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. Służba odpowiada również za bezpieczeństwo personelu Ministerstwa Obrony, bezpieczeństwo 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] Państwa omawiane w publikacji są prezentowane w kolejności alfabetycznej (przyp. red.).

Najważniejszym elementami systemu prawnego Belgii 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 to lub uniemożliwiało wykonanie innych zadań, służba niezwłocznie informuje o tym ministra spraw wewnętrznych. Nie zwalnia to jednak VSSE z obowiązku wykonania 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 zapewnianiem 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 z szerzeniem propagandy, nawoływaniem 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 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 albo 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 wywarcia wpływu na procesy decyzyjne metodami nielegalnymi.

Artykuł 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 oraz 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 oraz interesów państw, których cele są zbieżne z celami Belgii, a także organizacji międzynarodowych i ponadnarodowych. Ochrona osób jest natomiast rozumia-

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

2. Realizacja zadań służb wywiadowczych i bezpieczeństwa

W ramach realizacji zadań ustawowych służby mogą stosować instrumenty ograniczające konstytucyjne prawa i wolności wyłącznie na podstawie i w granicach obowiązujących przepisów prawnych. Mogą one 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, w jakim 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, że 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 norm ogólnych, zgodnie z którymi funkcjonariusze pozyskujące informacje 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 zadań ustawowych, 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 wiadomości 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 miejsc publicznych lub miejsc prywatnych dostępnych dla publiczności z wykorzystaniem środków technicznych lub obserwację miejsc prywatnych niedostępnych dla publiczności, z wykorzystaniem środków technicznych lub bez ich wykorzystania;

[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 zamkniętych przedmiotów (obiektów) znajdujących się w tych miejscach;
3) pozyskiwanie informacji identyfikujących nadawcę lub adresata przesyłki albo 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 albo 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 zamkniętych przedmiotów (obiektów) znajdujących się w tych lokalach;
3) utworzenie lub wykorzystanie osoby prawnej w celu wsparcia działań operacyjnych oraz wprowadzenie funkcjonariuszy działających pod fałszywą tożsamością;
4) otwarcie przesyłki powierzonej operatorowi pocztowemu lub innej przesyłki i zapoznanie z jej treścią;
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 przedmiotami są 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 danych 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 być 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 w celach 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 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 te informacje dotyczą.

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

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 nmpi przez VSSE 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, 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 wtedy, 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 nmpi: dostęp do miejsc, w których są przechowywane i przetwarzane informacje zebrane przy wykorzystaniu nmpi, wysłuchanie funkcjonariuszy służb oraz zabezpieczanie 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, oznaczany 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 wpływające na zakończenie stosowania nmpi nie ulegają zmianie; przesłankami są: ustanie zagrożenia i nieprzydatność 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. o 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 dla 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 dotyczącego 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 do 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) współpracę 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 albo 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, spowodowanie zagrożenia ruchu drogowego), mających na celu poważne zastraszenie ludności, organów Danii lub innego państwa w celu zmuszenia ich do określonego działania lub zaniechania działania, 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 zmierzającą 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 zmierzającą do ograniczenia swobody działalności organów administracji publicznej przez wykorzystywanie obaw przed obcą interwencją zbrojną, prowadzoną 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 służby specjalne Francji stanowią 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 tego 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 stosuje wiele metod zdobywania tego rodzaju danych, m.in. wykorzystywanie źródeł osobowych, środków technicznych (przechwytywanie elektromagnetyczne i obrazowanie satelitarne), działań operacyjno-rozpoznawczych i 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 ustawie o wywiadzie przyjętej w lipcu 2015 r., 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 jest to jedyna służba odpowiedzialna 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 DGSI niezwłocznie 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 albo 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 DGSI 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: Dz.U. 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 oraz 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 tych sił. 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 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 przetwarzania automatycznego, 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 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 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. Koordynację zadań sprawuje Rządowa

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.

Komisja 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 interesy gospodarcze i polityczne, 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 oraz zgodna z celami wyznaczonymi przez rząd. Zdobyte 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 relacje 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 zadań współpracuje z pozostałymi hiszpańskimi służbami informacyjnymi. W skład Rządowej Komisji Delegatów do Spraw Wywiadowczych (sprawującej kontrolę nad

[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].

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 ich 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 tym 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 w holenderskim systemie prawnym uwzględnia się 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, podczas których są poruszane kwestie najważniejsze z punktu widzenia funkcjonowania służb (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 oraz 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 legalne pojęć w niej używanych. Zakres przedmiotowy pojęcia informacje został skonstruowany w sposób szeroki – pod tym pojęciem ustawa rozumie dane osobowe oraz inne informacje. Dane osobowe 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) w stosunku do których zachodzi uzasadnione podejrzenie, że stanowią zagrożenie demokratycznego państwa prawnego, bezpieczeństwa lub innych fundamentalnych interesów państwa;
2) które wyraziły zgodę na przetwarzanie swoich danych osobowych w celu przeprowadzenia postępowania sprawdzającego;
3) których dane muszą być przetworzone w związku z czynnościami prowadzonymi przez służby, dotyczącymi innych państw;
4) których dane uzyskały inne służby wywiadowcze lub służby bezpieczeństwa;
5) których dane są niezbędne do zapewnienia prawidłowej realizacji ustawowych zadań służb;
6) które były funkcjonariuszami służb w przeszłości lub które aktualnie pełnią w nich służbę;
7) 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 zastosowanie również w odniesieniu do procesu przetwarzania tych danych przez funkcjonariuszy lub pracowników innych służb wykonujących określone czynności na zlecenie AIVD. Przetwarzanie przez wymienione osoby danych osobowych na zlecenie AIVD jest ściśle oddzielone 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 danych, 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 jej 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 trzy miesiące.

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, które pozwalają 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 danych 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 jakich dokonanie ww. czynności jest niezbędne.

Gdy w chwili sporządzania wniosku o udzielenie zgody na wykorzystanie tych 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 są wymieniane przy użyciu bezprzewodowych sieci telekomunikacyjnych. Wytypowanie określonego procesu wymiany informacji, który ma zostać objęty tym instrumentem, odbywa się na podstawie analizy jego charakterystyki technicznej. Taka charakterystyka 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 danych telekomunikacyjnych 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 informacje mają dotyczyć.

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 wówczas niezwłocznie 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 tę 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 Luksemburga 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 Luksemburga, jego suwerenność i niepodległość, bezpieczeństwo jego instytucji, poprawne funkcjonowanie instytucji państwa prawa lub może 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 ustawy SRE dba o zapewnienie sprawnej współpracy zarówno z organami policyjnymi, sądowymi i administracyjnymi, jak i z zagranicznymi służbami

specjalnymi. Ustawa zobowiązuje wprost tę służbę 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. 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 oraz 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 zadań ustawowych 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 (Biuletynu 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 zadania są realizowane również przy pomocy krajowych urzędów ochrony konstytucji (Landesbehörden für Verfassungsschutz – LfV) działających na poziomie krajów związkowych (landów). 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 przez nich 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. z mediów. 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

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 oraz 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 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 oraz które:

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].

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) zapewnianie 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 sobie niezwłocznie informacje istotne dla wykonywania swoich zadań. W sytuacji, gdy organ przesyłający zrobi zastrzeżenie, przekazywane informacje 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. Konieczne jest zapewnienie możliwości ustalenia organu, który wprowadzał dane. Z kolei wyszukanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne 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 upoważnionych do rejestracji danych lub analiz. Prawo dostępu do dokumentów zawierających dane jest ograniczone do osób, które są bezpośrednio zaangażowane w wykonywanie 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 informacje 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, 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 z 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 usługi oraz skali korzystania z nich,
   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 pozyskiwania informacji, które mogą dotyczyć danych zdobytych 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[33].

2.6. Ograniczenie praw podstawowych

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

[33] 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 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, a także podejmowanie decyzji co do informowania osób, wobec których te 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.

Przechwytywane rozmowy prywatne prowadzone w mieszkaniach mogą 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 powinno 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 otrzymana na czas. Taką decyzję należy jednak uzyskać niezwłocznie. Właściwy do tego jest sąd, w którego okręgu BfV ma siedzibę. Ponadto w tych 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 jedynie, 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) jest to niezbędne do uzyskania i zabezpieczenia dostępu do informacji,
3) nie jest nieproporcjonalny do wagi wyjaśnianych faktów.

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 tego typu źródłami.

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 wykorzystanie 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 niezbędne zweryfikowanie 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 albo 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 temu 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 tę służbę nie mogą zostać przekazane stronie trzeciej bez jej zgody i że mogą zostać wykorzystane wyłącznie w celach, w jakich zostały przekazane.

SZWAJCARIA

1. Federalna Służba Wywiadowcza (ang. Federal Intelligence Service – FIS)[34]

Federalna Służba Wywiadowcza istnieje od 1 stycznia 2010 r.[35] Powstała w następstwie decyzji Parlamentu Konfederacji Szwajcarskiej z kwietnia 2009 r. przez połączenie dwóch poprzednich służb – Służby Wywiadu Strategicznego (Strategic Intelligence Service – 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 tę służbę[36] jest ona organizacją wykorzystującą 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

[34] 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].

[35] *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].

[36] Tamże, s. 5.

przedstawia zagrożenia w takich dziedzinach, jak polityka, gospodarka, obrona narodowa, proliferacja bmr, prowadzenie nielegalnych działań wywiadowczych, zagrożenia w cyberprzestrzeni, ekstremizm i terroryzm. Jednocześnie poziom gradacji zagrożenia został określony w następujący sposób: od poziomu ukrytego zagrożenia przez wczesne ostrzeżenie dzięki otrzymaniu istotnych informacji aż do punktów krytycznych[37].

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 bieżącego oceniania 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[38].

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:

1) które nie są publicznie dostępne,
2) które 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*

[37] Tamże, s. 6.
[38] Tamże, s. 7.

intelligence – 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[39].

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:

1) *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;
2) *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 związane 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 bmr.

Prace nad nową ustawą o służbie wywiadowczej[40] toczyły się od października 2010 r. Została ona uchwalona przez parlament[41] z datą wejścia w życie 1 września 2017 r. i ma 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, obserwację osób podejrzanych – także w pomieszczeniach prywatnych – oraz infiltrację komputerów i sieci)[42].

[39] Tamże, s. 8.

[40] *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).

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

[42] *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)[43]

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[44].

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 osób zainteresowanych. 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,

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

że te podejrzenia są nieuzasadnione. FIS może ponadto pozyskiwać 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. *watchlist*, lista osób i podmiotów obserwowanych), 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[45].

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 wykrycia i zapobieżenia 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),
   f) ekstremizmem z użyciem przemocy;
2) wykrywania, monitorowania i oceny istotnych wydarzeń dotyczących polityki bezpieczeństwa, do których dochodzi za granicą;
3) zabezpieczania zdolności państwa do działania;
4) ochrony innych ważnych interesów narodowych, na wyraźne polecenie Rady Federalnej;
5) oceny sytuacji pod kątem ewentualnego zagrożenia i poinformowania organów państwowych, kantonów, organów ścigania o wszelkich zagrożeniach i podjętych środkach, a także planowanych działaniach w ramach niniejszej ustawy;
6) informowania innych agend federalnych i kantonów, przy zachowaniu ochrony źródeł, o zdarzeniach i ustaleniach dotyczących utrzymania bezpieczeństwa wewnętrznego lub zewnętrznego;

[45] *Bundesgesetz über den Nachrichtendienst*…

7) zapewniania wczesnego ostrzegania w celu ochrony infrastruktury krytycznej;
8) utrzymywania relacji z zagranicznymi służbami wywiadowczymi;
9) prowadzenia programów profilaktycznych w zakresie uświadamiania o zagrożeniach bezpieczeństwa wewnętrznego lub zewnętrznego;
10) 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, tj.:
  – 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 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[46].

1.4. Nadzór i kontrola nad FIS[47]

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 międzydepartamentalnym (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*. Wybiera również członków Niezależnej Władzy Kontrolnej i autoryzuje oraz nadzoruje kontakty międzynarodowe ze służbami zagranicznymi.

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

[46] Tamże.
[47] *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[48]

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[49]

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 odpowiednim komitetom Rady Federacyjnej. W skład

[48] Tamże, s. 13.
[49] 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[50]

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 działała łączność z podmiotami prywatnymi. W celu osiągnięcia powyższego zamie-

[50] Tamże, s. 15–17.

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

1.8. Współpraca z zagranicznymi służbami partnerskimi[51]

Rozwijanie relacji międzynarodowych jest nieodłączną oraz zasadniczą częścią pracy FIS. Służba wykorzystuje takie kontakty, aby uzupełnić wiedzę w tych obszarach, które tego wymagają. Dzięki temu 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[52]

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.

[51] Tamże, s. 18.
[52] Tamże, s. 22–23.