

CZĘŚĆ III

Przepisy szczególne dotyczące funkcjonowania służb specjalnych

BELGIA

1. Ochrona informacji niejawnych

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

2. Sposoby realizacji zadań

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

3. Wyłączenie odpowiedzialności funkcjonariuszy

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

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

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

4. Ochrona danych osobowych

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

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

HISZPANIA

Narodowe Centrum Wywiadowcze

*Ustawa nr 2/2002 z dnia 6 maja 2002 r. regulująca uprzednią kontrolę sądową Narodowego Centrum Wywiadowczego*¹ – wyciąg

Sekcja 1. Uprzednia kontrola sądowa Narodowego Centrum Wywiadowczego.

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

Okres zastosowania ww. środków nie może przekroczyć 24 godzin – jeśli dotyczą one prawa do prywatności, oraz 3 miesięcy – w przypadku przechwycenia poczty, komunikacji telefonicznej lub jakiegokolwiek innej. Wymienione terminy mogą zostać przedłużone o okres, na który zostały złożone wnioski o ich zastosowanie.

4. Sąd powinien udzielić zgody lub odmówić wydania nakazu w okresie 72 godzin. Wymieniony okres ulega skróceniu do 24 godzin w przypadku nagłej potrzeby, uzasadnionej we wniosku o nakaz sekretarza stanu – dyrektora CNI, który we wszystkich sprawach powinien wskazać elementy określone powyżej. Sąd powinien podjąć niezbędne kroki w celu ochrony niejawności działań, które powinny być klasyfikowane jako „ściśle tajne”.
5. Sekretarz stanu – dyrektor CNI zarządza niezwłoczne zniszczenie wszelkich informacji zebranych na mocy nakazu, o którym mowa w niniejszej sekcji, niepowiązanych z celem tego nakazu.

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

*Ustawa 11/2002 z dnia 6 maja 2002 r. regulująca funkcjonowanie Narodowego Centrum Wywiadowczego*² – wyciąg

Sekcja 4. Funkcje Narodowego Centrum Wywiadowczego:

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

Sekcja 5. Czynności podejmowane przez Narodowe Centrum Wywiadowcze.

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

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

KANADA

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

Art. 2. Zagrożenia bezpieczeństwa Kanady oznaczają:

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

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

2. Obowiązki i zadania służby

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

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

3. Instrumenty zwalczania zagrożeń bezpieczeństwa Kanady

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

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

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

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

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

⁴ We francuskojęzycznej wersji ustawy posłużono się terminem *contrôle d'application de la*

4. Działania niedozwolone

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

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

5. Ocena bezpieczeństwa

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

6. Funkcje konsultacyjno-doradcze wobec ministrów

Art. 14. Służba może:

- a) doradzać ministrom w sprawach dotyczących bezpieczeństwa Kanady;
- b) udzielać ministrom informacji dotyczących bezpieczeństwa lub działalności przestępczej – istotnych z punktu widzenia kompetencji ministrów lub wykonywania przez nich jakichkolwiek czynności zgodnie z ustawą o obywatelstwie albo z ustawą o imigracji i ochronie uchodźców.

7. Postępowania

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

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

8. Zbieranie informacji dotyczących innych państw i osób zagranicznych

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

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

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

⁵ Ocena lojalności wobec Kanady, w zakresie, w jakim ma to związek z wiarygodnością danej osoby.

(3) Służba wykonuje czynności wynikające z § 1:

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

9. Kontrola sądowa

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

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

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

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

- a) wejścia do miejsc lub pomieszczeń w celu uzyskania dostępu do znajdujących się w nich przedmiotów;

- b) poszukiwania, usuwania, zwrotu, badania, pobrania próbek, kopiowania lub utrwalania w inny sposób informacji, zapisów, dokumentów lub przedmiotów;
- c) zainstalowania, utrzymywania lub usuwania jakichkolwiek przedmiotów.

10. Działania poza terytorium Kanady

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

11. Elementy nakazu

Art. 21.1. (5) Nakaz wydany na podstawie § 3 powinien zawierać:

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

12. Maksymalny czas trwania nakazu

Art. 21. 1 (6) Nakaz może zostać wydany na okres nieprzekraczający:

- a) 60 dni – jeżeli został wydany w celu upoważnienia służby do zbadania zagrożenia bezpieczeństwa Kanady w rozumieniu § d sekcji 2 zawierającego definicję pojęcia zagrożenia bezpieczeństwa Kanady;
- b) 120 dni – w innych przypadkach.

13. Przedłużenie nakazu

Art. 22. Sędzia może na wniosek osoby upoważnionej do złożenia wniosku o wydanie nakazu, po uzyskaniu przez tę osobę zgody ministra, przedłużyć stosowanie nakazu na czas nieprzekraczający okresu, na który nakaz może zostać wydany zgodnie z art. 21 (6), jeżeli dowody wskazują, że:

- a) nakaz jest niezbędny do umożliwienia służbie zbadania zagrożenia bezpieczeństwa Kanady lub do wykonywania przez służbę zadań zgodnie z art. 16;
- b) następują fakty, o których mowa w art. 21 (2) b (nieskuteczność innych metod).

22.1. (1) Sędzia może – na wniosek osoby upoważnionej do złożenia wniosku o wydanie nakazu, po uzyskaniu zgody ministra, jeżeli w uzasadnionej opinii tej osoby nakaz jest w dalszym ciągu niezbędny do zwalczania zagrożeń bezpieczeństwa Kanady – przedłużyć stosowanie nakazu, jeżeli dowody wskazują, że:

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

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

14. Ograniczenia w wykonywaniu nakazu

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

LUKSEMBURG

1. Ochrona informacji niejawnych

Ustawa z dnia 15 czerwca 2004 r. o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa⁶ – wyciąg

Art. 2. Pojęcia używane w niniejszej ustawie oznaczają:

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

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

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

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

Art. 21. Krajowa Władza Bezpieczeństwa może pozyskiwać, na potrzeby postępowania sprawdzającego, informacje o stanie cywilnym, wypłacalności, sytuacji społecz-

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

nej i zawodowej – zarówno aktualnej, jak i przeszłej – reputacji oraz podatności i wrażliwości na formy nacisku osoby, wobec której toczy się postępowanie sprawdzające.

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

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

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

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

Informacje uzyskane w ramach postępowania sprawdzającego podlegają zniszczeniu lub usunięciu:

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

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

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

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

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

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

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

2. Dostęp do baz danych

Art. 4.1. Przetwarzanie przez SRE informacji uzyskanych w toku realizacji jej ustawowych zadań odbywa się zgodnie z zasadami przewidzianymi w rozporządzeniu, do którego wydania zobowiązuje ustawa o ochronie danych osobowych.

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

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

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

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

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

SZWAJCARIA

Ustawa o Federalnej Służbie Wywiadowczej⁹ – wyciąg

Rozdział I. Ogólne postanowienia i zasady

Zbieranie informacji

Art. 2. Cele.

Ustawa ma na celu:

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

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

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

Art. 3. Zastosowanie w szczególnych sytuacjach.

Rada Federalna może w szczególnych sytuacjach zlecić NBD)¹⁰ ochronę innych niezbędnych interesów narodowych; do podstawowych działań tego typu należy: ochrona konstytucyjnych podstaw Szwajcarii, wsparcie szwajcarskiej polityki zagranicznej i ochrona szwajcarskiej gospodarki, przedsiębiorstw oraz instytucji finansowych.

(...)

Art. 5. Zasady gromadzenia informacji.

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

Rozdział II. *Zadania i współpraca NDB*

Art. 6. Zadania NDB.

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

¹⁰ Nachrichtendienst des Bundes.

- atakiem na systemy informatyczne, komunikację, energetykę, transport i inne elementy infrastruktury istotne dla funkcjonowania społeczeństwa, biznesu i administracji publicznej (infrastruktura krytyczna),
 - ekstremizmem z użyciem przemocy;
 - b) wykrywaniu, monitorowaniu i ocenie polityki bezpieczeństwa istotnych zdarzeń za granicą;
 - c) zabezpieczeniu zdolności Szwajcarii do działań;
 - d) ochronie podstawowych interesów narodowych na mocy art. 3, jeżeli takie zadania zostały zlecone przez Radę Federalną.
2. NDB dokonuje oceny zagrożenia państwa oraz informuje zainteresowane kantonalne i lokalne organy ścigania o wszelkich niebezpieczeństwach i podjętych środkach oraz o planowanych działaniach w ramach niniejszej ustawy.
 3. NDB informuje inne agencje federalne, kantonalne, przestrzegając zasady ochrony źródeł, o zdarzeniach i ustaleniach, które dotyczą utrzymania bezpieczeństwa wewnętrznego lub zewnętrznego państwa.
 4. NDB utrzymuje relacje ze służbami zagranicznymi.
 5. NDB wykorzystuje systemy wczesnego ostrzegania w celu ochrony infrastruktury krytycznej.
 6. NDB prowadzi programy informacyjne i uświadamiające dotyczące zagrożeń bezpieczeństwa wewnętrznego lub zewnętrznego państwa.
 7. NDB chroni swoich pracowników, źródła oraz przetwarzane informacje.
- (...)

Art. 12. Współpraca z państwami obcymi.

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

Rozdział III. Informacje**Sekcja I. Gromadzenie informacji bez autoryzacji.****Art. 13.** Źródła informacji dostępne publicznie.

Publicznymi źródłami informacji są przede wszystkim:

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

Art. 14. Obserwacja w miejscach publicznych.

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

Art. 15. Źródła osobowe.

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