



WYŻSZE KURSY OBRONNE

Martin Bożek
Iwona Stankowska
Sławomir Zalewski

OCHRONA INFORMACJI NIEJAWNYCH

Wybrane zagadnienia



Warszawa 2003

56804

Martin Bożek
Iwona Stankowska
Sławomir Zalewski



OCHRONA INFORMACJI NIEJAWNYCH

Wybrane zagadnienia

Warszawa 2003



Niniejszy materiał studyjny jest przeznaczony
do wykorzystania na Wyższych Kursach Obronnych
dla kierowniczej kadry administracji publicznej
i został rekomendowany przez Departament Ochrony Informacji
Niejawnych Agencji Bezpieczeństwa Wewnętrznego.

SPIS TREŚCI

Wprowadzenie	5
Rozdział 1. Zagadnienia wstępne (<i>Iwona Stankowska</i>)	7
1.1. Pojęcie i geneza tajemnicy	7
1.2. Obowiązek ochrony tajemnicy państwowej	19
1.3. Rodzaje tajemnic prawnie chronionych	26
Rozdział 2. Organizacja ochrony informacji niejawnych w Polsce (<i>Martin Bożek</i>)	46
2.1. Zakres przedmiotowy i podmiotowy	46
2.2. System ochrony informacji niejawnych	48
2.3. Rozwiązania instytucjonalne	54
2.4. Organizacja systemu ochrony informacji niejawnych w podmiotach stosujących przepisy o ochronie informacji niejawnych	58
2.5. Obieg informacji niejawnych	63
Rozdział 3. Dostęp do informacji niejawnych (<i>Iwona Stankowska, Sławomir Zalewski</i>)	67
3.1. Postępowanie sprawdzające – cele i zakres	67
3.2. Procedura odwoławcza i skargowa w przedmiocie odmowy wydania poświadczenia bezpieczeństwa	85
Rozdział 4. Udostępnianie informacji niejawnych (<i>Martin Bożek</i>) ...	96
4.1. Udostępnianie danych z ewidencji i akt postępowań sprawdzających	96
4.2. Udostępnianie informacji w świetle ustawy o ochronie informacji niejawnych	98
4.3. Zasady zwalniania z obowiązku zachowania tajemnic	100
Rozdział 5. Odpowiedzialność za naruszenie przepisów o ochronie informacji niejawnych (<i>Iwona Stankowska</i>)	102
5.1. Odpowiedzialność karna	102
5.2. Odpowiedzialność dyscyplinarna i służbowa	113
5.3. Odpowiedzialność za naruszenie przepisów procedury sprawdzeniowej	116

Zakończenie	119
Aneks	121
Bibliografia	128

WPROWADZENIE

Wejście w życie Ustawy o ochronie informacji niejawnych wytworzyło nową sytuację w zakresie ochrony tajemnicy państwowej i służbowej. Określiło funkcje i zadania służb specjalnych jako służb ochrony państwa.

Wykonując ustawowe zadania, służby prowadzą postępowania sprawdzające wobec osób zatrudnionych na stanowiskach związanych z dostępem do informacji niejawnych bądź aspirujących do uzyskania takiego zatrudnienia, przeprowadzają procedury w zakresie bezpieczeństwa przemysłowego wobec podmiotów gospodarczych oraz wydają certyfikaty w zakresie bezpieczeństwa teleinformatycznego. Zadania służb ochrony państwa obejmują też kontrolę przestrzegania zasad ochrony informacji niejawnych, która obejmuje zarówno zagadnienia bezpieczeństwa osobowego, przemysłowego, jak również teleinformatycznego w zakresie przewidzianym ustawą. Służby prowadzą także stały nadzór nad działalnością pionów ochrony i pełnomocników ochrony w organach administracji, instytucjach oraz podmiotach gospodarczych, w których informacje niejawne są wytwarzane, przetwarzane bądź przechowywane. Prawną pozycję służb specjalnych wyznacza również funkcja krajowych władz bezpieczeństwa, którą szefowie Agencji Bezpieczeństwa Wewnętrznego oraz Wojskowych Służb Informacyjnych wykonują w kontaktach międzynarodowych związanych z ustawowymi zadaniami w sferze ochrony informacji niejawnych.

Powstał zatem nowy system ochrony informacji niejawnych, w którym służby ochrony państwa spełniają szczególną rolę wobec organów administracji publicznej, podmiotów gospodarczych oraz obywateli – realizowaną w sferze bezpieczeństwa narodowego. Zarówno w spełnianiu tej funkcji, jak i innych służby specjalne poddane są nadzorowi właściwych organów władzy wykonawczej oraz kontroli cywilnej sprawowanej przez niezawisłe sądy oraz przedstawicieli władzy ustawodawczej. Służby funkcjonują zatem w strukturach demokratycznego państwa i działają na rzecz ochrony jego ważnych interesów, związanych z ochroną informacji niejawnych.

Celem tego opracowania jest skrótowne ukazanie problematyki ochrony informacji niejawných ze szczególnym uwzględnieniem zakresu spraw sytuowanego w obszarze tzw. bezpieczeństwa osobowego. Przedmiotowa problematyka została ukazana w aspektach prawnych oraz organizacyjnych i obejmuje przegląd pojęć podstawowych związanych z ochroną tajemnicy, zagadnieniami organizacji ochrony informacji niejawných, procedur uzyskiwania dostępu do tych informacji, zasad i trybu ich udostępniania oraz odpowiedzialności za naruszenie przepisów o ochronie informacji niejawných.

Autorzy wyrażają nadzieję, że takie ujęcie przedmiotowej problematyki może być pomocne wszystkim tym, którzy swoje role zawodowe realizują na stanowiskach związanych z dostępem do informacji niejawných, może być także przydatne jako punkt wyjścia do dalszych studiów nad przedmiotową problematyką.

Rozdział 1

ZAGADNIENIA WSTĘPNE

Spośród terminów przydatnych do charakteryzowania problematyki ochrony informacji niejawnych kluczowe jest pojęcie tajemnicy. Towarzyszy ona od zarania dziejów człowiekowi i wszelkim formom jego organizacji, w tym państwu. Jest czynnikiem bezpieczeństwa, bywa postrzegana jako walor człowieka godnego zaufania: „kto zdradza tajemnicę, traci zaufanie... Bo rana może być opatrzona, obelga darowana, ale ten kto wyjawiał tajemnicę nie ma już nadziei”¹.

1.1. Pojęcie i geneza tajemnicy

Tajemnica jest pojęciem wieloznacznym. Oznacza coś tajnego, rzecz, której nie należy rozgłaszać, która nie powinna wyjść na jaw; sekret².

Według „Nowej Encyklopedii Powszechnej” „tajemnicą” jest określona przez przepisy wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo³. Inne źródło podaje, że tajemnicą jest wiadomość, która dotyczy okoliczności nieznanych ogółowi, lecz tylko ograniczonemu relatywnie kręgowi osób. Liczba i rodzaj osób, które mogą wiadomość już znać, a mimo to nadal kwalifikuje się ją jako tajemnicę, nie da się mechanicznie określić; jest to rzecz względna, którą można ustalić i ocenić tylko na tle konkretnego życiowego przypadku⁴.

Ogólnie można przyjąć, że pod pojęciem „tajemnica” kryje się wiadomość (informacja) znana określonym jednostkom lub grupom,

¹ *Stary Testament, Mądrość Syracha* (27, 16, 21).

² S. Skorupko, H. Auderska, Z. Łempicka, *Mały słownik języka polskiego*, Wyd. PWN, Warszawa 1969, s. 819.

³ *Nowa Encyklopedia Powszechna*, t. 7, Wyd. PWN, Warszawa 1996.

⁴ J. Sawicki, *Tajemnica zawodowa dziennikarza*, „Prasa Polska”, nr 11, s. 24.

a nie przeznaczona do udostępnienia osobom postronnym (nieuprawnionym). Tajemnicą nie może być wiadomość o faktach powszechnie znanych ani informacja powszechnie dostępna w różnego rodzaju publikacjach (będących w obiegu nieoficjalnym) i przez to stanowiąca rodzaj „publicznej tajemnicy”¹.

Polskie ustawodawstwo, wzorem wielu innych państw, nie określa w przepisach prawa pojęcia „tajemnica”. Można zgodzić się z opiniami tych autorów, którzy uważają, że nie jest to konieczne. Przepisy prawne wszak nie chronią tajemnicy rozumianej w sposób generalny, lecz jedynie pewne jej zakresy².

Potrzeba ochrony tajemnicy pojawiła się już w najdawniejszych czasach istnienia ludzkości. Wiązała się z koniecznością zatajenia wobec nieprzyjaciela informacji z życia społeczeństw i państw w imię ich bezpieczeństwa zewnętrznego. Zdrada takiej tajemnicy związana była nierozdzielnie z działaniem objętym dziś pojęciem szpiegostwa.

Szpiegostwo traktowane początkowo jako grzech wobec bóstwa stało się wraz z rozwojem państwowości przestępstwem przeciwko panującemu, a potem przeciwko państwu. W prawie karnym Aten i Sparty przekazywanie nieprzyjacielowi tajemnic państwowych lub wojskowych było przestępstwem zdrady przeciwko państwu. W prawie rzymskim udzielenie tajemnic państwowych wrogowi mieściło się w pojęciu „proditio” lub „preduellio”³.

Podobnie regulacje dotyczące tajemnicy kształtowały się w prawie polskim. W epoce średniowiecza ujawnienie wrogowi tajemnic państwowych było przestępstwem publicznym, podobnie jak i inne

¹ Sąd Najwyższy przyjął, że „fakty powszechnie znane” – to m.in. fakty historyczne, utrwalone w piśmiennictwie naukowym, a więc te relacje o pewnych mających miejsce w przeszłości zdarzeniach, w tym także politycznych, które w sposób zgodny z zasadami metodologii naukowej, a więc w oparciu o różnorodne źródła, ujawnione zostały przez historyków. W takim przypadku fakt staje się elementem świadomości zbiorowej danego społeczeństwa i bez względu na próby interpretowania go przez różne podmioty zbiorowe staje się on dla członków tejże zbiorowości faktem powszechnie znanym. Wyrok SN z dnia 9 marca 1993 r., WRN 8/93, OSNKW 1993, nr 7–8, poz. 49.

² Bliżej B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*, Warszawa 2000, s. 250–251.

³ H. Rajzman, *Zdrada kraju w prawie polskim*, Warszawa 1948, s. 19–23; J. Bronisławski, *Szpiegostwo, wywiad, paragrafy*, Warszawa 1974, s. 11–14.

czyny skierowane przeciwko państwu. W Konstytucji sejmu koronnego z 1588 r. zdrada nieprzyjacielowi tajemnic Rzeczypospolitej była przestępstwem zdrady kraju.

W czasach nowożytnych katalog czynów karalnych przeciwko państwu znacznie się rozbudował. Prawo o sądach sejmowych z 1791 r. przewidywało sankcje karne za zdraдлиwe wydanie tajemnic państwowych obcemu narodowi¹.

W Kodeksie karzącym z 1818 r. karze podlegało „szpiegowanie” lub „udzielanie stosownych do celu tajemnic i układów”, jeśli było sposobem „przedsiębrania” lub „wykonania zbrodni stanu” (art. 67).

W latach transformacji ustrojowej termin „tajemnica” przeszedł pewną ewolucję. Niewątpliwie wiązało się to z burzliwą historią naszego narodu, który wielokrotnie poddawany był ciężkiej próbie w walce o utrzymanie państwowości i odzyskanie niepodległości. Obce wpływy i zależności zawsze odciskały swoje piętno na naszym narodzie we wszystkich sferach jego życia.

Do problematyki bezpieczeństwa informacji i ochrony tajemnicy w różnych okresach historii podchodzono niejednokrotnie w sposób irracjonalny. W postulowanych rozwiązaniach brakowało często pragmatycznego podejścia pozwalającego na precyzyjną regulację pojęciową, proceduralną oraz decyzyjną. Nie dotyczy to samego terminu „tajemnica”, którego znaczenie objaśniają encyklopedie, leksykony, słowniki. Trudności pojawiają się w aspekcie interpretacji pojęcia „tajemnica państwowa”, jego zakresu i szczegółowości.

W pierwszych latach po odzyskaniu przez Polskę niepodległości, po ponad 100-letnim okresie zaborów, państwo, chroniąc swoje interesy, posługiwało się przepisami zaborczych kodeksów karnych z 1871 i 1903 r. oraz przepisami niemieckiej Ustawy z dnia 3 czerwca 1914 r. o zdradzie tajemnic wojskowych².

Pruski kodeks karny z 1871 r. ujawnienie tajemnicy państwowej określał w art. 92: *Kto by umyślnie tajemnice stanu lub plany twierdz albo także dokumenty, papiery lub wiadomości, o których wie, że dla dobra Rzeszy lub kraju związkowego winny być trzymane w tajemnicy przed obcym rządem, temu rządowi podawał do wiadomości albo*

¹ J. Rafacz, *Dawne prawo sądowe polskie w zarysie*, Warszawa 1936, s. 397, 399 i 402.

² DzU Rzeszy, s. 195.

publicznie wyjawiał... . Przestępstwo to zagrożone było karą śmierci, ciężkiego więzienia, konfiskatą majątku, wysokimi grzywnami i pozbawieniem praw publicznych i honorowych.

W byłym zaborze rosyjskim obowiązywała Ustawa karna z 1903 r., która długoletnią karę więzienia przewidywała za zbieranie, publikowanie, komunikowanie lub udzielanie innej osobie, bez należytego upoważnienia, wiadomości, przedmiotów, które winny być zachowane w tajemnicy, a dotyczyły zewnętrznego bezpieczeństwa państwa, jego sił zbrojnych lub urzędów przeznaczonych do wojskowej ochrony kraju¹.

Wpływy tych przepisów znalazły odbicie w Rozporządzeniu prezydenta Rzeczypospolitej z dnia 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciwko państwu².

Rozporządzenie, wzorem pruskiego kodeksu karnego, rozgraniczało szpiegostwo od ujawnienia tajemnicy państwowej, różnicując nadto ujawnienie na umyślne i nieumyślne, co wiązało się z wysokością kary pozbawienia wolności. Art. 1 w § 1 tego rozporządzenia przewidywał, że: *Kto umyślnie ujawnia innej osobie wiadomości, dokumenty lub inne przedmioty, które ze względu na dobro Państwa Polskiego należy zachować w tajemnicy przed rządem państwa obcego, ulega karze więzienia do lat pięciu.*

Nieumyślne ujawnienie tajemnicy mogło nastąpić według rozporządzenia tylko w postaci niedbalstwa, zniszczenia lub zagubienia dokumentów. Czyny, które dotyczyły wojskowej obrony państwa lub jego sił zbrojnych – zagrożone były karą ciężkiego więzienia od roku do lat dziesięciu.

Po raz pierwszy definicja tajemnicy państwowej pojawiła się w Rozporządzeniu prezydenta Rzeczypospolitej z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa³. Zawierało ono następującą definicję (art. 9, § 1): *Tajemnicę państwową stanowią wiadomości, dokumenty lub inne przedmioty, które z powodu ich treści lub jakości należy ze względu na dobro Państwa Polskiego zachować w tajemnicy przed rządem państwa obcego, choćby nawet zarządzenia normujące czynności służbowe nie*

¹ J. Bronisławski, *Szpiegostwo...*, wyd. cyt.

² DzU RP nr 18, poz. 160.

³ DzU RP nr 19, poz. 851.

uznawały ich za tajne, albo choćby zachowanie ich w tajemnicy przed pewnym gronem osób było niemożliwe.

Rozporządzenie to rozszerzało katalog czynów karalnych oraz zwiększało wymiar odpowiedzialności karnej. Na uwagę zasługuje art. 21, § 1, w myśl którego odpowiedzialność karną ponosił również ten: *Kto otrzymawszy, w chwili gdy można szkodzić zapobiec, wiarygodną wiadomość o zamierzonym przestępstwie (określonym w tym przepisie), zaniecha zawiadomienia o tym władzy powołanej do ścigania przestępstw.* Przepis dotyczył przestępstwa ujawnienia innej osobie tajemnicy państwowej.

Po wojnie problem ochrony tajemnicy uregulowano w Dekrecie z dnia 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej¹. Zgodnie z nim tajemnicę państwową stanowiły wszelkie wiadomości, dokumenty lub inne przedmioty, które ze względu na ochronę, bezpieczeństwo lub ważne interesy gospodarcze bądź polityczne Państwa Polskiego albo państw zaprzyjaźnionych mogły być udostępnione wyłącznie osobom do tego uprawnionym.

Szczególną cechą dekretu, poza tym że zawierał zwięzłe definicje obydwu tajemnic (również służbową), było to, że przewidywał delegację fakultatywną dla Rady Ministrów do szczegółowego określenia zakresu wiadomości stanowiących tajemnicę państwową i upoważnienie dla państwowych władz naczelnych do wydania zarządzeń wykonawczych zabezpieczających ochronę tajemnicy państwowej oraz znacznie rozbudowane przepisy karne.

Dekret z 1949 r. utracił moc z dniem 1 stycznia 1970 r. wraz z wejściem w życie kodeksu karnego z dnia 19 kwietnia 1969 r.²

Pojęcie tajemnicy państwowej w kodeksie karnym z 1969 r. ujęte zostało zbiorczo z definicją tajemnicy służbowej. Ustawodawca umieścił je w słowniczku kodeksowym – art. 120, § 15 i 16 kk. Zgodnie z przepisem „tajemnicą państwową” objęta była wiadomość, której ujawnienie osobom nieuprawnionym mogło narazić na szkodę bezpieczeństwo lub inny ważny interes polityczny lub gospodarczy Polskiej Rzeczypospolitej Ludowej.

¹ DzU nr 55, poz. 437.

² DzU nr 13, poz. 94.

Tajemnicę służbową stanowiła z kolei wiadomość, z którą pracownik zapoznał się w związku ze swoją pracą w instytucji państwowej lub społecznej, a której ujawnienie osobom nieuprawnionym mogło narazić na szkodę społecznie uzasadniony interes.

W przeciwieństwie do obowiązującego przed wejściem w życie kodeksu karnego z 1969 r. – Dekretu o ochronie tajemnicy państwowej i służbowej, który rozróżniał pojęcia wiadomości, dokumentów lub innych przedmiotów w definicjach obu wymienionych tajemnic, kodeks karny przyjął zbiorcze pojęcie „wiadomość”. Obejmowało ono również dokument lub przedmiot.

Wiadomość oznaczała informację lub sumę informacji o osobie albo o stanie rzeczy stanowiącą logiczną całość. Utrwalona mogła być zarówno w pamięci osoby, która ją poznała, lub też poprzez inny zapis w najróżniejszych jego formach (pismo ręczne, maszynopis, druk, taśma magnetofonowa). Dokument zatem lub inny przedmiot to tylko różne sposoby utrwalenia wiadomości. Rozróżnienie więc tych pojęć w dekreście wydaje się zbędne.

Ustawodawca z 1969 r. wzorując się na dekreście z 1949 r. oparł się na materialnym określeniu zarówno tajemnicy państwowej, jak i służbowej. Definicje te bowiem wskazują, choć bardzo ogólnie, jakiej treści, jakiego rodzaju wiadomości stanowią tajemnicę w rozumieniu kodeksu karnego.

Przyjęcie przez ustawodawcę formalnego określenia tajemnicy oznaczałoby oparcie się na woli organów właściwych do decydowania o charakterze informacji, utajnienia wiadomości.

Skutkiem takiego rozwiązania byłoby określenie mianem tajemnicy tylko tych wiadomości, które za takie zostały uznane¹.

Kodeks karny z 1969 r. nie penalizował odrębnie różnych wyspecjalizowanych rodzajów sekretu, jak np. tajemnica wojskowa, gospodarcza, urzędnicza, funkcyjna itp., posługując się tylko pojęciami tajemnicy państwowej i służbowej, w których to pojęciach mieścić się

¹ I. Andrejew, W. Świda, W. Wolter, *Kodeks karny z komentarzem*, Warszawa 1973, s. 806–807; także O. Chybiński, W. Gutekunst, W. Świda, *Prawo karne. Część szczególna*, Wrocław 1971, s. 418.

mogły różne wyspecjalizowane rodzaje sekretu, jeśli oczywiście wyczerpywały definicję tych tajemnic¹.

Wprowadzenie stanu wojennego 13 grudnia 1981 r. sprawiło, że za tajemnicę państwową zaczęto powszechnie uważać wszystkie wiadomości dotyczące nazwy uzbrojenia i sprzętu wojskowego, danych techniczno-taktycznych opisu technicznego, dokumentacji i produkcji, sprzętu wojskowego, a w szczególności dokumentacji technologicznej, wyposażenia jednostek wojskowych, a także fotografie, filmy, rysunki obiektów i przedmiotów wojskowych.

Kształtująca się i wciąż zmieniająca scena polityczna, tworzenie nowej ekonomiki państwa, zmiany społeczne, negowanie dotychczasowych rozwiązań spowodowały konieczność uchwalenia nowego aktu normatywnego regulującego zagadnienie ochrony tajemnicy. Wynikiem tych dążeń była uchwalona przez Sejm PRL w dniu 14

¹ Na wady przyjęcia takiej koncepcji wskazuje B. Kunicka-Michalska. Przyjęcie wskazanego rozwiązania w ustawodawstwie pociąga za sobą pewne konsekwencje. Otóż, przy interpretacji poszczególnych, określonych prawnie rodzajów sekretu, trzeba mieć na uwadze wypracowane już w doktrynie zasady dotyczące samego pojęcia „tajemnica” w jego prawniczym rozumieniu. Zgodnie z nimi tajemnicą chronioną prawnie nie może być ani tzw. tajemnica absolutna, która obejmuje fakty nieznane jeszcze nikomu, ani tzw. fakty niepoznane, czyli informacje powszechnie znane lub powszechnie dostępne, lecz nieznane tylko pewnym jednostkom, które nie zapoznały się z nimi. Nie może być bowiem tajemnicą państwową, służbową, ani żadną inną chronioną prawnie wiadomość, która nie posiada cech tajemnicy w prawniczym rozumieniu tego terminu.

Tajemnica w prawniczym rozumieniu to taka, która nadaje się do ochrony prawnej, która może być naruszona (naruszalna i zdradzalna) i nie pokrywa się z potocznym i szerokim rozumieniem tego terminu. Tajemnicą chronioną prawnie może być jedynie tajemnica relatywna (względna), to jest fakt znany pewnemu kręgowi osób lub pojedynczej osobie. W grupie osób, której znane są wiadomości wymagające dyskrecji, wyróżnia się dysponenta, tzw. pana tajemnicy, czyli tego, kto jest uprawniony do rozstrzygania, czy dany fakt powinien pozostać zachowany w dyskrecji i jej powiernika, czyli tzw. sługę tajemnicy, a więc tego, kto nie może rozporządzać tajemnicą, lecz jest zobowiązany do milczenia.

Opierając się na tych rozważaniach, należy przyjąć, że tajemnicą państwową, służbową czy inną, niezależnie od ich ujęcia w przepisach prawa, może być tylko wiadomość znana dysponentom lub ewentualnie powiernikom tajemnicy. *Ochrona tajemnicy w kodeksie karnym*, Acta Universitatis Nicolai Copernici, 1978; Prawo XVI z. 1989, s. 86–87.

grudnia 1982 r. Ustawa o ochronie tajemnicy państwowej i służbowej¹.

Przepisy tego aktu określały pojęcie tajemnicy państwowej i służbowej, regulowały tryb ustalania wiadomości stanowiących te tajemnice, ustalały sposób dopuszczania osób do tajemnic i cofanie wydanych w tym względzie upoważnień oraz określały zasady i sposób postępowania z wiadomościami klasyfikowanymi.

Z art. 2, ust. 1 ustawy wynikało, że tajemnicą państwową jest wiadomość, której ujawnienie osobom nieupoważnionym może narazić na szkodę obronność, bezpieczeństwo lub inny ważny interes państwa, dotycząca w szczególności:

- 1) przygotowań obronnych w gospodarce narodowej i administracji państwowej; rodzaju i ilości uzbrojenia, wyposażenia obronnego, stanu liczbowego, organizacji, struktur, rozmieszczenia, gotowości bojowej oraz planów mobilizacyjnych i operacyjnych sił zbrojnych; potencjału i zdolności produkcyjnych oraz wielkości i rodzaju produkcji przemysłu obronnego; danych z dziedziny geodezji, kartografii, topografii, grawimetrii i magnetyzmu Ziemi, zdjęć lotniczych i fotogrametrycznych, opisów topograficznych obiektów, urządzeń i terenów wojskowych – mających ważne znaczenie dla obronności kraju oraz współpracy z zagranicą w zakresie układów obronnych;
- 2) organizacji organów ochrony porządku i bezpieczeństwa publicznego, ich wyposażenia oraz form i metod pracy, a także danych identyfikujących funkcjonariuszy tych organów i osoby współdziałające z organami ochrony bezpieczeństwa publicznego, wykonujących zadania z zakresu wywiadu i kontrwywiadu; wyposażenia obiektów, urządzeń i terenów mających ważne znaczenie dla bezpieczeństwa państwa; organizacji i systemu ochrony granicy państwowej oraz łączności szyfrowej i kodowej sił zbrojnych, organów ochrony porządku i bezpieczeństwa publicznego i innych służb państwowych;
- 3) prac naukowo-badawczych, projektowych, technologicznych i konstrukcyjnych, inwestycji, wynalazków i wzorów

¹ DzU nr 40, poz. 271 ze zm.

użytkowych mających związek z obronnością lub bezpieczeństwem państwa;

- 4) produkcji o podstawowym znaczeniu dla gospodarki narodowej, stanu i rozmieszczenia rzeczowych rezerw państwowych ważnych dla gospodarki narodowej, obronności i bezpieczeństwa państwa;
- 5) działalności banków związanej z projektowaniem emisji znaków pieniężnych oraz bankowych papierów wartościowych, przechowywania i transportu wartości pieniężnych, sytuacji kredytowej banków dewizowych, obsługi bankowej jednostek wydzielonych oraz innych spraw w zakresie bankowości o szczególnie ważnym znaczeniu ze względu na interes państwa;
- 6) przygotowań i negocjacji w sprawie zawarcia umów międzynarodowych, w tym międzynarodowych umów handlowych.

Art. 2, ust. 2 ustawy stanowił, że tajemnicą państwową jest również treść umowy międzynarodowej lub wiadomość występująca w stosunkach międzynarodowych, jeżeli tajność tej umowy lub wiadomości została zastrzeżona co najmniej przez jedną ze stron.

Ustawa w ten sposób zarysowała materię tajemnicy państwowej, natomiast jej szczegółowe określenie ustawodawca przekazał do kompetencji naczelnym i centralnym organom państwowym oraz terenowym organom administracji państwowej stopnia wojewódzkiego. Zgodnie z ust. 1, art. 6 do organów tych należało ustalenie:

- a) wykazów rodzajów wiadomości stanowiących tajemnicę państwową oraz
- b) wykazów rodzajów wiadomości stanowiących tajemnicę państwową o szczególnie ważnym znaczeniu dla obronności państwa, sił zbrojnych i bezpieczeństwa państwa – występujących w zakresie działania tych organów oraz w działalności jednostek organizacyjnych im podległych lub przez nie nadzorowanych. W zakresie działania banków kompetencje do szczegółowego określenia wiadomości stanowiących tajemnicę państwową (tajne i tajne specjalnego znaczenia) przysługiwały prezesowi Narodowego Banku Polskiego (art. 6, ust. 2).

Wymienione wykazy, przed ich opublikowaniem, wymagały uzgodnień z ministrem spraw wewnętrznych i administracji; natomiast

te, które zawierały wiadomości z zakresu obronności państwa – także z ministrem obrony narodowej, a wykazy zawierające wiadomości dotyczące stosunków z zagranicą – z ministrem spraw zagranicznych. Nie podlegały ogłoszeniu jedynie wykazy wiadomości dotyczących obronności, sił zbrojnych i bezpieczeństwa państwa.

Definicja tajemnicy państwowej, zawarta w ustawie z 1982 r. ma, w przeciwieństwie do poprzedniego stanu prawnego, charakter materialno-formalny, co oznacza, że wiadomość będzie stanowić tajemnicę państwową, gdy jej ujawnienie może narazić na szkodę ważny interes państwa oraz gdy, z woli organów uprawnionych, została objęta wykazem oraz oznaczona jednym z dwóch gryfów tajności (*tajne* lub *tajne specjalnego znaczenia*).

Nowy przepis wymienia odrębnie obronność, pomija podział na interes polityczny i gospodarczy, mówiąc zbiorczo o innym ważnym interesie państwa, a ponadto wylicza w długim wykazie, czego ma wiadomość dotyczyć. Wyliczenie nie jest wyczerpujące, o czym świadczy zwrot „w szczególności” użyty w art. 2, ust. 1 ustawy. Niektóre ujęte w nim zakresy nasuwają wątpliwości i mogą stwarzać okazję do szerokiej ich interpretacji¹.

Pojęcia „interesu państwa” oraz „ważnego interesu państwa” są pojęciami mało precyzyjnymi, nieostrymi i kryjącymi w sobie niebezpieczeństwo dowolności w interpretacji. Podobne uwagi należy odnieść do zwrotu „może narazić na szkodę... interes”.

Termin ten oznacza, że aby stwierdzić czy dana wiadomość stanowi tajemnicę państwową, należy wykazać, że jej ujawnienie mogło narazić na szkodę realną, a nie abstrakcyjną oraz na czym ten („naruszony”) interes polegał.

Ustawie z 14 grudnia 1982 r. postawiono wiele innych zarzutów, w szczególności że jest sprzeczna z istotą państwa demokratycznego, które, strzegąc swoich tajemnic, nie powinno i nie może ponad miarę ograniczać wolności obywatelskich, takich jak wolność słowa czy wolność badań naukowych. Uznano ją za przestarzałą, niehumanitarną, nie odpowiadającą wymogom państwa prawnego, wreszcie zarzucono jej, że nosi piętno stanu wojennego.

¹ Bliżej B. Kunicka-Michalska, *Nowe przepisy o ochronie tajemnicy państwowej i służbowej*, „Państwo i Prawo” 1983, nr 11, s. 35 i in.

W związku z tym natychmiast po zmianie polityczno-ustrojowej, jaka dokonała się w Polsce w wyniku historycznych wyborów do Sejmu i Senatu w dniu 4 czerwca 1989 r. – odezwały się głosy o pilnej konieczności uchwalenia nowej ustawy o ochronie tajemnicy państwowej i służbowej.

Prace nad nową ustawą podjął rząd Tadeusza Mazowieckiego. Projekt miał być przegłosowany na ostatnim posiedzeniu Sejmu przed upływem jego kadencji, jednak nie doszło do tego z braku wymaganej konstytucyjnej bezwzględnej większości głosów. Kolejny projekt ustawy był przedmiotem obrad komisji sejmowych, które wiosną 1992 r. odmówiły nad nim dalszych prac. Formalnym powodem był fakt, że ówczesny minister spraw wewnętrznych – Antoni Macierewicz przedstawił komisjom daleko idące autopoprawki, do których nie miał upoważnienia od rządu. Po odwołaniu, w czerwcu 1992 r., rząd Jana Olszewskiego kolejny wycofał ustawę z Sejmu.

Rząd Hanny Suchockiej pracował nad nowym projektem do lata 1993 r. Dodać należy, że projekt został przekazany Sejmowi już po jego rozwiązaniu przez prezydenta Lecha Wałęsę. W związku z tym, że w wyniku wcześniejszych wyborów nastąpiły istotne zmiany w składzie Sejmu i rządu – nowy Sejm zwrócił ustawę nowemu rządowi z prośbą o zajęcie stanowiska.

Rząd Waldemara Pawlaka przedstawił Sejmowi ten sam projekt – już jako własną inicjatywę ustawodawczą. Po roku debat parlamentarnych Sejm uchwalił nową ustawę w dniu 15 września 1994 r.

Uchwalony tekst został – w stosunku do projektu rządowego – znacznie zliberalizowany. Mimo to spotkał się z krytyką przedstawicieli partii opozycyjnych – jako zbyt rygorystyczny. Dnia 6 października cztery komisje senackie (głosami senatorów ugrupowania SLD i PSL) postanowiły rekomendować Senatowi zgłoszenie poprawek wypracowanych przy udziale przedstawicieli rządu i sprawozdawców komisji sejmowych. Ostatecznie w dniu 7 października Senat postanowił odrzucić ustawę.

Odrzucenie weta Senatu pozbawiałoby ustawę liberalizujących poprawek. Natomiast jego przyjęcie oznaczałoby konieczność rozpoczęcia prac od początku. Posłowie apelowali do rządu, aby przedstawił nowy projekt przed ostateczną decyzją Sejmu w sprawie weta Senatu. Rząd wciąż odmawiał, argumentując, że nadal trwają parlamentarne prace nad uchwaloną ustawą. Wyjście z patowej sytuacji

zapropowowali posłowie Klubu Unii Pracy oraz grupa posłów PSL. W lutym 1995 r. zgłoszono dwa odrębne projekty ustawy. Rząd poparł obydwie, przedstawiając kilka własnych propozycji. Pozwoliło to na „zamknięcie” procesu legislacyjnego nad projektem rządowym i wiosną 1995 r. Sejm przyjął weto Senatu. Liczono na szybkie uchwalenie nowej ustawy na podstawie gotowych projektów. Wydarzenia polityczne – wybory prezydenckie, oczekiwanie na wybory do Sejmu – spowodowały, że zarówno ówczesnej koalicji, jak i partiom opozycyjnym zabrakło woli politycznej do kontynuowania prac. Woli tej wystarczyło jedynie, aby w dniu 27 sierpnia 1997 r. Sejm mógł uchwalić ograniczoną nowelizację ustawy o ochronie tajemnicy państwowej i służbowej, podyktowaną potrzebą dostosowania polskich przepisów w tym zakresie do rozwiązań przyjętych w państwach należących do NATO w związku z planowanym przystąpieniem do tej organizacji.

Wraz z upływem kadencji Sejmu (jesienią 1997 r.) utraciły moc obydwie poselskie projekty ustawy. Oznaczało to konieczność rozpoczęcia od początku prac legislacyjnych.

W dniu 26 listopada 1998 r. rząd RP skierował do Sejmu projekt ustawy o ochronie informacji niejawnych. Na początku grudnia został skierowany do rozpatrzenia przez Komisję Nadzwyczajną, następnie uchwalony przez Sejm. Ustawa weszła w życie z dniem 11 marca 1999 r.¹

Celem ustawodawcy było stworzenie podstaw prawnych dla zorganizowania i funkcjonowania w Polsce takiego systemu ochrony informacji niejawnych, który – z jednej strony – uwzględniałby interes bezpieczeństwa państwa demokratycznego, z drugiej zaś – spełniałby wymagania Organizacji Traktatu Północnoatlantyckiego. Ochroną najważniejszych tajemnic rządziły dotąd mechanizmy przestarzałe, nie dające gwarancji należytego zabezpieczenia interesów państwa i jego obywateli.

Nowa ustawa w sposób diametralny zmieniła zasady ochrony informacji i wprowadziła jasno określone reguły dostępu do nich. Zgodnie z art. 2, pkt. 1 ustawy – „tajemnicą państwową” jest informacja niejawna określona w wykazie rodzajów informacji niejawnych, stanowiącym załącznik nr 1, której nieuprawnione ujawnienie

¹ DzU nr 11, poz. 95 ze zm.

może spowodować istotne zagrożenia dla podstawowych interesów Rzeczypospolitej Polskiej, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę.

Z ustawowej definicji wynika, że krąg chronionych informacji nie ma charakteru zamkniętego. O tym, czy dana informacja należy do kategorii wiadomości chronionych, decyduje jej treść oraz skutek, jaki może spowodować jej bezprawne ujawnienie.

Wykaz informacji niejawnych stanowiących tajemnicę państwową obejmuje 30 rodzajów informacji kwalifikowanych jako *ściśle tajne*, 40 – jako *tajne* ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny, a także 26 rodzajów informacji *tajnych* ze względu na ważny interes państwa.

1.2. Obowiązek ochrony tajemnicy państwowej

Obowiązek przestrzegania tajemnicy państwowej wynika wprost z konstytucji – art. 93 przepisów konstytucyjnych z 1952 r. obowiązujących do października 1997 r. stanowił: *Czułość wobec wrogów narodu oraz pilne strzeżenie tajemnicy państwowej jest obowiązkiem każdego obywatela*, natomiast: *Zdrada ojczyzny – szpiegostwo, osłabienie sił zbrojnych, przejście na stronę wroga – karana jest z całą surowością prawa jako najcięższa zbrodnia*. Nadto w myśl art. 92, ust. 1 *Obrona ojczyzny jest najświętszym obowiązkiem każdego obywatela*.

Konstytucja RP z dnia 2 kwietnia 1997 r.¹ już w art. 1 głosi, że *Rzeczpospolita Polska jest dobrem wspólnym wszystkich obywateli*, a wśród niewielu przepisów określających nasze obowiązki znalazł się m.in. obowiązek wierności państwu polskiemu oraz troska o wspólne dobro (art. 82) oraz obrona Ojczyzny (art. 85, ust. 1).

Szczegółową regulację dotyczącą zachowania tajemnicy państwowej zawierała Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej. Zgodnie z art. 5, ust. 1 – zachowanie tajemnicy państwowej jest obowiązkiem każdego, do czyjej wiadomości

¹ DzU nr 78, poz. 483.

dotarła. Oznacza to, że obowiązek ten ciążył nie tylko na osobach, które weszły w jej posiadanie z tytułu obowiązków służbowych, ale na wszystkich – bez względu na sposób, w jaki tajemnicę poznali.

Przepisy Zarządzenia nr 60/83 ministra spraw wewnętrznych z dnia 29 czerwca 1983 r. w sprawie szczegółowych zasad i sposobu postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową (niepublikowane)¹ już w postanowieniach ogólnych (§ 1, pkt 1) przewidywały obowiązek podjęcia niezbędnych przedsięwzięć w celu zapewnienia ochrony tajemnicy państwowej i służbowej przez naczelne i centralne organy administracji państwowej, jak również kierowników państwowych, spółdzielczych i społecznych jednostek organizacyjnych realizujących przepisy Ustawy o ochronie tajemnicy państwowej i służbowej z dnia 14 grudnia 1982 r. Wymienione jednostki nałożony obowiązek miały realizować w szczególności poprzez:

- 1) wprowadzenie w życie zasad ochrony tajemnicy określonych przepisami prawa oraz sprawowania nadzoru nad ich przestrzeganiem,
- 2) organizowanie systematycznego szkolenia pracowników,
- 3) stałe podnoszenie u pracowników poczucia odpowiedzialności i troski o zachowanie tajemnicy,
- 4) organizowanie instruktażu dla podległych pracowników upoważnionych do kontaktów służbowych z obywatelami państw obcych,
- 5) przeprowadzanie co najmniej raz w roku analizy i oceny stanu ochrony tajemnicy.

Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych nakłada obowiązek zachowania tajemnicy państwowej na osoby, które posiadają poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą *tajne* lub *ściśle tajne*.

Obowiązek przestrzegania tajemnicy państwowej zapisany został także w aktach normatywnych regulujących stosunek pracy lub wykonywanie niektórych zawodów.

Ogólną i mającą najszersze zastosowanie regulację zawiera Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy². Przepis art. 100 w § 2 wśród obowiązków pracowniczych wymienia zachowanie w tajemnicy.

¹ Zarządzenie to pierwotnie opatrzone było klauzulą *poufne*, jednak została ona uchylona decyzją ministra spraw wewnętrznych nr 319 z dnia 30 grudnia 1993 r.

² DzU nr 24, poz. 141 ze zm.

mnicy informacji, które mogłyby narazić pracodawcę na szkodę (pkt 4) oraz obowiązek przestrzegania tajemnicy określonej w odrębnych przepisach (pkt 5).

Z postanowieniami tymi koresponduje regulacja zawarta w § 3 Rozporządzenia ministra pracy i polityki socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych¹, który stanowi: *Pracodawca przed dopuszczeniem pracownika do pracy uzyskuje jego pisemne potwierdzenie zapoznania się z treścią Regulaminu pracy oraz z przepisami i zasadami dotyczącymi bezpieczeństwa i higieny pracy, a także z zakresem informacji objętych tajemnicą określoną w obowiązujących ustawach dla umówionego z pracownikiem rodzaju pracy*".

O obowiązku zachowania tajemnicy państwowej przypomina się w wielu ustawach dotyczących określonych grup pracowniczych lub zawodowych albo funkcji społecznych.

Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych² w art. 17, ust. 2, pkt 5 wymienia dochowanie tajemnicy państwowej i służbowej. Naruszenie obowiązków pracowniczych przez urzędnika państwowego mianowanego skutkuje odpowiedzialnością porządkową lub dyscyplinarną czy nawet karną. Natomiast urzędnicy państwowi niebędący mianowanymi ponoszą odpowiedzialność na zasadach określonych w kodeksie pracy.

Członek korpusu służby cywilnej jest zobowiązany w szczególności dochować tajemnicy ustawowo chronionej oraz przestrzegać Konstytucji Rzeczypospolitej Polskiej i innych przepisów prawa (art. 67, ust. 1), podobnie pracownik samorządowy. Zobowiązanie to wprost wynika z art. 15, ust. 2, pkt 4 ustawy³.

Zgodnie z art. 13 ust. 2 Ustawy o ochronie danych osobowych⁴ generalny inspektor oraz pracownicy biura są obowiązani zapewnić ochronę wiadomościom stanowiącym tajemnicę państwową lub służbową podczas kontroli przetwarzania danych.

Do obowiązków osoby nadzorującej lub wykonującej czynności kontrolne, obok bezstronnego i terminowego wykonywania zadań,

¹ DzU nr 62, poz. 286.

² DzU nr 86, poz. 953.

³ DzU nr 21, poz. 124 ze zm.

⁴ DzU nr 133, poz. 883.

obiektywnego ustalania i rzetelnego dokumentowania wyników kontroli, godnego zachowania się w służbie i poza nią oraz stałego podnoszenia kwalifikacji zawodowych, należy także przestrzeganie tajemnicy ustawowo chronionej (art. 71).

Określone obowiązki, dotyczące zachowania dyskrecji, ciąży na sędziach i prokuratorach również na podstawie przepisów regulujących ich status. Sędzia jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na swoje stanowisko poza jawną rozprawą sądową, przy czym obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego. Obowiązek ten z kolei ustaje, gdy sędzia składa zeznanie przed sądem, chyba że ujawnienie tajemnicy zagraża dobru państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W tych wypadkach z obowiązku zachowania tajemnicy może zwolnić sędziego minister sprawiedliwości (art. 67, § 3).

Podobną regulację zawiera Ustawa o prokuraturze¹. Obowiązek dotyczy okoliczności sprawy, o których prokurator powziął wiadomość w postępowaniu przygotowawczym lub poza jawną rozprawą sądową. Prokuratora od obowiązku zachowania tajemnicy zwolnić może prokurator generalny.

Ustawa z dnia 6 kwietnia 1990 r. o Policji² w art. 21 przewiduje zakaz udzielania informacji uzyskanych w czasie wykonywania czynności operacyjno-rozpoznawczych. Wiadomości te oznaczone są klauzulą tajności i udzielane mogą być wyłącznie na żądanie sądu lub prokuratora, a ich wykorzystanie może nastąpić jedynie w celu ścigania karnego. Zakaz ten nie ma zastosowania, jeżeli ustawa nakłada obowiązek udzielania takich informacji określonemu organowi albo gdy obowiązek wynika z umów lub porozumień międzynarodowych, a także w przypadkach gdy ich zatajenie prowadziłoby do zagrożenia życia lub zdrowia innych osób.

Podobną regulację prawną opisuje Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, a także ustawy normujące działalność Straży Granicznej, Inspekcji Celnej (obecnie Służby Celnej) czy kontroli skarbowej (wywiadu skarbowego).

¹ DzU z 1994 r., nr 19, poz. 70 ze zm.

² DzU nr 30, poz. 179 ze zm.

Ustawa o Narodowym Banku Polskim¹ zawiera również ogólną normę dotyczącą ochrony tajemnic. Artykuł 55 stanowi, że: *Pracownicy NBP oraz członkowie Rady, a także organów opiniotawczo-doradczych przy Zarządzie NBP są obowiązani do nieujawnienia osobom nieupoważnionym wiadomości stanowiących tajemnicę państwową, służbową i bankową, z którymi zapoznali się podczas pracy w NBP lub członkostwa w wymienionych wyżej organach. Obowiązek ten trwa również po rozwiązaniu stosunku pracy oraz po ustaniu członkostwa we wspomnianych organach*".

O tajemnicach jest mowa w Ustawie z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu². Obowiązek zachowania tajemnicy państwowej wprost wynika z art. 20 ustawy: *Pracownicy Instytutu Pamięci, także po ustaniu stosunku pracy, są zobowiązani zachować w tajemnicy wszystkie wiadomości związane z działalnością Instytutu Pamięci powzięte w związku z zatrudnieniem w tej jednostce. Natomiast prezes Instytutu może, w szczególnie uzasadnionych wypadkach, zezwolić na ujawnienie wiadomości stanowiącej tajemnicę państwową lub służbową oraz na udostępnienie dokumentów lub materiałów objętych tajemnicą państwową określonej osobie lub instytucji, jeżeli zachowanie tajemnicy uniemożliwiłoby wykonanie wskazanych w ustawie zadań Instytutu Pamięci*.

Obowiązek przestrzegania tajemnicy państwowej zapisany został w niektórych rotach ślubowania – sędzieja przy powołaniu na urząd, wobec prezydenta Rzeczypospolitej Polskiej ślubuje wiernie służyć państwu polskiemu, stać na straży prawa, obowiązki sędziego wypełniać sumiennie, sprawiedliwość wymierzać zgodnie z przepisami prawa, dochować tajemnicy państwowej i służbowej, a w postępowaniu kierować się zasadami godności i uczciwości; podobne zdania zawiera ślubowanie składane przez prokuratora, rzecznika praw obywatelskich.

Przyrzeczenie zachowania tajemnicy państwowej, podczas ślubowania, składa także policjant, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Straży Granicznej, Służby Więziennej.

¹ DzU nr 140, poz. 938 ze zm.

² DzU nr 155, poz. 1016 ze zm.

Tajemnica państwowa chroniona jest również w licznych przepisach prawa procesowego – art. 179 kpk dotyczy przesłuchania osób zobowiązanych do zachowania tajemnicy państwowej. Dyspozycja zapisana w tym przepisie stanowi względny zakaz dowodowy adresowany zarówno do osoby zobowiązanej do zachowania tajemnicy państwowej, jak i do organu procesowego. Organ procesowy musi bowiem uzyskać, w celu przesłuchania osoby zobowiązanej do zachowania tajemnicy państwowej co do okoliczności, na które rozciąga się ten obowiązek, zwolnienie przez uprawniony organ przełożony.

Organami tymi są kierownicy jednostek organizacyjnych, w których informacje stanowiące tajemnicę państwową są wytwarzane, przetwarzane, przekazywane lub przechowywane, odpowiedzialni za ich ochronę (art. 18, ust. 1 w zw. z art. 4, ust. 1 Ustawy o ochronie informacji niejawnych w zw. z art. 179, § 1 kpk).

Niewątpliwie stosowne kompetencje w omawianej kwestii posiadają służby ochrony państwa (Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne), którym powierzono kontrolę ochrony informacji niejawnych (art. 14, ust. 1, pkt 1 w zw. z art. 49, ust. 1 ustawy).

Generalne upoważnienie do udostępniania informacji niejawnych, stanowiących tajemnicę państwową, określonej osobie lub instytucji powierzono szefom kancelarii: prezydenta RP, Sejmu, Senatu, prezesa Rady Ministrów, prezesa Narodowego Banku Polskiego, ministra właściwego dla określonego działu administracji rządowej, kierownika urzędu centralnego, a w sytuacji ich braku – właściwym służbom ochrony państwa (art. 49, ust. 1 ustawy).

Art. 179, § 3 kpk przewiduje specjalne uprawnienie do zwrócenia się o zwolnienie świadka od obowiązku zachowania tajemnicy państwowej bezpośrednio do naczelnego organu administracji rządowej. Uprawnienie to jest zarezerwowane wyłącznie dla dwóch organów procesowych – sądu i prokuratora.

Należy zauważyć, że względny zakaz dowodowy (art. 179, § 1) dotyczy osoby obowiązanej do zachowania tajemnicy państwowej. Osoba ta może wystąpić w procesie karnym w charakterze świadka, a także biegłego (art. 197, par. 3 kpk), specjalisty (art. 206, § 2 kpk) i tłumacza (art. 204, § 3 kpk).

Kontrowersje dotyczą oskarżonego (podejrzanego). Wielu autorów uważa, że obowiązek zachowania tajemnicy państwowej dotyczy także oskarżonego¹. Inni stoją na stanowisku, że w tym przypadku pierwszeństwo należy przyznać prawu do obrony².

Sąd Najwyższy w wyroku z dnia 11 kwietnia 1983 r.³ wyraził pogląd, że art. 162, § 1 dkpk (obecnie art. 179, § 1 kpk) dotyczy wszystkich osób zobowiązanych do zachowania tajemnicy państwowej, czyli także oskarżonych.

Osoby zwolnione od zachowania tajemnicy państwowej przesłuchuje się na okoliczności, na które rozciąga się ta tajemnica, z wyłączeniem jawności. Podzielając zdanie, że oskarżony, broniąc się, może być przesłuchany na takie okoliczności bez zezwolenia, należy pamiętać, iż sąd wyłącza jawność rozprawy, m.in. ze względu na ważny interes państwa (art. 360, § 1 pkt 3 kpk).

Ustawa z dnia 6 lipca 1995 r. o zmianie kodeksu postępowania karnego⁴ wprowadziła do kpk z 1969 r. nowe regulacje dotyczące zachowania w tajemnicy danych umożliwiających ujawnienie tożsamości świadka.

W kodyfikacji karnej z 1997 r. problematyki tej dotyczą zwłaszcza art. 184 i 393, § 4 kpk dotyczące świadka anonimowego.

W przypadku zagrożenia życia lub zdrowia świadka koronnego lub osoby dla niego najbliższej mogą być oni objęci ochroną osobistą, a także uzyskać pomoc w zakresie zmiany miejsca pobytu lub zatrudnienia, a w szczególnie uzasadnionych wypadkach można wydać im dokumenty umożliwiające używanie innych niż własne danych osobowych, w tym uprawniające do przekroczenia granicy państwowej⁵.

Okoliczności dotyczące ochrony lub pomocy stanowią tajemnicę państwową. Tajemnicą tą objęty jest także przebieg i treść czynności

¹ J. Bafia i inni, *Kodeks postępowania karnego z komentarzem*, Warszawa 1976 r., s. 237, teza 5.

² R. Stefański, J. Bratoszewski i inni, *Kodeks postępowania karnego z komentarzem*, t. I, s. 483, teza 7.

³ IKR 393/82, niepubl.

⁴ DzU nr 89, poz. 444.

⁵ Szczegółowe warunki, zakres i sposób udzielania ochrony i pomocy przewidziane w Ustawie z dnia 25 maja 1997 r. o świadku koronnym (DzU nr 114, poz. 738 i nr 160, poz. 1083) określi Rada Ministrów w drodze rozporządzenia.

związanych z instytucją świadka koronnego do chwili wydania przez sąd postanowienia o dopuszczeniu dowodu z zeznań tegoż świadka.

1.3. Rodzaje tajemnic prawnie chronionych

Tajemnica państwowa i służbowa nie są jedynymi prawnie chronionymi. Sekretów takich, nie zawsze nazwanych wprost, jest bardzo wiele. Związane są z wykonywaniem określonych zawodów, z pracą w niektórych instytucjach lub z pełnieniem pewnej funkcji społecznej. Lista tajemnic chronionych obecnie w Polsce jest bardzo długa.

Tajemnica przedsiębiorstwa – należy rozważać tę tajemnicę na gruncie działalności gospodarczej, z nią właśnie związana jest sama instytucja przedsiębiorcy jako podmiotu prowadzącego działalność określaną mianem przedsiębiorstwa.

Definicja tajemnicy przedsiębiorstwa zawarta jest w Ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji¹. W myśl art. 11, ust. 4 ustawy przez tajemnicę tę rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Z powyższego uregulowania prawnego wynika, że określone informacje mogą stanowić tajemnicę przedsiębiorstwa wówczas, gdy spełnione zostaną następujące przesłanki:

1. Informacje dotyczyć muszą danych technicznych, technologicznych, handlowych lub organizacyjnych, co do których przedsiębiorca podjął działanie w celu zachowania ich poufności; najczęściej dotyczyć to będzie takich informacji, jak np. opatentowane lub nieopatentowane wynalazki, wzory użytkowe lub zdobnicze, plany techniczne, sposoby zbierania informacji, metody kontroli jakości towarów i usług, wyniki prób i badań, bazy danych klientów, organizacja pracy i schematy organizacyjne.

2. Poufny charakter informacji, co oznacza, że tajemnicę przedsiębiorstwa będą stanowić tylko takie informacje, które nie zostały ujawnione poprzez podanie do publicznej wiadomości i nie powinny

¹ DzU nr 47, poz. 211.

być do wiadomości publicznej podane w przyszłości. Należy przyjąć, że ochrona tajemnicy przedsiębiorstwa przestaje obowiązywać wówczas, gdy dana informacja została ujawniona w taki sposób, że każdy zainteresowany może się z nią zapoznać bez zgody jakiegokolwiek podmiotu uprawnionego w tym zakresie.

3. Podjęcie przez przedsiębiorcę działań zmierzających do skutecznego nadania informacjom charakteru poufnego, np. poprzez: zapewnienie odpowiedniego obiegu dokumentów zawierających informacje klasyfikowane, nadanie danym dokumentom klauzuli tajności czy nadanie odpowiednich klauzul na zawierane umowy, porozumienia i inne podobne akty dotyczące współpracy z innymi podmiotami.

Zgodnie z art. 11 ust. 1 ustawy przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża istotnym interesom przedsiębiorcy, jest czynem nieuczciwej konkurencji. Przepis ten ma zastosowanie nie tylko do obecnych pracowników przedsiębiorstwa, lecz także do osoby, która świadczyła pracę na podstawie stosunku pracy lub innego stosunku prawnego przez okres trzech lat od jego ustania, chyba że umowa stanowi inaczej albo ustał stan tajemnicy. Nie jest natomiast nieuczciwą konkurencją nabycie od nieuprawnionego, w dobrej wierze i na podstawie odpłatnej czynności prawnej, informacji stanowiącej tajemnicę przedsiębiorstwa¹.

Tajemnica bankowa – została zdefiniowana w art. 104, ust. 1 Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe². Obejmuje wszystkie wiadomości dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane

¹ Bliżej A. Bień, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, Warszawa 1999, s. 111 i nast.; M. Mozgawa, *Ustawa o zwalczaniu nieuczciwej konkurencji, przestępstwa i wykroczenia*, Rzeczpospolita 1993, nr 127; M. Mozgawa, *Ochrona informacji stanowiących tajemnicę przedsiębiorstwa w świetle Ustawy o zwalczaniu nieuczciwej konkurencji*, Toruń 1994, s. 317 i nast.; S. Sołtyński, *Ustawa o zwalczaniu nieuczciwej konkurencji, komentarz*, Warszawa 1994, s. 101 i nast., P. Bogdalski, *Tajemnica przedsiębiorstwa – zagadnienia konstrukcyjne*, „Monitor Polski” 1997, nr 6.

² DzU nr 140, poz. 939.

z zawarciem umowy z bankiem i jej realizacją (z wyjątkiem wiadomości, bez których ujawnienia nie jest możliwe należyte wykonanie zawartej umowy), a także wiadomości dotyczące osób, które, nie będąc stroną umowy z bankiem, dokonały czynności pozostających w związku z zawarciem takiej umowy, z wyjątkiem przypadków gdy ustawa przewiduje ich ujawnienie.

Z powyższego zapisu wynika, że tajemnicą bankową objęte zostały praktycznie wszystkie czynności bankowe, jak też informacje dotyczące osób fizycznych i prawnych będących stronami umów negocjacyjnych, zawieranych i realizowanych przez bank, a także innych osób wykonujących czynności związane z tymi umowami.

Poprzednio obowiązujące prawo bankowe nie przewidywało sankcji za ujawnienie tajemnicy bankowej. Obecnie obowiązujące przepisy (art. 171, ust. 4) przewidują odpowiedzialność osoby zobowiązanej do podania uprawnionym organom informacji dotyczących banku i klientów banku w zakresie ustalonym w ustawie, która podaje nieprawdziwe lub zataja prawdziwe dane.

Prawo bankowe zatem nie stwarza dla pracowników banku sytuacji klarownej, jeśli chodzi o odpowiedzialność karną za naruszenie tajemnicy bankowej lub nieudostępnienie informacji. Wręcz przeciwnie, zawiera przepisy tzw. stresogenne, powodujące sytuację, że cokolwiek pracownik zrobi, może narazić się na odpowiedzialność w postaci kary pozbawienia wolności do lat 3 lub grzywny do 1 000 000 zł.

Tajemnica giełdy – wynika z przepisów Ustawy z dnia 21 sierpnia 1997 r. – Prawo o publicznym obrocie papierami wartościowymi¹. Występuje w dwóch postaciach – jako tajemnica zawodowa oraz informacja poufna. Zgodnie z art. 4, pkt 18 ustawy przez tajemnicę zawodową rozumie się informacje związane z publicznym obrotem, których ujawnienie mogłoby naruszyć interes uczestników tego obrotu.

Natomiast jak wynika z art. 4, pkt 19 ustawy z 1997 r., informacją poufną są wiadomości dotyczące emitenta lub papieru wartościowego, które nie zostały przekazane do publicznej wiadomości, a które po ujawnieniu mogłyby w istotny sposób wpłynąć na cenę papieru wartościowego.

¹ DzU nr 118, poz. 754 ze zm.

Ustawa dotycząca publicznego obrotu papierami wartościowymi reguluje kwestie odpowiedzialności w przypadku ujawnienia tajemnicy giełdy. Zgodnie z art. 175 tej ustawy: „*Kto, będąc obowiązany do zachowania tajemnicy zawodowej, ujawnia lub wykorzystuje w obrocie papierami wartościowymi informacje stanowiące tajemnicę zawodową, podlega karze pozbawienia wolności do lat 3 i grzywny do 1 000 000 zł*”¹.

Natomiast odpowiedzialność za ujawnienie informacji poufnej ustawodawca opisał w art. 176, ust. 1 Prawa o publicznym obrocie papierami wartościowymi: „*Kto w obrocie papierami wartościowymi ujawnia informację poufną, podlega karze pozbawienia wolności do lat 3 i grzywny do 1 000 000 zł*”. Wyższą karą – pozbawienia wolności od 6 miesięcy do lat 5 i grzywny do 5 000 000 zł – zagrożone jest wykorzystanie informacji poufnej w obrocie papierami wartościowymi². Przepisy art. 175 i 176 ustawy stanowią *lex specialis* w stosunku do odpowiedzialności przewidzianej odpowiednio w art. 266 i 267 kk.

Tajemnica statystyczna – określona w przepisach Ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej³ obejmuje dane indywidualne i osobowe. Podlegają szczególnej ochronie, ich wykorzystywanie może mieć wyłącznie odniesienie do opracowań, zestawień i analiz statystycznych oraz do tworzenia przez służby statystyki operatu do prowadzonych przez nie badań statystycznych. Wykorzystywanie danych do innych celów jest zabronione.

Osoby wykonujące prace związane z przygotowaniem, przeprowadzeniem i opracowaniem wyników spisu są obowiązane do bezwzględnego przestrzegania tajemnicy statystycznej. Osoby te

¹ Artykuł 175 Prawa o publicznym obrocie papierami wartościowymi jest ujęty w sposób niezręczny, a przy tym mało klarowny. Przepis ten powinien być rozbity na dwa paragrafy – pierwszy powinien penalizować ujawnienie tajemnicy zawodowej przez osobę obowiązaną do jej zachowania, drugi – wykorzystanie w obrocie papierami wartościowymi przez taką osobę informacji stanowiących tajemnicę zawodową. Obecne ujęcie bowiem dopuszcza interpretację, że ujawnienie tajemnicy zawodowej przez osobę zobowiązaną do jej zachowania karalne jest jedynie wtedy, gdy następuje w obrocie papierami wartościowymi, a bezkarne, gdy ma miejsce poza obrotem.

² Bliżej M. Bojarski, W. Radecki, *Przewodnik po pozakodeksowym prawie karnym*, Wrocław 1998, s. 499.

³ DzU nr 88, poz. 439.

mogą być dopuszczone do wykonywania takich prac po przeszkoleniu i pouczeniu o istocie tajemnicy statystycznej oraz po złożeniu pismennego przyrzeczenia (zgodnego z art. 12 ustawy).

Naruszenie tajemnicy statystycznej stanowi przestępstwo – zgodnie z art. 54 ustawy: „*Kto narusza tajemnicę statystyczną, podlega karze pozbawienia wolności do lat 3*”. Powiązany z omawianą problematyką jest też art. 55, który ma brzmienie następujące: „*Kto w celu osiągnięcia korzyści majątkowej lub osobistej wykorzystuje dane statystyczne, z którymi zapoznał się w związku z wykonywaniem pracy lub czynności na zlecenie prowadzącego badania statystyczne statystyki publicznej, podlega karze pozbawienia wolności do lat 5*”¹.

Tajemnica dziennikarska – regulowana przepisami ustawy z dnia 26 stycznia 1984 r.²

Prawo prasowe stanowi, że dziennikarz ma obowiązek zachowania w tajemnicy:

1) danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych,

2) wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Powyższy obowiązek dotyczy również innych osób zatrudnionych w redakcjach, wydawnictwach prasowych i innych prasowych jednostkach organizacyjnych.

Zgodnie z art. 16 Prawa prasowego, dziennikarz jest zwolniony z obowiązku zachowania tajemnicy zawodowej wówczas, gdy infor-

¹ Bliżej M. Bojarski, W. Radecki, *Przewodnik...*, wyd. cyt., s. 620 i nast. Zagadnienie tajemnicy statystycznej zostało uregulowane także w Ustawie z dnia 2 grudnia 1999 r. o narodowym spisie powszechnym ludności i mieszkań (DzU nr 1 z 2000 r., poz. 1). W myśl art. 9 tej ustawy wszystkie zbierane i gromadzone w spisie dane osobowe i dane indywidualne są poufne i podlegają szczególnej ochronie tajemnicą statystyczną. Wydane na podstawie art. 31 ustawy Rozporządzenie prezesa Rady Ministrów z dnia 20 września 1999 r. dotyczy określania wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 1999 (DzU nr 78, poz. 879).

² DzU nr 5, poz. 24 ze zm.

macja, materiał prasowy, list do redakcji lub inny materiał o tym charakterze dotyczą przestępstwa określonego w art. 240 kk albo autor lub osoba przekazująca taki materiał wyłącznie do wiadomości dziennikarza wyrazi zgodę na ujawnienie jej nazwiska lub całego materiału¹.

Zagadnienie tajemnicy zawodowej dziennikarza reguluje także kodeks postępowania karnego z 1997 r. Art. 180, § 2 stanowi, że osoby zobowiązane do zachowania tajemnicy dziennikarskiej mogą być przesłuchane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu².

Z uregulowaną przepisami prawa prasowego tajemnicą dziennikarską pozostaje w pewnej analogii postanowienie art. 84 Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych³. Z treści tego przepisu wynika, że twórca, a wydawca lub producent na żądanie twórcy mają obowiązek zachowania w tajemnicy źródeł informacji wykorzystanych w utworze oraz nieujawniania związanych z tym dokumentów. Ujawnienie tajemnicy jest dozwolone, w tej sytuacji, za zgodą osoby, która powierzyła tajemnicę, lub na podstawie postanowienia właściwego sądu.

¹ Odpowiedzialności z art. 240 kk podlega zaniechanie obowiązku zawiadomienia o przestępstwach w tym przepisie wymienionych, tj.: ludobójstwa, zamachu na niepodległość Rzeczypospolitej Polskiej, zdrady dyplomatycznej, szpiegostwa, zamachu na życie prezydenta RP, zamachu na jednostkę sił zbrojnych RP, zabójstwa, sprowadzenia katastrofy, terrorystycznego przejęcia statku, wzięcia zakładnika. Wiadomość o przestępstwie musi być wiarygodna, czyli zasługująca na zaufanie, chociażby sprawca nie miał ostatecznej pewności co do jej prawdziwości. Odpowiedzialności z art. 240 kk podlega nie tylko zaniechanie zawiadomienia o przestępstwie dokonanym, ale także o usiłowaniu tego przestępstwa, jak również o jego przygotowaniu. J. Wojciechowski, *Kodeks karny – komentarz, orzecznictwo*, Warszawa 1998, s. 429; zob. też S. Hoc, *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Opole 2002.

² B. Michalski słusznie zwraca uwagę na niejasności mogące w przyszłości powodować kontrowersje w praktyce, z których najważniejszą jest wynikająca z art. 180 kpk owa możliwość zwolnienia dziennikarza z zachowania tajemnicy zawodowej, wtedy gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dowodzona okoliczność nie może być ustalona na podstawie innego dowodu. B. Michalski, *Podstawowe problemy prawa prasowego*, Warszawa 1998, s. 60.

³ DzU nr 24, poz. 83 ze zm.

Obok obowiązku zachowania tajemnicy zawodowej przez dziennikarza z przepisów wprost wynika obowiązek udzielania informacji. Zgodnie z art. 4, ust. 2 ustawy: „*Odmowa udzielania informacji może nastąpić jedynie ze względu na ochronę tajemnicy państwowej i służbowej oraz innej tajemnicy chronionej ustawą*”¹. W Ustawie z dnia 28 września 1991 r. o kontroli skarbowej² znajduje się następujący przepis: „*Na żądanie dyrektora urzędu kontroli skarbowej wydawca i redaktor dziennika lub czasopisma są obowiązani do udzielania posiadanych informacji o nazwach i adresach przedsiębiorców lub nazwiskach i adresach osób fizycznych zamieszczających odpłatne ogłoszenia i reklamy w sprawach działalności gospodarczej*” (art. 35). Podobny zapis znajduje się w art. 27, ust. 3 Ustawy z dnia 6 czerwca 1997 r. o Inspekcji Celnej³.

Z problemami dotyczącymi tajemnicy zawodowej dziennikarza związane są też inne, niż omówione, przepisy prawa prasowego, także rozporządzenia wykonawcze, inne ustawy oraz liczne dokumenty międzynarodowe⁴.

Tajemnica lekarska – uregulowana jest w Ustawie z dnia 5 grudnia 1996 r. o zawodzie lekarza⁵. W oparciu o przepisy ustawy lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu. Przepis nie ma zastosowania, jeśli:

- tak stanowią przepisy;
- badanie lekarskie zostało przeprowadzone na żądanie uprawnionych, na podstawie odrębnych ustaw, organów i instytucji (wówczas lekarz jest zobowiązany poinformować o stanie zdrowia pacjenta wyłącznie te organy i instytucje);
- zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub inny sposób;
- pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach jej ujawnienia;

¹ Więcej J. Sobczak, *Ustawa – Prawo prasowe. Komentarz*, Warszawa 1999, s. 54 i nast.

² DzU nr 100, poz. 442 ze zm.

³ DzU nr 71, poz. 449.

⁴ Więcej J. Sobczak, *Prawo środków masowej informacji. Prasa, radio, telewizja*, Toruń 1999.

⁵ DzU nr 28, poz. 152 ze zm.

– zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innemu lekarzowi lub uprawnionym osobom uczestniczącym w udzielaniu tych świadczeń;

- jest to niezbędne do praktycznej nauki zawodów medycznych;
- jest to niezbędne dla celów naukowych.

W powyższych przypadkach ujawnienie tajemnicy lekarskiej może nastąpić wyłącznie w niezbędnym zakresie. Obowiązek zachowania tajemnicy nie kończy się wraz ze śmiercią pacjenta, którego bezpośrednio dotyczy.

Przepis kodeksu postępowania karnego w art. 180, § 2 dopuszcza możliwość przesłuchania co do faktów objętych tajemnicą lekarską osoby zobowiązane do zachowania tej tajemnicy, ale tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Decyzję w tym zakresie podejmuje sąd.

Kwestie związane z tajemnicą lekarską zostały uregulowane także w innych ustawach¹ oraz aktach prawnych niższego rzędu².

Specyficzną tajemnicą lekarską jest sekret lekarza psychiatry i personelu z nim związanego. Problemy tej tajemnicy reguluje Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego³. Zgodnie z art. 50, pkt 1 osoby wykonujące czynności, wynikające z tej ustawy,

¹ Ustawa o służbie medycyny pracy (DzU z 1997 r. nr 96, poz. 593) w art. 11, ust. 3 opisuje tajemnicę danych dokumentacji medycznej; Ustawa o pobieraniu i przeszczepianiu tkanek i narządów (DzU z 1995 r. nr 138, poz. 682) w art. 12 przewiduje tajemnicę transplantacyjną, chroniącą dane osobowe dawcy i biorcy przeszczepu; Ustawa o publicznej służbie krwi (DzU z 1997 r. nr 106, poz. 68) w art. 13 definiuje tajemnicę dawcy krwi; ustawa o izbach lekarskich (DzU z 1989 r., nr 30, poz. 158 ze zm.) w art. 15, pkt 1 przewiduje obowiązek zachowania tajemnicy lekarskiej oraz sankcje w przypadku jej ujawnienia.

² Rozporządzenie ministra zdrowia i opieki społecznej w sprawie orzekania o czasowej niezdolności do pracy (DzU z 1996 r., nr 63, poz. 302); Rozporządzenie ministra pracy i polityki socjalnej w sprawie szczegółowych zasad i trybu wystawiania zaświadczeń lekarskich, wzoru zaświadczenia lekarskiego i zaświadczenia lekarskiego wydanego w wyniku kontroli lekarza orzecznika Zakładu Ubezpieczeń Społecznych (DzU z 1999 r., nr 65, poz. 741). Rozporządzenia zawierają wzory zaświadczeń lekarskich poufnych i poufnych zaświadczeń kontroli. Rodzaje dokumentacji medycznej oraz sposoby jej prowadzenia i udostępniania przez zakłady opieki zdrowotnej utworzone przez przedsiębiorstwo państwowe „Polskie Koleje Państwowe” zawiera Rozporządzenie ministra transportu i gospodarki morskiej (DzU z 1999 r., nr 75, poz. 851).

³ DzU nr 111, poz. 535 ze zm.

są obowiązane do zachowania w tajemnicy wszystkiego, o czym powezmą wiadomość w związku z wykonywaniem tych czynności, stosownie do odrębnych przepisów, a nadto z zachowaniem przepisów ustawy. W myśl pkt. 2, art. 50 osoby te są zwolnione od obowiązku zachowania tajemnicy w stosunku do:

- lekarza sprawującego opiekę nad osobą z zaburzeniami psychicznymi;
- właściwych organów administracji rządowej lub samorządowej co do okoliczności, których ujawnienie jest niezbędne do wykonywania zadań z zakresu opieki społecznej;
- osób współuczestniczących w wykonywaniu czynności w ramach pomocy społecznej w zakresie, w jakim jest to niezbędne;
- służb ochrony państwa i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych.

W ustawie o ochronie zdrowia psychicznego znajduje się przepis – art. 52, który wprowadza zakaz przesłuchiwania osób zobowiązanych do zachowania tajemnicy w charakterze świadków na okoliczność przyznania się osoby z zaburzeniami psychicznymi do popełnienia czynu zabronionego pod groźbą kary. Zakaz ten stosuje się odpowiednio do lekarzy wykonujących czynności biegłego.

Omawiana ustawa rozszerzyła zatem zawarty w art. 178 kpk katalog osób, których nie można przesłuchiwać jako świadków, obejmując nim (oprócz wymienionego w tym przepisie obrońcy i duchownego) także osobę wykonującą czynności przewidziane w tej ustawie w zakresie faktu przyznania się osoby z zaburzeniami psychicznymi do popełnienia czynu zabronionego pod groźbą kary¹. Zakaz dotyczy zakresu, o którym mowa w art. 52 Ustawy o ochronie zdrowia psychicznego. W pozostałym zakresie ma zastosowanie art. 180, § 2 kpk.

Tajemnica adwokacka i radcowska – tajemnica zawodowa adwokata została uregulowana w Ustawie z dnia 26 maja 1982 r. – Pra-

¹ Blżej S. Dąbrowski, L. Kubicki, *Ustawa o ochronie zdrowia psychicznego. Przegląd ważniejszych zagadnień*, Instytut Psychiatrii i Neurologii, Warszawa 1994, s. 53–56; S. Dąbrowski, J. Pietrykowski, *Ustawa o ochronie zdrowia psychicznego – komentarz*, Warszawa 1997.

wo o Adwokaturze¹, natomiast sekret radcy prawnego opisuje Ustawa z dnia 6 lipca 1982 r. o radcach prawnych².

W odniesieniu do adwokatów zasadnicze znaczenie mają przepisy art. 6, ust. 1–3, w myśl których adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę. Do innych przypadków tajemnicy adwokackiej odnosi się art. 180, § 2 kpk, który stanowi: *„Osoby obowiązane do zachowania tajemnicy adwokackiej (...) mogą być przesłuchane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. O przesłuchaniu lub zezwoleniu na przesłuchanie decyduje sąd”*. Istnieje więc wyraźna niespójność między cytowanym przepisem a ustawą – Prawo o Adwokaturze³.

Obowiązek zachowania tajemnicy zawodowej wpisany jest w tekst roty ślubowania.

Z kolei w odniesieniu do radców prawnych obowiązują przepisy art. 3, ust. 1–5 wspomnianej wyżej ustawy przewidujące, że radca prawny jest obowiązany zachować w tajemnicy wszystko, czego

¹ DzU nr 16, poz. 124 ze zm.

² DzU nr 19, poz. 145 ze zm.

³ Sprawa stosunku przepisów kodeksu postępowania karnego z 1969 r. do obowiązku tajemnicy adwokackiej na tle dawnego tekstu ustawy o adwokaturze była w literaturze prawnokarnej od dawna przedmiotem zainteresowania. Sąd Najwyższy w uchwale z dnia 16 czerwca 1994 r. przyjął, że adwokata nie wolno przesłuchiwać jako świadka co do faktów, o których dowiedział się jako obrońca, udzielając porady prawnej lub prowadząc sprawę. W innych wypadkach adwokat może odmówić zeznań co do okoliczności, na które rozciąga się obowiązek zachowania tajemnicy zawodowej, chyba że sąd lub prokurator zwolni go od tego obowiązku na podstawie art. 163 kpk. Zwolnienie jednak może nastąpić tylko wtedy, gdy ujawnienie okoliczności objętych tajemnicą w drodze przesłuchania adwokata jako świadka jest nieodzowne dla zapewnienia prawidłowego wyrokowania w sprawie. Sąd Najwyższy zatem uznał, iż przepis art. 163 kpk stanowi lex specialis w stosunku do normującego w sposób generalny instytucję tajemnicy adwokackiej przepisu art. 6 prawa o Adwokaturze – tekst uchwały wraz z uzasadnieniem został opublikowany w Palestrze 1994, nr 7–8, s. 194–208; OSNKW 1994, nr 7–8, poz. 41.

dowiedział się w związku z udzieleniem pomocy prawnej. Obowiązek ten nie może być ograniczony w czasie, a radca prawny nie może być z niego zwolniony w odniesieniu do faktów, o których dowiedział się, udzielając pomocy prawnej lub prowadząc sprawę.

Dla każdego klienta adwokata czy radcy prawnego ważne jest przekonanie, że reprezentujący go przed sądem lub udzielający mu innego rodzaju pomocy prawnej adwokat lub radca prawny dochowa tajemnicy. Obowiązek zachowania sekretu wpisany jest w zasady etyki obydwu zawodów. Zarówno adwokat, jak i radca prawny mają obowiązek zachowania w tajemnicy wszystkich uzyskanych informacji, w szczególności treści dokumentów, notatek, akt, materiałów utrwalonych metodą elektroniczną czy innymi środkami technicznymi. Obejmuje on nie tylko zakaz ujawniania informacji uzyskanych przy okazji czy w związku z wykonywaniem zawodu, ale również skorzystania z nich w interesie własnym lub osób trzecich. Obowiązek ten również nie jest ograniczony w czasie.

Ustawy – Prawo o Adwokaturze oraz o radcach prawnych nie uznają ujawnienia tajemnicy zawodowej ani za odrębne przestępstwo, ani za wykroczenie. Należy wobec tego przyjąć, że w przypadku naruszenia przepisów ustawy – adwokat oraz radca prawny będą odpowiadać karnie na podstawie przepisów kodeksu karnego. Ujawnienie przez nich tajemnicy może pociągać za sobą także odpowiedzialność dyscyplinarną.

Warto dodać, że w omawianej kwestii ustawodawstwa całego niemal świata zawierają podobne rozwiązania prawne. W Stanach Zjednoczonych Ameryki prawnicy są zobowiązani do zachowania w tajemnicy poufnych informacji swoich klientów. W postępowaniu dowodowym wykluczona jest możliwość zadawania pytań klientowi i jego adwokatowi przez stronę przeciwną odnośnie tego, co dany klient i jego obrońca przekazali sobie w zaufaniu.

Współczesne orzeczenia sądowe i reguły procesowe uznają również przywilej nieujawniania treści dokumentów sporządzonych przez prawnika przygotowującego obronę swojego klienta. Chronione są sekrety samego klienta przed wykorzystywaniem ich przez prawnika w celach komercyjnych. Istnieją również specjalne regulacje zawarte w różnych kodeksach postępowania zawodowego prawników amerykańskich nakładające na nich obowiązek nieujawniania informacji o kliencie.

Tajemnica sędziego i prokuratora – obowiązek zachowania tajemnicy sędziego określa art. 85 Ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych¹. Zgodnie z powołanym przepisem sędzia jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na swoje stanowisko poza jawną rozprawą sądową.

Obowiązek trwa także po ustaniu stosunku służbowego, natomiast ustaje w chwili, kiedy sędzia składa zeznania jako świadek przed sądem, chyba że ujawnienie tajemnicy zagraża dobru państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W tych wypadkach od obowiązku zachowania tajemnicy może zwolnić sędziego minister sprawiedliwości.

Natomiast obowiązek tajemnicy ciążyący na prokuratorze określa Ustawa z dnia 20 czerwca 1985 r. o prokuraturze². Zgodnie z art. 48 tej ustawy prokurator jest obowiązany zachować w tajemnicy okoliczności sprawy, o których w postępowaniu przygotowawczym, a także poza jawną rozprawą sądową, powziął wiadomość ze względu na swoje stanowisko prokuratora.

Obowiązek trwa także po ustaniu stosunku służbowego, ustaje wówczas, gdy prokurator składa zeznania jako świadek w postępowaniu przygotowawczym lub przed sądem, chyba że ujawnienie tajemnicy zagraża dobru państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W takich wypadkach od obowiązku zachowania tajemnicy może zwolnić prokuratora prokurator generalny.

Tajemnica notarialna i komornika sądowego – tajemnicy notarialnej dotyczy art. 18 Ustawy z dnia 14 lutego 1991 r. – Prawo o notariacie³. Przepis ten stanowi: „*Notariusz jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności notarialne.*”

Obowiązek trwa także po odwołaniu notariusza, natomiast ustaje, gdy notariusz składa zeznania jako świadek przed sądem, chyba że ujawnienie tajemnicy zagraża dobru państwa albo ważnemu intere-

¹ DzU nr 98, poz. 1070.

² DzU z 1994 r., nr 19, poz. 70.

³ DzU nr 22, poz. 91 ze zm.

sowi prywatnemu. W tych wypadkach od obowiązku zachowania tajemnicy może zwolnić notariusza minister sprawiedliwości”¹.

Natomiast z Ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji² wynika obowiązek komornika do zachowania w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności.

Obowiązek trwa także po odwołaniu komornika, ustaje w chwili, gdy komornik składa zeznanie przed sądem w charakterze świadka.

Dochowanie tajemnicy państwowej i zawodowej zapisane jest w rocie ślubowania, którą komornik przy powołaniu składa wobec ministra sprawiedliwości.

Do zasad etyki zawodowej z kolei nawiązuje art. 16 ustawy. Zgodnie z tym przepisem komornik jest zobowiązany postępować zgodnie z przepisami prawa, złożonym ślubowaniem i zasadami etyki zawodowej, jest również zobowiązany do podnoszenia kwalifikacji zawodowych.

Zarówno Ustawa o komornikach sądowych i egzekucji, jak i Ustawa o prokuraturze nie zawierają przepisów karnych. W związku z tym ujawnienie tajemnicy karane będzie zgodnie z przepisami kodeksu karnego.

Tajemnica danych osobowych – uregulowana jest przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych³. Kwestie ochrony danych osobowych reguluje wiele dokumentów międzynarodowych⁴.

¹ Problem tajemnicy zawodowej notariusza w niedawnym czasie wzbudził duże zainteresowanie w związku z postulatami zmiany przepisu art. 18 ustawy poprzez pozbawienie władzy wykonawczej możliwości zwalniania z obowiązku tajemnicy. Rozważa się też problem pominięcia notariusza w grupie zawodów uprzywilejowanych (adwokat, lekarz, dziennikarz) w art. 180 kpk. Problem tajemnicy zawodowej notariusza był przedmiotem konferencji naukowej „Notariat a tajemnica zawodowa”.

² DzU nr 133, poz. 882 ze zm.

³ DzU nr 133, poz. 883 ze zm.

⁴ Konwencja Rady Europy z dnia 28 stycznia 1981 r. (Nr 108) o ochronie jednostki w związku z automatycznym przetwarzaniem danych osobowych; Rekomendacje Rady Europy: R(81)1 z dnia 23 stycznia 1981 r., R(83)10 z dnia 23 października 1983 r., R(85)20 z dnia 25 października 1985 r., R(86)1 z dnia 23 stycznia 1986 r., R(87)15 z dnia 17 września 1987 r., R(89)2 z dnia 18 stycznia 1989 r., R(90)19 z dnia 13 września 1990 r., R(91)10 z dnia 9 września 1991 r. Dyrektywa 95/46 Wspólnoty Europejskiej z dnia 24 października 1995 r. dotycząca ochrony osób fizycznych w procesie przetwarzania danych osobowych i ich swobodnego przepływu; Dyrektywa Wspólnoty Europejskiej przyjęta przez Parlament Europejski i Radę Unii Europejskiej w dniu 15 grudnia 1997 r. dotycząca ochrony danych w telekomunikacji, a także liczne konwencje dotyczące współpracy sądowej międzynarodowej i regionalnej.

Za dane osobowe w rozumieniu ustawy uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie jej tożsamości. Obowiązek zachowania w tajemnicy tych danych ciąży na osobach zatrudnionych przy ich przetwarzaniu oraz osobach mających dostęp do danych osobowych. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Naruszenie postanowień ustawy w zakresie ochrony danych osobowych jest zagrożone sankcją karną. Przepisy karne zawarte w ustawie dotyczą różnych występków. W szczególności należy wskazać na art. 49–52 ustawy, w myśl których:

– kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2; jeżeli czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3 (art. 49);

– kto, administrując zbiorem danych, przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do roku (art. 50);

– kto, administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych, udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2; jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 51);

– kto, administrując danymi, narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 52).

Tajemnica skarbowa – uregulowana została w Ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa¹; o tajemnicy skarbowej jest

¹ DzU nr 137, poz. 926 ze zm.

też mowa w Ustawie z dnia 28 września 1991 r. o kontroli skarbowej¹.

W art. 34, w ust. 1 tej ustawy określone zostało pojęcie tajemnicy skarbowej. Zgodnie z tym przepisem tajemnicę skarbową stanowią informacje gromadzone i przetwarzane w ramach kontroli skarbowej. Obowiązkiem zachowania tej tajemnicy objęci są pracownicy urzędów kontroli skarbowej, generalny inspektor kontroli skarbowej oraz pracownicy Ministerstwa Finansów, a także osoby, które na podstawie odrębnych przepisów odbywają praktykę zawodową w urzędach kontroli skarbowej.

W świetle art. 293, § 1 ustawy tajemnicę skarbową stanowią dane zawarte w deklaracjach oraz innych dokumentach składanych przez podatników, płatników i inkasentów.

Zakres jej obejmuje także informacje podatkowe przekazywane organom podatkowym przez podmioty nienależące do grupy podatników, płatników czy inkasentów, dane zawarte w aktach dokumentujących czynności sprawdzające, kontroli podatkowej oraz aktach spraw karnych skarbowych, dane zawarte w informacjach uzyskanych z banków oraz innych źródeł.

Obowiązkiem przestrzegania tajemnicy skarbowej są objęci pracownicy urzędów i izb skarbowych, wójtowie lub burmistrzowie (prezydenci miast) oraz pracownicy samorządowych służb finansowych, członkowie samorządowych kolegiów odwoławczych, a także pracownicy biur tych kolegiów, wreszcie minister finansów i pracownicy Ministerstwa Finansów oraz osoby, które na podstawie odrębnych przepisów odbywają praktykę zawodową w Ministerstwie Finansów lub w organach podatkowych.

Obowiązek zachowania tajemnicy skarbowej wprost wynika z przyrzeczenia, które każda z wymienionych wyżej osób składa na piśmie. Zachowanie tej tajemnicy obowiązuje również po ustaniu zatrudnienia lub zakończeniu praktyki zawodowej.

Tajemnica skarbowa nie tylko ogranicza możliwości wykorzystywania danych zawartych w aktach objętych tą tajemnicą, lecz także uprawnia do udostępniania takich danych wyłącznie podmioty ściśle określone przez przepisy prawne. Artykuł 82, § 3 Ordynacji podatkowej zobowiązuje banki oraz inne instytucje finansowe, na pisemne

¹ DzU nr 100, poz. 442 ze zm.

żądanie ministra finansów oraz jego upoważnionego przedstawiciela, do udzielania informacji w sytuacji wystąpienia władz podatkowych państw obcych w zakresie i na zasadach wynikających z umów o unikaniu podwójnego opodatkowania.

Z kolei na żądanie urzędu skarbowego banki są zobowiązane do sporządzania i przekazywania informacji o zdarzeniach stanowiących podstawę do skorzystania przez podatnika z ulg podatkowych, jeżeli zostały wykazane w deklaracji przez niego złożonej (art. 295, § 2), a także do sporządzania i przekazywania informacji dotyczących numerów rachunków bankowych osób prawnych, jednostek organizacyjnych niemających osobowości prawnej, osób fizycznych prowadzących działalność gospodarczą lub wykonujących wolny zawód (art. 82, § 2).

Szczególnym rodzajem informacji podatkowych objętych tajemnicą skarbową są dane o wysokości zaległości podatkowych podatnika. Dane takie organy podatkowe mogą udostępniać tylko na żądanie jednostek organizacyjnych uprawnionych do udzielania kredytów (pożyczek), kontrahentów podatników prowadzących działalność gospodarczą, małżonka podatnika, wspólnika spółki cywilnej jawnej oraz komandytowej. Zaświadczenie takie może być wydane tylko wówczas, gdy podatnik wyrazi zgodę.

Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa zawiera przepisy karne chroniące tajemnicę skarbową. Art. 306 dotyczy odpowiedzialności za ujawnienie tej tajemnicy przez osobę zobowiązaną do jej zachowania. Sprawcy grozi kara pozbawienia wolności do lat 5 w przypadku, gdy jest to jednocześnie tajemnica bankowa – kara pozbawienia wolności jest orzekana w wymiarze od 6 miesięcy do lat 5. W sytuacji gdy działanie sprawcy było nieumyślne, kara pozbawienia wolności zostaje zawężona do 2 lat.

Przepis art. 306 Ordynacji podatkowej stanowi *lex specialis* w stosunku do art. 266 kk¹.

Tajemnica głosowania – podstawy prawne sięgają konstytucji RP, która gwarantuje tajność głosowania w wyborach do Sejmu, Senatu, w wyborach prezydenta RP (art. 96, ust. 2, art. 97, ust. 2, art. 127, ust. 1), a także tajność w wyborach organów stanowiących jednostki

¹ Trafne określenie przyjęli M. Bojarski, W. Radecki, *Przewodnik po pozakodeksowym prawie karnym*, Wrocław 1998, s. 515–516.

samorządu terytorialnego (art. 169, ust. 2). Wcześniej prawa te zapisane były w art. 3 ust. 1 i art. 29 ust. 2 Ustawy z dnia 17 października 1992 r., tzw. „Małej konstytucji”.

Regulacja ta znajduje rozwinięcie w ustawach zwanych ordynacjami wyborczymi. Ustawa z dnia 28 maja 1993 r. – Ordynacja wyborcza do Sejmu RP¹ stanowi m.in., że wybory posłów na Sejm Rzeczypospolitej Polskiej są przeprowadzane w głosowaniu tajnym. Inne przepisy tej ustawy zawierają konkretne postanowienia gwarantujące realizację w praktyce głosowania, zachowanie jego tajności (np. art. 39, ust. 1 wprost instruuje, że po otrzymaniu karty do głosowania wyborca udaje się do miejsca zapewniającego tajność głosowania znajdującego się w lokalu wyborczym, ust. 3 tego artykułu stanowi, że wyborca wrzuca do urny kartę do głosowania w taki sposób, aby strona zadrukowana nie była widoczna).

Ustawa z dnia 10 maja 1991 r. – Ordynacja wyborcza do Senatu RP² w art. 1, ust. 1 stanowi, że wybory do Senatu odbywają się przy odpowiednim zastosowaniu przepisów Ordynacji wyborczej do Sejmu. Oznacza to, że przyjęte rozwiązanie prawne gwarantujące tajność głosowania przy wyborze posłów są identyczne jak przy głosowaniu na senatorów.

Kolejna Ustawa z dnia 27 września 1990 r. o wyborze prezydenta Rzeczypospolitej Polskiej³ w art. 6 stwierdza, że wybory odbywają się w tajnym głosowaniu; w lokalu wyborczym muszą znajdować się pomieszczenia za osłoną zapewniającą tajność głosowania. Kartę do głosowania wyborca wrzuca do opieczętowanej urny wyborczej.

Problematyka wyborów do organów stanowiących jednostki samorządu terytorialnego uregulowana została w Ustawie z dnia 16 lipca 1998 r. w – Ordynacji wyborczej do rad gmin, rad powiatów i sejmików województw⁴. W myśl art. 2, ust. 1 ustawy wybory odbywają się w głosowaniu tajnym. Przed rozpoczęciem głosowania obwodowa komisja wyborcza sprawdza, czy urna jest pusta, następnie zamyka ją i opieczętowuje. Wyborca, po otrzymaniu karty, udaje się

¹ DzU nr 45, poz. 205 ze zm.

² DzU z 1994 r., nr 54, poz. 398 ze zm.

³ DzU nr 67, poz. 398 ze zm.

⁴ DzU nr 95, poz. 602 ze zm.

do miejsca zapewniającego tajność głosowania znajdującego się w lokalu wyborczym¹.

Tajemnica korespondencji – wyjaśnienie znaczenia „tajemnicy korespondencji” można znaleźć w art. 267 kk, w myśl którego obejmuje ona informacje przeznaczone dla innej osoby, znajdujące się w zamkniętym piśmie lub zabezpieczone, np. elektronicznie, magnetycznie lub w inny szczególnie sposób. Pojęcie „tajemnica korespondencji” obejmuje zatem nie tylko fizyczną ochronę informacji, które stanowią same w sobie tajemnicę, ale również okoliczności, których dana osoba lub instytucja nie ma obowiązku ujawniać osobom trzecim.

Ochronę korespondencji gwarantowały przepisy konstytucyjne z 1952 r. stanowiące w art. 87, ust. 2, że ustawa ochrania nienaruszalność mieszkań i tajemnicę korespondencji. Konstytucja RP uchwalona 2 kwietnia 1997 r. w art. 49 zapewnia wolność i ochronę tajemnicy komunikowania się.

Konstytucyjną zasadę rozwija m.in. Ustawa z dnia 30 lipca 1997 r. o państwowym przedsiębiorstwie użyteczności publicznej „Poczta Polska”, która w art. 7 stanowi, że przedsiębiorstwo zapewnia w obrocie pocztowym ochronę tajemnicy korespondencji oraz poufność informacji o świadczonej usłudze.

Materialną ochronę tajemnicy korespondencji zawierał art. 172 kk z 1969 r. Przewidywał on odpowiedzialność osoby, która bez uprawnienia otwiera zamknięte pismo (dla niej nieprzeznaczone) albo ukrywa lub niszczy cudzą korespondencję, zanim adresat się z nią zapoznał, lub też przyłącza się do przewodu służącego do podawania wiadomości, albo podstępnie uzyskuje nieprzeznaczoną dla niej wiadomość nadaną przy użyciu środków telekomunikacji, a także taką

¹ Należy podkreślić, że tajność głosowania w wyborach do parlamentu gwarantowana jest także przez prawo międzynarodowe, np. stanowi o tym przepis art. 3 Protokołu nr 1 do Konwencji o ochronie praw człowieka i podstawowych wolności, przyjętego w Paryżu w dniu 20 marca 1952 r. – DzU z 1995 r., nr 36, poz. 175. Tajność głosowania do organów stanowiących jednostki samorządu terytorialnego znajduje natomiast stosowne umocowanie w Europejskiej Karcie Samorządu Terytorialnego, sporządzonej w Strasburgu w dniu 15 października 1985 r., ratyfikowanej przez Polskę w roku 1993 (DzU z 1994 r., nr 124, poz. 607).

samą odpowiedzialność osoby, która w ten sposób uzyskaną informację przekazuje dalej.

Wzmoczoną ochronę przed bezprawnym uzyskaniem informacji, w tym także informacji zawartych w korespondencji, zawierają przepisy art. 267 i 268 obecnie obowiązującego kodeksu karnego¹ – zgodnie z § 1, art. 267 – „*Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*”. Tej samej sankcji podlega ten, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym (§ 2) oraz ten, kto ujawnia innej osobie informację uzyskaną w wyżej opisany sposób (§ 3).

Natomiast art. 268 kk przewiduje odpowiedzialność karną osoby, która, nie będąc do tego uprawnioną, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią.

W związku z tajemnicą korespondencji trudno pominąć przepisy kodeksu postępowania karnego. Regulacje zawarte w kpk z 1969 r. w sposób istotny ograniczały omawiany rodzaj tajemnicy. Zgodnie z przepisami (art. 198) sąd lub prokurator mógł, po wszczęciu postępowania, wydać postanowienie o udostępnieniu korespondencji, przesyłek albo o utrwaleniu treści rozmów telefonicznych, jeśli miało to znaczenie dla toczącego się postępowania. Z kolei urzędy pocztowe, celne, telekomunikacyjne były zobowiązane do udzielania wspomnianych informacji².

W polskim prawie katalog tajemnic chronionych nie jest zamknięty. Poza wyżej opisanymi istnieje jeszcze wiele innych, jak choćby tajemnica spowiedzi, geologiczna, akt stanu cywilnego, wynalazcza, organizacji społecznych, postępowania karnego, celnego. Rozwój życia społecznego, przemiany w sferze gospodarczej, a także

¹ Ustawa z dnia 6 czerwca 1997 r. (DzU nr 88, poz. 553 i nr 128, poz. 840).

² Szczegółową regulację w tym zakresie zawierają przepisy 237–242 kpk z 1997 r. Opisują problematykę kontroli i utrwalania treści rozmów telefonicznych, a także przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne.

wzrost świadomości obywateli sprawiają, że wciąż pojawiają się nowe informacje klasyfikowane stanowiące różne tajemnice, coraz więcej jest też osób odpowiedzialnych za ich ochronę.

Rozdział 2

ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH W POLSCE

Organizacja ochrony informacji niejawnych może być charakteryzowana jako ta sfera aktywności organów państwa, która jest związana najściślej z potrzebą zapewnienia jego prawidłowego funkcjonowania. Całokształt przedsięwzięć w tym zakresie można charakteryzować w aspekcie przedmiotowym, obejmującym rodzaje i charakter informacji niejawnych oraz podmiotowym, odnoszącym się do sfery instytucjonalnej. W tym drugim ujęciu problem daje się charakteryzować w ujęciu systemowym, a zatem w kategoriach analizy poszczególnych elementów struktury (organów, instytucji, podmiotów gospodarczych) i wzajemnych między nimi powiązań, których charakter określają normy wskazane w Ustawie o ochronie informacji niejawnych i przepisach wykonawczych. W tym ujęciu można zatem mówić o systemie ochrony informacji niejawnych.

2.1. Zakres przedmiotowy i podmiotowy

Mówienie o zakresie przedmiotowym i podmiotowym ochrony informacji niejawnych wymaga ustosunkowania się do dwóch zasadniczych kwestii. Po pierwsze należy wskazać te spośród informacji publicznych¹, które mają charakter niejawny. Po drugie należy określić podmioty obowiązane na podstawie przepisów prawa do zapewnienia ochrony informacji niejawnych. W Polsce obie te kwestie kompleksowo normowane są przepisami Ustawy z 22.01.1999 r. o ochronie informacji niejawnych. W art. 1, ust. 1 ustawy nazwano rodzajowo informacje podlegające ochronie przed ich nieuprawnio-

¹ W świetle Ustawy z 6.09.2001 r. o dostępie do informacji publicznej (DzU z 2001 r., nr 117, poz. 1198) informacją publiczną jest każda informacja o sprawach publicznych, która podlega udostępnieniu na zasadach przewidzianych przepisami prawa (art. 1, ust. 1).

nym ujawnieniem. W świetle tego przepisu ochronie podlegają wszystkie informacje niejawne stanowiące tajemnicę państwową oraz tajemnicę służbową.

Definicje obu tajemnic zawiera z kolei art. 2 ustawy. W myśl jego postanowień **tajemnicą państwową jest informacja niejawna określona w wykazie rodzajów informacji niejawnych, stanowiącym załącznik nr 1 do ustawy, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów RP, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę¹.**

Wykaz składa się z dwóch części, w których wskazano rodzaje informacji niejawnych stanowiących tajemnicę państwową. W pierwszej części znajdują się rodzaje informacji oznaczonych klauzulami *ściśle tajne*, zaś w drugiej te oznaczone klauzulami *tajne*. Wykaz nie jest zamkniętym katalogiem informacji niejawnych stanowiących tajemnicę państwową, lecz ma raczej charakter poglądowy. Spełnia rolę przewodnika, dzięki któremu można dokonywać klasyfikowania informacji niejawnych, czyli nadawania określonym informacjom lub materiałom właściwych klauzuli tajności. Zgodnie z wykazem tajemnicę państwową stanowią informacje dotyczące m.in.:

- zagrożeń zewnętrznych bezpieczeństwa państwa o charakterze militarnym, (plany i prognozowanie obronne oraz wynikające z nich decyzje i zadania),
- szczegółowej struktury sił zbrojnych,
- organizacji, form i metod pracy operacyjnej organów, służb i instytucji państwowych uprawnionych do wykonywania czynności operacyjno-rozpoznawczych,
- szczegółowych kierunków pracy operacyjnej i zainteresowań służb ochrony państwa.

Tajemnicę służbową art. 2 definiuje jako informację niejawną, niebędącą tajemnicą państwową, uzyskaną w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której

¹ W myśl art. 115, § 5 kodeksu karnego (DZU z 1997 r., nr 88, poz. 553 ze zm.) szkoda znacznej wartości obejmuje wartość przekraczającą 200-krotną wysokość najniższego wynagrodzenia. Natomiast w myśl § 6 szkoda wielkich rozmiarów obejmuje wartość przekraczającą 1000-krotną wysokość najniższego miesięcznego wynagrodzenia.

nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Ustawa, inaczej niż w przypadku tajemnicy państwowej, nie zawiera żadnego katalogu rodzajów informacji niejawnych stanowiących tajemnicę służbową. Zaliczenie określonej informacji do tajemnicy służbowej wymaga udzielenia odpowiedzi na pytanie: w jakie dobra lub interes prawnie chroniony godziłoby ujawnienie klasyfikowanej informacji.

Wskazanie podmiotów obligatoryjnie zajmujących się ochroną informacji niejawnych ma miejsce w ust. 2, art. 1 ustawy z 22.01.1999 r. W ten sposób ustawa określa zakres podmiotowy obowiązywania jej postanowień oraz ochrony informacji niejawnych. W świetle tego przepisu podmiotami, które mają obowiązek zapewnić ochronę informacji niejawnych, stosując przepisy ustawy, są:

- 1) organy władzy publicznej (Sejm, Senat, prezydent RP, organy administracji rządowej, organy jednostek samorządu terytorialnego, sądy i trybunały, organy kontroli państwowej i ochrony prawa),
- 2) siły zbrojne RP oraz jednostki organizacyjne sił zbrojnych,
- 3) Narodowy Bank Polski i banki państwowe,
- 4) państwowe osoby prawne i państwowe jednostki organizacyjne,
- 5) podmioty realizujące zadania publiczne (przedsiębiorcy, jednostki naukowe lub badawczo-rozwojowe) ubiegające się lub wykonujące umowy związane z dostępem do informacji niejawnych.

Z przedstawionego powyżej katalogu podmiotów stosujących przepisy o ochronie informacji niejawnych wynika jasno, że zadanie zapewnienia ochrony informacji niejawnych spoczywa przede wszystkim na aparacie państwowym, wojsku oraz państwowych jednostkach organizacyjnych. Przyjęcie takich rozwiązań stanowi prostą konsekwencję znaczenia, jakie dla bezpieczeństwa państwa posiada informacja uzyskiwana i przetwarzana przez instytucje publiczne.

2.2. System ochrony informacji niejawnych

System ochrony informacji niejawnych należy postrzegać wieloaspektowo. Z jednej strony jest on bowiem zespołem określonych instytucji funkcjonalnie ze sobą powiązanych, tworzących model postępowania z informacjami niejawnymi w sposób zapewniający ich

ochronę przed nieuprawnionym ujawnieniem. Z drugiej zaś strony system ochrony informacji niejawnych stanowi istotną część instytucjonalnego systemu bezpieczeństwa państwa¹.

System ochrony informacji niejawnych w pierwszym znaczeniu powinno postrzegać się jako ogół unormowań charakteryzujących metody, które pozwalają klasyfikować informacje niejawne oraz środki służące ich zabezpieczeniu przed nieuprawnionym ujawnieniem. W drugim ujęciu system ochrony informacji niejawnych wymaga zaś wskazania poszczególnych jego elementów (podmiotów), charakteru ich wzajemnych powiązań i funkcji. Pierwszy zabieg jest podejściem do omawianej problematyki w sposób funkcjonalny, drugi natomiast stanowi próbę rozpatrywania zagadnienia w płaszczyźnie organizacyjnej. Pierwszy zostanie omówiony w tym podrozdziale, drugi w kolejnym.

W aspekcie funkcjonalnym system ochrony informacji niejawnych można traktować dwustopniowo. Pozwalają na to przepisy ustawy z 22.01.1999 r., które oddzielnie regulują kwestię zasad i trybu klasyfikowania informacji niejawnych oraz środków fizycznej ochrony takich informacji.

Klasyfikowanie informacji niejawnych polega na pewnej systematyzacji tej informacji, dokonanej zgodnie z procedurą opisaną w postanowieniach ustawy. Punktem wyjścia podejmowanych w tym zakresie działań są zawsze – przedstawione w rozdziale II – ustawowe definicje tajemnicy państwowej i tajemnicy służbowej. Stanowi to jednak pierwszy krok w procesie klasyfikowania, ponieważ w ramach obu kategorii tajemnic ustawa rozróżnia informacje niejawne odpowiednio: *ściśle tajne* i *tajne* (tajemnica państwowa) oraz *poufne* i *zastrzeżone* (tajemnica służbowa). Dokonany przepisami art. 23 ustawy podział informacji stanowiących tajemnicę państwową na *ściśle tajne* i *tajne* oraz tajemnicę służbową na *poufne* i *zastrzeżone* należy traktować jako ostateczny cel klasyfikowania informacji niejawnych.

Stanowi o tym art. 19, ust. 1 ustawy, w świetle którego klasyfikowanie informacji niejawnych oznacza przyznanie tej informacji, w sposób wyraźny, przewidzianej w ustawie jednej z klauzul tajności:

¹ Zob. *Bezpieczeństwo i porządek publiczny*, wprowadzenie R. Zakrzewski, Warszawa 1997, s. XXVIII.

ściśle tajne, tajne, poufne, zastrzeżone. Użyty w ustawie termin „przyznanie” klauzuli należy przy tym interpretować szerzej niż dosłowne jego znaczenie, gdyż zakres pojęciowy słowa „przyznanie” obejmuje takie czynności, jak: nadanie, obniżenie lub zniesienie klauzuli tajności.

Informacje niejawne stanowiące tajemnicę państwową oznacza się klauzulą *ściśle tajne*, jeżeli:

ich nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych RP albo zagrażać nieodwracalnymi lub wielkimi stratami dla interesów obronności, bezpieczeństwa państwa i obywateli lub innych istotnych interesów państwa, albo narazić te interesy na szkodę wielkich rozmiarów;

klauzulą *tajne*, jeżeli:

ich nieuprawnione ujawnienie mogłoby spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę.

Informacje niejawne stanowiące tajemnicę służbową oznacza się klauzulą *poufne* w przypadku, kiedy:

ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli;

klauzulą *zastrzeżone*, jeśli:

ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

Przyznanie informacji niejawnej określonej klauzuli tajności zależy zatem od dobra lub interesu, który ma podlegać ochronie. Wiedza dotycząca potencjalnych, ale także konkretnych zagrożeń wymierzonych w wartości chronione klauzulami tajności, pozwala trafnie sklasyfikować daną informację. Świadomość występowania oraz prognoza zaistnienia danego zagrożenia to warunek wstępny prawidłowego klasyfikowania informacji niejawnych.

Klasyfikowanie informacji niejawnych ujmowane w kategoriach określonego działania – postępowania w zakresie przyznawania klauzul tajności – musi odbywać się zgodnie pewną procedurą. Procedurę, czyli pewien wzór postępowania, opisuje ustawa w rozdziale czwar-

tym, w którym wskazuje się podmioty uprawnione do klasyfikowania informacji niejawnych, odpowiedzialne za przyznawanie klauzul tajności oraz okresy przechowywania informacji niejawnych oznaczonych poszczególnymi klauzulami.

Zgodnie z art. 21, ust. 1 i 2 klauzule tajności przyznaje (nadaje, obniża i znosi) osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Uprawnienie to przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych stwierdzonego odpowiednim poświadczeniem bezpieczeństwa. Osoba uprawniona, która przyznała klauzulę tajności, ponosi odpowiedzialność za swoje działanie i bez jej zgody albo jej przełożonego klauzula nie może zostać obniżona lub zniesiona (art. 21, ust. 3). Przełożonym uprawnionym do zmiany (zniesienia lub obniżenia) klauzuli jest każdy przełożony osoby nadającej klauzulę, a nie tylko przełożony bezpośredni¹.

Uprawnienia osoby do klasyfikowania informacji niejawnych oraz określania okresu, przez jaki informacja niejawna podlega ochronie, przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji dotyczącej stanowiska lub funkcji tej osoby, na jej następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na właściwą służbę ochrony państwa (art. 25, ust. 5).

Zawyżanie lub zaniżanie klauzul tajności jest niedopuszczalne. Zasada ta – zawarta w ust. 4, art. 21 – adresowana jest zarówno do osób przyznających klauzule tajności, jak i odbiorców dokumentu lub materiału, których treści zostały oznaczone klauzulami tajności. Tym samym zarówno na jednych, jak i drugich nakłada określone, choć nieco odmienne obowiązki. Osoby uprawnione do nadawania klauzul muszą starannie oceniać klasyfikowaną informację, uwzględniając skutki jej ewentualnego nieuprawnionego ujawnienia. Z kolei adresaci sklasyfikowanych już informacji powinni reagować na oznaczenie danej treści nieadekwatną klauzulą.

Jak stanowi art. 19, ust. 2, klasyfikowanie informacji niejawnych zawartych w dokumencie polega na oznaczeniu tego dokumentu odpowiednią klauzulą tajności. Informacjom niejawnym, materiałom,

¹ Zob. P. Szkudlarek, *Glosa do wyroku SN z 30.05.2000 r.*, IV CKN 1042/00, Orzecznictwo Sądów Polskich 2001/6/89.

dokumentom lub ich zbiorom przyznaje się klauzulę tajności co najmniej równą najwyższej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze. Dopuszczalne jest jednak przyznawanie różnych klauzul tajności częściom dokumentu (rozdziałom, załącznikom, aneksom) lub poszczególnym dokumentom w zbiorze dokumentów, pod warunkiem wyraźnego ich oznaczenia i wskazania klauzuli tajności po odłączeniu dokumentu lub jego części.

Szczegółowe zasady i tryb nadawania klauzul tajności na dokumentach i materiałach¹ określa Rozporządzenie ministra spraw wewnętrznych i administracji oraz ministra obrony narodowej w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach (DzU z 1999 r., nr 18, poz. 167).

Prawidłowe nadawanie klauzul tajności jest ważne dla dalszego postępowania z już sklasyfikowaną informacją niejawną. Ustawa w tym względzie przewiduje określone warunki, w jakich informacje niejawne mogą być przechowywane, udostępniane oraz okresy czasu, na jakie informacje niejawne podlegają ochronie. W zależności od przyznanej klauzuli – zgodnie z przepisami ustawy – postępowanie z informacjami niejawnymi poddane jest nieco różnym rygorom.

Art. 20 wskazuje przy tym na trzy takie główne zasady postępowania z informacjami niejawnymi. Po pierwsze informacje niejawne mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli tajności. Po drugie informacje takie muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieupraw-

¹ Jak stanowi art. 2, pkt. 5 i 6 w rozumieniu ustawy:

– **dokumentem** – jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych,

– **materialem** – jest dokument, jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia.

nione ujawnienie. Po trzecie informacje niejawne muszą być chronione, odpowiednio do przyznanej klauzuli tajności, przy zastosowaniu właściwych środków ochrony fizycznej.

Okresy ochrony informacji niejawnych również są różne dla poszczególnych klauzul tajności. Informacje niejawne stanowiące tajemnicę państwową podlegają ochronie przez okres 50 lat od daty ich wytworzenia. Informacje niejawne stanowiące tajemnicę służbową podlegają ochronie przez okres:

- 5 lat – oznaczone klauzulą *poufne*,
- 2 lata – oznaczone klauzulą *zastrzeżone*.

W przypadku informacji stanowiących tajemnicę służbową osoba upoważniona do klasyfikowania informacji niejawnych może określić krótszy okres ochrony. Ponadto, po dokonaniu przeglądu materiałów zawierających informacje stanowiące tajemnicę służbową, osoba uprawniona może przedłużać okres ochrony tych informacji na kolejne okresy nie dłuższe niż:

- 5 lat (dla oznaczonych klauzulą *poufne*),
- 2 lata (dla oznaczonych klauzulą *zastrzeżone*),

w sumie nie dłużej jednak, niż na okres do 50 lat od daty ich wytworzenia.

Z uwagi na specyfikę pewnych działań niektórych organów państwowych oraz ich znaczenie dla zapewnienia bezpieczeństwa państwa, jak i ze względu na pewne zobowiązania międzynarodowe państwa określone informacje niejawne podlegają ochronie bezterminowo. W świetle art. 25, ust. 2 chronione bez względu na upływ czasu pozostają:

- dane identyfikujące funkcjonariuszy i żołnierzy służb ochrony państwa wykonujących czynności operacyjno-rozpoznawcze,
- dane identyfikujące osoby, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych organom, służbom i instytucjom państwowym uprawnionym do ich wykonywania na podstawie ustawy,
- informacje niejawne uzyskane od innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

Z wyjątkiem informacji chronionych bezterminowo Rada Ministrów może określić – w drodze rozporządzenia – które spośród informacji niejawnych oznaczonych klauzulą *tajne* przestały stanowić tajemnicę państwową, jeżeli od ich powstania upłynęło 20 lat.

2.3. Rozwiązania instytucjonalne

Instytucjonalizacja jakiejkolwiek działalności podejmowanej w każdej sferze oznacza nade wszystko jej organizację. Nie jest też inaczej w przypadku systemu ochrony informacji niejawnych. Organizacja takiego systemu, jak każdego innego, wymaga ustanowienia kompetentnych organów państwowych, które będą zdolne realizować zadania z obszaru ochrony informacji niejawnych. Ustawą z 22.01.1999 r. zadanie z zakresu budowania i kontroli systemu ochrony informacji niejawnych postawiono przed dwoma polskimi służbami specjalnymi: Agencją Bezpieczeństwa Wewnętrznego¹ oraz Wojskowymi Służbami Informacyjnymi.

W art. 2, pkt. 3 ustawy obie te formacje nazwano służbami ochrony państwa. Natomiast w świetle art. 15 szef Agencji Bezpieczeństwa Wewnętrznego i szef Wojskowych Służb Informacyjnych w stosunkach międzynarodowych pełnią funkcję krajowej władzy bezpieczeństwa.

ABW oraz WSI jako służby ochrony państwa mają przeciwdziałać naruszeniom tajemnicy państwowej i służbowej, w szczególności w drodze prowadzonych postępowań sprawdzających oraz kontroli przestrzegania przepisów o ochronie informacji niejawnych. Niekiedy, w literaturze przedmiotu mówi się o funkcji ochronno-kontrolnej, którą wykonują służby ochrony państwa². Rozwiązania prawne³, na podstawie których funkcjonują obie służby, pozwalają z kolei twierdzić, że rozpoznawanie zagrożeń powodujących nieuprawnione ujawnianie informacji niejawnych stanowi jeden z zasadniczych fragmentów działalności ABW i WSI. Wzmacnia też to przekonanie fakt powołania w obu służbach specjalnych pionów funkcjonalnych, wyłącznie realizujących zadania z obszaru ochrony informacji niejawnych.

¹ Funkcję cywilnej służby ochrony państwa do 29.06.2002 r. (do czasu wejścia w życie Ustawy z 24.05.2002 r. o ABW oraz AW) pełnił Urząd Ochrony Państwa (DzU z 1999 r., nr 51, poz. 526 ze zm.).

² Zob. S. Zalewski, *Służby specjalne w państwie demokratycznym*, AON, Warszawa 2002, s. 75.

³ Chodzi o Ustawę z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Ustawę z 9.07.2003 r. o Wojskowych Służbach Informacyjnych (DzU z 2003 r., nr 139, poz. 1326).

Właściwość rzeczową ABW i WSI w zakresie ochrony informacji niejawnych, czyli katalog zadań tych służb, określa art. 14, ust. 1 ustawy. Stanowi on, że służby ochrony państwa właściwe są w sprawach:

- kontroli ochrony informacji niejawnych oraz kontroli przestrzegania przepisów wydanych w tym zakresie,
- realizacji zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych,
- prowadzenia postępowania sprawdzającego według zasad określonych w ustawie,
- ochrony informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi,
- szkolenia i doradztwa w zakresie ochrony informacji niejawnych,
- wykonywania innych zadań, w zakresie ochrony informacji niejawnych, określonych odrębnymi przepisami.

W celu realizacji ustawowych zadań służby ochrony państwa współpracują z instytucjami i organami administracji rządowej oraz dokonują kontroli stanu zabezpieczenia informacji niejawnych w podmiotach stosujących przepisy o ochronie informacji niejawnych. Współpraca ta przybiera różne postacie, ale w szczególności polega na udostępnianiu przez instytucje państwowe służbom ochrony państwa wszelkich informacji niezbędnych dla prowadzenia poszerzonych i specjalnych postępowań sprawdzających. Współdziałanie organów i jednostek organizacyjnych obrazuje wykres (zob. Aneks, wykres 1).

Służby ochrony państwa, w zakresie koniecznym do wykonywania swoich zadań w celu ochrony informacji niejawnych mogą także korzystać z informacji uzyskanych przez Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy służby celnej i kontroli skarbowej, a także zwracać się do tych służb i organów o udzielenie niezbędnej pomocy przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających (art. 14, ust. 2).

Obowiązek współdziałania z służbami ochrony państwa ciąży również na kierownictwie podmiotów obligatoryjnie stosujących przepisy o ochronie informacji niejawnych. W świetle art. 14, ust. 3 kierownicy takich podmiotów są obowiązani udostępniać funkcjonariuszom albo żołnierzom służb ochrony państwa pozostające w ich dyspozycji informacje i dokumenty niezbędne dla stwierdzenia, czy

osoba objęta postępowaniem sprawdzającym daje rękojmię zachowania tajemnicy.

Funkcjonariuszom i żołnierzom służb ochrony państwa dokonującym kontroli w podmiotach stosujących przepisy o ochronie informacji niejawnych przysługują odpowiednio uprawnienia pracowników Najwyższej Izby Kontroli. W takim też zakresie do czynności kontrolnych wykonywanych przez funkcjonariuszy (żołnierzy) mają odpowiednie zastosowanie przepisy Ustawy z dnia 23.12.1994 r. o Najwyższej Izbie Kontroli (DzU z 1995 r., nr 13, poz. 59 ze zm.).

Niezależnie od tych unormowań, w zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych stanowiących tajemnicę państwową, upoważnieni pisemnie funkcjonariusze lub żołnierze służb ochrony państwa mają prawo do:

- swobodnego wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są wytwarzane, przetwarzane, przechowywane lub przekazywane,
- wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej,
- żądania udostępnienia do kontroli sieci lub systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania tych informacji,
- przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji,
- żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień oraz posiadanych przez nich informacji dotyczących działalności wywiadowczej albo terrorystycznej skierowanej przeciwko Rzeczypospolitej Polskiej, jej siłom zbrojnym, przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym, w odniesieniu do prowadzonej produkcji albo usług stanowiących tajemnicę państwową ze względu na bezpieczeństwo lub obronność państwa, a także na potrzeby sił zbrojnych,
- zasięgania, w związku z przeprowadzaną kontrolą, informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z wytwarzaniem, przechowywaniem, przetwarzaniem, przekazywaniem lub ochroną informacji niejawnych stanowiących

tajemnicę państwową, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek,

- korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych,

- uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Zgodnie ze standardami państwa demokratycznego, działalność ABW i WSI podlega kontroli cywilnej zarówno ze strony organów władzy wykonawczej jak i władzy ustawodawczej. Wyrazem uprawnień władzy ustawodawczej w tym zakresie jest art. 3 Ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w myśl którego działalność szefa ABW i szefa WSI podlega kontroli Sejmu. Kontrola organów władzy wykonawczej stanowi natomiast element nadzoru sprawowanego nad ABW przez prezesa Rady Ministrów, a nad WSI przez ministra obrony narodowej. Istotną rolę w tym nadzorze, choć pośrednią, odgrywa działające przy Radzie Ministrów Kolegium do spraw Służb Specjalnych¹.

Kolegium działa jako organ opiniodawczo-doradczy w sprawach programowania, nadzorowania i koordynowania działalności służb specjalnych: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu i Wojskowych Służb Informacyjnych. Do zadań kolegium należy także formułowanie ocen oraz wyrażanie opinii w sprawach współdziałania służb specjalnych z innymi organami i służbami funkcjonującymi w obszarze bezpieczeństwa państwa (m.in. Policji, Straży Granicznej, Żandarmerii Wojskowej). Od momentu wejścia w życie ustawy z 24.05.2002 r. – czyli od 29. czerwca 2002 r. – kolegium jest również właściwe w sprawach ochrony informacji niejawnych, którymi to sprawami do tego czasu zajmował się Komitet Ochrony Informacji Niejawnych.

¹ Kolegium działa na podstawie Ustawy o ABW oraz AW oraz Rozporządzenia Rady Ministrów z 2.07.2002 r. w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium ds. Służb Specjalnych oraz zakresu czynności sekretarza tego kolegium (DzU z 2002 r., nr 103, poz. 929).

W skład kolegium wchodzi: przewodniczący – prezes Rady Ministrów, sekretarz kolegium, minister spraw wewnętrznych i administracji, minister spraw zagranicznych, minister obrony narodowej, minister finansów, szef Biura Bezpieczeństwa Narodowego. W posiedzeniach kolegium uczestniczą również: szef ABW, szef AW, szef WSI oraz przewodniczący Sejmowej Komisji ds. Służb Specjalnych. Do udziału w pracach kolegium swojego przedstawiciela może delegować także prezydent RP.

W zakresie ochrony informacji niejawnych do zadań kolegium należy formułowanie ocen lub wyrażanie opinii w sprawach:

- zagrożeń o zasięgu ogólnokrajowym w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową,
- sposobów postępowania w sytuacji zagrożenia o zasięgu ogólnokrajowym, powstałej wskutek ujawnienia informacji niejawnych stanowiących tajemnicę państwową oraz dokonywanie oceny skutków ujawnienia takich informacji,
- projektów aktów normatywnych i innych dokumentów rządowych dotyczących ochrony informacji niejawnych,
- innych spraw zleczanych przez Radę Ministrów lub prezesa Rady Ministrów oraz wnoszonych przez ministrów w zakresie realizacji zadań związanych z ochroną informacji niejawnych.

2.4. Organizacja systemu ochrony informacji niejawnych w podmiotach stosujących przepisy o ochronie informacji niejawnych

Drugą, oprócz służb ochrony państwa, znaczącą dla systemu ochrony informacji niejawnych jest instytucja pełnomocnika do spraw ochrony informacji niejawnych. Pełnomocnik powoływany jest w każdym podmiocie stosującym przepisy o ochronie informacji niejawnych. Aktu tego dokonuje kierownik podmiotu jako osoba odpowiedzialna za ochronę informacji niejawnych w jednostce organizacyjnej, w której takie informacje są wytwarzane, przetwarzane, przekazywane lub przechowywane (art. 18, ust. 1).

Zgodnie z wymogami ustawy pełnomocnikiem może być osoba, która:

- posiada obywatelstwo polskie,
- posiada co najmniej średnie wykształcenie,
- posiada odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa po przeprowadzeniu postępowania sprawdzającego,
- odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

Pełnomocnik do spraw ochrony informacji niejawnych podlega bezpośrednio kierownikowi. Zakres zadań pełnomocnika wyznacza ust. 2, art.18, który stanowi, że pełnomocnik odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Pełnomocnik ochrony, w zakresie realizacji swoich zadań, w razie wprowadzenia stanu nadzwyczajnego (tzn. stanu wyjątkowego, wojennego lub klęski żywiołowej), ma prawo żądać od komórek organizacyjnych w swojej jednostce organizacyjnej udzielenia natychmiastowej pomocy. W zakresie realizacji swoich zadań pełnomocnik ochrony współpracuje z właściwymi jednostkami i komórkami organizacyjnymi służb ochrony państwa. Pełnomocnik ochrony na bieżąco informuje kierownika jednostki organizacyjnej o przebiegu tej współpracy. Pełnomocnik ochrony opracowuje ponadto plan postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego. Pełnomocnik ochrony podejmuje również działania zmierzające do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych, zawiadamiając o tym kierownika jednostki organizacyjnej, a w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą *poufne* lub wyższą, również właściwą służbę ochrony państwa.

Pełnomocnik ochrony nade wszystko kieruje wyodrębnioną wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych, nazywaną ***pionem ochrony***. W świetle art. 18, ust. 4 do zadań pionu ochrony należy:

- zapewnienie ochrony informacji niejawnych,
- ochrona systemów i sieci teleinformatycznych,
- zapewnienie ochrony fizycznej jednostki organizacyjnej,
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
- okresowa kontrola ewidencji, materiałów i obiegu dokumentów,

- opracowywanie planu ochrony jednostki organizacyjnej i nadzorowanie jego realizacji,
- szkolenie pracowników w zakresie ochrony informacji niejawnych.

Pracownikiem pionu ochrony może być osoba, która:

- posiada obywatelstwo polskie,
- posiada odpowiednie poświadczenie bezpieczeństwa wydane po przeprowadzeniu postępowania sprawdzającego,
- odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

Postanowienia ustawy z 22.01.1999 r. stawiają także pewne wymagania co do właściwego postępowania z informacjami i materiałami niejawnymi w jednostkach organizacyjnych. Jak stanowi art. 50, ust. 1 w podmiotach, w których są wytwarzane i przechowywane informacje *poufne* lub stanowiące tajemnicę państwową, obligatoryjnie tworzy się **kancelarie tajne**¹. Utworzenie w takim przypadku w danej jednostce organizacyjnej kancelarii tajnej – w myśl § 2, ust. 1, Rozporządzenia Rady Ministrów z 9.02.1999 r. w sprawie organizacji kancelarii tajnych (DzU z 1999 r., nr 18, poz. 156 ze zm.) – stanowi zadanie kierownika podmiotu mającego obowiązek stosowania przepisów o ochronie informacji niejawnych.

Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie takich dokumentów uprawnionym osobom (art. 50, ust. 2). W świetle § 2 rozporządzenia RM kancelarią kieruje kierownik kancelarii, wyznaczany przez kierownika jednostki organizacyjnej na wniosek pełnomocnika do spraw ochrony informacji niejawnych. Do obowiązków kierownika kancelarii należy w szczególności:

- bezpośredni nadzór nad obiegiem dokumentów niejawnych w jednostce organizacyjnej,
- udostępnianie lub wydawanie dokumentów niejawnych osobom posiadającym stosowne poświadczenie bezpieczeństwa,
- egzekwowanie zwrotu dokumentów zawierających informacje niejawne,

¹ Zob. *Instrukcja ochrony informacji niejawnych* (opracowanie Iwona Ruszczyk), Gdańsk 1999, s. 10.

- kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii tajnej oraz jednostce organizacyjnej,
- wykonywanie poleceń pełnomocnika ochrony,
- prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom.

Kancelaria tajna powinna być zorganizowana w wyodrębnionym pomieszczeniu, zabezpieczonym zgodnie z przepisami o środkach ochrony fizycznej informacji niejawnych i być obsługiwana przez pracowników pionu ochrony. W uzasadnionych przypadkach w jednostce organizacyjnej mogą zostać utworzone oddziały kancelarii, prace których koordynuje kierownik kancelarii.

Zgodnie z § 5 rozporządzenia RM kancelaria powinna być zlokalizowana w strefie bezpieczeństwa¹ na piętrze, z wyłączeniem poddaszy. Kancelaria powinna też być oddzielona od innych pomieszczeń trwałymi, niepalnymi, o dużej wytrzymałości ścianami i stropami. Ponadto kancelaria tajna powinna spełniać szereg innych wymogów określonych bliżej przepisami rozporządzenia RM. Wymienić należy najważniejsze z nich, takie jak:

- odpowiednia jakość i grubość drzwi kancelarii (powinny być metalowe lub obite blachą stalową o grubości 2 mm, z zabezpieczeniem antywłamaniowym, oraz wyposażone w dwa zamki o skomplikowanym mechanizmie),
- zabezpieczenie okien (okna kancelarii powinny być zabezpieczone stalowymi kratami oraz przed obserwacją kancelarii z zewnątrz),
- wyposażenie kancelarii (powinny stanowić szafy pancerne z zamkami o skomplikowanym mechanizmie),
- system nadzoru (w kancelarii można zainstalować system nadzoru wizyjnego wyłącznie w celu kontroli dostępu do pomieszczeń),

¹ W świetle art. 57, pkt 1 ustawy z 22.01.1999 r. *strefy bezpieczeństwa* to wydzielone części obiektu, które poddane są szczególnej kontroli wejść i wyjść oraz kontroli przebywania. Zgodnie z pkt. 2, art. 57 wokół stref bezpieczeństwa wydziela się – co do zasady – *strefy administracyjne* służące do kontroli osób lub pojazdów.

– pomieszczenia specjalne (w kancelarii można wydzielić pomieszczenie, w którym osoby posiadające poświadczenie bezpieczeństwa mogą zapoznawać się z dokumentami na miejscu).

Kancelaria tajna jest zorganizowana odrębnie dla dokumentów o określonej klauzuli tajności, z tym że dopuszczalne jest zorganizowanie jednej kancelarii, pod warunkiem że dokumenty o różnych klauzulach są fizycznie od siebie oddzielone i obsługiwane przez osobę posiadającą poświadczenie bezpieczeństwa odpowiednie do najwyższej klauzuli wytwarzanych, przetwarzanych, przekazywanych lub przechowywanych w kancelarii dokumentów. W kancelarii nie mogą natomiast być przechowywane dokumenty niezawierające informacji niejawnych, chyba że wchodzi one w skład zbioru dokumentów (§ 6 ust. 1 rozporządzenia RM).

Organizacja pracy kancelarii tajnej musi zapewniać możliwość ustalenia w każdych okolicznościach, gdzie znajduje się dokument klasyfikowany pozostający w dyspozycji jednostki organizacyjnej.

Kierownik jednostki organizacyjnej może wyrazić zgodę na przechowywanie dokumentów zawierających informacje niejawne poza kancelarią, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do ich klauzul tajności, na czas niezbędny do realizacji zadań związanych z dostępem do tych informacji. Przedmioty lub urządzenia o dużych wymiarach, stanowiące bądź zawierające informacje tajne, przechowuje się w oddzielnych pomieszczeniach spełniających wymogi kancelarii.

Dokumenty oznaczone klauzulami: *ściśle tajne* i *tajne* mogą być wydawane poza kancelarię tajną wyłącznie w przypadku, gdy odbiorca zapewnia warunki ochrony takich dokumentów przed nieuprawnionym ujawnieniem. W razie wątpliwości co do zapewnienia warunków ochrony, dokument może być udostępniony wyłącznie w kancelarii tajnej. Kancelaria tajna może udostępniać dokumenty osobie posiadającej stosowne poświadczenia bezpieczeństwa, upoważniające ją do dostępu do informacji oznaczonych daną klauzulą.

Jak stanowi § 4 ust. 1 w przypadku zmiany na stanowisku kierownika kancelarii sporządza się, w dwóch egzemplarzach, protokół zdawczo-odbiorczy w obecności pełnomocnika ochrony, kierownika zdającego obowiązki oraz osoby przejmującej obowiązki kierownika. Protokół przechowywany jest w kancelarii, drugi egzemplarz zaś – u pełnomocnika ochrony. Protokół zdawczo-odbiorczy sporządza się

również w przypadku likwidacji kancelarii. Jeśli jest to sytuacja czasowej nieobecności kierownika kancelarii jego obowiązki przejmuje upoważniony pracownik kancelarii, a w razie braku stałego pracownika w kancelarii, kancelarię przejmuje protokolarnie, posiadający stosowne poświadczenie bezpieczeństwa, inny pracownik wyznaczony przez pełnomocnika ochrony.

2.5. Obieg informacji niejawnych

Podstawowym aktem prawnym normującym kwestię obiegu informacji niejawnych jest – przywoływane w poprzednim podrozdziale – Rozporządzenie Rady Ministrów z 9.02.1999 r. w sprawie organizacji kancelarii tajnych. Znamiennej rolę w tym zakresie odgrywa też Rozporządzenie ministrów spraw wewnętrznych i administracji oraz obrony narodowej z 26.02.1999 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów (DzU z 1999 r., nr 18, poz. 168).

Nieco inaczej sprawa wygląda jeżeli chodzi o dokumenty stanowiące tajemnice służbową oznaczone klauzulą *zastrzeżone*. Do obiegu dokumentów oznaczonych taką klauzulą stosuje się przede wszystkim przepisy właściwych instrukcji kancelaryjnych. Instrukcje kancelaryjne będą wydawać kierownicy poszczególnych podmiotów stosujących przepisy o ochronie informacji niejawnych.

Obieg informacji niejawnych w ramach struktury jednego podmiotu, jak i między podmiotami, odbywa się zawsze za pośrednictwem kancelarii tajnej. Kancelaria, w celu kontroli tego obiegu, prowadzi odpowiednie rejestry dokumentów. W świetle § 8 rozporządzenia RM w skład tej ewidencji wchodzi:

- dziennik korespondencji dokumentów oznaczonych klauzulą *ściśle tajne*,
- dziennik korespondencji dokumentów oznaczonych klauzulą *tajne*,
- dziennik korespondencji dokumentów oznaczonych klauzulą *poufne*,
- karty zapoznania się z dokumentami oznaczonymi klauzulami *ściśle tajne i tajne*,
- książkę doręczeń przesyłek miejscowych,

- dziennik ewidencji wykonanych dokumentów oznaczonych klauzulą *ściśle tajne*, *tajne* i *poufne*,
- wykaz przesyłek nadanych,
- rejestr teczek dokumentów niejawnych, dzienników i książek ewidencyjnych.

Oprócz kontroli obiegu dokonywanej przy pomocy powyższych rejestrów i dzienników, obieg informacji niejawnych powinien odbywać się zgodnie z określonymi zasadami. O najważniejszych z nich mówi się w postanowieniach rozporządzenia z 9.02.1999 r. Warto wskazać, że § 9 tego aktu stanowi, że przesyłki lub dokumenty zawierające informacje niejawne stanowiące tajemnicę państwową przyjmuje się za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej. Niezależnie od tego pracownik kancelarii tajnej przy przyjmowaniu przesyłki ma obowiązek sprawdzić:

- prawidłowość adresu,
- całość pieczęci i opakowania,
- zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
- zgodność numerów na przesyłce z numerami w wykazie przesyłek nadanych lub w książce doręczeń.

Jeżeli w trakcie tych czynności stwierdzone zostanie uszkodzenie przesyłki lub ślady jej otwierania, pracownik kancelarii wraz z doręczającym sporządza protokół uszkodzenia przesyłki. Protokół przekazuje się nadawcy, kierownikowi jednostki organizacyjnej i przewoźnikowi – jeżeli pośredniczył w obiegu przesyłek. Jednocześnie kierownik kancelarii odmawia przyjęcia przesyłki, w której stwierdzono powyższe nieprawidłowości.

W sytuacji nie stwierdzenia uszkodzenia przesyłki bądź innych nieprawidłowości przesyłka zostaje otwarta. Po jej otwarciu pracownik kancelarii:

- sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
- ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych pismach.

Kolejne czynności, które wykonuje kierownik kancelarii lub uprawniony pracownik, polegają na rejestracji przyjętych dokumentów w odpowiednich rejestrach (§ 10). I tak dokumenty oznaczone

klauzulą *ściśle tajne* w dzienniku korespondencji dokumentów oznaczonych klauzulą *ściśle tajne*, zaś oznaczone klauzulą *tajne* w dzienniku korespondencji dokumentów oznaczonych klauzulą *tajne*. Dokumenty oznaczone klauzulą *poufne* rejestruje się natomiast w dzienniku korespondencji dokumentów oznaczonych klauzulą *poufne*. Ponadto, dla każdego dokumentu zawierającego informacje niejawne oznaczone klauzulami *ściśle tajne* i *tajne*, z chwilą zarejestrowania w odpowiednim dzienniku korespondencji, zakłada się kartę zapoznania z dokumentem, którą dołącza się do dokumentu.

Każdą otrzymaną i wysyłaną przesyłkę wpisuje się pod kolejną pozycją właściwego dziennika korespondencji. Zapisów w dziennikach korespondencji dokonuje się atramentem lub tuszem, a zmiany zapisów w tych dziennikach – kolorem czerwonym, z datą i czytelnym podpisem dokonującego zmiany. Zabronione jest wycieranie i zamazywanie zapisów w dziennikach korespondencji.

Zgodnie z § 12 w kancelarii tajnej nie otwiera się przesyłek oznaczonych „do rąk własnych”, wpisując do dziennika korespondencji z opakowania nadawcę, numer i datę wpływu pisma. Dodatkowo w rubryce „Uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”.

Na opakowaniu takich przesyłek wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę w dzienniku korespondencji. Przesyłkę przekazuje się bezpośrednio adresatowi, a w razie jego nieobecności, osobie przez niego upoważnionej do odbioru – za pokwitowaniem w dzienniku korespondencji. Zatrzymanie przez kierownika jednostki organizacyjnej dokumentu, adresowanego „do rąk własnych”, odnotowuje się w dzienniku korespondencji w rubryce „Uwagi”. Przesyłki oznaczone „do rąk własnych”, po wykorzystaniu, zwraca się do kancelarii w stanie otwartym bądź zamkniętym. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu tych przesyłek w książce doręczeń przesyłek miejscowych odnotowuje się godzinę doręczenia.

Następnym etapem obiegu informacji niejawnych, które wpłynęły już do kancelarii, jest droga jaką te informacje pokonują z kancelarii tajnej do ostatecznego adresata. Tutaj zaś obowiązują różne zasady w zależności od rodzaju informacji niejawnych, tzn. czy stanowią tajemnicę państwową czy też oznaczone są klauzulą *poufne*.

W pierwszym przypadku – w świetle § 10, ust. 4 – dokumenty oznaczone klauzulą *ściśle tajne* i *tajne* kierownik kancelarii udostępnia upoważnionym pracownikom jednostki organizacyjnej na miejscu, czyniąc odpowiednią adnotację w dzienniku korespondencji. W szczególnie uzasadnionych przypadkach i w trybie przyjętym w art. 49 Ustawy z 22.01.1999 r. o ochronie informacji niejawnych, dokumenty oznaczone klauzulą *ściśle tajne* lub *tajne* mogą być wydane poza kancelarię osobie spoza jednostki organizacyjnej posiadającej odpowiednie poświadczenie bezpieczeństwa. Dokument wydaje kierownik kancelarii na podstawie pisemnej zgody kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej za pokwitowaniem w dzienniku korespondencji oraz ze stosowną adnotacją w karcie zapoznania się z dokumentem. W drugim przypadku, kierownik kancelarii lub osoba upoważniona przekazuje dokumenty oznaczone klauzulą *poufne* właściwemu pracownikowi, za pokwitowaniem w dzienniku korespondencji.

Dokumenty wykorzystane do ostatecznego załatwienia danej sprawy, z wyjątkiem oznaczonych klauzulą *zastrzeżone*, wszywa się do teczki, zgodnie z rzeczowym podziałem akt i całość kwalifikuje według dokumentu o najwyższej klauzuli tajności. Akta spraw zakończonych przechowuje się w kancelarii tajnej przez okres dwóch lat. Po upływie tego okresu akta przekazuje się do archiwum zakładowego lub składnicy akt, jeżeli jednostka organizacyjna takim dysponuje.

Rozdział 3

DOSTĘP DO INFORMACJI NIEJAWNYCH

Dostęp do informacji niejawnych jest kluczowym problemem sytuowanym w obszarze bezpieczeństwa osobowego. Czynnikiem ludzki jest najbardziej wrażliwym elementem systemu ochrony informacji niejawnych. Ocenia się, że około 80–90% tajemnic z każdej jednostki organizacyjnej wpływa za pośrednictwem pracowników, natomiast 10–20% poprzez środki techniczne (braki zabezpieczeń sieci komputerowych, telefony, faksy)¹. Z tych względów, najistotniejszym wyzwaniem w zakresie organizacji pracy na stanowiskach związanych z dostępem do informacji niejawnych jest dobór personelu. Podstawowym środkiem tu stosowanym jest postępowanie sprawdzające. Przyjęte w warunkach polskich rozwiązania odpowiadają standardom wypracowanym w państwach NATO oraz UE. Są również zgodne z wymogami demokratycznego państwa prawnego – uprawnienia służb prowadzących postępowania sprawdzające wobec obywateli zawarte są w aktach prawa powszechnie obowiązującego – ustawie oraz wydanych na jej podstawie rozporządzeniach, a od odmowy wydania poświadczenia bezpieczeństwa przysługują środki odwoławcze i skargowe.

3.1. Postępowanie sprawdzające – cele i zakres

W państwach będących członkami NATO, jak też Unii Europejskiej, główny ciężar tworzenia systemu bezpieczeństwa wewnętrznego ponoszą kraje członkowskie. Różnorodność tradycji prawnych oraz systemów administracyjnych w tych krajach powoduje, że muszą być one dostosowane do standardów NATO i UE. W krajowych regulacjach prawnych standardy te są rozwijane w system czynności

¹ P.Thiem, *Ochrona informacji niejawnych*, materiały do szkolenia pracowników, ODiDK, Gdańsk 2003, s. 56.

i procedur zapewniających osiągnięcie zamierzonego celu – bezpieczeństwa informacji, obiektów oraz osób.

Przed Polską, jako jednym z krajów członkowskich, stało zadanie przeorientowania systemu ochrony tajemnicy, począwszy od zmiany filozofii myślenia o bezpieczeństwie narodowym. Problem ochrony tajemnicy państwowej i służbowej regulowany był dotychczas aktami normatywnymi pochodzącymi z lat osiemdziesiątych. Akty te wydane w okresie „realnego socjalizmu” oraz tworzące je rozwiązania, dostosowane do warunków społeczno-ekonomicznych i politycznych tamtego okresu, w warunkach Rzeczypospolitej Polskiej, jako państwa demokratycznego, nie mogły stanowić podstawy dla nowych rozwiązań organizacyjnych. Pojawiła się konieczność zmiany prawa tak, aby niedookreśloność przepisów była zastąpiona precyzyjnie opisanymi procedurami sprawdzeniowymi oraz działaniami o charakterze profilaktycznym i szkoleniowym. Dokonując zmian Polska opierała się na sprawdzonych rozwiązaniach funkcjonujących w krajach Sojuszu.

3.1.1. Postępowanie sprawdzające do informacji niejawnych NATO

Podpisanie przez Rzeczpospolitą Polską Umowy o Bezpieczeństwie z NATO, przystąpienie do Paktu, a także wciąż trwający proces integracyjny z Unią Europejską, nakładają na stronę polską szereg zobowiązań. Problem dostosowania zarówno norm prawa, jak też infrastruktury organizacyjnej do wymogów Sojuszu w zakresie bezpieczeństwa wewnętrznego jest jednym z najważniejszych wyzwań dla Polski. Partnerem w zakresie projektowania i wprowadzania mechanizmów oraz procedur związanych z wymogami Organizacji Traktatu Północnoatlantyckiego w tym zakresie jest Biuro Bezpieczeństwa NATO, które zajmuje się wypracowaniem zasad polityki bezpieczeństwa oraz standardami służącymi do jej realizacji.

Podstawowym aktem prawnym określającym zasady współdziałania krajów członkowskich NATO w tej dziedzinie jest umowa pomiędzy stronami Traktatu Północnoatlantyckiego w sprawie ochrony informacji, podpisana 6 marca 1997 r. w Brukseli. Sygnatariusze porozumienia, deklarując wolę wprowadzenia w życie standardów

bezpieczeństwa informacji klasyfikowanych NATO, zobowiązują się do:

- ochrony i zabezpieczania przed ujawnieniem informacji niejawnych NATO, dokumentów przekazywanych NATO przez państwa członkowskie oraz informacji tajnych wymienianych między partnerami Sojuszu w ramach realizacji programu, projektu lub kontraktu NATO;

- przestrzegania zasady, że informacje i materiały oznaczone klauzulą tajności będą w taki sam sposób traktowane przez wszystkich członków Sojuszu i chronione według wspólnie ustalonych norm;

- wykorzystywania informacji klasyfikowanych tylko w celach określonych w Traktacie Północnoatlantyckim bądź przy podejmowaniu decyzji zmierzających do realizacji programu lub rezolucji wspólnoty;

- nie przekazywania informacji i materiałów niejawnych stronom nie będącym członkami NATO bez zgody strony, która je dostarczyła

- powołania Krajowych Władz Bezpieczeństwa, które wprowadzą w życie środki bezpieczeństwa, zapewniając jednolity system ochrony informacji niejawnych we wszystkich krajach członkowskich.

Unormowania NATO ściśle określają prawa dostępu do informacji i materiałów chronionych klauzulami tajności. Warunkiem dopuszczenia do tajemnic Sojuszu jest stwierdzenie, że osoba, której przyznano takie prawo, nie zagrozi – wskutek świadomego działania bądź jakichkolwiek zaniedbań – bezpieczeństwu wspólnoty i nie narazi na uszczerbek jej interesów.

Nakłada to na organy odpowiedzialne za ochronę informacji klasyfikowanych w agencjach NATO i krajach członkowskich obowiązek uprzedniego sprawdzenia czy osoby dopuszczone do informacji klasyfikowanych dają rękojmię zachowania tajemnicy, czy są godne zaufania i można im powierzyć informacje cechowane określoną klauzulą tajności bez obawy ich utraty bądź nieuprawnionego ujawnienia. Służyć temu mają procedury sprawdzające, prowadzone według wspólnie ustalonych reguł¹.

Upoważnienie osoby do dostępu do informacji o klauzuli NATO CONFIDENTIAL lub wyższej, poprzedza decyzja Krajowej Władzy Bezpieczeństwa potwierdzająca, że osoba ta spełnia warunki bez-

¹ CM (2002) 49; AC/35-D (2002).

pieczeństwa (*personnel security clearance; PSC*). Decyzja ważna jest na czas upoważnienia, które musi być udzielone zgodnie z zasadą *need to know*, (ograniczonego dostępu). Na podstawie zasady:

- do informacji klasyfikowanych NATO mogą być dopuszczone wyłącznie osoby, którym informacje te są potrzebne do wykonania powierzonej pracy i związanych z tym obowiązków;

- osobom tym można udostępnić informacje niejawne NATO tylko w takim zakresie, jaki uzasadnia rzeczywista potrzeba poznania ich zawartości.

Zasada ograniczonego dostępu do informacji niejawnych NATO uznawana jest za fundamentalną, gdyż konsekwencje jej stosowania mają decydujący wpływ na organizację i mechanizmy ochrony tajemnic Sojuszu. Jako nadrzędna norma bezpieczeństwa osobowego, wyznacza środki i zakres niezbędnych zabezpieczeń fizycznych oraz kontroli dostępu do miejsc przechowywania informacji niejawnych.

Osoby, które powinny mieć dostęp do informacji o klauzuli NATO CONFIDENTIAL lub wyższej, poza uzyskaniem decyzji potwierdzającej spełnienie warunków bezpieczeństwa, muszą dodatkowo zostać poddane procedurze sprawdzeniowej. Zakres postępowania sprawdzającego zależy od klauzuli informacji klasyfikowanych NATO, do których dana osoba ma uzyskać dostęp. Procedury sprawdzeniowe muszą być zgodne z polityką bezpieczeństwa NATO i dyrektywami wykonawczymi. Następnie osoby, wobec których postępowanie sprawdzające zakończyło się wynikiem pozytywnym, przechodzą szkolenie w zakresie procedur bezpieczeństwa NATO oraz składają zobowiązanie, że są świadome odpowiedzialności w tym zakresie. Dostęp do informacji niejawnych NATO na określonym poziomie tajności musi wynikać z ich obowiązków służbowych. Natomiast w przypadku dostępu do informacji o klauzuli NATO RESTRICTED nie jest wymagane przeprowadzenie postępowania sprawdzającego, chyba że wymagają tego przepisy i regulacje krajowe. Osoby ubiegające się o dostęp do informacji na tym poziomie tajności muszą jedynie być poinformowane o ciężącej na nich odpowiedzialności w zakresie bezpieczeństwa.

Wydanie decyzji potwierdzającej, że dana osoba spełnia warunki bezpieczeństwa, nie powinno być uznawane za zakończenie działań w zakresie bezpieczeństwa osobowego. Wymagana jest weryfikacja, że dana osoba wciąż spełnia warunki dostępu do informacji klasy-

fikowanych NATO. Cel ten może być osiągnięty poprzez ciągły proces dokonywania oceny przez władze bezpieczeństwa i kadre kierowniczą, a także poprzez szkolenia w zakresie bezpieczeństwa i programy uświadamiające zagrożenia, które przypominają pracownikom o ich obowiązkach w zakresie bezpieczeństwa i o konieczności zgłaszania przełożonym lub pracownikom pionu ochrony informacji, które mają znaczenie dla oceny spełnienia warunków bezpieczeństwa.

Prowadzenie postępowań sprawdzających, związanych z dostępem do informacji niejawnych NATO, w państwach członkowskich oraz powiadamianie organów NATO o ich rezultatach należy do obowiązków Krajowych Władz Bezpieczeństwa (w Polsce status Krajowej Władzy Bezpieczeństwa posiadają: Agencja Bezpieczeństwa Wewnętrznego i Wojskowe Służby Informacyjne). Delegując swoich przedstawicieli do pracy w organach, dowództwach bądź agencjach NATO, Krajowe Władze Bezpieczeństwa muszą zapewnić, że osoby te zostały sprawdzone i posiadają wymagane upoważnienia (certyfikaty bezpieczeństwa NATO). Upoważnienie powinno zostać wycofane, gdy Krajowe Władze Bezpieczeństwa otrzymają sygnały mogące wskazywać na brak lojalności czy też rzetelności osoby upoważnionej do dostępu do tajemnic NATO. Jeśli informacja taka dotyczy obywatela innego państwa członkowskiego wspólnoty, to władze tego kraju muszą być o tym niezwłocznie powiadomione.

Wszystkie instytucje publiczne, placówki naukowo-badawcze i przedsiębiorstwa, które posiadają informacje niejawne NATO, powinny prowadzić rejestry swoich pracowników posiadających dostęp do informacji chronionych. W wypadku uzyskania przez instytucję informacji poddającej w wątpliwość lojalność osoby już upoważnionej do dostępu do tajemnic Sojuszu, należy jak najszybciej zwrócić się do Krajowej Władzy Bezpieczeństwa z wnioskiem o sprawdzenie, czy podejrzenia te są uzasadnione. Potwierdzenie zarzutów wyklucza możliwość dalszego zatrudnienia danej osoby na stanowisku wymagającym dostępu do informacji klasyfikowanych NATO.

3.1.1.1. Kryteria postępowania sprawdzającego do informacji niejawnych NATO

Postępowanie sprawdzające polega na ustaleniu faktycznych przesłanek decyzji o przyznaniu prawa dostępu do informacji niejawnych NATO. Czynności podejmowane w toku procedury mają na celu:

- wykluczenie wątpliwości co do wiarygodności i lojalności danej osoby wobec własnego kraju i pracodawcy;
- ustalenie czy osoba ta przestrzega porządku konstytucyjnego;
- sprawdzenie czy obce służby specjalne nie próbowały jej werbować lub nawiązywać z nią kontaktu;
- zbadanie czy postępowanie danej osoby, cechy jej charakteru, zwyczaje i powiązania nie stwarzają ryzyka ujawnienia informacji klasyfikowanych.

W ramach postępowania sprawdzającego konieczne jest prześledzenie przeszłości osoby sprawdzanej z wykorzystaniem wszelkich dostępnych i wiarygodnych informacji. Zazwyczaj badany jest okres ostatnich dziesięciu lat, w przypadku osoby młodej – od chwili ukończenia 18 roku życia. Sprawdzenia powinny być dokonywane na podstawie oficjalnych rejestrów ludności, akt stanu cywilnego, rejestrów i kartotek instytucji wdrażania prawa: sądów, policji i służb specjalnych. Należy również przeprowadzić rozmowy z osobą objętą postępowaniem oraz ludźmi, którzy są w stanie bezstronnie ją ocenić.

Przed wszystkim należy sprawdzić wiarygodność danych dotyczących tożsamości i obywatelstwa osoby sprawdzanej oraz jej najbliższej rodziny; wykształcenia (ukończone szkoły, studia itp.) i statusu zawodowego (przebieg pracy, opinie pracodawców i przełożonych). Dalsze czynności będą miały na celu ustalenie:

- czy sprawdzana osoba była karana za naruszenie prawa;
- czy figuruje w rejestrach służb specjalnych bądź w kartotekach policyjnych;
- czy z uwagi na związki łączące ją z zagranicą może być podatna na presję obywateli innych krajów;
- czy była członkiem organizacji terrorystycznej lub dywersyjnej, ugrupowania bądź ruchu dążących do przejęcia władzy na drodze pozakonstytucyjnej; czy łączyły ją związki z ludźmi zaangażowanymi w działalność takich organizacji;

– czy cieszy się opinią osoby wiarygodnej finansowo i nie ma zobowiązań niewspółmiernych do osiągniętych dochodów;

– czy jest świadoma wagi dopuszczenia do informacji chronionych tajemnicą i odpowiedzialności za naruszenie zasad ich ochrony.

Krajowa Władza Bezpieczeństwa jest zobowiązana do uwzględnienia wszystkich dostępnych informacji w celu określenia, czy dana osoba spełnia warunki bezpieczeństwa.

Podjmując ostateczną decyzję o przyznaniu – bądź odmowie – prawa dostępu do informacji klasyfikowanych NATO, należy również brać pod uwagę cechy charakteru ocenianej osoby, sposób jej zachowania, zwyczaje i nałogi, zdolność panowania nad emocjami. Należy sprawdzić czy osoba sprawdzana nie jest uzależniona od narkotyków, czy nie nadużywa alkoholu; czy nie cierpi lub nie cierpiała na chorobę lub czy nie miała innych problemów natury psychicznej lub emocjonalnej, które mogą wywoływać poważne braki w zdolności dokonywania ocen, wiarygodności lub też spowodować, że osoba ta – w sposób niezamierzony – będzie stanowić zagrożenie dla bezpieczeństwa.

Negatywna informacja dotycząca jednego z wymienionych kryteriów może nie być wystarczającym powodem podjęcia decyzji o odmowie dopuszczenia do informacji niejawnych. Krajowa Władza Bezpieczeństwa musi w każdym przypadku dokonać oceny ryzyka w celu określenia, czy można uznać, że osoba sprawdzana spełnia warunki bezpieczeństwa.

Dyrektywy NATO dotyczące procesu dopuszczenia do informacji klasyfikowanych są przyjęte i realizowane przez wszystkie kraje członkowskie. Odrębne ustawy i przepisy prawne szczegółowo określają instytucje, które są odpowiedzialne za prowadzenie weryfikacji, opisują rodzaje sprawdzeń oraz zakres odpowiedzialności w przypadku nieuprawnionego ujawnienia informacji niejawnych.

3.1.2. Postępowanie sprawdzające – rozwiązania krajowe

Dokonując zmian w przepisach o ochronie tajemnicy państwowej i służbowej, Polska wzorowała się na rozwiązaniach funkcjonujących w poszczególnych krajach Sojuszu. Na podstawie założeń i systemów tam występujących wypracowano najbardziej odpowiedni dla warunków polskich, model wypełnienia standardów bezpieczeństwa Sojuszu

Północnoatlantyckiego. Efektem jest Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych. Reguluje ona zagadnienia dotyczące ochrony tajemnicy państwowej i służbowej – klasyfikowanie informacji, dostęp do nich, przebieg postępowania sprawdzającego, udostępnianie, podstawy prowadzenia kancelarii tajnych oraz kontroli obiegu dokumentów, a ponadto przebieg szkolenia w zakresie ochrony informacji niejawnych, środki ich fizycznej ochrony oraz zasady bezpieczeństwa systemów i sieci teleinformatycznych, a także podstawy prawne bezpieczeństwa przemysłowego.

Zgodnie z ustawą informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy, odpowiednio przeszkolonej i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy. Ponadto ustawa precyzuje dwa dodatkowe formalne wymogi, które muszą być bezwzględnie spełnione aby osoba uzyskała dostęp do informacji niejawnych stanowiących tajemnicę państwową:

- posiadanie obywatelstwa polskiego (z wyjątkami przewidzianymi w rozdziale 11 – Bezpieczeństwo przemysłowe);
- brak skazania prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą.

Postępowanie sprawdzające przeprowadzają, w zakresie swej właściwości, służby ochrony państwa – Wojskowe Służby Informacyjne i Agencja Bezpieczeństwa Wewnętrznego oraz pełnomocnicy ochrony.

Służby specjalne przeprowadzają postępowania poszerzone i specjalne (ramowy układ czynności zob. Aneks, Wykres 2) – w stosunku do osób ubiegających się o dopuszczenie do informacji stanowiących tajemnicę państwową o klauzulach *tajne* i *ściśle tajne* oraz postępowania wobec pełnomocników ochrony:

- Wojskowe Służby Informacyjne – wobec osób ubiegających się o zatrudnienie lub zlecone prace związane z dostępem do informacji niejawnych dotyczących obronności państwa;
- Agencja Bezpieczeństwa Wewnętrznego – w sytuacjach nie podlegających właściwości WSI.

Pełnomocnicy ochrony przeprowadzają postępowania zwykłe wobec pracowników danej jednostki organizacyjnej, związane z dostępem do informacji niejawnych stanowiących tajemnicę służbową

o klauzulach *zastrzeżone i poufne*, a także wobec osób zatrudnionych przez przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową, która ubiega się o zawarcie lub wykonuje umowę związaną z dostępem do informacji niejawnych na rzecz jednostki „macierzystej” (na pisemne polecenie jej kierownika, który tym samym uwzględnia wniosek złożony w tej sprawie przez przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową).

Ustawa uprawnia ponadto Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Policję, Straż Graniczną oraz Służbę Więzienną do samodzielnego prowadzenia procedur sprawdzeniowych wobec osób ubiegających się o przyjęcie do służby lub pracy oraz już pełniących służbę bądź zatrudnionych w tych instytucjach.

W zależności od stanowiska lub zleconej pracy, o które ubiega się dana osoba, przeprowadza się postępowania sprawdzające:

- **zwykle** – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych stanowiących tajemnicę służbową;
- **poszerzone** – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą *tajne*;
- **specjalne** – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą *ściśle tajne*.

Postępowania powtarzane są odpowiednio co 10, 5 i 3 lata. Procedura może być przeprowadzona bez uwzględnienia ustawowych terminów, jeśli pojawią się przesłanki kwestionujące rękojmię zachowania tajemnicy przez daną osobę. W takiej sytuacji o wszczęciu kolejnego postępowania sprawdzającego pełnomocnik lub służby ochrony państwa (w zależności od tego, kto prowadzi postępowanie) zawiadamiają osobę odpowiedzialną za obsadę stanowiska oraz osobę sprawdzaną. Do rozpoczęcia procedury sprawdzeniowej nie jest niezbędny wniosek osoby upoważnionej do obsady stanowiska czy kierownika jednostki organizacyjnej. Kolejne postępowanie przeprowadza się na ogólnych zasadach wskazanych w ustawie o ochronie informacji niejawnych, lecz z pominięciem obowiązku wypełnienia nowej ankiety przez osobę sprawdzaną¹.

¹ Ustawodawca wprowadzając ten zapis chciał uniknąć sytuacji, kiedy to osoba sprawdzana odmówi wypełnienia ankiety bezpieczeństwa osobowego. Bez ankiety nie można rozpocząć postępowania sprawdzającego. Zatem gdyby nie wprowadzenie tego przepisu, osoba wobec której zostały ujawnione nowe fakty wskazujące na brak dawania przez nią rękojmi zachowania tajemnicy posługiwałaby się ważnym poświadczeniem bezpieczeństwa.

Podstawą wszczęcia postępowania sprawdzającego przez pełnomocnika ochrony jest pisemne polecenie kierownika jednostki organizacyjnej. Natomiast właściwa służba ochrony państwa rozpoczyna procedurę sprawdzeniową na pisemny wniosek osoby upoważnionej do obsady stanowiska lub zlecenia pracy, w tym kierownika jednostki organizacyjnej. Do wniosku dołączona jest ankieta bezpieczeństwa osobowego wypełniona w zakresie odpowiednim do określonego we wniosku poziomu dostępu. Ankietę osobiście wypełnia osoba ubiegająca się o uzyskanie poświadczenia bezpieczeństwa lub certyfikatu bezpieczeństwa NATO, zgodnie ze swoją wiedzą, świadoma, że każde niezgodne z prawdą stwierdzenie lub zatajenie istotnego faktu może być wystarczającym powodem do wstrzymania postępowania sprawdzającego i może stanowić podstawę odmowy wydania poświadczenia bezpieczeństwa lub certyfikatu bezpieczeństwa NATO. Podpisując ankietę, osoba sprawdzana wyraża jednocześnie zgodę na prowadzenie wobec niej procedur sprawdzeniowych. Sytuacja taka oznacza, że nie są wymagane dodatkowe dokumenty, np. oświadczenie o wyrażeniu zgody na sprawdzenia w ewidencjach i kartotekach powszechnie niedostępnych.

Celem postępowania sprawdzającego jest ustalenie, czy osoba sprawdzana **daje rękojmię zachowania tajemnicy**. Zgodnie z definicją ustawową przez rękojmię zachowania tajemnicy należy rozumieć **spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem**, czyli przekazaniem informacji chronionych poza krąg osób prawnie do nich dopuszczonych.

Wymaga to wykluczenia wszelkich wątpliwości związanych z:

- lojalnością osoby sprawdzanej wobec RP;
- powiązaniami osoby sprawdzanej z podmiotami, które mogą być zainteresowane nieuprawnionym zapoznaniem się z informacjami niejawnymi;
- zdolnością osoby sprawdzanej do poddania się szczególnym rygorom, związanym z ochroną informacji niejawnych.

Zwykłe postępowanie sprawdzające obejmuje sprawdzenia, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym oraz Biurze Informacji i Statystyki, danych zawartych w ankiecie. Wyłącznie w odniesieniu do osób kandydujących na stanowiska z dostępem do informacji nie-

jawnych oznaczonych klauzulą *poufne* konieczne jest zweryfikowanie danych zawartych w ankiecie dodatkowo w ewidencjach i kartotekach powszechnie niedostępnych, przeprowadzone na piśmie wnioski pełnomocnika ochrony przez odpowiednie służby ochrony państwa. Pełnomocnik w toku zwykłego postępowania sprawdzającego dokonuje również sprawdzeń akt stanu cywilnego osoby ubiegającej się o dostęp do informacji stanowiących tajemnicę służbową.

W ramach sprawdzeń, służby ochrony państwa mają prawo przeprowadzić rozmowę z osobą sprawdzaną w celu uniknięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach. Przekazują następnie pełnomocnikowi pisemną informację o wynikach podjętych czynności. Zwykłe postępowanie sprawdzające powinno zakończyć się w ciągu miesiąca od wydania polecenia jego przeprowadzenia.

Więcej czynności wymaga przeprowadzenie poszerzonego i specjalnego postępowania sprawdzającego, które uprawnia do dostępu do informacji niejawnych stanowiących tajemnicę państwową. Dodatkowo, poza czynnościami wymaganymi przy postępowaniu zwykłym, należy ustalić, czy istnieją wątpliwości związane z wyraźną różnicą między poziomem życia osoby sprawdzanej a uzyskiwanymi przez nią dochodami, zweryfikować ewentualne informacje o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową, czy też informacje, z których wynika, że osoba sprawdzana jest uzależniona od alkoholu czy narkotyków. W celu dokonania tych ustaleń służba ochrony państwa może zobowiązać osobę sprawdzaną do poddania się badaniom specjalistycznym oraz udostępnienia ich wyników. W toku postępowania sprawdzającego weryfikowane są informacje o kandydacie w celu stwierdzenia czy nie zachodzi wobec niego ryzyko podatności na szantaż lub wywieranie presji oraz czy nie występują inne fakty wywołujące wątpliwości co do rękojmi zachowania tajemnicy¹.

¹ Określone w art. 35 ustawy.

W uzasadnionych przypadkach przeprowadza się rozmowę z osobą sprawdzaną, jej przełożonym, a także, obligatoryjnie w postępowaniu specjalnym, trzema osobami wskazanymi przez opiniowaną w celu potwierdzenia jej tożsamości. W celu potwierdzenia danych zawartych w ankiecie, jeżeli jest taka konieczność, właściwe służby przeprowadzają wywiad w miejscu zamieszkania osoby sprawdzanej, zgodnie z przepisami kodeksu postępowania karnego.

Informacje wskazujące na brak rękojmi zachowania tajemnicy muszą być wiarygodne, pochodzić z kilku źródeł lub być potwierdzone odpowiednimi opiniami albo zaświadczeniami. Podstawą kwestionowania rękojmi zachowania tajemnicy może być zarówno jednorazowe dopuszczenie się przez osobę sprawdzaną poważnego naruszenia zasad lub popełnienie przestępstwa, jak i wielokrotne powtarzanie się nawet drobnych naruszeń przepisów i zasad. Przy ocenie każdego faktu należy brać pod uwagę następujące czynniki:

- charakter, zakres i waga danego zachowania;
- motywacja;
- częstotliwość;
- stopień świadomości i dobrowolności negatywnych zachowań;
- wiek i stopień dojrzałości osoby sprawdzanej w chwili negatywnego zachowania;
- okres czasu, jaki minął od negatywnego zachowania;
- istotne zmiany na lepsze w postępowaniu osoby sprawdzanej;
- możliwość wywierania na osobę sprawdzaną presji, nacisków, podejmowania prób szantażu w związku z negatywnym zachowaniem;
- prawdopodobieństwo kontynuowania lub nawrotu negatywnych zachowań.

Dane zachowanie należy ocenić łagodniej, jeżeli było ono incydentalne; miało miejsce dawno temu i więcej się nie powtórzyło; wynikało z braku świadomości zagrożeń oraz braku odpowiedniego przeszkolenia. Natomiast konieczne jest zaostrożenie oceny w przypadku, gdy negatywne zachowania często się powtarzają; miały miejsce po dopuszczeniu osoby sprawdzanej do tajemnicy i po jej przeszkoleniu; miały miejsce niedawno i brak jest przesłanek by sądzić, że nie powtórzą się w przyszłości.

Dokonując oceny rękojmi zachowania tajemnicy należy także brać pod uwagę postawę osoby sprawdzanej – otwarte, uczciwe i pełne

informowanie osoby prowadzącej postępowanie o wszystkich istotnych okolicznościach; gotowość zastosowania się do zaleceń (przepisów i wymogów w zakresie bezpieczeństwa).

Ustawa nie podaje listy kryteriów oceny dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną. Należy więc brać pod uwagę każdą okoliczność, która może mieć znaczenie dla takiej oceny.

Jeżeli w toku poszerzonego lub specjalnego postępowania sprawdzającego wystąpią wątpliwości nie pozwalające na ustalenie, czy osoba poddana procedurze sprawdzeniowej daje rękojmię zachowania tajemnicy, służba ochrony państwa zapewnia tej osobie możliwość osobistego ustosunkowania się do przesłanek faktycznych stwarzających te wątpliwości. Wysłuchanie odbywa się w sposób zapewniający ochronę informacji. Osoba, której dotyczy wysłuchanie może stawić się ze swoim pełnomocnikiem. Służby ochrony państwa odstępują od przeprowadzenia tej czynności, jeżeli jej przeprowadzenie mogłoby spowodować naruszenie zasad ochrony informacji niejawnych stanowiących tajemnicę państwową.

Poszerzone postępowanie sprawdzające powinno zakończyć się w ciągu 2 miesięcy od daty złożenia wniosku z wypełnioną ankietą, postępowanie specjalne w ciągu 3 miesięcy.

Zakończenie postępowania sprawdzającego z wynikiem pozytywnym, czyli uznanie, iż w świetle dokonanych ustaleń nie istnieją wątpliwości, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, jest potwierdzane wydaniem poświadczenia bezpieczeństwa. Dokument ten upoważnia osobę, której został wydany do dostępu do informacji niejawnych oznaczonych klauzulą w nim określoną, a także niższymi, w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej pracy zleconej. Wydane poświadczenie bezpieczeństwa przekazywane jest osobie sprawdzanej, jednocześnie zawiadamiając osobę upoważnioną do obsady stanowiska. Zakończenie procedury sprawdzeniowej wynikiem negatywnym skutkuje koniecznością poinformowania o tym fakcie – na piśmie – osobę upoważnioną do obsady stanowiska.

Zgodnie z przepisami ustawy o ochronie informacji niejawnych, odmowa wydania poświadczenia bezpieczeństwa nie jest wiążąca dla osoby upoważnionej do obsady stanowiska, z którym wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową. Pomimo

więc negatywnego wyniku postępowania sprawdzającego, osoba może dalej wykonywać pracę na danym stanowisku. Decyzję taką podejmuje osoba upoważniona do obsady stanowiska i ponosi za nią pełną odpowiedzialność.

W przypadku obsady stanowiska lub zlecenia pracy osobie, w stosunku do której odmówiono wydania poświadczenia bezpieczeństwa dotyczącego informacji niejawnych oznaczonych klauzulą *poufne*, osoba upoważniona do obsady stanowiska ma obowiązek niezwłocznego poinformowania o tym właściwą służbę ochrony państwa (art. 41, ust. 2). Z brzmienia tego przepisu nie wynika więc obowiązek zwolnienia osoby nieposiadającej dokumentu upoważniającego do dostępu do tajemnicy służbowej z zajmowanego stanowiska lub odsunięcia od wykonywanej pracy.

Z kolei art. 28, ust. 1, pkt. 3 ustawy zawiera zakaz dopuszczenia do pracy lub pełnienia służby albo do wykonywania prac zleconych, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę państwową, osoby nieposiadającej poświadczenia bezpieczeństwa.

Z porównania obydwu przepisów jednoznacznie wynika, że w sytuacji opisanej w art. 40, ust. 2 ustawy, nadal może pracować lub pełnić służbę na stanowisku związanym z dostępem do informacji niejawnych o klauzuli *poufne* osoba nie posiadająca poświadczenia bezpieczeństwa. Nie może ona natomiast, zgodnie z treścią art. 52, ust. 3 ustawy, otrzymać z kancelarii tajnej dokumentu oznaczonego klauzulą *poufne*. W żadnym wypadku natomiast nie może pełnić obowiązków służbowych na stanowisku związanym z dostępem do informacji stanowiących tajemnicę państwową osoba bez poświadczenia bezpieczeństwa, gdyż wyraźnie zakazuje tego przepis art. 28, ust. 1, pkt 3 ustawy.

Kolejne postępowanie sprawdzające wobec osoby, która nie uzyskała poświadczenia bezpieczeństwa można przeprowadzić najwcześniej po roku od daty odmowy wydania dokumentu upoważniającego do dostępu do informacji stanowiących tajemnicę.

Ustawa określiła krąg osób, które mogą mieć dostęp do informacji niejawnych bez konieczności przeprowadzania wobec nich postępowania sprawdzającego. Należą do niego osoby sprawujące urzędy: prezydenta Rzeczypospolitej Polskiej, marszałka Sejmu i Senatu.

Posłowie i senatorzy są uprawnieni do dostępu do informacji niejawnych do poziomu *tajne* z racji ich roli konstytucyjnej. Jednak w przypadku, gdy ich obowiązki wymagają korzystania z informacji niejawnych oznaczonych klauzulą *ściśle tajne*, marszałek Sejmu lub Senatu występuje do odpowiedniej służby ochrony państwa z wnioskiem o przeprowadzenie postępowania sprawdzającego.

Obowiązek przeprowadzenia postępowania sprawdzającego nie dotyczy również osób zajmujących najwyższe stanowiska państwowe: prezes Rady Ministrów, członek Rady Ministrów, pierwszy prezes Sądu Najwyższego, prezes Naczelnego Sądu Administracyjnego, prezes Trybunału Konstytucyjnego, prezes Narodowego Banku Polskiego, prezes Najwyższej Izby Kontroli, rzecznik interesu publicznego, członkowie Rady Polityki Pieniężnej, członkowie Krajowej Rady Radiofonii i Telewizji oraz szefowie kancelarii: prezydenta RP, Sejmu, Senatu i prezesa Rady Ministrów.

Właściwa służba ochrony państwa przeprowadza jednak postępowania wobec kandydatów na te stanowiska na wniosek organu uprawnionego do ich powołania.

Ustawodawca przewidział także możliwość uzyskania dostępu do informacji niejawnych przez osoby nieposiadające poświadczenia bezpieczeństwa. W szczególnie uzasadnionych przypadkach udostępnienie informacji niejawnych stanowiących tajemnicę państwową określonej osobie lub instytucji może nastąpić na podstawie pisemnej zgody odpowiednio szefów kancelarii: prezydenta RP, Sejmu, Senatu lub prezesa Rady Ministrów albo ministra właściwego dla określonego działu administracji rządowej lub kierownika urzędu centralnego, a w przypadku ich braku – na podstawie pisemnej zgody właściwej służby ochrony państwa. Natomiast zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową może wyrazić na piśmie kierownik jednostki organizacyjnej, jednak wyłącznie w odniesieniu do informacji wytworzonych w jego jednostce.

Przewidziano również możliwość odstąpienia od wymaganych procedur sprawdzeniowych w warunkach stanu nadzwyczajnego. prezydent RP lub prezes Rady Ministrów, każdy w swoim zakresie, mogą wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego wobec osoby, która ma uzyskać dostęp do informacji niejawnych, chyba, że istnieją przesłanki kwestionujące rękojmę zachowania przez nią tajemnicy.

Ponadto nie przeprowadza się postępowania sprawdzającego wobec obywateli innych państw, którzy wykonują w RP pracę w interesie innego państwa lub organizacji międzynarodowej, jeśli obowiązek ich dopuszczenia do informacji niejawnych wynika z ratyfikowanych przez RP umów międzynarodowych, na zasadzie wzajemności.

Ustawą z 22 stycznia 1999 r. o ochronie informacji niejawnych, Polska stworzyła własny system ochrony informacji klasyfikowanych. Odpowiada on krajowym uwarunkowaniom, jednak główne założenia, mechanizmy zabezpieczenia informacji są zgodne z dyrektywami Kwatery Głównej NATO. Wprowadzenie ich w życie stanowi gwarancję, że zarówno informacje niejawne wymieniane przez organy i agencje Sojuszu, jak i pomiędzy państwami członkowskimi NATO będą w jednakowym stopniu i z równą starannością chronione.

3.1.3. Dostęp do informacji klasyfikowanych Unii Europejskiej

W kwietniu 2003 roku rząd RP podpisał traktat akcesyjny dokumentujący nasze członkostwo w strukturach UE. Nastąpiła wymiana listów pomiędzy Sekretarzem Generalnym Rady UE/Wysokim Przedstawicielem ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa a polskim ministrem spraw zagranicznych, na mocy której rząd RP zobowiązał się do przestrzegania decyzji Rady UE, głównie w zakresie wymiany informacji klasyfikowanych.

Kwestie prowadzenia postępowań sprawdzających i wydawania poświadczeń bezpieczeństwa osobowego UE osobom zatrudnionym przez instytucje państwa członkowskiego oraz w agendach UE, regulują dwa dokumenty:

- Decyzja Rady UE 2001/264/EC z dnia 19 marca 2001 r. (*Security Regulations of the Council of the European Union*);
- Decyzja Komisji Europejskiej 2001/844/EC z dnia 29 listopada 2001 r. (*Rules on Security* stanowiące załącznik do dokumentu *Rules of Procedure C(2001)3031*).

Zgodnie z przyjętymi przez organy UE regulacjami, warunkiem dostępu do informacji klasyfikowanych jest poddanie się postępowaniu sprawdzającemu, uzyskanie upoważnienia do dostępu do taje-

mnicy (poświadczenia bezpieczeństwa osobowego UE) oraz odbycie odpowiedniego przeszkolenia.

Postępowania sprawdzające prowadzone jest wobec:

- osób, których obowiązki służbowe wiążą się z dostępem do informacji klasyfikowanych UE (np. urzędnicy państwowi – zaangażowani we współpracę z organami UE oraz urzędnicy unijni);
- osób niezatrudnionych w instytucjach rządowych, w szczególności ekspertów i konsultantów, które mają uczestniczyć w przedsięwzięciach związanych z dostępem do informacji klasyfikowanych UE (np. udział w dyskusjach, przygotowywanie ekspertyz);
- osób, które z racji wykonywanych funkcji (jak np. kurierzy, konserwatorzy, sprzątaczk, strażnicy) mogą uzyskać nieuprawniony dostęp do informacji klasyfikowanych UE, w tym pracowników, którzy odpowiadają za konserwację systemów i sieci przetwarzających informacje klasyfikowane lub wykonywanie czynności technicznych w ramach takich systemów.

Zapewnienie dostępu do informacji klasyfikowanych UE o klauzuli EU CONFIDENTIAL/CONFIDENTIEL UE lub wyższej, wszystkim osobom, które ten dostęp mieć powinny, należy do Krajowej Władzy Bezpieczeństwa (osoby mające mieć dostęp do informacji o klauzuli RESTREINT UE/EU RESTRICTED powinny jedynie zostać zapoznane z obowiązującymi zasadami bezpieczeństwa oraz konsekwencjami wynikającymi z ich naruszenia – wobec tych osób nie przeprowadza się postępowania sprawdzającego).

Sprawdzenia są realizowane zgodnie z przepisami krajowymi, z zastrzeżeniem zachowania szczególnej staranności, jeśli dana osoba:

- ma uzyskać dostęp do informacji o klauzuli TRES SECRET UE/EU TOP SECRET;
- zajmuje stanowisko związane ze stałym dostępem do dużej ilości informacji SECRET UE;
- wykonuje obowiązki służbowe, które wiążą się z dostępem do szczególnie istotnych systemów i sieci teleinformatycznych, przez co ma możliwość uzyskania nieuprawnionego dostępu do dużej ilości informacji klasyfikowanych UE lub spowodowania znaczących szkód.

Czynności podejmowane w toku postępowania mają na celu ustalenie, czy osoba sprawdzana:

- daje gwarancję lojalności;

- swoim zachowaniem i cechami charakteru potwierdza zdolność do prawidłowego postępowania z informacjami niejawnymi;
- może być podatna na naciski ze strony obcych (zewnętrznych) instytucji czy osób.

Postępowanie sprawdzające kończy się wydaniem lub odmową wydania dokumentu upoważniającego do dostępu do informacji klasyfikowanych UE o określonej klauzuli tajności.

Obecnie strona polska dąży do:

- wprowadzenia poświadczeń bezpieczeństwa osobowego UE, dokumentu upoważniającego do dostępu do informacji klasyfikowanych UE o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej;
- wyraźnego powiązania upoważnienia do dostępu do informacji klasyfikowanych UE z pracą w konkretnej instytucji, przede wszystkim z uwagi na silne akcentowanie w przepisach bezpieczeństwa Unii związku upoważnienia z zakresem obowiązków służbowych, a także odrębny tryb upoważnienia do dostępu do informacji niejawnych obywateli polskich zatrudnionych w instytucjach unijnych. Proponowane rozwiązanie zapobiegne możliwości legitymowania się poświadczeniem bezpieczeństwa osobowego UE jako dokumentem „powszechnie obowiązującym”, w oderwaniu od aktualnych obowiązków służbowych danej osoby;
- zapewnienia, że poświadczenia bezpieczeństwa osobowego UE będą mogły być wydawane wyłącznie przez Krajowe Władze Bezpieczeństwa (ABW i WSI), gdyż to one odpowiadają przed organami UE za zapewnienie właściwej ochrony informacji klasyfikowanych. Ponadto należy pamiętać, że przepisy unijne wymagają, w niektórych przypadkach, szczególnie rygorystycznego przeprowadzenia procedury sprawdzieniowej. Do oceny, jaki zakres sprawdzenia jest wystarczający do podjęcia decyzji o upoważnieniu do dostępu do informacji klasyfikowanych UE, powinna być uprawniona wyłącznie Krajowa Władza Bezpieczeństwa, np. w stosunku do osoby, która ma być poddana sprawdzeniu w związku z przewidywanym dostępem do dużej ilości informacji o klauzuli SECRET UE/EU SECRET, konieczne może być przeprowadzenie także przewidzianych w ustawie dla postępowania poszerzonego czynności fakultatywnych.

3.2. Procedura odwoławcza i skargowa w przedmiocie odmowy wydania poświadczenia bezpieczeństwa

Służby specjalne, działając w warunkach demokracji konstytucyjnej, podlegają kontroli wykonywanej przez niezależne od nich organy władzy publicznej. Kształtowanie cywilnej i demokratycznej kontroli służb specjalnych jest procesem, którego istoty należy upatrywać w dążeniu do eliminowania dysproporcji pomiędzy uprawnieniami z jednej strony służb specjalnych wobec obywateli, z drugiej zaś organów, których zadaniem jest ogląd działalności służb w różnych jej aspektach. Służby muszą posiadać zdolność realizacji swych ustawowych celów w obszarze bezpieczeństwa i obronności państwa, natomiast organy nadzorujące i wyposażone w funkcje kontrolne wobec służb, muszą dysponować prawnymi instrumentami kontroli ich działań. W warunkach polskich można zatem mówić o nadzorze nad służbami specjalnymi, którą to funkcję przypisuje się organom władzy wykonawczej oraz kontroli tych służb, co sytuuje się w obrębie uprawnień władzy sądowniczej, a także w dużym stopniu ustawodawczej.¹

W państwie prawa każda działalność służb specjalnych wobec obywateli rozpatrywana jest poprzez pryzmat wzajemnych między nimi relacji, tj. uprawnień służb, celów ich działalności, ale też obowiązków obywateli oraz ich praw i wolności. Służby specjalne, które posiadają prawo gromadzenia informacji o obywatelach również w toku czynności operacyjno-rozpoznawczych, w swojej działalności mają potencjalne możliwości ingerencji w sferę wolności i praw jednostki. Aby zapobiec możliwym nieprawidłowościom przy realizacji tego typu czynności, tworzone są prawne instrumenty kontroli działań podejmowanych przez służby w obszarze narodowego bezpieczeństwa.

W kompleksie tych zagadnień należy rozpatrywać problem kształtowania się procedur odwoławczych i skargowych w przedmiocie odmów wydania poświadczeń bezpieczeństwa. Ustawa o ochronie informacji niejawnych jest bowiem aktem prawa powszechnie obowiązującego, którego nadrzędną funkcją jest zapewnienie

¹ Szerzej aspekty kontroli i nadzoru nad służbami specjalnymi zob. S. Zalewski, *Służby specjalne w państwie demokratycznym*, AON, Warszawa 2002.

prawidłowego funkcjonowania państwa, skutecznego działania jego organów, w szczególności na rzecz bezpieczeństwa i obronności. Funkcja służb ochrony państwa, powierzona służbom specjalnymi ustawą o ochronie informacji niejawnych z 1999 roku, określiła ich nowe uprawnienia względem obywateli. W konsekwencji zatem wywołała potrzebę wytworzenia nowych mechanizmów kontrolnych.

3.2.1. Środki odwoławcze jako gwarancja ochrony praw obywatelskich.

Istotą relacji pomiędzy służbą ochrony państwa a obywatelem jest wykazanie przez tę służbę, w toku procedury określanej mianem postępowania sprawdzającego, zdolności obywatela do zachowania tajemnicy, co z kolei ustawodawca nazywa rękojmią zachowania tajemnicy. Postępowanie sprawdzające jest procedurą ściśle opartą o przepisy ustawy, której charakter jednak uniemożliwia obywatelowi ogląd zebranych na jego temat informacji i materiałów. Procedura ta ma zatem charakter odbiegający od typowych procedur administracyjnych – do postępowania sprawdzającego nie stosuje się (z nielicznymi wyjątkami) przepisów Kodeksu postępowania administracyjnego¹. Na znaczeniu zyskuje tu zatem problem zgodności tego typu rozwiązań z międzynarodowymi regulacjami praw człowieka, a w szczególności aktami będącymi źródłem prawa powszechnie obowiązującego.

W Konwencji o ochronie praw człowieka i podstawowych wolności wskazuje się, że „każda osoba, której prawa i wolności zawarte w niniejszej konwencji zostały naruszone, ma prawo do skutecznego odwołania się do właściwego organu państwowego, niezależnie od tego, czy naruszenie takie zostało dokonane przez osoby działające w związku z wykonywaniem funkcji urzędowych”.²

W państwach, w których służby specjalne mają prawo podejmowania decyzji o charakterze aktów władzy publicznej wobec oby-

¹ Zob. art. 42, ust. 1a, *Ustawy o ochronie informacji niejawnych* z 22.01.1999 r., DzU nr 11, poz. 95 ze zm.

² Art.13 Konwencji o ochronie praw człowieka i podstawowych wolności (Rzym, 4 listopada 1950 r.) – „Prawa człowieka – dokumenty międzynarodowe” COMER, Toruń 1993.

wateli a takimi są poświadczenia bezpieczeństwa przepisy prawa ustanawiają skuteczne środki odwoławcze chroniące przed naruszeniem praw i wolności obywatelskich. W państwach, takich jak Francja, Włochy czy Hiszpania istnieje możliwość odwołania się obywateli od ich zdaniem niesłusznej odmowy wydania poświadczenia bezpieczeństwa do odpowiedników polskiego Naczelnego Sądu Administracyjnego. We wszystkich europejskich państwach o ukształtowanej demokratycznej formie rządów istnieją prawnie zagwarantowane jeśli nie sądowe, to przynajmniej niezależne od służb specjalnych instancje odwoławcze a procedury w tym zakresie są przejrzyste¹.

Wyrazem szczególnej troski o istnienie skutecznych środków ochrony wolności i praw jednostki w zetknięciu z działalnością służb specjalnych są orzeczenia Europejskiego Trybunału Praw Człowieka. Trybunał ten wskazuje na to, że działania służb specjalnych związane z gromadzeniem informacji o osobie powinny podlegać kontroli w toku procedur odwoławczych, stosowanych przez niezależne od służb instancje, a w przynajmniej w ostatniej instancji kontroli sądowej².

W przedmiotowych kwestiach zabierały głos organizacje pozarządowe, w tym Helsińska Fundacja Praw Człowieka. Wskazywano, że „prawo do rzetelnego procesu sądowego oraz do sądowej ochrony praw podlegają ochronie nawet gdy władze publiczne utrzymują, iż w grę wchodzi sprawa bezpieczeństwa narodowego. Każda jednostka ma prawo do skutecznej ochrony sądowej przed naruszeniem prawa przez tajne służby, co obejmuje prawo dostępu do informacji o takich naruszeniach”³.

¹ Patrz orzeczenie Trybunału Konstytucyjnego z 10 maja 2000 r. również wypowiedź dla Polskiej Agencji Prasowej Frederica Kruga – szefa Biura Bezpieczeństwa NATO z tego samego dnia, cyt. za D. Mędrala, *Polskie służby specjalne w systemie ochrony informacji niejawnych*, praca studyjna, Wojskowa Akademia Techniczna, Warszawa 2000, s. 54.

² Orzeczenie w sprawie Rotaru przeciwko Rumunii maja 2000 r. Porównaj wcześniejsze orzeczenia Trybunału Praw Człowieka dotyczące obowiązku zapewnienia skutecznego środka odwoławczego od decyzji organów państwa, np. Leander przeciwko Szwecji (1987), Friedl przeciwko Austrii (1995), Valsamis przeciwko Grecji (1996).

³ Cyt. za: *Służby Specjalne w demokracji konstytucyjnej: zasady kontroli i odpowiedzialności*, Helsińska Fundacja Praw Człowieka, www.hfrplo.waw.pl

W Polsce ewolucja podejścia do problemu otwarcia drogi do sądu obywatelom, którym służby specjalne odmówiły wydania poświadczeń bezpieczeństwa, wywołana była dość powszechną oceną, utrzymującą się w piśmiennictwie i publicystyce w początkowym okresie obowiązywania ustawy, która obejmowała szereg zarzutów wobec przyjętych rozwiązań. Wskazywano, że budowie nowego systemu ochrony informacji niejawnych po 1999 roku, nie towarzyszyło wprowadzenie do aktów prawnych efektywnych instrumentów nadzoru organów władzy wykonawczej nad tym procesem, zarówno w odniesieniu do cywilnego nadzoru nad działalnością służb specjalnych działających tu jako służby ochrony państwa, jak również w zakresie stymulowania wykonywania ustawowych powinności w terminach, określonych w przepisach prawa, przez administrację publiczną oraz przedsiębiorstwa. Postępowań sprawdzających w tym okresie nie obejmowała również kontrola sądowa. W publicznym obiegu informacji – zarówno w publicystyce, jak również opracowaniach naukowych – sformułowano szereg istotnych uwag pod adresem ustawy¹. Generalnym problemem, podnoszonym w tego typu opracowaniach, było zagadnienie zgodności z konstytucją przepisów ustawy, gdzie wskazywano problem wyłączenia postępowania sprawdzającego z zakresu postępowania administracyjnego, co skutkowało ustawowym wyłączeniem prawa obywatela do sądu. W konsekwencji, sprawa była przedmiotem skargi rzecznika praw obywatelskich do Trybunału Konstytucyjnego.

Nowelizacja ustawy o ochronie informacji niejawnych², dokonana wskutek wyroku Trybunału Konstytucyjnego³, wprowadziła do przepisów tryb odwoławczy od odmowy wydania poświadczenia bezpieczeństwa (zob. Aneks, Wykres 3) oraz tryb skargowy do Naczelnego

¹ Można tu przywołać m.in.: E. Jarzęcka-Siwik, *Nowy system ochrony tajemnicy państwowej i służbowej, Kontrola państwowa*, wyd. NIK, nr 6/1999 s. 35; S. Hoc, *Ochrona informacji niejawnych* (wybrane problemy), Wojskowy Przegląd Prawniczy, wyd. Naczelna Prokuratura Wojskowa i Izba Wojskowa Sądu Najwyższego, nr 3–4 z 1999 r., s. 3; P. Wojciechowski, *Praca dla stolarza a bezpieczeństwo państwa*, Rzeczpospolita z 26.02.1999 r.; I. Rutkiewicz, *Tajemnica państwowa i wolność informacji. Więc gdzie te ustawy?*, Tygodnik Powszechny z 28.02.1999 r.

² DzU z 2001 r., nr 22, poz. 247.

³ Wyrok TK z dnia 10.05.2000 r., Sygn. K. 21/99.

Sądu Administracyjnego (zob. Aneks, Wykres 5). Otwarto tym samym drogę do sądu obywatelom, którym pełnomocnicy ochrony w postępowaniach zwykłych lub służby ochrony państwa w postępowaniach poszerzonych i specjalnych, odmówiły wydania poświadczeń bezpieczeństwa.

3.2.2. Procedura odwoławcza

Do czasu opisanej wyżej nowelizacji ustawy o ochronie informacji niejawnych w 2001 roku jedyną formą zewnętrznego, względem służb ochrony państwa oglądu postępowania sprawdzającego, była kontrola tego postępowania przez prezesa Rady Ministrów. Tryb wszczynania tej kontroli nie obejmował jednak jej inicjowania przez obywatela poddanego sprawdzeniu przez służbę we właściwym postępowaniu. Uprawnienie do wnioskowania o przeprowadzenie kontroli posiadała natomiast osoba uprawniona do obsady stanowiska, na którym wykonywano prace związane z dostępem do informacji niejawnych. Wobec tej ustawowej procedury formułowano zatem uprawniony zarzut o pozbawieniu obywatela, poddanego postępowaniu sprawdzającemu, skutecznego środka odwoławczego.

Wprowadzona w wyniku nowelizacji z 2001 roku procedura odwoławcza od odmowy wydania poświadczenia bezpieczeństwa, istotnie zmieniła ten stan rzeczy. Obecnie, obywatel któremu służba ochrony państwa odmówiła wydania poświadczenia bezpieczeństwa, ma prawo w terminie 14 dni od doręczenia odmowy odwołać się do prezesa Rady Ministrów. Warto tu zaznaczyć, że służby ochrony państwa prowadzą postępowania specjalne i poszerzone (do informacji stanowiących tajemnicę państwową odpowiednio o klauzuli *ściśle tajne* i *tajne*). Natomiast postępowania zwykłe – do tajemnicy służbowej – prowadzą pełnomocnicy ochrony i od tych postępowań odwołanie przysługuje do szefa właściwej służby ochrony państwa¹.

Odwołanie do prezesa Rady Ministrów wnosi się za pośrednictwem szefa właściwej służby ochrony państwa, która jest zobowiązana w terminie 14 dni przesłać akta postępowania sprawdzającego. Od dnia nadesłania odwołania prezes Rady Ministrów ma trzy

¹ Zob. art. 48a oraz 48i Ustawy o ochronie informacji niejawnych.

miesiące na rozpatrzenie odwołania. Warto przy tym zaznaczyć, że ustawodawca obok służb ochrony państwa (Agencji Bezpieczeństwa Wewnętrznego i Wojskowych Służb Informacyjnych) wyposażył szereg innych organów w uprawnienia do prowadzenia postępowań sprawdzających wobec osób ubiegających się o przyjęcie do służby oraz pełniących służbę. Uprawnienia takie posiadają poza służbami ochrony państwa: Agencja Wywiadu, Policja, Żandarmeria Wojskowa, Straż Graniczna i Służba Więzienna¹. Tak więc, w zakresie postępowania odwoławczego i skargowego, przepisy dotyczące postępowania sprawdzającego dotyczącego służb ochrony państwa, stosuje się odpowiednio do wymienionych wyżej służb, co obejmuje również stosowanie przepisów dotyczących szefów tych służb². Stąd odwołania dotyczące np. funkcjonariuszy policji czy Straży Granicznej, kierowane do prezesa Rady Ministrów wnoszą się za pośrednictwem odpowiednio komendantów głównych Policji i Straży Granicznej.

Przepisy Ustawy o ochronie informacji niejawnych bezpośrednio nie wskazują przebiegu i sposobu prowadzenia czynności w procedurach odwoławczych od odmowy wydania poświadczenia bezpieczeństwa. Brak precyzyjnych przepisów w tym zakresie nie zdejmuje jednak obowiązku ukształtowania procedury z zachowaniem wymogów obiektywizmu i należytej staranności.

Z ustawy wynika szereg rekomendacji dla procedury odwoławczej (ramowy układ czynności w toku tej procedury zob. Aneks, Wykres 4). Wstępną czynnością jest zbadanie, czy zachodzą przesłanki wydania postanowień, o których mowa w art. 48 c Ustawy o niedopuszczalności odwołania oraz o uchybieniu terminu do wniesienia odwołania. W sytuacji, gdy następuje uchybienie terminu do wniesienia odwołania lub zachodzą okoliczności, które czynią odwołanie niedopuszczalnym rekomenduje się podjęcie decyzji o wydaniu postanowienia prezesa Rady Ministrów na podstawie art. 48 c ustawy.

Celem procedury odwoławczej jest ustosunkowanie się do przesłanek faktycznych (udokumentowanych przez prowadzących postępowanie faktów) świadczących o wątpliwościach, co do rzekomych zachowania tajemnicy przez osobę sprawdzaną.

¹ Zob. art. 30 Ustawy o ochronie informacji niejawnych.

² Art. 48 m Ustawy o ochronie informacji niejawnych.

Czynności w toku odwołania zmierzają do oceny prawidłowości postępowania, w tym jego staranności i są dokonywane na podstawie dokumentów przedstawionych przez właściwą służbę ochrony państwa. W przypadku stwierdzenia w toku procedury odwoławczej, że służba nie przeprowadziła w postępowaniu sprawdzającym czynności, wskazanej w ustawie, jako obligatoryjnej lub mogącej mieć wpływ na wynik postępowania, zleca się służbie ochrony państwa przeprowadzenie dodatkowych czynności w celu uzupełnienia materiałów i dowodów w tym postępowaniu (w trybie art. 48d ustawy). W przypadku stwierdzenia w toku procedury odwoławczej, że czynność przeprowadzona przez służbę w postępowaniu, ze względu na jej przebieg, okoliczności lub sposób udokumentowania, może budzić wątpliwości co do zachowania ustawowych zasad bezstronności i obiektywizmu, a także najwyższej staranności, zleca się ponowne przeprowadzenie ww. czynności (w trybie art. 48d ustawy).

W procedurze odwoławczej bada się zarówno formalny przebieg postępowania sprawdzającego, jak również treść materiałów zgromadzonych w jego toku. Określenie wymogów formalnych zmierza do odpowiedzi na pytanie, czy służba ochrony państwa wykonała czynności w postępowaniu sprawdzającym z poszanowaniem zasad bezstronności i obiektywizmu (art. 34) oraz najwyższej staranności. W szczególności dotyczy to stwierdzenia:

- czy dotrzymano terminów określonych ustawą dla poszczególnych rodzajów postępowania (art. 42, pkt. 2),
- czy wykonano wszystkie czynności przewidziane dla danego rodzaju postępowania (art. 37, 38, 39, 40),
- czy odmowa wydania poświadczenia bezpieczeństwa zawiera właściwe pouczenia o dopuszczalności odwołania (art. 36, ust. 5) oraz czy została właściwie doręczona – z zachowaniem wymogów określonych w kpa (art. 37, ust.10).

Określenie wymogów merytorycznych sprowadza się do stwierdzenia, czy służba ochrony państwa – zgodnie z ustawą – ustaliła faktyczne przesłanki odmowy wydania poświadczenia bezpieczeństwa, a w szczególności dotyczy to przypadków, gdy w stosunku do osoby sprawdzanej występują wątpliwości dotyczące:

- uczestnictwa, współpracy lub popierania działalności szpiegowskiej, terrorystycznej itd. (art. 35, pkt. 2, ust. 1),

– ukrywania lub świadomego, niezgodnego z prawdą podawania informacji mających znaczenie dla ochrony informacji niejawnych (art. 35, pkt. 2, ust. 2),

– uczestnictwa lub współpracy z partiami politycznymi lub innymi organizacjami, o których mowa w art. 13 Konstytucji (art. 35, pkt. 2, ust.3),

– prób werbunku lub kontaktu ze strony obcych służb specjalnych (art. 35, pkt. 2, ust.4),

– istotnej różnicy w poziomie życia a dochodów (art. 35, pkt. 3, ust.1),

– zakłóceń czynności psychicznych, uzależnień itp. (art. 35, pkt. 3, ust. 2, 3),

– innych ważnych powodów określonych w ustawie.

Czynności w toku procedury odwoławczej od odmowy wydania poświadczenia bezpieczeństwa kończą wnioski, wraz z rekomendacją do podjęcia decyzji: o nakazie wydania poświadczenia bezpieczeństwa lub o utrzymaniu w mocy odmowy poświadczenia bezpieczeństwa. Decyzje i postanowienia, o których wyżej mowa, a także zlecenia służbie ochrony państwa przeprowadzenia dodatkowych czynności w postępowaniu sprawdzającym, podpisuje prezes Rady Ministrów.

Po zakończeniu procedury odwoławczej decyzje lub postanowienia są przysyłane osobie sprawdzanej, osobie upoważnionej do obsady stanowiska (wnioskującej o przeprowadzenie postępowania sprawdzającego) oraz właściwej służbie ochrony państwa – prowadzącej postępowanie. Na decyzje prezesa Rady Ministrów o utrzymaniu w mocy odmowy wydania poświadczenia bezpieczeństwa oraz postanowienia o uchybieniu terminu do wniesienia odwołania oraz niedopuszczalności wniesienia odwołania, osobie sprawdzanej przysługuje skarga do Naczelnego Sądu Administracyjnego w terminie 30 dni od dnia doręczenia decyzji lub postanowienia (art. 48j).

Istotnym niedostatkiem rozwiązań ustawowych, widocznym w relacji do procedury odwoławczej, jest niemożność uchylenia odmowy wydania poświadczenia bezpieczeństwa przez organ odwoławczy – prezesa Rady Ministrów. Ma on możliwość wydania – zgodnie z ustawą – decyzji nakazującej wydanie poświadczenia bądź też decyzji utrzymującej w mocy odmowę wydania poświadczenia przez służby ochrony państwa (także postanowień w zakresie nie-

dopuszczalności i przekroczenia terminu do wniesienia odwołania). Jednak brak możliwości uchylenia odmowy wydania poświadczenia nie pozwala na powtórne przeprowadzenie całego postępowania (możliwość uchylenia odmowy ma jedynie NSA), co może być potrzebne w sytuacji, gdy służba prowadząca postępowanie nie dochowywałaby ustawowych wymogów należytej staranności i obiektywizmu w postępowaniu, przy jednoczesnym zgromadzeniu w aktach postępowania sprawdzającego informacji pozwalających ocenić, że istnieją faktyczne przesłanki wywołujące wątpliwości co do rękojmi zachowania tajemnicy przez osobę sprawdzaną. Postulat udoskonalenia rozwiązań stosowanych w toku procedury odwoławczej, może być przedmiotem prac w toku kolejnych nowelizacji ustawy o ochronie informacji niejawnych.

3.2.3. Skarga do sądu administracyjnego

Ważnym elementem sądowego nadzoru nad działaniami służb specjalnych było wprowadzenie do przepisów ustawy o ochronie informacji niejawnych drogi skargowej do Naczelnego Sądu Administracyjnego od odmowy wydania poświadczenia bezpieczeństwa utrzymaną w mocy przez organ odwoławczy (prezesa Rady Ministrów), a także od postanowień wydanych w trybie odwoławczym. Droga skargowa została wprowadzona do ustawy o ochronie informacji niejawnych wskutek wyroku Trybunału Konstytucyjnego¹, który zakwestionował zgodność z konstytucją (art. 45, ust. 1 i art. 77, ust. 2) oraz Konwencją o ochronie praw człowieka i podstawowych wolności (art. 13)² niektórych przepisów ustawy, zamykających de facto obywatelowi drogę do sądu – to jest pozbawiających go jakiegokolwiek skutecznego środka odwoławczego, od odmowy wydania poświadczenia bezpieczeństwa przez służby ochrony państwa. Znowelizowane przepisy ustawy wskazały na niejawny tryb rozpatrywania skargi obywatela przed NSA. Ramowy schemat postępowania przed NSA ukazano na wykresie (zob. Aneks, wykres 5). Zatem – zważywszy na charakter sprawy – obywatel, nie dający

¹ Wyrok z 10.05.2000 r., Sygn K21/99

² DZU z 1993 r., nr 61, poz. 284 z późn. zm.

według służby ochrony państwa rękami zachowania tajemnicy, nie jest pełnoprawnym uczestnikiem postępowania sądowego, nie jest bowiem dopuszczony do tajemnicy państwowej – jeśli materiały postępowania są oznaczone taką klauzulą.

Charakteryzując rolę sądu w omawianej materii należy odnotować postęp, jaki uczynił ustawodawca w zakresie wzmacniania prawnych gwarancji obywatelskich praw. Nie należy jednak prognozować rychłego zakończenia dyskusji i prac legislacyjnych nad doskonaleniem skargi do sądu administracyjnego, jako instrumentu zabezpieczania obywateli przed możliwymi nadużyciami służb prowadzących postępowania sprawdzające – dalej bowiem mamy do czynienia z brakiem możliwości reprezentowania interesu strony skarżącej przed sądem. Istotne jest również, że sąd ma prawne możliwości tylko w zakresie rozstrzygnięcia na rzecz skarżącego (uwzględnienie skargi), co skutkuje uchYLENIEM decyzji tak podjętej w procedurze odwoławczej od odmowy wydania poświadczenia, jak też uchYLENIEM samej odmowy wydania poświadczenia. Nie jest natomiast równoznaczne z wydaniem poświadczenia bezpieczeństwo lub choćby z nakazaniem wydania takiego poświadczenia służbie ochrony państwa – ten instrument przysługuje organowi odwoławczemu, tj. prezesowi Rady Ministrów.

Należy jednak zaakcentować, że już samo doprowadzenie do niezależnej od służb specjalnych oceny materiałów postępowań prowadzonych przez te służby, jest istotnym elementem nadzoru sądowego nad ich działalnością.

Najbliższe perspektywy sądowej kontroli służb ochrony państwa wyznacza wchodząca po 1 stycznia 2004 roku Ustawa z dnia 30 sierpnia 2002 r. prawo o postępowaniu przed sądami administracyjnymi¹, która wprowadza dwuinstancyjność w zakresie rozpatrywania spraw przed sądami administracyjnymi. Obok NSA pojawią się zatem – w pierwszej instancji – wojewódzkie sądy administracyjne, właściwe w rozpatrywaniu wszystkich spraw niezastrzeżonych dla NSA, który będzie rozpoznawał środki odwoławcze od orzeczeń woje-

¹ DzU z 2002 r., nr 153, poz. 1270; zob. również Ustawę z 30 sierpnia 2002 r. Przepisy wprowadzające ustawę – Prawo o ustroju sądów administracyjnych i ustawę – Prawo o postępowaniu przed sądami administracyjnymi, która w art. 62 zmienia szereg przepisów ustawy o ochronie informacji niejawnych (DzU z 2002 r., nr 153, poz. 1271).

wódzkich sądów administracyjnych, podejmował uchwały mające na celu wyjaśnienia przepisów prawnych wywołujących rozbieżności w orzecznictwie sądów administracyjnych oraz uchwały zawierające rozstrzygnięcia zagadnień prawnych budzących poważne wątpliwości w konkretnych sprawach sądowo-administracyjnych. Właściwość NSA będzie też obejmowała rozstrzyganie sporów pomiędzy organami samorządu terytorialnego, samorządowymi kolegiatami odwoławczymi oraz spory pomiędzy organami tych jednostek a organami administracji rządowej. Ramową strukturę postępowania przed sądami administracyjnymi po 1 stycznia 2004 r. obrazuje wykres (zob. Aneks, Wykres 6).

Reasumując orzecznictwo NSA wpływa w największym stopniu na praktykę postępowań sprawdzających prowadzonych przez służby ochrony państwa oraz inne służby, którym ustawodawca przyznał uprawnienia do prowadzenia procedur wobec własnych funkcjonariuszy oraz procedur odwoławczych prowadzonych w Kancelarii Prezesa Rady Ministrów. Sądowa kontrola nad działalnością organów prowadzących czynności w postępowaniach sprawdzających oraz procedurach odwoławczych od odmów wydania poświadczeń bezpieczeństwa jest zatem jedną z istotniejszych form kontroli i doskonalenia przedmiotowych procedur, ale też gwarancji praw obywatelskich, które mogą być naruszane w ich toku.

Rozdział 4

UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH

W całokształcie zagadnień związanych z ochroną informacji niejawnych istotną rolę można przypisać problemowi ich udostępniania. Informacje, stanowiące tajemnicę państwową lub służbową, nie podlegają absolutnej ochronie w każdej sytuacji i każdym przypadku. Ustawodawca przewidział zatem sytuacje, w których interes państwa wymaga udostępnienia informacji niejawnych. Problem ten należy ponadto postrzegać poprzez unormowania konstytucyjne wolności informacji. Zasadą w demokracji politycznej jest bowiem prawo obywatela do dostępu do informacji publicznej, zaś ograniczenia tego dostępu są wyjątkiem od reguły.

4.1. Udostępnianie danych z ewidencji i akt postępowań sprawdzających

Akta zakończonych postępowań sprawdzających, prowadzonych w odniesieniu do osób ubiegających się o stanowisko lub zlecenie pracy, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę służbową, przechowywane są przez pełnomocnika ochrony (art. 42, ust. 3). Akta takich postępowań mogą być udostępniane do wglądu wyłącznie:

- osobie sprawdzanej ubiegającej się o stanowisko,
- na żądanie sądu lub prokuratora w celu ścigania karnego albo prezesowi Rady Ministrów, szefowi Agencji Bezpieczeństwa Wewnętrznego, szefowi Wojskowych Służb Informacyjnych, komendantowi głównemu Policji, komendantowi głównemu Żandarmerii Wojskowej, komendantowi głównemu Straży Granicznej lub dyrektorowi generalnemu Służby Więziennej w celu rozpatrzenia odwołania,
- Naczelnemu Sądowi Administracyjnemu w związku z rozpatrywaniem skargi,

– osobie upoważnionej do obsady stanowiska lub właściwym służbom ochrony państwa dla celów postępowania sprawdzającego.

W świetle art. 42, ust. 4 akta zakończonych postępowań sprawdzających prowadzonych w odniesieniu do osób ubiegających się o stanowiska lub zlecenie pracy, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę państwową, przechowywane są jako wyodrębniona część w archiwach służb ochrony państwa.

Służby ochrony państwa, każda w zakresie swojego działania, prowadzą ewidencję osób, które uzyskały poświadczenie bezpieczeństwa, a także osób, które zajmują stanowiska lub wykonują prace, z którymi łączy się dostęp do informacji niejawnych oznaczonych klauzulą *poufne* lub stanowiących tajemnicę państwową. Prowadzą także ewidencję osób, którym odmówiono wydania poświadczenia bezpieczeństwa.

Dane z przedmiotowej ewidencji oraz akta postępowań sprawdzających prowadzonych przez służby ochrony państwa – zgodnie z ust. 5, art. 42 – mogą być udostępnione wyłącznie na żądanie:

- sądu lub prokuratora w celu ścigania karnego,
- służbom ochrony państwa dla celów postępowania sprawdzającego.

Mogą też być udostępnione prezesowi Rady Ministrów, szefowi Agencji Bezpieczeństwa Wewnętrznego, szefowi Wojskowych Służb Informacyjnych, komendantowi głównemu Policji, komendantowi głównemu Żandarmerii Wojskowej, komendantowi głównemu Straży Granicznej lub dyrektorowi generalnemu Służby Więziennej w celu rozpatrzenia odwołania oraz Naczelnemu Sądowi Administracyjnemu w związku z rozpatrywaniem skargi.

Udostępniane dane z ewidencji i akt postępowań sprawdzających prowadzonych przez służby ochrony państwa mogą obejmować wyłącznie:

- w odniesieniu do osoby – jej imię i nazwisko, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, nazwę i adres jednostki organizacyjnej, w której osoba jest zatrudniona, nazwę komórki organizacyjnej i stanowiska oraz sygnaturę akt postępowania sprawdzającego,
- w odniesieniu do stanowiska lub pracy zleconej – datę objęcia stanowiska lub rozpoczęcia pracy, określenie z dostępem do jakich

informacji niejawnych łączy się to stanowisko, datę wydania i numer poświadczenia bezpieczeństwa.

Sposób i tryb udostępniania danych z ewidencji oraz akt postępowań sprawdzających sądowi lub prokuratorowi oraz służbom ochrony państwa określa Rozporządzenie prezesa Rady Ministrów z 25.02.1999 r. (DzU z 1999 r., nr 18, poz. 161). W świetle § 3 rozporządzenia udostępnienie danych może nastąpić wyłącznie na pisemne żądanie sądu lub prokuratora albo służby ochrony państwa, które zawiera oznaczenie zakresu żądanych danych. Dane z ewidencji udostępnia szef właściwej służby ochrony państwa lub upoważniony przez niego funkcjonariusz albo żołnierz. Udostępnienie danych z ewidencji następuje w formie pisemnej oraz w terminie i w zakresie określonym w żądaniu. Żądane dane mogą także być przekazane za pomocą systemu lub sieci teleinformatycznej służącej wytwarzaniu, przechowywaniu, przetwarzaniu lub przekazywaniu informacji niejawnych.

4.2. Udostępnianie informacji w świetle ustawy o ochronie informacji niejawnych

W myśl postanowień Ustawy z 6.09.2001 r. o dostępie do informacji publicznej (DzU z 2001 r., nr 112, poz. 1198) każda informacja o sprawach publicznych stanowi informację publiczną i podlega udostępnieniu każdemu, kto tego żąda. Od osoby domagającej się informacji nie wolno żądać wykazania interesu prawnego lub faktycznego. Do udostępnienia informacji publicznej obowiązane są wszystkie władze publiczne, w tym także te wytwarzające, przekazujące i przechowujące informacje niejawne.

Prawo do informacji publicznej podlega jednak ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych.

Jak stanowi art. 49 Ustawy o ochronie informacji niejawnych w szczególnie uzasadnionych przypadkach udostępnienie informacji niejawnych stanowiących tajemnicę państwową określonej osobie lub instytucji może nastąpić na podstawie pisemnej zgody odpowiednio szefów kancelarii: prezydenta Rzeczypospolitej Polskiej, Sejmu,

Senatu lub prezesa Rady Ministrów albo ministra właściwego dla określonego działu administracji rządowej, prezesa Narodowego Banku Polskiego lub kierownika urzędu centralnego, a w przypadkach szczególnych na podstawie pisemnej zgody właściwej służby ochrony państwa.

Zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową może wyrazić na piśmie kierownik jednostki organizacyjnej (stosującej obligatoryjnie przepisy ustawy o ochronie informacji niejawnych), wyłącznie w odniesieniu do informacji wytworzonych w tej jednostce.

Wyrażenie zgody na udostępnienie informacji niejawnych nie może powodować zmiany lub zniesienia klauzuli tajności przyznanej informacji, a ponadto powinno określać zakres podmiotowy i przedmiotowy udostępnienia. Pierwszy warunek oznacza precyzyjne wskazanie osób, którym mogą być udostępniane informacje niejawne. Drugi natomiast stwarza możliwość udostępnienia informacji niejawnych w całości albo w jakimś ściśle wyznaczonym fragmencie. Decyzja w jakiej części powinno nastąpić udostępnienie informacji zależeć będzie od powodów, dla których to się dzieje.

Niektóre unormowania ustawowe dodatkowo zaostrzają powyżej przedstawiony tryb i zasady na jakich mogą zostać udostępniane informacje niejawne. Szczególne znaczenie pewnych kategorii informacji chociażby dla bezpieczeństwa państwa stanowią wystarczające uzasadnienie przyjmowania takich rozwiązań. Dotyczy to w szczególności informacji uzyskiwanych i przetwarzanych przez organy zajmujące się rozpoznawaniem zagrożeń i przestępstw w drodze czynności operacyjno-rozpoznawczych. Znamiennym przykładem takich regulacji są przepisy, na podstawie których działają służby specjalne¹.

¹ W świetle ustawy o ABW oraz AW szef ABW może zezwolić funkcjonariuszom i pracownikom agencji oraz byłym funkcjonariuszom i pracownikom, po ustaniu stosunku służbowego lub stosunku pracy w agencji, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych, na udzielenie informacji niejawnej określonej osobie lub instytucji. Uprawnienie to szefowi ABW przysługuje także wobec byłych funkcjonariuszy i pracowników Urzędu Ochrony Państwa.

Zezwolenie nie może dotyczyć udzielenia informacji o:

4.3. Zasady zwalniania z obowiązku zachowania tajemnic

W literaturze przedmiotu okoliczności związane z obowiązkiem zachowania tajemnicy nazywa się zakazami dowodowymi¹. Oznaczają one pewnego rodzaju ograniczenia przewidziane w Kodeksie postępowania karnego² w korzystaniu w procesie karnym z jakiegoś dowodu lub środka dowodowego (np. zakaz przesłuchania osoby obowiązanej do zachowania tajemnicy państwowej bez uprzedniego uzyskania zgody właściwego organu). Powszechnie przyjmuje się, że zakazy dowodowe funkcjonują w postępowaniu karnym z uwagi na konieczność ochrony pewnych wyższych interesów niż interes ścigania karnego. Takim interesem może być np. interes państwa, który w niektórych sytuacjach wymaga zachowania tajemnicy państwowej bez względu na inne racje przemawiające za jej ujawnieniem.

W sytuacji kiedy jednak dochodzą one do głosu, trudno byłoby dociekać prawdy pomimo zakazów dowodowych. W takich też przy-

– osobie, jeżeli zostały uzyskane w wyniku prowadzonych przez agencje albo inne organy, służby lub instytucje państwowe czynności operacyjno-rozpoznawczych,

– szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz o stosowanych w związku z ich prowadzeniem środkach i metodach,

– osobie udzielającej pomocy agencji,

– osobie udzielającej pomocy Urzędowi Ochrony Państwa w wykonywaniu czynności operacyjno-rozpoznawczych.

Nie dotyczy to jednak sytuacji, kiedy udostępnienia informacji niejawnych żąda prokurator albo sąd, zgłoszonego w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, albo żądania rzecznika interesu publicznego w celu przeprowadzenia postępowania lustracyjnego, lub realizacji zadań rzecznika interesu publicznego lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych.

Podobnie jest w przypadku żądania udostępnienia informacji niejawnych przez prokuratora lub sąd uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych.

¹ Zob. T. Grzegorzczak, *Kodeks postępowania karnego (komentarz)*, Zakamycze 1998, s. 339.

² Ustawa z 6.06.1998 r. (DzU z 1998 r., nr 88, poz. 553 ze zm.).

padkach Kodeks postępowania karnego pozwala korzystać z instytucji zwalniania z obowiązku zachowania tajemnicy. Zasady i tryb zwalniania z obowiązku zachowania tajemnicy określają postanowienia rozdziału 21kpk zatytułowanego „Świadkowie”.

W świetle art. 179, § 1 osoby obowiązane do zachowania tajemnicy państwowej mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od obowiązku zachowania tajemnicy przez uprawniony organ przełożony. Organem do którego zwraca się prokurator (sąd) w sprawie zwolnienia z zachowania tajemnicy państwowej jest ten organ kierujący podmiotem, w którym pracuje (pełni służbę) osoba zobowiązana do zachowania tajemnicy państwowej.

Zwolnienia wolno odmówić tylko wtedy, gdyby złożenie zeznania wyrządzić mogło poważną szkodę państwu. W przypadku odmowy sąd lub prokurator może jednak zwrócić się do właściwego naczelnego organu administracji rządowej o zwolnienie świadka od obowiązku zachowania tajemnicy.

W świetle art. 180, § 1 osoby obowiązane do zachowania tajemnicy służbowej lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania tajemnicy. Zwolnienie osób z obowiązku zachowania tajemnicy służbowej powinno zostać odnotowane w protokole przesłuchania świadka. Osoby zwolnione od obowiązku zachowania tajemnicy państwowej i służbowej sąd przesłuchuje na rozprawie z wyłączeniem jawności (art. 181 kpk).

Rozdział 5

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

Ustawa o ochronie informacji niejawnych, oprócz nowego ujęcia problematyki ochrony i postępowania z informacjami niejawnymi, zawiera definicję tajemnicy państwowej i służbowej, a także wykazy rodzajów informacji tajnych i ściśle tajnych. Pomija natomiast kwestie odpowiedzialności za naruszenie jej przepisów. Ustawodawca uznał, że w sposób wystarczający informacje klasyfikowane chroni kodeks karny.

5.1. Odpowiedzialność karna

Doceniając problematykę ochrony informacji, kodeks karny wprowadził nowe typy przestępstw, związane z nowoczesnymi technicznymi środkami przekazu informacji wykorzystywanymi do ujawnienia tajemnicy. Ustawodawca umieścił je w osobnym XXXIII rozdziale kodeksu karnego, zatytułowanym „Przestępstwa przeciwko ochronie informacji”¹ – jest ich pięć – począwszy od art. 265, kończąc na art. 269. Przedmiotem ochrony jest informacja. Rozdział XXXIII chroni informację w trzech kierunkach, w trzech grupach przepisów – chroniących informację jako tajemnicę, zabezpieczających informację przed zniszczeniem lub uszkodzeniem, wreszcie chroniących urządzenia służące do utrwalania i przekazywania informacji.

¹ J. Wojciechowski, *Kodeks karny. Komentarz i orzecznictwo*, Warszawa 1998.

5.1.1. Ujawnienie tajemnicy państwowej

Ujawnienie tajemnicy państwowej to podstawowy typ przestępstwa przeciwko ochronie informacji (art. 265, § 1 kk). Jest to przestępstwo polegające na ujawnieniu osobie nieupoważnionej informacji stanowiących tajemnicę państwową bądź wykorzystaniu takich informacji wbrew przepisom ustawy, w wyniku czego narażono na szkodę obronność, bezpieczeństwo lub inny ważny interes państwa.

Ujawnienie – to uczynienie jawnym tego, co dotychczas nie było jawne. O ujawnieniu informacji mówimy wówczas, gdy informacja do tej pory niejawna, zarówno w sensie prawnym, jak i faktycznym, wbrew woli jej wytwórcy utraciła ten atrybut – stała się jawna i mogły ją poznać nie tylko osoby uprawnione. Zachowanie to ma charakter jednorazowy – osoba ujawniająca tajemnicę państwową czyni ją jawną dla kolejnych odbiorców. Powtarzanie, przekazywanie lub rozpowszechnianie takiej informacji, wcześniej ujawnionej przez inną osobę, nie stanowi przestępstwa ujawnienia tajemnicy państwowej.

Bezprawne ujawnienie informacji stanowiącej tajemnicę państwową polega na przekazaniu jej poza krąg osób prawnie do niej dopuszczonych. Nie ma w tym wypadku znaczenia liczba osób nieuprawnionych, do których informacja ta dotarła, ani sposób jej przekazania. Ujawnieniem będzie zarówno przekazanie – ustne, pismne czy telefoniczne – takiej informacji mediom, jak i jednej tylko osobie nie należącej do kręgu osób uprawnionych. Nie poniesie natomiast odpowiedzialności za ujawnienie tajemnicy państwowej dziennikarz, który ujawnioną informację rozpowszechnia.

Ze względu na cechy przestępstwa ujawnienia tajemnicy państwowej, sprawcami tego czynu mogą być osoby uprawnione do dostępu do takich informacji w związku ze sprawowanym urzędem lub pełnioną funkcją, bądź z tytułu posiadania odpowiedniego poświadczenia bezpieczeństwa. Osoba nie należąca do tego kręgu może natomiast odpowiadać za przestępstwo z art. 265 w jego drugiej postaci, czyli za wykorzystanie tajemnicy państwowej wbrew przepisom prawa.

Niezgodne z prawem wykorzystanie informacji o klauzuli „tajne” lub „ściśle tajne” polega na zrobieniu z niej użytku prawnie niedopuszczalnego, np. wykorzystanie informacji sklasyfikowanych jako „tajne” w jawnych negocjacjach handlowych, publikacjach itp. O popełnienie czynu może być oskarżony dziennikarz, który opubli-

kuje dokument stanowiący tajemnicę państwową, jeśli uzyskał go od osoby uprawnionej do dostępu do takich informacji. W tym wypadku przestępstwo ujawnienia tajemnicy państwowej popełnia osoba przekazująca dziennikarzowi dokument niejawny. Natomiast opublikowanie tego dokumentu może stanowić przestępstwo bezprawnego wykorzystania tajemnicy państwowej, czyli spożytkowania takich informacji do celów niezgodnych z przepisami prawa.

Podmiotem przestępstwa ujawnienia tajemnicy państwowej nie mogą być naczelne i centralne organy administracji rządowej, które są uprawnione do udostępniania informacji stanowiących tajemnicę państwową (art. 49, ust. 1 Ustawy o ochronie informacji niejawnych).

Strona podmiotowa czynu sprowadza się do umyślnego działania sprawcy, tak więc może być ono popełnione zarówno w zamiarze bezpośrednim, jak i ewentualnym. Przykładem działania w zamiarze bezpośrednim będzie ujawnienie osobie nieuprawnionej dokumentu o klauzuli *ściśle tajne*, wtedy tylko, gdy sprawca ma pełną świadomość, że treść ujawnionego dokumentu stanowi tajemnicę państwową i wolę udostępnienia tego dokumentu osobie nieuprawnionej. Natomiast niewłaściwa ochrona takiego dokumentu i stworzenie w ten sposób możliwości zapoznania się z jego treścią osoby nieupoważnionej – to zamiar ewentualny.

Przedmiotem ujawnienia, o którym mowa w art. 265, § 1 kk jest informacja stanowiąca tajemnicę państwową. Definicja tajemnicy państwowej, do której odnosi się art. 2, pkt 1 Ustawy o ochronie informacji niejawnych, jest w stosunku do poprzedniego stanu prawnego rozwiązaniem nowym, ma bowiem charakter materialno-formalny. I tak informacja podlegająca ochronie jest tajemnicą państwową jeżeli spełnia łącznie dwa warunki:

- mieści się w wykazie rodzajów informacji niejawnych stanowiących tajemnicę państwową (Załącznik nr 1 do ustawy o ochronie informacji niejawnych);
- jej ujawnienie może doprowadzić do poważnego zagrożenia podstawowych interesów RP albo narazić te interesy na co najmniej znaczną szkodę.

Sformułowana w ten sposób definicja tajemnicy państwowej rodzi domniemanie, iż dokument opatrzony cechą tajności zawiera informacje, których ujawnienie może doprowadzić do poważnego zagrożenia podstawowych interesów RP albo narazić te interesy na co

najmniej znaczną szkodę. W postępowaniu karnym domniemanie to może być obalone przez udowodnienie, że mimo cechy tajności, ujawnienie treści dokumentu w istocie nie powoduje szkód dla podstawowych interesów RP.

Nowe rozwiązanie, polegające na zamieszczeniu w ustawie, w formie załącznika, wykazu rodzajów informacji stanowiących tajemnicę państwową, stwarza znacznie dogodniejszą sytuację dowodową w postępowaniu karnym, niż w czasie obowiązywania Ustawy o ochronie tajemnicy państwowej i służbowej z dnia 14 grudnia 1982 r. Obecnie nikt nie może tłumaczyć się nieznajomością prawa, co w poprzednim stanie prawnym było powszechnie stosowaną metodą obrony. Sytuacja taka był możliwa ze względu na fakt, że wykaz wiadomości stanowiących tajemnicę państwową opatrzony był klauzulą tajności, a więc dostęp do nich był ograniczony – teraz wykaz jest jawny i dostęp do niego jest powszechny.

W obowiązującym kodeksie karnym nie zostały **stypizowane przestępstwa ujawnienia tajemnicy państwowej w postaci kwalifikowanej ze względu na treść informacji oznaczonych klauzulą ściśle tajne**. W poprzednim stanie prawnym (art. 260, § 2 kk z 1969 r.) ujawnienie wiadomości tajnych specjalnego znaczenia stanowiło kwalifikowaną postać przestępstwa, a sprawca takiego czynu ponosił surowszą odpowiedzialność niż za ujawnienie informacji oznaczonych klauzulą *tajne*. Według nowych przepisów (art. 265, § 1 kk.) sprawcy grozi kara pozbawienia wolności od 3 miesięcy do 5 lat bez względu na to, czy ujawnił informację ściśle tajną, czy tajną. W tej sytuacji zróżnicowanie odpowiedzialności karnej może jedynie nastąpić w ramach sądowego wymiaru kary.

Typ kwalifikowany występku ujawnienia tajemnicy państwowej polega na nieuprawnionym ujawnieniu takiej informacji osobie działającej w imieniu lub na rzecz podmiotu zagranicznego (art. 265, § 2 kk). Znajduje to wyraz w wyższej sankcji karnej (od 6 miesięcy do 8 lat pozbawienia wolności). Według poprzedniego stanu prawnego, czyn był zbrodnią zagrożoną karą od 3 do 15 lat pozbawienia wolności.

Analogicznie jak w omówionym wyżej § 1, art. 265, przestępstwo to może być popełnione wyłącznie z winy umyślnej. Istota kwalifikowanej postaci ujawnienia tajemnicy państwowej, sprowadza się do specyficznego odbiorcy tej informacji – może nim być wyłącznie

osoba działająca w imieniu lub na rzecz podmiotu zagranicznego. **Przepis ma zastosowanie tylko wówczas, gdy zagranicznym podmiotem, do którego informacja dociera, nie jest obcy wywiad.** Działania na rzecz obcego wywiadu, przez udzielanie mu informacji mogących wyrządzić szkodę RP, stanowi odrębną kategorię przestępstwa – zbrodnię szpiegostwa, zagrożoną karą pozbawienia wolności na czas nie krótszy od 3 lat (art. 130, § 2 kk).

Kodeks karny, **oprócz postaci podstawowej i kwalifikowanej, określa również uprzywilejowaną – ze względu na nieumyślność – postać przestępstwa ujawnienia tajemnicy państwowej** (art. 265, § 3 kk), co znalazło wyraz w niższej sankcji karnej za popełnienie tego typu występku (grzywna, ograniczenie wolności, pozbawienie wolności do roku). Poza nieumyślnością przestępstwo charakteryzuje się określonym w sposób szczególny podmiotem. **Za nieumyślne ujawnienie informacji stanowiących tajemnicę państwową może odpowiadać jedynie osoba zobowiązana do ich ochrony, która zapoznała się z ich treścią z tytułu pełnienia funkcji publicznej lub posiadania poświadczenia bezpieczeństwa.** Przestępstwo to może być popełnione np. przez ministra, posła, senatora albo inną osobę, która w wyniku postępowania sprawdzającego uzyskała odpowiednie poświadczenie bezpieczeństwa osobowego, jeżeli nie zachowała należytej ostrożności i przez to doprowadziła do ujawnienia informacji tajnych osobie nieuprawnionej. Na podstawie tego przepisu odpowiadać będzie również osoba, która zagubiła dokument oznaczony klauzulą *tajne*, ale poniesie ona odpowiedzialność karną tylko wtedy, gdy dojdzie do ujawnienia zawartych w nim informacji. Należy udowodnić nie tylko zagubienie dokumentu, lecz także ujawnienie jego treści osobie nieuprawnionej. W kodeksie karnym z 1969 r. (art. 261) omawiane przestępstwo miało charakter formalny – do jego znamion nie należało ujawnienie treści zagubionego dokumentu, wystarczyło udowodnić jedynie fakt jego utraty lub zagubienia.

5.1.2. Wyłączenie odpowiedzialności karnej za ujawnienie tajemnicy państwowej

Za ujawnienie informacji stanowiących tajemnicę państwową nie ponoszą odpowiedzialności osoby, które z mocy prawa są upoważnione do udostępniania takich informacji określonym podmiotom, a także osoby zwolnione z obowiązku zachowania tajemnicy państwowej.

Ustawa o ochronie informacji niejawnych (art. 49, ust. 1) upoważnia naczelne i centralne organy administracji rządowej do udostępniania informacji stanowiących tajemnicę państwową określonej osobie lub instytucji w szczególnie uzasadnionych przypadkach. Informacje takie mogą być udostępniane na podstawie pisemnej decyzji, z zachowaniem posiadanej klauzuli, np. sądom lub prokuratorowi.

Naczelne i centralne organy administracji rządowej są również upoważnione do zwalniania z obowiązku zachowania tajemnicy państwowej osoby przesłuchiwane w postępowaniu karnym w charakterze świadków (art. 179, § 1 kpk). Zwolnienia można odmówić, gdy złożenie zeznań mogłoby wyrządzić poważną szkodę państwu. Udzielając zgody należy określić zakres zwolnienia z obowiązku zachowania tajemnicy państwowej. Udostępnienie informacji tajnych osobie uprawnionej w trybie, o którym mowa w art. 49, ust. 1 ustawy, a także złożenie zeznań co do okoliczności zawierających w treści informacje stanowiące tajemnicę państwową, w trybie określonym w art. 179, § 1 kpk nie stanowi przestępstwa ujawnienia tajemnicy państwowej.

Reasumując należy stwierdzić, że za ujawnienie tajemnicy państwowej mogą odpowiadać przede wszystkim osoby uprawnione do dostępu do informacji niejawnych tej kategorii, jeśli świadomie przekażą informację stanowiącą tajemnicę państwową osobie nieuprawnionej, bądź umożliwią jej dostęp do tajemnicy wskutek niezachowania należytej ostrożności. Popęlni także przestępstwo poseł, senator, minister czy funkcjonariusz ABW, który przekaże dziennikarzowi dokument o klauzuli *ściśle tajne*, zawierający informacje objęte wykazem stanowiącym załącznik nr 1 do ustawy. Ujawni tajemnicę państwową dziennikarz czy pracownik naukowy, który za zgodą uprawnionego organu uzyskał dostęp do informacji o najwyż-

szym stopniu tajności i ujawnił je wbrew przyjętemu zobowiązaniu zachowania tajemnicy.

Za bezprawne wykorzystanie tajemnicy państwowej może ponieść odpowiedzialność publicysta, przedsiębiorca lub urzędnik, który posłuży się informacją stanowiącą tajemnicę państwową – ujawnioną wcześniej przez inną osobę – w sposób niezgodny z przepisami ustawy, np. rozpowszechni taką informację lub wykorzysta ją w jawnych negocjacjach handlowych.

5.1.3. Przestępstwo ujawnienia informacji stanowiących tajemnicę służbową

Zgodnie z przepisami Ustawy o ochronie informacji niejawnych do prawnie chronionych informacji należą również te, które stanowią tajemnicę służbową. Ujawnienie tajemnicy służbowej – to przestępstwo z art. 266, § 2 kk. **Podmiotem tego indywidualnego występku może być wyłącznie funkcjonariusz publiczny**, a więc osoba pełniąca funkcje publiczne – poseł, senator, sędzia, pracownik administracji rządowej, funkcjonariusz ABW, Policji (art. 115, § 13 kk).

Przestępstwo to jest umyślnym występkiem; nieumyślne ujawnienie informacji stanowiących tajemnicę służbową nie podlega odpowiedzialności karnej.

Istota tego czynu sprowadza się do przekazania osobie nieuprawnionej informacji stanowiących tajemnicę służbową lub uzyskanych w związku z wykonywaniem czynności służbowych, gdy ich ujawnienie może narazić na szkodę prawnie chroniony interes – publiczny, obywatela lub jednostki organizacyjnej.

Ujawnienie tajemnicy służbowej nie występuje w kodeksie karnym w postaci kwalifikowanej ze względu na przekazanie informacji poza granice kraju (art. 264, § 2 kk z 1969 r.). Ustawa o ochronie informacji niejawnych nie zawiera wykazu informacji stanowiących tajemnicę służbową.

Kodeks karny przewiduje natomiast (art. 266, § 1) odpowiedzialność karną za ujawnienie chronionej ustawowo tajemnicy, innej niż tajemnica państwowa czy służbowa. Przedmiotem ochrony jest – prócz tajemnicy służbowej i zawodowej – szczególny rodzaj tajemnicy, która wynika z przyjętego zobowiązania do zachowania

poufności. Przykładem może być informacja, którą powierzono osobie prowadzącej badania naukowe, zobowiązując ją do dochowania tajemnicy – nie jest to tajemnica służbowa ani zawodowa, lecz podlega ochronie na mocy art. 266, § 1 kk. Odpowiedzialność z tego artykułu poniesie również osoba nie będąca funkcjonariuszem publicznym, która ujawniła informacje stanowiące tajemnicę służbową udostępnione jej w związku z wykonywaną pracą.

Usankcjonowanie innych niż tajemnica państwowa i służbowa rodzajów tajemnicy jest rozwiązaniem nowym, nie mającym swojego odpowiednika w poprzednio obowiązującym kodeksie karnym. Za przestępstwo to grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Ściganie tego występkę następuje na wniosek pokrzywdzonego.

5.1.4. Wyłączenie odpowiedzialności karnej za ujawnienie informacji stanowiących tajemnicę służbową

Za ujawnienie informacji poufnej nie ponoszą odpowiedzialności karnej osoby, które z mocy prawa są upoważnione do udostępniania takich wiadomości, a także osoby zwolnione z obowiązku zachowania tajemnicy służbowej. Ustawa (art. 49, ust. 2) upoważnia kierownika jednostki organizacyjnej do udostępniania informacji stanowiących tajemnicę służbową wytworzonych w danej jednostce.

W postępowaniu karnym z obowiązku zachowania tajemnicy służbowej mogą być zwolnione osoby przesłuchiwane w charakterze świadków. Do podjęcia takiej decyzji uprawniony jest sąd lub prokurator.

Udostępnienie informacji poufnych, w trybie o którym mowa w art. 49, ust. 2 ustawy, a także złożenie zeznań co do okoliczności zawierających w treści informacje stanowiące tajemnicę służbową, w trybie określonym w art. 180, § 1 kpk, nie stanowi przestępstwa ujawnienia tajemnicy służbowej.

Za ujawnienie tajemnicy służbowej mogą karne odpowiadać poseł, senator, minister oraz inne osoby, jeśli posiadają status funkcjonariusza publicznego.

5.1.5. Przestępstwo nielegalnego uzyskania informacji

Sankcji karnej za ujawnienie tajemnicy państwowej lub służbowej podlegają sprawcy dopuszczający się nieupoważnionego przekazania chronionych informacji osobie nieuprawnionej. Natomiast osoba uzyskująca taką informację, jeśli nie przekaze jej innej osobie (nie ujawni), nie ponosi odpowiedzialności karnej.

Kodeks karny sankcjonuje nowy typ przestępstwa, wprowadzając w art. 267, § 1 odpowiedzialność karną za nielegalne uzyskanie informacji. Istota tego przestępstwa sprowadza się do uzyskania informacji prawnie chronionych oraz przełamania zabezpieczeń mających na celu ich ochronę.

Uzyskanie informacji oznacza zapoznanie się z jej treścią i jest nielegalne tylko wówczas, gdy następuje w wyniku:

- otwarcia zamkniętego pisma,
- podłączenia się do przewodu służącego do przekazywania informacji (linii telefonicznej, sieci komputerowej),
- przełamania zabezpieczeń elektronicznych, magnetycznych lub usunięcia czy sforsowania innych specjalnych środków ochronnych, zastosowanych w celu uniemożliwienia nieuprawnionego dostępu do informacji (kod, hasło, szyfr).

Przestępstwo to jest umyślnym występkiem, może być popełnione przez każdego – kara – grzywna, ograniczenie wolności lub pozbawienie wolności do lat 2.

Analizowany przepis to rozwiązanie nowe na gruncie polskiego prawa karnego, mające na celu lepsze zabezpieczenie informacji prawnie chronionych, również ze sfery życia prywatnego obywateli (art. 49 konstytucji RP). Wzorem były regulacje prawne z lat 80., obowiązujące w państwach europejskich. W latach 90., w związku ze szkodami wyrządzonymi przez hakerów, zmodyfikowano odpowiedzialność karną za takie czyny. Obecnie, np. w Wielkiej Brytanii, odpowiedzialności karnej podlega już samo przełamanie zabezpieczeń stosowanych w urządzeniach elektronicznych czy magnetycznych. Dla bytu tego przestępstwa nie ma znaczenia, czy sprawca po przełamaniu zabezpieczeń (hasła, kodu) zapoznał się z treścią informacji przechowywanej w pamięci komputera.

Nielegalne uzyskanie informacji może również polegać na użyciu do tego celu urządzenia podsłuchowego, wizualnego lub innego

urządzenia specjalnego. Przepis opisane w art. 267, § 2 kk jest występkiem celowościowym i może być popełnione wyłącznie w zamiarze bezpośrednim.

Przepis nie odnosi się do podmiotu instalującego podsłuch, podgląd czy inne urządzenie specjalne, zgodnie z ustawowymi uprawnieniami do zastosowania tego typu środków.

Odpowiedzialności karnej podlega także ujawnienie innej osobie nielegalnie uzyskanej informacji (art. 267, § 3 kk).

Omówione wyżej rodzaje przestępstwa nielegalnego uzyskania informacji są ścigane na wniosek pokrzywdzonego.

Odpowiedzialność karłą za nielegalne uzyskanie informacji może zatem ponieść zarówno funkcjonariusz publiczny, jak i inna osoba, która weszła w posiadanie informacji po przełamaniu zabezpieczeń, np. listonosz otwierający zamkniętą korespondencję, „pajęczarz” podłączający się do sieci telefonicznej, haker przełamujący hasła, kody i wchodzący nielegalnie do bazy danych systemu teleinformatycznego.

5.1.6. Przestępstwo niszczenia informacji

Stypizowanie w § 1, art. 268 kk przestępstwo niszczenia informacji ma na celu ochronę integralności zapisu utrwalającego informacje oraz zapewnienie ich dostępności, czyli możliwości swobodnego korzystania z informacji przez osoby uprawnione. Przepis chroni nie każdą informację, lecz jedynie tę, która jest informacją istotną w znaczeniu obiektywnym. Podmiotem tego umyślnego występkę może być każdy, kto nie jest uprawniony do dokonywania zmian w zapisie informacji.

Istota tego przestępstwa polega na niszczeniu, uszkodzeniu, usuwaniu albo zmianie zapisu istotnej informacji, a także innym działaniu udaremniającym lub znacznie utrudniającym osobie uprawnionej zapoznanie się z tymi informacjami. Czyn zagrożony jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

Kwalifikowany typ przestępstwa, ze względu na znaczną szkodę, jaka powstała w wyniku zniszczenia, został określony w § 2, art. 268 kk. Przepis dotyczy zapisu na komputerowym nośniku

informacji i z uwagi na tę okoliczność sankcja karna została zaostrzona do 3 lat pozbawienia wolności.

Naruszenie integralności zapisu komputerowego jest przestępstwem umyślnym, które może być popełnione zarówno w zamiarze bezpośrednim, jak i ewentualnym. Nie jest natomiast przestępstwem nieumyślnie przeniesienie do cudzego komputera wirusów komputerowych na skutek niezachowania należytej ostrożności. Warunkiem odpowiedzialności za dokonanie tego przestępstwa jest udaremnienie lub znaczne utrudnienie osobie uprawnionej zapoznania się z informacją. Nie każdy przypadek „zawirusowania” komputera warunkiem ten będzie spełniał. Zniszczenie lub usunięcie zapisu informacji nie będzie stanowiło przestępstwa z art. 268, § 2 kk jeśli np. pokrzywdzony dysponuje kopią zapisu (dyskietką).

Kwalifikowany, ze względu na znaczną szkodę majątkową, typ przestępstwa zniszczenia informacji określa § 3, art. 268 kk. Szkodę uznaje się za znaczną, jeżeli straty poniesione w jej wyniku przekraczają dwustukrotną wysokość najniższego miesięcznego wynagrodzenia (art. 115, § 7 w zw. z § 5 i 6 kk). Ten typ przestępstwa zagrożony jest karą pozbawienia wolności od 3 miesięcy do lat 5.

Omówione rodzaje przestępstwa niszczenia informacji ścigane są na wniosek pokrzywdzonego.

Odpowiedzialność karłą za niszczenie informacji (art. 268 kk) poniesie zarówno funkcjonariusz publiczny, jak i inna osoba, która nie posiadając uprawnień dokonuje zmian w komputerowej bazie danych, co prowadzi do zniekształcenia informacji, a w konsekwencji – do uniemożliwienia osobom uprawnionym korzystanie z zasobów tej bazy.

5.1.7. Przestępstwo sabotażu komputerowego

Naruszenie integralności zapisu komputerowego informacji należy również do znamion przestępstwa określonego jako sabotaż komputerowy (art. 269 kk). Z występką tym mamy do czynienia wówczas, gdy zmieniony bądź uszkodzony został zapis informacji o szczególnie znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej lub samorządowej. Istotą sabotażu komputerowego jest także działanie zakłócające lub

uniemożliwiające automatyczne gromadzenie bądź przekazywanie informacji. Przestępstwo to jest umyślnym występkiem, za który grozi kara pozbawienia wolności od 6 miesięcy do lat 8.

Sprawca zamachu na funkcjonowanie urządzeń służących do gromadzenia i transmisji danych poniesie odpowiedzialność karną jeżeli:

- dojdzie do zakłóceń lub uniemożliwienia automatycznego gromadzenia albo przekazywania informacji chronionej przez te przepisy;
- można będzie postawić zarzut, że sprawca przewidywał lub co najmniej godził się na wywołanie tego rodzaju następstw.

Niszczenie nośnika informacji (np. dyskietki), a także niszczenie lub uszkodzenie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przesyłania informacji stanowi odrębny typ przestępstwa sabotażu komputerowego (art. 269, § 2 kk). Czyn jest umyślnym występkiem, zagrożony karą analogiczną jak w art. 269, § 1 kk. O odpowiedzialności karnej mówimy wówczas, gdy istotnie doszło do zakłóceń w gromadzeniu bądź przekazie informacji, a sprawca przewidywał takie następstwa lub co najmniej się na nie godził.

Przestępstwo sabotażu komputerowego może popełnić zarówno funkcjonariusz publiczny, jak i inna osoba, która zniszczy utrwaloną na nośniku komputerowym informację o szczególnym znaczeniu, np. dla służb specjalnych, Ministerstwa Obrony Narodowej czy funkcjonowania innych podmiotów administracji rządowej.

5.2. Odpowiedzialność dyscyplinarna i służbowa

Konsekwencją naruszenia przepisów ustawy o ochronie informacji niejawnych, obok odpowiedzialności karnej, może być odpowiedzialność dyscyplinarna i służbowa.

Odpowiedzialności dyscyplinarnej podlegają pracownicy, których stosunek pracy został zawarty w drodze mianowania, a ich uprawnienia i obowiązki są określone w odrębnych ustawach – pragmatykach. Tego rodzaju odpowiedzialność ponoszą przede wszystkim następujące grupy pracownicze:

- **urzędnicy służby cywilnej** zatrudnieni w urzędach administracji rządowej, np. w ministerstwach (Ustawa o służbie cywilnej z dnia 18 grudnia 1998 r., DzU z 1999 r., nr 49, poz. 483 ze zm.);

- **urzędnicy państwowi** zatrudnieni w:

- kancelariach: sejmu, senatu, prezydenta RP i prezesa RM;
- Krajowym Biurze Wyborczym oraz biurach: Trybunału Konstytucyjnego, Rzecznika Praw Obywatelskich, Krajowej Rady Radiofonii i Telewizji, Rzecznika Interesu Publicznego, Generalnego Inspektora Ochrony Danych Osobowych;

- Państwowej Inspekcji Pracy oraz Instytucie Pamięci Narodowej – Głównej Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
- ministerstwach oraz centralnych i terenowych organach administracji państwowej (Ustawa o pracownikach urzędów państwowych z dnia 16 września 1982 r., DzU nr 31, poz. 214 ze zm.);

- **mianowani pracownicy samorządowi** (Ustawa o pracownikach samorządowych z dnia 22 marca 1990 r., DzU nr 21, poz. 124 ze zm.);

- **pracownicy organów kontroli państwowej**, w tym zatrudnieni w NIK (Ustawa o Najwyższej Izbie Kontroli z dnia 23 grudnia 1994 r., DzU nr 13, poz. 59 ze zm.);

- **prokuratorzy** (Ustawa o prokuraturze z dnia 20 czerwca 1985 r., DzU nr 13, poz. 59 ze zm.);

- **sędziowie** (Ustawa prawo o ustroju sądów powszechnych z dnia 27 lipca 2001 r., DzU nr 98, poz. 1070);

- **funkcjonariusze Inspekcji Celnej** (Ustawa z dnia 7 lipca 1997 r., DzU nr 71, poz. 449 ze zm.);

- **funkcjonariusze ABW, AW, Policji, Straży Granicznej.**

Odpowiedzialność dyscyplinarną ponoszą prawnie określone grupy podmiotów za przewinienia dyscyplinarne, których istotą jest niewypełnianie obowiązków wynikających z pragmatyk, a także za popełnienie przestępstwa.

Wśród obowiązków wymienianych we wszystkich pragmatykach główne miejsce zajmuje obowiązek zachowania tajemnicy państwowej i służbowej. Niewypełnienie tego obowiązku polegające na naruszeniu przepisów zachowania tajemnicy, jeżeli występują ustawowe znamiona przestępstwa, podlega odpowiedzialności karnej, która nie wyklucza odpowiedzialności dyscyplinarnej. Organami właściwymi do orzekania w sprawach dyscyplinarnych są komisje dyscyplinarne działające w systemie II – instancyjnym. Organami właściwymi do

prowadzenia postępowań dyscyplinarnych są również przełożeni służbowi – dotyczy to głównie funkcjonariuszy służb zmilitaryzowanych.

W wyniku postępowania dyscyplinarnego mogą być wymierzone następujące kary:

- upomnienie,
- nagana,
- nagana z pozbawieniem możliwości awansu,
- przeniesienie na niższe stanowisko,
- zakaz zajmowania stanowisk kierowniczych w służbie cywilnej,
- obniżenie kategorii urzędniczej,
- wydalenie z pracy w urzędzie.

Odpowiedzialność dyscyplinarna nie zawsze musi być łączona z odpowiedzialnością karną, ponieważ nie każde przewinienie służbowe jest przestępstwem.

Postępowanie dyscyplinarne może być zatem prowadzone także samoistnie i zakończyć się wymierzeniem jednej z kar dyscyplinarnych:

– funkcjonariusz Inspekcji Celnej, który przekaze osobie nieuprawnionej informację uzyskaną w wyniku czynności operacyjno-rozpoznawczych, popełnia zarówno przestępstwo, jak i przewinienie służbowe. Może być ukarany przez sąd karą pozbawienia wolności do lat 5, a w ramach postępowania dyscyplinarnego – karą wydalenia ze służby,

– pracownik, który zagubi powierzony mu dokument zawierający informacje objęte ochroną, jeżeli ich treść nie dotarła do osoby nieupoważnionej, ponosi wyłącznie odpowiedzialność dyscyplinarną i może być ukarany, np. naganą lub przeniesieniem na niższe stanowisko służbowe.

Odpowiedzialność służbową ponoszą wszyscy pracownicy, bez względu na sposób nawiązania stosunku pracy, przed przełożonymi służbowymi. Istota tej odpowiedzialności sprowadza się do możliwości pozbawienia pracownika premii, awansu, ukarania go wystawieniem negatywnej opinii aż do zwolnienia z pracy łącznie.

W zależności od rodzaju przewinienia odpowiedzialność służbową może wystąpić samoistnie lub łącznie z odpowiedzialnością karną i dyscyplinarną:

- pracownik pionu ochrony, który niewłaściwie zabezpiecza dokumenty prawnie chronione, przechowuje je luzem, bez segregatorów z opisem zawartości – może ponieść odpowiedzialność służbową w postaci pozbawienia premii – jeżeli natomiast dojdzie do zagubienia dokumentu, może ponieść dodatkowo odpowiedzialność dyscyplinarną w postaci np. nagany. W przypadku gdy treść zagubionego dokumentu zawierającego informacje stanowiące tajemnicę państwową dotrze do osoby nieuprawnionej, może nastąpić kumulacja odpowiedzialności karnej, dyscyplinarnej i służbowej, co w konsekwencji doprowadzi do wymierzenia kar, np. roku pozbawienia wolności z zawieszeniem wykonania kary, obniżenia zajmowanego stanowiska służbowego i pozbawienia premii.

5.3. Odpowiedzialność za naruszenie przepisów procedury sprawdzeniowej

Naruszenie przepisów regulujących zasady i tryb postępowania sprawdzającego może stanowić przestępstwo lub przewinienie dyscyplinarne.

Naruszeniem tajemnicy służbowej będzie np. udostępnienie osobie nieupoważnionej treści ankiety bezpieczeństwa osobowego. Osoba, która dopuści się tego umyślnego występku (art. 266, § 2 kk) poniesie odpowiedzialność karną wówczas, gdy ujawnienie danych zawartych w ankiecie naruszy prawnie chroniony interes osoby sprawdzanej lub jednostki organizacyjnej. Wykorzystanie informacji chronionych ustawą o ochronie danych osobowych (art. 266, § 1 i 3 kk), uzyskanych w wyniku postępowania sprawdzającego, będzie również przestępstwem ujawnienia tajemnicy służbowej. Warunkiem odpowiedzialności karnej jest złożenie przez pokrzywdzonego wniosku o ściganie.

Zniszczeniem informacji będzie np. usunięcie informacji uzyskanych w wyniku postępowania sprawdzającego z komputerowej bazy danych, jeżeli uniemożliwi to korzystanie z gromadzonych w ten sposób zasobów (art. 268 kk). Sprawca dopuszczający się tego umyślnego występku poniesie surowszą odpowiedzialność karną, gdy w wyniku zniszczenia informacji nastąpi znaczna szkoda majątkowa.

Ponadto funkcjonariusz ABW, Policji czy Straży Granicznej, który w toku postępowania sprawdzającego:

- **przekroczy swoje uprawnienia lub nie dopełni ustawowych obowiązków, popełnia przestępstwo nadużycia funkcji** (art. 231 kk)

Przekracza swoje uprawnienia funkcjonariusz publiczny, który podejmuje działania nie mieszczące się w zakresie kompetencji przynależnych jego funkcji lub działa w ramach kompetencji, lecz nie zgodnie z ich treścią. Niedopełnienie obowiązku polega bądź na całkowitym zaniechaniu wypełnienia obowiązku nałożonego z racji pełnienia funkcji publicznej, bądź na wykonaniu obowiązku niezgodnie z jego treścią. Jest to tzw. przestępstwo urzędnicze, którego podmiotem może być wyłącznie funkcjonariusz publiczny, a przedmiotem przekroczenie uprawnień lub niedopełnienie obowiązków ze szkodą dla interesu publicznego czy prywatnego. Nie jest przy tym konieczne wyrządzenie szkody, wystarczy działanie na szkodę, stwarzanie warunków do jej powstania. Surowsza kara jest przewidziana w przypadku niedopełnienia obowiązków lub przekroczenia uprawnień w celu osiągnięcia korzyści majątkowej lub osobistej (do 10 lat pozbawienia wolności).

- **przyjmie korzyść majątkową lub takiej korzyści zażąda, poniesie odpowiedzialność karną za przestępstwo biernego przekupstwa** (art. 228 kk).

Odpowiada z art. 228 kk ten funkcjonariusz publiczny, który przyjmie korzyść majątkową lub osobistą, czyli staje się odbiorcą wręczonej mu łapówki. Czyn taki może mieć charakter prostego, fizycznego przyjęcia korzyści (np. odbioru przekazanej do ręki gotówki), albo postać bardziej złożoną (gdy korzyść została przysporzona w inny sposób).

Czyn z art. 228 kk może również polegać na przyjęciu obietnicy korzyści bądź żądaniu korzyści przez funkcjonariusza publicznego. W drugim przypadku nie jest istotne, czy osoba do której kierowane było żądanie, spełniła je, ponieważ już samo wyrażenie przez funkcjonariusza takiego żądania jest dokonaniem przestępstwa z art. 228 kk.

Słowo „żądać” oznacza domagać się czegoś, usilnie dopominać się o coś, wymagać; żądanie to życzenie wyrażone w kategorycznej formie. Dla oceny, czy zachowanie sprawcy było w istocie żądaniem, ważny jest kontekst zdarzenia, a zwłaszcza sytuacja osoby, do której żądanie zostało skierowane.

Przyjęcie lub żądanie korzyści musi być związane z pełnieniem funkcji publicznej, a więc załatwieniem spraw należących do obowiązków funkcjonariusza. Surowszą odpowiedzialność poniesie ten funkcjonariusz, który uzależni wynik postępowania sprawdzającego od wartości korzyści (do 10 lat pozbawienia wolności).

- **poświadczy nieprawdę co do okoliczności istotnych dla uzyskania poświadczenia bezpieczeństwa, popełnia przestępstwo, za które grozi surowsza kara, jeżeli było ono dokonane w celu osiągnięcia korzyści majątkowej lub osobistej** (art. 271 kk).

Podmiotem przestępstwa może być, poza funkcjonariuszem publicznym, także inna osoba upoważniona do wystawienia dokumentu.

Poświadczenie nieprawdy oznacza potwierdzenie faktów lub okoliczności niezgodnych z prawdą. Polegać może, zarówno na poręczeniu danych samym tylko podpisem złożonym na dokumencie, jak i sporządzeniu, całego dokumentu.

Przestępstwo z art. 271 kk może być popełnione wyłącznie umyślnie – sprawca musi mieć świadomość, że potwierdza fakty lub okoliczności niezgodne ze stanem faktycznym i że skutek takiego postępowania będzie miał znaczenie prawne.

ZAKOŃCZENIE

Rosnące znaczenie informacji we współczesnym świecie oraz rozwój techniki ułatwiający jej szybkie przekazywanie, doprowadziły do urynkowienia wszelkiego rodzaju informacji. W tej sytuacji stała się ona przedmiotem obrotu mającym swoistą wartość. Podmioty będące jej wytwórcami, jak i dysponentami w coraz większym stopniu zainteresowane są jej kompleksową ochroną. W tym kontekście szczególne znaczenie przypada informacjom niejawnym dotyczącym obronności i bezpieczeństwa państwa.

W Polsce nowoczesny system ochrony informacji niejawnych – dostosowany do standardów NATO – określa Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych oraz wydane do niej akty wykonawcze. Ustawa, poza nowym ujęciem problematyki ochrony i postępowania z informacjami niejawnymi, normuje zasady dostępu do tajemnic, reguły nadawania informacjom cech tajności, a ponadto zawiera rozwiązania instytucjonalne – wprost wskazuje podmioty odpowiedzialne za ochronę tajemnic.

Stworzony w Polsce system ochrony informacji niejawnych, wzorowany na rozwiązaniach NATO, zachował jednak pewne cechy autonomii i odpowiada lokalnym rozwiązaniom. Na uwagę zasługuje choćby odmienna rola pełnomocnika ochrony w postępowaniu sprawdzającym czy struktura kancelarii tajnych. Główne jednak założenia systemu, mechanizmy zabezpieczania informacji, pozostały zgodne z dyrektywami Kwatery Głównej NATO. Przyjęte rozwiązanie stanowi gwarancję, że zarówno informacje niejawne wymieniane przez organy i agencje Sojuszu, jak i pomiędzy państwami członkowskimi, będą w jednakowym stopniu i z równą starannością chronione.

System ochrony informacji niejawnych obowiązujący w Polsce musi być również dostosowany do wymogów Unii Europejskiej. W kwietniu 2003 r. rząd RP podpisał traktat akcesyjny dokumentujący nasze członkostwo w strukturach UE. Nastąpiła wymiana listów pomiędzy Sekretarzem Generalnym Rady UE/Wysokim Przedstawicielem ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa a polskim ministrem spraw zagranicznych, na mocy której rząd RP zobowiązał się do przestrzegania decyzji Rady UE, głównie w za-

kresie wymiany informacji klasyfikowanych. Obecnie wciąż trwają prace nad wypracowaniem szczegółowych rozwiązań znajdujących potwierdzenie w przepisach i dostosowanych do uwarunkowań naszego państwa.

ANEKS

Wykres 1. Współdziałanie organów i jednostek organizacyjnych w dziedzinie ochrony informacji niejawnych

Wykres 2. Ramowy układ czynności w poszerzonym i specjalnym postępowaniu sprawdzającym

Wykres 3. Procedura odwoławcza od odmowy wydania poświadczenia bezpieczeństwa

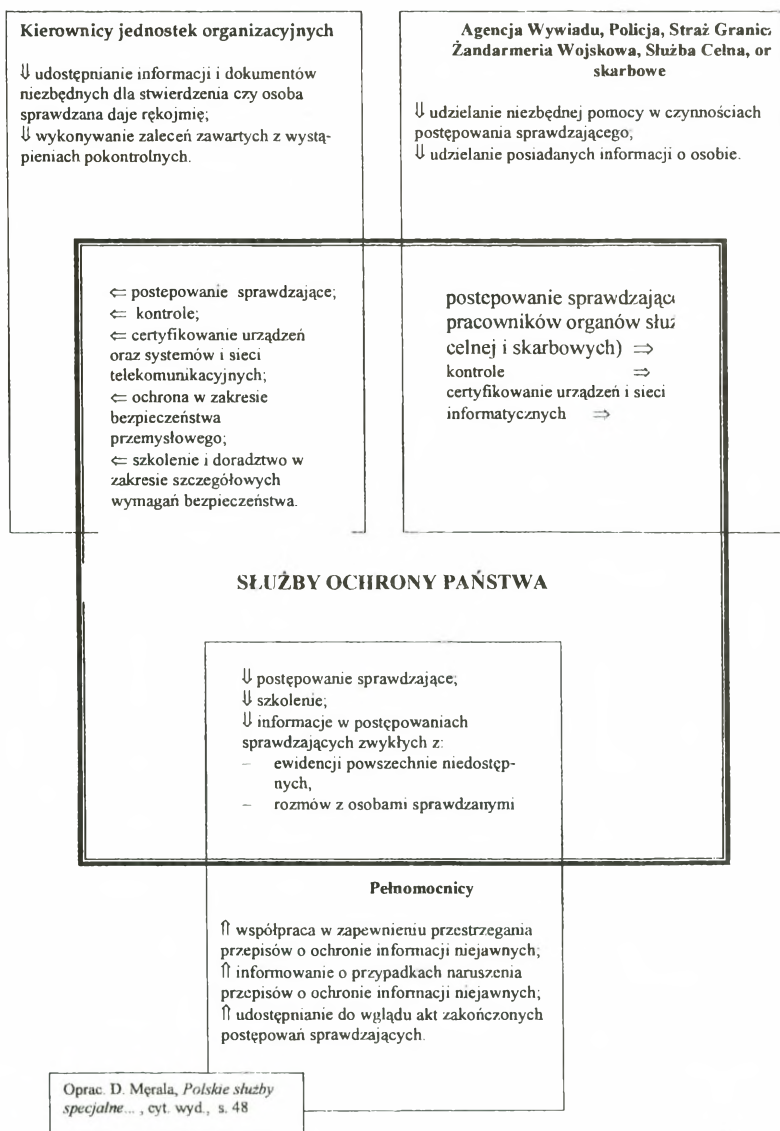
Wykres 4. Ramowy układ czynności w procedurach odwoławczych od odmów wydania poświadczenia bezpieczeństwa

Wykres 5. Tryb skargowy do NSA w przedmiocie odmowy wydania poświadczenia bezpieczeństwa
obowiązujący do 31.12.2003 r.

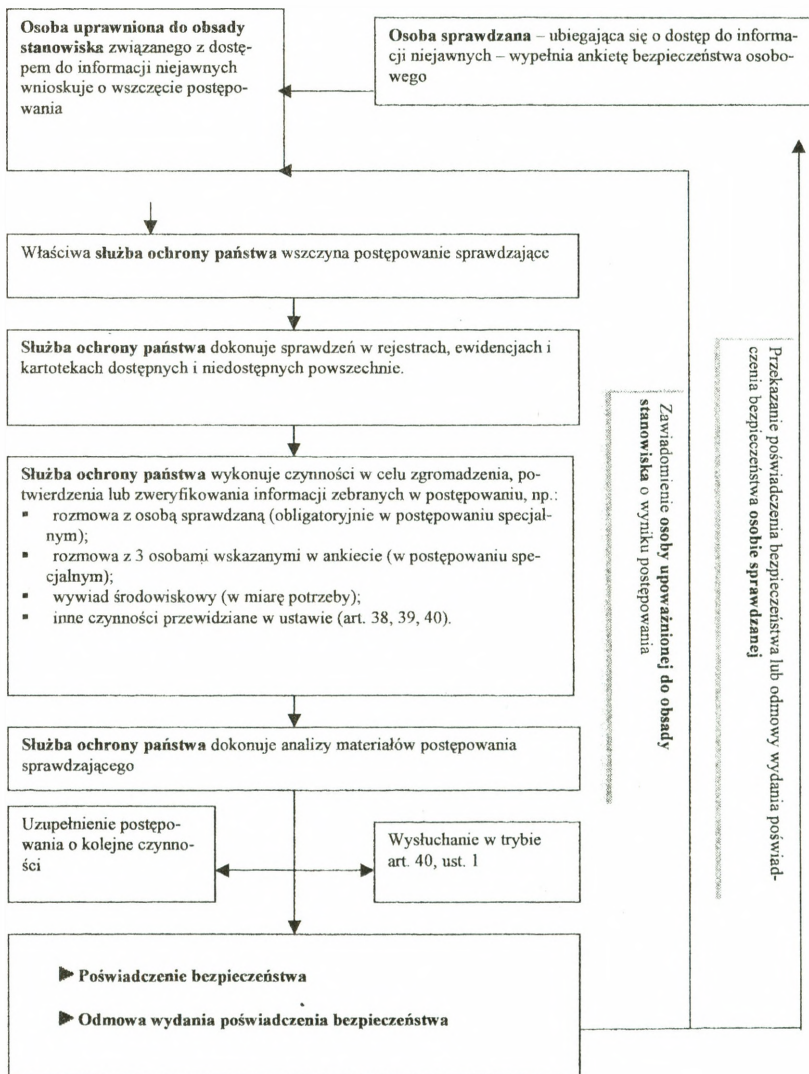
Wykres 6. Tryb skargowy do sądu administracyjnego w przedmiocie odmowy wydania poświadczenia bezpieczeństwa
obowiązujący od 1.01.2004 r.

Wykres 1

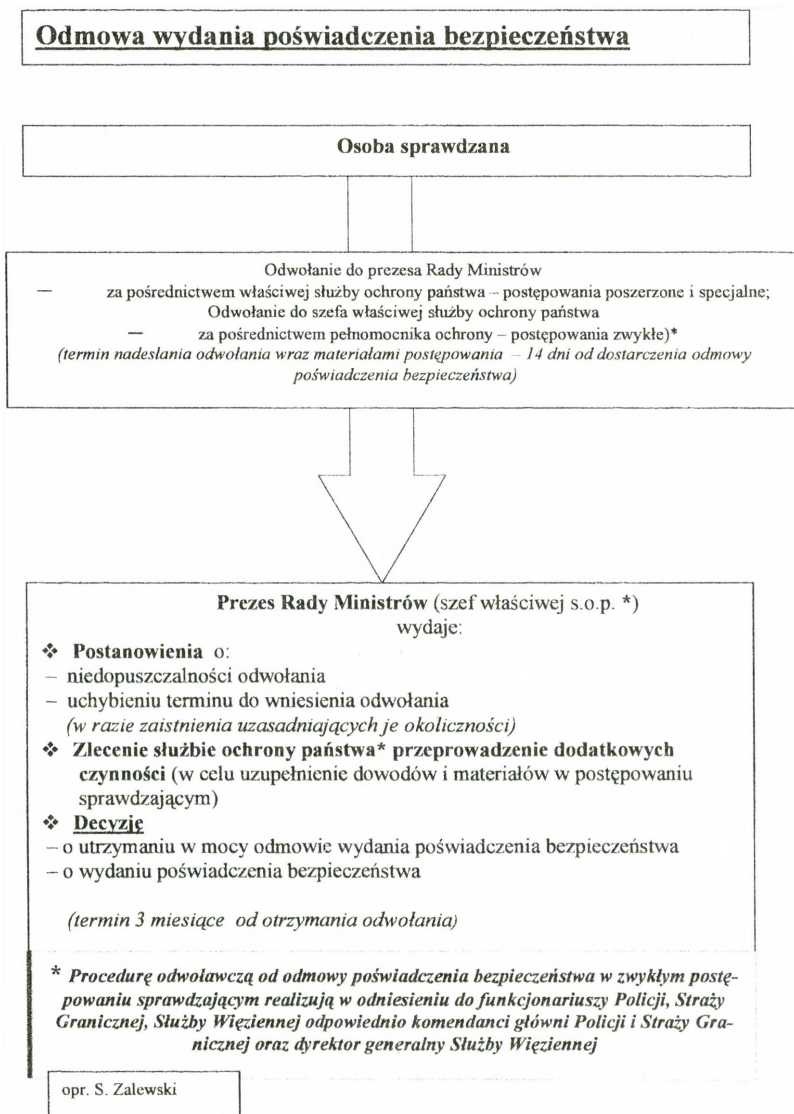
Współdziałanie organów i jednostek organizacyjnych w dziedzinie ochrony informacji niejawnych



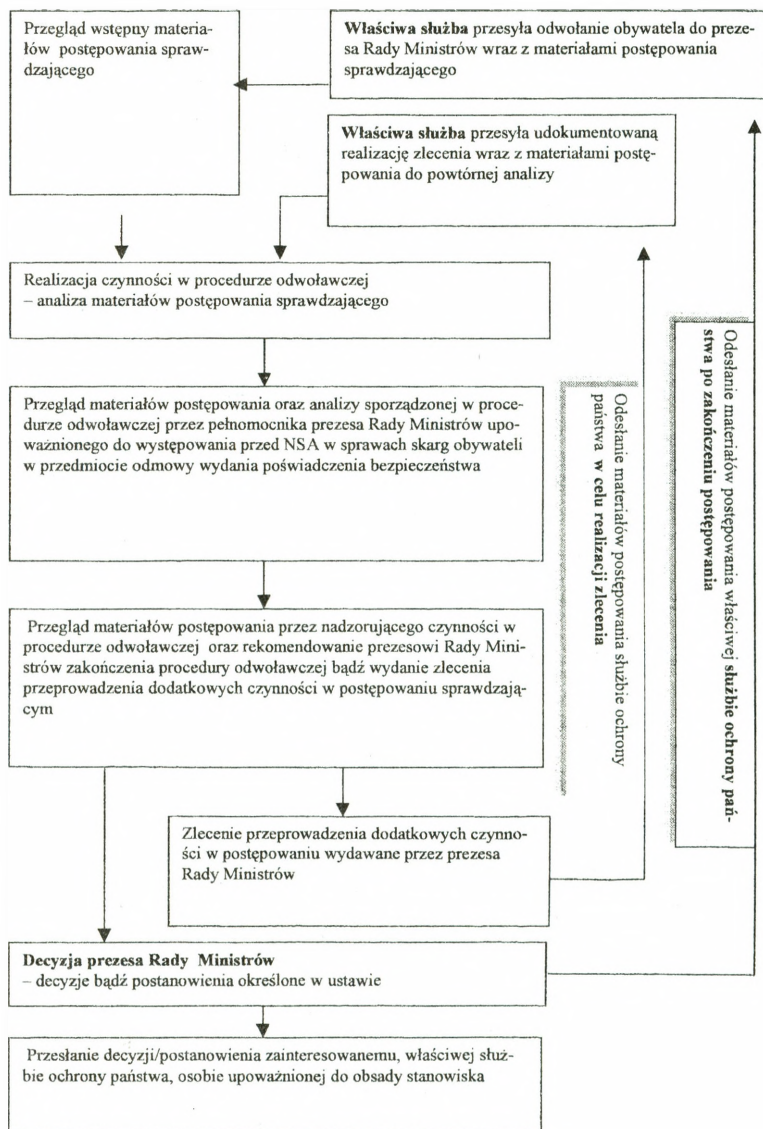
Wykres 2
Ramowy układ czynności
w poszerzonym i specjalnym postępowaniu sprawdzającym



Wykres 3
Procedura odwoławcza
od odmowy wydania poświadczenia bezpieczeństwa



Wykres 4
Ramowy układ czynności
w procedurach odwoławczych od odmów wydania poświadczenia
bezpieczeństwa



Wykres 5
Tryb skargowy do NSA
w przedmiocie odmowy wydania poświadczenia bezpieczeństwa
obowiązujący do 31.12.2003 r.

Odmowa wydania poświadczenia bezpieczeństwa:

- przez służbę ochrony państwa utrzymana w mocy na podstawie decyzji prezesa Rady Ministrów
- przez pełnomocnika ochrony utrzymana w mocy w wyniku rozpatrzenia odwołania przez szefa właściwej służby ochrony państwa*

Postanowienie prezesa Rady Ministrów (szefa właściwej s.o.p. *) :

- o niedopuszczalności odwołania
- o uchybieniu terminu do wniesienia odwołania

Osoba sprawdzana,
której odmówiono wydania poświadczenia bezpieczeństwa może złożyć skargę do NSA w terminie
30 dni od dnia doręczenia postanowienia lub decyzji.

Naczelny Sąd Administracyjny

- rozpatruje skargę na posiedzeniu niejawnym
- wydaje wyrok, w którym może:
 - uwzględnić skargę (zgodnie z art. 22, ust. 1 ustawy o NSA)
 - oddalić skargę w razie jej nieuwzględnienia
 - odrzucić skargę w razie upływu terminu do jej wniesienia, stwierdzenia niedopuszczalności,
 - lub gdy nie uwzględniono w wyznaczonym terminie braków skargi
- odpis wyroku z uzasadnieniem doręcza tylko właściwej służbie ochrony państwa*
- odpis wyroku (bez uzasadnienia) doręcza skarżącemu oraz osobie upoważnionej do obsady stanowiska

Orzeczenia NSA są prawomocne

Rewizja nadzwyczajna na warunkach art. 57 ustawy o NSA przysługuje: ministrowi sprawiedliwości, prokuratorowi generalnemu, pierwszemu prezesowi Sadu Najwyższego oraz RPO

** W postępowaniu skarbowym na odmowę wydania poświadczenia bezpieczeństwa przepisy dotyczące służby ochrony państwa stosuje się do Policji, Straży Granicznej, Służby Więziennej a szefa ABW lub WSI odpowiednio do komendantów głównych Policji i Straży Granicznej oraz dyrektora generalnego Służby Więziennej*

Opr. S. Zalewski

Wykres 6

Tryb skargowy do sądu administracyjnego
w przedmiocie odmowy wydania poświadczenia bezpieczeństwa
obowiązujący od 1.01.2004 r.

Odmowa wydania poświadczenia bezpieczeństwa:

- przez służbę ochrony państwa utrzymana w mocy na podstawie decyzji prezesa Rady Ministrów
- przez pełnomocnika ochrony utrzymana w mocy w wyniku rozpatrzenia odwołania przez szefa właściwej służby ochrony państwa*

Postanowienie prezesa Rady Ministrów:

- o niedopuszczalności odwołania
- o uchybieniu terminu do wniesienia odwołania

Osoba sprawdzana, której odmówiono wydania
poświadczenia bezpieczeństwa może złożyć skargę do sądu administracyjnego w terminie 30 dni od dnia doręczenia postanowienia lub decyzji

Wojewódzki sąd administracyjny

- odrzuca skargę wydając postanowienie (w przypadkach określonych w art. 58, § 1 Ustawy prawo o postępowaniu przed sądami administracyjnymi) lub →
- rozpoznaje skargę na posiedzeniu niejawnym i wówczas →
- wydaje wyrok, w którym może:
 - uwzględnić skargę (zgodnie z art. 145, § 1 Ustawy prawo o postępowaniu przed sądami administracyjnymi);
 - oddalić skargę w razie jej nieuwzględnienia;
- odpis wyroku z uzasadnieniem doręcza służbie prowadzącej postępowanie
- odpis wyroku (bez uzasadnienia) doręcza skarżącemu

Skarga kasacyjna do Naczelnego Sądu Administracyjnego
która może wnieść strona postępowania, prokurator lub rzecznik praw obywatelskich

Naczelny Sąd Administracyjny

- odrzuca skargę wydając postanowienie (w przypadku określonym w art. 150, § 1 Ustawy prawo o postępowaniu przed sądami administracyjnymi) lub →
- rozpoznaje skargę na posiedzeniu niejawnym i wówczas →
- wydaje wyrok, w którym może:
 - uwzględnić skargę (zgodnie z art. 185, § 1 Ustawy prawo o postępowaniu przed sądami administracyjnymi);
 - oddalić skargę w razie jej nieuwzględnienia;
- odpis wyroku z uzasadnieniem doręcza służbie prowadzącej postępowanie
- odpis wyroku (bez uzasadnienia) doręcza skarżącemu

BIBLIOGRAFIA

I. Akty prawne

- Umowa pomiędzy stronami Traktatu Północnoatlantyckiego w sprawie ochrony informacji. Bruksela 6 marzec 1997 r.
- Dyrektywa Bezpieczeństwa Narodowego USA nr 63 z 21 października 1991 r.
- Ustawa o Kanadyjskiej Służbie Wywiadu i Bezpieczeństwa (CSIS) z 1984 r.
- Ustawa o Urzędzie Ochrony Konstytucji Niemiec (BfV) par.3 ust.2 nr 1 wraz z par. 3536, ust. 2 i par. 55 Federalnego Kodeksu Karnego.
- Ogólna Międzyministerialna Instrukcja Ochrony Tajemnicy i Informacji Francji z 12 marca 1982 r.
- Ustawa o ochronie informacji niejawnych z 22 stycznia 1999 r. (DzU 1999, nr 11, poz. 95).

II. Literatura przedmiotu

- Andrejew I., Świda W., Wolter W., *Kodeks karny z komentarzem*, Warszawa 1973.
- Bafia J. i inni, *Kodeks postępowania karnego z komentarzem*, Warszawa 1976.
- Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, Warszawa 1999.
- Bojarski M., Radecki W., *Przewodnik po pozakodeksowym prawie karnym*, Wrocław 1998.
- Bronisławski J., *Szpiegostwo, wywiad, paragrafy*, Warszawa 1974.
- Chybiński O., Gutekunst W., Świda W., *Prawo karne. Część szczególna*, Wrocław 1971.
- Dąbrowski S., Kubicki L., *Ustawa o ochronie zdrowia psychicznego. Przegląd ważniejszych zagadnień*, Instytut Psychiatrii i Neurologii, Warszawa 1994.
- Dąbrowski S., Pietrykowski J., *Ustawa o ochronie zdrowia psychicznego – komentarz*, Warszawa 1997.
- Grzegorzczak T., *Kodeks postępowania karnego (komentarz)*, Kraków 1998.

- Hoc S., *Ochrona informacji niejawnych (wybrane problemy)*, Wojskowy Przegląd Prawniczy, Naczelna Prokuratura Wojskowa i Izba Wojskowa Sądu Najwyższego, nr 3–4 z 1999 r.
- Hoc S., *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Opole 2002.
- Jarzęcka-Siwik E., *Nowy system ochrony tajemnicy państwowej i służbowej*, Kontrola państwowa, NIK, nr 6/1999.
- Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*, Warszawa 2000.
- Kunicka-Michalska, *Nowe przepisy o ochronie tajemnicy państwowej i służbowej*, Państwo i Prawo 1983, nr 11.
- Mędrala, *Polskie służby specjalne w systemie ochrony informacji niejawnych*, Warszawa 2000, s. 54.
- Michalski B., *Podstawowe problemy prawa prasowego*, Warszawa 1998.
- Mozgawa M., *Ochrona informacji stanowiących tajemnicę przedsiębiorstwa w świetle ustawy o zwalczaniu nieuczciwej konkurencji*, Toruń 1994.
- Nowa Encyklopedia Powszechna, Warszawa 1996.
- Pikulski S., *Karnomaterialne i kryminologiczne aspekty bezpieczeństwa państwa*, Warszawa 1996.
- Rajzman H., *Zdrada kraju w prawie polskim*, Warszawa 1948.
- Rafacz J., *Dawne prawo sądowe polskie w zarysie*, Warszawa 1936.
- Rutkiewicz, *Tajemnica państwowa i wolność informacji. Więc gdzie te ustawy?*, Tygodnik Powszechny z 28.02.1999.
- Skorupko S., Auderska H., Łempicka Z., *Mały słownik języka polskiego*, Warszawa 1969.
- Sobczak J., *Ustawa Prawo prasowe. Komentarz*, Warszawa 1999.
- Sobczak J., *Prawo środków masowej informacji. Prasa, radio, telewizja*, Toruń 1999.
- Sołtysiński S., *Ustawa o zwalczaniu nieuczciwej konkurencji, komentarz*, Warszawa 1994.
- Szkudlarek P., Głosa do wyroku SN z 30.05.2000 r. IV CKN 1042/00, Orzecznictwo Sądów Polskich 2001/6/89.
- Thiem P., *Ochrona informacji niejawnych. Materiały do szkolenia pracowników*, Gdańsk 2003.
- Wojciechowski J., *Kodeks karny – komentarz, orzecznictwo*, Warszawa 1998.

- Woyciechowski P., *Praca dla stolarza a bezpieczeństwo państwa*, Rzeczpospolita z 26.02.1999 r.
- Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002.



Druk AON zam. nr 1102/WW

