CZASOPISMO PRAWNO-HISTORYCZNE
Tom LXV — 2013 — Zeszyt 1

ANDRZEJ SZYMCZAK (Poznań)

O systemie ochrony informacji niejawnych w Polsce w latach 1918-2011

Dla każdego państwa niezwykle istotna jest umiejętność ochrony informacji o kluczowym znaczeniu. Powodem tego jest rosnąca rola infrastruktury opartej na gromadzeniu i wykorzystaniu wszelkiego rodzaju danych. W takiej sytuacji utrata informacji może stanowić zagrożenie dla jego bezpieczeństwa. Dotyczy to zarówno sfery cywilnej (np. tajemnic handlowych) jak i wojskowej. Społeczeństwa rozwinięte korzystają w coraz większym stopniu z systemów teleinformatycznych. Dostęp do aktualnej i pewnej informacji jest niezbędnym warunkiem skutecznego działania, decydując o sprawności zarówno państwa jak i przedsiębiorstwa w dążeniu do wyznaczonego celu. Informacja jest obecnie uznawana za element infrastruktury krytycznej i podlega szczególnej ochronie[1].

Trudno dziś wyobrazić sobie państwo, w którym nie chroniono by informacji o obywatelach, zdrowiu publicznym oraz działaniu służb specjalnych czy też sił zbrojnych. Dobrym przykładem może być historia złamania tajemnic niemieckiego systemu szyfrującego ENIGMA, przez trzech naukowców związanych z Uniwersytetem w Poznaniu, co w sposób istotny przyczyniło się do wygrania II wojny światowej przez aliantów[2]. Systemy służące do przechowywania informacji mogą stać się obiektem ataku nie tylko obcych służb wywiadowczych ale także działań terrorystycznych.

W Polsce po 1999 r. powstał spójny, nowoczesny system ochrony informacji niejawnych, o charakterze zapobiegawczym. Wynika to z filozofii ochrony

[1] Pojęcie infrastruktury krytycznej zdefiniowano w art. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.). Zaliczamy do niej systemy oraz wchodzące w ich skład obiekty, urządzenia, instalacje, oraz usługi kluczowe dla bezpieczeństwa państwa, obywateli, instytucji publicznych i przedsiębiorców. Infrastruktura krytyczna obejmuje m.in. systemy zaopatrzenia w energię i surowce energetyczne, łączność, sieci teleinformatyczne, usługi finansowe, zaopatrzenia w żywność, systemy ochrony zdrowia, transportu, ratownictwa, zapewniające ciągłość działania administracji publicznej, produkcji, przechowywania i stosowania substancji chemicznych i promieniotwórczych.

[2] Byli to: Marian Rejewski, Jerzy Różycki i Henryk Zygalski. S. Jakóbczyk (red.), J. Stokłosa, *Złamanie szyfru Enigma: poznański pomnik polskich kryptologów*, Wyd. PTPN, Poznań 2007.

informacji wzorowanej na systemie prawnym państw o ugruntowanym ustroju demokratycznym. Ochrona informacji stanowi wyjątek od ogólnej zasady jawności życia społecznego i powszechnej ich dostępności. Dlatego też ochroną powinny być objęte wyłącznie dane o podstawowym znaczeniu w sposób nienaruszający ogólnej zasady dostępności informacji o życiu publicznym. Należy bowiem pamiętać, że informacja stanowi narzędzie realizacji konstytucyjnych praw oraz wolności obywateli (w tym kontroli władzy). Obecny stan prawny należy uznać pod tym względem za zadowalający, a przyjęte rozwiązania za spełniające europejskie standardy. Nadal jednak zbyt wąski pozostaje zakres kontroli sądowniczej nad klasyfikacją danych (w szczególności brak możliwości zmiany decyzji władz w tym zakresie). W przypadku trzech podstawowych procedur udzielania dostępu do informacji niejawnych, tj. postępowań sprawdzających, postępowań bezpieczeństwa przemysłowego, bezpieczeństwa teleinformatycznego – ostatnie z nich pozostaje nadal poza kontrolą sądów administracyjnych. Ochrona informacji niejawnych kształtowała się od momentu odzyskania niepodległości w 1918 r. Jednak dopiero w 1983 r. uchwalono pierwszy przepis rangi ustawowej, który nie miał charakteru karnego. Od tego momentu datuje się rozbudowa procedur o charakterze prawno-administracyjnym, która trwa do chwili obecnej.

*

Zgodnie z treścią art. 54 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.) obywatele mają prawo do swobodnego pozyskiwania i rozpowszechniania informacji. Zasada ta została dodatkowo skonkre-tyzowana w art. 61 Konstytucji. Zgodnie z jego treścią uprawnienie to dotyczy w szczególności pozyskiwania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, działalności organów samorządu gospodarczego i za-wodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

Wspomniane prawo do informacji może być realizowane w najrozmaitszych formach. Konstytucja wymienia jedynie niektóre z nich. Do najważniejszych zaliczymy dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej, pochodzących z powszechnych wyborów (np. posiedzenia Sejmu, Senatu oraz organów stanowiących samorządu terytorialnego), z prawem rejestracji dźwięku lub zapisu. Realizacji prawa dostępu do informacji służą również środki masowego przekazu, które obszernie informują o działalności organów władzy publicznej, pokazują przebieg i wyniki ich obrad. Wspomnieć należy także o publikowaniu stenogramów z posiedzeń Sejmu oraz Senatu, co ułatwia opinii publicznej ocenę ich działalności.

Powyższe uprawnienia warunkują świadomy udział obywateli w życiu społecznym. Są również niezbędne do urzeczywistnienia zasady zwierzchnictwa narodu jako fundamentu ustroju państwa demokratycznego. Stanowią korelat innej zasady konstytucyjnej, mianowicie zasady jawności działania administracji publicznej. Z podporządkowania organów państwa obywatelom wynika konieczność zapewnienia tym ostatnim pełnej informacji na temat działań administracji, dzięki czemu powstaje realna odpowiedzialność osób sprawujących władzę wobec społeczeństwa. W przeciwnym wypadku obywatele pozbawieni informacji o biegu spraw publicznych (również w skali lokalnej) nie mogą realizować swoich praw jako członkowie społeczeństwa, do którego należy władza zwierzchnia. Z powyższego wynika, że dostęp do informacji nie jest celem samym w sobie, lecz narzędziem niezbędnym do efektywnego korzystania z wielu innych praw obywatelskich o fundamentalnym charakterze. Jest zatem istotną gwarancją praworządności[3].

Dostęp do informacji znajduje odzwierciedlenie także w aktach prawa międzynarodowego, których sygnatariuszem jest Polska. Należy tu wspomnieć o Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (Dz. U. z 1993 r. Nr 61, poz. 284). W art. 10 zagwarantowano prawo do otrzymywania i przekazywania informacji oraz idei bez ingerencji władz publicznych i bez względu na granice państwowe. Podobne uregulowania zapisano w art. 19 Międzynarodowego Paktu Praw Obywatelskich i Politycznych (Dz. U. z 1977 r. Nr 38, poz. 167). Na jego mocy każdy człowiek ma prawo do swobodnego wyrażania opinii, przy czym prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpo-wszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, w jakikolwiek sposób według własnego wyboru. W celu zapewnienia właściwego korzystania z prawa do informacji wprowadzono do systemu prawnego ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.). Zawiera ona uregulowania, w celu realizacji powyższych praw, ustanawiając procedury korzystania z informacji przez obywateli. W art. 2 ust. 2 wspomnianej ustawy umieszczono zakaz żądania wykazywania interesu prawnego od osób występujących z wnioskiem o udostępnienie tych informacji. Ponadto ustawa w sposób bardzo szeroki określa ramy dostępu, wskazując, że przysługu-

[3] Do wspomnianej kwestii odniósł się Trybunał Konstytucyjny w uchwale z 13 czerwca 1994 r. (W.3/94). Trybunał zajmował się m.in. wykładnią pojęcia tajemnicy państwowej – w szczególności danych identyfikujących funkcjonariuszy oraz osób współpracujących z organami ochrony bezpieczeństwa publicznego, wykonujących zadania wywiadu i kontrwywiadu. W uchwale stwierdzono, że stosowanie instytucji tajemnicy państwowej stanowi ograniczenie wolności przekazywania i komunikowania poglądów jak i prawa dostępu do informacji. Z tego też względu zawsze należy analizować przepisy o ochronie informacji niejawnych z uwzględnieniem zasady demokratycznego państwa prawnego. Tajemnica państwowa powinna być definiowana z dużą wstrzemięźliwością – głównie jako środek ochrony dóbr o szczególnym znaczeniu dla państwa – wskazanych przez ustawodawcę.

je on każdemu. Oznacza to jego przyznanie zarówno osobom prawnym jak i fizycznym. Ustawa nie zawiera również żadnych ograniczeń wynikających z posiadania obywatelstwa polskiego. Prawo to przysługuje więc na równi obywatelom polskim, cudzoziemcom oraz bezpaństwowcom. Z dostępu do informacji korzystają również osoby prawne nieposiadające siedziby na terenie kraju. W art. 6 umieszczono otwarty katalog zawierający 29 rodzajów informacji objętych dostępem obywateli na mocy ww. ustawy. W art. 13 przyjęto zasadę, że udostępnianie informacji powinno się odbywać bez zbędnej zwłoki, jednak nie później niż 14 dni od daty złożenia wniosku. Jeśli termin nie może zostać dotrzymany, należy uprzedzić o tym wnioskodawcę, wskazując termin udzielenia informacji (nie dłuższy niż 2 miesiące). Wspomniana jawność informacji nie jest jednak pełna.

W Konstytucji przewidziano możliwość ograniczenia dostępu obywateli do informacji. Zgodnie z art. 61 ust. 3 ograniczenie tego prawa może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa. Oznacza to wprowadzenie ogólnej zasady, iż dostęp do informacji ma charakter swobodny i powszechny z wyjątkiem informacji z niego wyłączonych – ze względu na ważny interes obywatela lub państwa. W art. 5 ustawy o dostępie do informacji publicznej przewidziano możliwość wyłączenia dostępu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz innych tajemnic prawnie (ustawowo) chronionych. Przy czym pojęcie tajemnicy prawnie chronionej nie ma precyzyjnej definicji. W praktyce za tajemnicę taką należy uznać wszelkie informacje, które na mocy przepisów ustawowych zostały wyłączone z dostępu do informacji publicznej. Wyłączenie to powinno mieć charakter wyraźny poprzez wprowadzenie zakazu ich ujawniania lub ustanowienie odrębnej procedury ujawniania. Obecnie możemy uznać za tajemnice prawnie chronione 48 rodzajów różnych informacji, opisanych w ustawach.

Lata 1918-1945. Po odzyskaniu niepodległości przez Polskę na terytorium państwa obowiązywały systemy prawne państw zaborczych. Mieliśmy do czynienia z prawem rosyjskim, pruskim i austriackim oraz węgierskim (na Spiszu i Orawie). Przy czym systemy te charakteryzowały się archaicznością rozwiązań oraz odmiennymi i trudnymi do pogodzenia cechami. W pierwszym okresie niepodległości narzędziem ochrony informacji niejawnych były przepisy karne. Aż do roku 1932 system prawa polskiego nie regulował tych zagadnień w sposób spójny. Na ziemiach dawnego zaboru rosyjskiego podstawą ochrony tych informacji był Kodeks Tagancewa z 1903 r., który obowiązywał w Polsce do wprowadzenia nowego kodeksu karnego. W art. 653-655 zawarto regulacje dotyczące przestępstwa ujawnienia tajemnic służ-

bowych[4]. Penalizowano umyślne ujawnienie wszelkich aktów rządowych, wiadomości i dokumentów, które należało zachować w tajemnicy ze względu na interes państwowy. W art. 653 kodeksu wprost wymieniono:

– ujawnienie tajemnicy korespondencji pocztowej;
– ujawnienie tajemnicy korespondencji telegraficznej;
– ujawnienie tajemnicy przez urzędnika poczty lub telegrafu.

Formę kwalifikowaną przewidywano jeśli ujawnienie wiązało się ze sprawami bezpieczeństwa kraju. Wyodrębniono uchybienie służbowe zagrożone karą do 6 lat pozbawienia wolności. Natomiast odrębnie definiowano zdradę, jako zamiar szkodzenia własnemu państwu. Ponadto w art. 654 przewidziano przestępstwo dopuszczenia do zabrania, zagubienia lub zniszczenia rysunków, dokumentów urzędowych na skutek niedbalstwa lub niewykonania przepisów. Przestępstwem było również ujawnienie w skutek niedbalstwa innej tajemnicy dotyczącej bezpieczeństwa zewnętrznego. Powyższe rozwiązania wskazują, że tajemnice prawnie chronione i informacje niejawne obecnie opisywane odrębnie były traktowane w sposób zbliżony i określane jako tajemnice urzędowe. Różnice oparto głównie na skutkach ich nieuprawnionego ujawnienia.

Na ziemiach dawnego zaboru pruskiego obowiązywał Landrecht pruski, który początkowo nie zawierał praktycznie żadnych odniesień do ochrony informacji niejawnych. Dopiero w skutek nowelizacji dokonanej w roku 1875 dodano § 353a w którym zapisano że karze ulegał urzędnik Ministerstwa Spraw Zagranicznych zarówno w centralnym zarządzie jak i w przedstawicielstwie państwa za granicą za umyślne ujawnienie tajemnic powierzonych mu z tytułu zajmowanego stanowiska[5]. Po odzyskaniu niepodległości dodano w § 92 znamiona przestępstwa umyślnego podania do wiadomości obcemu rządowi albo publicznego ujawnienia tajemnic Państwa Polskiego. Przestępstwo to dotyczyło wszelkiego rodzaju informacji i dokumentów (również wojskowych), które ze względu na interes państwa powinny zostać zachowane w tajemnicy. Przestępstwo to było zagrożone karą co najmniej dwóch lat ciężkiego więzienia. W przypadku wystąpienia okoliczności łagodzących wymierzano karę osadzenia w twierdzy na czas 6 miesięcy[6].

Na ziemiach wchodzących do roku 1918 w skład Austrii obowiązywał kodeks karny z 1787 r. (tzw. „Józefina"). Od 1 stycznia 1804 r. na terenie I i III zaboru austriackiego wprowadzono nową ustawę karną dla Galicji Zachodniej pod nazwą „Księga ustaw za zbrodnie ciężkie i policyjne przestępstwa". Usta-

[4] W. Makowski, *Prawo karne: o przestępstwach w szczególności: wykład porównawczy prawa karnego austrjackiego, niemieckiego i rosyjskiego, obowiązującego w Polsce*. Wyd. Księgarnia F. Hoesicka, Kraków 1924, s. 94-96.

[5] W. Makowski, op. cit., s. 97.

[6] J. Kałużniacki, *Ustawy byłej dzielnicy pruskiej. Ustawa Karna*, t. 1 wyd. II, Poznań 1921, s. 46-47.

wa ta, zwana „Franciszkanką", składała się z dwóch działów: prawa materialnego i procesowego. Przepisy (zawarte w rozdziale VII „O zbrodniach zdrady stanu, obrazy majestatu …") zawierały uregulowania dotyczące ochrony tajemnic (w tym państwowej i służbowej)[7].

W § 58 zdefiniowano zbrodnię zdrady stanu polegającą na dążeniu

> „do oderwania jednolitego związku państwa albo sprowadzenia lub zwiększenia niebezpieczeństwa albo buntu lub wojny domowej wewnątrz; czy to dzieje się publicznie lub tajnie przez jednostki lub przez inne związki, przez knowanie, wzywanie, pobudzanie, nakłanianie słowem, pismem, drukiem, Obrazowem przedstawianiem, poradą albo własnym czynem z bronią lub bez tejże, przez udzielanie prowadzących do tego tajemnic (…)".

Zbrodnia zdrady stanu była zagrożona karą śmierci. Karą obejmowano przywódców, podżegaczy, sprawców i współdziałających, pomocników. Rozdział X kodeksu dotyczył „Nadużycia władzy urzędowej" i dotyczył ochrony tajemnic przez funkcjonariuszy państwa. W § 101 zawarto definicję urzędnika – tj. osoby zobowiązanej do załatwiania interesów zwierzchności na mocy bezpośredniego lub pośredniego zlecenia publicznego po zaprzysiężeniu lub bez zaprzysiężenia. W art. 102c opisano przestępstwo polegające na wyjawieniu powierzonej tajemnicy urzędowej, zniszczeniu albo udzieleniu powierzonego dokumentu wbrew nałożonemu obowiązkowi. Do wypełnienia znamion zbrodni opisanej w art. § 102 lit c polegającej na bezprawnym udzieleniu dokumentu, nie wymagano aby wyjawiono w ten sposób tajemnicę urzędową. Udzieleniem w myśl tego paragrafu było już samo rozmyślne uczynienie tego dokumentu dostępnym osobom nieupoważnionym. Nie wymagano również aby osoba której udzielono dokumentu skorzystała z niego[8].

Problematykę ochrony informacji niejawnych poruszono również w kodeksie karnym wojskowym wprowadzony rozporządzeniem prezydenta RP z dnia 22 marca 1928 r. (Dz. U. RP nr 36, poz. 328). Zgodnie z art. 46

> „żołnierz, który spełni czyn, stanowiący bunt władzy zwierzchniej lub zdradę stanu lub inne przestępstwo przeciwko Państwu, ulega karze przewidzianej w kodeksie karnym z 1903 r. Kto w polu umyślnie naruszy obowiązek służbowy i tem spowoduje, że przedsięwzięcia nieprzyjacielskie doznają poparcia lub, że dla prowadzących wojnę wojsk polskich lub sprzymierzonych powstanie niebezpieczeństwo lub szkoda będzie karany zamknięciem w ciężkim więzieniu na czas

[7] W 1850 zmieniono przepisy prawa procesowego. W 1852 dokonano zmiany prawa materialnego. *Ustawa Karna Austrjacka o zbrodniach, występkach i wykroczeniach z dnia 27 maja 1852 r*. Nr 177 Dpp (obowiązująca w okręgach sądów apelacyjnych w Krakowie i we Lwowie oraz sądu okręgowego w Cieszynie – z przeglądem orzecznictwa) pod red. J. Przeworskiego. Wyd. Księgarnia F. Hoesicka, Warszawa 1924, s. 45-59.

[8] Op. cit., s. 71-81.

do lat dziesięciu, zastępującym dom poprawy lub w twierdzy na czas nie krótszy od roku jednego. W przypadkach mniejszej wagi i w przypadkach nieumyślnego naruszenia obowiązku służbowego będzie wymierzona kara zamknięcia w więzieniu lub w twierdzy na czas nie dłuższy od lat trzech".

Zakres podmiotowy kodeksu ograniczał się tylko do żołnierzy w służbie czynnej i stanie spoczynku, jeńców, innych osób wykonujących obowiązki służbowe przy jednostkach wojskowych i na okrętach wojennych.

W dniu 11 lipca 1932 r. Prezydent RP podpisał Kodeks karny (Dz. U. nr 60, poz. 571). Wraz z nim wprowadzono także Wojskowy kodeks karny. Kodeks stanowił nowoczesną jak na tamte czasy, kompleksową i pełną kodyfikację prawa karnego, która przetrwała do roku 1969. Objął mocą obowiązującą całe terytorium odrodzonego państwa polskiego.

Do problematyki ochrony informacji niejawnych odnosił się art. 289 § 1-3. Przestępstwem było zarówno umyślne jak i nieumyślne ujawnianie tajemnicy urzędowej na szkodę państwa polskiego[9]. Do wyczerpania znamion przestępstwa wystarczyło już niebezpieczeństwo wystąpienia owej szkody[10]. Ujawnieniem było zakomunikowanie lub udostępnienie tajemnicy osobie nieuprawnionej do jej posiadania. Sąd mógł w tej sprawie wymierzyć karę więzienia do 5 lat pozbawienia wolności. Jeżeli sprawca działał dla uzyskania korzyści był zagrożony karą surowszą – do lat 10 więzienia. W przypadku nieumyślnego ujawnienia tajemnicy przewidywano karę łagodniejszą – do 6 miesięcy aresztu. Jeśli ujawnienie tajemnicy nie wiązało się ze szkodą (nawet potencjalną) mieliśmy do czynienia z tzw. niedyskrecją służbową. Jako tajemnicę urzędową definiowano wszelkie wiadomości związane z czynnościami urzędowymi dotyczące spraw politycznych, ekonomicznych kraju tak w stosunkach zewnętrznych jak i wewnętrznych, których ujawnienie może wyrządzić szkodę państwu.

Lata 1956-1999. W okresie istnienia Polskiej Rzeczypospolitej Ludowej mieliśmy do czynienia z nowym podejściem do ochrony informacji niejawnych. Wynikało ono z autorytarnego charakteru państwa Ponadto w latach 1945-1956 prawo karne było otwarcie używane do walki z przeciwnikami politycznymi[11]. W dekrecie Rady Ministrów z 16 listopada 1945 r. o przestęp-

[9] „Ograniczyć się należy do ciaśniejszego pojęcia tajemnicy urzędowej, należy przyjąć, że obejmuje ona tylko takie wiadomości które dotyczą czynności przedsiębranych przez jednego urzędnika lub w gronie kilku, a które z istoty swej na czas pewien (np. na czas śledztwa sądowego) lub trwale nie powinny wyjść poza koło osób mających wyciągnąć z niej urzędowe konsekwencje". J. Makarewicz, *Kodeks karny z komentarzem*. Wyd. ZN im. Ossolińskich, Lwów 1932, s. 395.

[10] W. Makowski, *Kodeks karny. Komentarz*, Warszawa 1937, s. 870. Do kwestii tej odniósł się również Sąd Najwyższy w orzeczeniu z 31 grudnia 1934 r. (I K 602/34).

[11] Przykład może stanowić wydane przez Ministerstwo Sprawiedliwości w 1951 r. opracowanie J. Machowskiego pt. *Ochrona tajemnicy państwowej i służbowej*.

stwach szczególnie niebezpiecznych w okresie odbudowy Państwa (Dz. U. nr 53, poz. 300) zawarto przepisy dotyczące ochrony tajemnicy państwowej. Przestępstwo popełniał ten, kto działając na szkodę Państwa Polskiego gromadził lub przekazywał wiadomości, dokumenty, przedmioty stanowiące tajemnicę państwową lub wojskową. Karą było więzienie, dożywotnie więzienie albo kara śmierci (art. 8). Odpowiedzialnością objęto także czynności przygotowawcze jeśli sprawca wchodził w porozumienie z innymi osobami. Drugi typ przestępstwa dotyczył publicznego rozpowszechniania informacji dotyczących obrony państwa i Sił Zbrojnych, które mogły zagrażać interesom obrony. W tym wypadku przewidziano karę do 5 lat pozbawienia wolności (art. 10). Wyroki wydawały sądy wojskowe. W dekrecie zabrakło jakiejkolwiek definicji tajemnicy państwowej. Powyższe rozwiązania zostały powtórzone niemal dosłownie w następnym dekrecie Rady Ministrów z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa (Dz. U. nr 30, poz. 192 z późn. zm.). W jego art. 7 opisano przestępstwo polegające na gromadzeniu oraz przekazywaniu na szkodę Polski informacji, dokumentów i innych przedmiotów stanowiących tajemnicę państwową lub wojskową. Sprawca podlegał karze więzienia na czas nie krótszy niż 5 lat, karze dożywotniego pozbawienia wolności lub karze śmierci. Karze podlegały również czynności przygotowawcze. Na mocy art. 9 karano publiczne rozpowszechnianie informacji, dokumentów oraz innych danych dotyczących obrony państwa lub jego sił zbrojnych, których ujawnienie mogło zagrażać interesom obrony, oraz innych informacji objętych zakazem takiego rozpowszechniania. Sprawcy groziło więzienie orzekane w wysokości do 5 lat. Przepisy dekretu uchylono dopiero w 1969 r.

Kwestie ochrony tajemnic uregulowano także w dekrecie PKWN z 23 września 1944 r. Kodeks Karny Wojska Polskiego (Dz. U. nr 6, poz. 27 z późn. zm.). W art. 90 opisano przestępstwo którego dopuszczał się ten, kto działając na szkodę Państwa Polskiego, zbierał lub przekazywał wiadomości będące tajemnicą państwową oraz wojskową, przeszedł na stronę nieprzyjaciela lub zbiegł za granicę. Kodeks miał ograniczone zastosowanie (art. 5), ponieważ odnosił się do żołnierzy WP, osób obowiązanych do służby wojskowej lub pomocniczej z chwilą powołania, jeńców wojennych i zakładników pod nadzorem administracji wojskowej, oraz innych osób określonych prawem. Należy podkreślić, że przytoczone uregulowania pozostawały w kolizji z zakresem obowiązywania wspomnianego dekretu, który w założeniu obejmował także żołnierzy.

Następny akt prawny, tj. dekret Rady Ministrów z 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 55, poz. 437), również miał charakter głównie karny, obejmując odpowiedzialnością przestępstwa przeciwko powyższym tajemnicom. W artykułach 3-10 opisano następujące z nich:

– zbieranie, przechowywanie, przekazywanie, ujawnianie lub ogłaszanie przez osoby nieuprawnione wiadomości (dokumentów, innych przedmiotów) będących tajemnicą państwową;

– zbieranie, przechowywanie, przekazywanie, ujawnianie lub ogłaszanie przez urzędnika wiadomości będących tajemnicą państwową (w formie dokumentów, innych przedmiotów) pozyskanych w związku z obowiązkami służbowymi (czyn kwalifikowany). Do bytu przestępstwa nie było konieczne powstanie jakiejkolwiek szkody, ani nawet zagrożenie jej wystąpieniem. Łagodniej traktowano sprawców nieumyślnych ww. czynów;

– naruszanie zarządzeń władz wydanych w celu ochrony tajemnicy państwowej (art. 5 ust. 4 – także przez urzędnika w związku ze służbą);

– naruszanie zarządzeń władz wydanych w celu ochrony tajemnicy państwowej ze względu na obronę lub bezpieczeństwo Państwa (art. 6 ust. 4 – także przez urzędnika w związku ze służbą);

– utrata z winy urzędnika powierzonych mu dokumentów lub przedmiotów stanowiących tajemnicę państwową – jeśli spowodowała lub mogła spowodować jej ujawnienie;

– utrata z winy urzędnika powierzonych mu dokumentów lub przedmiotów stanowiących tajemnicę państwową ze względu na obronę lub bezpieczeństwo Państwa – jeśli spowodowała lub mogła spowodować jej ujawnienie. Podobnie jak poprzednio – przewidywano wyższe kary w przypadku informacji dotyczących obronności lub bezpieczeństwa;

– przekazywanie, ujawnianie lub rozgłaszanie informacji stanowiących tajemnicę służbową przez osoby nieuprawnione (w przypadku gdy sprawcą jest urzędnik – czyn kwalifikowany)[12];

– naruszanie przez urzędnika w związku ze służbą zarządzeń władz wydanych w celu ochrony tajemnicy służbowej.

Na podstawie art. 1 i 15 dekretu z 1949 r. o ochronie tajemnicy państwowej i służbowej wydawano przepisy wykonawcze określające zakres przedmiotowy ww. tajemnic oraz sposób jej ochrony. Uchwała Rady Ministrów nr 282/59 z dnia 2 lipca 1959 r. w sprawie organizacji ochrony tajemnicy państwowej i służbowej wprowadzała dwa rodzaje klauzul dotyczących tajemnicy państwowej:

– tajne specjalnego znaczenia (obejmująca wiadomości, dokumenty i przedmioty szczególnie ważne dla bezpieczeństwa Państwa, których ujawnienie mogło spowodować wyjątkowo poważne szkody dla Państwa lub państw sprzymierzonych);

– tajne (pozostałe dokumenty i przedmioty zawierające tajemnicę państwową).

Wiadomości i dokumenty stanowiące tajemnicę służbową oznaczano klauzulą poufne.

[12] Wyrok Sądu Najwyższego z 29 sierpnia 1950 r. (K 513/50).

W załączniku do uchwały zawarto ogólny wykaz wiadomości, dokumentów i innych przedmiotów stanowiących tajemnicę państwową. Wyróżniono trzy rodzaje takich wiadomości: dotyczące obronności państwa, dotyczące bezpieczeństwa państwa oraz interesów gospodarki narodowej.

Minister Spraw Wewnętrznych w porozumieniu z Ministrem Obrony Narodowej wydał zarządzenie nr 70/60 z dnia 31 marca 1960 r. w sprawie postępowania w kraju z dokumentami tajnymi i tajnymi specjalnego znaczenia. Zwoływano coroczne kolegia w ministerstwach i urzędach centralnych w celu zwiększenia nadzoru nad ochroną tajemnicy państwowej i służbowej. Ponadto każdy przypadek zagubienia dokumentu lub innego naruszenia tajemnicy państwowej kierownicy instytucji i zakładów pracy powinni zgłaszać wskazanym organom państwa (Milicji Obywatelskiej, prokuraturze, MSW itd.). Zarządzeniem tym wprowadzono również wzorcową *Instrukcję o postępowaniu z dokumentami tajnymi, tajnymi specjalnego znaczenia oraz dokumentami geodezyjnymi, kartograficznymi, i geologicznymi stanowiącymi tajemnicę państwową i służbową*.

28 czerwca 1961 r. Minister Spraw Wewnętrznych wydał tajne zarządzenie nr 099/61 w sprawie postępowania z dokumentami mobilizacyjnymi. Ustanowiono w nim odrębną instrukcję dla tej kategorii materiałów, odwołując się do wzorcowej instrukcji z dnia 31 marca 1960 r. Materiały mobilizacyjne oznaczano skrótem „MOB". Przesyłki oznaczano literą „S" umieszczaną obok pieczątki nagłówkowej. Niszczenie powyższych dokumentów odbywało się tylko protokolarnie. Ponadto instrukcja zawierała odrębny wykaz informacji z zakresu spraw mobilizacyjnych.

Minister Spraw Wewnętrznych wydał 25 maja 1960 r. zarządzenie wewnętrzne nr 0101 w sprawie zabezpieczenia tajemnicy państwowej i służbowej w resorcie spraw wewnętrznych. Określono w nim tryb postępowania w sprawach tajnych, zobowiązywano pracowników resortu do przestrzegania tajemnicy państwowej. Kierownicy wszystkich jednostek organizacyjnych mieli prowadzić stałą kontrolę stanu zabezpieczenia tajemnic oraz sposobu postępowania z dokumentacją. Minister Spraw Wewnętrznych wydał również 6 października 1963 r. pismo okólne nr 5/63 regulujące postępowanie z dokumentami stanowiącymi tajemnicę służbową i państwową, otrzymywanymi z zagranicy i wysyłanymi za granicę. Uregulowanie odsyłało do rozdziałów I i III opisanej wcześniej instrukcji z dnia 31 marca 1960 r. (wprowadzonej zarządzeniem 70/60) dotyczącej postępowania w kraju z dokumentami tajnymi i tajnym specjalnego znaczenia. Ponadto zakazywano zmian cech tajności na oryginałach (i kopiach) takich dokumentów. Dokumenty przesyłane za granicę zawierające tajemnicę służbową należało klasyfikować jako tajne. W przypadku gdyby zawierały tajemnicę państwową, oznaczano je jako „ściśle tajne" albo „ściśle tajne specjalnego znaczenia". Do ostatniej kategorii zaliczono wiadomości, dokumenty, przedmioty, o szczególnym znaczeniu dla

obronności, bezpieczeństwa lub interesów gospodarczych Polski lub państw sojuszniczych.

Ustawa z 19 kwietnia 1969 r. Kodeks karny (Dz. U. Nr 13, poz. 94 z późn. zm.) zawierała w art. 120 § 15 i 16 definicje tajemnicy państwowej i służbowej. Za tajemnicę państwową uznawano wiadomość, której ujawnienie osobom nieuprawnionym może narazić na szkodę bezpieczeństwo lub inny ważny interes polityczny lub gospodarczy PRL. Tajemnica służbowa to wiadomość, z którą pracownik zapoznał się w związku ze swoją pracą w instytucji państwowej lub społecznej, a której ujawnienie osobom nieuprawnionym może narazić na szkodę społecznie uzasadniony interes. Jak widać, w przytoczonych definicjach tajemnica była utożsamiana z informacją (wiadomością) bez odniesienia do materialnego substratu – jak to czyniono w dekrecie z 1949 r. Podkreślono tym samym konieczność ochrony takiej informacji bez względu na formę i sposób utrwalenia (nośnika)[13]. Inną cechą jest uznanie za tajemnice tylko takich wiadomości, których nieuprawnione ujawnienie musi co najmniej narażać na uszczerbek określone interesy państwa lub uzasadniony interes społeczny. Definicja zwęziła przez to zakres przedmiotowy odpowiedzialności karnej w porównaniu z dekretami z lat czterdziestych. W rozdziale XXXIV k. k., zatytułowanym „Przestępstwa naruszenia tajemnicy państwowej i służbowej", ustawodawca wskazał granice prawno-karnej ochrony informacji niejawnych (art. 260-264).

Przestępstwo popełniał ten kto umyślnie ujawniał tajemnicę państwową. Jeśli tajemnica państwowa dotyczyła obronności lub bezpieczeństwa PRL albo została ujawniona osobie działającej na rzecz zagranicznej instytucji lub przedsiębiorstwa mieliśmy do czynienia z czynami kwalifikowanymi (objętymi surowszą odpowiedzialnością karną). Sprawca opowiadał również za czyn nieumyślny jeśli ujawnił tajemnicę państwową, z którą zapoznał się z funkcją sprawowaną w instytucji państwowej lub społecznej.

Karze podlegała osoba, która nieumyślnie dopuściła do zagubienia powierzonego jej dokumentu lub przedmiotu zawierającego tajemnicę państwową. Jeśli tajemnica dotyczyła obronności lub bezpieczeństwa PRL, przewidywano surowszą karę. Ponadto karano naruszenie zarządzenia państwowego wydanego dla ochrony tajemnicy państwowej, jeśli naruszenie to groziło ujawnieniem tajemnicy.

W przypadku tajemnicy służbowej odpowiedzialności karnej podlegali urzędnicy (funkcjonariusze państwowi, pracownicy instytucji państwowej lub społecznej), Jeśli sprawca przekazywał informację poza granice kraju podlegał surowszej karze (czyn kwalifikowany). Zgodnie z art. 289 ww. przepisy stosowano wobec wszystkich obywateli (także żołnierzy LWP). Istotną zmia-

[13] Z. Młynarczyk, *Ochrona tajemnicy państwowej i służbowej w kodeksie karnym*, NP. 1971, Nr 1 s. 13 i n.

ną w stosunku do uregulowań uchylonego dekretu z 1949 r. było poddanie spraw karnych w zakresie ochrony tajemnicy – jurysdykcji sądów powszechnych (w miejsce sądów wojskowych).

Rada Ministrów w dniu 2 lipca 1971 r. podjęła uchwałę nr 128/71 w sprawie ochrony tajemnicy państwowej i służbowej. Zmodyfikowano tym samym system istniejący od roku 1959. Na podstawie nowych przepisów osobą odpowiedzialną za ochronę tajemnic był:

– kierownik instytucji centralnej lub naczelnej – w przypadku naczelnych i centralnych organów władzy oraz podległych im instytucji państwowych i społecznych (wszystkich stopni);

– przewodniczący prezydium wojewódzkiej rady narodowej – w odniesieniu do rady narodowej i podległych jej instytucji wszystkich stopni;

– kierownik instytucji (w przypadku instytucji państwowej lub samorządowej).

Do pracy na stanowiskach z dostępem do tajemnicy państwowej upoważniano wyłącznie osoby dające rękojmię jej zachowania. Pisemne upoważnienie wydawano w uzgodnieniu z Ministrem Spraw Wewnętrznych (w przypadku osób zatrudnionych w naczelnych i centralnych instytucjach państwowych lub społecznych) lub właściwym terytorialnie Komendantem Wojewódzkim Milicji Obywatelskiej (w przypadku osób zatrudnionych w instytucjach niższych stopni). Kierownicy naczelnych i centralnych instytucji państwowych zostali zobowiązani do utworzenia w podległych urzędach wyodrębnionych komórek ds. ochrony tajemnicy państwowej i służbowej. Dotyczyło to również podległych instytucji wszystkich stopni. Zadaniem komórek była koordynacja ochrony i kontrola przestrzegania przepisów oraz instrukcji wewnętrznych. W radach narodowych kontrolę i nadzór powierzono Wydziałom Spraw Wewnętrznych. Kierownicy instytucji każdego szczebla raz w roku musieli przeprowadzać analizę stanu ochrony tajemnicy państwowej i służbowej. Z wynikami analiz zapoznawano (w zależności od szczebla) Ministra Spraw Wewnętrznych albo Komendanta Wojewódzkiego MO. Ponadto, kierowników naczelnych i centralnych instytucji państwowych oraz samorządowych zobowiązano do sporządzenia wykazów wiadomości stanowiących tajemnicę państwową i służbową dostępnych w podległych i nadzorowanych komórkach wszystkich szczebli.

Minister Spraw Wewnętrznych wydał w dniu 30 sierpnia 1972 r. zarządzenie nr 89/72 w sprawie zasad i sposobu postępowania w kraju z wiadomościami stanowiącymi tajemnicę państwową i służbową. Uregulowano w nim podstawowe zasady ochrony informacji. Uchylono jednocześnie zarządzenie nr 70/60 oraz większość przepisów wykonawczych dotyczących tej tematyki. W zarządzeniu 89/72 zapisano podstawowe zasady postępowania kładąc nacisk na obowiązki każdego pracownika (dysponenta tajemnicy). Każda osoba posiadająca dostęp do tajemnic powinna zostać zapoznana z treścią przepisów oraz pouczona o odpowiedzialności karnej za ich naruszenie. Przyjęto zasa-

dę ograniczonego dostępu do tajemnicy – co oznaczało przekazywanie tylko informacji niezbędnych do pracy na danym stanowisku. Obowiązek zachowania tajemnicy obciążał pracownika zarówno w czasie trwania stosunku pracy jak i po jego zakończeniu. Kierownik jednostki organizacyjnej odpowiadał za szkolenie podległych mu pracowników.

Dnia 14 grudnia 1982 r. Sejm przyjął ustawę o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271 z późn. zm.). Zgodnie z jej treścią odebrano Radzie Ministrów prawo do określana zakresu wiadomości stanowiących tajemnicę (art. 22 ust. 2 u.o.t.). Do wiadomości stanowiących tajemnicę państwową zaliczono w ustawie takie, których ujawnienie osobom nieupoważnionym może narazić na szkodę obronność, bezpieczeństwo lub inny ważny interes państwa. Dotyczyły one w szczególności: przygotowań obronnych, organizacji służb ochrony porządku i bezpieczeństwa publicznego, prac naukowo-badawczych, projektowych, technologicznych i konstrukcyjnych (związanych z obronnością lub bezpieczeństwem państwa), produkcji o podstawowym znaczeniu dla gospodarki, strategicznych rezerw państwowych, emisji środków płatniczych i papierów wartościowych, negocjacji i przygotowania umów państwowych, treści umów międzyna-rodowych (jeśli zastrzegła to którakolwiek ze stron).

Wykaz powyższy nie stanowił katalogu zamkniętego. Wyraźnie podkreślono przy tym, że obowiązek zachowania tajemnicy dotyczy każdego, do czyjej wiadomości dotarła.

Tajemnicą służbową była natomiast wiadomość niestanowiąca tajemnicy państwowej, z którą pracownik zapoznał się w związku z pełnieniem swoich obowiązków w państwowej, spółdzielczej lub społecznej jednostce organizacyjnej, a której ujawnienie może narazić na szkodę interes społeczny, uzasadniony interes tej jednostki organizacyjnej lub obywatela. W art. 22 ust. 1 wspomnianej ustawy uchylono definicje dotyczące tych zagadnień funkcjonujące w Kodeksie karnym z 1969 r.

Tajemnica obowiązywała pracowników którzy zapoznali się z tego rodzaju informacjami w toku wykonywania obowiązków służbowych i to również po ustaniu stosunku pracy. Wiadomości stanowiące tajemnicę mogły być wyrażone za pomocą pisma (dokumenty), mowy (meldunki ustne), dźwięku, obrazu, rysunku, znaku jak również w postaci urządzenia, przyrządu lub w inny sposób. W ustawie zawarto zasadę, że dopuszczenie do tajemnicy państwowej możliwe było wobec obywatela polskiego dającego rękojmię zachowania tajemnicy i zarazem wykonującego pracę wymagającą dostępu do tego typu wiadomości. Podstawą dopuszczenia było uzyskanie pisemnego upoważnienia wydawanego przez kierownika jednostki organizacyjnej dysponującej informacjami. Wyjątki przewidziano dla:

– osób wskazanych przez Marszałka Sejmu – zatrudnionych w organach wykonawczych i doradczych Sejmu;

– osób wskazanych przez Przewodniczącego Rady Państwa – zatrudnionych w organach powoływanych, nadzorowanych i podległych Radzie Państwa;

– osób wskazanych przez Prezesa Rady Ministrów – zatrudnionych w naczelnych, centralnych i terenowych organach administracji państwowej.

Sporządzali oni wykazy stanowisk i funkcji, wiążących się z dostępem do informacji niejawnych bez konieczności uzyskiwania upoważnienia.

W ustawie z 1982 r. wymieniono następujące klauzule tajności: „ściśle tajne" – dla oznaczania wiadomości stanowiących tajemnicę państwową o szczególnym znaczeniu dla bezpieczeństwa i obronności państwa, „tajne" – dla oznaczania wiadomości stanowiących tajemnicę państwową innych niż poprzednio wymienione, „poufne" – dla oznaczania tajemnic służbowych. W art. 13 zawarto zasadę że w kontaktach z Układem Warszawskim i RWPG należy w pierwszej kolejności stosować reguły przyjęte w tych organizacjach. Organami odpowiedzialnymi za ochronę tajemnicy służbowej były naczelne i centralne organy państwowe (dla jednostek sobie podległych i nadzorowanych), terenowe organy administracji państwowej stopnia wojewódzkiego (wobec jednostek organizacyjnych podporządkowanych radom narodowym) oraz kierownicy państwowych, spółdzielczych i społecznych jednostek organizacyjnych. Powyższe przepisy zostały poddane wielu zmianom w latach 1989-1999. Wynikało to z przemian ustrojowych w Polsce jak i zmiany zasad funkcjonowania organów administracji publicznej[14]. Zniesiono szereg organów (np. Radę Państwa), powołując w ich miejsce inne o odmiennych kompetencjach.

Lata 1999-2011. W dniu 22 stycznia 1999 r. Prezydent RP podpisał ustawę o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95). Zmiana ustawy pociągnęła za sobą konieczność przyjęcia szeregu nowych aktów wykonawczych i procedur działania. Proces ten trwał do roku 2005, a jego celem było dostosowanie prawa polskiego do przepisów zarówno Organizacji Traktatu Północnoatlantyckiego (NATO), jak i Unii Europejskiej[15]. Ponadto nowe

[14] W latach 1989-1999 podejmowano działania legislacyjne w celu unowocześnienia całego systemu ochrony informacji niejawnych w państwie. 15 września 1994 r. Sejm uchwalił nową ustawę o ochronie tajemnicy państwowej i służbowej. Prezydent Lech Wałęsa zapowiedział zgłoszenie weta wobec ustawy popieranej przez rząd. W trakcie dalszego procesu legislacyjnego Senat postanowił odrzucić ustawę wbrew stanowisku Rady Ministrów. W dniu 7 października 1994 r. Sejm nie zdołał odrzucić weta Senatu i tym samym uchwalić ustawy. W 1994 r. zgłoszono jeszcze dwa poselskie projekty ustaw o ochronie informacji niejawnych oparte w swoich zrębach na tekście odrzuconej ustawy. Uwzględniono przy tym krytyczne uwagi zgłaszane przez senatorów. Jednak w obu przypadkach nie zdołano doprowadzić procesu legislacyjnego do końca. Wobec tego w dniu 27 sierpnia 1997 r. Sejm uchwalił ustawę o zmianie ustawy o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 110, poz. 714). Celem nowelizacji było m.in. przygotowanie Polski do członkostwa w NATO.

[15] Szerzej na ten temat w uzasadnieniu do projektu uoin – druk sejmowy nr 2791 z dnia 16 lutego 2010 r., s. 156-160.

uregulowania prawne uwzględniały rosnącą rolę systemów informatycznych używanych w codziennej działalności administracji publicznej.

Najistotniejsze zmiany dotyczyły:

– definicji i nazewnictwa informacji niejawnych;

– zakresu czasowego ochrony;

– szkoleń;

– wymaganej dokumentacji z zakresu ochrony.

W ustawie z 1999 r. po raz pierwszy wymieniono i opisano kluczowe elementy tworzące system ochrony informacji niejawnych. Zaliczono do niego:

– bezpieczeństwo osobowe zawierające procedury kontroli dostępu osób fizycznych do informacji;

– bezpieczeństwo fizyczne zawierające wymagania oraz sposób doboru środków ochrony fizycznej i technicznej;

– bezpieczeństwo teleinformatyczne – oparte na zastosowaniu procesu akredytacji i certyfikacji systemów teleinformatycznych;

– bezpieczeństwo przemysłowe – oparte na zastosowaniu ww. elementów w postaci spójnego zbioru działań podejmowanych przez przedsiębiorców.

W artykule 2 ustawy z 1999 r. ustawodawca zawarł definicję tajemnicy państwowej. Zgodnie z nią za tajemnicę państwową uznano taką informację, która spełniała łącznie dwa warunki: została zawarta w załączniku nr 1 do ww. ustawy i jej nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa. Definicja odnosiła się do czynników materialnych[16].

Zwolennicy definicji materialno-formalnej wymieniali dodatkowo trzeci warunek, który powinna spełnić informacja, aby można ją było uznać za tajemnicę państwową. Był nim zaklasyfikowanie, przez przyznanie jej w sposób wyraźny, jednej z klauzul tajności przewidzianych w art. 23 i 24 wspomnianej ustawy[17]. Fakt klasyfikacji miał natomiast wpływ na zakres odpowiedzialności karnej osoby, która znalazła się w posiadaniu nieoznaczonej tajemnicy państwowej (tj. pozbawionej wszelkich zewnętrznych znamion identyfikujących). Trudno sobie bowiem wyobrazić, aby obywatel samodzielnie dokonał klasyfikacji, jeśli nie zrobił tego podmiot, który dopuścił do utraty informacji niejawnej.

---

[16] T. Szewc, *Ochrona informacji niejawnych. Komentarz*, Wydawnictwo C.H. Beck 2007, s. 69-75.

[17] Był to pogląd dyskusyjny ponieważ w ustawie nie wymagano do uznania za tajemnicę państwową wystąpienia przesłanki w postaci klasyfikacji lub oznaczenia. Czynność miała więc charakter wtórny (podobnie jak w aktualnych przepisach). Potwierdzała ona jedynie fakt wystąpienia czynników natury obiektywnej. W innym przypadku ochrona informacji rozpoczynałaby się dopiero od momentu klasyfikacji – ponieważ wtedy nastąpiłoby uznanie jej za niejawną. Szerzej na ten temat: S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych – wybrane zagadnienia*. Wyd. Uniwersytetu Opolskiego, Opole 2006, s. 23-34.

W ramach tajemnicy państwowej wyróżniano informacje oznaczone klauzulą „ściśle tajne" i „tajne". Jednoznaczne odróżnienie jednych od drugich wynikało z umieszczenia w odrębnych częściach wspomnianego załącznika nr 1. W pierwotnym tekście ustawy z 1999 r. do pierwszej kategorii zaliczano informacje, których nieuprawnione ujawnienie mogło spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych. Były to więc tylko informacje o najwyższej wartości dotyczące podstaw bezpieczeństwa, niepodległości i suwerenności Polski. Ich utrata stanowiła istotne zagrożenie dla tych wartości. Do kategorii „tajne" zaliczano natomiast informacje, których nieuprawnione ujawnienie mogło spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę[18]. Wielu badaczy krytykowało zbyt kazuistyczny i szczegółowy charakter listy tajemnic państwowych zawartych we wspomnianym załączniku nr 1 do ustawy. Głosy te stały się podstawą przyjęcia odmiennych rozwiązań w ustawie z 2010 r. W przyjętej definicji próbowano godzić dwa przeciwstawne cele – z jednej strony zapewniać możliwość jednoznacznego odróżnienia informacji niejawnych od ogólnie dostępnych (w myśl zasady określoności prawa), z drugiej strony zagwarantować niezbędną elastyczność w toku praktycznego zastosowania przepisów. Definicja taka wpływała pośrednio na zakres odpowiedzialności karnej i granice swobód obywatelskich (tworząc próg dostępu obywatela do informacji publicznej). Załącznik nr 1 ustawy z 1999 r. zatytułowano „Wykaz rodzajów informacji, które mogą stanowić tajemnicę państwową". I część zawierała typologię informacji niejawnych mogących stanowić tajemnicę państwową o klauzuli „ściśle tajne". Dotyczyły one najważniejszych zagadnień obronności, bezpieczeństwa publicznego, interesów gospodarczych państwa.

Sprecyzowane je w postaci 29 zagadnień, które można podzielić na następujące grupy:

– informacje o systemie kierowania państwem i dowodzenia Siłami Zbrojnymi RP;

– sprawy gospodarczo-obronne (np. Centralny Plan Mobilizacji Gospodarki, militaryzacja, badania naukowe ważne dla bezpieczeństwa i obronności państwa);

– działania operacyjne Sił Zbrojnych;

– działania operacyjno-rozpoznawcze służb ochrony państwa (w tym dane osobowe ich funkcjonariuszy, żołnierzy, współpracowników – uprawnionych do wykonywania czynności operacyjno-rozpoznawczych);

[18] Trybunał Konstytucyjny w uchwale z 13 czerwca 1994 r. (W.3/94) zaznaczył, że „istotne interesy" państwa nie powinny mieć charakteru abstrakcyjnego i statycznego. Ich treść należy ściśle wiązać z aksjologią systemu prawnego RP.

– ochrona informacji niejawnych (m.in. sieci teleinformatyczne, hasła i kody dostępu do urządzeń służących do przechowywania, przetwarzania, przesyłania informacji oznaczonych klauzulą „ściśle tajne");

– informacje oznaczone jako „top secret" (lub równorzędne) – wymieniane przez Polskę w kontaktach z organizacjami międzynarodowymi.

W części drugiej załącznika zawarto informacje, które mogą zostać oznaczone klauzulą „tajne". Wymieniono je w postaci 59 zagadnień, które można podzielić na następujące grupy:

– sprawy gospodarczo-obronne (m.in. wojewódzkie i resortowe plany mobilizacji gospodarki, założenia finansowania państwa w stanie podwyższonej gotowości obronnej i wojny, produkcja specjalna przemysłu obronnego);

– budownictwo specjalne oraz obiekty inżynieryjnej rozbudowy terenu prognozowanych działań wojennych;

– sieć telekomunikacyjna państwa dla potrzeb obronnych;

– plany obrony cywilnej województw;

– rezerwy państwowe na wypadek wojny;

– informacje dotyczące osób podejrzanych o prowadzenie działalności godzącej w bezpieczeństwo, obronność, niezależność, całość oraz międzynarodową pozycję państwa albo działalność terrorystyczną;

– system ochrony granicy państwowej;

– dane dotyczące potencjału strategicznego państwa oraz zamówień rządowych w tym zakresie;

– technologia produkcji i zabezpieczenia dokumentów o szczególnym znaczeniu dla państwa (w tym: znaków pieniężnych, znaków akcyzy, dowodów tożsamości oraz papierów wartościowych emitowanych przez Skarb Państwa);

– działanie służby dyplomatycznej (m.in. poczta dyplomatyczna, ochrona placówek dyplomatycznych i konsularnych);

– obrót sprzętem specjalnym (w tym uzbrojeniem);

– informacje oznaczone jako „secret" (lub równorzędne) – wymieniane przez Polskę w kontaktach z organizacjami międzynarodowymi.

Porównując pierwszą i drugą część załącznika, było oczywiste, że w obu kategoriach pojawiały się informacje dotyczące tych samych zagadnień. Zatem granica pomiędzy informacjami określanymi jako „ściśle tajne" i „tajne" była płynna i trudna do określenia na pierwszy rzut oka. W takiej sytuacji stosowano zasadę, że informacja zbiorcza otrzyma klauzulę wyższą niż informacja cząstkowa wchodząca w jej skład.

W art. 2 ustawy z 1999 r. umieszczono również definicję tajemnicy służbowej. Była nią informacja niebędąca tajemnicą państwową uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, jeśli jej nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Wadą był brak wyraźnego rozróżnienia pomiędzy informacjami ozna-

czonymi klauzulą „zastrzeżone" i „poufne". Ponadto trudne do zaakceptowania było uznanie informacji za niejawną tylko ze względu na ochronę interesu jednostki organizacyjnej czy też obywateli. Powinna ona zostać uznana co najwyżej za tajemnicę przedsiębiorstwa lub za dane osobowe i objęta ochroną na podstawie innych przepisów. Takie zdefiniowanie tajemnicy służbowej wpłynęło na znaczne zwiększenie ogólnej liczby informacji niejawnych pozostających w obiegu. Miało również wpływ na zwiększenie liczby postępowań sprawdzających przeprowadzanych wobec urzędników samorządowych uzyskujących dostęp do takich informacji. Opisane wątpliwości uwzględniono w toku prac na ustawą obecnie obowiązującą.

Powyższe przepisy zostały poddane wielu zmianom w latach 1999-2010. Wynikało to ze zmian ustrojowych w Polsce, jak i zasad funkcjonowania organów administracji publicznej. Zmianie uległ podział terytorialny kraju oraz rola i kompetencje wielu organów. W toku kolejnych nowelizacji ustawy uwzględniano ponadto modyfikacje przepisów Organizacji Traktatu Północnoatlantyckiego (NATO) i Unii Europejskiej. Zaliczymy do nich:

– Umowę między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzoną w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740);

– wewnętrzne akty prawne UE: Decyzję Komisji 1999/218/WE z 25 lutego 1999 r. odnoszącą się do procedur, w ramach których urzędnicy i pracownicy Komisji Europejskiej mogą uzyskiwać dostęp do informacji niejawnych będących w posiadaniu Komisji [notyfikowana jako dokument C(1999) 423] (Dz. Urz. WE L 80 z 25.03.1999 r.); Regulamin Komisji (C(2000) 3614) z 29 listopada 2000 r. (Dz. Urz. WE L 308 z 08.12.2000 r. z późn. zm.).

Podstawy prawne ochrony informacji niejawnych – organizacja systemu. Podstawą prawną jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) – zwana dalej ustawą (uoin) oraz akty wykonawcze wydane do niej. Wspomniana ustawa zawiera definicję informacji niejawnych. Ma ona charakter materialny i jest oparta na kombinacji dwóch elementów: treści informacji oraz przewidywanych skutków ich ujawnienia. Do ww. grupy zaliczymy informacje dotyczące:

1. ochrony niepodległości, suwerenności oraz integralności terytorialnej Polski;
2. bezpieczeństwa wewnętrznego oraz ochrony porządku konstytucyjnego;
3. sojuszy i pozycji międzynarodowej Polski;
4. gotowości obronnej kraju;
5. interesów ekonomicznych Polski;
6. danych identyfikujących funkcjonariuszy, żołnierzy oraz pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, wykonującym czynności operacyjno-rozpoznawcze;

7. danych o działaniach funkcjonariuszy, żołnierzy lub pracowników, w zakresie wykonywanych przez nich czynności operacyjno-rozpoznawczych;

8. danych osób udzielających pomocy wspomnianym osobom opisanym w punktach 6-7;

9. informacji na temat świadków koronnych, osób im najbliższych oraz świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.) lub osób dla nich najbliższych.

Niezbędne jest równoczesne istnienie prawdopodobieństwa spodziewanej szkody wynikającej z nieuprawnionego ujawnienia informacji zaliczanej do powyższej grupy. Natężenie owej szkody decyduje o nadaniu właściwej klauzuli. W ustawie przewidziano cztery klauzule tajności od najwyższej do najniższej: „ściśle tajne", „tajne", „poufne", „zastrzeżone". Trzeba przy tym pamiętać, że ochronie podlegają informacje w każdej formie – tj. bez względu na ich substrat materialny. Mogą one zaistnieć zarówno w formie dokumentu, przedmiotu (w tym urządzenia lub wyposażenia), zbioru danych, obrazu i dźwięku (lub ich zapisu). Podstawą przyznania określonej klauzuli tajności jest dokonanie ich klasyfikacji, która polega na porównaniu cech informacji z treścią definicji ustawowej. Czynności tej dokonują osoby uprawnione do podpisywania dokumentów lub materiałów.

Wspomniana ustawa reguluje działanie następujących podmiotów:

a) organów władzy publicznej, w tym: Sejmu, Senatu, Prezydenta RP, organów administracji rządowej, organów jednostek samorządu terytorialnego, Narodowego Banku Polskiego;

b) innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych;

c) sądów i trybunałów;

d) organów kontroli państwowej i ochrony prawa;

e) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

f) państwowych osób prawnych i innych niż wymienione w lit. *a-e* – państwowych jednostek organizacyjnych;

g) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;

h) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy oraz wykonujących zadania związane z dostępem do informacji niejawnych na podstawie przepisów prawa.

Oznacza to, że przepisom tym będą podlegać również przedsiębiorcy wykonujący a nawet ubiegający się o wykonanie kontraktów komercyjnych na rzecz Sił Zbrojnych (np. z zakresu robót budowlanych) oraz agend państwowych.

W ustawie wymieniono i opisano najważniejsze elementy tworzące system ochrony informacji niejawnych w Polsce. Zaliczono do niego:

– bezpieczeństwo osobowe – oparte na procedurach kontroli dostępu osób fizycznych do informacji;

– bezpieczeństwo fizyczne – oparte na procedurach oceny zagrożeń oraz ryzyka dla informacji niejawnych (nieznanych we wcześniejsze ustawie z 1999 roku). W zależności od wyników obu czynności dobiera się adekwatne środki ochrony fizycznej i technicznej – dostosowane do potrzeb konkretnej jednostki organizacyjnej;

– bezpieczeństwo teleinformatyczne – oparte na zastosowaniu procesu akredytacji i certyfikacji systemów teleinformatycznych;

– bezpieczeństwo przemysłowe – oparte na zastosowaniu ww. elementów w postaci spójnego zbioru działań podejmowanych przez przedsiębiorców.

Mówiąc o podstawach prawnych ochrony informacji niejawnych, trudno pominąć akty prawa międzynarodowego, których stroną jest Rzeczpospolita Polska. Ich zastosowanie wynika m.in. z członkostwa w Unii Europejskiej i Traktacie Północnoatlantyckim (NATO) oraz współpracy cywilno-wojskowej z innymi państwami. Do aktów tych zaliczymy:

– umowy bilateralne pomiędzy Polską a innymi państwami (np. Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Państwa Izrael reprezentowanym przez Ministerstwo Obrony o wzajemnej ochronie informacji niejawnych związanych ze współpracą obronną i wojskową, podpisana w Jerozolimie dnia 24 lutego 2011 r. – Dz. U. z 2012 r. Poz. 253, czy też Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Francuskiej o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie dnia 28 maja 2008 r. – Dz. U. z 2009 r. Nr 49, poz. 394;

– akty prawa międzynarodowego podpisane przez Polskę w związku z przystąpieniem do organizacji międzynarodowych – najczęściej wielostronne (np. Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r. Dz. U. z 2000 r. Nr 64, poz. 740; Umowa między Rządem Rzeczypospolitej Polskiej a Organizacją do spraw Współpracy w Zakresie Uzbrojenia [OCCAR] o ochronie informacji niejawnych dotyczących realizacji Programu OCCAR ESSOR, podpisana w Warszawie dnia 29 kwietnia 2009 r. oraz w Bonn dnia 4 maja 2009 r. – Dz. U. z 2010 r. Nr 70, poz. 455);

– wewnętrzne akty prawne organizacji międzynarodowych, których członkiem jest Polska (np. Decyzja Komisji 1999/218/WE z 25 lutego 1999 r. odnosząca się do procedur, w ramach których urzędnicy i pracownicy Komisji Europejskiej mogą uzyskiwać dostęp do informacji niejawnych będących w posiadaniu Komisji [notyfikowana jako dokument C(1999) 423] (Dz. Urz. WE L 80 z 25.03.1999 r.); Regulamin Komisji (C(2000) 3614) z 29 listopada 2000 r. (Dz. Urz. WE L 308 z 08.12.2000 r. z poźn. zm.); De-

cyzja Rady 2011/292/EU z 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz. U. UE L 141 z 27.05.2011 r.).

Sytuację prawną komplikują również umowy podpisywane przez te organizacje z innymi państwami, ponieważ pośrednio wiążą także Polskę (np. Umowa między Unią Euro-pejską a rządem Stanów Zjednoczonych Ameryki w sprawie bezpieczeństwa informacji niejawnych – Dz. Urz. UE L 115 z 3.05.2007 r.).

Wpływ wspomnianych przepisów ma wiele praktycznych aspektów – np. wiąże się z koniecznością wydawania dodatkowych dokumentów poświadczających dostęp osób fizycznych do informacji niejawnych Unii Europejskiej i NATO.

W przepisach krajowych wskazano osoby odpowiedzialne za ochronę informacji niejawnych. Należą do nich:

a) kierownik jednostki organizacyjnej, w której przetwarza się informacje. Do jego zadań należy:

– zorganizowanie i zapewnienie funkcjonowania ich ochrony. Czyni to poprzez zatwierdzanie statutu i regulaminu tej jednostki oraz regulaminów wewnętrznych komórek organizacyjnych z uwzględnieniem zadań dotyczących ochrony informacji. W celu wykonania tego zadania może również powołać samodzielny pion ochrony informacji niejawnych;

– zatrudnienie pełnomocnika ds. ochrony informacji niejawnych i nadzorowanie jego pracy. Czyni to poprzez ustalenie zakresu obowiązków na wspomnianym stanowisku oraz planu pracy na kolejne lata oraz przyjmowanie i ocenę sprawozdania z wykonania zadań. Ustala również plan kontroli wewnętrznych prowadzonych przez pełnomocnika w danym roku i wydaje pisemne upoważnienia do ich przeprowadzenia. Po zakończeniu zapoznaje się z treścią protokołów kontroli i czuwa nad wykonaniem zaleceń w nich zawartych;

– przeprowadzanie cyklicznych przeglądów informacji niejawnych – nie rzadziej niż raz na 5 lat;

– zatwierdzanie dokumentacji wymaganej przepisami (w szczególności: planu ochrony informacji niejawnych, dokumentacji szacowania ryzyka);

– wydawanie pisemnych upoważnień – w celu udzielenia dostępu do informacji o klauzuli „zastrzeżone" osobom zatrudnionym w jednostce organizacyjnej;

– wydawanie pełnomocnikowi poleceń przeprowadzenia zwykłych postępowań sprawdzających;

– występowanie do ABW albo SKW z wnioskami o przeprowadzenie poszerzonych postępowań sprawdzających;

– informowanie ABW albo SKW o zatrudnieniu osób posługujących się ważnymi poświadczeniami bezpieczeństwa;

– udzielanie akredytacji bezpieczeństwa teleinformatycznego dla własnego systemu teleinformatycznego, przeznaczonego do przetwarzania informacji o klauzuli „zastrzeżone". Ponadto informowanie o tym ABW albo SKW oraz przesyłanie stosownej dokumentacji;

– opracowanie i przedłożenie ABW albo SKW dokumentacji w celu udzielenia przez Agencję akredytacji dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji oznaczonych klauzulą „ściśle tajne", „tajne", „poufne";

– wyznaczenie pracowników do obsługi ww. systemów teleinformatycznych (tj. inspektora bezpieczeństwa teleinformatycznego i administratora systemu);

– znoszenie i dokonywanie zmiany klauzul tajności przyznanych dokumentom wytworzonym w podległej jednostce organizacyjnej.

b) pełnomocnik ds. ochrony informacji niejawnych. Do jego zadań należy:

– zapewnienie ochrony informacji niejawnych oraz systemów teleinformatycznych przeznaczonych do ich przetwarzania;

– prowadzenie wewnętrznych kontroli z zakresu ochrony informacji niejawnych oraz przestrzegania przepisów w tym zakresie;

– prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających wobec osób zatrudnionych w jednostce organizacyjnej lub wykonujących na jej rzecz prace zlecone;

– prowadzenie wykazu osób zatrudnionych, pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, uprawnionych do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;

– opracowanie i aktualizowanie dokumentacji z zakresu ochrony informacji niejawnych w jednostce organizacyjnej;

– przekazywanie odpowiednio ABW lub SKW danych osób uprawnionych do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub podjęto decyzję o jego cofnięciu;

Pełnomocnik kieruje samodzielnym pionem ds. ochrony informacji niejawnych (jeśli pion został powołany)[19]. Należy podkreślić, że wspomniana osoba podlega bezpośrednio kierownikowi wymienionemu w lit. *a*.

c) kierownik kancelarii tajnej. Do jego obowiązków zaliczamy:

– nadzór nad obiegiem materiałów zawierających informacje niejawne, w tym ich rejestracja w urządzeniach ewidencyjnych;

– udostępnianie i wydawanie ww. materiałów osobom uprawnionym oraz egzekwowanie ich zwrotu;

– kontrola przestrzegania właściwego oznaczania materiałów.

---

[19] Z obecnej ustawy usunięto prerogatywę pełnomocnika zapisaną w art. 18 ust. 6 uoin z 1999 r. Mianowicie pełnomocnik miał prawo żądać (w zakresie realizacji swoich zadań) natychmiastowej pomocy od komórek organizacyjnych w swojej jednostce organizacyjnej na wypadek wprowadzenia stanu nadzwyczajnego.

Stanowisko to występuje w jednostkach posiadających kancelarie tajne (tj. przetwarzających materiały tajne lub ściśle tajne)[20]. W innym wypadku czynności te może dokonywać osobiście pełnomocnik lub upoważniony do tego pracownik. Zasady działania kancelarii reguluje rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631).

d) administrator systemu teleinformatycznego oraz inspektor bezpieczeństwa teleinformatycznego. Są to osoby odpowiedzialne za nadzór nad systemami teleinformatycznymi przeznaczonymi do przetwarzania informacji niejawnych. Dokładny zakres obowiązków tych osób wynika z treści dokumentacji wykonywanej dla każdego systemu odrębnie. Zawsze jednak należy do nich: weryfikacja i bieżąca kontrola zgodności działania systemu teleinformatycznego z dokumentacją bezpieczeństwa, obsługa systemu w tym udzielanie dostępu wyznaczonym użytkownikom oraz zapewnienie poufności, integralności i dostępności danych zawartych w systemie;

e) użytkownicy informacji niejawnych. Są to osoby przetwarzające informacje niejawne. Ciążą na nich następujące obowiązki:

---

[20] W art. 47 ust. 3 uoin wskazano podmioty, którym przyznano szerszą swobodę w zakresie kształtowania systemu ochrony. Ich kierownicy mogą w drodze aktów wewnętrznych zmienić sposób organizacji kancelarii tajnych oraz zakres obowiązków pełnomocników ochrony. Są to jednostki organizacyjne podległe m.in.: ministrowi właściwemu do spraw wewnętrznych, administracji publicznej, spraw zagranicznych, finansów publicznych, Ministrowi Obrony Narodowej, Ministrowi Sprawiedliwości, Prokuratorowi Generalnemu, Szefom: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Komendantowi Głównemu Policji, Komendantowi Głównemu Straży Granicznej, Szefowi Biura Ochrony Rządu. Wspomniana swoboda wynika z wielopoziomowej i zróżnicowanej struktury tych jednostek. W celu realizacji wspomnianego uprawnienia Komendant Główny Policji wydał zarządzenie nr 2020 z dnia 30.12.2010 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji (DZ. Urz. KGP z 2011 r. Nr 1, poz. 5). W § 4 i 7 zarządzenia wskazano możliwość ustanawiania oddziałów kancelarii tajnych, obsługiwanych przez osoby wyznaczone przez kierownika kancelarii tajnej za zgodą pełnomocnika ds. ochrony informacji niejawnych. Podwyższono standardy cyklicznej kontroli ewidencji oraz obiegu informacji niejawnych. W tym celu w każdym roku powołuje się komisje inwentaryzacyjne, które dokonują kontroli zgodności stanu faktycznego dokumentacji niejawnej ze stanem ewidencyjnym, za rok poprzedni. Funkcjonariusze i pracownicy Policji są zobowiązani do przekazania ww. komisjom wykazu posiadanych materiałów niejawnych. Do dnia 31 maja pełnomocnik ochrony przedkłada kierownikowi jednostki organizacyjnej protokół inwentaryzacyjny. Ponadto w Centralnym Biurze Śledczym, Biurze Spraw Wewnętrznych Komendy Głównej Policji, komendach wojewódzkich (stołecznej), powiatowych (miejskich, rejonowych), komisariatach i komisariatach specjalistycznych Policji, oddziałach prewencji, samodzielnych pododdziałach prewencji oraz samodzielnych pododdziałach antyterrorystycznych Policji można powołać inne niż kancelaria tajna komórki organizacyjne – odpowiedzialne za przetwarzanie materiałów niejawnych. Ich kontrolę zapewnia właściwy pełnomocnik ochrony.

– obowiązek bezwzględnego zachowania w tajemnicy informacji niejawnych, z którymi zapoznali się w toku czynności służbowych. Obowiązek ten trwa, pomimo zakończenia zatrudnienia, służby lub wykonywania zadań warunkujących dostęp do informacji;

– obowiązek przestrzegania przepisów, w toku pracy z materiałami zawierającymi informacje niejawne. W szczególności chodzi tu o takie obchodzenie się z nimi, które uniemożliwia utratę ich poufności.

Bezpieczeństwo osobowe. Zasady bezpieczeństwa osobowego opisano w rozdziale 5 ustawy. Oparto je na ograniczeniu dostępu do informacji niejawnych wyłącznie do osób upoważnionych, spełniających łącznie następujące warunki:

– posiadanie ważnego poświadczenia bezpieczeństwa lub pisemnego upoważnienia (ewentualnie przynależą do grupy osób zwolnionych z tego obowiązku);

– odbycie przeszkolenia z zakresu ochrony informacji niejawnych;

– wykonywanie zadań wymagających dostępu do informacji niejawnych[21].

W przypadku informacji oznaczonych klauzulą „zastrzeżone", wymaga się wydania pisemnego upoważnienia. Uprawniony do tego jest kierownik jednostki organizacyjnej. W ustawie zawarto niewiele informacji na temat treści, terminu i zakresu obowiązywania tego dokumentu. W upoważnieniu należy zawrzeć następujące informacje:

– dane wskazujące początek jego obowiązywania (miejsce i datę wydania);

– podstawę prawną;

– dane osoby upoważnionej (tj. imię i nazwisko, nr PESEL, imiona rodziców);

– zakres uprawnień (przez wskazanie klauzuli informacji niejawnych);

– zakres czasowy obowiązywania – poprzez ustanowienie terminu ważności lub w odmienny sposób np. umieszczenie zwrotu „wydano na czas zatrudnienia";

– podpis osoby udzielającej upoważnienia (jest to kierownik jednostki organizacyjnej).

Sprawą dyskusyjną jest obowiązywanie upoważnień na obszarze innych jednostek organizacyjnych. Na ogół przyjmuje się, że osoby wyznaczone do wykonania czynności w imieniu podmiotu upoważniającego mogą skutecznie posługiwać się tym dokumentem na terenie innej jednostki organizacyjnej.

Wyjątkiem od powyższej zasady są uprawnienia kierownika jednostki organizacyjnej, który posiada dostęp do informacji oznaczonych klauzulą „zastrzeżone" automatycznie, z tytułu zajmowanego stanowiska – tj. bez dodatkowego upoważnienia.

---

[21] „Posiadanie uprawnień do dostępu do informacji niejawnej (stosowny certyfikat) nie jest wystarczające, jeżeli dostęp do nich nie jest związany z wykonywaniem pracy lub pełnieniem służby na zajmowanym stanowisku" (Wyrok WSA z 14 sierpnia 2007 r., II SA/Wa 280/07).

W toku wydawania upoważnień nie przeprowadza się dodatkowych procedur sprawdzających. Pracodawca opiera się na aktach z zakresu kadr – zgromadzonych na podstawie przepisów prawa pracy.

W ustawie pominięto kwestie trybu i przyczyn ewentualnego odebrania upoważnienia. Niewątpliwie zaliczamy do nich:

– naruszenie przepisów o ochronie informacji niejawnych;

– ustanie potrzeby jego dalszego posiadania.

Uchylenie upoważnienia powinno nastąpić w tej samej formie, w której nastąpiło udzielenie tj. na piśmie. W ustawie nie przewidziano trybu odwoławczego na wypadek odmowy wydania upoważnienia bądź jego cofnięcia. Oznacza to, że w takiej sytuacji odwołanie nie przysługuje.

W przypadku udzielania dostępu do informacji wyższych klauzul („poufne", „tajne", „ściśle tajne") wymaga się przeprowadzenia postępowania sprawdzającego oraz wydania odrębnego dokumentu – poświadczenia bezpieczeństwa.

Celem postępowania jest ustalenie czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Pojęcie rękojmi zdefiniowano w art. 2 pkt 2 ustawy jako zdolność do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem.

Udzielenie dostępu do informacji oznaczonych klauzulą „poufne" jest poprzedzone zwykłym postępowaniem sprawdzającym. Natomiast poszerzone postępowanie sprawdzające przeprowadza się w przypadku udzielania dostępu do informacji o klauzuli „tajne", „ściśle tajne". Podlegają mu także pełnomocnicy ds. ochrony, kandydaci na to stanowisko, kierownicy jednostek organizacyjnych, w których są przetwarzane informacje co najmniej „poufne".

Zwykłe postępowania sprawdzające przeprowadzają pełnomocnicy ds. ochrony informacji niejawnych. Czynią to wobec pracowników tam zatrudnionych lub wykonujących prace zlecone. Podstawą czynności jest na pisemne polecenie kierownika jednostki.

Poszerzone postępowania sprawdzające przeprowadzają:

– Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego – odpowiednio do kompetencji ustawowych;

– Agencja Wywiadu, CBA, Biuro Ochrony Rządu, Policja, Służba Więzienna, Służba Wywiadu Wojskowego, Straż Graniczna oraz Żandarmeria Wojskowa. Przeprowadzają one samodzielne postępowania wobec własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy i osób wykonujących czynności zlecone lub ubiegających się o ich wykonywanie (art. 23 ust. 5 ustawy)[22].

[22] Należy pamiętać, że wydane w ten sposób poświadczenia zachowują swoją ważność jedynie przez czas pracy lub służby w powyższych instytucjach. Nie dotyczy to jednak poświadczeń wydanych pod rządami poprzedniej ustawy – tj. do dnia 1 stycznia 2011 r. Wynika to z treści art. 182 aktualnej uoin, w której zapisano, iż poświadczenia bezpieczeństwa wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.

W toku postępowania ww. podmioty dokonują sprawdzenia danych zebranych w rejestrach, ewidencjach i kartotekach. W szczególności chodzi tu o Krajowy Rejestr Karny i akta stanu cywilnego. Dokonuje się również sprawdzeń w kartotekach i ewidencjach powszechnie niedostępnych, pozostających w posiadaniu służb specjalnych.

W postępowaniach poszerzonych zakres sprawdzeń jest większy i może objąć badanie stanu i obrotu na rachunku bankowym, zadłużenia osoby sprawdzanej, kontrolę dokumentacji medycznej, wywiad środowiskowy. W szczególnych wypadkach można również żądać poddania się specjalistycznym badaniom lekarskim.

Podstawą ww. działań są przede wszystkim informacje zawarte w ankiecie bezpieczeństwa osobowego przekazanej przez osobę sprawdzaną.

W obu przypadkach procedura może się zakończyć:

– wydaniem poświadczenia bezpieczeństwa;

– odmową wydania poświadczenia bezpieczeństwa;

– umorzeniem postępowania (przyczyny wymieniono w art. 31 ustawy).

Poświadczenia bezpieczeństwa wydaje się na czas oznaczony:

– 10 lat w przypadku informacji oznaczonych klauzulą „poufne”;

– 7 lat w przypadku informacji oznaczonych klauzulą „tajne”;

– 5 lat w przypadku informacji oznaczonych klauzulą „ściśle tajne”[23].

Poświadczenie umożliwiające dostęp do informacji o wyższej klauzuli umożliwia dostęp także do informacji o niższej klauzuli. Postępowanie powinno trwać nie dłużej niż 3 miesiące, licząc od daty złożenia ankiety bezpieczeństwa osobowego. Termin ten ma charakter instrukcyjny.

Na zasadzie wyjątku od ogólnej zasady możliwe jest dopuszczenie do informacji niejawnych osób, które nie posiadają poświadczenia bezpieczeństwa. Szefowie instytucji opisanych ustawie mogą udzielić jednorazowej zgody na udostępnienie takiej informacji lub wydać upoważnienie tymczasowe osobie, wobec której wszczęto już postępowanie sprawdzające (art. 34 ust. 5 ustawy). Upoważnienie jest ważne przez okres trwania wspomnianego postępowania. Pozostali kierownicy jednostek organizacyjnych mogą wydać upoważnienie tymczasowe tylko do klauzuli „poufne”.

Istnieje grupa osób wyłączonych spod działania zwykłych procedur sprawdzających. Opisano ją w art. 34 ustawy. Zaliczymy do niej m.in. Prezydenta RP, Marszałków Sejmu i Senatu, Premiera, ministrów, posłów i senatorów. Ponadto Prezydent RP i Premier w stanach nadzwyczajnych mogą wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.

---

[23] W latach 1999-2005 obowiązywały krótsze terminy ważności poświadczeń. Było to odpowiednio 3 lata dla klauzuli „ściśle tajne”, 5 lat dla klauzuli „tajne”. W przypadku informacji oznaczonych jako „poufne” i „zastrzeżone” termin wynosił tak jak obecnie 10 lat. Po dokonaniu zmian ustawowych przedłużono termin ważności wydanych wcześniej dokumentów.

Podmiot prowadzący procedurę odmawia wydania poświadczenia jeśli osobę sprawdzaną skazano prawomocnym wyrokiem sądu na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego (również popełnione za granicą), lub umyślne przestępstwo skarbowe (jeżeli czyn, za który nastąpiło skazanie, wywołuje wątpliwości, o których mowa poniżej). Ponadto powodem odmowy jest wystąpienie nie dającej się usunąć wątpliwości wymienionej w art. 24 ust. 2 i 3 ustawy (dotyczące m.in.: ewentualnej działalności terrorystycznej, sabotażowej, szpiegowskiej, zagrożenia ze strony obcych służb specjalnych, przestrzegania porządku konstytucyjnego, uczestnictwa i wspierania działalności partii lub innych organizacji, o których mowa w art. 13 Konstytucji RP, zatajenia informacji ważnych dla ochrony informacji niejawnych, podatności na szantaż, niewłaściwego postępowania z informacjami niejawnymi). Ponadto dotyczące poziomu życia przewyższającego poziom dochodów, informacji o zakłóceniach czynności psychicznych lub chorobie psychicznej, które mogą negatywnie wpłynąć na zdolność do wykonywania prac związanych z dostępem do informacji niejawnych, uzależnienia od alkoholu, środków odurzających lub psychotropowych (tylko w postępowaniu poszerzonym).

Jeśli po wydaniu poświadczenia bezpieczeństwa pojawią się okoliczności wskazujące, że osoba taka nie daje rękojmi zachowania tajemnicy, możliwe jest wszczęcie kontrolnego postępowania sprawdzającego. Podmiotem uprawnionym jest organ właściwy do przeprowadzenia kolejnego postępowania – pełnomocnik u obecnego pracodawcy oraz ABW lub SKW w przypadkach uzasadnionych względami bezpieczeństwa państwa. Postępowanie to powinno zostać zakończone w terminie 6 miesięcy (z możliwością przedłużenia o następne 6 m-cy). Skutkiem wszczęcie postępowania kontrolnego jest odebranie osobie sprawdzanej dostępu do informacji niejawnych – na czas jego trwania[24].

Umorzenie postępowania, jego zawieszenie, odmowa wydania poświadczenia bezpieczeństwa lub jego cofnięcie mają formę decyzji administracyjnej, pochodzącej od organu prowadzącego postępowanie. W tym wypadku stosuje się przepisy art. 104 ustawy z dnia 14 czerwca 1960 r. Kodeksu postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.) oraz art. 3 i art. 30 ustawy. Prawo do wniesienia odwołania posiada każda

[24] Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 listopada 2007 r. II SA/Wa 1350/07 odniósł się do kwestii rozwiązywania stosunku służby z oficerem BOR, któremu prawomocnie cofnięto poświadczenie bezpieczeństwa. Zgodnie z art. 23 ust. 4 ustawy z 16 marca 2001 r. o Biurze Ochrony Rządu (Dz. U. z 2004 r. Nr 163, poz. 1712 ze zm.) warunkiem służby czynnej funkcjonariuszy tej formacji jest posiadanie stosownego poświadczenia bezpieczeństwa. W wyroku podkreślono, że brak dostępu do informacji niejawnych będący skutkiem wszczęcia postępowania kontrolnego nie stanowi wystarczającej przesłanki do zwolnienia ze służby. Jest to możliwe dopiero po uprawomocnieniu się decyzji o cofnięciu poświadczenia.

osoba, wobec której umorzono postępowanie, odmówiono wydania poświadczenia bezpieczeństwa lub poświadczenie takie cofnięto[25].

W przypadku decyzji wydawanych na podstawie art. 23 ust. 5 ustawy w Policji, Żandarmerii Wojskowej, Straży Granicznej, Agencji Wywiadu, Służbie Więziennej, Centralnym Biurze Antykorupcyjnym, Służbie Wywiadu Wojskowego (wymienione instytucje prowadzą samodzielnie postępowania sprawdzające wobec osób tam służących, zatrudnionych oraz ubiegających się o pracę lub przyjęcie do służby) oraz ABW i SKW – organem odwoławczym jest Prezes Rady Ministrów. W przypadku postępowań prowadzonych przez pełnomocników – organem odwoławczym jest Szef Agencji Bezpieczeństwa Wewnętrznego albo Szef Służby Kontrwywiadu Wojskowego[26]. Podział kom-

[25] Pierwotnie kwestie powyższe uregulowano w art. 42 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95). W ust. 1 zapisano „*Do postępowania sprawdzającego nie mają zastosowania przepisy Kodeksu postępowania administracyjnego oraz przepisy o zaskarżaniu do Naczelnego Sądu Administracyjnego*". Powyższy zapis został zaskarżony przez Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego jako niezgodny z konstytucją. Wyłączenie możliwości zastosowania Kodeksu postępowania administracyjnego w ramach postępowań sprawdzających było równoznaczne z odebraniem możliwość użycia środków kontrolnych właściwych dla decyzji administracyjnych. Skarżący argumentował, że treść przepisu narusza następujące zasady konstytucyjne: prawo do sądu opisane w art. 45 ust 1, zakaz zamykania drogi sądowej w celu dochodzenia naruszonych wolności i praw – opisane w art. 77 ust. 2 oraz prawo dostępu do służby publicznej – przyznane w art. 60. Wyrokiem z 10 maja 2000 r. (sygn. Akt k. 21/99) Trybunał Konstytucyjny uznał kwestionowany przepis za niezgodny z art. 45 i art. 77 Konstytucji RP. Uznano tym samym argumentację zawartą w skardze. Ponadto wskazano na sprzeczność tego przepisu z art. 13 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284). Wskazano jako niedopuszczalne pozbawienie osoby sprawdzanej jakiegokolwiek skutecznego środka zaskarżenia. TK zawarł we wspomnianym orzeczeniu wiele istotnych wniosków, mających wpływ na charakter postępowania sprawdzającego oraz wydawanych rozstrzygnięć. Efektem postępowania (zdaniem trybunału) jest wydanie aktu władczego, o skutkach w zakresie praw osoby sprawdzanej. Dlatego odmowa wydania poświadczenia musi być traktowana jako akt administracyjny z konsekwencjami w postaci kognicji sądu administracyjnego i prawa do procedury odwoławczej. Utrata mocy obowiązującej zaskarżonego przepisu nastąpiła w dniu 31 stycznia 2001 r.

Następstwem orzeczenia TK było uchwalenie ustawy z dnia 3 lutego 2001 r. o zmianie ustawy o ochronie informacji niejawnych – Dz. U. Nr 22, poz. 247, która weszła w życie z dniem 8 kwietnia 2001 r. Zmieniono treść art. 42 oraz uchylono art. 43. W miejsce dotychczasowego rozwiązania wprowadzono nowy rozdział 5a zatytułowany „Postępowanie odwoławcze i skargowe". Dodano art. 48a w brzmieniu „osobie sprawdzanej przysługuje skarga do Naczelnego Sądu Administracyjnego, w terminie 30 dni od dnia doręczenia decyzji lub postanowienia". Prezes Rady Ministrów wydał rozporządzenie z dnia 15 maja 2001 r. zmieniające rozporządzenie w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Janusza Pałubickiego (Dz. U. Nr 50, poz. 518). Tym samym premier upoważnił ministra koordynatora ds. służb specjalnych do wydawania decyzji i postanowień wg nowej procedury odwoławczej (w myśl art. 48c i 48f u.o.i.n. z 1999 r.).

[26] H. Sawicka, Postępowanie odwoławcze od decyzji pełnomocników do spraw ochrony informacji niejawnych – 10 lat doświadczeń szefa ABW jako organu II instancji. Przegląd Bezpieczeństwa Wewnętrznego nr 7 (4)/2012., s. 51-66. Od rozstrzygnięć wydanych w tym trybie odwoławczym przysługuje skarga do Wojewódzkiego Sądu Administracyjnego w Warszawie.

petencji ABW i SKW w rozpatrywania odwołań jest analogiczny do właściwości obu służb w ramach postępowań sprawdzających. Organ odwoławczy wydaje decyzję, w której:

1) utrzymuje w mocy decyzję organu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające;

2) uchyla decyzję wydaną w toku kontrolnego postępowania sprawdzającego zakończonego cofnięciem poświadczenia bezpieczeństwa;

3) uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające i nakazuje mu wydanie poświadczenia bezpieczeństwa;

4) uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia;

5) stwierdza nieważność decyzji podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające[27].

Skutkiem wniesienia odwołania jest brak ostateczności decyzji. Oznacza to, że decyzja taka nie przesądza definitywnie o odmowie dostępu do informacji niejawnych. Od decyzji przysługuje skarga do wojewódzkiego sądu administracyjnego.

Warunkiem otrzymania dostępu do informacji niejawnych jest ponadto odbycie szkolenia opisanego w art. 19 ustawy. Jego organizatorem jest pełnomocnik ochrony – wobec osób zatrudnionych w jednostce lub wykonujących na jej rzecz prace zlecone. Pełnomocników szkoli ABW lub SKW. Dotyczy to również kierowników jednostek organizacyjnych, w których przetwarza się informacje oznaczone klauzulą, co najmniej „tajne". Szkolenie powinno zostać potwierdzone pisemnym zaświadczeniem. Osoba przeszkolona jest ponadto zobowiązana do podpisania oświadczenia o zapoznaniu się z treścią przepisów[28]. Szkolenia powinny być ponawiane – nie rzadziej niż raz na 5 lat.

Bezpieczeństwo fizyczne. Zgodnie z treścią art. 45 ustawy jednostki organizacyjne, przetwarzające informacje niejawne, stosują środki bezpieczeństwa fizycznego dostosowane do poziomu zagrożeń. Zasady dokonywania oceny zagrożeń i standardy bezpieczeństwa opisano szczegółowo w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w prawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych

[27] Organy prowadzące postępowania sprawdzające mogą również wznowić postępowanie zakończone decyzją ostateczną o odmowie wydania albo o cofnięciu poświadczenia bezpieczeństwa – jeżeli decyzję tę wydano tylko w związku z przedstawieniem osobie sprawdzanej zarzutu popełnienia przestępstwa, postawieniem jej w stan oskarżenia lub skazaniem za przestępstwo umyślne (ścigane z oskarżenia publicznego) lub umyślne przestępstwo skarbowe). Warunkiem jest umorzenie lub zakończenie uniewinnieniem wspomnianego postępowania karnego.

[28] Treść oświadczenia nie została dokładnie wskazana w przepisach. Należy jednak przyjąć, że powinna w sposób jasny potwierdzać również znajomość reguł odpowiedzialności dyscyplinarnej i karnej na wypadek naruszenia przepisów.

(Dz. U. poz. 683). Procedura zapewnienia bezpieczeństwa fizycznego odbywa się dwuetapowo.

W pierwszym etapie należy dokonać oceny poziomu zagrożeń w oparciu o 6 kryteriów wymienionych w przywołanym rozporządzeniu. Zaliczamy do nich: klauzule tajności przetwarzanych informacji, liczbę materiałów niejawnych, postać informacji, liczbę osób (z dostępem do informacji niejawnych), lokalizację miejsc przechowywania, dostęp osób do budynku. Ponadto możliwe jest zastosowanie dodatkowych kryteriów (należy dołączyć co najmniej jeden czynnik o realnym znaczeniu: np. zagrożenie działaniem obcych służb specjalnych, sabotażem, zamachem terrorystycznym, pożarem, powodzią, przestępstwem pospolitym). Ocena odbywa się przez przyznanie liczby punktów odpowiadającej istotności każdego kryterium. Suma punktów wpływa na kwalifikację jednostki do jednego z istniejących poziomów zagrożenia. W rozporządzeniu wymieniono trzy poziomy: wysoki, średni i niski – przy czym każdemu z nich przyporządkowano określony przedział punktowy.

W drugim etapie następuje określenie wymagań dla danego poziomu zagrożeń. Wymagania zostały zawarte w formie tabeli i obejmują 6 rodzajów zabezpieczeń: szafy przeznaczone do przechowywania informacji (ocenie podlega konstrukcja i zamki do szaf), pomieszczenia (konstrukcja, zamki do drzwi), budynki, kontrola dostępu (systemy kontroli dostępu, kontrola osób), personel bezpieczeństwa i systemy sygnalizacji włamania i napadu (personel, systemy), granice (ogrodzenie, kontrola dostępu). Możliwe jest zastosowanie zmiennych kombinacji wspomnianych systemów. Niższe standardy w jednym obszarze mogą zostać uzupełnione zabezpieczeniem innego rodzaju na wyższym poziomie. Wymaga się osiągnięcia minimalnej – ogólnej liczby punktów dla sumy ww. środków bezpieczeństwa przy konkretnym poziomie zagrożenia i klauzuli informacji niejawnych. Wieloetapowy i zmienny sposób doboru środków umożliwia większą elastyczność działania oraz wpływa na obniżenie kosztów.

Wspomniana elastyczność ma jednak pewne granice, określone przez stałe elementy, które wymieniono głównie w rozdziale 7 ustawy oraz przywołanym rozporządzeniu. Zaliczymy do nich m.in. strefy ochronne – obowiązkowe w jednostce przetwarzającej informacje o klauzuli co najmniej „poufne". Strefa III – obejmuje pomieszczenie lub obszar o wyraźnych granicach, w obrębie których możliwe jest kontrolowanie osób i pojazdów. Strefa II – obejmuje pomieszczenie lub obszar, w których są przetwarzane informacje o klauzuli „poufne" lub wyższej w taki sposób, że wstęp nie umożliwia bezpośredniego dostępu do tych informacji, wejście do niej jest możliwe tylko ze strefy ochronnej (I, II, III). Strefa I – obejmuje pomieszczenie lub obszar, w których są przetwarzane informacje o klauzuli „poufne" lub wyższej w taki sposób, że wstęp do niej umożliwia bezpośredni dostęp do tych informacji, wejście do niej jest możliwe tylko ze strefy ochronnej (I, II, III). W miejscach wymaga-

jących ochrony tajności na najwyższym poziomie tworzy się specjalną strefę ochronną – umiejscowioną w obrębie strefy I lub II – zabezpieczoną przed podsłuchem. Powinna ona spełniać następujące wymagania dodatkowe:

– posiadać system sygnalizacji włamania i napadu;

– pozostawać zamknięta, gdy nikogo w niej nie ma;

– być chroniona przed wstępem osób nieupoważnionych;

– podlegać regularnym inspekcjom ABW lub SKW (co najmniej raz w roku);

– być pozbawiona linii komunikacyjnych, telefonów i innych urządzeń komunikacyjnych oraz sprzętu elektrycznego i elektronicznego (z wyjątkiem opisanego i zaakceptowanego w procedurach bezpieczeństwa).

Bezpieczeństwo teleinformatyczne. Przetwarzanie informacji niejawnych odbywa się przy użyciu akredytowanych systemów teleinformatycznych przygotowanych do tego celu. Akredytacja powinna zostać poprzedzona opracowaniem dokumentacji opisanej w rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).

Zapewnienie bezpieczeństwa wymaga przeprowadzenia następujących działań:

a) planowania – polegającego na ustaleniu parametrów systemu (tj. jego przeznaczenia, klauzul przetwarzanych informacji, liczby użytkowników, lokalizacji);

b) projektowania – na tym etapie należy przeprowadzić wstępne oszacowanie ryzyka, dokonać wyboru zabezpieczeń – fizycznych i technicznych oraz uzyskać ich wstępną akceptację, uzgodnić plan i harmonogram czynności z organem prowadzącym akredytację, opracować dokument pn. „szczególne wymagania bezpieczeństwa teleinformatycznego";

c) wdrażania – na tym etapie należy dokonać zakupu i montażu uprzednio wybranych elementów systemu, w tym narzędzi kryptograficznych, następnie należy opracować dokument pn. „procedury bezpiecznej eksploatacji" oraz przeprowadzić akredytację systemu teleinformatycznego;

d) eksploatacji – należy zapewnić ciągłość i niezawodność działania systemu oraz zgodność tego działania z dokumentacją bezpieczeństwa;

e) modyfikacji – polegającej na dokonywaniu zmian w podstawowych parametrach systemu (np. klauzul przetwarzanych dokumentów, lokalizacji, zastosowanych urządzeń oraz narzędzi kryptograficznych). Wiąże się z nimi obowiązek uzyskania akceptacji organu dokonującego akredytacji oraz dokonania zmian w dokumentacji bezpieczeństwa;

f) wycofywania – na tym etapie należy zaprzestać eksploatacji systemu, powiadomić organ dokonujący akredytacji oraz zwrócić wydane świadectwa akredytacji. Należy ponadto usunąć informacje niejawne z systemu teleinfor-

matycznego, w szczególności przez ich przeniesienie do innego systemu, zarchiwizowanie lub zniszczenie nośników danych (w tym dysków twardych).

W przypadku systemów przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" akredytacji dokonuje kierownik jednostki organizacyjnej, w której system działa. Jest jednak zobowiązany przesłać odpowiednio ABW albo SKW dokumentację bezpieczeństwa w terminie 30 dni. Wspomniane służby mogą w ciągu 30 dni przekazać zalecenia kierownikowi jednostki, w celu wprowadzenia zmian w organizacji zabezpieczeń. W uzasadnionych przypadkach mogą również nakazać wstrzymanie przetwarzania informacji.

Dla systemów przeznaczonych do informacji o klauzuli „poufne" lub wyższej – akredytacji dokonuje ABW albo SKW (zgodnie z właściwością ogólną wskazaną w art. 10-11 ustawy). Akredytacji udziela się na czas określony, nie dłuższy niż pięć lat w formie odrębnego dokumentu – świadectwa akredytacji[29]. ABW i SKW poprzedzają akredytację audytem bezpieczeństwa w toku którego badaniu podlegają wszystkie najistotniejsze parametry systemu, m.in.: usytuowanie urządzeń, systemy zabezpieczeń (w tym organizacja stref ochronnych, zastosowane zabezpieczenia techniczne) oraz struktury zarządzania. W systemach przeznaczonych do przetwarzania informacji o klauzuli „poufne" lub wyższej należy ponadto zastosować środki ochrony elektromagnetycznej, certyfikowane przez ABW i SKW. Dotyczy to również stosowanych narzędzi kryptograficznych. Certyfikaty są wydawane na okres nie krótszy niż 3 lata. Dokumentację bezpieczeństwa zatwierdza wyznaczona jednostka ABW albo SKW. Wspomniane instytucje mogą odstąpić od audytu jeśli system służy wyłącznie do przetwarzania informacji o klauzuli „poufne". W ustawie nie wskazano przesłanek podjęcia takiej decyzji. Zwykle następuje to w sytuacji, gdy zastosowane środki ochrony znacznie przewyższają wymagania w tym zakresie. Od odmowy przyznania akredytacji nie przysługuje odwołanie.

W toku sporządzania szczególnych wymagań bezpieczeństwa należy przeprowadzić szacowanie ryzyka dla bezpieczeństwa informacji niejawnych. Obejmuje ono analizę ryzyka, na którą składają się: jego identyfikacja, określenie wielkości ryzyk, ich ocena. Identyfikację ryzyka powinna uwzględniać: zasoby systemu teleinformatycznego (liczbę i klauzule dokumentów), realne zagrożenia, podatności, zabezpieczenia, skutki wystąpienia incydentu bezpieczeństwa. W procesie określania wielkości ryzyk należy wyznaczyć ich poziomy. W procesie oceny należy porównać wyznaczone poziomy ryzyk z tymi, które można zaakceptować oraz podjąć decyzję co do dalszego

[29] Zasady akredytacji systemów teleinformatycznych uregulowano w art. 60 uoin z 1999 r., w którym nie wyznaczono terminu obowiązywania akredytacji. Należy przyjąć, że pojawienie się nowych przepisów (zawierających taki termin) nakłada obowiązek ponownej akredytacji po upływie 5 lat – także dla systemów dopuszczonych do użytkowania na podstawie poprzednich przepisów.

z nimi postępowania. Szacowanie powinno zostać ponowione w przypadku wprowadzania istotnych zmian w systemie, w przypadku wykrycia nowych zagrożeń oraz cyklicznie w ramach zarządzania bezpieczeństwem. Kierownik jednostki organizującej system odpowiada za zapewnienie ciągłości procesu zarządzania ryzykiem.

Osobami bezpośrednio odpowiedzialnymi za działanie systemu teleinformatycznego są wyznaczeni przez wspomnianego kierownika: administrator systemu teleinformatycznego oraz inspektor bezpieczeństwa teleinformatycznego. Osoby te powinny posiadać dostęp do informacji niejawnych o klauzuli co najmniej równej klauzuli przetwarzanych informacji niejawnych oraz przejść szkolenie prowadzone przez ABW – udokumentowane pisemnym zaświadczeniem. Obowiązki przypisane obu stanowiskom powinny zostać wymienione w szczególnych wymaganiach bezpieczeństwa teleinformatycznego. Administrator systemu odpowiada za jego właściwe funkcjonowanie i bezpieczeństwo przetwarzaniach informacji, wdrożenie zabezpieczeń, zakładanie, usuwanie i nadzór nad kontami użytkowników, utrzymanie zgodności systemu z jego dokumentacją, szkolenie użytkowników, prowadzenie dziennika administratora. Inspektor odpowiada za udostępnianie stanowiska użytkownikom, weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu z dokumentacją, prowadzi dziennik systemu teleinformatycznego. Wspomniane osoby uczestniczą w opracowaniu i aktualizacji dokumentacji bezpieczeństwa.

Należy pamiętać, że proces przetwarzania informacji niejawnych przy użyciu środków teleinformatycznych powinien zawsze przebiegać pod kontrolą wyżej wymienionych osób. Wykorzystywanie do tego celu urządzeń pozbawionych akredytacji jest zabronione.

Bezpieczeństwo przemysłowe. Bezpieczeństwem przemysłowym nazywamy system przedsięwzięć, których celem jest zapewnienie ochrony informacji niejawnych udostępnianych przedsiębiorcy w związku z wykonaniem umów lub zadań powierzonych na podstawie przepisów prawa. Przedmiotem bezpieczeństwa przemysłowego są informacje niejawne oraz system organizacyjno-techniczny ich ochrony. Podmiotem jest przedsiębiorca ubiegający się o dostęp do informacji niejawnych w związku z realizacją wspomnianych umów lub zadań oraz zleceniodawcy (jednostki zlecające).

Jeśli wykonanie zadań wiąże się z dostępem do informacji niejawnych oznaczonych klauzulą „poufne", „tajne" lub „ściśle tajne", przedsiębiorca musi uzyskać odpowiednie świadectwo bezpieczeństwa przemysłowego. Obowiązek ten nie dotyczy osób fizycznych prowadzących działalność gospodarczą jednoosobowo (osobiście). Osoby te są obowiązane posiadać odpowiednie poświadczenie bezpieczeństwa. Świadectwo bezpieczeństwa przemysłowego jest dokumentem poświadczającym zdolność przedsiębiorcy do zapewnienia ochro-

ny informacji niejawnych, przed nieuprawnionym ujawnieniem. Świadectwo przyznaje Agencja Bezpieczeństwa Wewnętrznego albo Służba Kontrwywiadu Wojskowego. Jego wydanie jest poprzedzone postępowaniem bezpieczeństwa przemysłowego, które ma na celu ustalenie, czy przedsiębiorca jest zdolny do ochrony informacji niejawnych. Badaniu podlegają kwestie: finansowe, organizacyjne oraz kadrowe. W ramach procedur przeprowadza się postępowania sprawdzające wobec osób, które uzyskają dostęp do informacji niejawnych. Natomiast obowiązkiem zleceniodawcy zadania jest wprowadzenie do treści umowy lub zlecenia instrukcji bezpieczeństwa przemysłowego, w której zawarte są wymagania dotyczące ochrony informacji niejawnych, skutki oraz zakres odpowiedzialności z tytułu niewykonania obowiązków wynikających z ustawy lub instrukcji.

Jeśli przedsiębiorca zamierza przetwarzać informacje niejawne oznaczone klauzulą „poufne" lub wyższą zwraca się do ABW lub SKW z wnioskiem o przeprowadzenie postępowania bezpieczeństwa przemysłowego. Procedura obejmuje następujące zagadnienia dotyczące przedsiębiorcy:

– struktura kapitału i powiązania kapitałowe;
– źródła pochodzenia środków finansowych i sytuację finansową;
– strukturę organizacyjną oraz system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego;
– osoby wchodzące w skład organów zarządzających i kontrolnych (oraz osoby działające z ich upoważnienia). W uzasadnionych wypadkach sprawdzeniu podlegają również osoby już posiadające poświadczenia bezpieczeństwa.

Czynności przeprowadza się m.in. w oparciu o dane zawarte w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie.

W toku wspomnianej procedury przeprowadza się również postępowania sprawdzające wobec następujących osób:

– kierownika przedsiębiorcy;
– pełnomocnika ochrony lub jego zastępcy oraz pracowników pionu ochrony;
– administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego;
– pozostałych osób, które powinny mieć dostęp do informacji niejawnych.

Powyższych czynności dokonuje się głównie na podstawie kwestionariusza, który przedsiębiorca wypełnia i przekazuje ABW albo SKW. Postępowanie powinno trwać nie dłużej niż 6 miesięcy, licząc od daty złożenia przez przedsiębiorcę wszystkich niezbędnych dokumentów.

Postępowanie może się zakończyć:

– wydaniem świadectwa bezpieczeństwa przemysłowego;
– odmową wydania świadectwa;
– umorzeniem postępowania (przyczyny wymieniono w art. 62 ustawy).

Świadectwo bezpieczeństwa przemysłowego występuje w trzech odmianach, zależnie od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej:

1. pierwszego stopnia – jeśli potwierdza pełną zdolność do ochrony tych informacji;

2. drugiego stopnia – jeśli potwierdza zdolność do ochrony informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;

3. trzeciego stopnia – jeśli potwierdza zdolność do ochrony informacji, z wyłączeniem możliwości ich przetwarzania w obiektach użytkowanych przez przedsiębiorcę.

Świadectwo zachowuje ważność przez określony czas, odmienny dla każdej z klauzul. Dla klauzuli „ściśle tajne" potwierdza ono zdolność do ochrony informacji niejawnych o klauzuli:

a) „ściśle tajne" – przez okres 5 lat od daty wystawienia;

b) „tajne" – przez okres 7 lat;

c) „poufne" – przez okres 10 lat.

Dla klauzuli „tajne" potwierdza ono zdolność do ochrony informacji niejawnych o klauzuli:

a) „tajne" – przez okres 7 lat;

b) „poufne" – przez okres 10 lat.

Dla klauzuli „poufne" – świadectwo zachowuje ważność przez 10 lat.

Podmiot prowadzący postępowanie odmawia przyznania świadectwa jeśli:

– odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa kierownikowi przedsiębiorcy;

– wystąpiły wątpliwości co do pochodzenia środków finansowych;

– nie istnieje możliwość ustalenia struktury kapitałowej przedsiębiorcy;

– nie zorganizowano kompleksowego systemu ochrony informacji niejawnych – pomimo upływu 6 miesięcy od daty wszczęcia postępowania (tylko w przypadku świadectwa I lub II stopnia);

– przedsiębiorca zataił lub podał nieprawdziwe dane w kwestionariuszu przekazanym ABW albo SKW, ewentualnie podał nieprawdziwe informacje o zmianach, które nastąpiły w toku postępowania.

Podmiot prowadzący postępowanie może odmówić przyznania świadectwa jeśli:

– w toku postępowań sprawdzających prowadzonych wobec osób wchodzących w skład organów zarządzających i kontrolnych przedsiębiorcy (oraz działających z ich upoważnienia) pojawią się niedające się usunąć wątpliwości dotyczące rękojmi zachowania tajemnicy – opisane w art. 23 ust. 2 pkt. 1-3 lub 5 lub w art. 24 ust. 3 ustawy;

– wnioskodawca nie powiadomi o zmianie danych zawartych w złożonym w kwestionariuszu – w ciągu 30 dni od ich wystąpienia.

ABW oraz SKW mają prawo cofnięcia świadectwa bezpieczeństwa przemysłowego jeśli wspomniane powody ujawnią się w toku dokonywanych przez te instytucje – sprawdzeń lub kontroli przestrzegania zasad bezpieczeństwa przez przedsiębiorcę.

Umorzenie, zawieszenie postępowania, odmowa przyznania świadectwa bezpieczeństwa przemysłowego oraz jego cofnięcie mają charakter decyzji administracyjnej, od której przysługuje odwołanie do Prezesa Rady Ministrów oraz skarga do sądu administracyjnego na podstawie k.p.a. Zakres orzekania jest analogiczny jak w przypadku bezpieczeństwa osobowego.

*

W powyższym tekście przedstawiłem zarys problematyki dotyczącej ochrony informacji niejawnych w Polsce. Poruszyłem najistotniejsze zagadnienia składające się na podstawy systemu ochrony tych informacji. Ma on charakter w znacznym stopniu prewencyjny, wzorowany na rozwiązaniach istniejących w państwach o ugruntowanej demokracji. Z tego faktu wynika poboczna obecnie rola przepisów karnych, zawartych w art. 265-266 kodeksu karnego[30]. Znajdują one zastosowanie dopiero w przypadku rażącego naruszenia administracyjnych procedur ochrony. W tekście pominąłem niektóre szczegóły techniczne niezbędne do wykonania głównych zadań. Jednak są one łatwe do zidentyfikowania – ponieważ zostały opisane w treści wymienionych rozporządzeń.

[30] Szerzej na temat prawno-karnej ochrony informacji niejawnych – M. Leciak: *Tajemnica państwowa i jej ochrona w prawie karnym materialnym i procesie karnym*. Wyd. TNOIK Dom Organizatora, Toruń 2009.