem wyższym oraz poświadczeniem bezpieczeństwa i aktualnym zaświadczeniem o przeszkoleniu wydanymi przez ABW lub SKW powinien uzyskać zgodę szefa jednej z wymienionych służb (w zależności od tego, w czyjej właściwości podmiot się znajduje) na pełnienie tej funkcji. Powinna się z tym wiązać procedura przesyłania przez kierowników jednostek organizacyjnych do ABW lub SKW stosowych wniosków zawierających wykaz obowiązków i opis sposobu ich realizacji przez kandydata, dane o przebiegu jego kariery zawodowej oraz szczegółowe uzasadnienie zamiaru obsadzenia tej osoby na stanowisku pełnomocnika ochrony lub jego zastępcy. Ten warunek powinien być wprowadzony również w przypadku osób kandydujących na takie stanowiska, jak: kierownik kancelarii tajnej i jego zastępca oraz administrator systemu teleinformatycznego oraz inspektor bezpieczeństwa teleinformatycznego – w podmiotach odgrywających główną rolę w zapewnianiu bezpieczeństwa państwa.

Kolejnym problemem związanym z osobami najważniejszymi dla systemu ochrony informacji niejawnych są występujące przypadki, w których osoby niespełniające ustawowych wymogów obejmowały funkcję pełnomocnika ochrony (lub zastępcy) i wydawały poświadczenia bezpieczeństwa, które następnie musiały być przez ABW lub SKW unieważniane (w trybie określonym w kodeksie postępowania administracyjnego) ze względu na ich wadę prawną, tj. wydanie przez nieuprawniony organ. Dlatego też, mając na uwadze potrzebę uszczelnienia systemu ochrony informacji niejawnych w tym zakresie, zasadne byłoby wprowadzenie obowiązku informacyjnego zobowiązującego kierownika jednostki organizacyjnej do uzyskania z ABW lub SKW potwierdzenia spełniania ustawowych wymogów formalnych przez osoby, które miałby zamiar zatrudnić na stanowisku pełnomocnika ochrony lub jego zastępcy. To rozwiązanie dotyczyłoby wszystkich pełnomocników (i ich zastępców), nie tylko tych zatrudnionych w podmiotach najważniejszych z punktu widzenia zapewniania bezpieczeństwa państwa.

[2] Wykaz głównych podmiotów powinien zostać dookreślony w odrębnym akcie prawnym.

Dobór osób zatrudnianych w pionie ochrony jednostki organizacyjnej jest ściśle powiązany z odpowiedzialnością nałożoną przez ustawodawcę na szefów ABW i SKW – organów odpowiedzialnych za nadzór nad systemem ochrony informacji niejawnych w Polsce. Wskazane powyżej propozycje nowych rozwiązań są motywowane koniecznością uzyskania przez szefa ABW i szefa SKW, jako głównych podmiotów odpowiedzialnych za kontrwywiadowcze i antyterrorystyczne (ABW) bezpieczeństwo państwa, realnego i skutecznego narzędzia do prawidłowego, również w aspekcie prewencyjnym, kształtowania polityki i standardów w tym zakresie. Z założenia mają więc wykluczyć możliwość obsadzania wspomnianych stanowisk osobami przypadkowymi, nieprzygotowanymi i nieświadomymi zagrożeń wynikających z niewłaściwego przetwarzania informacji niejawnych.

3. Właściwość ABW i SKW

W nawiązaniu do wskazanej, zasadniczej roli ABW i SKW w systemie ochrony informacji niejawnych, należy podkreślić, że ta rola może być odgrywana w pełni efektywnie wtedy, gdy przepisy prawa odpowiednio precyzyjnie określą właściwość obu organów w zakresie czynności realizowanych przez obie służby. Tak więc w celu zapewnienia większej przejrzystości i zapobieżenia sporom dotyczącym właściwości obu służb zasadne jest jej doprecyzowanie. Przy czym wskazane jest jednoznaczne przypisanie właściwości SKW wszystkich struktur wojskowych, w tym spółek podległych ministrowi obrony narodowej publikowanych w wykazie[3], a także sądów wojskowych oraz osób zatrudnionych w międzynarodowych dowództwach wojskowych, wielonarodowych jednostkach wojskowych z udziałem wojska polskiego lub innych podmiotach wielonarodowych z siedzibą na terytorium RP zajmujących się obronnością i wojskowością. Tak określona właściwość byłaby naturalną konsekwencją i dopełnieniem odpowiedzialności SKW (wynikającej z odrębnych przepisów), a nie ABW, w zakresie zapewniania także kontrwywiadowczej ochrony tych podmiotów. Sugerowane włączenie sądów wojskowych do jednostek organizacyjnych będących we właściwości SKW jest podyktowane także statusem tych sądów. Są one bowiem jednostkami wojskowymi w rozumieniu przepisów ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej oraz ustawy o służbie wojskowej żołnierzy, w związku z czym cała problematyka związana ze stosowaniem przez sądy wojskowe przepisów wykonawczych dotycząca ochrony informacji niejawnych opiera się na odpowiednich przepisach wydanych przez ministra obrony narodowej.

Przy uwzględnieniu występujących niekiedy w praktyce przypadków, gdy względy bezpieczeństwa państwa uzasadniają odstępstwo od ustalonej właściwości wymienionych powyżej organów, należy również rozważyć wprowadzenie w przepisach zasady, że niezależnie od właściwości do prowadzenia konkretnego postępowania wynikającego z ustawy, w szczególnie uzasadnionych okolicznościach Prezes Rady Ministrów mógłby zlecić innemu organowi (np. organowi nadzorującemu system ochrony informacji niejawnych – zob. pkt I pt. *Organizacja systemu ochrony informacji niejawnych*) wszczęcie i prowadzenie tego postępowania.

[3] Obecnie jako taki wykaz traktuje się *Obwieszczenie Ministra Obrony Narodowej z dnia 24 sierpnia 2016 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych*.

4. Bezpieczeństwo osobowe (postępowania sprawdzające)

W wyniku kilkunastoletniej praktyki prowadzenia postępowań sprawdzających stwierdzono, że liczba wydawanych poświadczeń bezpieczeństwa stale rośnie. Ta tendencja – w opinii autorów opracowania – nie jest niestety wynikiem rzeczywistej potrzeby udostępniania informacji niejawnych coraz większej liczbie osób, lecz traktowaniem postępowań sprawdzających przez jednostki organizacyjne jako procedury kadrowej, co faktycznie wypacza ich cel określony w ustawie. Mając więc na względzie konieczność zapobiegania zjawisku „nadprodukcji" tego typu poświadczeń, zasadne byłoby wprowadzenie mechanizmu korygującego i filtrującego zasadność kierowania do ABW lub SKW wniosków o wydanie takich poświadczeń – wymogu uzasadnienia wniosku, które musiałoby zawierać wskazanie zadań danej osoby powiązanych ze wskazaniem konkretnej klauzuli i rodzaju informacji niejawnych (informacje niejawne krajowe lub międzynarodowe), do których dostęp byłby niezbędny przy realizacji tych zadań. Przy tym rozwiązaniu ABW i SKW powinny mieć prawo – w razie wątpliwości co do treści takiego uzasadnienia (np. po stwierdzeniu braku związku pomiędzy zadaniami a koniecznością uzyskania dostępu do informacji niejawnych) – zwrócenia się do wnioskodawcy o przekazanie bardziej szczegółowego uzasadnienia. W takim przypadku realizacja postępowania następowałaby dopiero z chwilą uzyskania odpowiedzi od wnioskodawcy.

Współpraca w toku postępowań z innymi podmiotami

Z punktu widzenia jakości i sprawności prowadzenia postępowań, o których mowa w ustawie, rzeczą elementarną jest zapewnienie prawnej możliwości zebrania na temat osoby lub podmiotu, których dotyczy postępowanie, wszelkich informacji mogących mieć wpływ na jego wynik. Najważniejsza do osiągnięcia tego celu jest sprawna wymiana informacji zarówno z jednostkami organizacyjnymi niebędącymi podmiotami ustawy, jak i służbami uprawnionymi do prowadzenia wspomnianych postępowań[4]. Niestety, w czasie wieloletniej praktyki służby prowadzące postępowania sprawdzające niejednokrotnie napotykały poważne problemy z uzyskiwaniem informacji, obowiązujące przepisy pozwalają bowiem na różne interpretacje prowadzące w skrajnych przypadkach do odmowy przez niektóre jednostki (głównie niepaństwowe, w tym banki, biura maklerskie, placówki służby zdrowia i komorników) przekazania informacji niezbędnych do skutecznego przeprowadzenia procedury albo żądania opłat za realizację sprawdzeń. Z tego powodu zasadne jest rozważenie wprowadzenia takich zmian w ustawie, które umożliwią skuteczne przeprowadzenie czynności sprawdzających w każdej jednostce organizacyjnej, a nie tylko w jednostce organizacyjnej będącej podmiotem ustawy (czyli takiej, w której przetwarza się informacje niejawne).

Liczne doświadczenia negatywne wynikają również ze współpracy służb między sobą w zakresie wymiany informacji na temat osób, które przechodziły z właściwości jednej służby we właściwość innej. Tu problemem było uzyskanie danych na ich temat. Obecne przepisy pozwalają na odmowę przekazania informacji (a nawet tę odmowę wymuszają), nawet jawnych, mogących mieć wpływ na dawanie rękojmi zachowania tajemnicy, ponieważ przekazanie danych przez służby może nastąpić (…) *wyłącznie w przypadku, gdy w ich opinii osoba objęta postępowa-*

[4] Oprócz ABW i SKW, są to: SWW, CBA, Policja, Żandarmeria Wojskowa, Straż Graniczna, Służba Więzienna i Biuro Ochrony Rządu (Państwowa Służba Ochrony).

niem sprawdzającym lub kontrolnym postępowaniem sprawdzającym nie daje rękojmi zachowania tajemnicy[5] (a dodatkowo nakłada się na to problem ograniczeń dotyczących udostępniania akt postępowań sprawdzających przez większość służb specjalnych). Dlatego też należy rozważyć przyjęcie takiego rozwiązania ustawowego, że odmowa udzielenia informacji między służbami odpowiedzialnymi za bezpieczeństwo państwa i jego obywateli dotyczyłaby jedynie niektórych informacji o klauzuli „ściśle tajne" o szczególnym znaczeniu dla bezpieczeństwa państwa (lub interesu służby), stanowiących większe dobro niż dokonanie oceny dawania rękojmi zachowania tajemnicy przez organ prowadzący postępowanie. *Lex specialis* w stosunku do powyższego przepisu powinien nadal stanowić art. 72 odnoszący się do udostępniania akt postępowań sprawdzających.

Ogólne zasady dostępu osób do informacji niejawnych

Przepisy ustawy określają warunki, jakie powinny spełniać osoby uzyskujące dostęp do informacji niejawnych, przy czym podkreślenia wymaga to, że ujawnienie każdej informacji niejawnej – niezależnie od jej klauzuli tajności – osobom nieupoważnionym, może przynieść państwu określone szkody. Dotyczy to także informacji niejawnych o najniższej klauzuli, tj. „zastrzeżone", czyli tych, których ujawnienie może mieć negatywny wpływ na wykonywanie zadań związanych z bezpieczeństwem państwa[6]. Przepisy obecnie obowiązującej ustawy nie narzucają żadnej weryfikacji osób, którym informacje o tej klauzuli mają być udostępnione, pozostawiając decyzję w tej sprawie kierownikowi jednostki organizacyjnej. W tej sytuacji zasadne byłoby umożliwienie minimalnej weryfikacji osób, które mają zapoznawać się z tego typu informacjami, i wykluczenie występującej obecnie uznaniowości kierownika jednostki organizacyjnej w dopuszczaniu osób do dostępu do nich (w tym np. osób skazanych). Z uwagi na dotychczasową całkowitą dowolność i brak jakichkolwiek uregulowań dotyczących zasad wydawania upoważnień osobom, które mają mieć dostęp do tak oznaczonych informacji niejawnych, należy rozważyć uregulowanie w przepisach prawa zasad wydawania tych upoważnień**.** I tak np. kierownikom jednostek organizacyjnych upoważnienia byłyby wydawane przez ABW lub SKW, pełnomocnicy ochrony zaś – oraz ABW i SKW w odniesieniu do samych kierowników – byliby uprawnieni do sprawdzania osób ubiegających się o wydanie upoważnienia w Krajowym Rejestrze Karnym[7].

Warto nadmienić, że osoby uzyskujące dostęp do informacji niejawnych o klauzuli odpowiadającej klauzuli „zastrzeżone" podlegają sprawdzeniom m.in. w takich krajach, jak Kanada[8], Dania, Luksemburg oraz Turcja.

---

[5] Art. 13 ust. 3 ustawy.

[6] Art. 5 ust. 4 ustawy: „Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania opraw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej*"*.

[7] ABW i SKW dodatkowo byłyby uprawnione do sprawdzania osób ubiegających się o wydanie upoważnienia w ewidencjach niejawnych.

[8] W przypadku dostępu do informacji niejawnych oznaczonych klauzulą „NATO RESTRICTED" lub odpowiednikami tej klauzuli stosowanymi przez inne państwa (brak odpowiednika kanadyjskiego wymienionej klauzuli).

Zakres przedmiotowy postępowań sprawdzających – ważność poświadczeń (upoważnień)

Zgodnie z przepisami ustawy w trakcie zwykłego postępowania sprawdzającego (prowadzonego przez pełnomocników ochrony konkretnych jednostek organizacyjnych do poziomu „poufne") nie są weryfikowane: stan zdrowia psychicznego (w tym uzależnienia) oraz sytuacja finansowa osoby sprawdzanej. W konsekwencji choroba psychiczna lub uzależnienie od narkotyków albo alkoholizm nie są przeszkodami w uzyskaniu (lub podstawą do pozbawienia) dostępu do informacji niejawnych o klauzuli „poufne" – co jest nie do utrzymania nie tylko z punktu widzenia elementarnej logiki, lecz także przede wszystkim z punktu widzenia interesu ochrony informacji niejawnych, a co za tym idzie – także interesu bezpieczeństwa państwa. Zasadne byłoby zatem stwierdzanie niedawania rękojmi zachowania tajemnicy w odniesieniu do osób objętych zwykłymi postępowaniami sprawdzającymi także w przypadku wątpliwości natury zdrowotnej i finansowej, jednakże z uwzględnieniem możliwości uzyskiwania i weryfikacji przez pełnomocnika ochrony tylko informacji o stanie zdrowia osoby sprawdzanej (oczywiście wraz z możliwością zobowiązywania tej osoby do poddania się specjalistycznemu badaniu). W przypadku wątpliwości dotyczących sytuacji finansowej, jakkolwiek ich stwierdzenie mogłoby stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa w zwykłym postępowaniu sprawdzającym (np. w sytuacji, gdyby te wątpliwości zostały ustalone we wcześniej przeprowadzonym poszerzonym postępowaniu sprawdzającym), to jednak pełnomocnik ochrony nie powinien mieć możliwości gromadzenia i weryfikacji szczegółowych informacji w tym zakresie, przede wszystkim z uwagi na to, że sytuacja finansowa osoby sprawdzanej jest z reguły rozpatrywana nie tylko wyłącznie w odniesieniu do niej samej, ale często również w kontekście innych osób (np. rodziców, współmałżonka, darczyńców), a także z uwagi na szczególną wrażliwość ochrony danych finansowych (przede wszystkim stanowiących tajemnicę bankową).

Przetwarzanie informacji w ramach postępowania

Zgodnie z przepisami ustawy organ prowadzący postępowanie sprawdzające ma możliwość przetwarzania w ramach tego postępowania informacji o osobie sprawdzanej, najbliższych członkach jej rodziny oraz ewentualnie innych osobach wskazanych w ankiecie bezpieczeństwa osobowego. Jednocześnie jednak przepisy ustawy zobowiązują organ prowadzący postępowanie sprawdzające m.in. do ustalenia, czy poziom życia osoby sprawdzanej jest adekwatny do uzyskiwanych przez nią dochodów (oczywiście w znaczeniu dochodu legalnie uzyskanego). Tymczasem jedynym punktem odniesienia do poziomu życia osoby sprawdzanej wcale nie muszą być – i w zdecydowanej większości przypadków nie są – tylko jej własne dochody, ale także dochody współmałżonka, a nierzadko także dochody innych osób – w przypadku, gdy te osoby przekazały osobie sprawdzanej np. darowiznę (lub darowiznę otrzymały)[9]. W obecnym stanie prawnym, jeżeli te osoby nie zostały wymienione w ankiecie, to organ nie może przetwarzać informacji na ich temat.

Analogiczny problem dotyczy osób podejrzewanych o kontakty z obcym wywiadem czy grupami przestępczymi. W celu określenia dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną organ powinien mieć możliwość sprawdzenia wszystkich

[9] W tym przypadku celem sprawdzenia jest ustalenie, czy tego typu operacja nie miała na celu np. ukrycia majątku przed opodatkowaniem.

osób, które się z nią kontaktowały albo kontaktują, lub z członkiem jej bliskiej rodziny. Powinno to nastąpić także wtedy, gdy te osoby nie są wymienione w ankiecie, a zwłaszcza – gdy nie są wymienione w ankiecie, a być powinny. Tak więc skuteczność postępowania (rzetelność dokonania oceny, czy osoba sprawdzana daje rękojmię zachowania tajemnicy) jest obecnie uzależniona od danych przekazanych przez osobę sprawdzaną.

Z tego względu jak najbardziej zasadne jest poszerzenie kręgu osób, których dane można przetwarzać w ramach postępowania, szczególnie biorąc pod uwagę dobro, jakim jest bezpieczeństwo państwa, w tym informacji niejawnych (oraz informacji niejawnych międzynarodowych, których zachowania w tajemnicy Rzeczpospolita Polska zobowiązała się strzec). Nie chodzi przy tym o możliwość przetwarzania dowolnych danych o dowolnych osobach, a jedynie tych danych (i tylko o tych osobach), które są niezbędne do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

Byłoby zatem wskazane dopuszczenie możliwości przetwarzania w ramach postępowań sprawdzających nie tylko informacji o osobie sprawdzanej, najbliższych członkach jej rodziny oraz ewentualnie innych osobach wymienionych w ankiecie (tak jak w obecnie obowiązującej ustawie), lecz także o wszystkich innych osobach, również niewymienionych w ankiecie, z którymi kontakty – choćby pośrednie – mogą mieć wpływ na ocenę dawania rękojmi zachowania tajemnicy. Dotyczy to przede wszystkim prowadzenia przez tego typu osoby (mające kontakt z samą osobą sprawdzaną, członkami jej rodziny, ale też np. z obywatelami innych państw, z którymi kontakt utrzymuje osoba sprawdzana) działalności w obcym wywiadzie, zorganizowanej grupie przestępczej albo w innej organizacji o podobnym charakterze.

Narzędzia weryfikacji danych

W aktualnie obowiązujących przepisach dotyczących czynności podejmowanych w ramach postępowań sprawdzających niewątpliwie brakuje regulacji umożliwiających wykorzystywanie badania poligraficznego jako skutecznego narzędzia weryfikacji zebranych informacji. Warto zaznaczyć, że wprowadzenie do ustawy możliwości wykonania takiego badania byłoby korzystne zarówno dla osoby poddanej postępowaniu (wprowadzenie możliwości przeprowadzenia badania wyłącznie na wniosek tej osoby w przypadku wątpliwości służby prowadzącej postępowanie dotyczących dawania przez nią rękojmi, przy zastrzeżeniu, że to badanie dotyczyłoby tylko weryfikacji występowania tych wątpliwości), jak i z punktu widzenia bezpieczeństwa państwa (wprowadzenie możliwości zobowiązania osoby sprawdzanej do poddania się takiemu badaniu w przypadku ściśle określonych wątpliwości[10]). Przy tym rozwiązaniu badanie powinny przeprowadzać wyłącznie służby uprawnione do realizacji poszerzonych postępowań sprawdzających. Nie powinno być ono przeprowadzane w przypadku wątpliwości natury zdrowotnej.

Analizując rozwiązania w powyższym zakresie obowiązujące w prawodawstwach innych państw, można stwierdzić, że badanie poligraficzne bywa elementem – obligatoryjnym lub fakultatywnym – postępowań sprawdzających (m.in. na Litwie, w Kanadzie i Rumunii) albo też niezbędnym uzupełnieniem tych postępowań (w USA – przy niektórych kategoriach dostępu do informacji niejawnych).

[10] Chodzi o wątpliwości dotyczące zagrożeń ze strony obcych służb specjalnych, grup terrorystycznych, wywrotowych lub przestępczych, a także niewłaściwego postępowania osoby sprawdzanej z informacjami prawnie chronionymi.

Poświadczenia bezpieczeństwa

Zasadne wydaje się wprowadzenie zmiany dotyczącej ważności (w znaczeniu: odpowiedniości) poświadczeń bezpieczeństwa wydanych przez inne służby niż ABW i SKW, zgodnie z którą poświadczenia w zakresie dostępu do informacji niejawnych o klauzuli „poufne" wydawane przez te organy byłyby ważne także poza służbą w tych organach[11]. To rozwiązanie jest w pełni uzasadnione pozycją wspomnianych służb w systemie organów państwowych odpowiedzialnych za bezpieczeństwo państwa, nawet w sytuacji, gdy postępowania poprzedzające wydanie takich poświadczeń nie będą podlegać kontroli zewnętrznej. Trudno bowiem uznać, że tego typu postępowania są i będą prowadzone według gorszych standardów niż zwykłe postępowania sprawdzające prowadzone przez pełnomocników ochrony w innych instytucjach państwowych, samorządowych oraz u przedsiębiorców, w których wyniku wydane poświadczenia umożliwiające dostęp do informacji o klauzuli „poufne" są przecież ważne po zmianie miejsca pracy osoby posiadającej takie poświadczenie.

Decyzja o odmowie wydania poświadczenia bezpieczeństwa

O prawnych podstawach decyzji negatywnej (odmowie wydania lub cofnięciu poświadczenia) powinien być informowany także kierujący wniosek o przeprowadzenie postępowania. Jest to całkowicie logiczne ze względu na dalsze konsekwencje tej decyzji w kontekście np. przepisów prawa pracy i korzystne dla obywateli. Warto przypomnieć, że obecnie kierownik jednostki otrzymuje jedynie informację o sposobie zakończenia postępowania.

Ponadto należy zauważyć, że przepisy ustawy w jej obecnym kształcie nie wykluczają sytuacji, gdy osoba, w stosunku do której stwierdzono, że nie daje rękojmi zachowania tajemnicy, nadal (przynajmniej na jakiś czas lub nawet w dłuższym okresie) będzie miała dostęp do informacji niejawnych na podstawie dotychczas posiadanych poświadczeń lub upoważnień. W związku z powyższym właściwe jest wprowadzenie zasady, zgodnie z którą w przypadku stwierdzenia przez służby uprawnione do prowadzenia poszerzonych postępowań sprawdzających, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy (a więc odmowy wydania poświadczenia bezpieczeństwa), z mocy prawa, bez konieczności wszczynania odrębnych, kontrolnych postępowań sprawdzających (szczególnie w sytuacji, gdy musiałby to zrobić inny organ niż ten, który odmówił wydania poświadczenia bezpieczeństwa), tracą ważność wszystkie posiadane przez taką osobę poświadczenia bezpieczeństwa, a także wydane przez ABW lub SKW upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone". Takie rozwiązanie w konsekwencji wymagałoby obowiązkowego poinformowania o takiej decyzji wszystkich organów, które wydały wcześniej wyżej wymienionej osobie poświadczenia i upoważnienia, ważne w chwili wydania decyzji o odmowie. Analogicznie, należałoby również rozważyć wprowadzenie wspomnianej zmiany do kontrolnych postępowań sprawdzających.

[11] Chodzi o przywrócenie stanu prawnego obowiązującego w latach 1999–2010, choć niezapisanego wprost w obowiązujących wówczas przepisach, a bazującego na opinii prawnej Agencji Bezpieczeństwa Wewnętrznego.

Decyzja o cofnięciu poświadczenia bezpieczeństwa

W celu uwzględnienia interesu obywateli, którzy z powodu braku zatrudnienia nie mają już dostępu do informacji niejawnych i o taki dostęp nie zamierzają się ubiegać, a jednocześnie nie życzą sobie być objętymi postępowaniami kontrolnymi, byłoby wskazane wprowadzenie prawnej możliwości skutecznego „zabezpieczenia" się przed taką aktywnością służb. Dana osoba powinna mieć możliwość złożenia oświadczenia o zrzeczeniu się uprawnień do dostępu do informacji niejawnych, jednocześnie jednak powinna odesłać oryginały posiadanych poświadczeń do organu, który je wydał (i zawiadomić o tym ABW lub SKW). Zasadne jest, aby w takim przypadku organ był zobowiązany do umorzenia już wszczętego postępowania kontrolnego oraz aby nie mógł wobec takiej osoby wszcząć tego typu postępowania.

Zasady realizacji postępowania kontrolnego

Z punktu widzenia systemu bezpieczeństwa informacji niejawnych istotna jest możliwość odpowiednio szybkiego i skutecznego reagowania przez ABW i SKW na nowe fakty dotyczące osoby posiadającej poświadczenie bezpieczeństwa, które mogą wpływać na jej wiarygodność (np. w sytuacji, gdy osoba zatrudniona w MSZ wstąpi w związek małżeński z obywatelem innego państwa). W powyższym zakresie przepisy ustawy nie zapewniają organom możliwości w pełni elastycznego reagowania i dlatego należy rozważyć ich uzupełnienie.

Przede wszystkim dla systemu ochrony informacji niejawnych byłoby istotne wprowadzenie możliwości weryfikacji przez służby tych danych, które mogą mieć kluczowe znaczenie dla oceny dawania rękojmi zachowania tajemnicy przez osobę posiadającą ważne poświadczenie bezpieczeństwa i zajmującą stanowisko związane z dostępem do informacji niejawnych. Ta weryfikacja powinna z jednej strony polegać na dokonaniu określonych sprawdzeń[12], a z drugiej – na zobowiązaniu osoby do uaktualnienia niezbędnych informacji zawartych w ankiecie (niewypełnienie tego zobowiązania będzie mogło stanowić podstawę do wszczęcia postępowania kontrolnego).

Warto dodać, że analogiczne lub zbliżone do proponowanych powyżej, a niekiedy nawet bardziej restrykcyjne, rozwiązania są stosowane przez takie państwa europejskie, jak m.in. Wielka Brytania[13], Niemcy czy Belgia[14].

[12] Nie tylko sprawdzenie w ewidencjach, rejestrach i kartotekach oraz innych zasobach informacyjnych, w tym niejawnych, w KRK, także uzyskanie informacji lub sprawdzenie innych danych zdobytych w toku postępowania, ale również rozmowa z osobą sprawdzaną oraz z innymi osobami, jeżeli mogą one dysponować informacjami, które mają wpływ na ocenę dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną.

[13] Przykładowe rozwiązanie: informację wskazującą, że osoba może niewłaściwie postępować z informacjami niejawnymi, przekazuje drogą elektroniczną (formularz – *Aftercare Incident Report*) właściwemu organowi pełnomocnik ochrony albo każda inna osoba, w której ocenie istnieją uzasadnione wątpliwości w tym zakresie.

[14] W przypadku poinformowania właściwego organu o zawarciu małżeństwa lub nawiązaniu trwałej relacji z partnerem (partnerką) przez osobę mającą ważne uprawnienia w zakresie dostępu do informacji niejawnych, a jeżeli ta osoba ma dostęp do klauzuli odpowiadającej polskiej klauzuli „ściśle tajne" – w przypadku pojawienia się nowych pełnoletnich współmieszkańców osoby sprawdzonej – pełnomocnik ochrony składa wniosek o przeprowadzenie wobec tej osoby kolejnego postępowania sprawdzającego.

Zwolnienia z postępowań. Specjalny tryb realizacji postępowań sprawdzających

Względy bezpieczeństwa państwa skłaniają do rozważenia ewentualnych korekt w odniesieniu do ustawowego wykazu osób zwolnionych z obowiązku poddania się postępowaniu sprawdzającemu. Wyłączeniu z obowiązku poddania się postępowaniom sprawdzającym (wyłącznie w przypadku dostępu do „krajowych" informacji niejawnych o klauzuli nie wyższej, niż „tajne") – ze względu na umocowanie ustrojowo-konstytucyjne – powinni podlegać tylko sędziowie i prokuratorzy, a nie ławnicy i asesorzy, jak jest obecnie w ustawie. W stosunku zaś do samych sędziów i prokuratorów właściwe byłoby rozważenie wprowadzenia zasady, *per analogiam* do regulacji dotyczących posłów i senatorów, że wyłączenie z obowiązku poddania się sędziów i prokuratorów postępowaniom sprawdzającym nie będzie dotyczyło przypadków, gdy mają oni uzyskać dostęp do informacji niejawnych o klauzuli „ściśle tajne".

Odwołania i zasady realizacji postępowań odwoławczych

Zgodnie z przepisami ustawy w przypadku wydania przez pełnomocnika ochrony decyzji o odmowie wydania lub cofnięciu poświadczenia bezpieczeństwa albo decyzji o umorzeniu postępowania sprawdzającego postępowanie odwoławcze prowadzi ABW lub SKW. Ponieważ jednak większość decyzji pełnomocnika o odmowie wydania poświadczeń bezpieczeństwa oraz zdecydowana większość decyzji o ich cofnięciu była wydawana na podstawie informacji uzyskanych z ABW lub SKW, wskazane jest, aby organem odwoławczym od tych decyzji był organ inny (np. KPRM) niż wymienione powyżej. W opinii autorów opracowania nie jest właściwe, aby sama służba rozpatrywała odwołanie od decyzji wydanej na podstawie własnej opinii (osoby sprawdzane mogłyby wtedy podnosić, że wynik takiego postępowania łatwo przewidzieć). Powyższa zmiana z pewnością poprawiłaby pozycję obywatela w procesie odwoławczym. Zasadne jest zatem, aby wszystkie postępowania odwoławcze, w tym postępowania prowadzone po wydaniu decyzji przez pełnomocnika ochrony, prowadził wskazany w ustawie organ wyższej instancji, inny niż ABW i SKW[15].

5. Kontrole

W sferze kontroli stanu zabezpieczenia informacji niejawnych najczęściej spotykanym problemem jest brak możliwości zweryfikowania wszelkich informacji zebranych w ramach kontroli od osób oraz podmiotów, które nie są jej przedmiotem – chodzi o weryfikację informacji u byłych pracowników kontrolowanej jednostki, a także w podmiotach, których działalność pozostaje w związku z kontrolowaną jednostką. Obecne uprawnienie polegające na możliwości zasięgania – z uwagi na przeprowadzaną kontrolę – informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądanie wyjaśnień od kierowników i pracowników tych jednostek nie pozwala na wszechstronną weryfikację informacji uzyskanych w takim trybie. Tym samym nie można w sposób jednoznaczny ustalić stanu faktycznego badanych okoliczności.

[15] Dotyczy to również składania zażaleń na postanowienia wydawane w trakcie postępowań sprawdzających (o zawieszeniu postępowania lub postępowania kontrolnego oraz o podjęciu zawieszonego postępowania lub zawieszonego postępowania kontrolnego, a także na postanowienie o odmowie wszczęcia postępowania) – art. 40 ustawy.

Wskazane byłoby więc umożliwienie odbierania wyjaśnień właśnie od byłych pracowników kontrolowanej jednostki organizacyjnej, co zresztą pozostawałoby w korespondencji z uprawnieniami kontrolerów NIK w tym zakresie. Ponadto zasadne byłoby dodanie możliwości wykonywania określonych uprawnień kontrolnych (m.in. żądania udzielania wyjaśnień, dokonywania oględzin, badania obiegu informacji niejawnych) w stosunku do jednostek niekontrolowanych, ale wyłącznie w zakresie weryfikacji ustaleń, które pozostają w związku z prowadzoną kontrolą w jednostce kontrolowanej. Uprawnienie w nowej formule miałoby na celu umożliwienie dogłębnego ustalenia stanu faktycznego przez weryfikację uzyskanych informacji czy ustaleń mających lub mogących mieć wpływ na stan zabezpieczenia informacji niejawnych, bez konieczności wszczynania odrębnej kontroli w jednostce niebędącej jej przedmiotem.

6. Bezpieczeństwo fizyczne

W obszarze wskazanym w tytule uwagę zwraca brak jednolitych wymagań dotyczących stosowania wyposażenia i urządzeń służących ochronie informacji niejawnych we wszystkich jednostkach organizacyjnych, w których są przetwarzane informacje oznaczone klauzulą „poufne" i wyższą. Przepisy ustawy powinny nałożyć obowiązek stosowania przez te jednostki jednolitych wymogów określonych szczegółowo w odpowiednich aktach prawnych (rozporządzeniach) w odniesieniu do dedykowanych środków bezpieczeństwa fizycznego.

Wprowadzenie powyższej zmiany pozwoliłoby na określenie wykazu środków bezpieczeństwa fizycznego wraz z wymaganiami, jakie winny spełniać poszczególne urządzenia i wyposażenie, by mogły być wykorzystywane do ochrony informacji niejawnych (np. posiadanie certyfikatu, poświadczenia zgodności czy spełniania określonych parametrów technicznych lub norm). Metodologie oraz dobór tych środków w zależności od poziomu zagrożeń byłyby regulowane, podobnie jak to jest dotychczas, odpowiednimi przepisami wykonawczymi z uwzględnieniem statusu (charakteru) danej jednostki organizacyjnej (tj. rozporządzenie, zarządzenie).

Opisane propozycje rozwiązań nie powinny natomiast dotyczyć służb (ABW, SKW, SWW, CBA, BOR, Policji, ŻW, Służby Więziennej, Straży Granicznej[16]), ale jedynie w zakresie wymogów określonych w rozporządzeniu. Jest to uzasadnione przyjętymi rozwiązaniami w zakresie bezpieczeństwa fizycznego w tych służbach, które z uwagi na specyfikę ich zadań przewyższają ogólne standardy wynikające z obowiązujących przepisów w tej materii. W związku z tym brak powyższego wymogu nie spowodowałby zagrożenia bezpieczeństwa informacji niejawnych przetwarzanych przez te służby. Wyłączenie, o którym mowa, nie powinno dotyczyć wyposażenia i urządzeń służących ochronie informacji niejawnych międzynarodowych ze względu na odrębne przepisy w tym zakresie.

7. Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

Przepisy regulujące problem udostępniania akt postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego nie-

[16] Te służby nie będą np. zobligowane do stosowania certyfikowanego wyposażenia i urządzeń służących ochronie informacji niejawnych.

jednokrotnie uniemożliwiają wyjaśnienie wątpliwości dotyczących dawania rękojmi zachowania tajemnicy, także przez osoby ważne dla bezpieczeństwa państwa, tylko dlatego, że służba, która przeprowadziła poprzednie postępowanie, nie może udostępnić akt służbie prowadzącej kolejne lub kontrolne postępowanie sprawdzające. Bardzo rygorystyczne regulacje w tym zakresie uniemożliwiają ponadto najważniejszym organom odpowiedzialnym za bezpieczeństwo państwa zapoznanie się z ustaleniami służb specjalnych powołanych m.in. w celu realizacji procedur określonych w ustawie, zmierzających do zapewnienia tego bezpieczeństwa. W ustawie nie wskazano również, że przepisy dotyczące udostępniania akt postępowań sprawdzających dotyczą także akt kontrolnych postępowań sprawdzających.

W związku z powyższym rozważenie wprowadzenia w przepisach takich zmian, które wyeliminowałyby część ograniczeń w udostępnianiu akt postępowań, a także zawartych w nich informacji i dokumentów (wyciągów), należy uznać za priorytetowe. Przede wszystkim udostępnieniu powinny podlegać nie tylko same akta zgodnie z przepisami art. 72 ustawy, lecz także konkretne informacje zgromadzone w tych aktach, przy czym służba – dysponent akt (także informacji z akt) – powinna mieć możliwość odmówienia ich udostępnienia z uwagi na jej ważny interes. Powyższe mogłoby dotyczyć także udostępniania akt (także informacji z akt) właściwemu organowi do celów postępowania karnego, karno-skarbowego oraz podatkowego.

Ze względów praktycznych wskazane byłoby również zrezygnowanie z ograniczenia dotyczącego udostępniania akt postępowań tylko na potrzeby postępowań prowadzonych wobec tej samej osoby – także dlatego, że taki zapis czyni martwym przepis o udostępnianiu akt postępowań bezpieczeństwa przemysłowego. Niejednokrotnie też informacje i dokumenty zgromadzone przez służbę wobec jednej osoby mogłyby zostać wykorzystane do postępowania prowadzonego wobec małżonka tej osoby, co z jednej strony ułatwiłoby prowadzenie postępowania organowi, a z drugiej – byłoby mniej uciążliwe dla osoby sprawdzanej.

Istotną propozycją, której wprowadzenie należy rozważyć, jest możliwość udostępnienia informacji z akt postępowań najwyższym organom państwa: Prezydentowi RP, Prezesowi Rady Ministrów, Marszałkowi Sejmu, jak również ministrowi nadzorującemu służby specjalne. Dodatkowo proponuje się rozważenie wprowadzenia regulacji, aby za zgodą tego ostatniego informacje te mogły zostać udostępnione ministrowi obrony narodowej, ministrowi sprawiedliwości oraz ministrom właściwym do spraw wewnętrznych i do spraw zagranicznych. Ma to uzasadnienie z uwagi na odpowiedzialność wyżej wymienionych organów za bezpieczeństwo państwa.

Zasadne wydaje się również wprowadzenie dodatkowej regulacji prawnej, na której podstawie dane z ewidencji osób mających dostęp do informacji niejawnych, prowadzonej przez ABW i SKW, w celu potwierdzenia posiadania lub braku uprawnień do dostępu do informacji niejawnych przez konkretne osoby, będą mogły dodatkowo zostać udostępnione podmiotowi, który wykaże interes prawny w uzyskaniu takich informacji, jeżeli nie będzie to stało w sprzeczności z interesem ochrony informacji niejawnych.

8. Bezpieczeństwo przemysłowe

Zgoda na dostęp przedsiębiorcy do informacji niejawnych

Zgodnie z przepisami ustawy upoważnieni do wydawania przedsiębiorcy zgody na dostęp do informacji niejawnych są: szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów, minister właściwy dla okre-

ślonego działu administracji rządowej oraz prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku – szef ABW albo szef SKW[17]. Tak wiele podmiotów uprawnionych do wydawania powyższej zgody niewątpliwie nie sprzyja bezpieczeństwu informacji niejawnych udostępnianych przedsiębiorcy objętemu zgodą, ponieważ większość z wymienionych organów nie ma uprawnień do wykonywania jakichkolwiek sprawdzeń i gromadzenia informacji o takim przedsiębiorcy. W celu zapewnienia właściwego poziomu ochrony informacjom przekazywanym w tym trybie i uniknięcia wydawania przedmiotowych zgód bez jakichkolwiek sprawdzeń w służbach odpowiedzialnych za ten obszar bezpieczeństwa państwa, należy rozważyć zawężenie kręgu podmiotów uprawnionych do wydawania zgody w zakresie dostępu do krajowych informacji niejawnych o klauzuli „poufne" lub wyższej przedsiębiorcom, wobec których wszczęto postępowanie bezpieczeństwa przemysłowego lub postępowanie sprawdzające (w przypadku przedsiębiorców prowadzących działalność jednoosobowo i osobiście), a także podmiotom, wobec których nie wszczęto postępowania (tzw. zgoda jednorazowa). Zgodę w powyższym zakresie wydawałyby wyłącznie ABW albo SKW, czyli organy uprawnione do prowadzenia postępowań bezpieczeństwa przemysłowego i postępowań sprawdzających, które z racji posiadanych uprawnień mogą dysponować szerszą wiedzą dotyczącą wnioskodawcy.

Kaskada świadectw bezpieczeństwa przemysłowego (ŚBP) I stopnia

Jeden z poważniejszych problemów w sferze bezpieczeństwa przemysłowego dotyczy następstw upływu terminu ważności akredytacji bezpieczeństwa systemu teleinformatycznego w przypadku przedsiębiorcy posiadającego ważne świadectwo bezpieczeństwa przemysłowego I stopnia[18]. W tej sytuacji ustawa dopuszcza dwa warianty postępowania: pierwszy z nich przewiduje zrzeczenie się przez przedsiębiorcę uprawnień określonych w posiadanym świadectwie (w rzeczywistości brak możliwości przetwarzania informacji niejawnych), drugi zaś – możliwość cofnięcia przez ABW lub SKW przedsiębiorcy świadectwa po stwierdzeniu utraty przez niego zdolności do ochrony informacji niejawnych z powodu utarty funkcjonalności sytemu ochrony tych informacji. Oba warianty skutkują brakiem możliwości wykonywania przez przedsiębiorcę umów związanych z dostępem do informacji niejawnych.

Proponowanym, niewątpliwie korzystnym dla przedsiębiorców, rozwiązaniem byłoby wprowadzenie tzw. kaskady stopni świadectwa bezpieczeństwa przemysłowego. Kaskada dotyczyłaby świadectwa pierwszego stopnia i skutkowałaby utrzymaniem ważności świadectwa bezpieczeństwa przemysłowego na poziomie stopnia drugiego[19] w przypadku upływu terminu ważności akredytacji bezpieczeństwa teleinformatycznego. Zastosowanie powyższego rozwiązania byłoby korzystne z punktu widzenia tych przedsiębiorców wykorzystujących systemy teleinformatyczne, w których przypadku w okresie ważności ŚBP upływa termin ważności wspomnianej akredytacji; w tej sytuacji zachowaliby oni możliwość realizowania umów wymagających posiadania świadectwa drugiego lub trzeciego stopnia[20], co nie pozostaje bez znaczenia również dla pod-

[17] Art. 54 ust. 7 ustawy

[18] Świadectwo potwierdzające pełną zdolność przedsiębiorcy do ochrony informacji niejawnych.

[19] Świadectwo potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych.

[20] Świadectwo potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych, z wyłączeniem

miotów zlecających realizację umów związanych z dostępem do informacji niejawnych, miałyby one bowiem możliwość podpisania umowy w zakresie świadectwa drugiego i trzeciego stopnia z przedsiębiorcą legitymującym się świadectwem bezpieczeństwa przemysłowego pierwszego stopnia, bez ryzyka utraty przez wykonawcę umowy – w trakcie jej realizacji – zdolności do ochrony informacji niejawnych z powodu upływu terminu ważności akredytacji bezpieczeństwa systemu teleinformatycznego.

Przesłanki odmowy wydania świadectwa bezpieczeństwa przemysłowego i cofnięcia posiadanego świadectwa

Praktyka stosowania przepisów ustawy w obszarze bezpieczeństwa przemysłowego skłania do rozważenia zmiany w zakresie przesłanek odmowy wydania świadectwa bezpieczeństwa przemysłowego:

a) przesłanki obligatoryjne:
   - obecna ustawa zawiera nieprecyzyjny zapis, zgodnie z którym ABW lub SKW odmawia wydania świadectwa z powodu (…) *braku możliwości ustalenia* (…) *źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy*[21], co wpływa na to, że ten zapis może być interpretowany jako konieczność ustalenia jedynie źródła wspomnianych środków, z pominięciem legalności ich uzyskania. To z punktu widzenia przyznania jakichkolwiek uprawnień podmiotowi nie może być akceptowane. Dlatego też należy rozważyć rozszerzenie katalogu przesłanek obligatoryjnych wprost o brak możliwości ustalenia legalności pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy. Chodzi o możliwość wydania decyzji o odmowie przyznania świadectwa przedsiębiorcy w przypadku uzasadnionego podejrzenia pochodzenia tych środków ze źródła nielegalnego;
   - stwierdzono również przypadki, w których członkami organów zarządzających lub kontrolnych przedsiębiorcy oraz osobami powoływanymi do pełnienia funkcji kierownika jednostki organizacyjnej zostają osoby, które de facto nie mają realnego wpływu na działalność przedsiębiorcy. Faktycznie natomiast działalnością podmiotu kieruje osoba, wobec której występują wątpliwości mogące mieć szkodliwy wpływ na poziom ochrony informacji niejawnych przetwarzanych przez przedsiębiorcę. Chodzi zarówno o osoby dysponujące bezpośrednio lub pośrednio większością głosów na zgromadzeniu wspólników lub walnym zgromadzeniu sprawdzanego przedsiębiorcy, jak i posiadające możliwość samodzielnego decydowania o powołaniu większości członków rady nadzorczej i zarządu oraz wywierania decydującego wpływu na działalność podmiotu np. przez umowę na zarządzanie podmiotem. Wskazane jest więc rozważenie poszerzenia wykazu przesłanek obligatoryjnych o wystąpienie negatywnych okoliczności[22] związanych z osobą, która ma rzeczywisty

możliwości ich przetwarzania w użytkowanych przez niego obiektach.

[21] Art. 64 ust. 2 pkt 2 ustawy.

[22] Skazanie prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe albo nieprawomocne skazanie lub oskarżenie albo przedstawienie zarzutów popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3.

wpływ na działalność przedsiębiorcy[23]. Obecnie fakultatywną podstawą do odmowy wydania świadectwa są niedające się usunąć wątpliwości (określone w ustawie[24]) dotyczące wyłącznie osób wchodzących w skład organów zarządzających, kontrolnych oraz osób działających z ich upoważnienia.
Proponowana zmiana miałaby na celu uzależnienie wyniku postępowania od niewystępowania wątpliwości wobec osób będących faktycznymi zarządcami lub właścicielami przedsiębiorstwa.

b) przesłanki fakultatywne:
   – w coraz większej liczbie podmiotów instytucjonalnych mających udziałowców zagranicznych może występować ryzyko związane z nielegalną działalnością ze sfery terroryzmu czy szpiegostwa lub występowaniem innych przestępstw. Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego, jako organy prowadzące postępowania bezpieczeństwa przemysłowego, muszą mieć możliwość adekwatnego reagowania w wymienionych przypadkach przez negatywną ocenę zdolności do ochrony informacji niejawnych tych przedsiębiorców. Dlatego też należy rozważyć uwzględnienie w przepisach, co najmniej jako przesłanki fakultatywnej, negatywnych wyników sprawdzeń podmiotu zagranicznego posiadającego wkład, udziały lub akcje w sprawdzanym podmiocie, wobec którego organ prowadzący postępowanie bezpieczeństwa przemysłowego uzyskał informacje o jakiejkolwiek działalności nielegalnej.

Konsekwencją ewentualnego wprowadzenia powyższych rozwiązań powinno być wprowadzenie analogicznych zmian w przepisach dotyczących podstawy (obligatoryjnej bądź fakultatywnej) cofnięcia posiadanego świadectwa bezpieczeństwa przemysłowego.

Warto wspomnieć, że problematyka dotycząca wpływu podmiotów zagranicznych na zdolność przedsiębiorcy do ochrony informacji niejawnych jest w ostatnich latach mocno eksponowana przez zagranicznych ekspertów w dziedzinie ochrony tego typu informacji w sferze bezpieczeństwa przemysłowego. Przepisy wykonawcze w tym zakresie wprowadziły do swojego systemu prawnego m.in. Stany Zjednoczone Ameryki[25], Kanada[26] i Wielka Brytania[27].

9. Wzór ankiety bezpieczeństwa osobowego

Uwzględniając dynamiczny rozwój informatyczny, należy dokonać zmian dotyczących wzoru ankiety bezpieczeństwa osobowego, będącego załącznikiem do ustawy, i sposobu jego przesyłania do organu prowadzącego postępowanie. Należy zmierzać do takiego rozwiązania, aby ankieta bezpieczeństwa osobowego mogła stać się dokumen-

[23] Obecnie są to jedynie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia.

[24] Artykuł 24 ust. 2 pkt 1–3 lub 5 lub art. 24 ust. 3 ustawy – uczestnictwo w działalności wymierzonej przeciwko RP (szpiegostwo, terroryzm, sabotaż); zagrożenia ze strony obcych służb specjalnych; nieprzestrzeganie porządku konstytucyjnego; okoliczności powodujące podatność na szantaż lub wywieranie presji; poziom życia wyraźnie przewyższający uzyskiwane dochody; choroby psychiczne i uzależnienia (alkohol, środki odurzające lub substancje psychotropowe).

[25] Department of Defense Manual 5220.22 „National Industrial Security Program: Procedures For Government Activities Relating To Foreign Ownership, Control Or Influence (FOCI)".

[26] „Industrial Security Manual", Public Works and Services Canada.

[27] „Security Requirements for List X Contractors", Cabinet Office, National Security and Intelligence, Government Security Profession.

tem wypełnianym za pośrednictwem odpowiedniego programu komputerowego, dostępnego do jednorazowego pobrania ze strony ABW lub SKW (podobnie jak w przypadku deklaracji podatkowych). W dalszej perspektywie należy przeanalizować możliwość przesyłania wypełnionej ankiety do ABW lub SKW także drogą elektroniczną. Użycie odpowiedniego programu umożliwiłoby „spłaszczenie" ankiety w postaci eliminacji wszystkich jej podpunktów powiązanych z nadrzędnym pytaniem, jeżeli odpowiedź na to pytanie czyni bezzasadnym ich wypełnienie. Przy każdym pytaniu powinna istnieć możliwość wyświetlenia szczegółowych wskazówek dotyczących sposobu udzielania odpowiedzi (wypełnienia tego konkretnego punktu).

Tak jak podkreślono na wstępie, opracowanie jest oparte na subiektywnej ocenie autorów i jest ich propozycją zmian wybranych zagadnień z zakresu ochrony informacji niejawnych. Należy je traktować jako głos w szerszej dyskusji dotyczącej konieczności dostosowywania wszelkich środków bezpieczeństwa państwa do zmieniającej się rzeczywistości, nowych zagrożeń i oczekiwań skierowanych do służb specjalnych w zakresie skutecznego reagowania na te zagrożenia. Ponieważ mowa jest o bezpieczeństwie państwa, dyskusja na temat ewentualnych zmian w obowiązujących przepisach związanych z ochroną informacji niejawnych, jako integralnego elementu tego bezpieczeństwa, wydaje się nieunikniona i niezbędna.

Wybrana bibliografia

1. Bąk T., *Ustawodawstwo antyterrorystyczne w państwach Unii Europejskiej*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

2. Bożek M., *Nadzór Prezesa Rady Ministrów nad służbami specjalnymi i sposoby jego realizacji w świetle obowiązującego ustawodawstwa*, „Przegląd Sejmowy" 2010, nr 3.

3. Budyn-Kulik M., *Komentarz aktualizowany do art. 130 Kodeksu karnego*, LEX/el.

4. Burczaniuk P., *Znaczenie lobbingu w kontekście bezpieczeństwa wewnętrznego państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

5. Caparini M., *Controlling and overseeing intelligence services in democratic states*, w: *Democratic Control of Intelligence Services*, Ed.H. Born, M. Caparini, London 2007.

6. Fetke F., *Szpiegostwo w polskim prawie karnym – czy istnieje potrzeba zmian legislacyjnych?,* „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3.

7. Gardocki L., *Prawo karne*, Warszawa 2009, C.H. Beck.

8. Grzelak A., *Glosa do wyroku TS z dnia 21 grudnia 2016 r. C-203/15 oraz C-698/15. Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności*, „Europejski Przegląd Sądowy" 2017, nr 3.

9. Grzelak A., *Komentarz do art. 72 i komentarz do art. 73*, w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, A. Wróbel, N. Półtorak, D. Miąsik (red.), Warszawa 2012, Wolters Kluwer.

10. Grzelak A., *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015, Oficyna Wydawnicza SGH.

11. Hoc S., *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Opole 2002, bw.

12. Kardas P., *Kodeks karny. Część szczególna*, t. 2, A. Zoll (red.), Kraków 1999, Zakamycze.

13. Kardas P., *Komentarz do art. 130 Kodeksu karnego*, LEX/el.

14. Kłączyńska N., *Komentarz do art. 130 Kodeksu karnego*, LEX/el.

15. Kuć T., *Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16.

16. Kulicki J., *Kontrola skarbowa w systemie kontroli państwowej*, LEX/el.

17. Lebiedowicz A., *Istota szpiegostwa w polskim prawie karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2017, z. 2.

18. Lubiewski P., *Ustawa antyterrorystyczna wobec służb specjalnych. Rozszerzenie czy aktualizacja uprawnień*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

19. Michalczyk T., *Zamachy terrorystyczne w Europie – jak skutecznie prowadzić działania antyterrorystyczne w Polsce*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

20. Pogonowski P., *Nadzór nad służbami specjalnymi a bezpieczeństwo państwa na tle doświadczeń krajów demokratycznych*, w: *Interdyscyplinarność nauk o bezpieczeństwie. Paradygmat, wiedza, demokracja*, K. Raczkowski, K. Żukrowska, M. Żuber (red.), Warszawa 2013, Difin.

21. Popper K., *Społeczeństwo otwarte i jego wrogowie*, t. 1, Warszawa 2010, Wydawnictwo Naukowe PWN.

22. Popper K., *Społeczeństwo otwarte i jego wrogowie*, t. 2, Warszawa 2010, Wydawnictwo Naukowe PWN.

23. Pożaroszczyk D., *Federalny Urząd Ochrony Konstytucji – zadania i charakterystyka zwalczanych zagrożeń*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8.

24. Sacewicz K., *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7.

25. Skrzydło W., *Komentarz do art. 95 Konstytucji Rzeczypospolitej Polskiej*, LEX/el.

26. Szpunar M., *Komentarz do art. 267 Traktatu o funkcjonowaniu Unii Europejskiej*, w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 3, A. Wróbel (red.), Warszawa 2012, WKP.

27. Taras T., *Przestępstwo szpiegostwa w świetle nowego kodeksu karnego z 1969 r.*, „Palestra" 1970, 14/3 (147).

28. Tyburska, A. Jewartowski B., *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

29. Verpeaux M., *La loi sur le renseignement, entre sécurité et libertés; À propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*.

30. Wasilewska M.A., *Terroryzm CBRN a terroryzm biologiczny. Współczesne zagrożenie*, w: *Oblicza współczesnego terroryzmu*, K. Kowalczyk, W. Wróblewski (red.), Toruń 2006, Adam Marszałek.

31. Wierzbowski M., *Prawo administracyjne*, wyd. 4, Warszawa 2001, LexisNexis.

32. Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999, Wolters Kluwer.

33. Zając B., *Terroryzm zmusza do rewizji przepisów i poglądów* – Teza nr 1, Lex nr 31614/1.

34. Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002, Wydawnictwo Akademii Obrony Narodowej.

35. Zalewski S., *Służby specjalne w państwie demokratycznym*, wyd. II, Warszawa 2005, Akademia Obrony Narodowej, Wydział Wydawniczy.

36. Zubrzycki W., *Dzieje ustawy antyterrorystycznej w Polsce*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

37. *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, Zubrzycki W., Jałoszyński K., Babiński A. (red.), Szczytno 2016, Wyższa Szkoła Policji w Szczytnie.

38. Zwoliński I., *Komentarz do art. 130 Kodeksu karnego*, LEX/el.

39. Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej*, Kraków 2005, Abrys.

(fragment ze wstępu)
Problematyka dotycząca zagrożeń bezpieczeństwa narodowego leży w kręgu zainteresowań służb specjalnych, zarówno polskich, jak i zagranicznych. Obecnie obowiązujące uregulowania prawne w tym zakresie zostały wykreowane przed laty, często w okresie zimnej wojny, na podstawie ówczesnej siatki zagrożeń, w wielu wymiarach stanowiących reakcję na dwubiegunowy podział świata. Pojawienie się nowych rodzajów zagrożeń o charakterze hybrydowym, łączących w sobie działania destabilizacyjne, konwencjonalne, nieregularne, cybernetyczne czy też dezinformacyjne, oraz zagrożeń asymetrycznych, takich jak terroryzm, wreszcie postępująca informatyzacja praktycznie wszystkich dziedzin życia oraz rozwój nowych technologii i miniaturyzacja technologii, stanowią asumpt do podjęcia dyskusji na temat gruntownej redefinicji zadań i narzędzi organów odpowiadających za bezpieczeństwo państwa, w tym służb specjalnych, a zwłaszcza ich organizacji. Znalezienie właściwego remedium na współczesne zagrożenia – przy jednoczesnym zagwarantowaniu konstytucyjnych wolności i praw człowieka i obywatela – jest kwestią niezwykle istotną nie tylko z punktu widzenia organów władzy wszystkich państw na świecie, lecz także społeczeństwa obywatelskiego.

prof. dr hab. Piotr Pogonowski
Szef Agencji Bezpieczeństwa Wewnętrznego

Opracowania zamieszczone w niniejszej publikacji poruszają wiele wątków związanych z bezpieczeństwem narodowym, oscylujących wokół zagadnień pozostających we właściwości polskich służb specjalnych. Ich różnorodność jest tu atutem, gdyż ich autorzy, patrząc z perspektywy teorii i praktyki, ukazują różne punkty widzenia pozwalające na kompleksową ocenę współczesnych zagrożeń. Prezentowany materiał jest zbiorem zagadnień o charakterze prawnym, prawnomiędzynarodowym, ale i praktycznym. Jednym z głównych jego walorów jest aspekt analityczny. Dlatego powinien on zainteresować zarówno przedstawicieli służb, jak i środowiska akademickiego.

Piotr Burczaniuk

ISBN 978-83-938217-4-7