Zbigniew Wróblewski

Ochrona informacji niejawnych. Zagadnienia ogólne

1. Wstęp

Problem ochrony pewnych informacji o charakterze niejawnym zawsze odgrywał szczególną rolę z punktu widzenia bezpieczeństwa danego państwa. Po odzyskaniu przez Polskę niepodległości w 1918 r. sprawy związane z ochroną interesów państwa chronione były przepisami kodeksów karnych państw zaborczych z lat 1871 i 1903 oraz przepisami niemieckiej ustawy z dnia 3 czerwca 1914 r. o zdradzie tajemnic wojskowych. Kompleksowa regulacja dotycząca ochrony ważnych tajemnic została zawarta w rozporządzeniu Prezydenta Rzeczypospolitej Polskiej z dnia 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciwko państwu, które zostało zastąpione rozporządzeniem wydanym przez ten sam organ państwa w dniu 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa. W przedmiotowym rozporządzeniu tajemnica państwowa została określona jako wiadomości, dokumenty lub inne przedmioty, które z powodu ich treści lub jakości należy ze względu na dobro państwa polskiego zachować w tajemnicy przed rządem państwa obcego, choćby nawet zarządzenia normujące czynności służbowe nie uznawały ich za tajne albo choćby zachowanie ich w tajemnicy przed pewnym gronem osób nie było możliwe. Ustawodawca odniósł się także do środowiska cywilnego – w kodeksie handlowym z roku 1934 przewidziana została sankcja karna za naruszenie „tajemnicy handlowej".

W okresie powojennym kwestie związane z ochroną tajemnicy uregulowane zostały w dekrecie z dnia 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej, zawierającym bardzo zwięzłe definicje obu tajemnic. Zastąpiony on został w tym zakresie kodeksem karnym z dnia 19 kwietnia 1969 r., a następnie przepisami ustawy z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej. Wobec przystąpienia Polski do paktu północnoatlantyckiego nastąpiła potrzeba dostosowania polskich przepisów w tym zakresie do rozwiązań obowiązujących w państwach członkowskich NATO. Ustawa o ochronie informacji niejawnych, której przepisy weszły w życie dnia 11 marca 1999 r., została uchwalona przez Sejm Rzeczypospolitej Polskiej dnia 22 stycznia 1999 r. Według zapewnień jej projektodawców miał to być akt prawny o nowoczesnej konstrukcji, zgodny ze standardami „zachodnimi", mający za zadanie ochronę informacji niejawnych przed ich ujawnieniem nieuprawnionym podmiotom. Przedmiotowy akt prawny zdefiniował pojęcie informacji niejawnych, dokonując podziału tych informacji na tajemnicę państwową i służbową, wprowadził nowe pojęcie: „służba ochrony państwa". Ustawa wprowadziła także generalną zasadę, że informacje niejawne mogą być udostępniane wyłącznie osobom dającym rękojmię zachowania tajemnicy, tj. spełnienia przez te osoby ustawowych wymogów zapewnienia ochrony informacji niejawnych przed

ich nieuprawnionym ujawnieniem[1]. Z zasadą tą wiąże się ściśle obowiązek zastosowania wobec osoby, która ubiega się o dostęp do informacji niejawnych, postępowania sprawdzającego, przeprowadzanego przez określone w ustawie podmioty, oraz przeszkolenia w zakresie ochrony informacji niejawnych. Z uwagi że informacje niejawne są materią niezwykle „wrażliwą", ustawodawca skonstruował wachlarz środków ich ochrony, poczynając od organów i osób, a kończąc na systemach i urządzeniach, aby jak najdokładniej zabezpieczyć je przed nieuprawnionym ujawnieniem.

2. Zakres obowiązywania ustawy. Organy ochrony informacji niejawnych

Obecnie podstawowym aktem prawnym określającym zasady ochrony informacji niejawnych, stanowiących tajemnicę państwową i służbową przed ich nieuprawnionym ujawnieniem jest ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych[2]. Oprócz określenia zasad ochrony tajemnicy państwowej i służbowej reguluje ona także kwestie klasyfikowania informacji niejawnych, udostępniania informacji niejawnych, postępowania sprawdzającego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej „postępowaniem sprawdzającym", szkolenia w zakresie ochrony informacji niejawnych, ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi zachowania tajemnicy, w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w kwestionariuszu bezpieczeństwa osobowego i kwestionariuszu bezpieczeństwa przemysłowego, organizacji kontroli przestrzegania zasad ochrony informacji niejawnych, ochrony informacji niejawnych w systemach i sieciach teleinformatycznych, stosowania środków fizycznej ochrony informacji niejawnych.

Przepisy ustawy mają zastosowanie do organów władzy publicznej, a w szczególności do Sejmu i Senatu Rzeczypospolitej Polskiej, Prezydenta Rzeczypospolitej Polskiej, organów administracji rządowej i samorządowej, sądów i trybunałów, a także organów kontroli państwowej i ochrony prawa, oraz w stosunku do: organów Sił Zbrojnych Rzeczypospolitej Polskiej, Narodowego Banku Polskiego i banków państwowych, innych państwowych osób prawnych i państwowych jednostek organizacyjnych, przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych, dotyczące realizacji zadań opłacanych w całości lub części ze środków publicznych w rozumieniu przepisów ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych[3]. Pamiętać jednak należy, że zgodnie z treścią art. 1 ust. 3 ustawy o ochronie informacji niejawnych[4] ustawa nie narusza przepisów innych ustaw odnoszących się do tajemnicy zawodowej lub innych tajemnic prawnie chronionych. Dotyczy to tajemnicy bankowej, lekarskiej, handlowej, statystycznej itp. Oznacza to, że do wszystkich innych rodzajów informacji niejawnych stosuje się przepisy tych ustaw, w których zawarta jest regulacja odnosząca się do danej tajemnicy.

---

[1] B. K u r z ę p a, *Ochrona informacji niejawnych. Ochrona danych osobowych. Zbiór przepisów*, Bielsko-Biała 2000, s. 10.

[2] Tekst jedn., Dz. U. z 2005 r. Nr 196, poz. 1631.

[3] Dz. U. z 1998 r. Nr 119, poz.773, z późn. zm.

[4] *Ibidem*.

Ustawa chroni dwa rodzaje tajemnic: tajemnicę państwową i tajemnicę służbową. Wprowadzenie rozgraniczenia informacji niejawnych na informacje stanowiące tajemnicę państwową i tajemnicę służbową nie jest w polskim ustawodawstwie w tym zakresie niczym nowym. Takie rozgraniczenie nastąpiło też pod rządami obowiązującej przed wejściem w życie ustawy o ochronie informacji niejawnych, a mianowicie ustawy z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej[5]. Zgodnie z definicją ustawową tajemnicą państwową jest informacja niejawna określona w wykazie informacji niejawnych (załącznik nr 1 do ustawy), której nieuprawnione ujawnienie może spowodować istotne zagrożenie podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa. Tajemnicę służbową stanowi informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi lub wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Różnice między tu wymienionymi informacjami niejawnymi, stanowiącymi tajemnicę państwową i służbową, są następujące: wykaz informacji niejawnych stanowiących tajemnicę państwową jest ściśle określony w załączniku nr 1 do ustawy o ochronie informacji niejawnych, podczas gdy takiego samego wykazu informacji mogących stanowić tajemnicę służbową nie sporządzono. Tajemnicą państwową staje się informacja niejawna przez sam fakt umieszczenia jej w załączniku nr 1, natomiast informacja niejawna staje się tajemnicą służbową dopiero po jej uzyskaniu w związku z upoważnieniami służbowymi lub wykonywaniu prac zleconych. Nieuprawnione ujawnienie tajemnicy państwowej godzi w podstawowe interesy państwa, podczas gdy ujawnienie tajemnicy służbowej naraża jedynie na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej.

Służby ochrony państwa (służby specjalne) to ogólna nazwa opisująca instytucje, które prowadzą działania operacyjno-rozpoznawcze o charakterze niejawnym. Głównym zadaniem tych służb jest pozyskiwanie i ochrona informacji istotnych do usprawnienia zewnętrznego i wewnętrznego bezpieczeństwa państwa. Służbami ochrony państwa są obecnie Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego, właściwe do kontroli i ochrony informacji niejawnych oraz kontroli przestrzegania przepisów w tym zakresie. Realizują zadania w zakresie bezpieczeństwa systemów i sieci teleinformatycznych. Natomiast niezwykle istotnym zadaniem tych służb jest prowadzenie – według zasad określonych w ustawie o ochronie informacji niejawnych oraz przepisów zmieniających ustawę – postępowań sprawdzających, a także ochrona informacji niejawnych przez Polskę z innymi państwami i organizacjami międzynarodowymi. Sprawują one też kontrolę merytoryczną dotyczącą ochrony informacji niejawnych w zakresie realizacji przepisów ustawy przez pełnomocnika ds. ochrony informacji niejawnych, kolejnego podmiotu działającego w sferze ochrony tajemnicy państwowej i służbowej powołanego na mocy przepisów ustawy o ochronie informacji niejawnych.

Pełnomocnik do spraw ochrony informacji niejawnych zwany pełnomocnikiem ochrony, jest podmiotem odgrywającym ważną rolę w systemie ochrony informacji niejawnych, powoływanym w jednostkach organizacyjnych, w których informacje takie są wytwarzane, przetwarzane, przekazywane lub przechowywane. Podlega on bezpośrednio kierownikowi danej jednostki organizacyjnej. Jest to osoba, której kierownik jednostki organizacyjnej udziela pełnomocnictwa o szczególnym charakterze – czuwania nad przestrzeganiem przepisów do-

---

[5] Dz. U. z 1982 r. Nr 40, poz. 271, z późn. zm.

tyczących ochrony tajemnicy państwowej i służbowej. Biorąc pod uwagę całość stanu prawnego dotyczącego ochrony informacji niejawnych (ustawa oraz przepisy wykonawcze), zakres obowiązków pełnomocnika ochrony jest bardzo rozległy i obejmuje następujące zagadnienia dotyczące ochrony informacji niejawnych: ponosi odpowiedzialność za przestrzeganie przepisów o ochronie informacji, kieruje komórką organizacyjną ds. ochrony informacji niejawnych, zapewnia ochronę informacji niejawnych, zapewnia ochronę systemów i sieci teleinformatycznych oraz ochronę fizyczną jednostki organizacyjnej, kontroluje przestrzeganie przepisów o ochronie informacji niejawnych, przeprowadza okresową kontrolę ewidencji materiałów i obiegu dokumentów w danej jednostce organizacyjnej, prowadzi na polecenie kierownika jednostki organizacyjnej postępowania sprawdzające oraz szkolenia pracowników w zakresie ochrony informacji niejawnych, opracowuje plan ochrony jednostki organizacyjnej i nadzoruje jego realizację. Po zmianie przepisów ustawy w roku 2005 kierownik jednostki organizacyjnej może w razie potrzeby powołać zastępcę pełnomocnika ochrony.

3. Klasyfikowanie informacji niejawnych. Klauzule tajności

Klasyfikowanie informacji niejawnych oznacza przyznanie tym informacjom w sposób wyraźny jednej z czterech przewidzianych w ustawie klauzul tajności. Klasyfikowanie informacji niejawnej zawartej w materiale, a zwłaszcza utrwalonej w dokumencie, polega na oznaczeniu tego materiału odpowiednią klauzulą tajności[6]. Ustawodawca wyróżnia cztery rodzaje klauzul informacji niejawnych: „ściśle tajne", „tajne", „poufne", „zastrzeżone". Przy czym informacje niejawne, którym nadana została klauzula tajności „ściśle tajne" i „tajne", stanowią tajemnicę państwową, natomiast „poufne" i „zastrzeżone" stanowią tajemnicę służbową. Informacjami niejawnymi oznaczonymi klauzulą „ściśle tajne" są informacje, których nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych Rzeczypospolitej Polskiej albo zagrażać nieodwracalnymi lub wielkimi stratami interesów obronności, bezpieczeństwa państwa albo narazić je na szkodę w wielkich rozmiarach. Klauzulą „tajne" oznaczone są informacje, których nieuprawnione ujawnienie mogłoby spowodować zagrożenie międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę. „Poufne" są informacje, których nieuprawnione ujawnienie narażałoby na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli. Natomiast informacje, których nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej, oznacza się klauzulą „zastrzeżone". Informacje niejawne stanowiące tajemnicę państwową oznaczone klauzulą „ściśle tajne" i „tajne" znalazły się w załączniku do ustawy o ochronie informacji niejawnych, który zawiera 88 rodzajów informacji zakwalifikowanych przez ustawodawcę jako tajemnica państwowa. Do grupy obejmującej informacje niejawne oznaczone klauzulą „ściśle tajne" zaliczono 29 rodzajów informacji, w grupie informacji niejawnych oznaczonych klauzulą „tajne" znalazło się 59 rodzajów informacji. Pierwotny tekst ustawy z 1999 r. zawierał 96 rodzajów informacji niejawnych oznaczonych wyżej wymienionymi klauzulami tajności stanowiących tajemnicę państwową. W grupie infor-

[6] I. R u s z c z y k, *Instrukcja ochrony informacji niejawnych*, Gdańsk 2002, s. 39.

macji niejawnych oznaczonych klauzulą „tajne" rozróżniono ogólnie 66 rodzajów informacji ze względu na obronność, bezpieczeństwo państwa i porządek publiczny (40 rodzajów), ze względu na ważny interes państwa (26 rodzajów), obecnie taki podział już nie występuje. Wśród informacji niejawnych oznaczonych klauzulą „ściśle tajne" ustawodawca umieścił 30 rodzajów informacji. Po zmianie ustawy o ochronie informacji niejawnych w roku 2005 liczba rodzajów informacji stanowiących tajemnicę państwową została zmniejszona i wynosi ogółem 88.

Z określeniem pewnego rodzaju informacji jako niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „poufne" lub „zastrzeżone" sytuacja jest całkowicie inna niż w przypadku tajemnicy państwowej. Jeżeli w wypadku informacji niejawnych stanowiących tajemnicę państwową ustawodawca sporządził wykaz tych informacji będący załącznikiem do ustawy, to w przypadku tajemnicy służbowej brakuje takiego wykazu. Dana informacja staje się niejawna wraz z określoną klauzulą jej tajności, tj. „ściśle tajne" bądź „tajne", już przez sam fakt umieszczenia jej w przedmiotowym wykazie. W instrukcji postępowania z materiałami niejawnymi[7] Piotr Thiem wskazuje, że materiały zawierające informacje niejawne stanowiące tajemnicę służbową oznacza się klauzulą „zastrzeżone", gdy ich nieuprawnione ujawnienie mogłoby narazić na szkodę prawnie chroniony interes obywateli lub jednostki organizacyjnej. W przypadku jednostek organizacyjnych są to informacje mające bliski związek z tajemnicą przedsiębiorstwa, która została ustanowiona na mocy przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[8]. Zważywszy, że przepisy ustawy o ochronie informacji niejawnych mają zastosowanie do wielu różnorodnych z punktu widzenia wykonywanych przez nie zadań podmiotów, tak też i rodzaje informacji niejawnych stanowiących tajemnicę służbową o klauzuli „zastrzeżone" mogą być całkowicie odmienne, np. informacje niejawne występujące w organach administracji publicznej a informacje występujące w jednostkach organizacyjnych wykonujących działalność gospodarczą czy handlową. Wobec tego nie jest chyba możliwe w sposób kompleksowy opracowanie w formie załącznika do ustawy wykazu informacji niejawnych stanowiących tajemnicę służbową, obowiązującego we wszystkich podmiotach, do których stosuje się przepisy ustawy o ochronie informacji niejawnych, głównie ze względu na specyfikę i różnorodność zadań wykonywanych przez te podmioty. Pełnomocnik ochrony opracowujący w danej jednostce organizacyjnej taki wykaz musi głównie kierować się prawnie chronionym interesem tej jednostki. Pod pojęciem oznaczania informacji niejawnych klauzulami tajności należy rozumieć umieszczanie klauzul tajności na materiałach, dokumentach lub innej dokumentacji uznanej za informacje niejawne.

Szczegółowe zagadnienia związane z oznaczaniem materiałów i umieszczaniem klauzul tajności regulują przepisy rozporządzenia Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności[9]. Miejscem przechowywania, wytwarzania, przetwarzania, przekazywania oraz przechowywania dokumentów zawierających informacje niejawne jest kancelaria tajna. Jest jednym z wielu elementów ogólnej polityki bezpieczeństwa informacji niejawnych jednostki organizacyjnej. Wymóg zorganizowania kancelarii tajnej zachodzi w jednostkach organizacyjnych, w których występują informacje niejawne o klauzuli co najmniej „poufne". Obowiązek ten nie dotyczy jednak sytuacji, gdy dokumenty oznaczone są klauzulą

---

[7] P. T h i e m, *Instrukcja postępowania z materiałami niejawnymi z komentarzem*, Gdańsk 2002, s. 51.

[8] Dz. U. z 1993 r. Nr 47, poz. 221 z późn. zm.

[9] Dz. U. z 2005 r. Nr 205, poz. 1696.

tajności „zastrzeżone”[10]. Kwestie związane z organizacją i funkcjonowaniem kancelarii tajnych regulują w szczególności przepisy ustawy o ochronie informacji niejawnych oraz rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych[11]. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową lub służbową uprawnionym osobom, natomiast jej obsługa może być wykonywana wyłącznie przez pracowników pionu ochrony. Za zorganizowanie kancelarii tajnej w danej jednostce organizacyjnej odpowiada pełnomocnik ochrony, któremu bezpośrednio podlega kierownik kancelarii tajnej odpowiadający za bieżący, codzienny nadzór nad obiegiem dokumentów zawierających informacje niejawne.

4. Dostęp do informacji niejawnych. Postępowanie sprawdzające

Generalna zasada związana z udostępnianiem informacji niejawnych zawarta jest w art. 3 ustawy o ochronie informacji niejawnych[12], który stanowi, że informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez tę osobę pracy lub pełnienia służby na zajmowanym stanowisku albo innej pracy zleconej. Przy czym przez rękojmię zachowania tajemnicy należy rozumieć spełnienie przez określoną osobę ustawowych wymogów zapewniających ochronę przed nieuprawnionym ujawnieniem informacji niejawnych. Dopuszczenie do pracy na stanowisku, pełnienie służby lub wykonywanie pracy zleconej, mogącej łączyć się z dostępem do informacji niejawnych, stanowiących bądź to tajemnicę państwową, bądź tajemnicę służbową, może nastąpić po spełnieniu dwóch przesłanek, tj. przeprowadzeniu postępowania sprawdzającego względem osoby ubiegającej się o pracę na tym stanowisku oraz po przeszkoleniu tej osoby w zakresie ochrony informacji niejawnych. Postępowania sprawdzającego nie przeprowadza się wobec następujących osób sprawujących urząd: Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu Rzeczypospolitej Polskiej, Marszałka Senatu Rzeczypospolitej Polskiej, Prezesa Rady Ministrów. Osoby te zapoznają się z przepisami o ochronie informacji niejawnych i składają oświadczenie o znajomości tych przepisów. Postępowania sprawdzającego nie przeprowadza się również wobec: posłów i senatorów, członków Rady Ministrów, Pierwszego Prezesa Sądu Najwyższego, Prezesa Naczelnego Sądu Administracyjnego, Prezesa Trybunału Konstytucyjnego, Prezesa Narodowego Banku Polskiego, Prezesa Najwyższej Izby Kontroli, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, członków Rady Polityki Pieniężnej, członków Krajowej Rady Radiofonii i Telewizji, Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, szefów kancelarii: Prezydenta, Sejmu, Senatu Rzeczypospolitej Polskiej i Prezesa Rady Ministrów. Osoby te składają oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych po odbyciu szkolenia w zakresie ochrony informacji niejawnych.

---

[10] T. S z e w c, *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007, s. 228.
[11] Dz. U. z 2005 r. Nr 208, poz. 1741.
[12] Tekst jedn., Dz. U. z 2005 r. Nr 196, poz. 1631.

W stosunku do kandydatów na wymienione stanowiska postępowanie sprawdzające przeprowadza właściwa służba ochrony państwa na wniosek organu uprawnionego do powołania na to stanowisko. Jeżeli chodzi o udostępnianie informacji niejawnych sędziom, asesorom sędziowskim oraz prokuratorom i asesorom prokuratorskim, sprawy te są regulowane przez przepisy ustawy o ustroju sądów powszechnych, o ustroju sądów wojskowych oraz o prokuraturze. Kierownik jednostki organizacyjnej może w formie pisemnej wyrazić zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową osobie, wobec której wszczęto zwykłe postępowanie sprawdzające. W przypadku dostępu do informacji niejawnych stanowiących tajemnicę państwową zgodę taką wydaje Szef Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów, minister właściwy do określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku właściwa służba ochrony państwa.

Do pracy lub pełnienia służby na stanowisku lub wykonywania pracy zleconej związanej z dostępem do informacji niejawnych stanowiących tajemnicę państwową nie mogą być dopuszczone osoby, które nie mają polskiego obywatelstwa, chyba że przepisy ustawy o ochronie informacji niejawnych stanowią inaczej, skazane prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, nie mają poświadczenia bezpieczeństwa. Przeszkolenie z zakresu ochrony informacji niejawnych może nastąpić po uprzednim sprawdzeniu przeprowadzonym i pozytywnie zakończonym postępowaniem sprawdzającym.

Wykaz stanowisk w administracji rządowej, których zajmowanie wiąże się z dostępem do informacji niejawnych stanowi załącznik do ustawy o ochronie informacji niejawnych. W przypadku występowania w danej jednostce organizacyjnej informacji niejawnych stanowiących tajemnicę służbową wykaz stanowisk, których zajmowanie lub wykonywanie wiąże się z dostępem do tajemnicy służbowej, określa kierownik danej jednostki organizacyjnej. W tej sytuacji określenie takich wykazów następuje przy uwzględnieniu specyfiki działalności danej jednostki organizacyjnej, a co za tym idzie, wyodrębnienia z tej działalności takich rodzajów spraw, które zostaną sklasyfikowane jako informacje niejawne stanowiące tajemnicę służbową z nadaniem im odpowiednio klauzul tajności, tj. „zastrzeżone" bądź „poufne". Celem szkolenia w zakresie ochrony tajemnicy państwowej lub służbowej jest zapoznanie kandydata do objęcia stanowiska z następującymi sprawami z zakresu ochrony informacji niejawnych: zagrożeniami ze strony obcych służb specjalnych, których działania skierowane są przeciwko Rzeczypospolitej Polskiej oraz państwom sojuszniczym, zagrożeniami ze strony organizacji terrorystycznych, zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, sposobami ochrony informacji niejawnych stanowiących tajemnicę państwową oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia, odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych.

Szkolenie w zakresie ochrony informacji niejawnych przeprowadzają funkcjonariusze i żołnierze służb ochrony państwa lub pełnomocnicy ochrony w stosunku do osób zatrudnionych lub pełniących służbę w jednostkach organizacyjnych. Po przeprowadzeniu szkolenia osobie przeszkolonej wydaje się zaświadczenie stwierdzające odbycie przeszkolenia w zakresie ochrony informacji niejawnych.

Postępowanie sprawdzające ma na celu ustalenie, czy osoba, której mają być udostępnione informacje niejawne stanowiące tajemnicę państwową lub służbową, daje rękojmię zachowania tajemnicy, tj. spełnia ustawowe wymogi zapewnienia ochrony informacji niejaw-

nych przed ich nieuprawnym ujawnieniem, czyli tzw. wiedzy koniecznej[13]. W jego trakcie ustala się, czy istnieją wątpliwości dotyczące uczestnictwa, współpracy bądź prowadzenia przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej lub innej wymienionej przeciwko Rzeczypospolitej Polskiej, ukrywania lub świadomego podawania niezgodnego z prawem danych mających znaczenie dla informacji niejawnych, przestrzegania porządku konstytucyjnego RP, jak też wątpliwości odnośnie do zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych, właściwego postępowania z informacjami niejawnymi, różnic między poziomem życia a uzyskanymi przez osobę sprawdzaną dochodami, ewentualnych informacji o chorobie psychicznej lub innych zaburzeniowych czynności psychicznych ograniczających sprawność psychiczną, związane z uzależnieniem od alkoholu lub narkotyków. Ustawa wyróżnia trzy rodzaje postępowań sprawdzających: zwykłe – przy obsadzie stanowisk i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone" i „poufne", poszerzone – przy obsadzie stanowisk i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne" oraz specjalne – przy obsadzie stanowisk i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne".

W związku ze zmianą przepisów ustawy dokonaną w 2005 r. odnośnie postępowania sprawdzającego ustawodawca wprowadził dwie nowe instytucje prawne, a mianowicie zawieszenie i umorzenie tego postępowania. Wprowadzenie zmian w procedurze sprawdzającej uwzględniło kilkuletnie doświadczenia obowiązywania ustawy, a działania takie są możliwe w przypadku zaistnienia okoliczności utrudniających lub uniemożliwiających jej kontynuowanie.

Postępowanie sprawdzające przeprowadzają następujące podmioty: Służba Kontrwywiadu Wojskowego w sytuacji ubiegania się danej osoby o zajmowanie stanowiska lub wykonywania pracy zleconej związanej z obronnością państwa, tj. w stosunku do żołnierzy służby czynnej i pracowników wojska, w wojskowych organach ochrony prawa i wojskowych organach porządkowych, w przedsiębiorstwach i jednostkach naukowych lub badawczo-rozwojowych oraz innych jednostkach organizacyjnych, dla których organem założycielskim jest Minister Obrony Narodowej, lub zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa; Agencja Bezpieczeństwa Wewnętrznego w innych sprawach niż wyżej wymienione; pełnomocnicy ochrony w przypadku zwykłych postępowań sprawdzających. Postępowanie sprawdzające można zawiesić w przypadku: długotrwałej choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego; wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo skarbowe, umyślne, ścigane z oskarżenia publicznego; wyjazdu osoby sprawdzanej za granicę na okres przekraczający 30 dni.

Zawieszone postępowanie sprawdzające podejmuje się po uzyskaniu informacji o ustaniu przyczyny będącej do jego zawieszenia. O fakcie tym pełnomocnik ochrony lub służba ochrony państwa zawiadamiają wnioskodawcę i osobę sprawdzaną. Przepisy ustawy nie wskazują formy, w jakiej zawieszenie lub podjęcie zawieszonego postępowania następuje, a w związku z tym nie uwzględniają żadnych środków zaskarżenia w tej kwestii. Ta sytuacja dotyczy także instytucji umorzenia postępowania sprawdzającego, które może nastąpić w przypadku: śmierci osoby sprawdzanej, rezygnacji osoby sprawdzanej z ubiegania się lub zajmowania stanowiska czy wykonywania prac łączących się z dostępem do informacji nie-

[13] B. Jakubas, M. Ryszkowski, *Ochrona informacji niejawnych*, Warszawa 2001, s. 39.

jawnych, odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych. W przypadku umorzenia postępowania sprawdzającego służba ochrony państwa lub pełnomocnik ochrony zawiadamiają o tym fakcie wnioskodawcę, a w przypadku umorzenia postępowania w razie rezygnacji danej osoby lub odstąpienia przez kierownika jednostki organizacyjnej od obsady stanowiska lub zlecenia pracy – osobę sprawdzaną.

Bardzo ważnym elementem postępowania sprawdzającego jest wypełnienie przez osobę, która ma być poddana temu postępowaniu, dokumentu zwanego ankietą bezpieczeństwa osobowego. Ankietę taką wypełniają osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone", „poufne", „tajne" i „ściśle tajne". Są to więc osoby, które mają dostęp do tajemnicy państwowej i służbowej. Ankieta bezpieczeństwa osobowego ma na celu ustalenie, czy osoba poddana postępowaniu sprawdzającemu daje rękojmię zachowania tajemnicy, oraz ma służyć wyłącznie ochronie bezpieczeństwa narodowego przed zagrożeniami ze strony obcych służb specjalnych, ugrupowań terrorystycznych lub grup przestępczych. Z chwilą wejścia w życie przepisów ustawy o ochronie informacji niejawnych dnia 1 marca 1999 r. obowiązywał jeden wzór ankiety bezpieczeństwa osobowego. Obowiązek jej wypełnienia miały wszystkie osoby sprawdzane niezależnie od rodzaju przeprowadzonego postępowania sprawdzającego. Ankieta powinna być wypełniona pismem drukowanym, w miarę możności pismem na maszynie, podpisana przez: osobę, która ją wypełniła, kierownika jednostki organizacyjnej, pełnomocnika ds. ochrony informacji niejawnych wraz z podaniem miejscowości i daty jej wypełnienia oraz ostemplowana. Po nowelizacji ustawy o ochronie informacji niejawnych w załączniku nr 2 do ustawy znajdują się trzy wzory ankiet bezpieczeństwa osobowego przeznaczone dla osób podlegających postępowaniu sprawdzającemu zwykłemu, poszerzonemu i specjalnemu. Zasadnicze zmiany ankiety poprzednio obowiązującej polegały na konstruowaniu ankiety w taki sposób, aby wyeliminować z niej elementy, które w danym postępowaniu sprawdzającym są zbędne.

Zwykłe postępowanie sprawdzające prowadzone jest w stosunku do osoby ubiegającej się o pracę na stanowisku lub wykonywanie prac zleconych, z którymi wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową, będą to więc informacje oznaczone klauzulą „zastrzeżone" lub „poufne". Postępowanie to prowadzone jest przez pełnomocnika ds. ochrony informacji niejawnych, a jego wszczęcie następuje na pisemne polecenie kierownika jednostki organizacyjnej. Po otrzymaniu polecenia pełnomocnik ochrony informuje osobę, która ma być poddana procedurze sprawdzającej o tym fakcie, przekazując jej do wypełnienia ankietę bezpieczeństwa osobowego. Podpisując ankietę, osoba sprawdzana wyraża zgodę na przeprowadzenie wobec niej czynności przewidzianych w ustawie. Podczas trwającego postępowania sprawdzającego osoba sprawdzana w każdym czasie w formie pisemnej może wycofać swoją zgodę na dalsze prowadzenie postępowania sprawdzającego lub odmówić poddania się określonym czynnościom procedury (np. poddaniu się badaniu lekarskiemu w związku z podejrzeniem zaburzeń psychicznych). Fakt taki jest jednoznaczny z rezygnacją z kandydowania do obsady stanowiska lub ubiegania się o wykonywanie pracy związanej z dostępem do informacji niejawnych, a sytuacja taka dotyczy wszystkich rodzajów postępowań sprawdzających. Zwykłe postępowanie sprawdzające obejmuje sprawdzenie w niezbędnym zakresie danych zawartych w ankiecie wypełnionej i podpisanej przez osobę sprawdzaną, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym oraz Centralnym Zarządzie Służby Więziennej. Ponadto obejmuje sprawdzenie – na pisemny wniosek pełnomocnika ochrony skierowany do właściwej służby ochrony państwa – danych znajdujących się w ewidencjach i kartotekach powszechnie

niedostępnych, jeżeli osoba sprawdzana ubiega się o uzyskanie dostępu do informacji niejawnych oznaczonych klauzulą „poufne". Właściwa służba ochrony państwa przekazuje pełnomocnikowi ochrony w formie pisemnej informację o danej osobie. Jeżeli jest to konieczne w związku z uzyskanymi informacjami, podmiot prowadzący postępowanie sprawdzające może przeprowadzić z osobą sprawdzaną rozmowę wyjaśniającą nieścisłości lub sprzeczności zawarte w uzyskanych informacjach. Postępowanie sprawdzające przeprowadza pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej lub właściwa służba ochrony państwa wobec kandydatów na pełnomocników ochrony na pisemny wniosek osoby upoważnionej do obsady stanowiska. Zwykłe postępowanie sprawdzające powinno być zakończone przed upływem dwóch miesięcy od daty pisemnego polecenia przeprowadzenia tego postępowania lub złożenia wniosku wraz z wypełnioną ankietą.

Poszerzone postępowanie sprawdzające przeprowadza się w stosunku do osób, które ubiegają się o zajmowanie stanowisk lub wykonywanie prac zleconych związanych z dostępem do informacji niejawnych, stanowiących tajemnicę państwową, oznaczonych klauzulą „tajne". Poszerzone postępowanie sprawdzające przeprowadza właściwa służba ochrony państwa na pisemny wniosek osoby upoważnionej do obsady stanowiska. Podjęcie czynności sprawdzających przez właściwą służbę ochrony państwa wobec osoby sprawdzanej wymaga uzyskania jej pisemnej zgody. Poszerzone postępowanie sprawdzające obejmuje przeprowadzenie następujących czynności: sprawdzenie w niezbędnym zakresie danych zawartych w ankiecie wypełnionej przez osobę sprawdzaną, w ewidencjach, rejestrach i kartotekach, a w szczególności w Krajowym Rejestrze Karnym oraz Centralnym Zarządzie Służby Więziennej; przeprowadzenie z osobą sprawdzaną rozmowy, jeżeli potrzeba taka zachodzi w związku z uzyskanymi informacjami; sprawdzenie danych zawartych w ankiecie w ewidencjach i kartotekach niedostępnych powszechnie; przeprowadzenie w miejscu zamieszkania osoby sprawdzanej wywiadu, jeżeli jest to konieczne do potwierdzenia danych zawartych w ankiecie; przeprowadzenie rozmowy z przełożonymi osoby sprawdzanej, jeżeli taka konieczność zachodzi na podstawie uzyskanych informacji; sprawdzenie w uzasadnionych przypadkach stanu i obrotów na rachunku bankowym osoby sprawdzanej na podstawie przepisów prawa bankowego. W sytuacji gdy w toku poszerzonego postępowania sprawdzającego (dotyczy to również postępowania specjalnego) wystąpią wątpliwości co do tego, że osoba sprawdzana daje rękojmię zachowania tajemnicy, służba ochrony państwa zapewnia tej osobie możliwość osobistego ustosunkowania się w toku wysłuchania do kwestii powodujących te wątpliwości. Na wysłuchanie osoba sprawdzana może stawić się z pełnomocnikiem ochrony. Sytuacja taka nie dotyczy przypadków, w których przeprowadzenie wysłuchania mogłoby naruszyć zasady ochrony informacji niejawnych stanowiących tajemnicę państwową. Poszerzone postępowanie sprawdzające powinno być zakończone przed upływem dwu miesięcy od daty złożenia wniosku o jego przeprowadzenie.

Specjalne postępowanie sprawdzające przeprowadza się przy obsadzie stanowisk lub pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne". Postępowanie specjalne prowadzone jest przez właściwą służbę ochrony państwa na pisemny wniosek osoby upoważnionej do obsady stanowiska. W toku przedmiotowego postępowania podmiot je prowadzący dokonuje tych samych czynności sprawdzających jak te, które przeprowadzane są w stosunku do osoby sprawdzanej w postępowaniu zwykłym i poszerzonym. Ponadto przeprowadza się rozmowę z osobą sprawdzaną oraz trzema osobami wskazanymi przez tę osobę w ankiecie bezpieczeństwa w celu potwierdzenia jej tożsamości oraz innych informacji mających wpływ na wynik postępowania sprawdzającego, a związanych z tą osobą. Specjalne postępowanie sprawdzające powinno zakończyć się przed upły-

wem trzech miesięcy od daty złożenia wniosku o jego przeprowadzenie wraz z wypełnioną przez daną osobę ankietą bezpieczeństwa.

W przypadku pozytywnego dla osoby sprawdzanej zakończenia postępowania sprawdzającego, to jest uznania, że w świetle dokonanych ustaleń nie ma żadnych wątpliwości, czy osoba ta daje rękojmię zachowania tajemnicy, służba ochrony państwa lub pełnomocnik ochrony wydają poświadczenie bezpieczeństwa. Dokument ten upoważnia daną osobę do dostępu do informacji niejawnych o klauzuli w nim określonej, a także do informacji oznaczonych klauzulami niższymi w zakresie niezbędnym związanym z zajmowanym stanowiskiem lub wykonywania określonej pracy zleconej. Wydanie poświadczenia bezpieczeństwa, np. do klauzuli „tajne", wcale nie oznacza, że dana osoba uzyskała dostęp do wszelkich informacji niejawnych stanowiących tajemnicę państwową, a jedynie do tych informacji, które będą jej niezbędne do wykonywania pracy na zajmowanym stanowisku lub wykonywania określonej pracy zleconej. Poświadczenie bezpieczeństwa powinno zawierać podstawę prawną, wskazanie wnioskodawcy postępowania sprawdzającego, określenie służby ochrony państwa lub pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające, datę i miejsce wydania, imię, nazwisko i datę urodzenia osoby sprawdzanej, rodzaj przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli informacji niejawnych, do których osoba ta ma mieć dostęp, oraz termin jego ważności. Poświadczenie zaopatruje się także w imienną pieczęć i czytelny podpis upoważnionego żołnierza lub funkcjonariusza służby ochrony państwa lub pełnomocnika ochrony, wydaje je się na czas określony w zależności od rodzaju klauzuli informacji niejawnych, i tak: przy klauzuli: „poufne" i „zastrzeżone" na 10 lat, „tajne" na 7 lat, „ściśle tajne" na 5 lat. Niewątpliwie poświadczenie bezpieczeństwa jest aktem administracyjnym, w znaczeniu sformalizowanego objawu woli organu administracyjnego skierowanego do zindywidualizowanego adresata, wywołującym skutki prawne w sferze prawa administracyjnego[14]. Gdy w trakcie postępowania sprawdzającego dojdzie do stwierdzenia na podstawie ustawowych przesłanek, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy, podmiot prowadzący postępowanie wydaje decyzję o odmowie wydania poświadczenia bezpieczeństwa. Podstawą do wydania takiej decyzji mogą być następujące przesłanki: świadome podanie przez osobę sprawdzaną w toku postępowania sprawdzającego nieprawdziwych informacji, uczestnictwo, współpraca lub popieranie działalności szpiegowskiej, skazanie osoby sprawdzanej prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, nieprzestrzeganie porządku konstytucyjnego Rzeczypospolitej Polskiej, zagrożenie osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu, informacje o chorobie psychicznej lub innych zakłóceniach czynności psychicznych mogących negatywnie wpływać na zdolność osoby sprawdzanej do zajmowania stanowiska lub wykonywania prac związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową, wyraźna różnica między poziomem życia osoby sprawdzanej a uzyskiwanymi przez nią dochodami, uzależnienie od alkoholu lub narkotyków. Przesłanki wydania decyzji o cofnięciu poświadczenia bezpieczeństwa są podobne. Decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać takie same elementy jak poświadczenie bezpieczeństwa oraz uzasadnienie faktyczne i prawne. Od uzasadnienia faktycznego można odstąpić lub je ograniczyć w zakresie, w jakim udostępnienie informacji osobie sprawdzanej mogłoby spowodować istotne zagrożenie podstawowych interesów Rzeczypospolitej Polskiej, dotyczących porządku publicznego,

---

[14] J. B o ć (red.), *Prawo administracyjne*, Kolonia Limited 2007, s. 320.

obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa. Zarówno decyzje te, jak i poświadczenie bezpieczeństwa zawierają elementy właściwe aktom administracyjnym wydawanym w postępowaniu administracyjnym. Są to z pewnością decyzje administracyjne w rozumieniu kwalifikowanych aktów prawnych wydawanych na podstawie obowiązujących przepisów prawa, rozstrzygających konkretną sprawę co do konkretnej osoby, wydawane w postępowaniu o prawnie unormowanej procedurze[15].

5. Postępowanie odwoławczo-skargowe

Na podstawie art. 1 pkt 20 ustawy z dnia 3 lutego 2001 r. o zmianie ustawy o ochronie informacji niejawnych[16] wprowadzony został rozdział 5a, z mocą obowiązującą od dnia 1 lutego 2001 r., który w całości normuje postępowanie odwoławcze i skargowe w przypadku odmowy wydania osobie sprawdzanej poświadczenia bezpieczeństwa lub jego cofnięcia. W przeciwieństwie do poprzednio obowiązującego stanu prawnego po nowelizacji ustawy osobie sprawdzanej w przypadku wydania jej negatywnego rozstrzygnięcia w zakresie dostępu do informacji niejawnych przysługują środki zaskarżenia na wzór tych, które występują w postępowaniu administracyjnym czy sądowo-administracyjnym, choć ustawodawca w żadnym z przepisów rozdziału 5a nie odnosi się do kodeksu postępowania administracyjnego z uwagi na specyfikę procedur związanych z ochroną informacji niejawnych. I tak: osoba, w stosunku do której właściwa służba ochrony państwa wydała decyzję o odmowie wydania poświadczenia bezpieczeństwa lub decyzję o jego cofnięciu, może złożyć odwołanie do Prezesa Rady Ministrów.

Odwołanie wnosi się w terminie 14 dni od dnia doręczenia osobie sprawdzanej przedmiotowej decyzji za pośrednictwem właściwej służby ochrony państwa. Odwołanie nie wymaga uzasadnienia. Jest to więc sytuacja podobna do wniesienia odwołania na gruncie przepisów postępowania administracyjnego. Służba ochrony państwa obowiązana jest w terminie 14 dni od dnia otrzymania odwołania przesłać je wraz z aktami sprawy Prezesowi Rady Ministrów. Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu trzech miesięcy od dnia otrzymania odwołania. Wniesienie odwołania do Prezesa Rady Ministrów następuje wtedy, gdy postępowanie sprawdzające przeprowadza właściwa służba ochrony państwa. Będzie to więc postępowanie poszerzone lub specjalne. Natomiast w sytuacji przeprowadzenia zwykłego postępowania sprawdzającego przez pełnomocnika ochrony, zakończonego wydaniem decyzji o odmowie wydania poświadczenia bezpieczeństwa bądź decyzji o jego cofnięciu, osobie sprawdzanej przysługuje odwołanie do Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Służby Kontrwywiadu Wojskowego za pośrednictwem pełnomocnika ochrony. Do postępowania odwoławczego przed wymienionymi podmiotami stosuje się przepisy ustawy dotyczące postępowania przed Prezesem Rady Ministrów. W przypadku uchybienia terminu co do wniesienia odwołania lub niedopuszczalności jego wniesienia Prezes Rady Ministrów wydaje w tych sprawach postanowienie, które jest ostateczne. Postanowienie to powinno zawierać w szczególności datę jego wydania, oznaczenie osoby sprawdzanej, powołanie podstawy prawnej, rozstrzygnięcie oraz uzasadnienie faktyczne i prawne. Musi zawierać też

---

[15] B. A d a m i a k, J. B o r k o w s k i, *Postępowanie administracyjne i sądowo-administracyjne*, Warszawa 2003, s. 245.

[16] Dz. U. z 2001 r. Nr 22, poz. 247.

pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego. W toku prowadzonego postępowania odwoławczego Prezes Rady Ministrów może na żądanie osoby sprawdzanej lub z urzędu zlecić służbie ochrony państwa przeprowadzenie dodatkowych czynności w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym. W przypadku śmierci osoby sprawdzanej lub cofnięcia odwołania przez osobę sprawdzaną postępowanie odwoławcze zostaje umorzone, jednakże Prezes Rady Ministrów nie uwzględni cofnięcia odwołania, jeżeli prowadziłoby to do naruszającego prawo lub interes bezpieczeństwa państwa utrzymania w mocy decyzji o odmowie wydania poświadczenia bezpieczeństwa. Po przeprowadzeniu postępowania odwoławczego Prezes Rady Ministrów wydaje decyzję utrzymującą w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa lub decyzję o cofnięciu poświadczenia bezpieczeństwa, uchylającą decyzję o odmowie wydania poświadczenia bezpieczeństwa, i nakazuje służbie ochrony państwa wydanie poświadczenia bezpieczeństwa albo uchylającą decyzję o cofnięciu poświadczenia bezpieczeństwa.

Prezes Rady Ministrów, wydając jedną z wymienionych decyzji, może odstąpić od uzasadnienia faktycznego decyzji lub ograniczyć je w takim zakresie, w jakim udostępnienie informacji osobie sprawdzanej mogłoby spowodować istotne zagrożenie podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa stosunków międzynarodowych lub gospodarczych państwa. Po zakończonym postępowaniu odwoławczym i wydaniu rozstrzygnięcia zwraca się akta dotyczące postępowania sprawdzającego właściwej służbie ochrony państwa. Decyzje i postanowienia doręcza się osobie sprawdzanej i właściwej służbie ochrony państwa na piśmie, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę upoważnioną do obsady stanowiska. Jak podano wyżej, taki tok postępowania odwoławczego, który obowiązuje przed Prezesem Rady Ministrów, obowiązuje przed Szefem ABW i SKW w przypadku przeprowadzenia zwykłego postępowania sprawdzającego przez pełnomocnika ochrony i zakończonego wydaniem niekorzystnego dla osoby sprawdzanej rozstrzygnięcia lub wydania decyzji o cofnięciu poświadczenia bezpieczeństwa.

Wydanie przez wymienione organy odwoławcze negatywnej dla osoby sprawdzanej decyzji kończącej postępowanie odwoławcze nie wyczerpuje jeszcze środków zaskarżenia przysługujących jej na gruncie przepisów znowelizowanej ustawy o ochronie informacji niejawnych. Osobie, wobec której w wyniku przeprowadzonego postępowania odwoławczego utrzymano w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa bądź decyzję o cofnięciu poświadczenia bezpieczeństwa lub wydano postanowienie o niedopuszczalności odwołania oraz uchybieniu terminu do wniesienia odwołania, służy skarga do sądu administracyjnego w terminie 30 dni od dnia doręczenia jej decyzji lub postanowienia. W kwestii terminu wniesienia skargi stosuje się przepis art. 53 ustawy z dnia 30 sierpnia 2002 r. – *Prawo o postępowaniu przed sądami administracyjnymi*[17]. Wobec faktu, że zarówno Prezes Rady Ministrów, jak i Szef Agencji Bezpieczeństwa Wewnętrznego mają siedzibę w Warszawie, zgodnie z właściwością terytorialną sądem właściwym do rozpatrzenia skargi jest Wojewódzki Sąd Administracyjny w Warszawie. Sąd administracyjny rozpoznaje skargę na posiedzeniu niejawnym. Wydany na posiedzeniu niejawnym wyrok uzasadnia się tylko w przypadku uwzględnienia skargi. Odpis wyroku z uzasadnieniem doręcza się tylko właściwej służbie ochrony państwa, osobie skarżącej i osobie upoważnionej do obsady stanowiska doręcza się odpis wyroku. Po wydaniu wyroku sąd administracyjny zwraca niezwłocznie właściwej

[17] Dz. U. z 2002 r. Nr 153, poz. 1270 z późn. zm.

służbie ochrony państwa akta postępowania sprawdzającego. Od wyroku wydanego przez Wojewódzki Sąd Administracyjny lub postanowienia kończącego postępowanie w sprawie przysługuje osobie sprawdzanej prawo do wniesienia skargi kasacyjnej do Naczelnego Sądu Administracyjnego. Przedmiotową skargę może również wnieść prokurator lub Rzecznik Praw Obywatelskich. Skarga powinna być sporządzona przez adwokata lub radcę prawnego. Wnosi się ją do sądu, który wydał zaskarżony wyrok lub postanowienie, w terminie 30 dni od dnia doręczenia odpisu orzeczenia osobie sprawdzanej. Tryb rozpoznania skargi przez Naczelny Sąd Administracyjny odbywa się w sposób podobny jak tryb jej rozpoznania przez Wojewódzki Sąd Administracyjny w Warszawie. Podkreślić należy tutaj, że w wyniku zmiany ustawy o ochronie informacji niejawnych w zakresie wprowadzenia przepisów regulujących postępowanie odwoławcze i skargowe, w przeciwieństwie do stanu prawnego obowiązującego przed jej zmianą, obecnie w celu dochodzenia swoich praw osoba sprawdzana w przypadku wydania w stosunku do niej negatywnego rozstrzygnięcia kończącego postępowanie sprawdzające korzystać może z szeregu środków zaskarżenia na drodze postępowania odwoławczego i sądowo-administracyjnego.

6. Bezpieczeństwo systemów i sieci teleinformatycznych. Polityka bezpieczeństwa informacji. Bezpieczeństwo przemysłowe

Bezpieczeństwo systemów i sieci teleinformatycznych to bardzo ważny element ochrony informacji niejawnych, albowiem w większości przypadków informacje te są wytwarzane, przetwarzane, przechowywane lub przekazywane na nośnikach elektronicznych. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc przed utratą właściwości informacje niejawne przetwarzane w wymienionych sieciach i systemach gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności. Kwestie związane z bezpieczeństwem teleinformatycznym informacji niejawnych regulują zarówno przepisy ustawy o ochronie informacji niejawnych, jak i rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[18]. Odpowiedzialność za organizację bezpieczeństwa teleinformatycznego w danej jednostce organizacyjnej ponosi jej kierownik, który w tym zakresie jest obowiązany zapewnić opracowanie dokumentacji bezpieczeństwa teleinformatycznego, realizację ochrony fizycznej, elektromagnetycznej i kryptograficznej systemu lub sieci teleinformatycznej, niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej, a także dokonać analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnić usunięcie stwierdzonych nieprawidłowości; osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej zorganizować przeszkolenia z zakresu bezpieczeństwa teleinformatycznego, zawiadomić właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych klauzulą co najmniej „poufne".

Budowa systemu zabezpieczeń, złożonego z wielu różnych elementów, zapewniającego ochronę informacji niejawnych, wymaga także wdrożenia określonych rozwiązań organizacyjnych zapewniających bezpieczeństwo tych informacji oraz jasne rozgraniczenie kompetencji i obowiązków osób za nie odpowiedzialnych. Stąd też kierownik jednostki organizacyj-

[18] Dz. U. z 2005 r. Nr 171, poz. 1433.

nej powinien wyznaczyć osobę lub zespół osób pełniących funkcję administratora systemu odpowiedzialnego za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemu ze szczególnymi wymaganiami bezpieczeństwa.

Polityka bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu, którego celem jest osiągnięcie bezpieczeństwa informacji na wszystkich poziomach i w każdej fazie życia systemu[19]. Obowiązek opracowania przez kierownika jednostki organizacyjnej dokumentu szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej wynika z przepisu art. 61 ustawy o ochronie informacji niejawnych[20]. Dokument ten powinien być sporządzony w formie pisemnej i zawierać: szczegóły budowy systemu teleinformatycznego wykorzystywanego do przetwarzania dokumentów zawierających informacje niejawne, opis zastosowanych w tym systemie zabezpieczeń programowych, elektromagnetycznych i kryptograficznych, plan wykonywania kopii bezpieczeństwa systemu, plan rozmieszczenia systemu wraz z opisem zastosowanych środków ochrony fizycznej, rysunkiem stref bezpieczeństwa i określeniem zadań poszczególnych osób odpowiedzialnych za eksploatację tego systemu. Opracowany dokument określający politykę bezpieczeństwa powinien określać także, jakie rodzaje informacji w systemie informatycznym mogą być przetwarzane oraz jakie warunki musi spełnić system, aby informacja w nim się znalazła.

Bezpieczeństwo systemów sieci komputerowych należy rozpatrywać na dwóch płaszczyznach: wewnętrznej i zewnętrznej. Płaszczyzna wewnętrzna obejmuje poufność gwarantującą, że dane znajdujące się w systemie nie będą udostępniane osobom nieuprawnionym; dostępność określającą, że dane będą zawsze udostępniane osobom, które tego zażądają, a osoby te są uprawnione; oraz integralność danych zgromadzonych w systemie i niemożność ich nieuprawnionych modyfikacji i zniekształceń. Pod pojęciem utraty dostępności należy rozumieć odmowę autoryzowanego dostępu lub opóźnienie operacji krytycznych pod względem czasu lub celu. Przez utratę integralności należy rozumieć nieautoryzowaną modyfikację informacji oraz utratę prawidłowego i spójnego działania systemu. Integralność opisuje stan poprawności działania sprzętu i oprogramowania oraz zapewnia ochronę przed nieupoważnioną modyfikacją danych. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych „strefami kontrolowanego dostępu" w zależności od klauzuli tajności, ilości, zagrożeń dla poufności, integralności lub dostępności informacji niejawnych, a także na zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed nieuprawnionym dostępem, podglądem czy podsłuchem. Ochrona kryptograficzna pozwala chronić poufność i autentyczność informacji, przy czym poufność oznacza, że informacja może być poprawnie odczytana jedynie przez upoważnione osoby lub programy; natomiast autentyczność oznacza, że informacja może być wygenerowana jedynie przez upoważnione osoby w sposób dający się poprawnie odczytać. Charakterystyki rozwiązań kryptograficznych, takie jak moc kryptograficzna, siła środków algorytmów, długość i charakter kluczy kryptograficznych, powinny być odpowiednio dobrane do klau-

---

[19] W. Dragoń, D. Mąka, M. Skawina, *Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, Warszawa 2004, s. 145.

[20] Tekst jedn., Dz. U. z 2005 r. Nr 196, poz. 1631.

zuli ochranianej informacji niejawnej. Cechy też podlegają ochronie na etapie projektowania, produkcji i eksploatacji[21].

Bezpieczeństwo przemysłowe można określić jako całokształt działań mających związek z zapewnieniem ochrony informacji niejawnych, które są udostępniane przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej w związku z umową lub zadaniem wykonywanym na podstawie przepisów prawa. Przedmiotem bezpieczeństwa przemysłowego są informacje niejawne stanowiące zarówno tajemnicę państwową, jak i służbową oraz ochrona tych informacji. Dokumentem potwierdzającym zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do ochrony informacji niejawnych stanowiących tajemnicę państwową jest wydane po przeprowadzeniu postępowania sprawdzającego świadectwo bezpieczeństwa przemysłowego.

7. Odpowiedzialność z tytułu naruszenia przepisów ustawy o ochronie informacji niejawnych

Kwestie związane z odpowiedzialnością za naruszenie przepisów ustawy o ochronie informacji niejawnych nie są uregulowane przepisami ustawy o ochronie informacji niejawnych, tylko ustawy z dnia 6 czerwca 1997 r. *Kodeks karny*[22]. Rozdział XXXIII kodeksu karnego poświęcony jest w całości przestępstwom przeciwko ochronie informacji, określając rodzaje przestępstw przeciwko ochronie informacji niejawnych wraz z sankcjami karnymi przewidzianymi za ich popełnienie. I tak: w przypadku ujawnienia lub wykorzystania wbrew przepisom ustawy informacji stanowiącej tajemnicę państwową sprawca podlega karze pozbawienia wolności od 3 miesięcy do lat 5; jeżeli przedmiotowa informacja została ujawniona osobie działającej na rzecz lub w imieniu podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do 8 lat. Natomiast nieumyślne ujawnienie przedmiotowej informacji przez osobę, która zapoznała się z jej treścią w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do 1 roku; zniszczenie, uszkodzenie, usunięcie lub zmiana zapisu istotnej informacji albo udaremnienie lub utrudnienie w inny sposób osobie uprawnionej zapoznania się z nią pociąga za sobą karę grzywny, ograniczenia lub pozbawienia wolności do lat 2; jeżeli czyn ten dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3, w przypadku wyrządzenia znacznej szkody majątkowej przez dopuszczenie się tego czynu sprawca podlega karze pozbawienia wolności od 3 miesięcy do 5 lat. Ściganie tego przestępstwa następuje na wniosek pokrzywdzonego. W przypadku nieuprawnionego ujawnienia przez funkcjonariusza publicznego informacji niejawnej stanowiącej tajemnicę służbową lub informacji pozyskanej w związku z wykonywaniem czynności służbowych, w przypadku narażenia na szkodę prawnie chronionego interesu czyn ten jest zagrożony karą pozbawienia wolności do 3 lat; uzyskanie bez uprawnienia informacji, nieprzeznaczonej dla danej osoby, przez otwarcie zamkniętego pisma lub podłączenie się do przewodu służącego do przekazu informacji albo przełamanie elektronicznego, magnetycznego, ewentualnie innego szczególnego jej zabezpieczenia jest zagrożone karą grzywny, ograni-

---

[21] K. L i d e r m a n, *Bezpieczeństwo teleinformatyczne*, Warszawa 2002, s. 37.

[22] Dz. U. z 1997 r. Nr 97, poz. 88 i 553 z późn. zm.

czenia lub pozbawienia wolności do lat 2. Taką samą sankcję może ponieść ten, kto w celu nieuprawnionego pozyskania informacji zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym. Wysoka sankcja karna przewidziana jest za niszczenie, uszkodzenie, usunięcie lub zmianę danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, jak też za zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych – czyn ten jest zagrożony karą pozbawienia wolności od 6 miesięcy do 8 lat.

8. Zakończenie

Polska została członkiem paktu północnoatlantyckiego dnia 10 marca 1999 r., a jednym z warunków członkostwa było stworzenie podstaw systemu ochrony informacji niejawnych zgodnego ze standardami NATO. Miała to uczynić ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych[23], w której główny akcent został postawiony na działania prewencyjne i edukację w dziedzinie bezpieczeństwa informacji. Wyraźnie zostały określone organy odpowiedzialne za ochronę tych informacji, metody klasyfikacji, sposób doboru pracowników, którym będą one udostępniane, przebieg postępowań sprawdzających. Praktyka paru lat stosowania przepisów tej ustawy wykazała, że w niektórych kwestiach nie była ona wolna od niedoskonałości, stąd też podjęto próby jej zmiany, które z pewnością nastąpią w przyszłości z uwagi na rozwój zjawisk mających bezpośredni związek z bezpieczeństwem informacji. Należy jednak podkreślić, że od chwili wejścia w życie przepisów ustawy w zakresie budowy kompleksowego systemu ochrony informacji niejawnych w Polsce wykonany został ogrom pracy, głównie ze strony służb ochrony państwa i pełnomocników ochrony. Przykładem tego może być przeprowadzenie przez te podmioty dziesiątków tysięcy postępowań sprawdzających wobec osób starających się o dostęp do informacji niejawnych. Aby zrealizować zasadę, że dostęp do tych informacji mają tylko te osoby, które dają rękojmię zachowania tajemnicy, przeprowadzono tysiące postępowań sprawdzających i szkoleń w zakresie ochrony informacji niejawnych. W jednostkach organizacyjnych, do których mają zastosowanie przepisy ustawy, powstały piony ochrony informacji niejawnych. Przeprowadzono zmianę przepisów ustawy o ochronie informacji niejawnych w zakresie środków odwoławczych przysługujących osobom, wobec których postępowanie sprawdzające zakończyło się wynikiem negatywnym, co pozwala odrzucić zarzut, że Polska nie przestrzega przyjętych norm prawa międzynarodowego wynikającego z treści art. 13 europejskiej *Konwencji o ochronie praw człowieka i podstawowych wolności*. Od roku 1999 przedstawiciele Biura Bezpieczeństwa NATO przeprowadzili kilka okresowych kontroli dotyczących przestrzegania przez Polskę przepisów związanych z bezpieczeństwem informacji. Wszystkie te inspekcje pozytywnie oceniły zastosowane w naszym kraju rozwiązania systemowe w zakresie informacji niejawnych, co stanowi pochlebną ocenę głównie dla służb ochrony państwa i innych podmiotów zajmujących się ich ochroną, gdyż system ten budowały od podstaw.

---

[23] Tekst jedn., Dz. U. z 2005 r. Nr 196, poz. 1631.

SUMMARY

The Protection of Confidental Information.General Issues

The article describes notions concerning of classifield information In general manner. The notions such as: official secrets, access to secret information, checking procedure, appeals, tele-informative security, responsibility for revealing official secrets. These matters are regulated according to law concerning protection of classifield information from 22nd January 1999 and the executive regulations. The issue of protecting classifield information was always playing paramount role in country's security system. Bill's regulations were enacted due to entering NATO by Poland. Poland was obliged to conform her law to law binding in NATO countries.

Literatura

Adamiak B., Borkowski J., *Postępowanie administracyjne i sądowo-administracyjne*, Warszawa 2003.

Boć J., (red.), *Prawo administracyjne*, Kolonia Limited 2007.

Dragoń W., Mąka D., Skawina M., *Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, Warszawa 2004.

Jakubas B., Ryszkowski M., *Ochrona informacji niejawnych*, Warszawa 2001.

Kurzępa B., *Dostęp do informacji niejawnych*, „Prawo i Prokuratura" 2000, nr 6.

Kurzępa B., *Ochrona informacji niejawnych. Ochrona danych osobowych. Zbiór przepisów*, Bielsko-Biała 2000.

Liderman K., *Bezpieczeństwo teleinformatyczne*, Warszawa 2002.

Mąka D., *Elementy analizy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego*, Warszawa 2003.

Mucha M., *NIP. Zasady ewidencji i identyfikacji podatników i płatników*, wyd. 2, Warszawa 2005.

Ruszczyk I., *Instrukcja ochrony informacji niejawnych, ściśle tajne, tajne, poufne, zastrzeżone, po nowelizacji*, Gdańsk 2002.

Szewc T., *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007.

Taradejna R., Taradejna M., *Tajemnica państwowa i inne tajemnice chroniące interesy obywateli. Zbiór przepisów z komentarzem*, Warszawa 1998.

Thiem P., *Instrukcja postępowania z materiałami niejawnymi z komentarzem*, Gdańsk 2002.

Źródła prawa

Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, tekst jedn. Dz. U. z 2005 r. Nr 196, poz. 1631.

Ustawa z dnia 3 lutego 2001 r. o zmianie ustawy o ochronie informacji niejawnych, Dz. U. z 2001r. Nr 22, poz. 247.

Ustawa z dnia 10 czerwca 1994 r. o zamówieniach publicznych, tekst jedn. Dz. U. z 1998 r. Nr 119, poz.773, z późn. zm.

Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej, Dz. U. z 1982 r. Nr 40, poz. 271, z późn. zm.

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego, Dz. U. z 2002 r. Nr 74, poz. 676.

Ustawa z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, Dz. U. z 1997 r. Nr 106, poz. 679, z późn. zm.

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz. U. z 1993r. Nr. 47, poz. 221, z późn. zm.

Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*, Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.

Ustawa z dnia 30 sierpnia 2002 r. *Prawo o postępowaniu przed sądami administracyjnymi*, Dz. U. z 2002 r. Nr 153, poz. 1270, z późn. zm.

Rozporządzenie Rady Ministrów z dnia 18 października 2005r. w sprawie organizacji i funkcjonowania kancelarii tajnych, Dz. U. z 2005 r. Nr 208, poz. 1741.

Rozporządzenie Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli, Dz. U. z 2005 r. Nr 205, poz. 1696.

Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. z 2005 r. Nr 171, poz. 1433.