Piotr Burczaniuk, Michał Kamiński,
Marcin Nowiński, Mateusz Wieczerza

ANALIZA ROZWIĄZAŃ PRAWNYCH W ZAKRESIE FUNKCJONOWANIA SŁUŻB SPECJALNYCH W WYBRANYCH PAŃSTWACH

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

Projekt okładki Piotr Chorbot

ISSN 2080-1335

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane
All the articles published in the magazine are subject to reviews

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną.
Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów.

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 maju 2017

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

SPIS TREŚCI

WSTĘP

Niniejsza publikacja stanowi kompendium wiedzy na temat uprawnień służb specjalnych wybranych państw. Zebrane informacje pozwoliły na opracowanie dokładnej analizy prawnoporównawczej kompetencji przysługujących konkretnym służbom, a jednocześnie posłużyły do przedstawienia regulacji prawnych i uprawnień tych służb w kontekście zwalczania szpiegostwa i terroryzmu. Autorzy przybliżyli szczegółowe rozwiązania zastosowane w ustawodawstwach omawianych państw odnoszące się do czynności operacyjno-rozpoznawczych i analityczno-informacyjnych oraz zobrazowali metody i techniki pracy operacyjnej, w tym narzędzia służące do niejawnego pozyskiwania informacji za pośrednictwem środków komunikacji elektronicznej, z uwzględnieniem prawa jednostki do ochrony prywatności, a przede wszystkim danych osobowych.

Opracowanie ma na celu przybliżenie osobom zajmującym się tematyką kontrwywiadowczą oraz dotyczącą terroryzmu rozwiązań prawnych zastosowanych przez poszczególne kraje, a także usystematyzowanie zebranej dotychczas wiedzy w tym zakresie. Takie syntetyczne ujęcie zagadnienia może okazać się pomocne przy wprowadzaniu ewentualnych zmian w prawie krajowym, dotyczących rozwiązań w powyższym zakresie.

Warto podkreślić, że informacje zebrane w publikacji pozwoliły na wyciągnięcie tezy, iż skuteczność służb wywiadowczych działających poza granicami kraju wynika z przepisów prawnych, które charakteryzują się wysokim stopniem ogólności. Takie rozwiązanie zapobiega nadmiernemu ograniczaniu swobody działania służb specjalnych oraz pozwala na realizowanie wielu zadań pozostających w ich kompetencjach.

CZĘŚĆ I

Ogólna charakterystyka uprawnień służb specjalnych wybranych państw[1]

BELGIA

System prawny Belgii wyodrębnia dwie służby specjalne: cywilną Służbę Bezpieczeństwa Państwa (Sûreté de l'État/Veiligheid van den Staat – VSSE) odpowiedzialną za bezpieczeństwo wewnętrzne państwa oraz Służbę Bezpieczeństwa i Wywiadu (Le Service Général du Renseignement et de la Securité – SGRS), wchodzącą w skład sił zbrojnych, działającą zarówno na terytorium kraju, jak i poza jego granicami. Zakres kompetencji obu służb został określony w sposób szeroki, a za kryterium tworzenia architektury instytucjonalnej systemu bezpieczeństwa przyjęto cywilny lub wojskowy charakter określonej służby. Prawodawca nie zdecydował się na utworzenie odrębnych służb o kompetencjach wywiadowczych (zewnętrznych) i kontrwywiadowczych (wewnętrznych).

VSSE jest wewnętrzną służbą bezpieczeństwa podlegającą ministrowi sprawiedliwości i w ograniczonym zakresie ministrowi spraw wewnętrznych. Do jej najważniejszych zadań należy: pozyskiwanie i analizowanie informacji o zagrożeniach demokracji i ustroju konstytucyjnego oraz przedstawianie tych analiz rządowi (m.in. dotyczących zagrożeń o charakterze terrorystycznym, ekstremistycznym, szpiegostwa, proliferacji broni masowego rażenia, działalności organizacji radykalnych, nieuprawnionej ingerencji w funkcjonowanie organów państwa, zorganizowanej przestępczości). Służba odpowiada również za ochronę najważniejszych osób w państwie i prowadzenie postępowań sprawdzających w zakresie dostępu do informacji niejawnych. Współpracuje także z organami wymiaru sprawiedliwości podczas postępowań karnych.

SGRS podlega ministrowi obrony narodowej i stanowi integralną część sił zbrojnych. Jej zadaniem jest pozyskiwanie i analizowanie informacji dotyczących działań zagrażających integralności terytorialnej, obronności, skuteczności wojskowych planów obronnych i bezpieczeństwu obywateli Belgii za granicą. Odpowiada również za bezpieczeństwo personelu Ministerstwa Obrony, infrastruktury wojskowej, ochronę tajemnicy wojskowej, potencjału technologicznego i naukowego sił zbrojnych oraz za ich bezpieczeństwo cybernetyczne. Prowadzi postępowania sprawdzające w stosunku do osób zatrudnionych w strukturach podlegających Ministerstwu Obrony Narodowej. Analogicznie do VSSE może ona również udzielać wsparcia organom wymiaru sprawiedliwości w toku postępowań karnych.

Dopełnienie systemu stanowią Rada Bezpieczeństwa Narodowego działająca pod przewodnictwem premiera, w której skład wchodzą m.in. minister sprawiedliwości, obrony narodowej, spraw wewnętrznych, spraw zagranicznych oraz Jednostka Koordynacji Oceny Zagrożeń (Coordination Unit for Threat Analysis – CUTA), która jest odpowiedzialna za dokonywanie oceny strategicznej zagrożeń o charakterze terrorystycznym i ekstremistycznym.

[1] Omawiane w publikacji państwa są prezentowane w kolejności alfabetycznej (przyp. red.).

Najważniejszym elementami systemu prawnego są: *Ustawa z dnia 30 listopada 1998 r. o służbach wywiadowczych i bezpieczeństwa*[2] (dalej: ustawa), określająca podstawy normatywne funkcjonowania służb specjalnych oraz *Ustawa z dnia 4 lutego 2010 r. o metodach pozyskiwania informacji przez służby wywiadowcze i bezpieczeństwa*[3].

1. Organizacja i zadania VSSE

Zgodnie z art. 5 ustawy VSSE podlega ministrowi sprawiedliwości. Jeśli zadania są związane z ochroną osób lub zapewnieniem bezpieczeństwa publicznego, minister spraw wewnętrznych może polecić służbie wykonanie konkretnych zadań, nie ingerując w sprawy związane z organizacją służby. Minister może również udzielić zaleceń precyzujących, jakie instrumenty mają zostać w tym celu wykorzystane. W przypadku gdy realizacja wskazanych zaleceń nie jest możliwa, gdyż utrudniałoby lub uniemożliwiało wykonanie innych zadań, służba niezwłocznie informuje o tym ministra spraw wewnętrznych. Nie zwalnia to jednak VSSE z obowiązku wypełnienia wyznaczonych zadań.

Minister sprawiedliwości odpowiada za organizację i zarządzanie służbą, szczególnie w sprawach związanych z polityką finansową, kadrową, kształceniem oraz wyposażeniem funkcjonariuszy. Jeśli sprawy organizacyjne mają bezpośredni wpływ na sposób realizacji zadań związanych z ochroną osób i zapewnieniem bezpieczeństwa publicznego, minister spraw wewnętrznych współdziała w tym zakresie z ministrem sprawiedliwości

Zgodnie z art. 7 ustawy do zadań VSSE należy:

1) zbieranie, analizowanie i przetwarzanie informacji dotyczących wszystkich działań zagrażających lub mogących stanowić zagrożenie bezpieczeństwa wewnętrznego państwa, trwałości ustroju demokratycznego i konstytucyjnego, bezpieczeństwa zewnętrznego państwa i stosunków międzynarodowych, potencjału naukowego lub gospodarczego oraz wszystkich innych fundamentalnych interesów państwa;
2) prowadzenie postępowań sprawdzających powierzonych służbie zgodnie z dyrektywami Komitetu Ministrów;
3) realizacja zadań powierzonych przez ministra spraw wewnętrznych w zakresie ochrony osób;
4) realizacja wszelkich innych zadań powierzonych służbie na mocy ustawy.

Art. 8 ustawy zawiera definicje legalne pojęć zawartych w art. 7:

1) działalność zagrażająca lub mogąca stanowić zagrożenie – wszelka działalność, indywidualna lub zbiorowa, prowadzona w kraju lub wywodząca się spoza jego granic, która może mieć związek ze szpiegostwem, ingerencją, terroryzmem, ekstremizmem, proliferacją, organizacjami radykalnymi, zorganizowanymi grupami przestępczymi, w tym szerzeniem propagandy, nawoływanie do bezpośredniego lub pośredniego wsparcia, zwłaszcza przez dostarczanie środków finansowych, technicznych lub logistycznych, informacji o potencjalnych celach, rozwijanie struktur i zakresu tej działalności oraz realizacja zamierzonych celów.

[2] *Loi organique des services de renseignement et de sécurité, 30 novembre 1998* [online], www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032 [dostęp: 14 II 2017].

[3] *Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité, 4 fevrier 2010* [online], www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=20100204026 [dostęp: 14 II 2017].

Pojęcia użyte w niniejszym punkcie oznaczają:

a) szpiegostwo – zbieranie lub dostarczanie informacji niedostępnych publicznie oraz podejmowanie działań mających na celu przygotowanie lub ułatwianie zbierania tych informacji;
b) terroryzm – użycie przemocy w stosunku do osób lub mienia, motywowane ideologicznie lub politycznie, w celu osiągnięcia określonych zamierzeń przez stosowanie terroru, zastraszanie lub groźby;
c) ekstremizm – koncepcje lub plany o charakterze rasistowskim, ksenofobicznym, anarchistycznym, nacjonalistycznym, autorytarnym lub totalitarnym, bez względu na to, czy są motywowane względami politycznymi, ideologicznymi, wyznaniowymi czy filozoficznymi, sprzeczne, w teorii lub w praktyce, z zasadami demokracji lub z prawami człowieka, z poprawnym funkcjonowaniem instytucji demokratycznych lub z innymi elementami niezbędnymi dla istnienia państwa prawa;
d) proliferacja – obrót lub transakcje, których przedmiotem są materiały, produkty, mienie lub know-how, które mogą przyczynić się do produkcji lub rozwoju niekonwencjonalnych lub bardzo zaawansowanych systemów uzbrojenia. To pojęcie obejmuje przede wszystkim rozwój broni nuklearnej, chemicznej, biologicznej, powiązanych z nimi systemów transmisji danych oraz osoby, struktury lub państwa zaangażowane w tę działalność;
e) organizacja radykalna – każde ugrupowanie o charakterze religijnym, filozoficznym lub określające się jako takie, dopuszczające się w swojej działalności nielegalnych czynów, wyrządzające szkodę osobom fizycznym, prawnym lub naruszające godność ludzką;
f) zorganizowane grupy przestępcze – ugrupowania liczące więcej niż dwie osoby utworzone w dającym się zdefiniować czasie, w celu wspólnego popełnienia zbrodni lub występków, uzyskania korzyści w sposób bezpośredni lub pośredni, wykorzystujące zastraszenie, groźby, przemoc, dopuszczające się oszustwa, korupcji lub wykorzystujące podmioty gospodarcze lub inne w celu ukrycia przestępczego charakteru swojej działalności lub ułatwienia dokonania czynu zabronionego. Pojęcie obejmuje zorganizowane grupy, których działalność ma związek ze zjawiskami opisanymi w pkt a–e oraz g niniejszego artykułu oraz których działalność może zdestabilizować sytuację polityczną lub społeczno-ekonomiczną;
g) ingerencja – usiłowanie wpłynięcia na procesy decyzyjne nielegalnymi metodami.

Art. 8 pkt 2 ustawy zawiera definicję legalną pojęcia bezpieczeństwo wewnętrzne państwa oraz trwałość porządku demokratycznego i konstytucyjnego, stanowiąc, że ten termin oznacza bezpieczeństwo instytucji państwa i ochronę prawidłowego funkcjonowania fundamentalnych elementów państwa prawa, instytucji demokratycznych, a także praw człowieka i podstawowych praw i wolności. Pod tym pojęciem należy też rozumieć bezpieczeństwo i ochronę osób oraz mienia.

Bezpieczeństwo zewnętrzne państwa i stosunki międzynarodowe określono jako ochronę integralności terytorialnej, suwerenności i niepodległości państwa, interesów państw, których cele są zbieżne z celami Belgii, praz organizacji międzynarodowych i ponadnarodowych. Ochrona osób jest natomiast rozumiana

jako zapewnienie ochrony życia i nietykalności cielesnej następujących osób: szefów państw i rządów, członków rodziny szefów państw i rządów, członków rządu Belgii oraz rządów innych państw oraz innych osób narażonych na zagrożenia, o których mowa w art. 8.

2. Realizacja zadań służb wywiadowczych i bezpieczeństwa

W ramach realizacji ustawowych zadań służby mogą stosować instrumenty ograniczające konstytucyjne prawa i wolności wyłącznie na podstawie i w granicach obowiązujących przepisów prawnych. Służby mogą pozyskiwać, gromadzić, otrzymywać i przetwarzać informacje oraz dane osobowe, które mogą mieć istotne znaczenie dla realizacji ich zadań oraz prowadzić dokumentację dotyczącą osób i zdarzeń istotnych z punktu widzenia ich działalności. Informacje zawarte w tej dokumentacji muszą mieć związek z celem, dla którego określony rejestr lub baza danych zostały utworzone.

Treść art. 13 została znacznie rozszerzona przez wspomnianą już ustawę o metodach pozyskiwania informacji, która upoważnia funkcjonariuszy służb do posługiwania się danymi legalizacyjnymi oraz wyłącza ich odpowiedzialność karną za popełnienie przestępstwa w związku z realizacją czynności służbowych, przy spełnieniu określonych przesłanek. W ujęciu ogólnym można uznać, iż ten przepis wprowadza instrumenty rozszerzające uprawnienia funkcjonariuszy pełniące przede wszystkim funkcję gwarancyjną rozumianą zarówno jako ochrona fizycznego bezpieczeństwa funkcjonariusza, jak i ograniczenie zakresu jego ewentualnej odpowiedzialności karnej za czyny popełnione w związku z realizacją czynności służbowych.

Na zasadzie odstępstwa od art. 231 kodeksu karnego funkcjonariusz może, ze względów bezpieczeństwa i w celu ochrony tajemnicy określonych czynności służbowych, używać danych legalizacyjnych.

Na zasadzie odstępstwa od ogólnych norm, zgodnie z którymi funkcjonariusze realizujący zadana pozyskiwania informacji nie mogą dopuszczać się przestępstw lub wykroczeń, art. 13/1 § 2 ustawy o służbach wywiadowczych i bezpieczeństwa stanowi, iż nie podlegają karze ci funkcjonariusze, którzy, wykonując czynności służbowe, naruszają przepisy ustawy o ruchu drogowym lub innych ustaw, jeżeli te naruszenia są bezwzględnie konieczne podczas realizacji określonego zadania lub w celu zagwarantowania bezpieczeństwa tym funkcjonariuszom lub innym osobom. Nie podlegają również karze funkcjonariusze, którzy po uzyskaniu uprzedniej i wyrażonej wprost zgody Komisji[4], udzielonej na podstawie art. 43/1 ustawy, dopuszczają się czynu zabronionego w toku realizacji czynności związanych z wykorzystaniem szczególnych metod pozyskiwania informacji, w zakresie niezbędnym do wykonania określonych zadań lub zapewnienia bezpieczeństwa tych funkcjonariuszy lub innych osób. Naruszenia, o których mowa w art. 13/1, muszą być wprost proporcjonalne do zamierzonego celu i w żadnym wypadku nie mogą stanowić zamachu na nietykalność cielesną.

Ustawa o metodach pozyskiwania informacji wprowadza zasadę rozgraniczenia czynności dochodzeniowo-śledczych prowadzonych przez służby wywiadowcze i bez-

[4] Komisja administracyjna utworzona na podstawie art. 43/1 ustawy jest odpowiedzialna za nadzór nad stosowaniem specjalnych i nadzwyczajnych metod pozyskiwania informacji przez służby wywiadowcze i bezpieczeństwa. Członkowie komisji i ich zastępcy są powoływani przez króla na wniosek ministra sprawiedliwości i ministra obrony. Komisja składa się z trzech członków mających tytuł sędziego. Kadencja członków trwa pięć lat, z możliwością dwukrotnego przedłużenia.

pieczeństwa oraz prokuraturę, stanowiąc, iż służby nie prowadzą dochodzeń, które mogą ingerować w kompetencje prokuratora królewskiego, federalnego lub sędziego śledczego, i mogą negatywnie wpływać na przebieg prowadzonego przez nich postępowania.

W sytuacji, gdy służby zdobywają informacje mogące mieć wpływ na postępowanie prowadzone przez wymienione podmioty, informują o tym komisję, która w porozumieniu w organami wymiaru sprawiedliwości i prokuraturą decyduje o tym, na jakich zasadach służby mogą kontynuować swoje działania w tego rodzaju sprawach.

2.1. Zwyczajne metody pozyskiwania informacji

Organy wymiaru sprawiedliwości i administracji publicznej oraz funkcjonariusze innych służb mogą przekazywać służbom wywiadowczym i bezpieczeństwa informacje, które mogą być istotne podczas realizacji ich ustawowych zadań. Przekazanie może nastąpić z własnej inicjatywy tych organów lub na wniosek służb wywiadowczych i bezpieczeństwa. W sytuacji, gdy powyższe podmioty uznają, iż przekazanie służbom informacji wskazanych we wniosku może negatywnie wpłynąć na toczące się postępowanie karne, zbieranie informacji, przewidziane w ustawie o przeciwdziałaniu wykorzystywaniu systemu finansowego w celu prania pieniędzy i finansowaniu terroryzmu, bądź może zagrażać określonej osobie – mogą odmówić przekazania informacji w terminie pięciu dni roboczych od otrzymania wniosku, uzasadniając pisemnie motywy tej odmowy.

W myśl *Ustawy z dnia 8 grudnia 1992 r. o ochronie prywatności w związku z przetwarzaniem danych osobowych*[5] służby wywiadowcze i bezpieczeństwa mogą żądać od osób fizycznych i podmiotów niepaństwowych udzielenia im informacji niezbędnych do realizacji ich ustawowych zadań, w tym danych osobowych.

Funkcjonariusze służb mogą, w każdym przypadku, wejść do miejsc dostępnych dla nieograniczonej liczby osób oraz do obiektów hotelowych i innych obiektów mieszkalnych, z uwzględnieniem zasady poszanowania miru domowego. Mogą również żądać od ich właścicieli lub zarządców dokumentów zawierających dane osób przebywających w obiektach.

Służby wywiadowcze i bezpieczeństwa mogą także korzystać z osobowych źródeł informacji. Są wówczas zobowiązane do zapewnienia bezpieczeństwa przekazywanych przez nie informacji oraz do ochrony danych umożliwiających identyfikację tych osób.

2.2. Specjalne oraz nadzwyczajne metody pozyskiwania informacji

Wykaz metod opisywanych powyżej został rozszerzony przez ustawę o metodach pozyskiwania informacji z 2010 r. Na jej podstawie wprowadzono zbiór tzw. specjalnych oraz nadzwyczajnych metod pozyskiwania informacji, które mogą być wykorzystywane zarówno przez VSSE, jak i SGRS.

Do **specjalnych metod pozyskiwania informacji** (dalej: smpi) zalicza się (art. 18/2 § 1):

1) obserwację, z wykorzystaniem środków technicznych, w miejscach publicznych lub w miejscach prywatnych dostępnych dla publiczności lub obserwację miejsc prywatnych niedostępnych dla publiczności, z wykorzystaniem lub bez środków technicznych;

[5] *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* [online], www.privacycommission.be/sites/privacycommission/files/documents/privacy_fr_0.pdf [dostęp: 14 II 2017].

2) inwigilację (inspekcję, kontrolę) za pomocą środków technicznych miejsc publicznych, miejsc prywatnych dostępnych dla publiczności oraz znajdujących się w tych miejscach zamkniętych przedmiotów (obiektów);
3) pozyskiwanie informacji identyfikujących nadawcę lub adresata przesyłki, lub posiadacza skrzynki pocztowej;
4) instrumenty identyfikujące abonenta lub użytkownika usługi komunikacji elektronicznej lub używanego środka komunikacji elektronicznej;
5) instrumenty umożliwiające pozyskanie danych o połączeniu dokonanym z użyciem środków komunikacji elektronicznej oraz o lokalizacji nadawcy i odbiorcy tego typu komunikacji.

Do **nadzwyczajnych metod pozyskiwania informacji** (dalej: nmpi) należą (art. 18/2 § 2):

1) obserwacja – z wykorzystaniem lub bez wykorzystania środków technicznych – miejsc prywatnych niedostępnych dla publiczności, miejsc zamieszkania lub ich przynależności, lub lokali wykorzystywanych w celach zawodowych lub jako miejsce zamieszkania przez adwokatów, lekarzy lub dziennikarzy;
2) inwigilacja – z wykorzystaniem lub bez wykorzystania środków technicznych – miejsc prywatnych niedostępnych dla publiczności, miejsc zamieszkania lub ich przynależności, lokali wykorzystywanych przez adwokatów, lekarzy bądź dziennikarzy w celach zawodowych lub jako miejsce zamieszkania oraz znajdujących się w tych lokalach zamkniętych przedmiotów (obiektów);
3) utworzenie lub wykorzystanie osoby prawnej w celu wsparcia działań operacyjnych oraz wprowadzenie funkcjonariuszy działających pod fałszywą tożsamością;
4) otwarcie i zapoznanie z treścią przesyłki powierzonej operatorowi pocztowemu lub innej przesyłki;
5) zbieranie informacji o kontach i transakcjach bankowych;
6) ingerencja w działanie systemu informatycznego – z wykorzystaniem lub bez wykorzystania środków technicznych – fałszywych sygnałów, haseł lub właściwości;
7) nasłuch, zapoznanie z treścią rozmów i ich rejestrowanie.

Wykorzystywanie zarówno specjalnych, jak i nadzwyczajnych metod zdobywania informacji w stosunku do adwokatów, lekarzy lub dziennikarzy, a także wykonywanie czynności, których przedmiotem jest miejsce zamieszkania lub środki komunikacji wyżej wymienionych osób, które te osoby wykorzystują w celach zawodowych, jest możliwe wyłącznie po uprzednim poinformowaniu przewodniczącego właściwego samorządu zawodowego. Ustawa wprowadza również dodatkowy mechanizm weryfikacji proporcjonalności przeprowadzania opisywanych czynności. Przewodniczący komisji w każdym przypadku ocenia, czy uzyskane w ten sposób informacje, które są chronione na podstawie przepisów o tajemnicy zawodowej wymienionych profesji, są bezpośrednio związane z konkretnym zagrożeniem. W przypadku zastosowania jednej z nadzwyczajnych metod pozyskiwania informacji w stosunku do adwokata, lekarza lub dziennikarza, niezbędnym warunkiem jej wykorzystania jest obecność przewodniczącego komisji lub delegowanego przez niego członka komisji.

2.2.1. Szczegółowe zasady stosowania specjalnych metod pozyskiwania informacji (smpi)

System wykorzystywania poszczególnych kategorii metod pozyskiwania informacji – zwykłych, specjalnych bądź nadzwyczajnych – został zbudowany na podstawie zasad subsydiarności, proporcjonalności i gradacji możliwości zastosowania danej metody w zależności od stopnia i charakteru konkretnego zagrożenia oraz od przydatności w konkretnym przypadku metod charakteryzujących się mniejszym stopniem inwazyjności. W myśl tych zasad art. 18/3 ustawy stanowi, że smpi mogą zostać wykorzystane, gdy zwyczajne metody pozyskiwania informacji, biorąc pod uwagę rodzaj i charakter zagrożenia, okażą się niewystarczające do zrealizowania zadań służby. Konkretna metoda powinna zostać dobrana z uwzględnieniem konkretnego zagrożenia. Wykorzystanie smpi następuje na podstawie pisemnej i uzasadnionej decyzji szefa służby oraz po uzyskaniu pozytywnej opinii komisji.

W ustawie przewidziano ograniczenie możliwości zastosowania smpi wobec adwokatów, lekarzy i dziennikarzy (dotyczy to również środków komunikacji wykorzystywanych przez nich dla celów zawodowych). Te metody mogą być zastosowane wobec wymienionych kategorii osób wyłącznie wtedy, gdy służby zdobędą informacje wzbudzające uzasadnione podejrzenie, że te osoby uczestniczą lub uczestniczyły osobiście w działaniach stwarzających potencjalne zagrożenie. Kolejnym warunkiem zastosowania smpi jest pozytywna opinia komisji po przedstawieniu jej okoliczności sprawy przez szefa służby.

Ustawa przyznaje komisji administracyjnej, o której mowa w art. 43/1 ustawy, szerokie uprawnienia kontrolne w zakresie stosowania smpi: każdego miesiąca komisja otrzymuje od właściwej służby listę środków, które zostały zastosowane. Jej członkowie mogą w każdej chwili dokonać weryfikacji legalności działań podejmowanych przez służby oraz badać, czy czynią one zadość zasadom subsydiarności i proporcjonalności. Komisja ma również prawo do dostępu do miejsc, w których są przechowywane informacje związane ze stosowaniem smpi, wglądu do dokumentów i uzyskiwania wyjaśnień od funkcjonariuszy służb. Informacje zebrane w sposób niezgodny z prawem są umieszczane pod nadzorem komisji, która uniemożliwia dostęp do nich funkcjonariuszom, a także zawiesza stosowanie smpi w sprawie, której informacje te dotyczą.

Stosowanie smpi może zostać przedłużone lub ulec odnowieniu wyłącznie po wydaniu przez szefa służby nowej decyzji spełniającej wymogi opisane powyżej.

2.2.2. Szczegółowe zasady stosowania nadzwyczajnych metod pozyskiwania informacji (nmpi)

Zgodnie z założeniem polegającym na dążeniu do dostosowania wyboru określonej metody pozyskiwania informacji do specyfiki i charakteru konkretnego zagrożenia art. 18/9 § 2 ustawy stanowi, że nmpi mogą być stosowane w wyjątkowych przypadkach, gdy zwyczajne lub specjalne środki pozyskiwania danych nie są wystarczające do zrealizowania określonego zadania. Szefowie służb mogą autoryzować ich wykorzystanie wyłącznie po uzyskaniu pozytywnej opinii komisji. Wybór konkretnej nmpi w danym przypadku musi uwzględniać stopień potencjalnego zagrożenia oraz ryzyko dla funkcjonariuszy lub osób trzecich wiążące się z jej zastosowaniem.

Ustawa określa szczegółowo przesłanki uzasadniające stosowanie nmpi. Do ich wykorzystania, podobnie jak w przypadku zwyczajnych i specjalnych metod pozyskiwa-

nia informacji, są uprawnione zarówno VSSE, jak i SGRS. Lista przesłanek uzasadniających stosowanie przez VSSE nmpi obejmuje: zagrożenie bezpieczeństwa wewnętrznego państwa, trwałości porządku demokratycznego i konstytucyjnego, bezpieczeństwa zewnętrznego państwa i stosunków międzynarodowych oraz potencjału naukowego i gospodarczego, gdy te zagrożenia są związane z działalnością szpiegowską, terrorystyczną, w tym z procesem radykalizacji, z proliferacją broni masowego rażenia, działalnością organizacji radykalnych lub zorganizowanych grup przestępczych.

Analogicznie jak w przypadku specjalnych metod pozyskiwania informacji nadzwyczajne metody mogą być zastosowane w stosunku do adwokatów, lekarzy lub dziennikarzy wyłącznie, gdy służby dysponują informacjami powodującymi uzasadnione podejrzenie, iż biorą lub brali oni udział w działalności stwarzającej zagrożenie w myśl art. 18/9 § 1, pkt 1 i 2 ustawy.

Proces autoryzacji nmpi

Szef służby przedkłada projekt autoryzacji do zaopiniowania komisji, która ocenia, czy wykorzystanie npmi jest zgodne z prawem i czy są spełnione wymogi proporcjonalności i subsydiarności. Z zastrzeżeniem wyjątków przewidzianych w przepisach szczególnych opisywane metody mogą być stosowane przez okres nieprzekraczający dwóch miesięcy. Szef służby może, po uzyskaniu pozytywnej opinii komisji, przedłużyć stosowanie nmpi na okres nieprzekraczający dwóch miesięcy, z zastrzeżeniem, że te czynności zostaną wstrzymane po ustaniu przyczyn uzasadniających ich stosowanie. W razie powzięcia informacji o nielegalnym wykorzystywaniu tego środka w konkretnym przypadku, szef zawiesza jego stosowanie. W dalszej kolejności przedkłada on komisji decyzję o zakończeniu lub zawieszeniu stosowania nmpi, w zależności od okoliczności danej sprawy. Kolejne przedłużenie jest możliwe wyłącznie w razie zaistnienia szczególnych okoliczności.

Członkowie komisji mogą w każdej chwili przeprowadzić kontrolę legalności stosowania nmpi, w tym poszanowania zasad subsydiarności i proporcjonalności. Ustawa przyznaje członkom komisji – analogiczne do opisanych powyżej szczególnych metod pozyskiwania informacji – uprawnienia kontrolne w odniesieniu do empi: dostęp do miejsc, w których są przechowywane i przetwarzane informacje zebrane przy wykorzystaniu nmpi, wysłuchanie funkcjonariuszy służb oraz zabezpieczenie dokumentów.

Komisja postanawia o zakończeniu stosowania nmpi w razie stwierdzenia, że zagrożenie uzasadniające ich stosowanie ustało lub jeżeli wykorzystywanie określonej metody przestało być użyteczne. W razie wykrycia nielegalności stosowania tej metody komisja postanawia o jej zawieszeniu. Informacje zebrane w sposób niezgodny z prawem są przechowywane pod kontrolą komisji.

Pod rygorem nieważności wniosek o autoryzację zastosowania nmpi jest sporządzany w formie pisemnej, oznaczony datą dzienną i zawiera:

- charakterystykę zagrożeń uzasadniających zastosowanie nmpi lub elementów wskazujących na udział adwokata, lekarza lub dziennikarza w działalności stwarzającej zagrożenie bezpieczeństwa państwa;
- określenie przyczyn, z jakich zastosowanie nmpi jest w konkretnym przypadku niezbędne;
- wskazanie osób fizycznych lub prawnych, stowarzyszeń lub ugrupowań, obiektów, miejsc, zdarzeń lub informacji mających stanowić przedmiot nmpi;

- wykaz środków technicznych, które mają zostać wykorzystane w celu zastosowania nmpi;
- okres stosowania nmpi, licząc od momentu udzielenia autoryzacji;
- nazwiska i stopnie służbowe funkcjonariuszy, którzy mają być odpowiedzialni za stosowanie nmpi.

Komisja wydaje opinię w terminie czterech dni od uzyskania wniosku. W przypadku sporządzenia przez komisję negatywnej opinii, zastosowanie nmpi w danej sprawie jest niemożliwe. Jeżeli komisja nie wyda takiej opinii w podanym terminie, służba (szef służby) może zwrócić się do właściwego ministra z wnioskiem o autoryzację, a ten wydaje decyzję w możliwie najkrótszym terminie. W razie autoryzacji przez ministra szef służby informuje go, w ustalonych przez ministra odstępach czasu, o przebiegu stosowania nmpi.

Niewydanie przez komisję opinii we wskazanym terminie pociąga za sobą modyfikację trybu autoryzacji polegającą na przeniesieniu obowiązków związanych z nadzorem nad stosowaniem omawianego instrumentu na właściwego ministra. W konsekwencji staje się on organem uprawnionym do podjęcia decyzji o zakończeniu stosowania nmpi (przesłanki zakończenia stosowania empi nie ulegają zmianie; przesłankami są ustanie zagrożenia i brak przydatności metody w danej sprawie).

W nagłych sytuacjach, gdy każda zwłoka może poważnie zagrozić interesom wymienionym w art. 18/9 ustawy, szef służby może dokonać pisemnej autoryzacji zastosowania nmpi na okres nieprzekraczający 48 godzin, po uprzednim uzyskaniu pozytywnej opinii przewodniczącego komisji. Autoryzacja wskazuje motywy, z których powodu zastosowano ten tryb, i jest niezwłocznie przekazywana wszystkim członkom komisji. W razie negatywnej opinii przewodniczącego co do zastosowania nmpi w trybie nagłym, ta metoda nie może zostać wykorzystana. W przypadku gdy przewodniczący komisji zwleka z wydaniem opinii, szef służby może zwrócić się o autoryzację do właściwego ministra, co pociąga za sobą zmianę dalszego trybu postępowania, analogicznie jak w przypadku autoryzacji dokonywanej w trybie zwyczajnym.

DANIA

System instytucjonalno-prawny wypracowany w Danii wyróżnia dwie służby specjalne: Służbę Bezpieczeństwa i Wywiadu (Politiets Efterrentningstjeneste – PET) oraz Służbę Wywiadu Obronnego (Forvarets Efterretningstjeneste – FE). PET pełni funkcję wewnętrznej służby kontrwywiadowczej, która jest częścią Policji, FE natomiast jest zewnętrznym organem wywiadowczym o charakterze wojskowym.

Podstawą normatywną działania PET jest *Ustawa z dnia 1 stycznia 2014 r. Służbie Bezpieczeństwa i Wywiadu*[6]. Określa ona zakres właściwości służby, sposób wykonywania czynności dochodzeniowo-śledczych, nadzór nad służbą oraz inne kwestie ustrojowo-prawne. Jak już wspomniano, PET stanowi integralną część Policji – jest jednym z jej departamentów. Zadania realizowane przez PET obejmują dwa zasadnicze komponenty: neutralizację zagrożeń bezpieczeństwa wewnętrznego oraz pełnienie funkcji krajowej władzy bezpieczeństwa i ochronę informacji niejawnych.

[6] *The Act on the Danish Security and Intelligence Service*, 1 January 2014. Dokument dostępny na stronie www.retsinformation.dk/Forms/R0710.aspx?id=165838.

Zgodnie z rozdziałem 1 ustawy do zadań służby należy:

1) zapobieganie przestępstwom przeciwko niepodległości i bezpieczeństwu państwa oraz przestępstwom przeciwko konstytucji i najwyższym władzom w rozumieniu rozdziałów 12 i 13 kodeksu karnego, ściganie ich oraz ich zwalczanie[7];
2) zapobieganie innym poważnym przestępstwom zagrażającym krajowemu lub międzynarodowemu porządkowi społecznemu;
3) przygotowywanie analiz zagrożeń i ryzyka zaistnienia sytuacji godzących w bezpieczeństwo państwa;
4) współdziałanie z innymi organami o charakterze policyjnym;
5) informowanie ministra sprawiedliwości o sprawach istotnych z punktu widzenia bezpieczeństwa narodowego, o innych kwestiach istotnych z punktu widzenia działalności służby oraz o najważniejszych sprawach indywidualnych;
6) pełnienie funkcji krajowej władzy bezpieczeństwa oraz udzielanie wsparcia podmiotom publicznym i prywatnym w zakresie spraw związanych z bezpieczeństwem, z uwzględnieniem udzielania niezbędnej pomocy przy prowadzeniu postępowań sprawdzających;
7) wykonywanie innych zadań nałożonych na służbę na podstawie odrębnych przepisów.

Minister sprawiedliwości może postanowić o przekazaniu polecenia wykonania określonych czynności, niezbędnych do realizacji zadań opisanych powyżej, jednostce wywiadowczej Policji.

Odwołanie expressis verbis do rozdziałów 12 i 13 kodeksu karnego zawarte w § 1 ustawy powoduje, że zakres kompetencji PET w kontekście zwalczania zagrożeń bezpieczeństwa wewnętrznego nie może pomijać charakterystyki przestępstw tam zawartych.

Rozdział 12 kodeksu karnego penalizuje następujące czyny określone jako przestępstwa przeciwko niepodległości i bezpieczeństwu państwa:

1) popełnienie czynu mającego na celu poddanie państwa lub jego części pod władzę innego państwa lub secesję jego części, z pomocą zagraniczną, z użyciem siły lub groźbą jej użycia, a także prowadzenie w tym celu działalności antypaństwowej, działalności mającej na celu obniżenie wydajności produkcji lub handlu oraz udział w tego rodzaju działaniach, ze świadomością celu, jakim mają one służyć;
2) prowadzenie zarówno działań, których celem jest doprowadzenie Danii lub państwa sprzymierzonego do udziału w wojnie, wrogiej okupacji terytorium lub innych agresywnych działań, np. blokada lub jakiekolwiek inne środki przymusu, jak i innych działań mających na celu naruszenie niepodległości Danii, dokonywanych przy współpracy z zagranicą;
3) publiczne wystąpienia mające na celu doprowadzenie do podjęcia wrogich działań przeciwko Danii lub spowodowanie ewidentnego zagrożenia tego rodzaju działaniami;
4) publiczne wystąpienia mające na celu wywołanie ingerencji obcego państwa w wewnętrzne sprawy Danii lub spowodowanie ewidentnego zagrożenia takiej ingerencji;
5) działania mające na celu organizację pomocy lub wsparcia dla obcego państwa w obliczu wojny, wrogiej okupacji lub jakichkolwiek innych agresywnych działań wymierzonych w Danię przez to państwo;

[7] *Danish Criminal Code* [online], https://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2005,pdf [dostęp: 14 II 2017].

6) udzielanie pomocy wrogiemu państwu w czasie wojny lub okupacji przez działanie lub poparcie werbalne, wspieranie wrogich interesów, a także obniżanie zdolności obronnych Danii lub państwa sprzymierzonego. Za udzielanie pomocy wrogiemu państwu kodeks uznaje:
   a) prowadzenie rekrutacji do sił zbrojnych obcego państwa znajdującego się w stanie wojny z Danią lub okupującego jej terytorium, a także do sił zbrojnych lub policyjnych współdziałających z nim, albo dla jakichkolwiek innych podobnych podmiotów lub organizacji,
   b) działalność w charakterze pracownika cywilnego w Policji lub administracji więziennej państwa znajdującego się w stanie wojny z Danią lub okupującego jej terytorium, jeżeli ta działalność uwzględnia nadzór nad osadzonymi lub ich przesłuchiwanie,
   c) udzielanie informacji lub współpracę o podobnym charakterze z organami wrogiego państwa lub podmiotami oraz osobami współdziałającymi z nimi, której konsekwencją jest pozbawienie wolności, ryzyko pozbawienia wolności lub uszczerbek na zdrowiu innych osób,
   d) prowadzenie działalności o charakterze propagandowym na rzecz obcego państwa znajdującego się w stanie wojny z Danią lub okupującego jej terytorium, zwłaszcza jako wydawca, redaktor lub członek personelu administracyjnego gazety, periodyku, wydawnictwa lub biura prasowego pracującego na rzecz promocji obcych interesów,
   e) udzielanie znacznej pomocy finansowej w celu wspierania działalności propagandowej prowadzonej przez podmioty, o których mowa w pkt d), lub jakimkolwiek innym organizacjom bezprawnie współdziałającym z obcym państwem znajdującym się w stanie wojny z Danią lub okupującym jej terytorium;
7) niewypełnienie postanowień umowy dotyczącej środków podejmowanych przez organy państwa w celach związanych z działaniami zbrojnymi lub okupacją;
8) współpraca z obcym państwem znajdującym się w stanie wojny z Danią lub okupującym jej terytorium w celach handlowych, bezpośrednio lub przez pośrednika, oraz pełnienie funkcji kierowniczych w podmiotach gospodarczych tego państwa;
9) działania mające na celu skłonienie organu obcego państwa znajdującego się w stanie wojny z Danią lub okupującego jej terytorium do naruszenia niezależności jakiegokolwiek duńskiego organu lub czerpanie bezprawnych korzyści z jakichkolwiek powiązań z władzami okupacyjnymi lub ze związanymi z nimi organizacjami i osobami;
10) działanie sprzeczne z interesem państwa w ramach wykonywania czynności polegających na negocjacjach lub uzgodnieniach z rządem innego państwa;
11) udzielanie, na zlecenie obcego państwa, obcej organizacji lub zatrudnionych w tych strukturach osób, informacji, które z punktu widzenia interesów Danii powinny być zachowane w tajemnicy, niezależnie od tego, czy są prawdziwe, a także podejmowanie działań mających na celu uzyskanie takich informacji w celu opisanym powyżej (szpiegostwo);
12) udzielanie służbom wywiadowczym innego państwa – bezpośrednio lub pośrednio – jakiejkolwiek pomocy innej niż szpiegostwo, umożliwiającej lub ułatwiającej im prowadzenie działalności wywiadowczej na terytorium Danii;

13) ujawnienie informacji o niejawnych negocjacjach, uzgodnieniach lub rozmowach dotyczących interesów Danii w stosunkach z innymi państwami, jej praw względem tych państw lub dotyczących jej fundamentalnych interesów gospodarczych w stosunkach międzynarodowych;
14) sfałszowanie, zniszczenie lub usunięcie dokumentu lub innego instrumentu mającego istotne znaczenie dla bezpieczeństwa państwa lub jego praw względem innych państw;
15) opisywanie, fotografowanie lub charakteryzowanie w inny sposób wojskowych instalacji obronnych, oddziałów, uzbrojenia, składów zaopatrzenia, materiałów itp. niedostępnych publicznie oraz kopiowanie i publikowanie tego rodzaju informacji;
16) udział w operacjach mających na celu naruszenie neutralności Danii względem innego państwa na zlecenie innego państwa;
17) naruszenie przepisów lub zakazów dotyczących obronności lub neutralności państwa;
18) naruszenie przepisów lub zakazów w sferze zobowiązań prawnomiędzynarodowych wynikających z członkostwa w ONZ lub UE;
19) znieważenie innego państwa, narodu, flagi lub godła państwowego bądź też flagi lub symboli ONZ lub UE.

Rozdział 13 penalizuje następujące czyny określone jako przestępstwa przeciwko konstytucji lub naczelnym organom państwa:

1) prowadzenie działań zmierzających do zmiany konstytucji lub zmniejszenia jej funkcjonalności z pomocą obcego państwa, z użyciem siły lub pod groźbą jej użycia;
2) popełnienie czynu wymierzonego przeciwko życiu monarchy lub regenta konstytucyjnego;
3) naruszenie bezpieczeństwa lub niezależności parlamentu lub działania mające na celu zmuszenie parlamentu do określonego działania lub uniemożliwienie mu swobodnego realizowania swoich funkcji ustawowych, z użyciem siły lub pod groźbą jej użycia, a także ingerencja w działanie lub zastosowanie przymusu wobec monarchy, regenta konstytucyjnego, ministra, Sądu Konstytucyjnego lub Sądu Najwyższego;
4) popełnienie jednego z przestępstw wymienionych w § 114 ust. 1 pkt 1–7 (m.in. zabójstwo, bezprawne pozbawienie wolności, sprowadzenie zagrożenia ruchu drogowego), mających na celu poważne zastraszenie ludności, organów Danii lub innego państwa w celu zmuszenia ich do określonego działania lub zaniechania diałania, destabilizację podstawowych struktur politycznych, ustrojowych, finansowych lub społecznych organizacji międzynarodowej, które mogą wywołać poważną szkodę dla tego państwa lub organizacji międzynarodowej (terroryzm);
5) finansowanie terroryzmu;
6) udzielanie wsparcia finansowego lub innego rodzaju pomocy zorganizowanej grupie mającej na celu bezprawne wywieranie wpływu, przy użyciu przemocy, na organy administracji publicznej lub stworzenie zagrożenia bezpieczeństwa i porządku publicznego;
7) udział w nielegalnej organizacji zbrojnej;
8) działalność zmierzająca do proliferacji broni masowego rażenia, m.in. nieuprawniony eksport komponentów tego rodzaju broni, udzielanie uprawnionym organom nieprawdziwych informacji dotyczących towarów podwójnego zastosowania oraz ich wykorzystywanie w sposób niezgodny z decyzją uprawnionego organu;

9) utrudnianie właściwego przebiegu procesu wyborczego;
10) działalność zmierzająca do ograniczenia swobody działalności organów administracji publicznej przez wykorzystywanie obaw przed obcą interwencją zbrojną, prowadzona z użyciem przemocy lub pod groźbą jej użycia.

Z analizy praktycznych aspektów funkcjonowania PET wynika, że jej działalność ma charakter przede wszystkim prewencyjny. Głównym elementem aktywności służby jest pozyskiwanie informacji o osobach lub grupach pozostających w sferze zainteresowania PET oraz o sposobach i celach ich działalności[8]. Na podstawie zebranych informacji służba przygotowuje tzw. analizy ryzyka służące ocenie stopnia prawdopodobieństwa popełnienia określonego przestępstwa lub wystąpienia zagrożenia bezpieczeństwa państwa. Te działania polegają w głównej mierze na prowadzeniu obserwacji i czynności operacyjno-rozpoznawczych. W odróżnieniu od organów o charakterze stricte policyjnym działania PET koncentrują się na zapobieganiu przestępstwom.

FRANCJA

System ustrojowo-prawny Francji wyróżnia sześć służb specjalnych, które wraz z Narodowym Koordynatorem ds. Wywiadu i Akademią Wywiadu tworzą tzw. francuską wspólnotę wywiadowczą. To pojęcie zostało wprowadzone na podstawie aktu wykonawczego (dekretu) dodającego do ustawy – Kodeks obrony[9] art. D 1122-8-1 w następującym brzmieniu: *Służby wyspecjalizowane w zakresie wywiadu, wymienione w art. R. 811-1 ustawy kodeks bezpieczeństwa wewnętrznego*[10], *tworzą wraz z Narodowym Koordynatorem ds. Wywiadu i Akademią Wywiadu francuską wspólnotę wywiadowczą*.

Zgodnie z art. R. 811-1 kodeksu bezpieczeństwa wewnętrznego do tych służb zaliczają się następujące podmioty:
1) Generalna Dyrekcja Bezpieczeństwa Zewnętrznego;
2) Dyrekcja Bezpieczeństwa i Ochrony Sił Zbrojnych;
3) Dyrekcja Wywiadu Wojskowego;
4) Generalna Dyrekcja Bezpieczeństwa Wewnętrznego;
5) Narodowa Dyrekcja Wywiadu i Dochodzeń Celnych;
6) Służba Zwalczania Nielegalnego Obrotu Środkami Finansowymi (TRACFIN).

1. Generalna Dyrekcja Bezpieczeństwa Zewnętrznego (Direction Générale de la Sécurité Extérieure – DGSE)

DGSE została utworzona na podstawie dekretu nr 82-306 z 2 kwietnia 1982[11], dodającego do ustawy – Kodeks obrony art. art. D-3126.1–D. 3126-4 określające ramy formalnoprawne funkcjonowania służby i zakres jej właściwości.

---

[8] Informacja Ministerstwa Spraw Zagranicznych Danii o stopniu dostosowania duńskiego systemu prawnego do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z kwietnia 2006 r.

[9] *Code de la defense* [online], version consolidée au 11 février 2017, www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307 [dostęp:14 II 2017].

[10] *Code de la sécurité intérieure* [online], version en vigeur au 10 octobre 2016, www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000031240607&dateTexte+&categorieLien=cid [dostęp: 14 II 2017].

[11] *Décret No 82-306 du 2 avril 1982 portant création et fixant les attributions de la direction générale de la sécurité extérieure* [online], www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000517072 [dostęp: 14 II 2017].

Do zadań DGSE, zgodnie z art. 2 dekretu, należy zarówno zbieranie oraz wykorzystywanie informacji wywiadowczych istotnych z punktu widzenia bezpieczeństwa Francji, jak i wykrywanie oraz zapobieganie działalności szpiegowskiej poza granicami kraju, której celem jest wyrządzenie szkody interesom Francji, i przeciwdziałanie jej negatywnym skutkom. Służbą kieruje Dyrektor Generalny podlegający bezpośrednio Ministerstwu Obrony, mianowany na podstawie dekretu Rady Ministrów (art. 1 dekretu).

Do ustawowych obowiązków DGSE należy:

1) podejmowanie działań mających na celu ustanowienie niezbędnych kontaktów z innymi służbami lub organami;
2) wykonywanie, w ramach swojej kompetencji, wszystkich działań zleconych przez rząd;
3) dostarczanie analiz informacji wywiadowczych (dekret nie precyzuje, jakim konkretnie podmiotom mają być dostarczane tego rodzaju analizy).

Głównym elementem działalności służby jest niejawne pozyskiwanie informacji wywiadowczych poza granicami kraju. DGSE wykorzystuje wiele metod pozyskiwania tego rodzaju informacji, m.in. źródła osobowe, środki techniczne (przechwytywanie elektromagnetyczne i obrazowanie satelitarne), działania operacyjno-rozpoznawcze i wykorzystywanie źródeł otwartych. Charakterystycznym elementem dla francuskiego systemu prawnego jest wysoki stopień ogólności i niedookreśloności przepisów, tzw. ustaw kompetencyjnych, normujących zadania i metody działań poszczególnych służb, zarówno w przypadku DGSE, jak i pozostałych służb specjalnych. Szczegółowe unormowania dotyczące sposobów realizacji ich ustawowych zadań zostały zawarte w przyjętej w lipcu 2015 r. ustawie o wywiadzie, regulującej w sposób kompleksowy sposób prowadzenia czynności polegających na niejawnym pozyskiwaniu informacji przez organy zaliczane do grupy tzw. służb wyspecjalizowanych w zakresie wywiadu.

2. Generalna Dyrekcja Bezpieczeństwa Wewnętrznego (Direction Générale de la Sécurité Intérieure – DGSI)

DGSI, utworzona na mocy dekretu z 30 kwietnia 2014 r.[12], zastąpiła Centralną Dyrekcję Wywiadu Wewnętrznego. W aktualnym stanie prawnym ta służba jest jedyną służbą odpowiedzialną za bezpieczeństwo wewnętrzne państwa. Podlega ona bezpośrednio ministrowi spraw wewnętrznych.

DGSI odpowiada za pozyskiwanie, konsolidację i wykorzystywanie informacji istotnych z punktu widzenia bezpieczeństwa narodowego lub fundamentalnych interesów państwa. W zakresie swojej właściwości współpracuje z Policją na zasadach określonych w kodeksie postępowania karnego[13].

Do ustawowych obowiązków DGSI zgodnie z art. 2 dekretu zalicza się:

1) zapobieganie wszelkim formom ingerencji zewnętrznej w funkcjonowanie państwa oraz ich zwalczanie;
2) zapobieganie aktom terrorystycznym lub działaniom zagrażającym bezpieczeństwu państwa, integralności terytorialnej lub ciągłości działania instytucji Republiki oraz ich zwalczanie;

[12] *Décret No 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité* [online], intérieure,www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028887486&categorieLien=id [dostęp: 14 II 2017].

[13] *Code de procedure penale* [online] ww.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT0000006071154 [dostęp: 14 II 2017].

3) inwigilacja osób fizycznych lub grup inspirowanych ideologiami o charakterze radykalnym, w stosunku do których zachodzi podejrzenie, że mogą stosować przemoc i stwarzać zagrożenie bezpieczeństwa narodowego;
4) zapobieganie działaniom stanowiącym zagrożenie tajemnicy obrony narodowej, potencjału ekonomicznego, przemysłowego lub naukowego państwa i ich zwalczanie;
5) zapobieganie działaniom mającym na celu pozyskanie lub wytwarzanie broni masowego rażenia oraz ich zwalczanie;
6) zwalczanie międzynarodowych organizacji przestępczych, których działania mogą stanowić zagrożenie bezpieczeństwa narodowego oraz ich zwalczanie;
7) zapobieganie przestępstwom związanym z technologiami informatycznymi i komunikacyjnymi oraz ich zwalczanie.

Wyłącznie w celu realizacji powyższych obowiązków DGSI może wykorzystywać instrumenty służące inwigilacji komunikacji elektronicznej i radioelektronicznej.

Wszystkie organy odpowiedzialne za zapewnianie bezpieczeństwa państwa przekazują niezwłocznie DGSI informacje, które mogą mieć znaczenie dla realizacji zadań służby opisanych w art. 2. Artykuł 3 *in fine* dekretu wprowadza właściwość konkurencyjną DGSI we wszystkich sprawach związanych z ochroną bezpieczeństwa państwa, stanowiąc, że w przypadku gdy inny organ, działający z upoważnienia prefekta Policji, wykonuje zadania związane z wywiadem wewnętrznym, DGSI może działać wspólnie z tym organem lub przejąć określoną sprawę lub jej część.

W skład służby, o której mowa, wchodzą centrala oraz terenowe jednostki organizacyjne podlegające wyłącznie Dyrektorowi Generalnemu. Szefowie terenowych jednostek organizacyjnych informują właściwych przedstawicieli władz centralnych w poszczególnych regionach o działaniach podejmowanych przez służbę.

DGSI, zgodnie ze swoimi właściwościami, zapewnia stworzenie niezbędnych instrumentów komunikacji z innymi służbami i organami, zarówno francuskimi, jak i zagranicznymi. Ustanawia w tym celu oficerów łącznikowych.

Charakterystycznym elementem systemu współpracy międzynarodowej jest brak ustawowego wymogu uzyskania zgody organu nadzorującego (ministra spraw wewnętrznych) na możliwość podjęcia współpracy z zagranicznymi służbami partnerskimi. Należy zauważyć, że zakres kompetencji DGSI w sferze współpracy międzynarodowej został uregulowany znacznie szerzej, niż ma to miejsce w przypadku ABW. Artykuł 8 ustawy o ABW oraz AW[14] uzależnia bowiem możliwość podjęcia współpracy międzynarodowej z innymi służbami od uzyskania zgody Prezesa Rady Ministrów. Należy zwrócić uwagę na to, że polski ustawodawca nie przewidział expressis verbis możliwości nawiązania współpracy z podmiotami innymi niż służby zagraniczne (np. organizacjami międzynarodowymi).

Biorąc pod uwagę ewolucję specyfiki zagrożeń bezpieczeństwa wewnętrznego państwa, głównym założeniem prac nad utworzeniem służby było połączenie elementów służby wywiadowczej z organem dochodzeniowo-śledczym, co w rezultacie miało doprowadzić do stworzenia instytucji zdolnej do prowadzenia kompleksowych, dwutorowych działań, zarówno w sferze wywiadowczej, jak i postępowania karnego. DGSI jest jedyną służbą upoważnioną do prowadzenia postępowań przygotowawczych w sprawach o szpiegostwo, bezprawne ujawnienie informacji niejawnych, ataki na System Automatycznego Przetwarzania Danych (*système de traitement automatisé de*

[14] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity: DzU z 2016 r. poz. 1897, ze zm.) – przyp. red.

données – STAD), ataki wymierzone w sieci teleinformatyczne użytkowane przez organy administracji rządowej oraz przez najważniejszych operatorów sieci komunikacyjnych (O.I.V), a także w sprawach dotyczących działań podejmowanych przeciwko urządzeniom znajdującym się w tzw. strefach ograniczonego dostępu (Z.R.R). Od 2011 r., zgodnie z *Ustawą o założeniach i planowaniu w zakresie bezpieczeństwa wewnętrznego*[15], służba jako jedyna jest upoważniona do przeciwdziałania proliferacji broni masowego rażenia.

3. Dyrekcja Wywiadu Wojskowego (Direction du Renseignement Militaire – DRM)

Brak spójności i skuteczności działań wywiadowczych podczas konfliktu w Zatoce Perskiej w 1991 r. stał się katalizatorem reformy struktury wywiadu wojskowego. Jej założeniem było stworzenie systemu gwarantującego dostarczanie władzom politycznym i siłom zbrojnym informacji pozwalających tym podmiotom na dokonywanie niezależnych od siebie ocen sytuacji w odniesieniu do międzynarodowych konfliktów zbrojnych i spraw związanych ze sferą wojskową, zarówno w wymiarze wewnętrznym, jak i zewnętrznym.

DRM została utworzona na podstawie dekretu z 16 czerwca 1992 r.[16] Fundamentalnym zadaniem służby jest dostarczanie informacji o zagrożeniach strategicznych najważniejszym organom cywilnym i wojskowym w celu wsparcia procesu decyzyjnego. Dychotomiczny charakter obowiązków informacyjnych służby wynika z art. 1 i 2 wspomnianego dekretu: art. 1 zobowiązuje dyrektora DRM do udzielania wsparcia i doradzania ministrowi przez dostarczanie mu informacji wywiadowczych, niezbędnych do wypełniania jego zadań. Z drugiej strony ta jednostka podlega szefowi Sztabu i jest obowiązana do przekazywania mu informacji wywiadowczych istotnych z punktu widzenia sił zbrojnych.

Dekret nakłada na DRM obowiązki związane z planowaniem i realizacją działań dotyczących wywiadu wojskowego. Służba odgrywa tu rolę podmiotu inicjującego działania w określonych obszarach i koordynującego współpracę innych organów.

Podczas realizacji funkcji ustawowych DRM wykorzystuje następujące instrumenty:

1) urządzenia techniczne pozwalające na rejestrowanie obrazu i dźwięku zdarzeń dotyczących aktywności osób oraz zachodzących w przestrzeni powietrznej, morskiej, kosmicznej i cybernetycznej;
2) analizę, weryfikację i przekazywanie pozyskanych informacji właściwym organom.

4. Dyrekcja Ochrony i Bezpieczeństwa Sił Zbrojnych (Direction de la Protection et de la Sécurité de la Défense – DPSD)

DPSD to organ odpowiedzialny za prowadzenie kompleksowych działań mających na celu przeciwdziałanie nieuprawnionej ingerencji w funkcjonowanie sił zbrojnych. Ta służba jest zaangażowana m.in. w zapobieganie i przeciwdziałanie aktom o charakterze terrorystycznym wymierzonym we francuskie siły zbrojne, ochronę interesów ekonomicznych Francji przez weryfikację prawidłowości działania podmiotów funkcjonują-

[15] *Loi N° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure* [online], www. legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id [dostęp: 14 II 2017].

[16] *Décret no 92-523 du 16 juin 1992 portant creation de la direction du renseignement militaire* [online], www. legifrance.gouv.ffsr/affichTexte.do?cidTexte=JORFTEXT000000357733&categorieLien=id [dostęp: 14 II 2017].

cych w sektorze obrony narodowej, np. przedsiębiorstw zbrojeniowych, czy zapewnienie bezpieczeństwa cybernetycznego armii.

Kompetencje i sposób funkcjonowania DPSD zostały uregulowane we wspomnianej już ustawie – Kodeks obrony (art. D 3126-5–D 3126-9). DPSD, zgodnie z art. D 3126-5, jest służbą wywiadowczą podległą ministrowi obrony, realizującą zadania w następujących zakresach:

1) bezpieczeństwo osobowe;
2) bezpieczeństwo informacji;
3) bezpieczeństwo materiałowe;
4) bezpieczeństwo obiektów i instalacji wrażliwych.

Zgodnie z art. D3126-6 kodeksu obrony DPSD pełni funkcję organu wspierającego w stosunku do nadrzędnych organów sił zbrojnych i innych jednostek organizacyjnych sił zbrojnych. W tym celu wykonuje następujące zadania:

1) bierze udział w opracowaniu i kontroli prawidłowości stosowania instrumentów ochrony i bezpieczeństwa sił zbrojnych;
2) zajmuje się wykrywaniem zamachów na obronność państwa w rozumieniu kodeksu postępowania karnego i kodeksu sprawiedliwości wojskowej, zwłaszcza przez stosowanie instrumentów zapobiegających nieuprawnionej ingerencji w celu przeciwdziałania wszystkim zagrożeniom, które mogą przybrać formę terroryzmu, szpiegostwa, dywersji, sabotażu lub przestępczości zorganizowanej;
3) bierze udział w zapewnianiu ochrony osobom, które mogą mieć dostęp do informacji niejawnych lub do stref, materiałów oraz instalacji zaklasyfikowanych jako wrażliwe. Prowadzi zwłaszcza postępowania sprawdzające na podstawie ustawy – Kodeks obrony;
4) bierze udział w badaniu poziomu bezpieczeństwa i w sporządzaniu zaleceń dotyczących sposobu przetwarzania informacji, szczególnie w zakresie automatycznego przetwarzania oraz kontroluje prawidłowość stosowania środków bezpieczeństwa.

DPSD uczestniczy także w opracowywaniu instrumentów niezbędnych do zapewnienia bezpieczeństwa personelu wojskowego, informacji, materiałów i instalacji wrażliwych istotnych z punktu widzenia obronności oraz weryfikuje prawidłowość ich stosowania przez następujące podmioty:

1) siły zbrojne, sztaby generalne rodzajów sił zbrojnych, dyrekcje i służby podlegające Ministerstwu Obrony oraz jednostki im podległe;
2) przedsiębiorstwa będące wykonawcami usług mających istotne znaczenie dla obronności lub podwykonawców działających na ich rzecz, których działalność wymaga przedsięwzięcia szczególnych środków bezpieczeństwa, zwłaszcza w sytuacji, gdy ci wykonawcy mogą przechowywać informacje niejawne;
3) przedsiębiorstwa związane z Ministerstwem Obrony, których działalność uzasadnia przedsięwzięcie szczególnych środków ostrożności, zwłaszcza wprowadzenie stref ograniczonego dostępu;
4) obiekty o szczególnym znaczeniu, które w celach bezpieczeństwa zostały oddane pod nadzór Ministerstwa Obrony, oraz wszystkie obiekty, w których są przechowywane przedmioty mające istotne znaczenie z punktu widzenia naukowego i technologicznego, oraz obiekty podlegające Ministerstwu Obrony.

5. Narodowa Dyrekcja Wywiadu i Dochodzeń Celnych (Direction Nationale du Renseignement et des Enquêtes Douanières – DNRED)

DNRED jest jednostką działającą w ramach Generalnej Dyrekcji Ceł i Podatków Pośrednich w Ministerstwie Finansów, utworzoną na podstawie zarządzenia z 1 marca 1998 r.[17] W ujęciu ogólnym można wyróżnić trzy zasadnicze kierunki działalności tego podmiotu:

1) zwalczanie wielkoskalowej działalności przemytniczej;
2) prowadzenie postępowań przygotowawczych dotyczących oszustw i defraudacji środków finansowych mających zasięg zarówno krajowy, jak i międzynarodowy;
3) pozyskiwanie, analiza i przekazywanie właściwym organom i służbom partnerskim informacji wywiadowczych dotyczących przestępczości celnej i finansowej.

Misją DNRED jest zwalczanie przemytu przez identyfikację i neutralizację zorganizowanych grup przestępczych, które zajmują się nielegalnym obrotem bronią, środkami odurzającymi, tytoniem i produktami oznaczonymi w sposób nieuprawniony znakami lub symbolami firmowymi innego wytwórcy.

W celu realizacji wymienionych zadań służba wykorzystuje instrumenty analityczne pozwalające na dokładne zbadanie struktury przepływów środków finansowych oraz dóbr i osób, instrumenty operacyjne pozwalające na niejawne pozyskiwanie informacji, a także instrumenty dochodzeniowo-śledcze.

W skład DNRED wchodzi:

1) Centrala (rola administracyjno-koordynacyjna);
2) Dyrekcja Wywiadu i Dokumentacji;
3) Dyrekcja Dochodzeń Celnych.

Dyrekcja Wywiadu i Dokumentacji, zgodnie z art. 2B dekretu, zdobywa i gromadzi informacje dotyczące oszustw finansowych oraz je weryfikuje, tak aby mogły je wykorzystać inne organy i służby. Dyrekcja dokonuje prospektywnej analizy informacji dostarczanych przez źródła osobowe w celu identyfikacji potencjalnych zagrożeń wystąpienia oszustwa lub defraudacji.

Ponadto jednostka przekazuje komórkom terenowym informacje pomocne w ukierunkowaniu ich działań wobec podmiotów najbardziej narażonych na ryzyko wystąpienia zjawisk niepożądanych, zgodnie z dyrektywami wydawanymi przez Dyrektora Generalnego. Dyrekcja prowadzi też bazy danych zawierające informacje o przestępstwach wchodzących w zakres jej właściwości w celu ich ewentualnego wykorzystania na etapie postępowania karnego.

Zadaniem Dyrekcji Dochodzeń Celnych jest prowadzenie postępowań przygotowawczych, kontrola wszelkich dokumentów, które mogą mieć istotne znaczenie dla realizacji jej ustawowych zadań, oraz wykrywanie i badanie naruszenia obowiązków wynikających z krajowych i międzynarodowych przepisów dotyczących uiszczania należności celnych.

6. Służba Zwalczania Nielegalnego Obrotu Środkami Finansowymi (Traitement du renseignement et action contre les circuits financiers clandestins – TRACFIN)

TRACFIN to jednostka wywiadu finansowego utworzona na podstawie dekretu z 9 maja 1990 r.[18] wchodząca w skład Ministerstwa Finansów. Do głównych zadań tej służby na-

[17] *L'arrêté du 1 mars 1988 portant creation de la direction nationale du renseignement et des enquêtes douanières et réorganisation du service des autorisations financierès et commerciales* [online], www.legifrance.gouv.fr.affichTexte.do?cidTexte=JORFTEXT000000296758 [dostęp: 14 II 2017].

[18] *Décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du rensei-*

leży: zwalczanie nielegalnego przepływu środków finansowych, prania pieniędzy i finansowania terroryzmu. Działalność TRACFIN polega na zbieraniu, analizowaniu oraz wykorzystywaniu informacji wywiadowczych pochodzących od osób odpowiedzialnych za przeciwdziałanie praniu pieniędzy, zatrudnionych m.in. w instytucjach finansowych, kredytowych i innych, w celu odtworzenia przebiegu określonej transakcji. Ponadto służba jest uprawniona do sporządzania analiz operacyjnych i strategicznych oraz prowadzenia szkoleń dla osób, które – zgodnie z kodeksem finansowym i pieniężnym – wykonują zadania związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu.

Szczegółowy zakres kompetencji TRACFIN został zawarty w art. 2 tworzącego go dekretu. Zgodnie z nim do zadań służby należy:

1) zbieranie, przetwarzanie i przekazywanie właściwym podmiotom informacji dotyczących nielegalnych przepływów środków finansowych i prania pieniędzy;
2) inicjowanie i koordynowanie działań dochodzeniowo-śledczych prowadzonych przez inne organy, zarówno na poziomie krajowym, jak i międzynarodowym, mających na celu wykrywanie sprawców przestępstw celnych lub podatkowych związanych z nielegalnymi przepływami środków finansowych lub z praniem pieniędzy;
3) współpraca z ministerstwami, podmiotami narodowymi i międzynarodowymi w celu wypracowania efektywnych metod zwalczania nielegalnych przepływów środków finansowych lub prania pieniędzy;
4) reprezentowanie pozostałych organów i służb zwalczających przestępstwa finansowe na poziomie krajowym i międzynarodowym.

Informacje wywiadowcze, które zostały zebrane przez TRACFIN, mogą być przekazane w sposób czyniący zadość wymogom wynikającym z odrębnych przepisów organom wymiaru sprawiedliwości, organom administracji publicznej i właściwym władzom innego państwa, z wyjątkiem sytuacji, w której te informacje podlegają szczególnej ochronie jako tajemnica obrony narodowej.

HISZPANIA

1. Narodowe Centrum Wywiadowcze (Centro National de Inteligencia – CNI)[19]

Narodowe Centrum Wywiadowcze jest odpowiedzialne za dostarczanie premierowi oraz rządowi Hiszpanii informacji, analiz, raportów lub rozwiązań, które umożliwiają zapobieganie niebezpieczeństwom oraz groźbom agresji kierowanym przeciwko niepodległości i integralności terytorialnej Hiszpanii, jej interesom narodowym, stabilności instytucji państwowych oraz praworządności.

Warto zaznaczyć, że CNI ma uprawnienia, które w innych państwach pozostają we właściwości dwóch lub więcej służb wywiadowczych. Powyższe pozwala na wszechstronną koordynację i wymianę informacji w obszarach, które są wzajemnie komplementarne, przy jednoczesnej optymalizacji źródeł.

Podstawową zasadą funkcjonowania CNI jest koordynowanie współpracy z innymi państwowymi służbami informacyjnymi. Koordynowanie zadań jest sprawowane

gnement et de l'action contre les circuits financiers clandestins (TRACFIN) [online], www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT0000007149&dateTexte= [dostęp: 14 II 2017].

[19] Ang. National Intelligence Centre.

przez Rządową Komisję Delegatów do Spraw Wywiadowczych (ang. Government Delegate Commission for Intelligence Affairs), na której czele stoi wiceprezes Rady Ministrów mianowany przez Prezesa Rady Ministrów. Komisja monitoruje właściwą koordynację wszelkich informacji państwowych i służb wywiadowczych tworzących wspólnotę wywiadowczą.

CNI jest odpowiedzialne również za ochronę informacji niejawnych oraz pełni funkcję krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych (ang. National Security Authority for the Protection of Classified Information). W celu wykonywania powyższych zadań sekretarza stanu – dyrektora CNI wspomaga Narodowe Biuro Bezpieczeństwa (ang. National Security Office) działające jako podmiot wykonawczy.

Najważniejszymi zadaniami należącymi do Narodowego Biura Bezpieczeństwa jest zawieranie umów międzynarodowych o ochronie informacji niejawnych z innymi państwami oraz organizacjami międzynarodowymi, a także uczestnictwo w komitetach i grupach roboczych – zarówno w strukturach UE, jak i NATO. Biuro odpowiada także za wydawanie poświadczeń bezpieczeństwa i świadectw bezpieczeństwa przemysłowego.

Struktura CNI została określona w następujących dekretach królewskich: 436/2002 z 10 maja 2002 r.[20] i 612/2006 z 19 maja 2006 r.[21] W skład CNI wchodzą: Kierownictwo, Sekretariat Generalny i trzy dyrektoriaty.

Kierownictwo – dyrektor CNI w randze sekretarza stanu, mianowany na podstawie dekretu królewskiego.

Sekretariat Generalny – sekretarz generalny powinien mieć rangę podsekretarza stanu i jest mianowany na podstawie dekretu królewskiego. Sekretarz generalny zastępuje sekretarza stanu – dyrektora CNI w przypadku absencji, wakatu lub choroby sekretarza stanu.

Dyrektoriaty – kierujące nimi osoby mają rangę dyrektorów generalnych i podlegają bezpośrednio sekretarzowi generalnemu. Dyrektor generalny jest odpowiedzialny za sprawy wywiadowcze, wspieranie wywiadu i źródła.

Organy wspierające sekretarza stanu – dyrektora CNI – jednostki podległe sekretarzowi generalnemu-dyrektorowi i Departament Prawny.

Część struktur CNI działa poza główną siedzibą służby – CNI jest obecne w państwach, z którymi Hiszpanię łączą gospodarcze i polityczne interesy, lub które są istotne z uwagi na bezpieczeństwo Hiszpanii.

Czynności podejmowane przez CNI, organizacja służby, struktura wewnętrzna, źródła, procedury, informacje o personelu, wyposażeniu, bazach danych, źródłach informacji i o informacjach lub danych, które mogą prowadzić do zdobycia wiedzy o powyższym, są oznaczone jako informacje niejawne o klauzuli „ściśle tajne" lub najwyższym poziomem niejawności, zgodnie z ustawą regulującą tajemnice służbowe oraz zgodnie z umowami międzynarodowymi[22].

---

[20] *Royal Decree 436/2002 of 10th May 2002* [online], www.cni.es/en/structure/ [dostęp: 10 II 2017]; *Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia* [online], https://www.boe.es/buscar/pdf/2002/BOE-A-2002-9161-consolidato.pdf.

[21] *Royal Decree 612/2006 of 19th May 2006* [online], www.cni.es/en/structure/ [dostęp: 10 II 2017]; *Real Decreto 612/2006, de 19 de mayo, de modificación del Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia* [online], https://www.boe.es/boe/dias/2006/05/pdfs/A199453-19453.pdf.

[22] Zob. *Act 11/2002 of 6th May regulating the Centro National de Inteligencia (National Intelligence Centre)* [online], https://www.cni.es/comun/recursos/descargas/11-2002-INGLES.pdf [dostęp: 10 II 2017]. Także: www.cni.es/en/Rules_and_regulations/ [dostęp: 10 II 2017].

Uprawnienie do wyznaczania zadań CNI przysługuje rządowi, który określa cele informacyjne w corocznej „dyrektywie wywiadowczej".

Zdobyta przez CNI informacja podlega procedurze ewaluacji i analizy, aby można było określić, czy jest ona wiarygodna i warta zainteresowania i zgodna z celami wyznaczonymi przez rząd. Uzyskane dane są gromadzone i przetwarzane, a powstały produkt finalny, zwany produktem wywiadowczym, ma wspomóc decydentów przy podejmowaniu decyzji.

Analizy sporządzone na podstawie informacji zebranych przez CNI są przekazywane premierowi i ministrom. Ministrowie zwykle otrzymują raporty od CNI oraz od Ministerstwa Spraw Zagranicznych i Współpracy, Ministerstwa Obrony i Ministerstwa Spraw Wewnętrznych. CNI ponadto przekazuje swoje raporty do innych departamentów administracji państwowej.

Jeśli CNI zgromadzi informacje o jakimkolwiek fakcie, który wymagałby natychmiastowych działań albo stanowił przestępstwo, przekazuje te dane – w zależności od natury zagadnienia – rządowi, aby wesprzeć proces decyzyjny, lub organom bezpieczeństwa i ochrony porządku publicznego, które podejmują właściwe czynności.

Funkcjonariusze CNI nie są w świetle prawa funkcjonariuszami organów bezpieczeństwa i ochrony porządku publicznego, z wyjątkiem tych, których zawodowa aktywność jest powiązana z ochroną personelu lub sprzętu.

CNI jest organem wspierającym proces decyzyjny; jego misja kończy się wtedy, gdy zaczyna się proces decyzyjny, za który odpowiadają inne organy. CNI nie jest odpowiedzialne za działania podjęte na podstawie jego raportów[23].

2. Ustawa 11/2002 regulująca funkcjonowanie Narodowego Centrum Wywiadowczego[24]

Z preambuły do ustawy wynika, że Narodowe Centrum Wywiadowcze ma status specjalnej instytucji publicznej. Jest to spowodowane tym, że CNI cechuje się niezbędną autonomią w funkcjonowaniu, służącą odpowiedniej realizacji nałożonych na nie zadań. Powyższy status wiąże się przede wszystkim ze szczególnymi zasadami dotyczącymi zatrudnienia w tej służbie, personelu i budżetu.

Ustawa upoważnia rząd do zatwierdzenia jednostkowego, jednolitego statutu dla całego personelu służącego w CNI. Personel ten powinien być poddany innym regulacjom prawnym, uwzględniającym jego status oraz relację z pozostałą częścią administracji rządowej.

Głównym zadaniem ustawowym CNI jest zapewnienie rządowi Hiszpanii informacji wywiadowczych niezbędnych do uniknięcia jakiegokolwiek ryzyka lub groźby, która mogłaby zagrozić niepodległości i integralności kraju, interesom narodowym oraz stabilności instytucji państwowych, a także praworządności.

CNI znajduje się w strukturze Ministerstwa Obrony. Podczas wykonywania swoich zadań współpracuje również z pozostałymi hiszpańskimi służbami informacyjnymi. W skład Rządowej Komisji Delegatów do Spraw Wywiadowczych (spra-

[23] www.cni.es/en/howdoesthecniwork/ [dostęp: 10 II 2017].

[24] *Act 11/2002 of 6th May regulating the Centro National de Inteligencia (National Intelligence Centre)* [online], https://www.cni.es/comun/recursos/descargas/11-2002-INGLES.pdf. Nazwa oryginalna dokumentu: *Ley 11/2002, de 6 de mayo regulatora del CNI* [online], https://www.cni.es/comun/recursos/descargas//Ley_11-2002_de_6_de_mayo_pdf [dostęp: 10 II 2017].

wującej kontrolę nad służbami) wchodzą: jako przewodniczący – wiceprezes Rady Ministrów, wyznaczony przez Prezesa Rady Ministrów, oraz minister spraw zagranicznych, minister obrony, minister spraw wewnętrznych, minister finansów, sekretarz generalny Biura Prezesa Rady Ministrów, sekretarz stanu ds. bezpieczeństwa oraz sekretarz stanu – dyrektor CNI.

Warto zaznaczyć, że ustawa przewiduje nadzór parlamentarny nad działaniami CNI. Niniejszy akt prawny, z uwzględnieniem autonomii parlamentarnej, ustanawia komisję, która kontroluje wykorzystanie funduszy niejawnych. Kontrola sądowa działań CNI jest uregulowana w oddzielnym akcie prawnym będącym uzupełnieniem ustawy pragmatycznej.

W omawianej ustawie wskazuje się na podległość zadań realizowanych przez CNI systemowi prawnemu Hiszpanii oraz na zasadę prowadzenia wszelkich czynności w zakresie przyznanych kompetencji, które są wyraźnie określone w tej ustawie i w ustawie o kontroli sądowej CNI. W ustawie potwierdzono również to, że CNI, wykonując swoje zadania, podlega zarówno kontroli parlamentarnej, jak i sądowej.

CNI w swoich działaniach powinno, co do zasady, realizować cele wywiadowcze ustalone przez rząd Hiszpanii, który jest zobowiązany corocznie je określić i zatwierdzić, zgodnie z „dyrektywą wywiadowczą" oznaczoną klauzulą „ściśle tajne"[25].

Funkcje CNI są realizowane zgodnie z zadaniami wyznaczonymi przez rząd i polegają na:

1) gromadzeniu, ocenie oraz interpretacji wiadomości i przekazaniu jej właściwym organom w celu ochrony i wspierania politycznych, gospodarczych, przemysłowych i handlowych interesów strategicznych Hiszpanii – wewnątrz i poza granicami państwa;
2) zapobieganiu, wykrywaniu i zapewnianiu neutralizacji działań prowadzonych przez jakiekolwiek służby obcych państw, grupę lub osobę powodującą zagrożenie atakiem na porządek konstytucyjny, prawa i wolności obywateli hiszpańskich, suwerenność, integralność i bezpieczeństwo państwa, stabilność jego instytucji, narodowe interesy gospodarcze, a także dobrobyt społeczeństwa;
3) wspieraniu współpracy ze służbami wywiadowczymi innych państw lub organizacjami międzynarodowymi w celu skutecznej realizacji swoich celów;
4) uzyskiwaniu, ewaluacji i interpretacji danych o ruchu sygnałów o znaczeniu strategicznym, w celu realizacji zadań wywiadowczych wyznaczonych służbie;
5) koordynowaniu czynności instytucji rządowych związanych ze stosowaniem szyfrowanych środków łączności lub procedur, w celu zagwarantowania bezpieczeństwa informacji; raportowaniu o zbiorach materiałów kryptologicznych, szkoleniu w przedmiotowym zakresie ekspertów, zarówno własnych, jak i z innych instytucji rządowych, w celu właściwego wykonywania zadań zgodnie z kompetencjami służby;
6) monitorowaniu zgodności działań z regulacjami dotyczącymi ochrony informacji niejawnych;
7) zapewnieniu bezpieczeństwa i ochrony własnych obiektów oraz urządzeń, informacji, materiałów, a także personelu.

[25] www.cni.es/en/Rules_and_regulations/ [dostęp: 10 II 2017].

HOLANDIA

Holenderski model służb specjalnych został uregulowany na podstawie ustawy o służbach wywiadowczych i bezpieczeństwa z 2002 r., powołującej dwie służby: cywilną – Generalną Służbę Bezpieczeństwa i Wywiadu (Algemeene Inlichtingen- en Veiligheidsdienst – AIVD) oraz wojskową – Agencję Wywiadu Obronnego (Militaire Inlichtingen- en Veiligheidsdienst – MIVD)[26]. Ustawa przewiduje powołanie instytucji koordynatora nadzorującego działania służb pełniącego funkcję sekretarza generalnego w Ministerstwie ds. Ogólnych (Ministry of General Affairs). Oprócz wymienionych służb holenderski system prawny przewiduje istnienie regionalnych organów wywiadowczych wchodzących w skład Policji.

Zadania koordynatora zostały wyszczególnione w art. 4 ustawy, zgodnie z którym jest on powoływany na podstawie dekretu królewskiego na wspólny wniosek premiera i ministra ds. ogólnych. Należą do nich: przygotowywanie konsultacji pomiędzy właściwymi ministrami, w których toku są poruszane najważniejsze z punktu widzenia funkcjonowania służb kwestie (ministrowie spraw wewnętrznych, obrony i spraw ogólnych), koordynacja wymiany informacji pomiędzy służbami, nadzór nad sposobem realizacji ustawowych zadań służb oraz informowanie ministrów o wszystkich sprawach, które mogą mieć istotne znaczenie dla bezpieczeństwa państwa.

Zakres właściwości AIVD został określony w art. 6 ustawy, zgodnie z którym ta służba realizuje, w interesie ochrony bezpieczeństwa narodowego, następujące zadania:

1) pozyskiwanie informacji dotyczących osób i podmiotów w związku z zagrożeniem ustroju demokratycznego, bezpieczeństwa lub innych fundamentalnych interesów państwa, powodowanym przez cele oraz charakter działalności tych osób lub podmiotów;
2) prowadzenie postępowań sprawdzających w rozumieniu ustawy o ochronie informacji niejawnych;
3) wspieranie prawidłowego funkcjonowania środków bezpieczeństwa, m.in. dotyczących ochrony informacji niejawnych oraz informacji na temat organów lub podmiotów gospodarczych, które, w opinii właściwych ministrów, mają zasadnicze znaczenie dla państwa;
4) pozyskiwanie informacji dotyczących innych państw, osób lub podmiotów wskazanych przez premiera lub ministra ds. ogólnych, w porozumieniu z właściwymi ministrami;
5) sporządzanie analiz ryzyka i ocen zagrożeń na wspólny wniosek ministra spraw wewnętrznych i ministra sprawiedliwości w celu ochrony określonych kategorii osób wskazanych w ustawie o policji.

Zadania MIVD realizowane w sferze wojskowej zostały określone w analogiczny sposób:

1) pozyskiwanie informacji dotyczących potencjału wojskowego innych państw w celu osiągnięcia równowagi między poszczególnymi komponentami sił zbrojnych i zapewnienia ich efektywnego wykorzystania;
2) pozyskiwanie informacji dotyczących spraw, które mogą mieć istotne znaczenie dla porządku międzynarodowego, jeżeli mogą się one wiązać z wykorzystaniem sił zbrojnych;

[26] *Intelligence and Security Services Act* (Wiv 2002), 29 May 2002 [online], https://english.aivd.nl/about-aivd/publications/2002/03/26/bulletin-of-acts-orders-and-decrees-of-the-kingdom-of-the-netherlands [dostęp: 14 II 2017].

3) prowadzenie postępowań sprawdzających w rozumieniu ustawy o ochronie informacji niejawnych;
4) gromadzenie informacji mających na celu zapobieżenie zdarzeniom negatywnie wpływającym na bezpieczeństwo lub gotowość bojową, zdolności organizacyjne i mobilizacyjne sił zbrojnych;
5) wspieranie prawidłowego funkcjonowania środków bezpieczeństwa, m.in. w zakresie ochrony informacji niejawnych w sferze wojskowej;
6) sporządzanie analiz ryzyka i ocen zagrożeń na wspólny wniosek ministra spraw wewnętrznych i ministra sprawiedliwości, w celu ochrony osób wskazanych w ustawie o policji (…).

Podkreślenia wymaga to, że art. 9 ustawy expressis verbis wyłącza możliwość prowadzenia przez ww. służby czynności dochodzeniowo-śledczych, co sprawia, iż zarówno AIVD, jak i MIVD są organami zorientowanymi na prowadzenie działań i analityczno-informacyjnych, i operacyjno-rozpoznawczych.

1. Przetwarzanie danych osobowych

Ustawa nakłada na służby daleko idące ograniczenia w zakresach możliwości przetwarzania informacji oraz dopuszczalności przetwarzania przez nie danych osobowych. Na uwagę zasługuje rozróżnienie między informacjami a danymi osobowymi, wynikające z art. 1 ustawy, zawierającego definicje legalnych pojęć w niej używanych. Zakres przedmiotowy pojęcia i n f o r m a c j e został skonstruowany w sposób szeroki – pod tym pojęciem ustawa rozumie dane osobowe oraz inne informacje. D a n e o s o b o w e w rozumieniu ustawy oznaczają natomiast informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Przetwarzanie informacji, zgodnie z art. 1 pkt f ustawy, oznacza jakiekolwiek działanie dotyczące informacji, polegające zarówno na zbieraniu, utrwalaniu, dostosowywaniu, przechowywaniu, aktualizowaniu, zmianie, poszukiwaniu lub korzystaniu z informacji, jak i na ich rozpowszechnianiu, udostępnianiu, poszukiwaniu między nimi powiązań, ich ochronie, wymianie lub niszczeniu.

Art. 13 ustawy zawiera wykaz przesłanek uprawniających AIVD do przetwarzania danych osobowych. Przetwarzane przez tę służbę dane osobowe mogą dotyczyć następujących kategorii osób:

1) osób, w stosunku do których zachodzi uzasadnione podejrzenie, że stanowią zagrożenie demokratycznego państwa prawnego, bezpieczeństwa lub innych fundamentalnych interesów państwa;
2) osób, które wyraziły zgodę na przetwarzanie swoich danych osobowych w celu przeprowadzenia postępowania sprawdzającego;
3) osób, których dane muszą być przetworzone w związku z czynnościami prowadzonymi przez służby, dotyczącymi innych państw;
4) osób, których dane uzyskały inne służby wywiadowcze lub służby bezpieczeństwa;
5) osób, których dane są niezbędne do zapewnienia prawidłowej realizacji ustawowych zadań służb;
6) osób, które były funkcjonariuszami służb w przeszłości lub które aktualnie pełnią w nich służbę;
7) osób, których dane muszą być przetworzone w związku z realizacją czynności związanych ze sporządzaniem analiz ryzyka oraz analiz zagrożeń bezpieczeństwa państwa.

Możliwość przetwarzania danych przez MIVD została uregulowana w sposób analogiczny.

Opisane powyżej zasady przetwarzania danych osobowych przez służbę mają również zastosowanie w odniesieniu do procesu przetwarzania tych danych przez funkcjonariuszy lub pracowników innych służb wykonujących określone czynności na zlecenie AIVD. Przetwarzanie przez ww. osoby danych osobowych na zlecenie AIVD jest ściśle oddzielony od przetwarzania przez nie tego rodzaju danych w toku realizacji innych zadań, wykonywanych niezależnie od współpracy z AIVD. Szef AIVD może wydawać w tym zakresie dalsze, bardziej szczegółowe instrukcje.

Szefowie służb realizują ponadto następujące czynności:

1) zapewniają poufność przetwarzanych informacji;
2) odpowiadają za zachowanie w tajemnicy tożsamości źródeł informacji;
3) odpowiadają za bezpieczeństwo osób współpracujących w toku pozyskiwania informacji przez służby;
4) ustanawiają zasady przetwarzania informacji mające stworzyć gwarancje ich poprawności i kompletności;
5) wprowadzają przepisy o charakterze organizacyjnym i technicznym w celu ochrony przed utratą informacji, naruszeniem ich integralności oraz przed ich nieuprawnionym przetwarzaniem;
6) wyznaczają osobę mającą wyłączne kompetencje co do określonych aspektów przetwarzania informacji.

2. Pozyskiwanie informacji

Podczas realizacji ustawowych zadań lub w celu usprawnienia sposobu ich wykonywania służby są uprawnione do zwracania się o udzielenie określonych informacji do następujących podmiotów:

1) organów administracji publicznej, osób zatrudnionych w podmiotach publicznych lub jakichkolwiek innych osób;
2) osób odpowiedzialnych za przetwarzanie określonych informacji.

Opisany powyżej sposób pozyskiwania danych można określić jako zwyczajny, oparty na współpracy z innymi podmiotami działającymi w sferze publicznej, zatrudnionymi w nich osobami lub innymi osobami dysponującymi informacjami istotnymi z punktu widzenia działalności służb. Ustawa zawiera również zamknięty wykaz specjalnych środków pozyskiwania informacji, które można scharakteryzować w sensie ogólnym jako czynności operacyjno-rozpoznawcze.

Artykuł 19 ustawy określa ogólne przesłanki stosowania specjalnych środków pozyskiwania informacji. Zgody na zastosowanie ww. środków udziela właściwy minister lub szef służby działający z upoważnienia ministra. Szef służby może upoważnić podległych mu funkcjonariuszy do udzielania zgody, o której mowa powyżej.

Zgoda na stosowanie specjalnych środków pozyskiwania informacji jest udzielana na okres trzech miesięcy, z możliwością każdorazowego przedłużenia na kolejne trzy miesiące. Ustawa nie przewiduje zatem górnej granicy czasowej stosowania tego typu środków.

Do specjalnych środków pozyskiwania informacji należą:

2.1. Obserwacja

1) obserwacja i utrwalanie informacji dotyczących zachowań osób fizycznych oraz przedmiotów, z wykorzystaniem lub bez wykorzystania środków technicznych;
2) śledzenie sposobu przemieszczania się osób fizycznych lub przedmiotów, z wykorzystaniem lub bez wykorzystania środków technicznych, instrumentów lokalizacji i urządzeń nagrywających.

Prowadzenie obserwacji i wykorzystywanie wymienionych urządzeń w budynkach mieszkalnych jest możliwe wyłącznie w przypadku, gdy właściwy minister udzielił szefowi służby pisemnej zgody na to. Wniosek o udzielenie zgody musi zawierać wskazanie adresu budynku, rodzaj instrumentu, który ma zostać wykorzystany, oraz uzasadnienie wskazujące powody, z jakich przeprowadzenie tego rodzaju czynności jest konieczne.

2.2. Pozyskiwanie informacji przez funkcjonariusza lub osobę działającą na zlecenie służb

Zgodnie z art. 21 służby są uprawnione do wykorzystania osoby fizycznej, posługującej się lub nieposługującej się danymi legalizacyjnymi, działającej pod kierunkiem danej służby, w celu:

1) pozyskiwania w sposób ukierunkowany i zgodnie z zaleceniami służb informacji o osobach fizycznych lub prawnych, które mogą mieć znaczenie dla realizacji zadań służb;
2) ochrony interesów istotnych z punktu widzenia służby.

Ponadto możliwe jest tworzenie osób prawnych w celu wsparcia działań operacyjno-rozpoznawczych.

Właściwy minister może polecić podległym mu organom administracji publicznej, aby udzieliły niezbędnej pomocy osobie posługującej się danymi legalizacyjnymi. W tym przypadku nie stosuje się powszechnie obowiązujących przepisów prawa w zakresie, w jakim wykluczają one podjęcie określonego działania lub zaniechania wobec tej osoby.

Osoba, o której mowa powyżej, może otrzymywać od służb instrukcje określonego zachowania się, które może stanowić przestępstwo lub pomocnictwo. Taka instrukcja może zostać wydana tylko wówczas, gdy jest to niezbędne do realizacji określonych zadań lub zapewnienia bezpieczeństwa osoby działającej na zlecenie służb. Ten dokument określa również okoliczności, w których osoba posługująca się danymi legalizacyjnymi może podjąć czynności mogące wypełniać znamiona czynu zabronionego oraz określić sposób ich dokonania.

2.3. Przeszukanie i badanie przedmiotów

Służby są uprawnione do realizacji przeszukania z wykorzystaniem lub bez wykorzystania instrumentów technicznych:

1) zamkniętych przestrzeni;
2) przedmiotów zabezpieczonych przed otwarciem.

Ponadto ustawa przewiduje możliwość zbadania przedmiotów, którego celem jest ustalenie tożsamości określonej osoby.

Jeżeli wymaga tego charakter określonej sprawy, służby mogą przejąć w posiadanie przedmiot znaleziony w toku realizacji czynności, o których mowa powyżej, jeżeli jego zbadanie w miejscu, w którym został znaleziony, jest niemożliwe oraz jeżeli

jest niemożliwe uzyskanie niezbędnych informacji w sposób mniej ingerujący w prawa i wolności obywatelskie.

Przeszukanie przestrzeni zamkniętych jest możliwe po uzyskaniu pisemnej zgody właściwego ministra, wydawanej maksymalnie na trzy dni. Wniosek szefa służby o udzielenie zgody przez ministra musi wskazywać adres budynku, w którym przeszukanie ma być dokonane, oraz uzasadniać przyczyny, z jakich podjęcie tego rodzaju czynności jest konieczne.

2.4. Otwarcie przesyłki

Po uzyskaniu zgody Sądu Rejonowego w Hadze udzielanej na wniosek szefa jednej ze służb omawiane organy mogą otwierać listy i inne przesyłki bez zgody ich nadawcy lub adresata. Wniosek o udzielenie zgody musi zawierać imię i nazwisko osoby lub nazwę firmy osoby prawnej będącej nadawcą lub adresatem przesyłki oraz wskazywać przyczyny uzasadniające otwarcie określonego listu lub przesyłki. Zgoda jest udzielana maksymalnie na okres trzech miesięcy.

2.5. Dostęp do zautomatyzowanej sieci informacji

Służby mogą – z wykorzystaniem lub bez wykorzystania środków technicznych, nieprawdziwych sygnałów, haseł lub identyfikatorów – uzyskać dostęp do zautomatyzowanej sieci informacji. To uprawnienie obejmuje również obejście systemów zabezpieczeń, wprowadzenie urządzeń technicznych mających na celu złamanie szyfrów zabezpieczających informacje przechowywane lub przetwarzane w tej sieci, a także kopiowanie tych informacji.

Osoby posiadające informacje pozwalające na złamanie szyfrów chroniących określone dane są zobowiązane, po otrzymaniu pisemnego żądania szefa służby, do udzielenia niezbędnej pomocy podczas uzyskiwania przez służby dostępu do zaszyfrowanych informacji.

2.6. Przechwytywanie i utrwalanie komunikacji

Ustawa upoważnia służby do przechwytywania treści, nagrywania i monitorowania w sposób ukierunkowany rozmów, informacji wymienianych z wykorzystaniem urządzeń telekomunikacyjnych oraz danych telekomunikacyjnych, niezależnie od miejsca, w którym są one prowadzone. To uprawnienie obejmuje również złamanie szyfrów zabezpieczających te informacje.

Wniosek o udzielenie zgody na zastosowanie opisywanej metody pozyskiwania informacji jest sporządzany przez szefa służby i zawiera co najmniej:

1) określenie czynności, jakie mają zostać dokonane;
2) dane osoby lub podmiotu będącego stroną połączenia, które mają zostać przechwycone lub utrwalone;
3) wskazanie przyczyn, z których powodu dokonanie ww. czynności jest niezbędne.

Gdy w chwili sporządzania wniosku o udzielenie zgody na wykorzystanie ww. czynności numer abonenta, którego komunikacja ma zostać przechwycona lub utrwalona, nie jest znany, zgoda może zostać udzielona wyłącznie po dokonaniu jego jednoznacznej identyfikacji. W tym celu służby mogą się posłużyć środkami techniczny-

mi umożliwiającymi identyfikację numeru. Ustawa wprowadza analogiczny warunek w przypadku braku określenia tożsamości osoby lub podmiotu będących stroną komunikacji w chwili sporządzania wniosku.

2.7. Monitorowanie międzynarodowej komunikacji bezprzewodowej

Artykuł 26 stanowi podstawę normatywną stosowania instrumentu przechwytywania i utrwalania komunikacji (rodzajowo zbliżonego do omówionego w poprzednim punkcie), polegającego na pozyskiwaniu i utrwalaniu wiadomości wysyłanych z zagranicy lub przeznaczonych dla odbiorców zagranicznych, które to są wymieniane przy użyciu bezprzewodowych sieci telekomunikacyjnych. Wytypowanie określonego procesu wymiany informacji, który ma zostać objęty omawianym instrumentem, odbywa się na podstawie analizy jego charakterystyki technicznej, która może wykazać istnienie potencjalnego związku z działaniami pozostającymi w sferze zainteresowań służb. Do czynności, które mogą zostać podjęte w ramach realizacji ww. uprawnienia, zalicza się również złamanie szyfrów zabezpieczających pozyskiwane informacje.

W razie ustalenia tożsamości osoby lub podmiotu będącego nadawcą lub odbiorcą komunikacji, informacje na jej temat mogą zostać utrwalone. Jeżeli po ustaleniu tożsamości okaże się, że niezbędne jest przechwycenie lub utrwalenie informacji wymienianych przy wykorzystaniu sieci telekomunikacyjnych, ustawa nakłada na służby obowiązek złożenia wniosku o udzielenie zgody na zastosowanie tego instrumentu w ciągu dwóch dni od ustalenia tożsamości osoby lub podmiotu, o którym mowa powyżej. Do czasu udzielenia zgody służby nie zapoznają się z treścią tej komunikacji. Jeżeli okaże się, że informacje zebrane podczas stosowania omawianego środka nie są niezbędne do prawidłowej realizacji zadań służb, to ulegają niezwłocznemu zniszczeniu.

2.8. Pozyskiwanie danych telekomunikacyjnych

Służby mogą się zwrócić do operatorów publicznych sieci telekomunikacyjnych oraz do operatorów publicznych usług telekomunikacyjnych w rozumieniu ustawy – Prawo telekomunikacyjne[27] z wnioskiem o udzielenie informacji o użytkowniku oraz danych dotyczących generowanego przez tego użytkownika tzw. ruchu telekomunikacyjnego (ang. *telecommunication traffic*). Może to dotyczyć zarówno informacji przetwarzanych przed złożeniem wniosku, jak i po jego złożeniu.

Artykuł 29 ust. 2 ustawy wprowadza definicję legalną pojęcia u ż y t k o w n i k t e l e k o m u n i k a c y j n y (ang. *user of telecommunication*). Jest to zarówno osoba fizyczna lub prawna, która zawarła umowę o korzystanie z publicznych sieci telekomunikacyjnych albo publicznych usług telekomunikacyjnych, jak i osoba fizyczna lub prawna aktywnie korzystająca z sieci lub usługi telekomunikacyjnej.

Wniosek o udostępnienie tych danych jest sporządzany przez szefa służby i zawiera następujące elementy:

1) numer w rozumieniu art. 1 bb ustawy – Prawo telekomunikacyjne[28];

[27] *Act of 19 October 1998 containing rules regarding telecommunication* (*Telecommunications Act*) [online], https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act [dostęp: 14 II 2017].

[28] Zgodnie z art. 1 bb pojęcie n u m e r oznacza – w rozumieniu ustawy – numery, litery lub inne symbole występujące (lub niewystępujące) w określonej kombinacji, mające na celu udzielenie dostępu lub identyfikację użytkowników, operatorów sieci lub usług, urządzeń końcowych albo innych elementów sieci.

2) imię, nazwisko i adres zamieszkania osoby lub nazwę i adres siedziby osoby prawnej, do której należy numer;
3) wskazanie informacji, które mają zostać udostępnione;
4) wyznaczenie okresu, którego mają dotyczyć informacje.

Artykuł 31 zawiera zbiór zasad mających na celu zapewnienie stosowania opisanych powyżej specjalnych metod pozyskiwania informacji w sposób proporcjonalny i subsydiarny. Wykorzystywanie omawianych metod jest możliwe tylko wówczas, gdy nie można uzyskać niezbędnych informacji w inny sposób. Jeżeli w konkretnej sprawie została udzielona zgoda na zastosowanie więcej niż jednego instrumentu tego rodzaju, służby są zobowiązane do wykorzystania wyłącznie instrumentu wywołującego najmniejsze szkody dla osób, których dotyczą czynności. Wybór metody najmniej zagrażającej prawom i wolności odbywa się z uwzględnieniem wszystkich okoliczności danej sprawy – powagi i rodzaju zagrożenia, charakteru chronionych dóbr i specyfiki konkretnej sprawy.

Określona metoda pozyskiwania informacji nie może zostać wykorzystana, jeżeli zagrożenie, jakie niesie za sobą jej ewentualne zastosowanie będzie nieproporcjonalnie wysokie w stosunku do zamierzonego celu działań. Prowadzenie wszelkich czynności związanych ze stosowaniem specjalnych metod pozyskiwania informacji ustaje, gdy zostanie osiągnięty ich cel lub gdy okoliczności sprawy pozwalają na zastosowanie innych, mniej inwazyjnych metod.

3. Współpraca z innymi organami i zagranicznymi służbami partnerskimi

Ustawa nakłada na AIVD i MIVD obowiązek udzielania sobie pomocy przez wymianę informacji lub wsparcie techniczne, lub w innej postaci – w związku ze stosowaniem specjalnych środków pozyskiwania informacji.

Szefowie służb są odpowiedzialni za utrzymywanie kontaktów z zagranicznymi służbami partnerskimi. AIVD i MIVD mogą udzielić służbom specjalnym innych państw informacji istotnych z punktu widzenia realizacji ich zadań, o ile nie zagraża to dobrom chronionym przez służby holenderskie i nie utrudnia realizacji ich zadań. Możliwe jest również, na tych samych zasadach, udzielenie służbom zagranicznym wsparcia o charakterze technicznym lub wsparcia innego rodzaju. Właściwy minister może upoważnić szefów służb do wydawania zgody na udzielenie informacji służbom innych państw lub na udzielenie im wsparcia w nagłych przypadkach. Szef służby niezwłocznie wówczas powiadamia właściwego ministra o każdorazowym udzieleniu zgody w trybie nagłym.

Ustawa reguluje ponadto tryb współpracy AIVD z organami krajowymi. Zgodnie z art. 60 szefowie Policji, Żandarmerii Królewskiej oraz Dyrektor Generalny Narodowego Biura Podatkowego działającego w ramach Ministerstwa Finansów wykonują czynności dla AIVD wynikające z odrębnych przepisów.

Prokuratura przekazuje służbom wszelkie informacje, które mogą mieć istotne znaczenie dla realizacji ustawowych zadań służby. W sprawach wymagających współpracy prokuratury i służb ustawa przewiduje obowiązek odbycia konsultacji z udziałem członka Rady Prokuratorów i szefa właściwej służby.

Zarówno AIVD, jak i MIVD są uprawnione – na podstawie pisemnego wniosku właściwego organu – do udzielenia wsparcia technicznego organom odpowiedzialnym za prowadzenie postępowań przygotowawczych.

LUKSEMBURG

Podstawę normatywną działalności jedynej służby specjalnej Luksemburga – Służby Wywiadu (Service de Renseignement de l'Etat – SRE) jest *Ustawa z dnia 15 czerwca 2004 r. o powołaniu Służby Wywiadu* (dalej: ustawa)[1]. Celem ustawy było dostosowanie zakresu kompetencji SRE oraz instrumentów wykorzystywanych przez służbę do współczesnych zagrożeń bezpieczeństwa państwa, a także wprowadzenie nowego modelu kontroli parlamentarnej.

Najistotniejszym elementem reformy było dodanie do zadań SRE ochrony bezpieczeństwa wewnętrznego. Przed przyjęciem wspomnianego wyżej aktu prawnego w zakresie kompetencji SRE leżało wyłącznie prowadzenie działań mających na celu zapewnienie bezpieczeństwa zewnętrznego Luksemburga i państw z nim sprzymierzonych. Reforma nadała zatem SRE charakter służby odpowiadającej za wszystkie aspekty ochrony fundamentalnych interesów państwa, zarówno w wymiarze wewnętrznym, jak i zewnętrznym.

1. Zadania SRE

Organem odpowiedzialnym za nadzór nad działalnością SRE jest premier. Zgodnie z art. 2 ustawy do zadań tej służby należy:

1) pozyskiwanie, analizowanie i przetwarzanie informacji dotyczących wszelkiej działalności zagrażającej lub mogącej zagrażać bezpieczeństwu Luksemburga, państw, z którymi Luksemburg zawarł porozumienia o wspólnej obronie, lub organizacji międzynarodowych mających siedzibę lub wykonujących zadania na terytorium Luksemburga, a także stosunkom międzynarodowym i potencjałowi naukowemu lub gospodarczemu tego państwa;
2) prowadzenie postępowań sprawdzających przewidzianych w ustawach lub wynikających z zobowiązań prawnomiędzynarodowych;
3) ochrona informacji niejawnych;
4) nadzór nad stosowaniem krajowych lub międzynarodowych przepisów prawnych dotyczących sfery bezpieczeństwa.

Artykuł 2 pkt 2 zawiera definicję legalną pojęcia d z i a ł a l n o ś ć z a g r a ż a j ą c a l u b m o g ą c a z a g r a ż a ć b e z p i e c z e ń s t w u L u k s e m b u r g a. Ten termin oznacza każdą działalność, indywidualną lub zbiorową, prowadzoną na terenie kraju lub inspirowaną spoza jego granic, która:

1) może mieć związek ze szpiegostwem, ingerencją innego państwa w wewnętrzne sprawy Luksemburga, terroryzmem, proliferacją broni niekonwencjonalnej lub związanych z nią technologii albo zorganizowaną przestępczością, jeżeli ma ona związek z wymienionymi zjawiskami;
2) może podważyć integralność terytorialną kraju, jego suwerenność i niepodległość, bezpieczeństwo jego instytucji, poprawne funkcjonowanie instytucji państwa prawa lub zagrażać bezpieczeństwu obywateli.

Rozdział II ustawy – *O pozyskiwaniu i przetwarzaniu informacji* – określa zasady współpracy SRE z innymi instytucjami państwa oraz podmiotami międzynarodowymi, a także zasady dostępu do informacji i ochrony źródeł informacji.

Zgodnie z art. 3 SRE dba o zapewnienie sprawnej współpracy zarówno z organami policyjnymi, sądowymi i administracyjnymi, jak i z zagranicznymi służbami specjal-

nymi. Ustawa zobowiązuje tę służbę wprost do przekazywania informacji zebranych podczas wykonywania jej ustawowych zadań organom policyjnym, sądowym i administracyjnym w zakresie, w jakim są one niezbędne do realizacji ich zadań ww. organów. Analogicznie – organy, o których mowa, są zobowiązane z kolei do przekazywania SRE informacji, które mogą mieć związek z jej zadaniami określonymi w art. 2 ustawy. Funkcję organu koordynującego działalność SRE i Policji Wielkiego Księstwa pełni komitet złożony z premiera oraz ministrów: spraw zagranicznych, obrony narodowej, sprawiedliwości i szefa Policji.

2. Dostęp do informacji

Przetwarzanie przez SRE informacji uzyskanych w czasie wykonywania jej ustawowych zadań odbywa się zgodnie z zasadami przewidzianymi w rozporządzeniu, do którego wydania zobowiązuje *Ustawa z dnia 2 sierpnia 2002 r. o ochronie danych osobowych*[29].

Podczas realizacji swoich ustawowych zadań SRE jest uprawniona do dostępu do następujących baz danych:

1) Ogólnego Rejestru Osób Fizycznych i Prawnych utworzonego na podstawie *Ustawy z dnia 30 marca 1979 roku o identyfikacji cyfrowej osób fizycznych i prawnych*;
2) części baz danych Policji umożliwiających wyszukiwanie danych osobowych;
3) jednego z biuletynów wchodzących w skład Rejestru Sądowego (Biuletyn nr 2);
4) bazy danych zawierającej informacje o cudzoziemcach, wykorzystywanej na rachunek komórki Policji ds. cudzoziemców, działającej w ramach Ministerstwa Sprawiedliwości;
5) bazy danych zawierającej informacje o pracownikach, pracodawcach i osobach wykonujących tzw. wolne zawody, zarządzanej przez organ ubezpieczeń społecznych zgodnie z art. 321 kodeksu ubezpieczeń społecznych;
6) bazy danych zawierającej informacje o pojazdach drogowych, ich właścicielach i posiadaczach, wykorzystywanej na rachunek Ministerstwa Transportu.

Przetwarzanie danych osobowych przez SRE, Policję, Służbę Celną i podmioty wchodzące w skład sił zbrojnych jest dokonywane pod nadzorem organu przewidzianego w art. 17 (2) ustawy[30], w którego skład wchodzą Prokurator Generalny lub jego zastępca oraz dwóch członków Narodowej Komisji Ochrony Danych Osobowych. Z uwagi na konieczność zapewnienia instrumentów umożliwiających wykonywanie temu organowi czynności kontrolnych, dostęp SRE do danych zawartych w bazach musi odbywać się w sposób umożliwiający późniejsze odtworzenie sposobu, czasu i innych informacji o dokonaniu wglądu do konkretnej bazy. Ponadto art. 4 ust. 3 ustawy expressis verbis zabrania SRE wykorzystywania informacji pozyskanych w toku realizacji zadań służbowych do jakichkolwiek innych działań niż wykonywanie zadań wynikających z art. 2 ustawy.

SRE może żądać od osób fizycznych oraz państwowych i prywatnych osób prawnych wszystkich informacji niebędących danymi osobowymi, niezbędnych do wykonywania swoich zadań ustawowych.

[29] www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf [dostęp: 14 II 2017].

[30] Ustawa o ochronie danych osobowych nie zawiera nazwy własnej tego organu, w tekście ustawy jest on określony jako „autorité de contrôle", co w dosłownym tłumaczeniu oznacza 'władza kontrolna' lub 'organ kontrolny'.

3. Ochrona źródeł

Zgodnie z art. 5 ustawy funkcjonariusze SRE, biorąc udział w postępowaniu administracyjnym lub sądowym w charakterze świadka, są zobowiązani do zachowania w tajemnicy informacji, które mogą skutkować ujawnieniem tożsamości osobowego źródła informacji współpracującego ze służbą. Ustawa wprowadza analogiczny zakaz w odniesieniu do osób, które powzięły tego rodzaju informacje w związku z wykonywaniem czynności zawodowych. Organy policyjne, sądowe i administracyjne nie mogą podejmować działań, których celem lub skutkiem byłoby ujawnienie tożsamości źródła.

Prezes Sądu Najwyższego może postanowić o zwolnieniu z obowiązku zachowania tajemnicy w toku postępowania, pod warunkiem, że ewentualne ujawnienie określonej informacji nie wpłynie negatywnie na działania podejmowane przez służbę oraz że nie będzie stanowiło zagrożenia dla osoby fizycznej. Zwolnienie z obowiązku, o którym mowa, nie może dotyczyć informacji udzielonych przez zagraniczne służby wywiadowcze.

Jeżeli informacje umożliwiające identyfikację źródła zostały uzyskane w toku postępowania, którego celem nie było ustalenie tożsamości źródła SRE, nie mogą zostać wykorzystane jako dowód w postępowaniu przed sądem, z wyjątkiem sytuacji, w których to wykorzystanie nie skutkowałoby ujawnieniem tożsamości źródła oraz w których o zwolnieniu od zachowania tajemnicy postanowił Prezes Sądu Najwyższego.

NIEMCY

1. Federalny Urząd Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV)

BfV jest służbą odpowiedzialną za bezpieczeństwo wewnętrzne. Związane z tym funkcje są realizowane również przy pomocy krajowych urzędów ochrony konstytucji (Landesbehörden für Verfassungsschutz – LfV) działających na poziomie krajów związkowych. Do podstawowych zadań BfV należy gromadzenie informacji o zagrożeniach porządku demokratycznego państwa godzących w bezpieczeństwo oraz istnienie RFN lub jednego z krajów związkowych, działalność kontrwywiadowcza, a także zapobiegająca jakimkolwiek działaniom sabotażowym wymierzonym w państwo.

Kompetencje omawianej służby szczegółowo regulują ustawy: o współpracy między Republiką Federalną a krajami związkowymi w zakresie dotyczącym ochrony konstytucji i o Urzędzie Ochrony Konstytucji[31]. Na jej mocy BFV zostało powierzone gromadzenie oraz analiza informacji o:

1) działaniach przeciwko podstawom porządku demokratycznego,
2) działaniach przeciwko istnieniu oraz bezpieczeństwu Republiki Federalnej lub jednego z jej krajów związkowych;
3) bezprawnych działaniach wymierzonych w funkcjonowanie konstytucyjnych organów Republiki Federalnej Niemiec lub jednego z jej krajów związkowych oraz jej funkcjonariuszy w czasie wykonywania obowiązków;

[31] Niem. *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschitzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BverfSchG)* [online], www.gesetze-im-internet.de/bverfschg/BJNR029700990.html [dostęp: 10 II 2017].

4) narażaniu na niebezpieczeństwo zagranicznych interesów Republiki Federalnej Niemiec przez użycie przemocy lub przygotowywanie ww. działań;
5) działaniach wymierzonych w międzynarodowy pokój (porozumienie), szczególnie przeciwko pokojowej koegzystencji obywateli.

Ponadto do zadań BfV należy gromadzenie oraz analizowanie informacji o podejmowanych czynnościach wywiadowczych prowadzonych na rzecz podmiotów zagranicznych (kontrwywiad).

Służba uczestniczy także w zwalczaniu działalności antypaństwowej i wydawaniu poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych oraz świadectw bezpieczeństwa przemysłowego[32].

BfV gromadzi najwięcej informacji z jawnych i ogólnie dostępnych źródeł, np. takich jak media. Funkcjonariusze BfV uczestniczą w różnych wydarzeniach publicznych i odbywają rozmowy z osobami, które mogą posiadać informacje istotne dla BfV.

2. Regulacje ustawowe – ustawa o BfV[33]

W rozdziale I ustawy o BfV przewidziano obowiązek współpracy w zakresie ochrony konstytucji zarówno na szczeblu związkowym jak i krajowym. Określono również podległość BfV ministrowi spraw wewnętrznych wskazano, że BfV nie może działać przy Policji. Poza uprawnieniami BfV, które zostały wskazane w podrozdziale 1, współpracujące z tą służbą krajowe urzędy ochrony konstytucji działają w zakresie:

1) wydawania poświadczeń bezpieczeństwa osobom, którym w związku z czynnościami służbowymi są powierzane informacje niejawne;
2) wydawania poświadczeń bezpieczeństwa osobom, które zajmują lub będą zajmować stanowiska istotne z punktu widzenia bezpieczeństwa życia lub obronności;
3) stosowania – w interesie publicznym – technicznych środków bezpieczeństwa w celu ochrony informacji niejawnych, ochrony przedmiotów lub dokonywania ustaleń dotyczących nieuprawnionego dostępu do tego typu informacji;
4) sprawdzania osób w przypadkach przewidzianych przez prawo.

Jednocześnie wszelkie działania prowadzone przez BFV muszą być podejmowane zgodnie z ustawą regulującą uprawnienia tej służby.

2.1. Obowiązki BFV

BfV w porozumieniu z krajowymi urzędami ochrony konstytucji może gromadzić w landach (krajach związkowych) informacje, wiadomości lub dokumenty odnośnie do spraw, które w rozumieniu ustawy są działaniami zgodnymi z § 3 ust. 1 nr 1–4 i z § 5:

1) w pełni lub częściowo są skierowane przeciwko związkowi;
2) są ukierunkowane na użycie przemocy, przygotowanie do użycia przemocy lub ją wspierają;
3) są prowadzone na obszarze kraju związkowego;
4) mają wpływ na sprawy zagraniczne RFN;
5) wymagają od krajowych urzędów ochrony konstytucji współpracy ze strony BfV.

[32] www. Verfassungsschutz.de/en/index-en.html [dostęp: 10 II 2017].

[33] Niem. Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschitzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BverfSchG), za: www.gesetz-im-internet.de/bverfschg/BJNR029700990.html [dostęp: 10 II 2017].

BfV ocenia i analizuje na poziomie centralnym wszystkie ustalenia dotyczące czynności, o których mowa w § 3 ust. 1. (również krajowe urzędy ochrony konstytucji mają obowiązek dokonywania takiej analizy). BFV przekazuje krajowym urzędom ochrony konstytucji, zgodnie z § 6 ust. 1, informacje sporządzone jako przekrojowe analizy w formie opracowań strukturalnych i metodycznych, a także regularnie przekazywanych ogólnokrajowych meldunków na temat istotnych zjawisk, przy uwzględnieniu sytuacji danego kraju związkowego.

BfV koordynuje współpracę krajowych urzędów ochrony konstytucji. Powyższa koordynacja dotyczy przede wszystkim uzgodnienia:

1) jednolitych przepisów zapewniających możliwości współpracy;
2) ogólnych priorytetów i podziału pracy oraz wykonywania zadań;
3) kryteriów ważności przekazywania informacji zgodnie z § 6 ust. 1.

Ponadto BfV jako centrala wspiera krajowe urzędy ochrony konstytucji przy wykonywaniu zadań, zgodnie z § 3, zwłaszcza przez:

1) zapewnienie wywiadowczego systemu informacyjnego;
2) centralne wyposażenie w obszarze czynności technicznych i specjalistycznych;
3) prowadzenie badań i rozwój metod i sposobów pracy w zakresie ochrony konstytucji;
4) szkolenie w szczególnych obszarach pracy.

W celu wykonywania zadań określonych w § 3 BfV jest zobowiązany do utrzymywania stosunków służbowych z właściwymi organami publicznymi innych państw. Krajowe urzędy ochrony konstytucji mogą, w porozumieniu z BfV, utrzymywać takie stosunki służbowe:

1) ze służbami sił zbrojnych stacjonujących w RFN,
2) ze służbami wywiadowczymi przyległych krajów sąsiednich, w sprawach regionalnych.

2.2. Wymiana i ochrona informacji

Władze krajowe oraz BfV przekazują niezwłocznie między sobą informacje istotne dla wykonywania swoich zadań. W sytuacji, gdy organ przesyłający zrobi zastrzeżenie, przekazywane dane mogą być udostępniane stronom trzecim tylko za jego zgodą.

W celu wypełnienia obowiązku informacyjnego przez BfV urzędy ochrony konstytucji są zobowiązane do prowadzenia wspólnych plików, które są wykorzystywane w sposób zautomatyzowany. Przechowywanie danych osobowych jest dopuszczalne zgodnie z wymaganiami określonymi w ustawie. Automatyczny dostęp innych organów jest niemożliwy. Odpowiedzialność za wprowadzone dane w zakresie ogólnych przepisów o ochronie danych osobowych spoczywa na każdym urzędzie ochrony konstytucji – tylko on może zmieniać te dane, blokować je lub usuwać. Koniecznością jest zapewnienie możliwości ustalenia organu, który wprowadzał dane. Z kolei wyszukanie danych jest dopuszczalne tylko wtedy, gdy jest to konieczne do realizacji zadań, za których wykonanie jest odpowiedzialny wnioskodawca. Prawo dostępu do danych, które nie są konieczne do wyszukiwania akt i identyfikacji osób, jest ograniczone do podmiotów, które są upoważnione do rejestracji danych lub analiz. Prawo dostępu do dokumentów zawierających dane jest ograniczone do osób, które są bezpośrednio zaangażowane do wykonywania tej pracy.

BfV w odniesieniu do udostępnianych informacji dotyczących środków technicznych i organizacyjnych podejmuje działania zgodnie z § 9 ustawy o ochronie danych. Na

potrzeby kontroli za każdym razem rejestruje dostęp do chronionych danych, czas dostępu, informacje umożliwiające określenie danych, których dotyczyło zapytanie, oraz organ występujący z zapytaniem. Analiza protokołowanych (rejestrowanych) informacji jest zagwarantowana zgodnie ze stanem technicznym. Te dane mogą być wykorzystane jedynie w celu kontroli ochrony danych, bezpieczeństwa danych lub zapewnienia właściwego systemu ich przetwarzania. Zarejestrowane dane niszczy się pod koniec roku kalendarzowego, który przypada po roku, w którym zostały one zaprotokołowane.

2.3. Uprawnienia BfV

W rozdziale II ustawy zostały określone uprawnienia BfV. Na tej podstawie służba może uzyskiwać, przetwarzać i wykorzystywać informacje niezbędne do wykonywania swoich zadań, w tym dane osobowe, o ile nie stoją temu na przeszkodzie przepisy o ochronie danych osobowych lub szczególne przepisy ustawy.

Wniosek BfV o udostępnienie danych osobowych powinien dotyczyć tylko tych danych osobowych, które są niezbędne do udzielenia informacji. Informacje wymagające ochrony, które dotyczą osoby zainteresowanej, mogą być ograniczone tylko w szczególnym zakresie. BfV w celu niejawnego pozyskiwania danych może również stosować metody, wykorzystywać obiekty i instrumenty, a także działania współpracowników i sprawdzonych osób, obserwację, nagrania obrazu i dźwięku, dokumenty legalizacyjne oraz niejawne oznakowanie. W sprawach dotyczących praw osobistych można ingerować ze wskazaniem szczególnego uprawnienia. Poza tym zastosowanie jednego wyżej wspomnianych środków nie może spowodować szkody, która jest niewspółmierna do znaczenia wyjaśnianych faktów. Środki, o których mowa powyżej, są określone w przepisach służbowych. Ich zastosowanie wymaga zgody Federalnego Ministerstwa Spraw Wewnętrznych, które informuje o tym parlamentarny organ kontrolny.

Należy również pamiętać, że BfV nie ma uprawnień policyjnych ani kompetencji np. do wystawiania mandatów. Co istotne, ta służba nie może również angażować policji przez współpracę mającą na celu wykorzystanie środków, do których stosowania sama nie jest uprawniona.

W przypadku, gdy dane osobowe osoby zainteresowanej są pozyskane za jej wiedzą, powinien zostać podany powód ich zebrania. Osoba zainteresowana podaje dane osobowe dobrowolnie. Ze środków, którymi dysponuje BfV, powinien zostać zastosowany ten, który wobec takiej osoby będzie najmniej dolegliwy. Żaden środek nie może powodować szkody, która jest wyraźnie nieproporcjonalna do zamierzonego rezultatu.

2.4. Specjalne wnioski o udzielenie informacji

BfV może w szczególnych przypadkach uzyskiwać informacje od:

1) przewoźników, a także operatorów systemów rezerwacji komputerowej i systemów dystrybucji globalnej dla lotów odnośnie do pytań zarówno o imiona lub nazwiska i adresy klientów, jak i o wykorzystanie okoliczności usług transportowych, szczególnie w momencie wysyłki (odprawy), odlotu i sposobu rezerwacji;
2) instytucji kredytowych, instytucji świadczących usługi finansowe oraz przedsiębiorstw, posiadaczy rachunków i innych uprawnionych oraz odnośnie do obrotu płatniczego uczestników, przepływu pieniądza, lokat kapitału, zwłaszcza jeśli chodzi o salda rachunku i płatności przychodzących oraz wychodzących;

3) osób świadczących usługi telekomunikacyjne lub współpracujących przy świadczeniu takich usług, zgodnie z ustawą o telekomunikacji, w zakresie danych dotyczących ruchu (w telekomunikacji) i innych niezbędnych danych w celu ustanowienia i utrzymania ruchu (w telekomunikacji);
4) osób świadczących usługi telekomunikacyjne lub współpracujących w tym zakresie, odnośnie do:
   a) danych istotnych do identyfikacji użytkownika tych usług (teleserwisu),
   b) informacji o początku i zakończeniu oraz skali korzystania z usług,
   c) danych o teleusługach wykorzystywanych przez użytkownika,

– w zakresie, w jakim jest to niezbędne do gromadzenia i analizy informacji i faktów, które uzasadniają, że zachodzi poważne zagrożenie dóbr określonych w § 3 ust. 1.

W § 3 ust. 1 nr 1 dotyczy to tylko zagrożeń, które spełniają poniższe kryteria przez zamiar lub sposób działania w zakresie:

1) podżegania do nienawiści lub samowolnych działań przeciwko części narodu lub do ataku na godność ludzką przez znieważenie, poniżanie lub oczernianie wynikające ze złej woli i tym samym wspieranie gotowości do użycia siły i zakłócenia ładu publicznego;
2) przygotowywania lub stosowania przemocy łącznie z nawoływaniem lub wspieraniem do użycia przemocy także przez wspieranie stowarzyszeń, które nakłaniają do ataków przeciwko osobom lub rzeczom, popierają takie działania lub grożą ich przeprowadzeniem.

2.5. Zasady proceduralne odnoszące się do wniosków o udzielenie informacji

Zarządzenia odnoszące się do określonych, specjalnych wniosków o udzielenie informacji są wydawane przez szefa BFV lub jego zastępcę. Wnioski są składane w formie pisemnej wraz z uzasadnieniem. Za wymienione zarządzenia jest odpowiedzialne Federalne Ministerstwo Spraw Wewnętrznych. Zarządzenia dotyczące pozyskania informacji, które mogą dotyczyć danych uzyskanych w przyszłości, jest wydawane na trzy miesiące. Przedłużenie takiego zarządzenia każdorazowo o nie więcej niż trzy miesiące jest dozwolone na wniosek, tak długo jak występują przesłanki określone w ww. zarządzeniu.

Federalne Ministerstwo Spraw Wewnętrznych informuje o wykonaniu zarządzeń Komisję G10[34].

2.6. Ograniczenie praw podstawowych

Podstawowe prawo tajemnicy telekomunikacyjnej (art. 10 Konstytucji) może na mocy ustawy o BFV podlegać ograniczeniu.

[34] Komisja G10 – nazwa tej Komisji jest związana z art. 10 Konstytucji RFN, stanowiącym o tajemnicy korespondencji i telekomunikacji. Odstępstwa od ww. zasady mogą mieć zastosowanie tylko w określonych sytuacjach. Komisja, o której mowa, zajmuje się przypadkami wkraczania w sferę regulowaną przez art. 10 Konstytucji. Zadaniem Komisji jest m.in. monitorowanie czynności w zakresie kontroli operacyjnej, ale również retencji, przetwarzania i wykorzystywania danych osobowych gromadzonych przez służby stosujące te czynności, jak również podejmowanie decyzji co do informowania osób, wobec których środki były stosowane.

2.7. Szczególne formy gromadzenia danych

BfV może gromadzić informacje, zwłaszcza dane osobowe, za pomocą środków określonych w ustawie, jeśli istnieją podstawy do przypuszczeń, że w ten sposób zostanie pozyskana wiedza o zagrożeniach lub działaniach, o których mowa w § 3 ust. 1, albo że będzie możliwe dotarcie do źródeł takiej wiedzy. Gromadzenie informacji, w tym danych osobowych, jest dopuszczalne, jeśli jest to konieczne do ochrony pracowników, urządzeń, obiektów i źródeł BfV przed działaniami zagrażającymi bezpieczeństwu lub działaniami wywiadowczymi. Uzyskanie informacji w powyższy sposób jest niedopuszczalne, jeśli istnieje ewentualność zbadania sprawy w inny sposób, mniej szkodzący osobie, np. ze źródeł powszechnie dostępnych lub przy pozyskiwaniu innych informacji. Zastosowanie środka zgodnie z § 8 ust. 2 nie może być wyraźnie niewspółmierne do znaczenia wyjaśnianych faktów. Jeżeli nie został osiągnięty zamierzony cel lub istnieją poszlaki, że nie będzie w ten sposób osiągnięty, należy odstąpić od stosowania danego środka.

Przechwytywanie rozmów prywatnych prowadzonych w mieszkaniach może być niejawnie rejestrowane za pomocą środków technicznych, jeśli jest to niezbędne w szczególnym przypadku do zapobieżenia bezpośredniemu niebezpieczeństwu lub bezpośredniemu zagrożeniu życia osób, a odpowiednie wsparcie policyjne dla zagrożonego dobra nie może być uzyskane bez zbędnej zwłoki. Powyższe ma zastosowanie odpowiednio do niejawnego wykorzystania środków technicznych w celu wykonania rejestracji obrazu. Te środki są zarządzane przez szefa BfV lub jego zastępcę, jeżeli decyzja sądowa nie może być uzyskana na czas. Taką decyzję należy jednak uzyskać niezwłocznie. Właściwym do tego jest sąd, w którego okręgu BfV ma siedzibę. Ponadto w powyższych przypadkach konstytucyjne prawo nienaruszalności mieszkania – zgodnie z art. 13 Konstytucji – ulega ustawowemu ograniczeniu.

Przy pozyskiwaniu danych, które w zakresie formy i znaczenia są tożsame i podlegają takiej samej ochronie w postaci tajemnicy korespondencji, tajemnicy pocztowej i tajemnicy telekomunikacyjnej, w tym szczególnie w ramach czynności przechwytywania i utrwalania prywatnych rozmów za pośrednictwem niejawnych środków technicznych:

1) osoba będąca w kręgu zainteresowań musi być po zakończeniu działań o nich poinformowana, tak szybko, jak tylko ryzyko dla celu, w związku z którym działania zostały podjęte, zostanie wykluczone,
2) musi zostać poinformowane kolegium parlamentarne.

BfV pod warunkami określonymi w ustawie może stosować środki techniczne do ustalenia lokalizacji aktywnie włączonego, działającego urządzenia mobilnego lub w celu dochodzenia numeru urządzenia lub numeru karty. Ten środek jest dopuszczalny tylko wtedy, gdy jest niemożliwe lub utrudnione ustalenie lokalizacji lub określenie numeru urządzenia albo numeru karty bez użycia środków technicznych. Dane osoby trzeciej mogą być zbierane tylko w ten sposób wówczas, gdy jest to konieczne ze względów technicznych, aby osiągnąć powyższy cel.

2.8. Funkcjonariusze pod przykryciem

BfV może wykorzystywać własnych pracowników, przyznając im fikcyjną tożsamość (legendę) w celu uzasadnienia działań zgodnie z art. 9 ust. 1 ustawy. Permanentne prowadzenie czynności mające na celu rozpoznawanie zagrożeń jest dozwolone tylko

w przypadku przeprowadzania poważnych działań, szczególnie gdy są one ukierunkowane na użycie siły lub przemocy.

Funkcjonariusze działający pod przykryciem nie powinni podejmować czynności zgodnie z § 3 ust. 1 ani kierować takimi czynnościami. Mogą działać w organizacjach przestępczych lub dla takich organizacji, aby wyjaśnić ich czyny. Ponadto udział w takiej działalności jest dopuszczany, jeżeli:

1) nie stanowi pogwałcenia praw osobistych,
2) oczekuje się, że jest to niezbędne do uzyskania i zabezpieczenia dostępu do informacji,
3) nie jest nieproporcjonalny do wagi wyjaśnianych faktów.
4) Jeśli istnieją wystarczające przesłanki, że funkcjonariusze działający pod przykryciem wbrew prawu popełnili poważny czyn przestępczy, działania powinny zostać natychmiast zakończone i powinny o tym zostać powiadomione organy ścigania. O wyjątkach zadecyduje szef służby lub jego zastępca.

2.9. Osobowe źródła informacji

Zgodnie z ustawą możliwa jest współpraca z osobami prywatnymi, których zaplanowana, długotrwała współpraca z BfV nie jest znana osobom trzecim (osobowe źródła informacji). Rząd Federalny co najmniej raz w roku składa Kolegium Parlamentarnemu sprawozdanie ze współpracy z osobowymi źródłami informacji.

O obowiązkach osobowych źródeł informacji decyduje szef lub jego zastępca. Jako osobowe źródła informacji nie mogą być rekrutowane albo wykorzystywane:

1) osoby ubezwłasnowolnione, zwłaszcza nieletni,
2) osoby zależne od wsparcia finansowego lub rzeczowego, które jest ich jedynym źródłem utrzymania,
3) osoby biorące udział w działalności izolującej od społeczeństwa (np. osoby funkcjonujące w sektach),
4) posłowie do Parlamentu Europejskiego, niemieckiego Bundestagu, parlamentu kraju związkowego lub pracownicy takich osób,
5) osoby, które figurują w Centralnym Rejestrze Federalnym w związku ze skazaniem za zbrodnię lub na karę pozbawienia wolności, której wykonanie nie zostało zawieszone.

2.10. Przechowywanie, zmiana i wykorzystania danych osobowych

BfV do wykonywania swoich zadań ustawowych może przechowywać, zmieniać i wykorzystywać dane osobowe w plikach, jeżeli:

1) zachodzą rzeczywiste przesłanki do przeprowadzenia działań lub czynności, o których mowa w § 3 ust. 1;
2) jest to niezbędne do badania i oceny działań lub czynności, o których mowa w § 3 ust. 1;
3) BfV wykonuje czynności zgodnie z § 3 ust. 2.

Dokumentacja dotycząca gromadzonych danych może być przechowywana także wtedy, gdy zawiera inne dane osób trzecich. Zabronione jest natomiast wystosowywanie zapytań o dane tych osób. Czas przechowywania dokumentacji został ograniczony do okresu wykonywania obowiązków przez BfV. Ponadto ta służba jest zobowiązana

do dokonywania korekty danych osobowych przechowywanych w plikach, jeśli są one niepoprawne, oraz do usuwania tych danych gromadzonych w plikach, gdy ich przechowywanie było niedozwolone lub gdy wiedza ich dotycząca nie jest potrzebna do wykonywania zadań przez BFV. Usunięcie danych powinno być wstrzymane, jeśli jest prawdopodobne, że ich zniszczenie może spowodować szkodę dla podmiotu. W takim przypadku te dane powinny być zablokowane. Ich przekazanie może jednak nastąpić tylko za zgodą podmiotu danych.

2.11. Wymiana danych z zagranicznymi służbami wywiadowczymi

BfV – w celu współpracy z organami obcych państw, którym powierzono zadania w sferze wywiadowczej, oraz dla celów prowadzonych czynności, które są związane z określonymi zdarzeniami lub grupami osób – może wymieniać informacje, jeśli:

1) jest niezbędna weryfikacja informacji o możliwym istnieniu poważnego zagrożenia bezpieczeństwa Republiki Federalnej Niemiec oraz innego państwa,
2) w innym państwie gwarantuje się przestrzeganie podstawowych zasad konstytucyjnych;
3) zobowiązania i postanowienia, o których mowa w § 5 zd. 1, są odpowiednio uregulowane (cele współpracy i dalsze wykorzystanie danych zostało określone w formie pisemnej, przed rozpoczęciem współpracy między służbami);
4) Ministerstwo Spraw Wewnętrznych udzieliło zgody.

Współpraca BfV ze służbą wywiadowczą państwa, które nie jest państwem członkowskim UE ani NATO, jest możliwa, jeśli wymagają tego szczególne interesy bezpieczeństwa. Są to przypadki czynności prowadzonych w celu zapobieżenia popełnieniu poważnych przestępstw przeciwko istnieniu lub bezpieczeństwu państwa lub organizacji międzynarodowej. Uczestnictwo takiej służby wywiadowczej wymaga jednak zgody ministra spraw wewnętrznych RFN.

Cele współpracy ze służbami zagranicznymi oraz dalsze wykorzystywanie przekazywanych informacji są regulowane w formie pisemnej przed rozpoczęciem tej współpracy, dzięki czemu jest zagwarantowany odpowiedni poziom ochrony tych informacji i zostają wyeliminowane przypadki ich niewłaściwego wykorzystania, zwłaszcza:

1) cel przekazania danych;
2) warunki zamierzonego wykorzystania danych;
3) modyfikowanie, poprawianie i usuwanie danych;
4) zobowiązanie do:
   a) niewykorzystywania danych bez zgody służby wywiadowczej przekazującej informacje w innych celach niż wymienione w pkt 1 lub przekazania ich stronie trzeciej,
   b) poinformowania o wykorzystaniu danych, które zostały uprzednio przekazane.

Dane, o których mowa, mogą zostać wykorzystane przez służby do wspólnego przeanalizowania informacji wywiadowczych, jeśli jest to niezbędne do ochrony bezpieczeństwa.

Ponadto BFV może, zgodnie z postanowieniami ustawy, uczestniczyć we wspólnych przedsięwzięciach (forach współpracy) przy zastrzeżeniu, że dane wprowadzone przez BFV nie mogą zostać przekazane stronie trzeciej bez zgody BFV i że mogą zostać wykorzystane wyłącznie w celach, w jakich zostały przekazane.

SZWAJCARIA

1. Federalna Służba Wywiadowcza (ang. Federal Intelligence Service – FIS)[35]

Federalna Służba Wywiadowcza istnieje od 1 stycznia 2010 r.[36] Powstała w następstwie decyzji Parlamentu Konfederacji Szwajcarskiej z kwietnia 2009 r. przez połączenie dwóch poprzednich służb – Służby Wywiadu Strategicznego (Strategic Intelligence Sernice, SIS), która w zakresie swoich właściwości zajmowała się sprawami międzynarodowymi, oraz Służby Analiz i Działań Zapobiegawczych (Service for Analysis and Prevention, SAP), odgrywającej zasadniczą rolę w zapewnianiu bezpieczeństwa wewnętrznego.

Działalność informacyjna FIS jest skierowana przede wszystkim do Rady Federalnej, departamentów oraz kantonów i ma na celu dostarczanie tym podmiotom informacji na najwyższym poziomie. Jednocześnie zarówno odbiorcy, jak i opinia publiczna muszą wiedzieć, jakie są podstawowe możliwości i ograniczenia FIS.

Zgodnie z definicją prezentowaną przez omawianą służbę FIS[37] to organizacja wykorzystująca instrumenty wywiadowcze do gromadzenia, analizowania, oceny i rozpowszechniania informacji w celu przygotowywania wszechstronnego zestawu informacji wywiadowczych, istotnych dla decydentów na wszystkich poziomach władzy.

Pod niżej przywołanymi pojęciami użytymi w definicji FIS należy rozumieć:

1) stosowanie instrumentów wywiadowczych – narzędzia gromadzenia informacji, które nie są dostępne dla innych instytucji federalnych;
2) istotne dla decydentów – FIS dostarcza informacji wywiadowczych najwyższym urzędnikom na szczeblu politycznym oraz wojskowym w celu wspomagania ich w procesie podejmowania decyzji;
3) działania prewencyjne – zestaw działań polegających na wykrywaniu i zwalczaniu wszystkich czynów, które zagrażają bezpieczeństwu państwa (na wczesnym etapie), przed zmaterializowaniem się zagrożenia i przed wystąpieniem podstaw do wszczęcia postępowania karnego.

FIS monitoruje rozwój wypadków i zagrożeń, sporządza oceny sytuacji, wydaje powiadomienia i ostrzeżenia w sytuacji narastających kryzysów lub nagłych wydarzeń. Dostarcza też odpowiednim organom informacje, które są niezbędne do ochrony istotnych interesów państwa, zapewnienia wewnętrznego oraz zewnętrznego bezpieczeństwa państwa i jego obywateli, a także organów bezpieczeństwa i ochrony porządku publicznego oraz zobowiązań międzynarodowych.

Istotnym narzędziem stosowanym przez FIS jest tzw. radar sytuacyjny (ang. *Situation Radar Tool*) stosowany w celu przedstawienia zagrożeń, na które jest narażone państwo szwajcarskie. Ten instrument wyraźnie wskazuje, za pomocą diagramu i załączonej do niego instrukcji szczegółowej, które zagrożenia bezpieczeństwa Szwajcarii są aktualnie uznawane przez FIS i inne agencje za najbardziej istotne lub mogące się zintensyfikować w najbliższej oraz dalszej przyszłości. Diagram w kształcie koła przed-

[35] Niem. Nachrichtendienst des Bundes (NDB). Podstawa prawna: *Loi du 30 mars organisant l'identification numérique des personnes physiques et morales* [online], www.legilux.public.lu/eli/etat/leg/loi/1979/03/30/n1/jo [dostęp: 19 IV 2017].

[36] *Swiss Confederation. The Federal Intelligence Service FIS* [online], s. 3. www.vbs.admin.ch/en/ddps/organisation/adminsitrative-units/intelligence-service.html [dostęp: 10 II 2017].

[37] Tamże, s. 5.

stawia zagrożenia w takich dziedzinach, jak polityka, gospodarka, obrona narodowa, proliferacja, prowadzenie nielegalnych działań wywiadowczych, zagrożeń w cyberprzestrzeni, ekstremizmu i terroryzmu. Jednocześnie poziom gradacji zagrożenia został określony w następujący sposób: od poziomu ukrytego zagrożenia przez wczesne ostrzeżenie dzięki otrzymaniu istotnych informacji aż do punktów krytycznych[38].

Oceny sytuacji przygotowywane przez FIS cechują się polityczną neutralnością i mogą różnić się od ocen sytuacji przygotowywanych przez inne agendy rządowe. Ich zasadniczym celem jest wzmocnienie oraz podniesienie poziomu procesu decyzyjnego najważniejszych organów w państwie.

Przez wykrywanie zagrożeń lub wyzwań, w których obliczu staje państwo szwajcarskie, FIS, przekazując informacje wyprzedzające o możliwych sytuacjach kryzysowych czy dostarczając raporty stanowiące oceny możliwego przebiegu wydarzeń w zakresie bezpieczeństwa, zapewnia podstawy politycznego procesu decyzyjnego. Powyższe wspomaga oraz wzmacnia swobodę szwajcarskiego rządu w działaniach.

Na poziomie federalnym FIS przekazuje rezultaty swojej pracy przede wszystkim Radzie Federalnej, departamentom, organom odpowiedzialnym za bezpieczeństwo (np. Komitetowi Bezpieczeństwa Rady Federalnej i Podstawowej Grupie ds. Bezpieczeństwa) oraz dowództwu sił zbrojnych. Służba regularnie zapewnia odbiorcom swoich informacji możliwość ich bieżącego oceniania ich zawartości pod kątem ich liczby, jakości, punktualności dostarczania, znaczenia oraz użyteczności.

FIS wspomaga również kantony w realizacji zadań w zakresie zapewniania bezpieczeństwa wewnętrznego oraz wspierania organów bezpieczeństwa i ochrony porządku publicznego na poziomie federalnym. Przekazuje także informacje (dotyczące np. eksportu materiałów wojennych i innych produktów kontrolowanych) organom federalnym i władzom kantonów. Służba wspomaga też kontrwywiadowczo instytucje rządowe i podmioty prywatne oraz prowadzi działania edukacyjno-uświadamiające dotyczące ujawniania obchodzenia lub zapobiegania obchodzeniu zobowiązań międzynarodowych w szwajcarskim sektorze finansowym i przemysłowym. FIS informuje również parlament, kantony oraz opinię publiczną o sytuacji zewnętrznej i wewnętrznej dotyczącej bezpieczeństwa[39].

Federalna Służba Wywiadowcza gromadzi i analizuje informacje, których inne agencje federalne, stosownie do ich kompetencji określonych regulacjami prawnymi oraz faktycznych możliwości, nie są w stanie uzyskać samodzielnie. Powyższe uwzględnia także informacje dostępne publicznie.

FIS jest jedyną agencją federalną mającą ustawowe kompetencje do zbierania, zarówno w Szwajcarii, jak i za granicą, informacji, które:

1) nie są publicznie dostępne,
2) podmioty rządowe oraz pozarządowe usiłują utrzymywać w tajemnicy,
3) których gromadzenie może pociągnąć za sobą naruszenie praw podstawowych (osobistych), chronionych zgodnie ze standardami praw człowieka lub zgodnie z prawem konstytucyjnym.

Powyższe uprawnienia są wykorzystywane wyłącznie w ramach wynikających z obowiązującego prawa oraz zgodnie z zasadą proporcjonalności działań podejmowanych przez państwo. Dodatkowo – poza uzyskiwaniem informacji od organów federalnych i kantonów – FIS korzysta również ze źródeł otwartych (ang. *open source intelli-*

[38] Tamże, s. 6.
[39] Tamże, s. 7.

gence – OSINT), a także dysponuje innymi środkami i metodami gromadzenia danych. Wśród powyższych należy wskazać źródła osobowe (ang. *human intelligence* – HUMINT), bieżący nasłuch radiowy i telekomunikacyjny (ang. *comunnications intelligence* – COMINT) oraz wymianę informacji z zagranicznymi służbami partnerskimi. Ponadto informacji wykorzystywanych następnie przez FIS dostarczają również szwajcarscy attaché wojskowi przebywający za granicą.

Gromadzenie i analiza informacji uzyskiwanych na szeroką skalę pozwala na wyłowienie cennych danych wywiadowczych, poza informacjami uzyskanymi z szeroko dostępnych źródeł. Informacje zdobyte z wykorzystaniem pracy wywiadowczej często odgrywają podstawową rolę w uzupełnianiu danych, które są dostępne publicznie. FIS stwarza obraz sytuacji, który został pod względem metodycznym drobiazgowo sprawdzony. Ponadto wydaje komunikaty o prawdopodobnym rozwoju wydarzeń dotyczących bezpieczeństwa oraz wykrywa dezinformację[40].

1.1. Ramy prawne oraz polityczne

FIS wykonuje swoje zadania, działając wyłącznie na podstawie szwajcarskiego prawa. Podstawami jej funkcjonowania są: konstytucja i ustawa, przy czym zasada legalności znajduje zastosowanie do działalności tej służby bez żadnych ograniczeń.

Dotychczas funkcje oraz działania FIS są szczegółowo regulowane w dwóch ustawach:

- *Ustawie federalnej z dnia 3 października 2008 r. o odpowiedzialności w obszarze cywilnej służby wywiadowczej (ZNDG; SR121).* Ta ustawa zasadniczo odnosi się do gromadzenia informacji wywiadowczych dotyczących państw obcych (bezpieczeństwo zewnętrzne). Zgodnie z tym dokumentem rolą FIS jest zbieranie informacji na temat państw obcych, które mogą mieć istotne znaczenie dla bezpieczeństwa Szwajcarii. Na służbę nałożono również obowiązek wszechstronnej oceny aktualnych zagrożeń;
- *Ustawie federalnej z dnia 21 marca 1997 r. o działaniach w celach zabezpieczenia bezpieczeństwa Wewnętrznego* – BWIS; SR 120. Ustawa nakładała na rząd federalny oraz na FIS następujące zadanie w związku z bezpieczeństwem wewnętrznym: wprowadzenie w życie środków zapobiegawczych służących wykrywaniu i zwalczaniu zagrożeń, którymi są: terroryzm, nielegalny wywiad (obcy), ekstremizm z użyciem przemocy i proliferacja;

Prace nad nową ustawą o służbie wywiadowczej[41] toczyły się od października 2010 r. Została ona uchwalonej przez parlament[42] z datą wejścia w życie 1 września 2017 r. Ma ona zastąpić obie dotychczas obowiązujące ustawy, czyli ZNDG oraz BWIS. Zgodnie z jej postanowieniami planuje się wprowadzenie (podlegające jednakże restrykcjom) specjalnych środków gromadzenia informacji wywiadowczych w Szwajcarii (monitorowanie poczty oraz ruchu telekomunikacyjnego, obserwacji osób podejrzanych – także w pomieszczeniach prywatnych – infiltracja komputerów i sieci)[43].

[40] Tamże, s. 8.

[41] *Bundesgesetz über den Nachrichtendienst* (*Nachrichtendienstgesetz*, NDG) z 25 sierpnia 2015 r., [online], www.Admin.ch/opc/de/federal-gazette/2015/7211.pdf [dostęp: 10 II 2017]. Ang. *Federal Act on Intelligence Service* (*Intelligence Service Act*, ISA).

[42] W dniu 25 września 2016 r. odbyło się ogólnokrajowe referendum na temat jej przyjęcia, w którym większość obywateli odpowiedziała się za przyjęciem ustawy.

[43] *Swiss Confederation. The Federal Intelligence*…, s. 10.

1.2. Podstawowe zasady polityki Rady Federalnej dotyczące służb wywiadowczych

W zakresie zdefiniowanym przez konstytucję i ustawę polityka Rady Federalnej określa warunki i podstawowe zasady, zgodnie z którymi służby wywiadowcze wypełniają swój mandat. Należy pamiętać, że polityka bezpieczeństwa Szwajcarii jest wspólnym zadaniem Konfederacji Szwajcarskiej, kantonów oraz gmin.

1.3. Nowe prawo federalne (Ustawa o Federalnej Służbie Wywiadowczej)[44]

Rozdział I – *Ogólne przepisy oraz zasady zbierania informacji* (art. 1–5).

W niniejszym rozdziale wskazano, że zgodnie z ustawą FIS może współpracować przy wykonywaniu zadań z innymi organami federalnymi, kantonami oraz sektorem prywatnym. Służba podlega również kontroli politycznej oraz nadzorowi nad prowadzonymi działaniami wywiadowczymi. Jako cel ustawy wskazano ochronę ważnych interesów narodowych. Wymieniony akt prawny przewiduje zapewnienie podstaw demokratycznych i konstytucyjnych Szwajcarii, ochronę wolności obywateli oraz zapewnienie bezpieczeństwa szwajcarskiemu społeczeństwu, w tym obywatelom tego kraju przebywającym za granicą. Ustawa ma się też przyczyniać do utrzymania bezpieczeństwa międzynarodowego. Innym zadaniem FIS wynikającym z ustawy jest ochrona ważnych interesów międzynarodowych, rozumianych jako:

1) ochrona fundamentów konstytucyjnych Szwajcarii;
2) wspieranie szwajcarskiej polityki zagranicznej;
3) ochrona interesów finansowych, przemysłowych i gospodarczych Szwajcarii.

Ustawa określa również, wobec kogo się ją stosuje. Wśród tych podmiotów wymieniono między innymi władze federalne, kantony, a także podmioty prywatne i publiczne[45].

W przepisach ustawy określono zasady zbierania informacji. Ustawa reguluje, że FIS nie jest zobowiązana do przekazywania informacji do wiadomości publicznej. Gromadząc informacje, FIS wykorzystuje źródła zarówno dostępne, jak i niedostępne publicznie. Stosuje środki pozyskiwania informacji, które wymagają lub nie wymagają autoryzacji i które są najbardziej odpowiednie i konieczne do osiągnięcia konkretnego celu, a jednocześnie najmniej ingerują w podstawowe prawa zainteresowanych osób. Jednocześnie FIS ma prawo do pozyskiwania danych dotyczących osób, wobec których są stosowane środki służące zbieraniu informacji bez ich wiedzy i zgody. FIS nie gromadzi ani nie przetwarza żadnych informacji odnoszących się do działalności politycznej lub swobody wyrażania opinii, swobody stowarzyszania się lub zrzeszania w Szwajcarii. W wyjątkowych sytuacjach może pozyskiwać dane dotyczące działalności politycznej lub swobody wyrażania opinii, swobody stowarzyszania się lub zrzeszania w Szwajcarii, dotyczące osób i podmiotów publicznych i prywatnych, jeśli posiada informacje wzbudzające uzasadnione podejrzenie, że wymienione osoby lub podmioty przygotowują lub prowadzą działalność terrorystyczną, szpiegowską albo związaną z radykalnym ekstremizmem. Jeżeli w ciągu jednego roku od momentu zdobycia takich informacji nie zostaną one potwierdzone, FIS usuwa wszelkie dane w tym zakresie; usuwa je niezwłocznie, jeżeli okaże się, że te podejrzenia są nieuzasadnione. FIS może ponadto pozyskiwać

[44] *Bundesgesetz über den Nachrichtendienst…*
[45] Tamże.

i przetwarzać informacje w rozumieniu pkt 5 (działalność polityczna lub dotycząca swobody wyrażania opinii, swobody stowarzyszania się lub zrzeszania w Szwajcarii), dotyczące wpisanych na listę organizacji i podmiotów pozostających w kręgu zainteresowań (tzw. lista osób i podmiotów obserwowanych[46]), o których mowa w art. 72. Na wyżej wymienionej liście znajdują się organizacje i grupy, w stosunku do których istnieje uzasadnione podejrzenie, że zagrażają bezpieczeństwu wewnętrznemu lub zewnętrznemu państwa. Akceptację na objęcie podmiotów lub osób wpisem wydaje się wtedy, gdy dana organizacja lub ugrupowanie widnieje w wykazie Organizacji Narodów Zjednoczonych lub Unii Europejskiej. Jednocześnie organizacja lub grupa jest usuwana z listy osób i podmiotów obserwowanych, kiedy wygasa podstawa, jaką jest zagrożenie bezpieczeństwa wewnętrznego i zewnętrznego państwa, które może stwarzać, oraz w przypadku, gdy zostaje usunięta z wykazu Organizacji Narodów Zjednoczonych lub Unii Europejskiej. Dotyczy to również informacji o osobach reprezentujących wymienione podmioty lub osoby obserwowane, jeżeli pozwalają one na ocenę zagrożenia stwarzanego przez te organizacje lub podmioty[47].

Rozdział II – *Zadania oraz współpraca FIS* (art. 6–8).

W tym rozdziale określono zadania FIS. Wskazano, że gromadzenie i przetwarzanie informacji przez tę służbę następuje w celu:

1) wczesnego wykrywania i zapobiegania zagrożeniom wewnętrznego lub zewnętrznego bezpieczeństwa państwa związanego z:
a) terroryzmem,
b) nielegalną działalnością wywiadowczą,
c) proliferacją broni jądrowej, biologicznej lub chemicznej, w tym środków do jej przenoszenia i wszystkich dóbr oraz technologii przeznaczonych do celów cywilnych lub wojskowych, niezbędnych do ich wytworzenia,
d) nielegalnym handlem materiałami radioaktywnymi, wojskowymi i innymi środkami uzbrojenia,
e) atakami na infrastrukturę informatyczną, komunikacyjną, energetyczną i transportową, a także inną infrastrukturę niezbędną do funkcjonowania społeczeństwa, gospodarki lub państwa (infrastruktura krytyczna),
1) ekstremizmem z użyciem przemocy;
1) wykrywania, monitorowania i oceny istotnych wydarzeń dotyczących polityki bezpieczeństwa, do których dochodzi za granicą;
2) zabezpieczania zdolności państwa do działania;
3) ochrony innych ważnych interesów narodowych, na wyraźne polecenie Rady Federalnej;
4) oceny sytuacji pod kątem ewentualnego zagrożenia i poinformowania organów państwowych, kantonów, organów ścigania o wszelkich zagrożeniach i środkach podjętych, a także planowanych działaniach w ramach niniejszej ustawy;
5) informowania innych agend federalnych i kantonów, przy zachowaniu ochrony źródeł, o zdarzeniach i ustaleniach dotyczących utrzymania bezpieczeństwa wewnętrznego lub zewnętrznego;
6) zapewniania wczesnego ostrzegania w celu ochrony infrastruktury krytycznej;

[46] Ang. *watchlist*.
[47] *Bundesgesetz über den Nachrichtendienst*…

7) utrzymywania relacji z zagranicznymi służbami wywiadowczymi;
8) prowadzenia programów profilaktycznych w zakresie uświadamiania o zagrożeniach bezpieczeństwa wewnętrznego lub zewnętrznego;
9) ochrony swoich pracowników lub funkcjonariuszy w instytucjach, ochrony źródeł i przetwarzanych informacji od nich pochodzących.

FIS podejmuje środki w celu zagwarantowania ochrony i bezpieczeństwa współpracujących z nim osób, ich danych oraz wyposażenia, a także może w tym celu podejmować następujące środki:

- dokonywać przeszukań osób wymienionych poniżej oraz ich mienia w lokalach należących do FIS:
  – osób współpracujących z FIS,
  – osób zatrudnionych w FIS na czas określony,
  – współpracowników przedsiębiorstw świadczących usługi w lokalach należących do FIS.

FIS może dodatkowo przeprowadzać kontrolę systemów w celu zapewnienia poszanowania przepisów o ochronie informacji niejawnych, prowadzić system nadzoru wizyjnego w archiwach oraz stref dostępu do swoich pomieszczeń. Wykorzystuje ponadto zabezpieczoną sieć informatyczną do zarządzania systemami informatycznymi, do których mają dostęp wyłącznie jej funkcjonariusze. Funkcjonariusze FIS podczas wykonywania swoich zadań w Szwajcarii mogą nosić broń, pod warunkiem, że realizowane przez nich obowiązki narażają ich na poważne ryzyko. Uzbrojeni funkcjonariusze FIS mogą używać broni wyłącznie w ramach obrony koniecznej lub w stanie wyższej konieczności, w sposób proporcjonalny do zagrożenia[48].

1.4. Nadzór i kontrola nad FIS[49]

Aktywność FIS podlega kontroli na różnych poziomach. Kontrola jest prowadzona przez następujące organy władzy wykonawczej:

1) Władzę Kontrolną Służby Wywiadowczej w Federalnym Departamencie Obrony, Ochrony Cywilnej i Sportu (DDPS), która sprawdza legalność, właściwość i skuteczność czynności podejmowanych przez FIS. Podczas kontroli są jednak brane pod uwagę priorytety wywiadowcze, które są określane przez polityczny szczebel decyzyjny państwa;
2) Niezależną Władzę Kontrolną będącą komitetem międzydepartementalnym (międzyministerialnym) weryfikującym legalność oraz proporcjonalność stosowania narzędzi wywiadowczych w odniesieniu do komunikacji (COMINT);
3) Komisarza Federalnego ds. Ochrony Danych Osobowych, który sprawdza legalność przetwarzania danych osobowych zbieranych w Szwajcarii;
4) Radę Federalną, która kieruje sprawami mającymi zasadnicze znaczenie polityczne oraz je kontroluje, a zwłaszcza przydziela podstawowe zadania, zatwierdza tzw. *watchlist* (listę podmiotów i osób obserwowanych). Wybiera również członków Niezależnej Władzy Kontrolnej i autoryzuje oraz nadzoruje kontakty międzynarodowe ze służbami zagranicznymi.

Poza kontrolą sprawowaną przez władzę wykonawczą prowadzona jest również kontrola parlamentarna. Delegacja Kontrolna Szwajcarskiego Parlamentu Federalnego

[48] Tamże.
[49] *Swiss Confederation. The Federal Intelligence*…, s. 11–12.

monitoruje legalność, właściwość oraz skuteczność działań służby oraz dysponuje wieloma instrumentami do dokonywania inspekcji. FIS jest ponadto corocznie poddawana audytowi przez Biuro Audytu, które działa z upoważnienia Delegacji Finansowej Szwajcarskiego Parlamentu Federalnego.

Jednocześnie kontrola FIS dotyczy również ochrony danych osobowych. Na podstawie wielu regulacji prawnych (dotychczasowych ustaw: BWIS, ZNDG i ustawy o ochronie danych osobowych) FIS jest upoważniona do zbierania, przetwarzania i przechowywania danych osobowych w celu zapewnienia bezpieczeństwa Szwajcarii oraz jej obywateli. Zarówno władze ustawodawcze, jak i organy nadzorcze określają wyraźne wytyczne dla FIS, które mają zagwarantować prawa konstytucyjne szwajcarskich obywateli i zapewnić równowagę między bezpieczeństwem a podstawowymi prawami mieszkańców.

Każdy obywatel może złożyć do FIS wniosek w formie pisemnej dotyczący udostępnienia mu danych pochodzących z zasobów systemów informatycznych służby. Służba, o której mowa, może w określonych wypadkach odmówić udostępnienia takich danych (odmowa realizacji wniosku).

1.5. Informacja o działalności FIS przekazywana opinii publicznej[50]

Władze, organy kontrolne i FIS informują opinię publiczną o swojej aktywności na tyle transparentnie, na ile jest to możliwe, jednakże w taki sposób, aby nie zagroziło to działaniom wywiadowczym. Ochrona źródeł jest regulowana w prawie wewnętrznym i jest przestrzegana w każdym przypadku.

FIS sporządza oficjalne raporty, m.in.:

1) raport roczny – Rada Federacji informuje parlament, kantony i opinię publiczną o swojej ocenie sytuacji oraz o stanie zagrożeń i działaniach podejmowanych przez federalne agencje bezpieczeństwa (w tym przez FIS). Tematy podejmowane w tych raportach odnoszą się do ustawowej działalności FIS;
2) coroczny raport sytuacyjny *Bezpieczeństwo Szwajcarii* – FIS publikuje taki raport także wraz z diagramem – radarem sytuacyjnym. Powyższy raport nie jest ograniczony wyłącznie do polityki bezpieczeństwa w wąskim znaczeniu, ale dotyczy też innych zagrożeń, które mogłyby spowodować znaczną szkodę dla państwa;
3) raport o aktywności służb wywiadowczych – Delegacja Kontrolna regularnie wydaje tego typu raport parlamentowi i opinii publicznej.

1.6. Zaangażowanie w zarządzanie polityką bezpieczeństwa[51]

FIS dostarcza wszechstronnej oceny i opisu sytuacji w obliczu zagrożeń.

W ramach Podstawowej Grupy Bezpieczeństwa służba przekazuje informacje niezbędne do dokonania wspólnej oceny sytuacji departamentom, które są reprezentowane w wymienionej Grupie. Kompetencje Podstawowej Grupy Bezpieczeństwa dotyczą monitorowania zagrożeń bezpieczeństwa wewnętrznego oraz zewnętrznego państwa, a także oceny sytuacji i wczesnego wykrywania zagrożeń.

Grupa, o której mowa, analizuje sytuację dotyczącą bezpieczeństwa i w razie potrzeby przedkłada propozycje do odpowiednich komitetów Rady Federacyjnej. W skład

[50] Tamże, s. 13.
[51] Tamże. s. 14.

Podstawowej Grupy Bezpieczeństwa wchodzą: Sekretarz Stanu (FDFA), Dyrektor Fedpol (FDJP) oraz Dyrektor FIS (DDPS). W ramach Grupy działa również podgrupa koordynacyjna wraz z przewodniczącym, w której skład wchodzą: przedstawiciel FIS, przedstawiciel Fedpol oraz przedstawiciel FDFA.

Należy podkreślić, że FIS blisko współpracuje z policjami kantonów w zakresie prewencyjnym, jednak zapewnianie bezpieczeństwa wewnętrznego na poziomie regionalnym jest zadaniem samych kantonów. Służba zapewnia ponadto kantonom wsparcie podczas znaczących wydarzeń (takich jak np. Światowe Forum Ekonomiczne w Davos czy konferencje międzynarodowe) przez narodową sieć wywiadowczą prowadzoną przez Federacyjne Centrum Sytuacyjne (FSC).

1.7. Współpraca z władzami federalnymi i kantonalnymi[52]

FIS współpracuje także z Biurem Prokuratora Generalnego i z Federalną Policją Kryminalną. Zarówno postępowania wywiadowcze, jak i postępowania karne są wszczynane na podstawie określonych przesłanek. W przypadku działań zapobiegawczych, które są prowadzone przez służby wywiadowcze, będą to przesłanki związane z możliwością wystąpienia istotnego zagrożenia bezpieczeństwa Szwajcarii lub jej społeczeństwa. Natomiast w przypadku służb policyjnych będzie to podejrzenie popełnienia określonego przestępstwa natury karnej.

W związku z kompetencjami, jakie obecnie ma FIS, służba musi polegać na bliskiej współpracy z organami policyjnymi na poziomie federalnym i kantonalnym. W służbach policyjnych kantonów istnieją 84 jednostki wywiadowcze, umiejscowione tam przez władze federalne i działające na poziomie kantonów.

Do kompetencji FIS należy kontrola wniosków o wjazd na terytorium Szwajcarii i pobyt w tym kraju pod kątem ewentualnego zagrożenia bezpieczeństwa państwa (również akredytacja dyplomatów, przedstawicieli organów międzynarodowych, wnioski o zatrudnienie cudzoziemców). FIS bierze również udział w procedurze konsultacyjnej Schengen (procedura VISION) oraz sprawdza wszelkie rejestry pod kątem zagrożenia bezpieczeństwa wewnętrznego Szwajcarii. Sprawdza także bazy danych dotyczące azylantów oraz wnioski cudzoziemców, którzy chcą przyjąć szwajcarskie obywatelstwo. W zakresie, w jakim występują poważne obawy o bezpieczeństwo państwa i obywateli, wnioski, o których mowa, mogą zostać odrzucone, jeśli taki środek jest konieczny, aby uniemożliwić wjazd na terytorium państwa osobie mogącej stanowić zagrożenie.

FIS jest również odpowiedzialne – na poziomie federalnym – za zapobieganie atakom na infrastrukturę krytyczną. Centrum Raportów i Analiz do Zapewnienia Informacji (ang. The Reporting and Analysis Centre for Information Assurance – MELANI) jest kierowane wspólnie przez Federalną Jednostkę Sterującą (FITSU) oraz FIS. Odpowiedzialność za strategiczne zarządzanie MELANI i za aspekty techniczne spoczywa na FITSU, podczas gdy odpowiedzialność za operacyjne jednostki wywiadowcze MELANI spoczywa na FIS. Zadaniem MELANI jest zapewnianie: wsparcia w zakresie ochrony infrastruktury Szwajcarii przez realizację procedur zapewniających przekazywanie informacji, w celu prowadzenia działań prewencyjnych (w przypadku incydentów IT oraz współkoordynujących), które mają zapewnić ciągłość infrastruktury informacyjnej, tak aby funkcjonowała łączność z podmiotami prywatnymi. W celu osiągnięcia powyższego

[52] Tamże, s. 15–17.

zamierzenia, MELANI i operatorzy szwajcarskiej infrastruktury krytycznej współpracują na zasadzie dobrowolnej w ramach partnerstwa publiczno-prywatnego.

1.8. Współpraca z zagranicznymi służbami partnerskimi[53]

Rozwijanie relacji międzynarodowych jest nieodłączną oraz zasadniczą częścią pracy FIS. Służba wykorzystuje takie kontakty, aby uzupełnić wiedzę w tych obszarach, które tego wymagają, dzięki czemu może wykonywać swoje zadania ustawowe w zakresie działań prewencyjnych, oceny sytuacji dotyczącej zagrożenia zewnętrznego i realizacji międzynarodowych zobowiązań Szwajcarii w sposób skuteczny. Relacje FIS z partnerami zagranicznymi są regulowane przez prawo. Rada Federacji udziela zgody na standardowe relacje ze służbami zagranicznymi corocznie. Jednocześnie FIS może utrzymywać kontakty z organizacjami oraz stowarzyszeniami międzynarodowymi.

FIS jest szczególnie zaangażowana w stałą współpracę z licznymi zagranicznymi służbami partnerskimi i organizacjami międzynarodowymi (np. z EU's Joint Situation Centre – INTCEN). Tego typu współpraca ma charakter nieformalny i jest oparta na zasadzie poufności i wzajemnego zaufania. Wymiana informacji jest możliwa zgodnie z zasadą wspólnych interesów. Informacje są jednak wymieniane fakultatywnie.

1.9. Organizacja[54]

Na czele struktury FIS stoi dyrektor, któremu podlega Biuro Obsługi (ang. Staff), a im – poszczególne piony służbowe. Biuro Obsługi zajmuje się sprawami dotyczącymi kompleksowej pracy FIS, w tym współpracy międzynarodowej z partnerami zagranicznymi, pełni funkcje kontrolne oraz jest odpowiedzialne za całościowe zarządzanie działalnością służby. Zarządza również wewnętrznym i zewnętrznym sposobem komunikacji.

[53] Tamże, s. 18.
[54] Tamże, s. 22–23.

CZĘŚĆ II

Definicje pojęć szpiegostwo i terroryzm

BELGIA

1. Ustawa o służbach wywiadowczych i bezpieczeństwa[1] (fragmenty)

Szpiegostwo – pozyskiwanie lub dostarczanie informacji niedostępnych publicznie oraz ułatwianie lub przygotowywanie tych czynności (art. 8 § 1 pkt a ustawy).

Terroryzm – użycie przemocy wobec osób lub dóbr materialnych z przyczyn ideologicznych lub politycznych w celu uzyskania określonych efektów przez stosowanie terroru, zastraszenia lub gróźb (art. 8. § 1 pkt b).

Ekstremizm – ideologia lub koncepcja o charakterze rasistowskim, ksenofobicznym, anarchistycznym, nacjonalistycznym, autorytarnym lub totalitarnym, wykorzystywana w wymiarze politycznym, ideologicznym, wyznaniowym lub filozoficznym, sprzeczna, w teorii i w praktyce, z zasadami demokracji i prawami człowieka, poprawnym funkcjonowaniem instytucji demokratycznych lub z innymi fundamentami państwa prawa (art. 8 § 1 pkt c).

Ustawa zawiera również definicję pojęcia proces radykalizacji. Zgodnie z art. 3 pkt 15 jest to proces wpływający na osobę fizyczną lub grupę osób w taki sposób, stają się one mentalnie przygotowane do dokonania aktu o charakterze terrorystycznym.

Zgodnie z art. 7 i 8 ustawy działalność kontrwywiadowcza jest jednym z elementów definicji działalności zagrażającej lub mogącej stanowić zagrożenie państwa, trwałości porządku demokratycznego itp. Zgodnie z art. 8 pod tym pojęciem należy rozumieć każdą działalność, indywidualną lub zbiorową, prowadzoną wewnątrz kraju lub inspirowaną z zewnątrz, która może mieć związek ze szpiegostwem, ingerencją zewnętrzną, terroryzmem, ekstremizmem, proliferacją broni masowego rażenia, działalnością organizacji radykalnych, grupami przestępczymi, w tym z propagandą, bezpośrednim lub pośrednim wsparciem wymienionych rodzajów działalności, zwłaszcza przez udzielanie środków finansowych, technicznych i logistycznych, udzielanie informacji o możliwych celach, rozwój struktur oraz zwiększanie potencjału tego rodzaju działalności.

Zbieżność znaczeniową z pojęciem szpiegostwo wykazuje również definicja ingerencji, określona w art. 8 pkt g ustawy jako dążenie do wywarcia wpływu na procesy decyzyjne przy wykorzystaniu nielegalnych, niejawnych metod lub przez wykorzystywanie nieprawdziwych informacji.

Art. 7 ustawy, określający zadania VSSE, został skonstruowany w sposób analogiczny do art. 5 pkt 1 ust. 4 ustawy o ABW oraz AW. Zgodnie z treścią przywołanego przepisu do zadań VSSE należy pozyskiwanie, analizowanie i przetwarzanie informacji o wszelkiego rodzaju działalności zagrażającej lub mogącej zagrażać określonym dobrom – m.in. integralności terytorialnej oraz potencjałowi naukowemu i gospodarczemu.

[1] *Loi organique des services de renseignement et de sécurité, 30 novembre 1998* [online], www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032 [dostęp: 14 II 2017].

Kodeks karny

Terroryzm (przepisy dotyczące terroryzmu zostały dodane do kodeksu na podstawie *Ustawy z dnia 19 grudnia 2003 roku o przestępstwach terrorystycznych*)[2]

Art. 137 § 1. Przestępstwo określone w § 2 i 3, które przez swój charakter lub okoliczności, w jakich zostało popełnione, może stwarzać poważne zagrożenie państwu lub organizacji międzynarodowej i które zostało popełnione umyślnie w celu poważnego zastraszenia ludności lub bezprawnego zmuszenia organów publicznych albo organizacji międzynarodowej do określonego działania lub zaniechania, albo które może spowodować poważną destabilizację fundamentalnych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych państwa albo organizacji międzynarodowej stanowi przestępstwo o charakterze terrorystycznym.

§ 2. Następujące przestępstwa stanowią przestępstwo o charakterze terrorystycznym, z zastrzeżeniem warunków określonych w § 1:

1) umyślne zabójstwo lub spowodowanie uszczerbku na zdrowiu;
2) wzięcie zakładnika określone w art. 347 bis;
3) uprowadzenie określone w art. 428–430, 434–437;
4) zniszczenie lub spowodowanie poważnych uszkodzeń określonych w kodeksie karnym i dyscyplinarnym marynarki handlowej, a także w ustawie z 21 marca 1991 r. o reformie niektórych przedsiębiorstw publicznych[3], mające na celu stworzenie zagrożenia życia lub spowodowanie poważnych strat gospodarczych;
5) uprowadzenie statku powietrznego;
6) przejęcie kontroli nad statkiem wodnym przez oszustwo, przemoc lub groźby pod adresem kapitana statku, a także akty piractwa określone w art. 3 ustawy z 30 grudnia 2009 r. o zwalczaniu piractwa morskiego[4];
7) przestępstwa określone w zarządzeniu królewskim z 23 września 1958 r. regulującym wytwarzanie, magazynowanie, przechowywanie, sprzedaż, transport i sposób wykorzystywania materiałów wybuchowych;
8) przestępstwa zagrażające życiu określone w kodeksie karnym i dyscyplinarnym marynarki handlowej;
9) przestępstwa określone w ustawie o działalności gospodarczej w sektorze zbrojeniowym;
10) przestępstwa określone w ustawie z 10 lipca 1978 r. ratyfikującej *Konwencję 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 1972 r.*[5];
11) usiłowanie popełnienia jednego z przestępstw wymienionych powyżej.

[2] *Loi relative aux infractions terroristes, 19 décembre 2003* [online], www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2003121934 [dostęp: 14 II 2017].

[3] *Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* [online], www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&caller=list&cn=1867060801&la=f&fromtab=loi [dostęp: 19 IV 2017].

[4] *Loi du 30 décembre 2009 relative à la lutte contre la piraterie maritime* [online], www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&caller=list&cn=1867060801&la=f&fromtab=loi [dostęp: 19 IV 2017].

[5] Dz.U. z 1976 r. Nr 1 poz. 1 (przyp. red.).

§ 3. Przestępstwo o charakterze terrorystycznym, z zastrzeżeniem warunków określonych w § 1, stanowi:

1) zniszczenie lub spowodowanie poważnych strat albo wywołanie podtopienia infrastruktury, systemu transportu, mienia stanowiącego własność publiczną lub prywatną, których skutkiem jest zagrożenie życia lub zagrożenie wystąpienia poważnych strat gospodarczych, innych niż wymienione w § 2;
2) uprowadzenie innych środków transportu niż określone w § 2 pkt 5 i 6;
3) wytwarzanie, posiadanie, nabywanie, transport lub dostarczanie broni nuklearnej, chemicznej, wykorzystywanie broni nuklearnej, biologicznej lub chemicznej, a także prowadzenie badań i prac nad bronią chemiczną;
4) uwolnienie niebezpiecznych substancji zagrażających życiu;
5) zakłócenie lub spowodowanie przerw w dostawie elektryczności, wody lub innych surowców naturalnych o zasadniczym znaczeniu zagrażających życiu;
6) groźba popełnienia przestępstwa określonego w § 2 lub 3.

Art. 139. Związek co najmniej dwóch osób, utworzony w określonym czasie, działający w sposób zorganizowany w celu popełnienia jednego z przestępstw określonych w art. 137., który posiada strukturę, stanowi ugrupowanie terrorystyczne.

Organizacja, której rzeczywiste cele działania mają wyłącznie charakter polityczny, związkowy, dobroczynny, filozoficzny lub religijny, lub która dąży do osiągnięcia innego celu zgodnego z prawem, nie może być uznana za ugrupowanie terrorystyczne w rozumieniu § 1 niniejszego artykułu.

Art. 140. Kto uczestniczy w działaniach ugrupowania terrorystycznego przez dostarczanie informacji, środków materialnych lub finansuje jego działalność w inny sposób, wiedząc, że ten udział przyczynia się do popełnienia przestępstwa lub deliktu przez to ugrupowanie, podlega karze od 5 do 10 lat pozbawienia wolności i grzywnie w wysokości od 100 do 5000 euro.

Art. 140 bis. Z zastrzeżeniem art. 140, kto rozpowszechnia lub w jakikolwiek inny sposób prezentuje publicznie treści z zamiarem podżegania, bezpośrednio lub pośrednio, do popełnienia jednego z przestępstw określonych w art. 137–140 ze zn. 6, z wyłączeniem art. 137 § 3 pkt 6, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro.

Art. 140 ze zn. 3. Z zastrzeżeniem art. 140, kto prowadzi rekrutację w celu popełnienia jednego z przestępstw wymienionych w art. 137–140 ze zn. 6, z wyłączeniem art. 137 § 3 pkt 6, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro.

Art. 140 ze zn. 4. Z zastrzeżeniem art. 140, kto udziela instrukcji lub szkoli inne osoby w zakresie produkcji lub wykorzystywania materiałów wybuchowych, broni palnej lub innego rodzaju broni, szkodliwych lub niebezpiecznych substancji albo w zakresie innych specjalnych metod w celu popełnienia jednego z przestępstw określonych w art. 137, z wyłączeniem art. 137 § 3 pkt 6, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro.

Art. 140 ze zn. 5. Z zastrzeżeniem art. 140, osoba, która otrzymuje instrukcje lub bierze udział w szkoleniu, o którym mowa w art. 140 ze zn. 4, na terytorium Belgii lub poza jej granicami, w celu popełnienia jednego z przestępstw określonych w art. 137, z wyłączeniem art. 137 § 3 pkt 6, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro.

Art. 140 ze zn. 6. Z zastrzeżeniem art. 140, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro:

1) kto wyjeżdża za granicę w celu popełnienia, na terytorium Belgii lub poza jej granicami, przestępstwa określonego w art. 137, 140 do 140 ze zn. 5 oraz w art. 141, z wyłączeniem art. 137 § 3 pkt 6;
2) kto wjeżdża na terytorium Belgii w celu popełnienia, na terytorium Belgii lub poza jej granicami, przestępstwa określonego w art. 137, 140 do 140 ze zn. 5 oraz w art. 141, z wyłączeniem art. 137 § 3 pkt 6.

Art. 141. Kto w przypadkach innych niż określone w art. 140, dostarcza środków materialnych, w tym pomocy finansowej, w celu popełnienia przestępstwa o charakterze terrorystycznym określonego w art. 137, podlega karze od 5 do 10 lat pozbawienia wolności oraz grzywnie w wysokości od 100 do 5000 euro.

Art. 141 bis. Przepisów niniejszego tytułu nie stosuje się do działań sił zbrojnych w czasie konfliktu zbrojnego w rozumieniu międzynarodowego prawa humanitarnego ani do wykonywania ich urzędowych funkcji, w zakresie, w jakim jest to uregulowane przez inne normy prawa międzynarodowego.

Art. 141 ze zn. 3. Żaden z przepisów niniejszego tytułu nie może być interpretowany w sposób, który ograniczałby lub niweczył podstawowe prawa i wolności, takie jak prawo do strajku, swoboda zrzeszania się, swoboda zgromadzeń, w tym prawo tworzenia związków zawodowych i przystępowania do nich w celu ochrony swoich interesów, prawo do udziału w manifestacjach, swoboda wyrażania opinii, szczególnie wolność prasy i swoboda wypowiedzi w innych mediach, zgodnie normami wynikającymi z art. 8–11 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*.

FRANCJA

1. Szpiegostwo

Kodeks karny[6]. Księga IV – *Przestępstwa i delikty przeciwko narodowi, państwu i porządkowi publicznemu*. Tytuł 1 – *Zamachy na fundamentalne interesy państwa*. Rozdział 1 – *O zdradzie i szpiegostwie*

[6] *Code pénal, version consolidée au 27 janvier 2017* [online], https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 [dostęp: 14 II 2017].

Art. 410-1. Fundamentalne interesy państwa w rozumieniu niniejszego tytułu oznaczają jego niepodległość, integralność terytorialną, bezpieczeństwo, republikańską formę instytucji, obronność, dyplomację, ochronę obywateli Francji w kraju i za granicą, ochronę środowiska naturalnego oraz najważniejsze elementy jego potencjału naukowego, gospodarczego i dziedzictwa kulturowego.

Art. 411-1. Czyny określone w art. 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.

Sekcja 2: Udzielanie informacji wywiadowczych obcemu mocarstwu

Art. 411-4. 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 albo aktów agresji wobec Francji podlega karze pozbawienia wolności na 30 lat i grzywnie w wysokości 450 000 euro.

Tej samej karze podlega działanie polegające na dostarczaniu obcemu mocarstwu, przedsiębiorstwu lub innemu zagranicznemu podmiotowi albo podmiotowi znajdującemu się pod kontrolą innego państwa, lub jego agentów środków pozwalających na wywołanie nieprzyjacielskich działań albo aktów agresji wobec Francji.

Art. 411-5. Jeżeli działanie polegające na udzielaniu informacji wywiadowczych obcemu mocarstwu, przedsiębiorstwu, innemu zagranicznemu podmiotowi lub podmiotowi znajdującemu się pod kontrolą innego państwa albo jego agentów może zagrozić fundamentalnym interesom państwa, sprawca podlega karze 10 lat pozbawienia wolności lub 150 000 euro grzywny.

Sekcja 3: 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 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, rozpowszechnianie lub połączenie w całość stanowi zagrożenie fundamentalnych interesów państwa, podlega karze 10 lat pozbawienia wolności i 150 000 euro grzywny.

Art. 411-8. Prowadzenie, 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, na rachunek obcego mocarstwa, przedsiębiorstwa lub podmiotu zagranicznego albo znajdującego się pod

kontrolą innego państwa lub jego agentów podlega karze 10 lat pozbawienia wolności lub 150 000 euro grzywny.

Sekcja 4: Sabotaż

Art. 411-9. Działanie polegające na zniszczeniu, uczynieniu niezdatnym do użytku, podrobieniu lub przerobieniu dokumentu, materiału, konstrukcji, wyposażenia, instalacji, urządzenia technicznego lub zautomatyzowanego przetwarzania informacji lub wywołaniu w nich wad, jeżeli może to zagrażać fundamentalnym interesom państwa, podlega karze 15 lat pozbawienia wolności lub 225 000 euro grzywny.

Sekcja 5: Udzielenie fałszywych informacji

Art. 411-10. Udzielenie władzom cywilnym lub wojskowym Francji fałszywych informacji w celu wprowadzenia ich w błąd i wywołania zagrożenia fundamentalnych interesów państwa z zamiarem realizacji interesów obcego mocarstwa, przedsiębiorstwa lub podmiotu zagranicznego albo znajdującego się pod kontrolą innego państwa podlega karze 7 lat pozbawienia wolności lub 10 000 euro grzywny.

Art. 411-11. Podżeganie do popełnienia ww. czynów, przez składanie obietnic, ofert, wywieranie nacisku, stosowanie gróźb lub przemocy, jeżeli do popełnienia czynu nie doszło z przyczyn niezależnych od woli podżegacza, podlega karze 7 lat pozbawienia wolności lub 100 000 euro grzywny.

2. Terroryzm

Art. 421-1. Następujące czyny, jeżeli są popełnione umyślnie w związku z indywidualnym lub zbiorowym przedsięwzięciem mającym na celu poważne zakłócenie porządku publicznego przez zastraszenie lub terror, stanowią akty o charakterze terrorystycznym:

1) umyślny zamach na życie, nietykalność cielesną, uprowadzenie i bezprawne pozbawienie wolności osoby, a także uprowadzenie statku powietrznego, wodnego lub jakiegokolwiek innego środka transportu;
2) kradzież, wymuszenie, zniszczenie, uszkodzenie lub uczynienie niezdatnym do użytku mienia, a także przestępstwa przeciwko systemom informatycznym;
3) przestępstwa związane z grupami o charakterze zbrojnym i organizacjami określonymi w art. 431-13–431-17 oraz przestępstwa określone w art. 434-6 (przestępstwa przeciwko wymiarowi sprawiedliwości) i w art. 441-2–441-5 (przestępstwa przeciwko dokumentom);
4) przestępstwa związane z uzbrojeniem, materiałami wybuchowymi lub jądrowymi;
5) paserstwo związane z przestępstwami opisanymi w pkt 1–4;
6) pranie pieniędzy;
7) czyny wymienione w art. 465-1–465-3 kodeksu monetarnego i finansowego (niezgodne z prawem wykorzystanie tzw. informacji uprzywilejowanej dotyczącej instrumentów finansowych).

Art. 421-2. Czyn polegający na emisji substancji, która może stwarzać zagrożenie zdrowia osób, zwierząt lub środowiska naturalnego, stanowi akt o charakterze terrorystycznym, jeżeli jest popełniony umyślnie w związku z indywidualnym lub zbiorowym przedsięwzięciem mającym na celu poważne zakłócenie porządku publicznego przez zastraszenie lub terror.

[Związek przestępczy powiązany z działalnością terrorystyczną – dop. aut.]

Art. 421-2-1 i 421-2-2 kodeksu karnego stanowią, że udział w ugrupowaniu mającym na celu przygotowanie aktu o charakterze terrorystycznym, potwierdzony przez jeden lub większą liczbę udowodnionych faktów, a także finansowanie przedsięwzięcia terrorystycznego, zbieranie lub zarządzanie środkami finansowymi lub innego rodzaju dobrami albo udzielanie porad w celu lub ze świadomością, iż służy to działaniom terrorystycznym, niezależnie od popełnienia lub niedopełnienia przestępstwa, stanowi akt o charakterze terrorystycznym.

Art. 421-2-1. Akt o charakterze terrorystycznym stanowi udział w ugrupowaniu mającym na celu przygotowanie do popełnienia jednego z czynów o charakterze terrorystycznym wymienionych w powyższych przepisach, potwierdzonego przez jeden lub większą liczbę udowodnionych faktów.

Art. 421-2-2. Akt o charakterze terrorystycznym stanowi finansowanie przedsięwzięcia terrorystycznego przez dostarczanie i zbieranie środków finansowych lub jakiegokolwiek mienia z zamiarem lub ze świadomością, iż zostaną one wykorzystane w całości lub w części w celu dokonania jednego z aktów o charakterze terrorystycznym wymienionych w niniejszym rozdziale, niezależnie od tego, czy do tego aktu faktycznie dojdzie, a także zarządzanie nimi i doradztwo w zakresie ich wykorzystania.

Art. 421-2-3. Niemożność udowodnienia pochodzenia środków utrzymania przez osobę mającą stałe kontakty z jedną osobą lub z większą liczbą osób prowadzących działalność, o której mowa w art. 421-1 do 421-2-2, podlega karze pozbawienia wolności i 100 000 euro grzywny.

Art. 421-2-4. Składanie innej osobie propozycji, ofert, obietnic, proponowanie korzyści majątkowej lub jakiejkolwiek innej, stosowanie wobec niej gróźb lub jakiegokolwiek innego nacisku w celu skłonienia jej do udziału w ugrupowaniu, o którym mowa w art. 421-2-1, lub do udziału w popełnieniu aktów o charakterze terrorystycznym wymienionych w art. 421-1 i 421-2 podlega karze 10 lat pozbawienia wolności i 150 000 euro grzywny, nawet jeśli do tego aktu nie doszło.

Art. 421-2-5. Podżeganie do popełnienia czynu o charakterze terrorystycznym lub publiczne nawoływanie do jego popełnienia podlega karze 5 lat pozbawienia wolności lub 75 000 euro grzywny.

Kara wynosi 7 lat pozbawienia wolności i 100 000 euro grzywny, jeżeli ww. czyn został dokonany z wykorzystaniem publicznej internetowej usługi komunikacji.

Jeżeli powyższe czyny zostały dokonane w formie pisemnej lub audiowizualnej za pośrednictwem prasy, lub z wykorzystaniem publicznej internetowej usługi komunikacyjnej, ustalenie odpowiedzialności poszczególnych osób odbywa się na zasadach określonych w przepisach szczególnych.

Art. 421-2-5-1. Umyślne pozyskiwanie, odtwarzanie i transmitowanie informacji publicznie gloryfikujących akty o charakterze terrorystycznym lub nawołujących do ich popełnienia w celu zmniejszenia skuteczności procedur, o których mowa w *Ustawie z dnia 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej*[7] lub w art. 706-23 kodeksu postępowania karnego, podlega karze 5 lat pozbawienia wolności i 75 000 euro grzywny.

Art. 421-2-5-2. Stałe korzystanie z usług publicznej komunikacji internetowej zawierających wiadomości, obrazy lub symbole prowokujące do popełnienia aktów o charakterze terrorystycznym lub stanowiące gloryfikację tego rodzaju działań, w przypadku gdy ta usługa wykorzystuje w tym celu obrazy ukazujące popełnienie tych czynów lub czynów stanowiących umyślny zamach na życie, podlega karze 2 lat pozbawienia wolności lub 30 000 grzywny.

Nie stanowi przestępstwa korzystanie z ww. usług, jeżeli jest ono prowadzone w dobrej wierze, wynika z normalnego toku wykonywania zawodu, którego celem jest informowanie społeczeństwa, lub jeżeli jest prowadzone w ramach badań naukowych albo jeżeli ma zostać wykorzystane jako dowód w postępowaniu.

Art. 421-2-6. I. Przygotowanie do popełnienia jednego z czynów wymienionych w pkt II niniejszego artykułu, jeżeli jest ono związane z indywidualnym przedsięwzięciem mającym na celu poważne naruszenie porządku publicznego przez zastraszenie lub terror i które charakteryzuje się występowaniem następujących elementów:

1) posiadaniem, dążeniem do pozyskania, nabyciem lub wytwarzaniem przedmiotów lub substancji mogących stwarzać zagrożenie;
2) działania, o których mowa, są powiązane z następującymi czynnikami:
   a) pozyskiwanie informacji o miejscach lub osobach, co ma pozwolić na przeprowadzenie określonych działań w tych miejscach lub na dokonanie zamachu na te osoby albo inwigilacja tych miejsc lub osób;
   b) szkolenie lub kształcenie w zakresie posługiwania się bronią lub jakimkolwiek innym instrumentem walki, wytwarzania lub wykorzystywania materiałów wybuchowych, zapalnych, nuklearnych, radiologicznych, biologicznych, chemicznych, a także w zakresie pilotażu statków powietrznych lub kierowania statkami wodnymi;
   c) stałe korzystanie z jednej lub większej liczby publicznych usług komunikacji internetowej albo posiadanie materiałów podżegających do popełnienia aktu o charakterze terrorystycznym lub gloryfikujących te akty;
   d) pobyt za granicą w strefie działań grup o charakterze terrorystycznym

– stanowi akt o charakterze terrorystycznym.

II. Punkt I stosuje się do przygotowania do popełnienia jednego z następujących przestępstw:

1. Aktów o charakterze terrorystycznym wymienionych w art. 421-1 pkt 1.
2. Aktów o charakterze terrorystycznym wymienionych w art. 421-1 pkt 2, jeżeli przygotowywany czyn ma polegać na zniszczeniu, wywołaniu poważnych szkód przez użycie materiałów wybuchowych lub zapalnych w takim miejscu lub czasie może to zagrażać życiu lub zdrowiu osób.

[7] *Loi No 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* [online], https://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164 [dostęp: 14 II 2017].

3. Aktów o charakterze terrorystycznym wymienionych w art. 421-2, jeżeli przygotowywany czyn może zagrażać życiu lub zdrowiu osób.

Art. 421-3. Górna granica kary pozbawienia wolności za przestępstwa wymienione w art. 421-1 ulega następującym obostrzeniom, jeżeli te przestępstwa stanowią akty o charakterze terrorystycznym:

1) kara dożywotniego pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 30 lat pozbawienia wolności;
2) kara 30 lat pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 20 lat pozbawienia wolności;
3) kara 20 lat pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 15 lat pozbawienia wolności;
4) kara 15 lat pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 10 lat pozbawienia wolności;
5) kara 10 lat pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 7 lat pozbawienia wolności;
6) kara 7 lat pozbawienia wolności, jeżeli przestępstwo jest zagrożone karą 5 lat pozbawienia wolności.
7) podwójny wymiar kary, jeżeli przestępstwo jest zagrożone karą co najmniej 3 lat pozbawienia wolności.

Art. 421-4. Akt o charakterze terrorystycznym określony w art. 421-2 podlega karze 20 lat pozbawienia wolności i 350 000 euro grzywny.

Jeżeli skutkiem dokonania ww. aktu jest śmierć jednej osoby lub większej liczby osób, ten czyn podlega karze dożywotniego pozbawienia wolności i 750 000 euro grzywny.

Art. 421-5 Akty o charakterze terrorystycznym określone w art. 421-2-1 i 421-2-2 podlegają karze 10 lat pozbawienia wolności i 225 000 euro grzywny.

Kierowanie ugrupowaniem lub organizowanie ugrupowania, o którym mowa w art. 421-2-1, podlega karze 30 lat pozbawienia wolności lub 500 000 euro grzywny.

Tej samej karze podlega usiłowanie dokonania czynu, o którym mowa w art. 421-2-2.

Akt o charakterze terrorystycznym, o którym mowa w art. 421-2-6, podlega karze 10 lat pozbawienia wolności i 150 000 euro grzywny.

Art. 421-6. Jeżeli celem ugrupowania, o którym mowa w art. 421-2-1, jest przygotowanie do popełnienia:

1) przestępstw przeciwko życiu lub zdrowiu osób wskazanych w art. 421-1 pkt 1;
2) przestępstw z wykorzystaniem materiałów wybuchowych lub zapalnych, których zamierzone miejsce i czas dokonania zagrażających życiu lub zdrowiu osób;
3) aktów o charakterze terrorystycznym określonych w art. 421-2, jeżeli ich skutkiem może być śmierć jednej lub większej liczby osób

– kara wynosi 30 lat pozbawienia wolności lub 450 000 euro grzywny.

Kierowanie ugrupowaniem, o którym mowa powyżej, lub organizowanie jego działalności podlega karze dożywotniego pozbawienia wolności lub 500 000 euro grzywny.

3. Kontrwywiad

Żaden z przeanalizowanych aktów prawnych nie zawiera wyrażonej expressis verbis definicji legalnej pojęcia k o n t r w y w i a d. Art. 2 pkt *Dekretu nr 2014-445 z dnia 30 kwietnia roku o zadaniach i organizacji Generalnej Dyrekcji Bezpieczeństwa Wewnętrznego*[8] definiujący katalog kompetencji ww. służby stanowi, że:

do zadań Generalnej Dyrekcji Bezpieczeństwa Wewnętrznego należy:

a) zapobieganie wszelkim formom ingerencji zagranicznej i jej zwalczanie;

(…)

d) zapobieganie działaniom stanowiącym zagrożenie dla tajemnicy obrony narodowej oraz działaniom zagrażającym potencjałowi gospodarczemu, przemysłowemu lub naukowemu i ich zwalczanie.

4. Rodzaje czynności operacyjno-rozpoznawczych

Francuski system prawny nie przewiduje systematyki instrumentów działania służb specjalnych polegającego na rozróżnieniu między czynnościami operacyjno-rozpoznawczymi, analityczno-informacyjnymi i dochodzeniowo-śledczymi. Instrumenty działania wykorzystywane przez wymienione służby zostały określone w ustawie o wywiadzie z 24 lipca 2015 r.[9] Zgodnie z art. L 811-3 tej ustawy służby mogą wykorzystywać tzw. techniki pozyskiwania informacji określone w tytule V ustawy, w celu zbierania informacji istotnych z punktu widzenia obronności i ochrony następujących fundamentalnych interesów państwa:

1. Niepodległości, integralności terytorialnej i obrony narodowej.
2. Istotnych interesów polityki zagranicznej, realizacji zobowiązań międzynarodowych i europejskich Francji oraz zapobiegania wszelkim formom zagranicznej ingerencji.
3. Istotnych interesów gospodarczych, przemysłowych i naukowych.
4. Zapobiegania terroryzmowi.
5. Zapobiegania:
   a) zamachom na republikańską formę instytucji;
   b) działaniom, których celem jest utrzymanie lub odtworzenie ugrupowań rozwiązanych na podstawie art. L 212-1 ustawy – Kodeks bezpieczeństwa wewnętrznego[10] stanowiącego, że na podstawie dekretu Rady Ministrów mogą być rozwiązane stowarzyszenia lub ugrupowania, które m.in. posługują się przemocą lub mają charakter grup zbrojnych albo paramilitarnych;
   c) zbiorowym aktom przemocy stanowiącym poważne zagrożenie porządku publicznego.
6. Zapobiegania przestępczości zorganizowanej.
7. Zapobiegania proliferacji broni masowego rażenia.

[8] *Décret No 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure* [online], https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028887486&categorieLien=id [dostęp: 14 II 2017].

[9] *Loi No 2015 -912 du 24 juillet 2015 relative au renseignement* [online], https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id [dostęp 14 II 2017].

[10] *Code de la sécurité intérieure* [online], www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132&dateTexte=20120618 [dostęp: 21 IV 2017].

Ustawa o wywiadzie wymienia następujące techniki pozyskiwania informacji:

1. Zbieranie w czasie rzeczywistym informacji o **połączeniach telefonicznych**, o sposobie używania środków komunikacji elektronicznej przez określoną osobę za pośrednictwem serwerów operatorów dostarczających usługi telekomunikacyjne –ten środek może być stosowany wyłącznie wobec osoby zidentyfikowanej jako zagrożenie terrorystyczne w celach prewencji i zapobiegania aktom terrorystycznym (art. L. 851-1 i L. 851-2).
2. Nałożenie na operatorów telekomunikacyjnych obowiązku wprowadzenia do ich sieci środków technicznych służących do automatycznego przetwarzania danych w celu wykrycia połączeń wskazujących na zagrożenie terrorystyczne **(tzw. czarne skrzynki**) – wyłącznie w celu zapobiegania terroryzmowi (art. L. 851-3). Dostawcy usług internetowych będą zobowiązani do zainstalowania na swoich serwerach urządzeń zbierających dane, np. dotyczące nadawcy lub odbiorcy wiadomości, adresu IP odwiedzanej strony, długości rozmów lub czasu, podłączenia komputera do Internetu, w celu wykrycia wzorców zachowań typowych dla członków grup terrorystycznych.
3. Wykorzystanie środków technicznych pozwalających na **lokalizację** osoby, pojazdu lub przedmiotu w czasie rzeczywistym (art. L. 851-5).
4. Wykorzystanie środków technicznych pozwalających na **identyfikację urządzeń końcowych** służących do przesyłania danych, takich jak indywidualne dane urządzenia, numer abonenta lub lokalizacja urządzeń końcowych (art. L. 851-6).
5. **Przechwytywanie informacji** ze względów bezpieczeństwa – dostęp administracyjny do danych o komunikacji elektronicznej określonej osoby został poddany w całości procedurze autoryzacji dokonywanej przez premiera, po uzyskaniu opinii Komisji. Tę procedurę określają rozdziały I i II tytułu IV kodeksu bezpieczeństwa wewnętrznego, ustanawiając wyjątek od zasady tajemnicy korespondencji gwarantowanej przez prawo.
6. Wykorzystanie środków technicznych pozwalających na **nagrywanie, odsłuchiwanie i transmisję** słów wypowiadanych przez określoną osobę lub **nagrywanie obrazu** w miejscu prywatnym w sytuacji, gdy nie jest możliwe uzyskanie niezbędnych informacji w inny sposób (L. 853-1).
7. Wykorzystanie narzędzi informatycznych pozwalających na **rejestrowanie, przechowywanie i przesyłanie danych informatycznych** zgromadzonych na serwerze (L. 853-2 pkt 1).
8. Dostęp, do **danych informatycznych** w postaci, w jakiej są widoczne na monitorze komputera użytkowanego przez określoną osobę, w jakiej wprowadza je do komputera za pomocą odczytania sekwencji symboli wpisywanych za pomocą klawiatury lub w jakiej są wprowadzane lub przesyłane za pomocą urządzeń audiowizualnych, a także ich przechowywanie i przesyłanie (L. 853-2 pkt 2).

5. Wyłączenie odpowiedzialności karnej funkcjonariuszy

Art. L 863-1 ustawy o wywiadzie.

Nie podlegają odpowiedzialności karnej funkcjonariusze, którzy w ramach realizacji ustawowych zadań wykonują następujące czynności:

1) nawiązywanie kontaktu w formie elektronicznej z osobami, które mogą zagrażać fundamentalnym interesom państwa w rozumieniu art. L 811-3;

2) pozyskiwanie i utrwalanie danych o osobach wymienionych w pkt 1 niniejszego artykułu;
3) pozyskiwanie i przesyłanie, na wyraźne żądanie innej osoby, oraz nabywanie lub przechowywanie treści nawołujących do popełnienia aktu o charakterze terrorystycznym lub stanowiących jego gloryfikację.

Jeżeli opisane powyżej działania wypełniają znamiona podżegania do popełnienia przestępstwa, podlegają karze 1 roku pozbawienia wolności lub 30 000 euro grzywny.

HOLANDIA

Kodeks karny[11] (fragmenty)

1. Terroryzm

Sekcja 83. Przestępstwo terrorystyczne oznacza:

1. Poważne przestępstwa określone w sekcjach: 9296 – przestępstwa przeciwko bezpieczeństwu państwa; 108 pkt 2 – zamach na członka rodziny królewskiej; 115 pkt 2 – zamach na życie głowy innego państwa; 117 (2) – zamach na życie osoby korzystającej z ochrony międzynarodowej[12]; 121 – zakłócenie działania parlamentu; 122 – porozumienie w celu zakłócenia działania parlamentu; 157 (3) – celowe wywołanie pożaru, wybuchu lub powodzi; 161 ze zn. 4 pkt 2 – umyślne narażenie człowieka, zwierzęcia, roślinności lub mienia na promieniowanie jonizujące radioaktywne; 164 (2) – umyślne sprowadzenie niebezpieczeństwa katastrofy w ruchu pojazdów mechanicznych lub kolejowych, którego skutkiem jest śmierć; 166 (3) – narażenie bezpieczeństwa transportu lotniczego lub morskiego przez celowe zniszczenie, uszkodzenie, usunięcie lub zamianę znaków albo symboli nawigacyjnych; 168 (2) – umyślne zniszczenie, uszkodzenie, uziemienie, spowodowanie niezdatności do użytku lub zatopienie pojazdu, statku wodnego lub powietrznego, jeżeli stwarza niebezpieczeństwo dla życia lub powoduje śmierć; 170 (3) – umyślne zniszczenie lub uszkodzenie budynku, struktury, instalacji morskiej lub położonej w miejscu publicznym; 174 (2) – nielegalna sprzedaż, oferowanie lub dostarczanie przedmiotów, które mogą zagrażać życiu, czego skutkiem jest śmierć; 289 – umyślne zabójstwo z premedytacją.

Za przestępstwa terrorystyczne kodeks uznaje m.in. poważne przestępstwa określone w ustawie o broni i amunicji, ustawie o przestępstwach gospodarczych, ustawie o cywilnym wykorzystywaniu materiałów wybuchowych oraz w ustawie o energii nuklearnej.

Sekcja 83a. Zamiar terrorystyczny oznacza zamiar wywołania strachu całości lub części społeczeństwa, bezprawnego skłonienia organów władzy publicznej albo organi-

[11] *Act of 24 June 2004 to amend and supplement the Penal Code and some other laws in connection with terrorist crimes* (*Crimes of Terrorism Act*).

[12] Sekcja 87b 1. Osoba korzystająca z ochrony międzynarodowej w rozumieniu art. 1 (1) *Konwencji o zapobieganiu przestępstwom i karaniu sprawców przestępstw przeciwko osobom korzystającym z ochrony międzynarodowej, w tym przeciwko dyplomatom*, sporządzonej w Nowym Jorku dnia 14 grudnia 1973 r. oraz art. 1 a i b *Konwencji o bezpieczeństwie personelu Organizacji Narodów Zjednoczonych i personelu współdziałającego, sporządzonej w Nowym Jorku dnia 9 grudnia 1994 r. wraz z Protokołem Fakultatywnym sporządzonym w Nowym Jorku dnia 8 grudnia 2005 r*.

zacji międzynarodowej do określonego działania bądź zaniechania lub do tolerowania określonych zachowań, a także poważne zakłócenie lub zniszczenie fundamentalnych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych państwa albo organizacji międzynarodowej.

2. Szpiegostwo

Sekcja 98 1. Kto umyślnie dostarcza lub udostępnia informacje oznaczone jako niejawne w interesie państwa lub jego sojuszników, przedmiot, za którego pomocą takie informacje lub dane mogą zostać uzyskane, osobie lub podmiotowi nieupoważnionemu, jeżeli osoba przekazująca wie lub powinna mieć świadomość, że ta informacja, przedmiot lub dane stanowią informacje niejawne, podlega karze pozbawienia wolności nieprzekraczającej 6 lat lub grzywnie piątej kategorii.

2. Kto umyślnie dostarcza lub udostępnia jakiekolwiek informacje pochodzące z miejsc, do których wstęp jest wzbroniony (*prohibited place*), istotnych dla bezpieczeństwa państwa i jego sojuszników, jakikolwiek przedmiot, za którego pomocą takie informacje lub dane mogą zostać przekazane osobie lub podmiotowi nieupoważnionemu, jeżeli osoba przekazująca wie lub powinna mieć świadomość, że te informacje, przedmioty lub dane mają tego rodzaju charakter, podlega takiej samej karze, jak czyn określony w § 1.

Sekcja 98a 1. Kto umyślnie ujawnia, dostarcza lub udostępnia informacje, przedmioty lub dane, o których mowa w sekcji 98, działając bez upoważnienia, innemu państwu, osobie przebywającej w innym państwie albo podmiotowi bądź osobie utworzonym za granicą, których cechy powodują, że zachodzi ryzyko, iż te informacje lub dane wejdą w posiadanie innego państwa, osoby lub podmiotu zagranicznego, jeżeli osoba przekazująca wie lub powinna mieć świadomość, że te informacje lub dane mają tego rodzaju charakter, podlega karze nieprzekraczającej 15 lat pozbawienia wolności lub grzywnie piątej kategorii.

2. Jeżeli sprawca dokonał czynu, o którym mowa w § 1, w czasie wojny lub wykonując rozkazy innego państwa, osoby przebywającej w innym państwie lub podmiotu utworzonego za granicą, karą jest dożywotnie pozbawienie wolności lub oznaczony czas pozbawienia wolności nieprzekraczający 30 lat lub grzywna piątej kategorii.

3. Działania prowadzone w ramach przygotowania do popełnienia czynów, o których mowa w § 1 i 2, podlegają karze nieprzekraczającej 6 lat pozbawienia wolności lub grzywnie piątej kategorii.

Sekcja 98b. Kto, będąc odpowiedzialnym za ochronę informacji, przedmiotów lub danych, o których mowa w sekcji 98, dopuszcza przez zaniedbanie do ich publicznego ujawnienia lub do ich ujawnienia osobie lub podmiotowi nieupoważnionemu, podlega karze pozbawienia wolności nieprzekraczającej jednego roku lub grzywnie trzeciej kategorii.

Sekcja 98c. Kto:

1) umyślnie wchodzi w posiadanie lub posiada, bez upoważnienia, informację, przedmiot lub dane, o których mowa w art. 98;
2) prowadzi działania mające na celu uzyskanie bez upoważnienia informacji, przedmiotu lub danych, o których mowa w art. 98;
3) wchodzi lub usiłuje wejść na teren miejsc ograniczonego dostępu, przebywa

w tych miejscach bądź opuszcza je lub próbuje opuścić w sposób niejawny, podając nieprawdziwe informacje, przez podstęp lub w jakikolwiek inny sposób niezgodny z prawem,

– podlega karze nieprzekraczającej 6 lat pozbawienia wolności lub grzywnie piątej kategorii.

LUKSEMBURG

Kodeks karny[13] (fragmenty)

1. Szpiegostwo (Rozdział II – *Przestępstwa i występki przeciwko bezpieczeństwu zewnętrznemu państwa***)**

Art. 114. Kto utrzymuje stosunki o charakterze wywiadowczym z obcym mocarstwem lub osobą działającą w jego interesie w celu zaangażowania tego mocarstwa w prowadzenie przeciwko Luksemburgowi wrogiej działalności lub w celu skłonienia go do prowadzenia wojny z Luksemburgiem albo dostarcza mu w tym celu środków, podlega karze 15 lat pozbawienia wolności lub karze dożywotniego pozbawienia wolności.

Art. 115. Karze dożywotniego pozbawienia wolności podlega:

- kto ułatwia wrogom państwa wejście na terytorium Luksemburga;
- kto oddaje wrogom państwa kontrolę nad miastami, urzędami pocztowymi, magazynami, składami uzbrojenia lub budynkami państwowymi;
- kto przyczynia się do postępów obcych sił zbrojnych na terytorium Luksemburga lub prowadzi działania przeciwko siłom zbrojnym Luksemburga przez obniżanie lojalności żołnierzy i obywateli wobec najwyższych organów państwa.

Porozumienie mające na celu osiągnięcie jednego z powyżej określonych zamierzeń podlega karze dożywotniego pozbawienia wolności, jeżeli jego skutkiem było przygotowanie ich dokonania, oraz karze od 5 do 10 lat pozbawienia wolności, jeżeli przygotowanie nie zaistniało.

Art. 116. Kto świadomie dostarcza lub przekazuje, w całości lub części, w postaci oryginalnej lub kopii, obcemu mocarstwu lub innej osobie działającej w jego interesie, przedmioty, plany, pisma, dokumenty lub informacje, których ujawnienie wrogiemu państwu ma istotne znaczenie dla obronności lub bezpieczeństwa państwa, podlega karze dożywotniego pozbawienia wolności.

Art. 117. Tej samej karze podlega, kto popełnia wyżej wymienione przestępstwa przeciwko państwom sprzymierzonym z Luksemburgiem, działającym przeciwko wspólnemu wrogowi.

Państwo sprzymierzone z Luksemburgiem oznacza każde państwo, które niezależnie od istnienia traktatu sojuszniczego prowadzi wojnę z państwem, z którym w stanie wojny jest również Luksemburg.

[13] *Code pénal en vigeur dans le Grand-Duché de Luxembourg* [online], www.legilux,public.lu/eli/etat/leg/code/penal [dostęp: 14 II 2017].

Art. 118. Kto świadomie dostarcza lub przekazuje, w całości lub części, w postaci oryginalnej lub jako kopię, obcemu mocarstwu lub innej osobie działającej w jego interesie, przedmioty, plany, pisma, dokumenty lub informacje, których ujawnienie wrogiemu państwu ma istotne znaczenie dla obronności lub bezpieczeństwa zewnętrznego państwa, podlega karze od 10 do 15 lat pozbawienia wolności.

Art. 120 bis. Karze pozbawienia wolności od 6 miesięcy do 5 lat oraz grzywnie w wysokości od 251 do 125 000 euro podlega:

1. Kto, posługując się przedmiotami utrudniającymi jego identyfikację lub ukrywając swoją tożsamość, zawód, pełnioną funkcję lub narodowość, przy wykorzystaniu metod mających na celu wprowadzenie w błąd osób odpowiedzialnych za ochronę, wchodzi do jakiegokolwiek obiektu o charakterze obronnym, posterunku, budynku wojskowego lub związanego z lotnictwem, składu, magazynu, placu budowy lub laboratorium, w których są prowadzone prace istotne z punktu widzenia obronności;
2. Kto, wykorzystując jeden z instrumentów opisanych w poprzednim paragrafie, wszedł w posiadanie planów, środków komunikacji, korespondencji lub informacji istotnych z punktu widzenia bezpieczeństwa zewnętrznego państwa;
3. Kto w celu pozyskania lub przekazania informacji istotnych z punktu widzenia obronności lub bezpieczeństwa zewnętrznego, nie posiadając ku temu niezbędnych uprawnień, organizuje lub wykorzystuje instrumenty przesyłania informacji na odległość.

2. Terroryzm (Rozdział III – *O terroryzmie***)**

Sekcja I – *Przestępstwa o charakterze terrorystycznym*

Art. 135-1. Każde przestępstwo i delikt zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, którego charakter lub kontekst, w jakim został popełniony, sprawia, że poważnie zagraża państwu, organizacji lub organizacji międzynarodowej i który został popełniony umyślnie w celu:

- poważnego zastraszenia ludności;
- bezprawnego zmuszenia władzy publicznej, organizacji lub organu międzynarodowego do określonego działania lub zaniechania;
- wywołania poważnej destabilizacji lub zniszczenia fundamentalnych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych państwa, organizacji lub organu międzynarodowego.

– stanowi akt o charakterze terrorystycznym.

Art. 135-2. Kto dokonuje aktu o charakterze terrorystycznym, podlega karze od 15 do 20 lat pozbawienia wolności.

Jeżeli skutkiem aktu, o którym mowa powyżej, jest śmierć jednej lub większej liczby osób, czyn ten jest zagrożony karą dożywotniego pozbawienia wolności.

Art. 135-3.1. Związek, mający strukturę, składający się z co najmniej dwóch osób i utworzony w dającym się określić czasie w celu dokonania w sposób zorganizowany

jednego lub więcej aktów o charakterze terrorystycznym wymienionych w pkt 2 niniejszego artykułu stanowi ugrupowanie terrorystyczne.

2. Punkt 1 niniejszego artykułu dotyczy następujących przestępstw:

- przeciwko osobom korzystającym z ochrony międzynarodowej (szefowie państw, rządów itd.);
- określonych w art. 135-1, 135-2, 135-5, 135-6, 135-9, 135-11 do 135-16 oraz 442-1;
- określonych w art. 31 i 31-1 ustawy o ruchu lotniczym;
- przestępstwa określonego w art. 2 ustawy ratyfikującej *Konwencję o ochronie fizycznej materiałów jądrowych*, otwartej do podpisu w Wiedniu i w Nowym Jorku 3 marca 1980 r.;
- przestępstwa określonego w art. 65-1 *Ustawy z dnia 14 kwietnia 1992 r. – Kodeks karny i dyscyplinarny marynarki wojennej*[14].

Art. 135-4.1. Kto w sposób dobrowolny i świadomy bierze aktywny udział w działalności ugrupowania terrorystycznego, podlega karze od roku do 8 lat pozbawienia wolności oraz grzywnie od 2500 do 12 500 euro lub jednej z tych kar, nawet jeśli nie ma zamiaru popełnienia przestępstwa w ramach działalności tej grupy ani wzięcia udziału w jego dokonaniu.

2. Kto bierze udział w przygotowaniu lub realizacji wszelkich niezgodnych z prawem działań ugrupowania terrorystycznego ze świadomością, że ten udział przyczynia się do osiągnięcia jego celów, podlega karze pozbawienia wolności od 1 roku do 8 lat i grzywnie od 2500 do 12 5000 euro lub jednej z tych kar.

3. Kto bierze udział w procesie decyzyjnym ugrupowania terrorystycznego, wiedząc, że ten udział przyczyni się do osiągnięcia jego celów, podlega karze pozbawienia wolności od 5 do 10 lat i grzywnie od 12 500 euro do 25 000 euro lub jednej z tych kar.

4. Kierujący ugrupowaniem terrorystycznym podlega karze pozbawienia wolności od 10 do 15 lat i grzywnie w wysokości od 25 000 do 50 000 euro lub jednej z tych kar.

5. Czyny wymienione w pkt 1–4 niniejszego artykułu dokonane na terytorium Luksemburga są ścigane na mocy prawa Luksemburga, niezależnie od miejsca, w którym ugrupowanie terrorystyczne ma swoją siedzibę lub prowadzi działalność.

Art. 135-5.1. Udzielanie lub pozyskiwanie, w jakikolwiek sposób, bezpośrednio lub pośrednio, dobrowolnie i niezgodnie z prawem, środków finansowych lub mienia jakiegokolwiek rodzaju, ze świadomością, że zostaną one wykorzystane, w całości lub w części, w celu usiłowania lub dokonania jednego z przestępstw określonych w pkt 2 niniejszego artykułu, nawet gdy nie zostały one faktycznie wykorzystane i nie są powiązane z jednym lub większą liczbą konkretnych aktów o charakterze terrorystycznym stanowi przestępstwo finansowania terroryzmu.

2. Punkt 1 niniejszego artykułu dotyczy następujących przestępstw:

1) przeciwko osobom korzystającym z ochrony międzynarodowej (szefowie państw, rządów itd.);
2) określonych w art. 31 i 31-1 *Ustawy z dnia 31 stycznia 1948 r. o ruchu lotniczym*[15];

[14] *Loi du 14 avril 1992 instituant un code disciplinaire et pénale pour la marine* [online], www.legilux.public.lu/eli/etat/leg/loi/1992/04/14/n3/jo [dostęp: 19 IV 2017].

[15] *Loi du 31 janvier 1948 relative à la réglementation de la navigation aérienne* [online], www.legilux.

3) określonych w art. 2 ustawy ratyfikującej *Konwencję o ochronie fizycznej materiałów jądrowych*, otwartej do podpisu w Wiedniu i w Nowym Jorku 3 marca 1980 r.;
4) przestępstwa określonego w art. 65-1 *Ustawy z dnia 14 kwietnia 1992 r. – Kodeks karny i dyscyplinarny marynarki wojennej*.

3. Udzielanie lub pozyskiwanie, w jakikolwiek sposób, bezpośrednio lub pośrednio, dobrowolnie i niezgodnie z prawem, środków finansowych lub mienia jakiegokolwiek rodzaju, ze świadomością, że zostaną one wykorzystane, w całości lub części, przez terrorystę lub ugrupowanie terrorystyczne, również wtedy, gdy nie ma ono związku z konkretnym aktem o charakterze terrorystycznym i wtedy, gdy te środki nie zostały faktycznie wykorzystane przez terrorystę lub ugrupowanie terrorystyczne stanowi przestępstwo finansowania terroryzmu.

Sekcja II – *Akty o charakterze terrorystycznym z użyciem materiałów wybuchowych*

Art. 135-9.1. Z zastrzeżeniem art. 520, kto umyślnie podkłada, powoduje eksplozję lub detonuje materiał wybuchowy lub inny śmiercionośny materiał w miejscu publicznym, w obiekcie rządowym lub w innym budynku o charakterze publicznym, środkach transportu zbiorowego lub w sposób zagrażający elementom infrastruktury:
1) w celu spowodowania śmierci lub wywołania poważnego uszczerbku na zdrowiu,
2) w celu spowodowania poważnych zniszczeń w miejscach wym. w pkt 1, jeżeli może to spowodować poważne straty

– podlega karze od 5 do 10 lat pozbawienia wolności.

2. Jeżeli skutkiem czynu określonego w pkt 1 jest uszczerbek na zdrowiu lub choroba, kara wynosi od 10 do 15 lat pozbawienia wolności.

3. Kara wynosi od 15 do 20 lat pozbawienia wolności, jeżeli:
1) skutkiem przestępstwa wymienionego w § 1 jest nieuleczalna choroba, trwała niezdolność do pracy, całkowity zanik czynności organu lub utrata części ciała;
2) skutkiem przestępstwa wymienionego w § 1 jest zniszczenie miejsca publicznego, obiektu rządowego lub innego obiektu publicznego, systemu transportu publicznego lub elementu infrastruktury albo jego poważne uszkodzenie.

4. Przestępstwo, o którym mowa w § 1, którego skutkiem jest śmierć, jest zagrożone karą dożywotniego pozbawienia wolności.

Sekcja III – *Przestępstwa związane z działalnością terrorystyczną*

Art. 135-11.1. Rozpowszechnianie lub jakiekolwiek publiczne udostępnianie wiadomości, także za pośrednictwem środków komunikacji elektronicznej, w celu nawoływania, bezpośrednio lub pośrednio, do popełnienia jednego z przestępstw określonych w niniejszym rozdziale stanowi podżeganie do terroryzmu.

2. Rozpowszechnianie wiadomości, o których mowa w § 1 w obecności wielu osób w miejscu publicznym lub w przestrzeni wirtualnej utworzonej przy wykorzystaniu środków telekomunikacji, otwartej dla określonej liczby osób, które mogą do niej dołączyć i z niej korzystać, stanowi podżeganie do terroryzmu.

public.lu/eli/etat/leg/loi/1948/01/31/n1/jo [dostęp: 19 IV 2017].

Art. 135-12.1. Przestępstwo rekrutacji do celów terrorystycznych popełnia osoba, która podżega lub usiłuje podżegać inną osobę do:

1) dokonania lub udziału w dokonaniu jednego z przestępstw określonych w niniejszym rozdziale;
2) stworzenia lub dołączenia do ugrupowania terrorystycznego w rozumieniu art. 135-3.

2. Przestępstwo rekrutacji do celów terrorystycznych popełnia osoba, która świadomie wstępuje do ugrupowania terrorystycznego z zamiarem popełnienia lub udziału w popełnieniu jednego z przestępstw o charakterze terrorystycznym, wymienionych w niniejszym rozdziale.

Art. 135-13.1. Przestępstwo szkolenia do celów terrorystycznych popełnienia osoba, która udziela instrukcji w zakresie wytwarzania lub wykorzystywania materiałów wybuchowych, broni palnej lub broni innego rodzaju, szkodliwych lub niebezpiecznych substancji, lub w zakresie innych metod i technik w celu popełnienia jednego z przestępstw określonych w niniejszym rozdziale, mając świadomość, że celem tych działań jest realizacja zamierzenia w postaci dokonania aktu o charakterze terrorystycznym.

2. Przestępstwo szkolenia w celach terrorystycznych popełnia osoba, która świadomie bierze udział w szkoleniu, o którym mowa w pkt 1 oraz która podżega lub nakłania, w jakikolwiek sposób, inne osoby do przeprowadzenia takiego szkolenia z jej udziałem.

Art. 135-14. Przygotowanie do popełnienia jednego z przestępstw określonych w niniejszym rozdziale, jeżeli charakteryzuje się występowaniem następujących elementów:

1) posiadanie, poszukiwanie, pozyskiwanie lub wytwarzanie materiałów wybuchowych, broni palnej lub broni innego rodzaju, szkodliwych lub niebezpiecznych substancji, poszukiwanie lub pozyskiwanie informacji o innych metodach i technikach umożliwiających przygotowanie lub dokonanie aktu o charakterze terrorystycznym oraz
2) zaistnieniem co najmniej jednego z poniższych elementów:
   a) pozyskiwanie informacji o miejscach lub osobach, w celu dokonania aktu o charakterze terrorystycznym w tych miejscach, lub przeciwko tym osobom, lub inwigilacja tych miejsc lub osób;
   b) szkolenie w zakresie wykorzystywania materiałów wybuchowych, broni palnej lub innego rodzaju broni, szkodliwych lub niebezpiecznych substancji, lub innych metod i technik, lub jakiejkolwiek innej formy walki lub pilotażu statków powietrznych, wodnych lub kierowania pociągami;
   c) stałe korzystanie z jednej lub większej liczby usług komunikacji elektronicznej, stałe utrzymywanie kontaktów ze środowiskami, o których mowa w art. 135-11 (2), lub posiadanie przedmiotów lub dokumentów prowokujących do dokonania aktu o charakterze terrorystycznym;
   d) pobyt za granicą w strefie działań ugrupowań terrorystycznych

– podlega karze przewidzianej w art. 135-17.

Art. 135-15. Osoba, która przebywając na terytorium Luksemburga, wyjeżdża lub przygotowuje się do wyjazdu do innego państwa z zamiarem popełnienia, zorganizowania, przygotowania lub udziału w dokonaniu jednego lub większej liczby aktów o charakterze terrorystycznym, określonych w niniejszym rozdziale podlega karze przewidzianej w art. 135-17.

Art. 135-16. Obywatel Luksemburga, który:
a) opuszcza terytorium Luksemburga, naruszając obowiązujący go zakaz opuszczania kraju;
b) unika wykonania ciążącego na nim obowiązku wydania paszportu lub dowodu osobistego właściwym organom
– podlega karze przewidzianej w art. 135-17.

Art. 135-17.1. Kto popełnia lub usiłuje popełnić przestępstwo określone w art. 135-11–135-16 podlega karze od roku do 8 lat pozbawienia wolności oraz grzywnie w wysokości od 2500 do 12 500 euro lub jednej z tych kar, nawet gdy nie zostało dokonane żadne z przestępstw, do których popełnienia zmierzały działania tej osoby.

2. W razie skazania obywatela Luksemburga za jedno z przestępstw określonych w art. 135-12–135-15 na karę inną niż kara pozbawienia wolności sąd może orzec dodatkowo zakaz opuszczania kraju na okres nieprzekraczający jednego roku. Jeżeli zakaz opuszczania kraju nie został orzeczony przez sędziego śledczego w postępowaniu przygotowawczym, po uznaniu oskarżonego za winnego przez sąd i orzeczeniu kary przewidzianej w niniejszym paragrafie skazany wydaje paszport i dowód osobisty.

Art. 136. Nie podlegają karze sprawcy przestępstw określonych w niniejszym tytule oraz w art. 111 (zamach na życie monarchy i członków rodziny królewskiej), którzy przed dokonaniem aktu o charakterze terrorystycznym i przed wszczęciem postępowania karnego udzielili właściwym organom informacji o planowanych działaniach oraz o osobach zaangażowanych w przygotowania do nich.

NIEMCY

Kodeks karny[16] (fragmenty)

Rozdział II

1. Szpiegostwo (zdrada i zagrożenie bezpieczeństwa wewnętrznego)

Sekcja 93. Pojęcie t a j e m n i c a p a ń s t w o w a oznacza:
1) fakty, obiekty, ustalenia udostępniane tylko ograniczonej liczbie osób, które są niejawne dla obcych sił, aby uniknąć ryzyka wystąpienia poważnej szkody dla bezpieczeństwa zewnętrznego Republiki Federalnej Niemiec;
2) okoliczności, które stanowią zagrożenie niepodległości, demokratycznego porządku konstytucyjnego lub umów międzynarodowych o kontroli zbrojeń, które pozostają niejawne dla stron traktatów zawartych z Republiką Federalną Niemiec i nie są tajemnicą państwową.

[16] Ang. *German Criminal Code*. Niem. *Strafgesetzbuch* (StGB) [online], www.gesetze-im-internet.de/englisch_stgb/index.html [dostęp: 10 II 2017].

Sekcja 94. Zdrada.

1. Ktokolwiek:
   a) ujawnia tajemnicę państwową zagranicznemu mocarstwu lub jednemu z jego pośredników, lub
   b) pozwala, by tajemnica państwowa została ujawniona nieuprawnionej osobie albo została upubliczniona w celu wyrządzenia szkody Republice Federalnej Niemiec lub osiągnięcia korzyści przez zagraniczne mocarstwo i w wyniku powyższego stwarza niebezpieczeństwo poważnej szkody dla zewnętrznego bezpieczeństwa Republiki Federalnej Niemiec, podlega karze pozbawienia wolności na czas nie krótszy niż rok.
2. W szczególnie poważnych przypadkach występuje zagrożenie karą dożywotniego pozbawienia wolności na czas nie krótszy niż 5 lat. Poważne przypadki występują wtedy, gdy:
   a) dana osoba nadużywa pozycji, zgodnie z której pełnieniem jest szczególnie zobowiązana do ochrony tajemnicy państwowej albo
   b) w wyniku przestępstwa powstaje zagrożenie wystąpienia szczególnej szkody dla zewnętrznego bezpieczeństwa Republiki Federalnej Niemiec.

Sekcja 95. Ujawnienie tajemnicy państwowej z zamiarem wyrządzenia szkody.

1. Ktokolwiek pozwala, aby tajemnica państwowa będąca w posiadaniu organu państwa została ujawniona osobie nieuprawnionej albo została przekazana do informacji publicznej i tym samym powoduje wyrządzenie poważnej szkody dla zewnętrznego bezpieczeństwa państwa, podlega karze pozbawienia wolności od 6 miesięcy do 5 lat, chyba że przestępstwo podlega karze zgodnie z sekcją 94 (zdrada).
2. Usiłowanie ujawnienia tajemnicy państwowej również jest karalne.
3. W poważnych przypadkach jest wymierzana kara pozbawienia wolności od roku do lat 10.

Sekcja 96. Zdrada i szpiegostwo; szpiegostwo w zakresie tajemnic państwowych.

1. Ktokolwiek uzyskuje tajemnicę państwową w celu ujawnienia jej, podlega karze pozbawienia wolności od roku do 10 lat.
2. Ktokolwiek uzyskuje tajemnicę państwową, która była w posiadaniu organu państwowego i ujawnia ją za namową, podlega karze wolności od 6 miesięcy do 5 lat. Usiłowanie jest karalne.

Sekcja 98. Działanie w zakresie zdrady jako agent.

1. Ktokolwiek:

a) uczestniczy w działalności na rzecz zagranicznego mocarstwa, którego działania są wymierzone w kierunku przechwycenia komunikacji lub tajemnic państwowych, lub

b) deklaruje chęć oraz gotowość do uczestnictwa w takiej działalności na rzecz zagranicznego mocarstwa lub jego pośredników, podlega karze pozbawienia wolności nieprzekraczającej 5 lat lub grzywny. W szczególnie poważnych przypadkach odpowiedzialność wynosi od roku do 10 lat.

2. Sąd wedle swojego uznania może złagodzić wyrok lub odstąpić od wymierzenia kary, jeśli oskarżony dobrowolnie zaprzestanie swojej działalności i ujawni

swoją wiedzę organom państwowym. Jeśli oskarżony został zmuszony do takiej działalności przez obce mocarstwo lub jego pośredników, nie podlega karze na podstawie niniejszego przepisu – o ile dobrowolnie zaprzestał tej działalności i ujawnił swoją wiedzę organom państwa.

Sekcja 99. Prowadzenie działalności wywiadowczej jako agent.

1. Ktokolwiek:
   a) uczestniczy w działalności wywiadowczej na rzecz służby wywiadowczej obcego państwa przeciwko Republice Federalnej Niemiec, która obejmuje: komunikację, przekazywanie informacji, obiektów lub wiedzy albo
   b) deklaruje służbom wywiadowczym zagranicznego mocarstwa lub jednemu z jego pośredników chęć oraz gotowość do uczestnictwa w takiej działalności,

   – podlega karze pozbawienia wolności nieprzekraczającej 5 lat lub karze grzywny.
2. W szczególnie poważnych przypadkach kara pozbawienia wolności wynosi od roku do lat 10.

2. Terroryzm[17]

Sekcja 129a. Tworzenie organizacji terrorystycznych.

1. Ktokolwiek formuje organizację, której cel lub działanie jest skierowane na popełnienie:
   a) morderstwa, w przypadku szczególnie obciążających okoliczności, morderstwa lub ludobójstwa, albo przestępstwa przeciwko ludzkości lub przestępstwa wojennego, albo też:
   b) przestępstwa przeciwko wolności osobistej,
   c) uchylony,

   lub ktokolwiek uczestniczący w takiej grupie jako członek – podlega karze pozbawienia wolności od roku do 10 lat.
2. Takiej samej karze podlega osoba tworząca organizację, której cele lub działania są skierowane na:
   a) wyrządzenie poważnych fizycznych lub psychicznych szkód innej osobie;
   [b), c), d) – odesłania do innych przestępstw wymienionych w innych przepisach kodeksu karnego – dop. aut.];
   e) popełnienie przestępstwa na podstawie sekcji 51 ustawy o broni, lub
   przez jakąkolwiek osobę, która uczestniczy w takiej grupie jako członek, jeśli jakiekolwiek z przestępstw wymienionych powyżej jest zamierzone i polega na zmuszeniu społeczeństwa do określonego działania, wymuszeniu na władzach lub na organizacji międzynarodowej określonego działania, przez użycie siły lub groźby albo znaczącym zaszkodzeniu fundamentom politycznym, konstytucyjnym, gospodarczym lub socjalnym strukturom państwa albo organizacji międzynarodowej, i które – biorąc pod uwagę konsekwencje poważnych przestępstw – mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej.
4. Jeżeli cele lub działania grupy są skierowane na zagrożenie popełnieniem jednego z przestępstw wymienionych w podsekcji 1 lub 2 powyżej, kara pozbawienia wolności wynosi od 6 miesięcy do 5 lat.

[17] Tamże.

5. Jeżeli przestępca jest jednym z prowokatorów, kara pozbawienia wolności wynosi nie mniej niż 3 lata – w przypadkach wskazanych w podsekcjach 1 i 2, i od 1 do 10 lat, w przypadkach wskazanych w podsekcji 3.

Sekcja 129b. Organizacje terrorystyczne i przestępcze za granicą, rozszerzona konfiskata i przepadek [mienia – dop. aut.].

Sekcje 129 i 129a mają zastosowanie do organizacji terrorystycznych za granicą. Jeżeli przestępstwo dotyczy organizacji działającej poza państwami członkowskimi Unii Europejskiej, niniejszy przepis nie ma zastosowania, chyba że przestępstwo zostało popełnione w taki sposób, iż niektóre czynności z nim związane były wykonywane na terytorium Republiki Federalnej Niemiec lub jeżeli przestępca albo ofiara są obywatelami niemieckimi albo zostali zlokalizowani na terytorium RFN. W przypadkach, do których ma zastosowanie zdanie drugie, przestępstwo jest ścigane na podstawie zgody Federalnego Ministerstwa Sprawiedliwości. Zgoda może zostać udzielona w indywidualnym przypadku oraz jako zgoda generalna w celu ścigania przyszłych przestępstw związanych ze szczególną organizacją. Federalne Ministerstwo Sprawiedliwości, wydając zgodę, uwzględnia, czy cele danej organizacji są skierowane przeciwko fundamentalnym wartościom państwowym, godności ludzkiej, przeciwko pokojowi lub współegzystencji narodów oraz waży wszelkie inne okoliczności sprawy.

Sekcje 73d i 74a mają zastosowanie do sekcji 129 i sekcji 129a, w każdym przypadku w związku z podsekcją 1.

STANY ZJEDNOCZONE AMERYKI

1. Szpiegostwo

*Kodeks Stanów Zjednoczonych***. Tytuł 18 –** *Przestępstwa i procedura karna***. Część I –** *Przestępstwa***. Rozdział 37 –** *Szpiegostwo i cenzura*

§ 793 – *Gromadzenie, przekazywanie lub utrata informacji dotyczących obrony*[18]

a) ktokolwiek – w celu uzyskania informacji odnoszących się do obrony narodowej z zamiarem lub przekonaniem, że ta informacja będzie wykorzystana w celu wyrządzenia szkody Stanom Zjednoczonym lub na rzecz jakiegokolwiek państwa zagranicznego, w wyniku wejścia, przejścia lub przelotu lub w inny sposób – uzyskuje informacje dotyczące jakiegokolwiek statku morskiego, powietrznego, prac w zakresie obrony narodowej, marynarki wojennej, baz podwodnych, stacji paliwowych, fortów, baterii, stacji torpedowych, doków, kanałów, linii kolejowych, arsenałów, ośrodków, fabryk, kopalni, telegrafów, telefonów, łączności bezprzewodowej, stacji sygnałów, budynków, biur, laboratoriów badawczych lub stacji albo innych miejsc związanych z obroną narodową posiadanych przez stany Zjednoczone lub budowanych przez to państwo albo będących pod kontrolą Stanów Zjednoczonych, lub jakichkolwiek ich oficerów, departamentów, agencji

[18] www.law.cornell.edu/uscode/text/18/part-I/chapter-37 [dostęp: 10 II 2017].

albo będących pod wyłączną jurysdykcją Stanów Zjednoczonych lub jakiegokolwiek miejsca, w którym jakikolwiek statek morski lub powietrzny, uzbrojenie, amunicja lub inne materiały albo narzędzia przeznaczone do użytku w czasie działań wojennych są wytwarzane, przygotowywane, naprawiane, przechowywane lub poddawane badaniom w celu rozwoju, będące wynikiem kontraktu lub umowy ze Stanami Zjednoczonymi lub jakimikolwiek departamentami albo agencjami Stanów Zjednoczonych lub jakiejkolwiek osoby działającej na rzecz Stanów Zjednoczonych albo jakichkolwiek miejsc, mających charakter niejawny na podstawie decyzji Prezydenta Stanów Zjednoczonych, w czasie wojny lub w przypadku krajowego stanu wyjątkowego, w których znajdują się jakiekolwiek przedmioty lub obiekty będące w fazie przygotowania lub przechowywane, które są wykorzystywane przez wojsko, marynarkę wojenną lub siły powietrzne, oraz informację dotycząca miejsc, które na mocy decyzji Prezydenta mają charakter niejawny, będzie uznawana za szkodliwą dla obrony narodowej lub

b) ktokolwiek w celach, o których mowa powyżej i z zamiarem lub przekonaniem, kopiuje, zabiera, wytwarza lub uzyskuje albo podejmuje próby kopiowania, zabrania, wytwarzania lub uzyskania szkiców, fotografii, negatywów fotograficznych, światłokopii, planów, map modeli, narzędzi, urządzeń, dokumentów, pisma lub notatek albo czegokolwiek mającego związek z obroną narodową; lub

c) ktokolwiek w celach, o których mowa powyżej, otrzymuje lub uzyskuje, uzgadnia albo próbuje otrzymać lub uzyskać od jakiejkolwiek osoby lub źródła jakikolwiek dokument, pismo, książkę z kodami, książkę z sygnałami, szkic, fotografię, negatyw, światłokopię, plan, mapę, model, narzędzia, urządzenia lub notatkę czegokolwiek powiązanego z obroną narodową, wiedząc lub mając przekonanie, w czasie gdy otrzymuje, uzyskuje, uzgadnia lub próbuje otrzymać lub uzyskać ww. rzecz, że zostało to lub zostanie uzyskane, powzięte, wykonane lub rozporządzone przez jakąkolwiek osobę niezgodnie z przepisami niniejszego rozdziału, lub

d) ktokolwiek, zgodnie z prawem posiadając, mając dostęp lub kontrolę, bądź komu powierzono jakikolwiek dokument, pismo, książkę z kodami, książkę z sygnałami, szkic, fotografię, negatyw, światłokopię, plan, mapę, model, narzędzia, urządzenia lub notatki dotyczące obrony narodowej lub informacje odnoszące się do obrony narodowej, które posiadacz może uważać za mogące zostać wykorzystanymi do wyrządzenia szkody Stanom Zjednoczonym lub wykorzystanymi przez jakiekolwiek państwo zagraniczne, umyślnie komunikuje się, dostarcza, przekazuje, lub podlega komunikowaniu, dostarczeniu, przekazaniu lub próbuje komunikacji, dostarczenia, przekazania bądź podlega próbie komunikowania się, dostarczenia, przekazania w stosunku do osoby, która nie jest do tego uprawniona lub umyślnie zachowuje to i nie dostarcza lub nie przekazuje na żądanie oficera lub pracownika Stanów Zjednoczonych uprawnionych do otrzymania tego, lub

e) ktokolwiek, będąc nieuprawnionym do posiadania, dostępu, kontroli nad jakimkolwiek dokumentem, pismem, książką z kodami, książką z sygnałami, szkicem, fotografią, negatywem, światłokopią, planem, mapą, modelem, narzędziami, urządzeniami, notatką dotyczącą obrony narodowej lub informacją dotyczącą obrony narodowej, które posiadacz może uważać za mogące zostać wykorzystanymi do wyrządzenia szkody Stanom Zjednoczonym lub wykorzystanymi przez jakiekolwiek państwo zagraniczne, umyślnie komunikuje się, dostarcza, przekazuje lub podlega komunikowaniu, dostarczeniu, przekazaniu lub próbuje komu-

nikacji dostarczenia lub przekazania bądź podlega próbie komunikowania się, dostarczenia, przekazania w stosunku do osoby, która nie jest do tego uprawniona albo umyślnie zachowuje to i nie dostarcza lub nie przekazuje na żądanie oficera lub pracownika Stanów Zjednoczonych uprawnionych do otrzymania tego, lub

f) ktokolwiek, komu powierzono lub kto zgodnie z prawem ma lub kontroluje jakikolwiek dokument, pismo, książki z kodami, książki z sygnałami, szkice, fotografie, negatywy, światłokopie, plany, mapy, modele, narzędzia, urządzenia, notatki lub informacje odnoszące się do obrony narodowej, (1) przez rażące zaniedbanie pozwala na usunięcie ww. przedmiotów z właściwego miejsca opieki lub dostarczenie do kogokolwiek z naruszeniem zasad, na jakich zostały one mu powierzone, lub zagubienie, kradzież, zagarnięcie albo zniszczenie, lub (2) mając wiedzę, iż ww. przedmioty zostały nielegalnie usunięte z właściwego miejsca ich opieki lub dostarczone do kogokolwiek z naruszeniem zasad, na jakich zostały mu powierzone, lub zagubione, skradzione, zagarnięte lub zniszczone, oraz w razie niezgłoszenia w formie raportu ww. zagubienia, kradzieży, zagarnięcia lub zniszczenia, do przełożonego oficera

– podlega karze grzywny na podstawie niniejszego tytułu lub pozbawienia wolności w wymiarze nie wyższym niż 10 lat, lub obydwu.

g) jeśli dwie lub więcej osób działają w porozumieniu (zmowie), w celu pogwałcenia jakiegokolwiek z ww. postanowień niniejszej sekcji, i jeśli jedna lub więcej z takich osób dopuszcza się jakiegokolwiek działania w zamiarze realizacji celu porozumienia (zmowy), każda ze stron powyższego porozumienia (zmowy) podlega takiej karze, jak za dokonanie przestępstwa objętego tym porozumieniem (zmową),

h) (1) jakakolwiek osoba skazana za pogwałcenie niniejszej sekcji traci na rzecz Stanów Zjednoczonych, niezależnie od jakichkolwiek postanowień prawa stanowego, jakąkolwiek nieruchomość ustanowioną, otrzymaną, jakiekolwiek dochody, jakie ta osoba osiągnęła, pośrednio lub bezpośrednio od jakiegokolwiek rządu państwa zagranicznego albo jakiejkolwiek frakcji i partii oraz jakiegokolwiek wojska, sił morskich państwa zagranicznego, niezależnie czy uznawanej, czy nieuznawanej przez Stany Zjednoczone, jako wynik takiego pogwałcenia. Na potrzeby niniejszej sekcji, termin p a ń s t w o obejmuje Stany Zjednoczone, Dystrykt Kolumbia i każdą wspólnotę, terytorium lub posiadłość Stanów Zjednoczonych;

(2) w stosunku do oskarżonego skazanego za pogwałcenie niniejszej sekcji sąd w wyroku zarządza przepadek wszystkich rzeczy, o których mowa w paragrafie 1 niniejszej sekcji, na rzecz Stanów Zjednoczonych.

(3) postanowienia podsekcji (b), (c), i (e) przez (p) sekcji 413 ustawy o zapobieganiu powszechnemu nadużywaniu środków odurzających i kontroli z 1970 r. (21 U.S.C. 853 (b), (c), i (e)–(p) mają zastosowanie do :

(A) nieruchomości podlegających przepadkowi na podstawie niniejszej podsekcji;

(B) jakiegokolwiek przejęcia lub rozdysponowania taką nieruchomością; i

(C) jakiejkolwiek procedury administracyjnej lub sądowej będącej w związku z taką nieruchomością

– jeśli nie odpowiadają niniejszej sekcji.

(4) pomimo sekcji 524 (c) tytułu 28, wszelkie dochody uzyskane z konfiskaty nieruchomości na podstawie tej sekcji, pozostające po zapłacie kosztów konfiskaty i sprzedaży, zgodnie z prawem są deponowane w Funduszu Ofiar Przestępstw prowadzonym przez Skarb Państwa.

2 Terroryzm

Kodeks Stanów Zjednoczonych. **Tytuł 18 –** *Przestępstwa i procedura karna*. **Część I –** *Przestępstwa*. **Rozdział 113B –** *Terroryzm*

§ 2331 – *Definicje* i § 2332b – *Akty terrorystyczne o charakterze transgranicznym*

Ustawodawstwo amerykańskie rozróżnia pojęcia terroryzm międzynarodowy i terroryzm krajowy.

Terroryzm międzynarodowy oznacza czyny, które zawierają następujące elementy:

- obejmują akty przemocy lub akty niebezpieczne dla życia ludzkiego, które naruszają prawo federalne lub stanowe;
- są podejmowane z zamiarem zastraszenia lub zmusenia społeczeństwa do określonych działań; aby wpłynąć na politykę rządu przez zastraszenie lub zmuszenie do określonego działania oraz aby wpłynąć na działanie rządu przez masową zagładę, zamach lub porwanie, i
- występują zasadniczo poza jurysdykcją terytorialną Stanów Zjednoczonych lub wykraczają poza granice krajowe w zakresie środków, za których pomocą są dokonywane, osób, które podejmują się tych czynów z zamiarem zastraszenia lub zmuszenia [do określonego działania], albo miejsca, w którym sprawcy działają lub szukają schronienia.

Krajowy terroryzm oznacza czyny, które zawierają następujące elementy:

- obejmują akty niebezpieczne dla ludzkiego życia, które naruszają prawo federalne lub stanowe;
- są podejmowane z zamiarem zastraszenia lub zmuszenia społeczeństwa do określonych działań, aby wpłynąć na politykę rządu przez zastraszenie lub zmuszenie do określonego działania oraz aby wpłynąć na działanie rządu przez masową zagładę, zamach lub porwanie i
- występują zasadniczo w jurysdykcji terytorialnej Stanów Zjednoczonych.

W prawie amerykańskim jest regulowane również pojęcie przestępstwo federalne terroryzmu, oznaczające przestępstwo, które:

- jest obliczone, aby wpłynąć lub dotyczyć postępowania rządu przez zastraszenie lub zmuszenie [do określonego działania] albo oznacza działanie odwetowe na rządzie, z uwagi na jego postępowanie, i
- jest pogwałceniem jednej z kilku wymienionych ustaw, włączając w to § 930(c) odnoszący się do zabójstwa lub usiłowania zabójstwa czasie ataku na obiekt rządowy z użyciem niebezpiecznego narzędzia, i § 1114 odnoszący się do zabójstwa lub próby dokonania zabójstwa oficerów i pracowników amerykańskiego rządu.

CZĘŚĆ III

Przepisy szczególne dotyczące funkcjonowania służb specjalnych

BELGIA

1. Ochrona informacji niejawnych

Zgodnie z art. 7 pkt 2 ustawy o służbach wywiadowczych i bezpieczeństwa do zadań VSSE należy prowadzenie postępowań sprawdzających powierzonych jej na mocy dyrektyw Komitetu Ministerialnego. Funkcję krajowej władzy bezpieczeństwa, zgodnie z dekretem wykonawczym do ustawy o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa z 24 marca 2000 r. pełni organ o nazwie Autorité Nationale de Securité (Narodowa Władza Bezpieczeństwa). Jest to organ kolegialny, który odpowiada za wydawanie i odbieranie poświadczeń bezpieczeństwa oraz za sprawowanie nadzoru nad systemem ochrony informacji niejawnych. Na zasadzie wyjątku, funkcje Narodowej Władzy Bezpieczeństwa w stosunku do osób zatrudnionych w VSSE i kandydatów do służby pełni dyrektor generalny VSSE.

2. Sposoby realizacji zadań

Art. 12 Służby wywiadowcze i bezpieczeństwa mogą pozyskiwać, gromadzić, otrzymywać i przetwarzać informacje oraz dane osobowe, które mogą być istotne z punktu widzenia realizacji ich zadań, oraz prowadzić dokumentację dotyczącą zdarzeń, ugrupowań i osób mających znaczenie dla realizacji tych zadań.

3. Wyłączenie odpowiedzialności funkcjonariuszy

Art. 13 § 2. Funkcjonariusze odpowiedzialni za prowadzenie czynności związanych z pozyskiwaniem informacji nie mogą podczas wykonywania tych czynności naruszać powszechnie obowiązujących przepisów prawa.

Na zasadzie wyjątku od zasady opisanej powyżej karze nie podlegają funkcjonariusze, którzy w toku realizacji swoich zadań naruszają przepisy kodeksu drogowego lub innych ustaw w celu zapewnienia skuteczności wykonywania zadań lub w celu ochrony własnego bezpieczeństwa lub bezpieczeństwa innych osób.

Karze nie podlegają funkcjonariusze, którzy w toku wykorzystywania specjalnych metod pozyskiwania informacji określonych w art. 18/2 popełniają, po uzyskaniu uprzedniej zgody komisji, przestępstwo absolutnie niezbędne do zagwarantowania skuteczności wykonywania określonego zadania lub w celu ochrony ich bezpieczeństwa albo bezpieczeństwa innych osób. Dotyczy to również osób, które udzieliły pomocy lub wsparcia niezbędnego do realizacji zadania.

4. Ochrona danych osobowych

Art. 21 Dane osobowe przetwarzane w ramach realizacji niniejszej ustawy są przechowywane przez okres niezbędny do osiągnięcia celów, w jakich zostały zebrane, z wyjątkiem danych o charakterze historycznym.

Dane, o których mowa powyżej, podlegają zniszczeniu po upływie określonego czasu od momentu ich ostatniego przetwarzania.

HISZPANIA

Narodowe Centrum Wywiadowcze

Ustawa nr 2/2002 z dnia 6 maja 2002 r. regulująca uprzednią kontrolę sądową Narodowego Centrum Wywiadowczego[1]

Sekcja 1. Uprzednia kontrola sądowa Narodowego Centrum Wywiadowczego.

1. Sekretarz stanu – nyrektor CNI składa wniosek do właściwego sędziego Sądu Najwyższego (zgodnie z ustawą o sądownictwie), w celu uzyskania nakazu zastosowania środków, które mogą oddziaływać na prawo do prywatności i tajemnicę komunikacji, pod warunkiem, że takie środki są konieczne do wykonania zadań powierzonych służbie.
2. Pisemny wniosek o nakaz, o którym mowa w ust. 1, powinien zawierać następujące elementy:
   a) wyszczególnienie środków, których wniosek dotyczy;
   b) okoliczności, na jakich podstawie wniosek jest oparty, cel takiego wniosku i powody uzasadniające wykorzystanie wymienionych środków;
   c) identyfikację osoby lub osób, wobec których zostaną zastosowane środki, jeśli są możliwe do zidentyfikowania i określenie miejsca, gdzie ww. środki będą stosowane.

   Okres zastosowania ww. środków nie może przekroczyć 24 godz., jeśli dotyczą one prawa do prywatności, oraz 3 miesięcy w przypadku przechwycenia poczty, komunikacji telefonicznej lub jakiejkolwiek innej. Wymienione terminy mogą zostać przedłużone o okres, na który zostały złożone wnioski o ich zastosowanie.
4. Sąd powinien udzielić zgody lub odmówić wydania nakazu w okresie 72 godz. Wymieniony okres ulega skróceniu do 24 godz. w przypadku nagłej potrzeby, uzasadnionej we wniosku o nakaz sekretarza stanu – dyrektora CNI, który we wszystkich sprawach powinien wskazać elementy określone powyżej. Sąd powinien podjąć niezbędne kroki w celu ochrony niejawności działań, które powinny być klasyfikowane jako „ściśle tajne".
5. Sekretarz stanu – dyrektor CNI zarządza niezwłoczne zniszczenie wszelkich informacji zebranych na mocy nakazu, o którym mowa w niniejszej sekcji, niepowiązanych z celem tego nakazu.

[1] *Organic Law 2/2002 of 6th May 2002 regulating a priori judicial control of the Centro National de Intelligencia* (*National Intelligence Centre*) [online], www.cni.es/en/Rules_and_regulations/ [dostep: 10 II 2017].

Ustawa 11/2002 z dnia 6 maja 2002 r. regulująca funkcjonowanie Narodowego Centrum Wywiadowczego[2]

Sekcja 4. Funkcje Narodowego Centrum Wywiadowczego.

a) gromadzenie, ocena i interpretacja informacji oraz przekazywanie niezbędnych danych wywiadowczych w celu ochrony i promowania politycznych, gospodarczych, przemysłowych, handlowych i innych strategicznych interesów Hiszpanii w kraju oraz za granicą;
b) zapobieganie, wykrywanie i neutralizacja działań zagranicznych służb, grup albo osób, które zagrażają konstytucyjnemu porządkowi, prawom i wolnościom hiszpańskich obywateli, suwerenności, integralności, bezpieczeństwu państwa, stabilności instytucji, narodowym interesom gospodarczym oraz dobrobytowi społeczeństwa;
c) promowanie współpracy z innymi służbami wywiadowczymi państw obcych lub organizacji międzynarodowych, w celu wykonywania zadań i poprawy efektywności pracy;
d) uzyskiwanie, ocena i interpretacja sygnałów o znaczeniu strategicznym dla wywiadu;
e) koordynacja czynności instytucji rządowych, które stosują szyfrowanie środków lub procedur w celu zagwarantowania bezpieczeństwa technologii informacji w tym obszarze; raportowanie o skoordynowanym gromadzeniu materiałów kryptograficznych oraz szkolenie ekspertów własnych lub innych agencji rządowych w celu zapewnienia właściwego funkcjonowania służby;
f) monitorowanie działań zgodnie z ustawodawstwem w zakresie ochrony informacji niejawnych;
g) gwarantowanie bezpieczeństwa i ochrona własnych obiektów, informacji, materiałów i źródeł osobowych.

Sekcja 5. Czynności podejmowane przez Narodowe Centrum Wywiadowcze.

1. Informacje dotyczące czynności podejmowanych przez CNI, a także jego organizacji i struktury wewnętrznej, źródeł i procedur, spraw dotyczące personelu, sprzętu, baz danych, źródeł informacji oraz informacji lub danych, które mogą pozwolić na zdobycie wiedzy w powyższych sprawach, są niejawne i oznaczone klauzulą „ściśle tajne" lub objęte najwyższym poziomem ochrony informacji niejawnych przewidzianym umowami międzynarodowymi.
2. CNI może na potrzeby prowadzonych działań stosować środki kamuflujące i operacje pod przykryciem, uzyskiwać zgody, ustalać tożsamości oraz dane dotyczące numerów tablic rejestracyjnych od organów, które odpowiadają za ich wydanie.
3. CNI wykonując zadania, może prowadzać postępowania sprawdzające osób fizycznych oraz przedsiębiorców, zgodnie z ustawą regulującą uprzednią kontrolę sądową tej służby. W celu prowadzenia ww. procedur podmioty prywatne i publiczne i inne instytucje mogą zostać zobowiązane do współpracy z CNI.

[2] *Act 11/2002 of 6th May regulating the Centro National de Inteligencia* (*National Intelligence Centre*) [online], https://www.cni.es/comun/recursos/descargas/11-2002-INGLES.pdf [dostep: 10 II 2017]. Nazwa oryginalna dokumentu: *Ley 11/2002, de 6 de mayo regulatora del CNI* [online], https://www.cni.es/comun/recursos/descargas//Ley_11-2002_de_6_de_mayo_pdf.

KANADA

1. Ustawa o Kanadyjskiej Służbie Bezpieczeństwa i Wywiadu (CSIS)[3] – wyciąg

Art. 2. Zagrożenia bezpieczeństwa Kanady oznaczają:

a) szpiegostwo i sabotaż wymierzone w Kanadę lub zagrażające jej interesom, a także działalność wspierająca szpiegostwo i sabotaż;
b) działania inspirowane z zagranicy, które są przeprowadzane w Kanadzie lub jej dotyczą, zagrażające interesom tego kraju, prowadzone w sposób niejawny, podstępny lub stanowiące zagrożenie dla osób;
c) działania prowadzone w Kanadzie lub jej dotyczące, które mają na celu wspieranie użycia poważnej przemocy lub gróźb jej użycia wobec osób lub mienia z zamiarem osiągnięcia celu politycznego, religijnego lub ideologicznego w Kanadzie lub w innym państwie;
d) działalność mająca na celu osłabienie lub obalenie przy użyciu siły systemu rządowego ustanowionego zgodnie z konstytucją, przez działania niejawne i bezprawne.

Źródło osobowe – osoba fizyczna, która po otrzymaniu gwarancji poufności dostarczyła, dostarcza lub jest prawdopodobne, że będzie dostarczać informacje CSIS.

2. Obowiązki i zadania służby

Art. 12. (1) CSIS zbiera, w zakresie, w jakim jest to absolutnie konieczne, analizuje i przechowuje informacje dotyczące aktywności, które mogą stanowić zagrożenie bezpieczeństwa Kanady, oraz przekazuje je rządowi i pełni wobec niego w tym zakresie funkcję konsultacyjną.

(2) CSIS może realizować zadania określone w § 1 na terytorium Kanady lub poza jej granicami.

3. Instrumenty zwalczania zagrożeń bezpieczeństwa Kanady

Art. 12.1. (1) Jeżeli zachodzi uzasadnione podejrzenie, że określona działalność stanowi zagrożenie bezpieczeństwa Kanady, CSIS może wykorzystywać przewidziane w ustawie środki w celu neutralizacji tego zagrożenia.

(2) Instrumenty powinny być wykorzystywane w sposób uzasadniony i proporcjonalny do okoliczności danej sytuacji, biorąc pod uwagę rodzaj zagrożenia, charakter instrumentów i dostępność innych środków, które mogą zneutralizować zagrożenie.

(3) Służba nie wykorzystuje instrumentów zwalczania zagrożeń bezpieczeństwa Kanady, jeżeli istnieje prawdopodobieństwo, że naruszą one prawa i wolności gwarantowane przez Kartę Praw i Wolności Kanady lub będą sprzeczne z innymi przepisami prawa, chyba że uzyskała zgodę na wykorzystanie tych instrumentów na mocy nakazu wydanego na podstawie art. 21.1.

(4) Żaden z przepisów zawartych w § (1) nie przyznaje służbie uprawnień policyjnych (*law enforcement power*)[4].

---

[3] *Canadian Security Intelligence Service Act. R.S.C., 1985, c. C-23* [online], www.laws-lois.justice.gc.ca/eng/acts/C-23/ [dostęp: 14 II 2017].

[4] We francuskojęzycznej wersji ustawy posłużono się terminem c o n t r ô l e d ' a p p l i c a t i o n d e l a

4. Działania niedozwolone

Art. 12.2. (1) Stosując instrumenty zwalczania zagrożeń bezpieczeństwa Kanady, służba nie może:

a) spowodować, umyślnie bądź przez zaniedbanie karalne, śmierci lub uszczerbku na zdrowiu osoby;
b) umyślnie dążyć do zakłócenia czynności wymiaru sprawiedliwości;
c) naruszać nietykalności seksualnej osoby.

5. Ocena bezpieczeństwa

Art. 13. (1) Służba może sporządzać oceny bezpieczeństwa (*security assessment*)[5] dla poszczególnych departamentów rządu Kanady.

6. Funkcje konsultacyjno-doradcze wobec ministrów

Art. 14. Służba może:

a) doradzać ministrom w sprawach dotyczących bezpieczeństwa Kanady;
b) udzielać ministrom informacji dotyczących bezpieczeństwa lub działalności przestępczej,

– istotnych z punktu widzenia kompetencji ministrów lub wykonywania przez nich jakichkolwiek czynności zgodnie z ustawą o obywatelstwie albo z ustawą o imigracji i ochronie uchodźców.

7. Postępowania

Art. 15. (1) CSIS może prowadzić postępowania (*investigations*) niezbędne do sporządzenia oceny bezpieczeństwa zgodnie z art. 13 lub w celu realizacji zadań konsultacyjno-doradczych określonych w art. 14.

(2) Służba może realizować zadania określone w § 1 na terytorium Kanady lub poza jej granicami.

8. Zbieranie informacji dotyczących innych państw i osób zagranicznych

Art. 16. (1) Służba może, na zasadach określonych w niniejszym artykule, udzielać wsparcia ministrowi obrony narodowej lub ministrowi spraw zagranicznych w sprawach dotyczących obronności lub stosunków międzynarodowych Kanady, w zakresie pozyskiwania informacji dotyczących zdolności, zamiarów lub działalności:

a) innego państwa lub grup innych państw;
b) osób innych niż:
   i) obywatel Kanady;
   ii) stały rezydent w rozumieniu podsekcji 2 (1) ustawy o imigracji i ochronie uchodźców;
   iii) osoba prawna utworzona na mocy ustawy lub przez organ prawodawczy prowincji.

---

l o i , co dosłownie można tłumaczyć jako ’kontrola stosowania prawa’.

[5] Ang. *security assessment* – ocena lojalności wobec Kanady, w zakresie, w jakim ma to związek z wiarygodnością danej osoby.

(…)

(3) Służba wykonuje czynności wynikające z § 1:

a) na osobisty, pisemny wniosek ministra obrony narodowej lub ministra spraw zagranicznych lub
b) po uzyskaniu pisemnej zgody ministra obrony narodowej lub ministra spraw zagranicznych.

9. Kontrola sądowa

Art. 21. (1) Jeżeli dyrektor lub funkcjonariusz upoważniony w tym celu przez ministra ma uzasadnione powody, aby sądzić, że wydanie nakazu zgodnie z niniejszym artykułem jest niezbędne do zbadania wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa Kanady lub do wykonania zadań zgodnie z art. 16 (zbieranie informacji), dyrektor lub pracownik może, po uzyskaniu zgody ministra, złożyć do sądu wniosek o wydanie nakazu na zasadach określonych w niniejszym artykule.

(2) Wniosek powinien mieć formę pisemną oraz zawierać oświadczenie określające następujące elementy:

a) fakty uzasadniające przeświadczenie, że zbadanie zagrożenia bezpieczeństwa Kanady lub pozyskiwanie informacji, o których mowa w art. 16, wymagają wydania nakazu;
b) wskazanie, że inne metody okazały się nieprzydatne do osiągnięcia zamierzonego celu lub że osiągnięcie tego celu przy ich wykorzystaniu jest mało prawdopodobne albo że skala i nieuchronność zagrożenia sprawia, że wykorzystanie innych metod byłoby niepraktyczne albo też wykazanie, że niewydanie nakazu spowoduje, że informacja mająca istotne znaczenie dla bezpieczeństwa Kanady nie zostanie uzyskana;
c) określenie rodzaju komunikacji, która ma zostać przechwycona, rodzaju informacji, wskazanie zapisów, dokumentów lub rzeczy, które mają zostać uzyskane, oraz określenie, które z metod wymienionych w § 3 a-c mają zostać w tym celu wykorzystane;
d) wskazanie tożsamości osoby, jeżeli jest ona znana służbie, której komunikacja ma zostać przechwycona lub która posiada informacje, zapisy, dokumenty lub rzeczy, które mają zostać uzyskane;
e) wskazanie osób lub grup osób, przeciwko którym nakaz ma zostać wydany;
f) ogólny opis miejsca, w którym nakaz ma zostać wykonany, jeżeli na podstawie posiadanych informacji jest to możliwe;
g) określenie okresu, nie dłuższego niż 60 dni lub 1 rok, w którym nakaz ma pozostawać w mocy zgodnie z § 5;
h) informację o ewentualnych wcześniejszych nakazach wydanych przeciwko tej samej osobie, datę tego nakazu oraz imię i nazwisko sędziego, który wydał ten nakaz.

(3) Bez uszczerbku dla norm wynikających z innych aktów prawnych, z zastrzeżeniem przepisów ustawy o statystyce, jeżeli sędzia, do którego wniosek został skierowany zgodnie z podsekcją 1 uzna, że istnieją przesłanki do wydania nakazu, może wydać taki nakaz upoważniający do przechwycenia komunikacji osoby, której wniosek dotyczy, oraz do uzyskania o niej wszelkich informacji, zapisów, dokumentów lub przedmiotów i dokonania – w celu pozyskania niezbędnych informacji – następujących czynności:

a) wejścia do miejsc lub pomieszczeń w celu uzyskania dostępu do znajdujących się w nich przedmiotów;
b) poszukiwania, usuwania, zwrotu, badania, pobrania próbek, kopiowania lub utrwalania w inny sposób informacji, zapisów, dokumentów lub przedmiotów;
c) zainstalowania, utrzymywania lub usuwania jakichkolwiek przedmiotów.

10. Działania poza terytorium Kanady

Art. 21.1. (4) Niezależnie od postanowień jakiejkolwiek innej ustawy, w tym aktów prawnych innych państw, sędzia może na podstawie nakazu wydanego zgodnie z podsekcją 3 wyrazić zgodę na podejmowanie czynności poza terytorium Kanady w celu zbadania zagrożenia jej bezpieczeństwa.

11. Elementy nakazu

Art. 21.1. (5) Nakaz wydany na podstawie § 3 powinien zawierać:
a) instrumenty, na których wykorzystanie ten dokument zezwala;
b) tożsamość osoby (jeżeli jest znana służbie), której komunikacja ma zostać przechwycona lub która jest w posiadaniu informacji, zapisu, dokumentu albo przedmiotu, który ma zostać pozyskany;
c) osoby lub kategorie osób, przeciwko którym nakaz jest skierowany;
d) ogólny opis miejsca, w którym nakaz ma zostać wykonany, jeżeli na podstawie posiadanych informacji jest to możliwe;
e) określenie, przez jaki okres nakaz jest ważny;
f) warunki lub elementy, których umieszczenie w nakazie sędzia uznaje za pożądane w interesie publicznym.

12. Maksymalny czas trwania nakazu

Art. 21. 1 (6) Nakaz może zostać wydany na okres nieprzekraczający:
a) 60 dni, jeżeli został wydany w celu upoważnienia służby do zbadania zagrożenia bezpieczeństwa Kanady w rozumieniu § d sekcji 2 zawierającego definicję pojęcia zagrożenia bezpieczeństwa Kanady;
b) 120 dni w innych przypadkach.

13. Przedłużenie nakazu

Art. 22. Sędzia może na wniosek osoby upoważnionej do złożenia wniosku o wydanie nakazu, po uzyskaniu przez tę osobę zgody ministra, przedłużyć stosowanie nakazu na czas nieprzekraczający okresu, na który nakaz może zostać wydany zgodnie z art. 21 (5), jeżeli dowody wskazują, że:
a) nakaz jest niezbędny do umożliwienia służbie zbadania zagrożenia bezpieczeństwa Kanady lub do wykonywania przez służbę zadań zgodnie z art. 16;
b) następują fakty, o których mowa w art. 21 (2) b (nieskuteczność innych metod).

22.1. (1) Sędzia może na wniosek osoby upoważnionej do złożenia wniosku o wydanie nakazu, po uzyskaniu zgody ministra, jeżeli w uzasadnionej opinii tej osoby

nakaz jest w dalszym ciągu niezbędny do zwalczania zagrożeń bezpieczeństwa Kanady, przedłużyć stosowanie nakazu, jeżeli dowody wskazują, że:

a) dalsze stosowanie nakazu jest konieczne w świetle zaistniałych okoliczności;
b) stosowanie nakazu jest w dalszym ciągu rozsądne i proporcjonalne, mając na względzie charakter zagrożenia, rodzaj wykorzystywanych środków i dostępność innych metod powalających na neutralizację zagrożenia.

(2) Stosowanie nakazu wydanego na podstawie art. 21.1 (3) może być przedłużone tylko dwa razy, z czego każdorazowo może być przedłużone na czas nieprzekraczający okresu określonego w art. 21.1 (6) (60 lub 120 dni).

14. Ograniczenia w wykonywaniu nakazu

Art. 22.2. Osoba lub grupa osób wykonująca czynności, które mają na celu realizacjęnakazu wydanego na podstawie art. 21.1, może podejmować środki określone w nakazie tylko wówczas, gdy w świetle okoliczności sprawy jest to uzasadnione, proporcjonalne i adekwatne do charakteru zagrożeń.

LUKSEMBURG

1. Ochrona informacji niejawnych

Ustawa z dnia 15 czerwca 2004 r. o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa[6] (wyciąg)

Art. 2. Pojęcia używane w niniejszej ustawie oznaczają:

1. Krajowa Władza Bezpieczeństwa – organ odpowiedzialny za zapewnienie ochrony informacji niejawnych. (…)

Art. 19. Funkcję Krajowej Władzy Bezpieczeństwa sprawuje Służba Wywiadu (SRE).

Art. 20. W toku realizacji jej kompetencji ustawowych Krajowa Narodowa Władza Bezpieczeństwa wykonuje następujące czynności:

- zapewnia ochronę informacji niejawnych przetwarzanych przez podmioty cywilne i wojskowe;
- współpracuje z organami sprawującymi funkcję krajowej władzy bezpieczeństwa w innych państwach, szczególnie należących do organizacji międzynarodowych, których członkiem jest Luksemburg;
- prowadzi postępowania sprawdzające, o których mowa w art. 14 niniejszej ustawy;
- prowadzi postępowania sprawdzające na wniosek organizacji międzynarodowych lub zagranicznych służb bezpieczeństwa w ramach realizacji umów międzynarodowych. Te postępowania są prowadzone na zasadach przewidzianych w niniejszej ustawie.

[6] *Loi du 15 juin 2004 relative à la classification des pieces et aux habilitations de sécurité* [online], www.legilux.public.lu/eli/etat/leg/loi/2004/06/15/n5/jo [dostęp: 19 IV 2017].

Art. 21. Krajowa Władza Bezpieczeństwa może pozyskiwać, na potrzeby postępowania sprawdzającego, informacje o stanie cywilnym, wypłacalności, sytuacji społecznej i zawodowej, zarówno aktualnej, jak i przeszłej – reputacji oraz podatności i wrażliwości na formy nacisku osoby, wobec której toczy się postępowanie sprawdzające.

Art. 22. Krajowa Władza Bezpieczeństwa może pozyskiwać na potrzeby postępowania sprawdzającego informacje z baz danych, o których mowa w art. 4 ustawy o Służbie Wywiadu, na zasadach określonych w tej ustawie.

Art. 23. Zasady przetwarzania informacji uzyskanych przez Krajową Władzę Bezpieczeństwa w toku realizacji jej ustawowych zadań określa rozporządzenie, o którym mowa w art. 17 *Ustawy z dnia 2 sierpnia 2002 r. o ochronie danych osobowych*[7].

Informacje zebrane przez Krajową Władzę Bezpieczeństwa mogą zostać wykorzystane wyłącznie w celu realizacji zadań, o których mowa w art. 20.

Dane z postępowań sprawdzających nie mogą być dołączane do akt osobowych funkcjonariusza, wobec którego toczyło się postępowanie.

Informacje uzyskane w ramach postępowania sprawdzającego podlegają zniszczeniu lub usunięciu:

- po upływie 6 miesięcy od wydania decyzji odmawiającej wydania poświadczenia bezpieczeństwa, chyba że powody, z jakich zostały one zebrane, są w dalszym ciągu istotne;
- po upływie 5 lat od chwili, gdy osoba sprawdzana przestała sprawować funkcję wymagającą dostępu do informacji niejawnych.

Art. 24. Krajowa Władza Bezpieczeństwa stosuje wewnętrzne środki ochrony w celu zapewnienia poufności informacji uzyskanych w toku postępowania sprawdzającego.

Art. 25. Krajowa Władza Bezpieczeństwa wszczyna postępowanie sprawdzające na wniosek pełnomocnika ochrony (dosł. oficera bezpieczeństwa), któremu podlega osoba, której stanowisko wymaga dostępu do ochrony informacji niejawnych. Do wniosku dołącza się wypełniony i podpisany przez tę osobę kwestionariusz.

Osoba, wobec której ma się toczyć postępowanie, musi przed jego wszczęciem wyrazić zgodę na jego przeprowadzenie.

Zgoda, o której mowa powyżej, nie jest wymagana, jeśli jest konieczne przeprowadzenie kolejnego postępowania, które ma na celu weryfikację informacji uzasadniających podejrzenie, że osoba posiadająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy.

Jeżeli osoba, której funkcja wymaga dostępu do informacji niejawnych, przebywa za granicą lub przejeżdża przez terytorium innego państwa, Krajowa Władza Bezpieczeństwa może zwrócić się do właściwych organów tych państw o udzielenie pomocy. Na zasadzie analogii – właściwe organy innych państw mogą zwrócić się do Krajowej Władzy Bezpieczeństwa o udzielenie pomocy, jeżeli osoba, której funkcja wymaga dostępu do informacji niejawnych na mocy prawa innego państwa, przebywa lub przejeżdża przez terytorium Luksemburga.

[7] *La loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* [online], www.legilux.public.lu/eli/etat/leg/loi/2002/08/02/n2/jo [dostęp: 19 IV 2017].

2. Dostęp do baz danych

Art. 4.1. Przetwarzanie przez SRE informacji uzyskanych w toku realizacji jej ustawowych zadań odbywa się zgodnie z zasadami przewidzianymi w rozporządzeniu, do którego wydania zobowiązuje *Ustawa z dnia 2 sierpnia 2002 r. o ochronie danych osobowych*.

Art. 4.2. W toku realizacji ustawowych zadań SRE jest uprawniona do dostępu do następujących baz danych:

- Ogólnego Rejestru Osób Fizycznych i Prawnych utworzonego na podstawie *Ustawy z dnia 30 marca 1979 r. o identyfikacji cyfrowej osób fizycznych i prawnych*[8],
- części baz danych Policji umożliwiających wyszukiwanie danych osobowych;
- biuletynu wchodzącego w skład Rejestru Sądowego (Biuletyn nr 2);
- bazy danych zawierającej informacje o cudzoziemcach wykorzystywanej na rachunek komórki Policji ds. cudzoziemców, działającej w ramach Ministerstwa Sprawiedliwości;
- bazy danych zawierającej informacje o pracownikach, pracodawcach i osobach wykonujących tzw. wolne zawody, zarządzanej przez organ ubezpieczeń społecznych zgodnie z art. 321 kodeksu ubezpieczeń społecznych;
- bazy danych zawierającej informacje o pojazdach drogowych, ich właścicielach i posiadaczach, wykorzystywanej na rachunek Ministerstwa Transportu; (…).

Dostęp do baz danych podlega kontroli organu, o którym mowa w art. 17 § 2 ustawy o ochronie danych osobowych W związku z realizacją kontroli SRE jest zobowiązana do wykorzystywania środków technicznych zapewniających możliwość każdorazowego ustalenia osób korzystających z tych baz i okoliczności dostępu do nich.

Art. 4.3. Informacje zebrane przez SRE mogą być wykorzystywane wyłącznie w celu realizacji zadań, o których mowa w art. 2 ustawy.

Art. 4.4. SRE może żądać od osób fizycznych i prawnych udostępnienia informacji niezbędnych do realizacji jej zadań niebędących danymi osobowymi.

SZWAJCARIA

Ustawa o Federalnej Służbie Wywiadowczej[9] (wyciąg)

Rozdział I. Ogólne postanowienia i zasady

Zbieranie informacji

Art. 2. Cele.

Ustawa ma na celu:

[8] *Loi du 30 mars organisant l'identification numérique des personnes physiques et morales* [online], www.legilux.public.lu/eli/etat/leg/loi/1979/03/30/n1/jo [dostęp: 19 IV 2017].

[9] Ang. *Federal Act on Intelligence Service* (*Intelligence Service Act*, ISA) [online], www. Admin.ch/opc/de/federal-gatette/2015/7211.pdf [dostęp: 10 II 2017].

a) zagwarantować demokratyczne i konstytucyjne podstawy państwa,
b) zapewnić bezpieczeństwo społeczeństwa Szwajcarii oraz działań prowadzonych za granicą państwa,
c) wspierać zdolności państwa do właściwego działania,
d) uczestniczyć w ochronie międzynarodowych interesów w zakresie bezpieczeństwa.

Art. 3. Zastosowanie w szczególnych sytuacjach.

Rada Federalna może w szczególnych sytuacjach zlecić Nachrichtendienst des Bundes (NBD) ochronę innych niezbędnych interesów narodowych; do podstawowych tego typu działań należy: ochrona konstytucyjnych podstaw Szwajcarii, wsparcie szwajcarskiej polityki zagranicznej i ochrona szwajcarskiej gospodarki, przedsiębiorstw oraz instytucji finansowych.

(…)

Art. 5. Zasady gromadzenia informacji.

1. W celu wykonywania swoich zadań NDB gromadzi informacje ze źródeł dostępnych publicznie.
2. NDB gromadzi informacje również ze źródeł niejawnych.
3. NDB stosuje takie środki gromadzenia informacji, które:
   a) są najbardziej odpowiednie i niezbędne do osiągnięcia konkretnego celu realizacji lub zadania,
   b) najmniej ingerują w podstawowe prawa osób zainteresowanych.
4. NDB może pozyskiwać dane osobowe podmiotów bez ich wiedzy.
5. NDB nie gromadzi ani nie przetwarza żadnych informacji na temat działań politycznych czy dotyczących wolności słowa oraz wyrażania opinii, a także wolności zgromadzeń i zrzeszania się w Szwajcarii.
6. NDB może w konkretnych przypadkach pozyskiwać informacje, o których mowa w pkt 5, od organizacji lub osób, jeśli wykonuje swoje uprawnienia w zakresie zwalczania terroryzmu lub działań ekstremistycznych.
7. NDB usuwa dane osobowe, jeśli tylko czynności, o których mowa w pkt 5, są zakończone, ale nie później niż po upływie roku od ich rozpoczęcia.
8. NDB może przeszukiwać siedziby organizacji znajdujących się na liście obserwowanych.

Rozdział II. Zadania i współpraca NDB.

Art. 6. Zadania NDB.

1. Gromadzenie i przetwarzanie informacji przez NDB ma służyć:
   a) wczesnemu wykrywaniu i zapobieganiu zagrożeniom bezpieczeństwa wewnętrznego lub zewnętrznego państwa związanym z:
      – terroryzmem,
      – działaniami obcych wywiadów,
      – rozprzestrzenianiem broni nuklearnej, chemicznej lub biologicznej, w tym środków jej przenoszenia i jej wytwarzania, w zakresie niezbędnym do celów wojskowych lub cywilnych; technologii (proliferacji) lub nielegalnego handlu substancjami radioaktywnymi, amunicją i sprzętem wojskowym,

– atakiem na systemy informatyczne, komunikację, energetykę, transport i inne elementy infrastruktury istotne dla funkcjonowania społeczeństwa, biznesu i administracji publicznej (infrastruktura krytyczna),
– ekstremizmem z użyciem przemocy;

b) wykrywaniu, monitorowaniu i ocenie polityki bezpieczeństwa istotnych zdarzeń za granicą;
c) zabezpieczaniu zdolności Szwajcarii do działań;
d) ochronie podstawowych interesów narodowych na mocy art. 3, jeżeli takie zadania zostały zlecone przez Radę Federalną.

2. NDB dokonuje oceny zagrożenia państwa oraz informuje zainteresowane kantonalne i lokalne organy ścigania o wszelkich niebezpieczeństwach i podjętych środkach oraz o planowanych działaniach w ramach niniejszej ustawy.
3. NDB informuje inne agencje federalne, kantonalne, z przestrzeganiem zasady ochrony źródeł, o zdarzeniach i ustaleniach, które dotyczą utrzymania bezpieczeństwa wewnętrznego lub zewnętrznego państwa.
4. NDB utrzymuje relacje ze służbami zagranicznymi.
5. NDB wykorzystuje systemy wczesnego ostrzegania w celu ochrony infrastruktury krytycznej.
6. NDB prowadzi programy informacyjne i uświadamiające dotyczące zagrożeń bezpieczeństwa wewnętrznego lub zewnętrznego państwa.
7. NDB chroni swoich pracowników, źródła oraz przetwarzane informacje.

(…)

Art. 12. Współpraca z państwami obcymi.

1. NDB może współpracować z zagranicznymi służbami wywiadowczymi i agencjami bezpieczeństwa. Ta współpraca polega na:
   a) odbieraniu i przesyłaniu odpowiednich informacji;
   b) odbywaniu wspólnych spotkań;
   c) przeprowadzaniu wspólnych działań mających na celu gromadzenie i analizę informacji oraz ocenę zagrożeń;
   d) uzyskiwaniu i przekazywaniu informacji państwu współpracującemu w celu:
      – ustalenia uczestnictwa danej osoby w prowadzeniu niejawnych projektów za granicą, ustalenia bezpieczeństwa wewnętrznego i zewnętrznego państwa, dostępu do informacji niejawnych, materiałów oraz sprzętu należącego do państwa zagranicznego;
   e) tworzeniu wspólnych systemów informacyjnych;
2. NDB w porozumieniu z Federalnym Departamentem Spraw Zagranicznych może zezwolić na promowanie kontaktów międzynarodowych pracowników (funkcjonariuszy) reprezentujących Szwajcarię za granicą. Wymienione działania mogą być prowadzone bezpośrednio z właściwymi organami państw trzecich.
3. W ramach postanowień niniejszej ustawy inne władze federalne i władze kantonów mogą otrzymać polecenie nawiązania i utrzymywania kontaktów z zagranicznymi służbami wywiadowczymi lub innymi podmiotami zagranicznymi.

Rozdział III. Informacje

Sekcja I. Gromadzenie informacji bez autoryzacji.

Art. 13. Źródła informacji dostępne publicznie.

Publicznymi źródłami informacji są przede wszystkim:

a) media dostępne publicznie,
b) rejestr publiczny władz federalnych i kantonów,
c) prywatne zbiory informacji publicznie dostępnych podmiotów prywatnych,
a) wystąpienia publiczne.

Art. 14. Obserwacja w miejscach publicznych.

1. NDB może prowadzić operacje w miejscach publicznych i obiektach powszechnie dostępnych, może także przechwytywać obraz i dźwięk. Przy wykonywaniu powyższych czynności może korzystać z urządzeń elektronicznych i satelitów.
2. Obserwacja i retencja obrazów i dźwięków pozyskanych w czasie operacji, które są przypisane do chronionej sfery prywatnej, jest niedozwolone.

Art. 15. Źródła osobowe.

1. Źródłami osobowymi są osoby, które:
   a) przekazują NDB informacje lub ustalenia,
   b) wykonują zadania zlecone przez NDB,
   c) wspierają NDB w pozyskiwaniu informacji.
2. NDB może wynagradzać źródła osobowe za ich usługi.
3. NDB podejmuje niezbędne środki w celu ochrony życia i zdrowia źródeł osobowych. Te środki mogą również być stosowane wobec osób związanych ze źródłami osobowymi.
4. Po zakończeniu współpracy ze służbą osobowym źródłom informacji – w celu ochrony ich życia i zdrowia – może być nadana legenda.

CZĘŚĆ IV

Przepisy regulujące działalność wywiadowczą poza granicami kraju

KANADA

Ustawa o obronie narodowej (National Defence Act – 1995[1]) (fragmenty)

Zakres kompetencji

Art. 273.64 (1) Do zadań Służby Bezpieczeństwa Komunikacji (Communications Security Establishment) należy:

a) pozyskiwanie i wykorzystywanie danych z globalnej sieci informacji (*global information infrastructure*) w celu dostarczania danych wywiadowczych zgodnie z priorytetami wywiadowczymi rządu Kanady;
b) pełnienie funkcji o charakterze konsultacyjno-doradczym oraz świadczenie usług, które mają na celu ochronę informacji elektronicznych i infrastruktury informacyjnej, istotnych dla rządu Kanady;
c) udzielanie wsparcia technicznego i operacyjnego federalnym organom ochrony bezpieczeństwa i porządku publicznego oraz służbom bezpieczeństwa podczas realizacji ich ustawowych zadań.

Ochrona obywateli Kanady

(2) Działania prowadzone na podstawie § (1) pkt a i b:

a) nie mogą być skierowane przeciwko obywatelom Kanady ani jakiejkolwiek osobie przebywającej na terytorium tego państwa;
b) podlegają instrumentom ochrony prywatności obywateli Kanady w zakresie wykorzystywania i retencji przechwyconych informacji.

Ograniczenia

(3) Działania prowadzone na podstawie § 1c podlegają wszelkim ograniczeniom ustawowym nałożonym na federalne organy ochrony bezpieczeństwa i porządku publicznego oraz na służby bezpieczeństwa.

Autoryzacja ministra

273.65. (1) Minister może, wyłącznie w celu pozyskiwania informacji od obcych wywiadów – wyrazić pisemną zgodę na przechwycenie przez Służbę Bezpieczeństwa Komunikacji prywatnej komunikacji mającej związek z działalnością lub z danym typem działalności wymienionymi w autoryzacji.

[1] www.laws-lois.justice.gc.ca/eng/acts/N-5 [dostęp: 14 II 2017].

Warunki autoryzacji

(2) Minister może – wydać autoryzację na podstawie podsekcji (1), jeżeli uzna, że:

a) przechwycenie rozmowy prywatnej będzie skierowane przeciwko obcym podmiotom znajdującym się poza terytorium Kanady;
b) nie jest możliwe pozyskanie określonych informacji w inny sposób;
c) wartość informacji uzyskanych dzięki przechwyceniu rozmowy prywatnej uzasadnia wykorzystanie tego środka;
d) istnieją wystarczające instrumenty, które chronią prywatność obywateli Kanady i zapewniają, że prywatna komunikacja będzie wykorzystywana lub będzie podlegać retencji wyłącznie wtedy, gdy będzie to miało istotne znaczenie dla polityki zagranicznej, obronnej lub dla bezpieczeństwa Kanady.

Autoryzacja ministra

(3) Minister może – wyłącznie w celu ochrony systemów lub sieci komputerowych rządu Kanady przed szkodą, nieuprawnionym użyciem lub ingerencją w ich funkcjonowanie w rozumieniu § 184 (2)(c) kodeksu karnego – wyrazić pisemną zgodę na przechwycenie przez Służbę Bezpieczeństwa Komunikacji prywatnej rozmowy dotyczącej działalności lub typów działalności wymienionych w autoryzacji.

Warunki autoryzacji

(4) Minister może wydać autoryzację, o której mowa w podsekcji (3), jeśli uzna, że:

a) przechwycenie jest niezbędne do identyfikacji, izolacji lub zapobieżenia zagrożeniu systemów lub sieci komputerowych rządu Kanady;
b) określonej informacji nie można uzyskać w inny sposób;
c) nie jest możliwe uzyskanie zgody osób, których prywatna komunikacja ma zostać przechwycona, na wykorzystanie tego instrumentu;
d) istnieją wystarczające instrumenty mające na celu zapewnienie, że zostaną wykorzystane lub będą podlegać retencji wyłącznie informacje niezbędne do identyfikacji, izolacji lub zapobieżenia zagrożeniu systemów lub sieci komputerowych rządu Kanady;
e) istnieją wystarczające instrumenty chroniące prywatność obywateli Kanady w związku z wykorzystywaniem lub retencją informacji uzyskanych przez przechwycenie rozmowy prywatnej.

Dodatkowe warunki przewidziane w autoryzacji

(5) Autoryzacja wydana na podstawie niniejszej sekcji może określać dodatkowe warunki, które w opinii ministra przyczynią się do ochrony prywatności obywateli Kanady, m.in. dodatkowe instrumenty ograniczające wykorzystywanie i retencję informacji uzyskanych przez przechwycenie prywatnej komunikacji, dostęp do nich oraz formy i sposoby ich ujawnienia.

Okres ważności autoryzacji

273.68. (1) Autoryzacja jest ważna przez wskazany w niej okres. Może też być przedłużona na czas określony na mocy decyzji o przedłużeniu jej ważności. Autoryza-

cja ani decyzja o przedłużeniu jej ważności nie mogą powodować jej stosowania przez okres dłuższy niż rok.

NIEMCY

Ustawa o Federalnej Służbie Wywiadowczej (Bundesnachrichtendienst – BND)[2] (wyciąg)

Sekcja 1 – Organizacja. Funkcje i uprawienia BND.

Art. 1. Organizacja i funkcje.

(…)

(2) W celu uzyskania danych wywiadowczych o państwach obcych, które są istotne dla Republiki Federalnej Niemiec z punktu widzenia jej polityki zagranicznej i bezpieczeństwa, BND gromadzi i analizuje niezbędne informacje. Jeśli informacje, w tym dane osobowe, są zbierane na podstawie ustawy o Federalnej Służbie Wywiadowczej, ich przetwarzanie i wykorzystywanie również następuje zgodnie z tą ustawą.

Art. 2. Uprawnienia.

(1) BND jest uprawniona do zbierania, przetwarzania i wykorzystywania informacji, w tym danych osobowych, z zastrzeżeniem, że takie działania nie mogą naruszać postanowień ustawy federalnej o ochronie danych lub szczególnych regulacji wymienionej ustawy,

1) w celu ochrony personelu, wyposażenia, obiektów i źródeł przed działaniami wywiadowczymi i innymi działaniami stanowiącymi zagrożenie dla bezpieczeństwa,
2) w celu sprawdzenia bezpieczeństwa osób, które obecnie są lub w przyszłości będą zatrudnione w BND,
3) w celu sprawdzenia otrzymywanych informacji,
4) w celu uzyskania informacji o zdarzeniach z zagranicy, które są istotne dla polityki zagranicznej i polityki bezpieczeństwa Republiki Federalnej Niemiec – jeśli mogą być uzyskane tylko w taki sposób i jeśli żaden inny organ państwowy nie jest odpowiedzialny za ich gromadzenie.

(…)

(3) BND nie posiada uprawnień policyjnych.

(4) W przypadku istnienia kilku możliwych opcji BND powinna wybierać tę, która jest najmniej dolegliwa wobec podmiotu, którego dotyczy. Podjęte środki nie powinny powodować negatywnych konsekwencji, niepozostających w relacji do zamierzonego skutku działań.

Art. 3. Specjalne wnioski o informacje.

[Takie wnioski mogą być składane w indywidualnych przypadkach, w celu wypełnienia obowiązków BND. Służba może gromadzić informacje na podstawie art. 8a i 8b *Ustawy o Ochronie Konstytucji Federalnej*[3] – dop. aut.].

[2] Niem. *Gesetz über den Bundesnachrichtendienst* [online], www.gesetze-im-internet.de/bndg/ [dostęp: 14 II 2017].

[3] Niem. *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungs-*

Art. 4. Dalsze wnioski o informacje.

[Jeśli takie wnioski są wymagane w celu wypełnienia zadań BND, strona przekazująca lub pomagająca w dostarczeniu usług telekomunikacyjnych, takich jak operacja komercyjna, może być zobligowana do przekazania informacji na temat wiadomości pozyskanych zgodnie z art. 95 i 111 ustawy federalnej o telekomunikacji – dop. aut.].

Art. 5. Specjalne rodzaje gromadzenia danych.

W celu gromadzenia danych, w tym danych osobowych, w sposób niejawny BND – na podstawie art. 8 ust. 2 *Ustawy o Ochronie Konstytucji Federalnej* – może stosować środki wymagane w celu wypełniania swoich obowiązków, jeśli istnieją ku temu uzasadnione powody.

Sekcja 2. Gromadzenie informacji wywiadowczych o cudzoziemcach za granicą.

Art. 6. Warunki gromadzenia i przetwarzania danych:

(1) W celu wypełniania swoich obowiązków BND może stosować środki techniczne z zamiarem gromadzenia i przetwarzania informacji, łącznie z danymi osobowymi, z sieci telekomunikacyjnych przez urządzenia telekomunikacyjne obcokrajowców, którzy znajdują się za granicą, jeśli takie informacje są wymagane w następujących celach:

1) identyfikacji i zwalczania we wczesnej fazie ryzyka odnoszącego się do bezpieczeństwa wewnętrznego lub zewnętrznego Republiki Federalnej Niemiec;
2) zagwarantowania Republice Federalnej Niemiec zdolności do działania lub
3) zdobycia informacji wywiadowczych istotnych z punktu widzenia polityki zagranicznej lub polityki bezpieczeństwa, dotyczących zdarzeń, które, w odniesieniu do ich rodzaju oraz zakresu, są określone przez Federalny Urząd Kanclerski w porozumieniu z Ministerstwem Spraw Zagranicznych, Ministerstwem Spraw Wewnętrznych, Federalnym Ministerstwem Obrony, Federalnym Ministerstwem Spraw Gospodarczych i Energii oraz Federalnym Ministerstwem Współpracy Gospodarczej i Rozwoju.

Informacje mogą być gromadzone wyłącznie z tych sieci telekomunikacyjnych, co do korzystania z których Federalny Urząd Kanclerski uprzednio wydał pozwolenie.

(2) BND może gromadzić wyłącznie informacje uzyskane podczas zdobywania danych wywiadowczych o cudzoziemcach z zagranicznych komunikatorów, opierając się na znacznikach wyszukiwania. Te znaczniki muszą być określone i odpowiednie do gromadzenia informacji wywiadowczych w zakresie spraw, o których mowa w pkt 1, zdanie 1. Ponadto ich wykorzystanie musi być zgodne z interesami Republiki Federalnej Niemiec ważnymi dla polityki zagranicznej i polityki bezpieczeństwa.

(3) Znaczniki wyszukiwania, które umożliwiają gromadzenie informacji odnoszących się do organów i instytucji Unii Europejskiej, władz publicznych państw członkowskich Unii lub jej obywateli mogą być wykorzystane, jeśli jest to niezbędne w celu:

1) identyfikacji i zwalczania ryzyka zgodnie z art. 5 zdanie 3 ustawy o ograniczeniu poufności poczty i telekomunikacji lub
2) uzyskania informacji zgodnie z ust. 1 zdanie 1 litery a–c, jeśli chodzi o dane dotyczące wydarzeń poza terytorium Unii Europejskiej, o ile mają one szczególne znaczenie dla bezpieczeństwa Republiki Federalnej Niemiec.

schutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BverfSchG) [online], https://www.gesetze-im-internet.de/bverfschg/ [dostęp: 20 IV 2017].

Znaczniki wyszukiwania, które prowadzą do gromadzenia informacji odnoszących się do obywateli UE mogą być wykorzystywane poza ww. zakresem, jeśli są wymagane do identyfikacji oraz zwalczania przestępstw w rozumieniu art. 3 ust. 1 ustawy o ograniczeniu poufności poczty i telekomunikacji.

(4) Jakiekolwiek gromadzenie danych pochodzących z ruchu telekomunikacyjnego obywateli niemieckich lub krajowych osób prawnych albo osób będących rezydentami na terytorium niemieckim jest zabronione.

(5) Gromadzenie informacji wywiadowczych o cudzoziemcach za granicą w celu uzyskania korzyści w konkurencyjności (szpiegostwo przemysłowe) jest zabronione.

(6) Dane o ruchu telekomunikacyjnym są przechowywane przez maksimum 6 miesięcy.

(7) Stosowanie środków technicznych, o których mowa w pkt 1 oraz wykonywanie czynności kontrolnych są określone w akcie wykonawczym wydawanym przez BND. Wydanie powyższego aktu wymaga zgody Federalnego Urzędu Kanclerskiego, który informuje o tym fakcie Parlamentarny Komitet Kontrolny.

Art. 7. Przetwarzanie i wykorzystywanie danych zebranych za granicą.

(1) Artykuł 6 ust. 1 zdanie 1 oraz ust. 3–6 mają zastosowanie do przetwarzania i wykorzystywania tych informacji pozyskiwanych o podmiotach zagranicznych, które są gromadzone przez BND.

(2) Szczegółowe regulacje odnoszące się do gromadzenia danych o organizacjach należących do Unii Europejskiej, organach publicznych należących do państw członkowskich Unii lub jej obywatelach przez zagraniczne organy publiczne za granicą może być zarządzone tylko przez BND na podstawie i przy poszanowaniu warunków określonych w art. 6 ust. 3.

(…)

Art. 13 Współpraca w zakresie prowadzenia wywiadu elektronicznego w Republice Federalnej Niemiec, dotyczącego cudzoziemców za granicą.

(1) W ramach prowadzenia wywiadu elektronicznego w Republice Federalnej Niemiec odnoszącego się do cudzoziemców za granicą, tak długo, jak Federalna Służba Bezpieczeństwa (BND) współpracuje z zagranicznymi organami publicznymi w zakresie wykonywania zadań wywiadowczych, informacje – w tym dane osobowe – mogą być gromadzone zgodnie z art. 14 oraz wymieniane zgodnie z art. 15;

(2) Współpraca z zagranicznymi organami publicznymi zgodnie z pkt 1 odpowiada regulacjom prawnym, jeśli:

1) służy celom wskazanym w art. 6 ust. 1 zd. 1 lit. a–c,
2) wykonanie zadań przez BND byłoby znacznie utrudnione lub niemożliwe bez takiej współpracy;

(3) Szczegóły współpracy są zawarte w oświadczeniu dotyczącym jej celów, uzgodnionym przez BND i zagraniczny organ publiczny przed rozpoczęciem współpracy. W oświadczeniu, o którym mowa, są określone:

1) cele współpracy,
2) zakres przedmiotowy współpracy,
3) okres trwania współpracy,
4) uzgodnienie poświadczające, że w zakresie współpracy zgromadzone dane mogą być wykorzystywane tylko w celach, w jakich zostały zgromadzone, i że ich wykorzystywanie jest zgodne z podstawowymi zasadami demokratycznymi,

5) uzgodnienie, że zagraniczny organ publiczny zaakceptował prośbę BND o uzyskanie pozwolenia dotyczącego wykorzystania danych,
6) zapewnienie zagranicznego organu publicznego zgadzającego się na odmowę BND dotyczącą przekazania prośby;

(4) Cele współpracy i jej zakres przedmiotowy są skoncentrowane na pozyskiwaniu informacji, mających służyć:

1) rozpoznawaniu i zapobieganiu groźbom międzynarodowego terroryzmu,
2) rozpoznawaniu i zapobieganiu groźbom nielegalnego handlu bronią i narkotykami,
3) wsparciu niemieckich sił zbrojnych i ochronie sił zbrojnych państw współpracujących,
4) wykorzystaniu podczas wydarzeń o znaczeniu krytycznym za granicą,
5) uzyskiwaniu wiedzy o zagrożeniach i sytuacji dotyczącej bezpieczeństwa za granicą odnoszących się do obywateli niemieckich oraz obywateli państw współpracujących,
6) uzyskiwaniu wiedzy o politycznych, biznesowych i militarnych operacjach za granicą, które mają znaczenie dla polityki zagranicznej i bezpieczeństwa lub
7) w sytuacjach analogicznych.

(5) Podpisanie oświadczenia dotyczącego celów wymaga zgody Federalnego Urzędu Kanclerskiego, jeśli współpraca odnosi się do zagranicznych organów publicznych państw członkowskich Unii Europejskiej, Europejskiego Obszaru Gospodarczego lub państw członkowskich NATO. Parlamentarny Komitet Regulacyjny jest informowany o każdym oświadczeniu dotyczącym celów.

Art. 14. Gromadzenie danych osobowych w zakresie współpracy.

(1) Gromadzenie danych osobowych w zakresie współpracy, zgodnie z art.13, jest zgodne z prawem, jeśli jest realizowane przez BND:

1) w celu osiągnięcia uzgodnionych celów współpracy,
2) jeśli podczas gromadzenia poszczególnych danych stosowane znaczniki wyszukiwania są skierowane wyłącznie na osiągnięcie celu współpracy.

Gromadzenie danych osobowych i stosowanie znaczników wyszukiwania pozostaje w zgodzie z polityką zagraniczną i polityką bezpieczeństwa Republiki Federalnej Niemiec.

(2) Artykuł 6 pkt 1 zdanie 2, pkt. 3–7 oraz art. 8–12 stosuje się odpowiednio.

(3) Rozpoznanie w zakresie przechwytywania komunikacji z obcego państwa może zostać przeprowadzone w ramach współpracy, o której mowa w art. 13, wyłącznie przez BND.

WIELKA BRYTANIA

Ustawa o służbach wywiadowczych (Intelligence Services Act)[4] – wyciąg

1. (1) Tajna Służba Wywiadu (dalej zwana Służbą Wywiadu) podlega sekretarzowi stanu. Do jej zadań, zgodnie z podsekcją (2) należy:

b) pozyskiwanie i udzielanie informacji dotyczących działań i zamiarów osób znajdujących się poza terytorium Wysp Brytyjskich,

[4] *Intelligence Services Act 1994* [online], www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf [dostęp: 14 II 2017].

c) wykonywanie innych zadań dotyczących działań i zamiarów tych osób.

(2) Służba Wywiadu realizuje swoje zadania wyłącznie:

(…)

b) w interesie bezpieczeństwa narodowego, szczególnie w zakresie obronności i polityki zagranicznej rządu Zjednoczonego Królestwa,
c) w celu ochrony interesów ekonomicznych Zjednoczonego Królestwa,
d) w celu wsparcia procesu zapobiegania i wykrywania poważnej przestępczości.

2. (1) Nadzór nad działalnością Służby Wywiadu sprawuje jej szef mianowany przez sekretarza stanu.

(2) Szef Służby Wywiadu jest odpowiedzialny za skuteczność działań tej służby. Do jego zadań należy:

a) zapewnienie, że istnieją instrumenty gwarantujące, że Służba nie pozyskuje żadnych informacji, jeżeli nie jest to niezbędne dla prawidłowej realizacji jej zadań oraz że żadna informacja nie zostanie przez nią ujawniona, chyba że jest to niezbędne ze względu na:
   i) prawidłowe wykonywanie zadań służby,
   ii) interes bezpieczeństwa narodowego,
   iii) zapobieganie i wykrywanie poważnej przestępczości,
   iv) interes postępowania karnego (…)
b) Służba Wywiadu nie prowadzi żadnych działań mających na celu wspieranie interesów partii politycznych działających w Zjednoczonym Królestwie.

(…)

(4) Szef Służby Wywiadu przedstawia premierowi i sekretarzowi stanu coroczny raport dotyczący jej działalności. W każdym momencie może poinformować premiera lub sekretarza stanu o każdej sprawie istotnej z punktu widzenia ich obowiązków.

Autoryzacja niektórych czynności

5. (1) Naruszenie własności prywatnej lub komunikacji bezprzewodowej nie jest bezprawne, jeżeli zostało autoryzowane na podstawie nakazu wydanego przez sekretarza stanu zgodnie z przepisami niniejszej sekcji.

(2) Sekretarz stanu może, na wniosek Służby Bezpieczeństwa, Służby Wywiadu lub GCHQ, wydać nakaz autoryzujący podjęcie, na zasadach określonych w podsekcji (3), wyszczególnionych w nim czynności w odniesieniu do każdej własności prywatnej lub komunikacji bezprzewodowej, jeżeli uważa on, że:

a) podjęcie tych czynności jest niezbędne z uwagi na to, że może to mieć zasadnicze znaczenie dla:
   i) Służby Bezpieczeństwa – w kontekście realizacji jej ustawowych zadań,
   ii) Służby Wywiadu – w kontekście realizacji jej zadań zgodnie z sekcją 1 niniejszej ustawy,
   iii) GCHQ – w kontekście realizacji jej zadań określonych w sekcji 3(1)(a) niniejszej ustawy oraz;
b) określony cel nie może być osiągnięty w inny sposób;
c) zostały wprowadzone instrumenty określone w sekcji 2(2)(a) ustawy o służbach bezpieczeństwa (*Security Services Act*) zapobiegające ujawnieniu informacji pozyskanych na zasadach określonych w tej sekcji.

(3) Nakaz autoryzujący podjęcie działań, które mają na celu wspieranie zapobiegania i wykrywania poważnych przestępstw, nie może dotyczyć własności na terenie Wysp Brytyjskich.

(4) Na zasadach określonych w podsekcji (5), Służba Bezpieczeństwa może złożyć wniosek, o którym mowa w podsekcji (2) o wydanie nakazu autoryzującego podjęcie przez nią lub przez osobę działającą na jej rzecz czynności określonych w nakazie w imieniu Służby Wywiadu lub GCHQ. Jeżeli taki nakaz został wydany, Służba Bezpieczeństwa jest odpowiedzialna za dokonanie wszystkich wymienionych w nim czynności, **nawet gdy w innym wypadku ich wykonanie wykraczałoby poza zakres kompetencji tej służby** (podkreślenie autorów – przyp. red.).

(5) Służba Bezpieczeństwa może złożyć wniosek o wydanie nakazu na zasadach określonych w podsekcji (4), z wyjątkiem sytuacji, gdy działania, które mają zostać autoryzowane przez nakaz:

a) są działaniami, w odniesieniu do których Służba Wywiadu lub GCHQ mogą złożyć samoistnie wniosek o autoryzację;
b) mają służyć innym celom niż wspieranie zapobiegania i wykrywania poważnych przestępstw.

6. (1) Nakaz może zostać wydany wyłącznie:

a) przez sekretarza stanu;
b) w nagłych wypadkach, jeżeli sekretarz stanu wyraził wprost zgodę na jego wydanie, a oświadczenie o tej zgodzie jest zawarte w treści dokumentu przez wysokiego rangą urzędnika jego departamentu (*senior official*).

(2) Nakaz, jeżeli nie został przedłużony na zasadach określonych w podsekcji (3), wygasa:

a) po upływie 6 miesięcy, licząc od dnia jego wydania, jeżeli został wydany przez sekretarza stanu;
b) wraz z upływem drugiego dnia roboczego po upływie okresu, na który został wydany – w innych przypadkach.

(3) Sekretarz stanu może przedłużyć stosowanie nakazu na okres kolejnych 6 miesięcy, jeżeli uzna, przed upływem okresu jego obowiązywania, że jego dalsze stosowanie jest niezbędne do realizacji celów, w jakich został wydany.

(4) Sekretarz stanu może unieważnić nakaz, jeżeli uzna, że prowadzenie określonych w nim działań nie jest już konieczne.

7. (1) Jeżeli osoba podlegałaby odpowiedzialności na terenie Zjednoczonego Królestwa za jakikolwiek czyn dokonany poza terytorium Wysp Brytyjskich, nie ponosi jej, jeżeli działanie, które może pociągnąć za sobą tę odpowiedzialność zostało dozwolone na podstawie autoryzacji sekretarza stanu, wydanej zgodnie z przepisami niniejszej sekcji.

(2) Termin p o d l e g a j ą c y o d p o w i e d z i a l n o ś c i w Z j e d n o c z o n y m K r ó l e s t w i e oznacza ponoszenia odpowiedzialności za określone działania lub zaniechania w rozumieniu prawa karnego lub prawa cywilnego.

(3) Sekretarz stanu wydaje autoryzację, jeżeli uzna, że:

a) działania, które mają zostać podjęte zgodnie z autoryzacją lub operacje, w których trakcie te działania mają zostać podjęte, są niezbędne do prawidłowej realizacji zadań Służby Wywiadu;
b) istnieją odpowiednie instrumenty zapewniające, że:
   i) na podstawie autoryzacji nie zostaną podjęte jakiekolwiek działania inne niż te, które są niezbędne do prawidłowej realizacji zadań Służby Wywiadu,

ii) charakter działań prowadzonych na podstawie autoryzacji i ich prawdopodobne konsekwencje będą uzasadnione, biorąc pod uwagę cele, w jakich mają zostać dokonane;

c) istnieją odpowiednie instrumenty wprowadzone zgodnie z sekcją 2 (2), regulujące możliwość ujawnienia informacji uzyskanych na zasadach określonych w tej sekcji oraz że postępowanie z jakimikolwiek informacjami uzyskanymi podczas działań przeprowadzanych na podstawie autoryzacji będzie prowadzone w sposób zgodny z normami wynikającymi z tych instrumentów.

(4) Bez uszczerbku dla ogólnego zakresu kompetencji sekretarza stanu do udzielania autoryzacji na podstawie niniejszej sekcji autoryzacja ta:

a) może dotyczyć indywidualnej i konkretnej czynności lub większej liczby czynności; czynności, których specyfikacja została zawarta w autoryzacji; czynności podejmowanych podczas operacji, której specyfikacja jest zawarta w autoryzacji;

b) może być ograniczona do konkretnie wskazanej osoby lub osób.

(5) Autoryzacja na podstawie przepisów niniejszej sekcji może być wydana:

a) przez sekretarza stanu,

b) w nagłych wypadkach, jeżeli sekretarz stanu wyraził wprost zgodę na jej wydanie, a oświadczenie o tej zgodzie jest zawarte w treści dokumentu przez wysokiego rangą urzędnika jego departamentu (*senior official*)

(6) Autoryzacja, jeżeli nie została przedłużona na zasadach określonych w podsekcji (7), wygasa:

a) po upływie 6 miesięcy, licząc od dnia jej udzielenia, jeżeli została wydana przez sekretarza stanu;

b) wraz z upływem drugiego dnia roboczego, po upływie okresu, na który została wydana – w innych przypadkach.

(7) Sekretarz stanu może przedłużyć autoryzację na kolejne 6 miesięcy, jeżeli uzna, przed upływem okresu jej ważności, że jej dalsze obowiązywanie jest niezbędne do realizacji celów, w jakich została udzielona.

(8) Sekretarz stanu może unieważnić autoryzację, jeżeli uzna, że wykonanie jakichkolwiek czynności, do których upoważniała ta autoryzacja, nie jest już konieczne.

PODSUMOWANIE

W niniejszym opracowaniu dokonano przeglądu służb specjalnych wybranych państw z uwzględnieniem ich uprawnień. Przedstawiono również definicje szpiegostwa oraz terroryzmu – przestępstw stanowiących obecnie jedno z największych zagrożeń bezpieczeństwa państwa. Dużo miejsca poświęcono także przepisom szczególnym odnoszącym się do najistotniejszych aspektów praktycznej działalności służb specjalnych, do których należy zaliczyć prowadzenie czynności operacyjno-rozpoznawczych i analityczno-informacyjnych. W opracowaniu zawarto też informacje na temat przepisów regulujących działalność wywiadowczą poza granicami kraju, prowadzoną przez służby odpowiedzialne za ochronę bezpieczeństwa zewnętrznego.

Na podstawie dokonanej analizy należy stwierdzić, że nie ma uniwersalnego ani powszechnie stosowanego modelu służb specjalnych. Zakres kompetencji tego typu struktur oraz sposób realizacji ich ustawowych zadań ściśle wynikają z modelu instytucjonalnego danego państwa oraz modelu służb ukształtowanego historycznie, a także ze specyfiki wyzwań oraz zjawisk, które mogą zagrażać ich bezpieczeństwu.

Należy podkreślić, że na regulacje prawne i zakres kompetencyjny dotyczące działania służb specjalnych mają wpływ wydarzenia bieżące. Działania w zakresie zapobiegania terroryzmowi oraz jego zwalczania, należące tradycyjnie do uprawnień służb ochrony bezpieczeństwa wewnętrznego państwa, jak np. MI5 lub ABW, są w dużym stopniu uzależnione od efektywnej realizacji ustawowych zadań służb wywiadowczych, które dysponują szczegółowymi informacjami dotyczącymi terroryzmu międzynarodowego lub wynikających z niego zagrożeń.

Ewolucji ulega także zakres kompetencji służb wywiadowczych i kontrwywiadowczych, które coraz większe znaczenie przywiązują do nowoczesnych instrumentów pozyskiwania oraz przetwarzania informacji. Na szczególną uwagę zasługują narzędzia służące do niejawnego pozyskiwania danych za pośrednictwem środków komunikacji elektronicznej. Wśród nich należy wymienić przechwytywanie informacji, możliwość uzyskiwania dostępu do nich oraz analizy wiadomości przekazywanych przy pomocy szyfrowanych środków łączności (np. komunikatorów internetowych). Jednym z najważniejszych wyzwań odnoszącym się do metod i technik pracy operacyjnej stosowanych przez służby specjalne pozostaje uzyskanie właściwych proporcji między zapewnieniem bezpieczeństwa narodowego a prawem do prywatności, w tym prawem do ochrony danych osobowych.

Analizowane ustawy kompetencyjne, na których podstawie działają służby specjalne poszczególnych krajów, zawierają regulacje prawne szczegółowo określające ich uprawnienia do prowadzenia czynności związanych ze środkami i metodami pracy operacyjnej, ale jednocześnie zawierają przepisy normujące zasady i tryb gromadzenia, przetwarzania oraz wykorzystywania danych osobowych w celach związanych z realizacją ich podstawowych zadań.

Warto zwrócić uwagę na to, że w zakresie regulacji dotyczących definicji przestępstwa szpiegostwa przepisy w poszczególnych państwach, pomimo generalnych podobieństw, wykazują istotne różnice co do szczegółowego ujęcia znamion tych przestępstw, ich zakresu podmiotowego oraz przedmiotowego.

Najważniejszą cechą wspólną definicji przestępstwa szpiegostwa jest przekazywanie informacji istotnych z punktu widzenia bezpieczeństwa państwa organom innego państwa lub podmiotom działającym na rzecz obcego państwa. Konkretne uregulowania prawnokarne charakteryzują się zróżnicowanym ujęciem systemowym. Z jednej strony są stosowane rozwiązania legislacyjne cechujące się wysokim stopniem kazuistyki i szczegółowości, określające wprost zamknięty wykaz zachowań wypełniających znamiona szpiegostwa (np. USA). Z drugiej zaś przyjęto rozwiązania legislacyjne o wysokim stopniu ogólności, całkowicie różne od wymienianych rozwiązań kazuistycznych, gdyż pozostawiają one organom stosującym przepisy prawa szeroki zakres swobody interpretacyjnej.

W przeciwieństwie do rozwiązań prawnych dotyczących szpiegostwa przepisy penalizujące terroryzm cechują się mniejszą rozbieżnością definicyjną, gdyż ich konstrukcja jest odzwierciedleniem regulacji prawnomiędzynarodowych oraz europejskich, które znacznie zawężają swobodę ustawodawcy w tym zakresie.

Warto zauważyć, że w przepisach prawa karnego lub ustaw kompetencyjnych służb specjalnych są stosowane klauzule generalne zawierające definicje pojęć istotnych z punktu widzenia realizacji zadań służb specjalnych, które pozwalają tym służbom na właściwe ukierunkowanie ich praktycznych działań w sposób zgodny z intencją ustawodawcy. Jako przykład należy wskazać pojęcie f u n d a m e n t a l n e i n t e r e s y p a ń s t w a zawarte we francuskim kodeksie karnym, które zostało dookreślone w celu właściwej interpretacji przepisów dotyczących szpiegostwa oraz innych przestępstw przeciwko narodowi, państwu i porządkowi publicznemu. Innym przykładem jest dookreślenie pojęcia d z i a ł a l n o ś ć w y w i a d o w c z a w niemieckim kodeksie karnym przez wskazanie konkretnych zachowań wypełniających znamiona przestępstwa szpiegostwa.

Immanentną cechą przepisów regulujących działalność służb wywiadowczych aktywnych poza granicami kraju jest wysoki stopień ich niedookreśloności i ogólności, co zapobiega nadmiernemu ograniczeniu ich swobody działania oraz pozwala na realizowanie wielu zadań pozostających w ich kompetencji. Należy również wskazać, że ogólną tendencją, którą można zauważyć po dokonaniu przeglądu omawianych przepisów, jest coraz szerszy zakres regulacji, odnoszących się do pozyskiwania informacji przy wykorzystaniu nowoczesnych technologii oraz urządzeń (m.in. monitorowanie ruchu internetowego, stosowanie selektorów oraz prowadzenie analizy pozyskiwanych informacji). Jednocześnie należy wskazać, że niektóre z omawianych służb nie mają wyrażonych expressis verbis uprawnień do stosowania „tradycyjnych" metod pracy operacyjnej, typowej w odniesieniu do zagrożeń występujących w końcowej fazie XX w.

BIBLIOGRAFIA

Źródła internetowe:

1. https://english.aivd.nl/about-aivd/publications/2002/03/26/bulletin-of-acts-orders-and-decrees-of-the-kingdom-of-the-netherlands
2. https://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164
3. https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act
4. https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719
5. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028887486&categorieLien=id
6. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id
7. https://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2005,pdf
8. www. Admin.ch/opc/de/federal-gazette/2015/7211.pdf.
9. www.cni.es/en/howdoesthecniwork/
10. www.cni.es/en/Rules_and_regulations/
11. www.cni.es/en/structure/
12. www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf
13. www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032
14. www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2003121934
15. www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=20100204026
16. www.gesetz-im-internet.de/bverfschg/BJNR029700990.html
17. www.gesetze-im-internet.de/englisch_stgb/index.html
18. www.gesetze-im-internet.de/bndg
19. www.laws-lois.justice.gc.ca/eng/acts/C-23/
20. www.laws-lois.justice.gc.ca/eng/acts/N-5
21. www.law.cornell.edu/uscode/text/18/part-I/chapter-113B
22. www.law.cornell.edu/uscode/text/18/part-I/chapter-37
23. www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000517072
24. www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028887486&categorieLien=id
25. www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id
26. www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000357733&categorieLien=id
27. www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT0000007149&dateTexte=

28. www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000031240607&dateTexte+&categorieLien=cid
29. www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307
30. www.legilux.public.lu/eli/etat/leg/loi/2004/06/15/n4/jo
31. www.legilux,public.lu/eli/etat/leg/code/penal
32. www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf
33. www.privacycommission.be/sites/privacycommission/files/documents/privacy_fr_0.pdf
34. www. Verfassungsschutz.de/en/index-en.html
35. www.vbs.admin.ch/en/ddps/organisation/adminsitrative-units/intelligence-service.html