BIBLIOTEKA PRZEGLĄDU BEZPIECZEŃSTWA WEWNĘTRZNEGO

BPBW 1

ISBN 978-83-929271-2-9

OCHRONA INFORMACJI NIEJAWNYCH

PORADNIK PRAKTYCZNY

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

CENTRALNY OŚRODEK SZKOLENIA
im. gen. Stefana Roweckiego „GROTA”

OCHRONA INFORMACJI NIEJAWNYCH

PORADNIK PRAKTYCZNY

dla osób i instytucji przetwarzających informacje niejawne

WARSZAWA 2011

Recenzja

dr hab. prof. Uniwersytetu Opolskiego Stanisław Hoc

Redakcja „PBW”

Zbigniew Nawrocki (redaktor naczelny)
Piotr Potejko (zastępca redaktora naczelnego)
Joanna Stępniak-Getke (sekretarz redakcji)
Justyna Kostarska-Seliga, Izabela Laskus,
Grażyna Osuchowska, Anna Przyborowska
(redakcja i korekta)
Piotr Tchorzewski
Antoni Podolski (konsultacja merytoryczna)

ISBN 978-83-929271-2-9

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia w Emowie
im. gen. Stefana Roweckiego „Grota”
05-462 Wiązowna, ul. Nadwiślańczyków

Redakcja
tel. (+48) 22 58 57 736
fax (+48) 22 58 57 014
e-mail: redakcja.pbw@abw.gov.pl

www.abw.gov.pl

Skład: Gabinet Szefa ABW

Druk: Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
12-100 Szczytno, ul. Piłsudskiego 111

Spis treści

Wstęp

W dniu 2 stycznia 2011 r. weszła w życie *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r. Nr 182, poz. 1228). W pracach nad projektem tej ustawy aktywnie uczestniczyli funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, którzy zaangażowali się również w opracowanie niniejszego poradnika.

Opracowanie to skierowane jest do wszystkich osób zainteresowanych problematyką ochrony informacji niejawnych, a w szczególności do kierowników jednostek organizacyjnych przetwarzających takie informacje, pełnomocników ochrony oraz pracowników pionów ochrony.

Poradnik poświęcony jest omówieniu zmian, jakie nowa ustawa wprowadza w poszczególnych częściach składowych systemu ochrony informacji niejawnych (przepisach ogólnych, klasyfikowaniu oraz organizacji ochrony informacji niejawnych, bezpieczeństwie osobowym, przemysłowym czy teleinformatycznym). Opracowanie nie stanowi zatem omówienia wszystkich przepisów ustawy.

Co równie ważne, niniejszy materiał nie ma charakteru dokumentu naukowego lub nawet quasi-naukowego. Świadomie zrezygnowano z komentarzy na temat okoliczności towarzyszących przyjęciu takich, a nie innych, rozwiązań oraz przewidywanych następstw zastosowania nowych uregulowań.

Autorzy mają nadzieję, że opracowanie to, wraz z materiałem zamieszczonym na stronie www.bip.abw.gov.pl oraz codziennymi działaniami funkcjonariuszy ABW o charakterze informacyjno-szkoleniowym, przyczyni się do lepszego zrozumienia zasad działania systemu ochrony informacji niejawnych w Polsce.

SZEF
AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

GEN. BRYG. KRZYSZTOF BONDARYK

Jolanta Frąckiewicz
Tomasz Gołębiewski
Tomasz Klimowicz
Dariusz Kubaszewski
Stanisław Smykla
Jarosław Stachura

Informacje niejawne bez tajemnic

Najważniejsze zmiany w systemie ochrony informacji niejawnych wprowadzone przepisami Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Wstęp

Jednym z warunków przyjęcia Rzeczypospolitej Polskiej do Sojuszu Północnoatlantyckiego było stworzenie nowego, zgodnego z przepisami NATO, systemu ochrony informacji niejawnych. Rozwiązania wprowadzone przez uchwaloną w dniu 22 stycznia 1999 r. (weszła w życie w dzień poprzedzający przystąpienie Polski do NATO) ustawę o ochronie informacji niejawnych wynikały z nierepresyjnej filozofii opierającej się na systemie prewencji, zapobiegania i minimalizowania zagrożeń w sferze ochrony informacji, w szczególności przypadków ujawniania informacji klauzulowanych podmiotom do tego nieuprawnionym, a gdy do takiego przypadku już dojdzie – na ustalaniu osób odpowiedzialnych za to i uzupełnianiu systemu ochrony tego typu danych o wnioski wynikające z wykrytych nieprawidłowości.

W ciągu przeszło 11 lat obowiązywania przywołanej ustawy, na podstawie systematycznie przeprowadzanych przez uprawnione podmioty diagnoz sytuacji i wypływających stąd wniosków oraz na skutek zmian w przepisach innych ustaw, przeprowadzane były jej nowelizacje oraz zmiany w aktach wykonawczych. Łącznie ustawę nowelizowano 23 razy. Mimo tych zmian, obowiązujące przepisy w powszechnym przekonaniu nie zapewniły w pełni skutecznej ochrony informacji, m.in. z uwagi na fakt, że:

- nie określały dostatecznie precyzyjnie przedmiotu ochrony (mimo wykazu stanowiącego załącznik do ustawy),
- narzucały konieczność wdrażania sztywnych, a przy tym kosztownych rozwiązań, nieuzasadnionych często ilością i wagą przetwarzanych informacji,

- nie określały wystarczająco jasno indywidualnej odpowiedzialności za ochronę informacji niejawnych na poziomie podmiotów ustawy,
- nie pozwalały na skuteczną ochronę informacji przed nowymi zagrożeniami.

Obowiązująca od 2 stycznia 2011 r. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228), zwana dalej „ustawą", w sposób kompleksowy uregulowała sferę ochrony informacji niejawnych, nie wprowadzając jednocześnie zasad i rozwiązań radykalnie odmiennych od dotychczasowych. Przeciwnie – można ją uznać za kolejny krok na drodze do pełnego wdrożenia w Polsce powszechnie przyjętych reguł podstawowych. Powinno to służyć wyeliminowaniu niedoskonałości dotychczasowego systemu, dostosowaniu go do nowych wyzwań, a także usprawnieniu współpracy międzynarodowej w dziedzinach wymagających wymiany informacji niejawnych. Celem projektodawców ustawy było zatem wprowadzenie racjonalnych, spójnych, konsekwentnych i zarazem elastycznych rozwiązań dotyczących bezpieczeństwa informacji niejawnych, co z jednej strony powinno podnieść efektywność całego systemu, z drugiej zaś – ułatwić sprawne i skuteczne wykonywanie zadań związanych z dostępem do tego typu informacji, zwłaszcza opatrzonych niższymi klauzulami tajności. Jest to szczególnie ważne w kontekście objęcia przez Polskę w 2011 r. przewodnictwa w Radzie Unii Europejskiej.

Przepisy dotyczące ogólnych zasad funkcjonowania systemu ochrony informacji niejawnych

Przepisy każdej ustawy zawarte w rozdziale zatytułowanym *Przepisy ogólne* mają szczególne znaczenie dla całego aktu prawnego. Dotyczą bowiem nie tylko wskazania obszaru uregulowanych spraw, właściwych podmiotów ustawy i objaśnienia użytych pojęć, ale również *postanowień wspólnych dla wszystkich albo dla większości przepisów merytorycznych zawartych w ustawie*[1]. Podobnie jest w przypadku rozdziału 1. ustawy o ochronie informacji niejawnych.

Należy przede wszystkim zauważyć, że zaszła zasadnicza zmiana w zakresie określenia przedmiotu ustawy. W art. 1 ust. 1, w którym wymieniono zasady ochrony informacji niejawnych, zastosowano zwrot *to jest zasady*, który de facto decyduje o ich zamkniętym katalogu. Dotychczas wykaz ten – dzięki użyciu zwrotu *a w szczególności* – był otwarty. Jest to o tyle ważne, że wśród podanych zasad nie zostały wymienione ani kwestie związane z prowadzeniem ewidencji czy udostępnianiem danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego, które zostały

[1] *Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (Dz.U. z 2002 r., Nr 100, poz. 908).

uregulowane w rozdziale dziesiątym przedmiotowej ustawy, ani kwestie dotyczące szkoleń z zakresu ochrony informacji niejawnych, którym poświęcono rozdział czwarty. Taki nieprecyzyjny zapis, mimo że nie było to intencją projektodawców[2], może budzić wątpliwości co do traktowania przedmiotowych zagadnień na równi z innymi zasadami dotyczącymi systemu ochrony informacji niejawnych.

Art. 1. 1. Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej „informacjami niejawnymi", to jest zasady:

1. *klasyfikowania informacji niejawnych;*
2. *organizowania ochrony informacji niejawnych;*
3. *przetwarzania informacji niejawnych;*
4. *postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym";*
5. *postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego";*
6. *organizacji kontroli stanu zabezpieczenia informacji niejawnych;*
7. *ochrony informacji niejawnych w systemach teleinformatycznych;*
8. *stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.*

Niezwykle ważne jest wprowadzenie w art. 1 ust. 3 formuły *z zastrzeżeniem art. 5* (której brak w analogicznym art. 1 ust. 3 ustawy poprzedniej), co wskazuje, że informacje chronione jako „tajemnica zawodowa" lub „inna tajemnica prawnie chroniona" nie są regulowane przepisami ustawy o ochronie informacji niejawnych, chyba że zachodzą przesłanki określone w art. 5^3.

3. *Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych, z zastrzeżeniem art. 5.*

Zmian dokonano także w art. 1 ust. 2, w którym wymieniono podmioty ustawy.

2. Przepisy ustawy mają zastosowanie do:

1) organów władzy publicznej, w szczególności:

a) Sejmu i Senatu,

b) Prezydenta Rzeczypospolitej Polskiej,

c) organów administracji rządowej,

[2] Zapis ten stanowi efekt przyjęcia stosownej poprawki Senatu.

[3] W artykule tym zdefiniowano informacje o wszystkich klauzulach tajności, tj. „ściśle tajne", „tajne", „poufne" i „zastrzeżone".

d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,

e) sądów i trybunałów,

f) organów kontroli państwowej i ochrony prawa;

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

3) Narodowego Banku Polskiego;

4) państwowych osób prawnych i innych niż wymienione w pkt 1-3 państwowych jednostek organizacyjnych;

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

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

Przede wszystkim, obok organów jednostek samorządu terytorialnego – art. 1 ust. 2 pkt 1 lit. d – podmiotami ustawy są także *inne podległe im jednostki organizacyjne lub przez nie nadzorowane*. Uproszczono ponadto nazewnictwo z zakresu wojskowości, ograniczając się do terminu funkcjonującego w innych ustawach (*jednostki podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane* – art. 1 ust. 2 pkt 2). Z katalogu podmiotów ustawy (z mocy prawa) wyłączono banki państwowe (w art. 1 ust. 2 pkt 3), które jako przedsiębiorcy mogą być podmiotami ustawy na podstawie art. 1 ust. 2 pkt 6. Najistotniejsza zmiana w zakresie określenia podmiotów ustawy dokonana została w art. 1 ust. 2 pkt 6, w którym wykreślono pojęcia jednostki naukowe lub badawczo-rozwojowe. Zmiana ta związana jest z zastosowaniem w ustawie definicji przedsiębiorcy *sensu largo* (art. 2 pkt 13), tj. (…) *przedsiębiorcą jest przedsiębiorca w rozumieniu art. 4 Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej* (…) *lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa.*

Art. 2. *W rozumieniu ustawy:*

1) jednostką organizacyjną - jest podmiot wymieniony w art. 1 ust. 2;

2) rękojmią zachowania tajemnicy - jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;

3) dokumentem - jest każda utrwalona informacja niejawna;

4) materiałem - jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;

5) przetwarzaniem informacji niejawnych - są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

6) systemem teleinformatycznym - jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204, z późn. zm.2);

7) dokumentem szczególnych wymagań bezpieczeństwa - jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;

8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego - jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;

9) dokumentacją bezpieczeństwa systemu teleinformatycznego - jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;

10) akredytacją bezpieczeństwa teleinformatycznego - jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;

11) certyfikacją - jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;

12) audytem bezpieczeństwa systemu teleinformatycznego - jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;

13) przedsiębiorcą - jest przedsiębiorca w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z późn. zm.3) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa;

14) kierownikiem przedsiębiorcy - jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy - cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę; w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej - wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej - komplementariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;

15) ryzykiem - jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

16) szacowaniem ryzyka - jest całościowy proces analizy i oceny ryzyka;

17) zarządzaniem ryzykiem - są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

18) zatrudnieniem - jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

Poza definicją przedsiębiorcy dodano w słowniczku inne nowe pojęcia, np.: przetwarzanie informacji niejawnych, kierownik przedsiębiorcy oraz zatrudnienie. Najwięcej, bo aż dziesięć, pojęć użytych w art. 2 odnosi się do zagadnień uregulowanych w rozdziale ósmym – *Bezpieczeństwo teleinformatyczne*.

Zmiana dokonana w art. 3 dotyczącym stosowania przepisów kodeksu postępowania administracyjnego do procedur opisanych w ustawie (postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego) oznacza wyłączenie postępowań odwoławczych spod stosowania tychże przepisów. Nowe przepisy kpa, które mają zastosowanie do wyżej wymienionych postępowań mają usprawnić realizację procedur[4].

Przepisy zawarte w art. 4 ustawy, kończącym rozdział pierwszy, dotyczące zasady *need to know* oraz zasad związanych ze zwalnianiem z obowiązku zachowania tajemnicy oraz dostępu do pomieszczeń i materiałów na podstawie innych ustaw, zostały wprost przyjęte z art. 3 i art. 4 poprzedniej ustawy.

Zasadnicze zmiany nowa ustawa wprowadza w zakresie definicji informacji niejawnych oraz ochrony i znoszenia klauzul tajności (rozdział drugi – *Klasyfikowanie informacji niejawnych*). Utrzymując dotychczasowe nazwy klauzul tajności („ściśle tajne", „tajne", „poufne" i „zastrzeżone"), zrezygnowano z podziału informacji niejawnych na *tajemnicę państwową* i *tajemnicę służbową*. W art. 5 zawarto nowe definicje informacji niejawnych oznaczonych poszczególnymi klauzulami tajności. Zrezygnowano z definicji, na którą w przypadku informacji o klauzulach „ściśle „tajne" i „tajne" składała się przesłanka formalna (potencjalna szkoda w przypadku nieuprawnionego ujawnienia) i materialna (odesłanie do wykazu stanowiącego załącznik do ustawy). Zmiany dotyczą także dotychczasowej *tajemnicy służbowej* – zrezygnowano z oznaczania klauzulami „poufne" lub „zastrzeżone" informacji chronionych na podstawie innych ustaw, a definicje tych klauzul, podobnie jak w przypadku klauzul „ściśle tajne" i „tajne", odniesiono jedynie do ewentualnych szkód, jakie ujawnienie tego typu informacji mogłoby przynieść dla bezpieczeństwa i interesów Rzeczypospolitej Polskiej.

W związku z powyższym, w przypadku informacji niejawnych o klauzulach „ściśle tajne", „tajne" i „poufne" muszą być spełnione łącznie dwie przesłanki:

[4] Art. 50 kpa – możliwość składania wyjaśnień przez pełnomocnika lub na piśmie, art. 55 kpa – ułatwienie komunikowania się ze stroną (np. telefonicznie), art. 65 kpa – brak negatywnych konsekwencji w kontekście zachowania terminu w przypadku wniesienia podania do niewłaściwego organu, art. 103 kpa – wstrzymanie biegu terminów w przypadku zawieszenia postępowania.

- nieuprawnione ujawnienie tych informacji musi zagrażać wymienionym enumeratywnie (zróżnicowanym adekwatnie do klauzuli) dobrom,
- nieuprawnione ujawnienie tych informacji spowoduje dla Rzeczypospolitej Polskiej – w przypadku informacji „ściśle tajnych" – *szkodę wyjątkowo poważną*, „tajnych" – *szkodę poważną*, „poufnych" – *szkodę*.

Informacjom niejawnym nadaje się natomiast klauzulę „zastrzeżone", *jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej* (art. 5 ust. 4).

> *4. Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.*

Należy zwrócić uwagę na zmianę definicyjną dotyczącą danych funkcjonariuszy, żołnierzy lub pracowników operacyjnych, które stanowią informacje niejawne o klauzuli „ściśle tajne". Klauzulę tę nadaje się informacjom, których nieuprawnione ujawnienie spowoduje wyjątkową szkodę dla RP poprzez to, że *doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie* (art. 5 ust. 1 pkt 5).

> *5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;*

Zgodnie zaś z definicją obowiązującą wcześniej, klauzula „ściśle tajne" powinna być nadawana danym identyfikującym lub mogącym doprowadzić do identyfikacji funkcjonariuszy i żołnierzy służb, o których mowa w pkt. 16 załącznika nr 1 do poprzedniej ustawy[5], realizujących czynności operacyjno-rozpoznawcze (art. 2 pkt 1 w związku z punktem I.18 tego załącznika).

[5] Tj. funkcjonariuszy i żołnierzy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego oraz byłego Urzędu Ochrony Państwa i byłych Wojskowych Służb Informacyjnych.

Zasadnicze zmiany zostały wprowadzone również w zakresie znoszenia lub zmiany nadanej klauzuli tajności, których głównym przejawem jest odejście od ustawowo określonych okresów ochrony na rzecz możliwości zniesienia lub zmiany klauzuli w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Powstawaniu ewentualnych nieracjonalnych sytuacji ma zapobiec:

- obowiązek przeglądu wszystkich wytworzonych dokumentów niejawnych raz na pięć lat w celu określenia, czy informacje te nadal spełniają ustawowe przesłanki, które były podstawą do nadania im klauzuli tajności (art. 6 ust. 4),

> *4. Kierownicy jednostek organizacyjnych przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.*

- obowiązek przeprowadzenia w terminie 36 miesięcy od dnia wejścia w życie ustawy przeglądu wytworzonych w podległych im jednostkach materiałów w celu ustalenia, czy spełniają przesłanki ochrony zgodne z nowymi definicjami informacji niejawnych wprowadzonymi przez ustawę (art. 181).

> **Art. 181.**
>
> 1. *Kierownicy jednostek organizacyjnych przeprowadzą, w terminie 36 miesięcy od dnia wejścia w życie ustawy, przegląd wytworzonych w podległych im jednostkach organizacyjnych materiałów zawierających informacje niejawne w celu ustalenia, czy spełniają ustawowe przesłanki ochrony na podstawie ustawy, i dokonają w razie potrzeby zmiany lub zniesienia klauzuli tajności.*
> 2. *Obowiązek, o którym mowa w ust. 1, nie dotyczy zbiorów materiałów spraw zakończonych oraz kartotek ewidencyjnych, w szczególności stanowiących materiał archiwalny przekazany do właściwych archiwów na podstawie odrębnych przepisów.*
> 3. *Kierownik właściwego archiwum, w uzasadnionych przypadkach, może zwrócić się do kierownika jednostki organizacyjnej, która przekazała materiał archiwalny, o którym mowa w ust. 2, o przeprowadzenie przeglądu tego materiału w celu ustalenia, czy spełnia ustawowe przesłanki ochrony, i dokonanie w razie potrzeby zmiany lub zniesienia klauzuli tajności.*

Wprowadzono ponadto możliwość określania z góry (niezależnie od klauzuli) daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności oraz nadawania odrębnie klauzul tajności poszczególnym częściom jednego materiału (art. 6 ust. 2 i 8 ustawy).

> *2. Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ust. 3, z zastrzeżeniem ust. 6. Osoba, o której mowa w ust. 1, może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.*
>
> *8. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.*

Uprawnienie w zakresie znoszenia lub zmiany klauzul tajności (*w przypadku ustania lub zmiany ustawowych przesłanek ochrony*) nadal posiada osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, ale normą ustawową (dotychczas kwestię tę regulowały przepisy odpowiedniego rozporządzenia) stał się *obowiązek wyrażenia pisemnej zgody* na to (art. 6 ust. 3).

> *3. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa w ust. 1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony, o których mowa w art. 5, z zastrzeżeniem ust. 5.*

Szczególnej ochronie poddano informacje o klauzuli „ściśle tajne", w przypadku których decyzję o zmianie lub zniesieniu klauzuli tajności może podjąć wyłącznie kierownik jednostki organizacyjnej, w której klauzula ta została nadana, a więc osoba, która na podstawie art. 14 ustawy w największym stopniu ponosi odpowiedzialność za ochronę informacji niejawnych w danej jednostce (art. 6 ust. 5).

> *5. Pisemną zgodę na wykonanie czynności, o których mowa w ust. 3, w przypadku informacji niejawnych o klauzuli „ściśle tajne" wyraża kierownik jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności.*

Możliwość dokonywania zmian i znoszenia klauzul tajności (o których mowa w art. 6 ustawy) nie dotyczy jednak wszystkich kategorii informacji niejawnych. Wyłączeniu w tym zakresie podlegają informacje wskazane w art. 7 ust. 1, które mają podlegać ochronie bez względu na upływ czasu, czyli takie, które mogą identyfikować funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania czynności operacyjno-rozpoznawczych, a także osoby udzielające pomocy w wykonywaniu tych czynności oraz informacje niejawne, uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

> **Art. 7.**
>
> *1. Chronione bez względu na upływ czasu, z zastrzeżeniem ust. 2, są:*
>
> *1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;*
>
> *2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;*
>
> *3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.*

Przepis ten nie jest prostym powtórzeniem art. 25 ust. 2 poprzedniej ustawy. Zgodnie bowiem z dotychczasowym stanem prawnym, ochronie bez względu na upływ czasu podlegać miały dane identyfikujące funkcjonariuszy i żołnierzy, ale tylko ABW, AW, SKW, SWW i CBA oraz byłego UOP i byłych WSI, wykonujących czynności operacyjno-rozpoznawcze, czyli funkcjonariuszy i żołnierzy służb specjalnych.

W art. 9 ustawy wprowadzono możliwość „odwołania się" od decyzji wytwórcy dotyczącej nadania klauzuli tajności do ABW lub SKW, a w przypadku, gdy stroną sporu jest jedna z tych służb – do Prezesa Rady Ministrów. W dotychczasowym systemie odbiorca mógł apelować o zmianę nieprawidłowej klauzuli tylko do wytwórcy.

Art. 9.

1. *Odbiorca materiału, w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności, może zwrócić się do osoby, która ją nadała, albo przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany.*
2. *W przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty złożenia wniosku, o którym mowa w ust. 1, odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW o rozstrzygnięcie sporu.*
3. *Spór, o którym mowa w ust. 2, ABW lub SKW rozstrzyga w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.*
4. *Jeżeli stroną sporu, o którym mowa w ust. 2, jest ABW albo SKW, to spór rozstrzyga Prezes Rady Ministrów w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.*
5. *Prezes Rady Ministrów może upoważnić Szefa Kancelarii Prezesa Rady Ministrów, sekretarza stanu albo podsekretarza stanu w Kancelarii Prezesa Rady Ministrów do wykonywania czynności, o których mowa w ust. 4.*

W rozdziale 1 (art. 8) wymieniono także ogólne zasady dotyczące ochrony informacji, które:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności,
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności,
- muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Art. 8.

Informacje niejawne, którym nadano określoną klauzulę tajności:

1) mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;

2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;

3) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Przepisy szczegółowo rozwijające te zasady znajdują się w kolejnych rozdziałach ustawy.

Przepisy dotyczące organizacji ochrony informacji niejawnych

Szczególne znaczenie wśród przepisów zawartych w rozdziale 3 – *Organizacja ochrony informacji niejawnych* – ma art. 10, w którym określono podział właściwości między Agencją Bezpieczeństwa Wewnętrznego i Służbą Kontrwywiadu Wojskowego. W poprzedniej ustawie takiego podziału nie było. Dokonywano go, posiłkując się określeniem kompetencji obu służb w odniesieniu do bezpieczeństwa osobowego (art. 29 ust. 1 poprzedniej ustawy). Wymienione w art. 10 ust. 1 uprawnienia zawężono w przypadku SKW do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, ataszatów obrony w placówkach zagranicznych oraz żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych. Przyjęcie tego rozwiązania niesie ze sobą daleko idące konsekwencje dotyczące ubiegania się o świadectwo bezpieczeństwa przemysłowego, o czym będzie mowa dalej.

Art. 10.

1. *ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ust. 2 i 3:*

1) prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;

2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;

3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;

4) zapewniają ochronę informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;

5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

Uwagę zwraca brak w art. 10 ust. 1, w którym wymieniono zadania ABW i SKW, przepisu (art. 14 ust. 1 pkt 6 poprzedniej ustawy) dotyczącego wykonywania przez te służby *innych zadań, w zakresie ochrony informacji niejawnych, określonych odrębnymi przepisami.*

Zasadniczą zmianą jest ustanowienie w art. 11 przedmiotowej ustawy jednej krajowej władzy bezpieczeństwa, której funkcję pełni Szef ABW (w poprzedniej ustawie – Szef ABW i Szef SKW).

Art. 11.

1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Co istotne, w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2, Szef ABW ma wykonywać swą funkcję za pośrednictwem Szefa SKW.

2. SKW realizuje zadania w odniesieniu do:

1) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

2) ataszatów obrony w placówkach zagranicznych;

3) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1 i 2.

Niezwykle ważne w tym kontekście będzie określenie w rozporządzeniu, które na podstawie art. 11 ust. 6 ustawy wyda Prezes Rady Ministrów, zakresu, trybu i sposobu współdziałania Szefów ABW i SKW w ramach wykonywania funkcji krajowej władzy bezpieczeństwa przez tego pierwszego. Rozporządzenie to uwzględni rolę Szefa ABW w nadzorze nad systemem ochrony informacji niejawnych wymienianych między Rzeczpospolitą Polską i innymi państwami lub organizacjami międzynarodowymi oraz konieczność zapewnienia jednolitości procedur stosowanych przez krajową władzę bezpieczeństwa w sferze cywilnej i wojskowej.

6. Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, tryb i sposób współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW.

W art. 12 ustawy określono uprawnienia ABW i SKW dotyczące realizacji czynności kontrolnych w zakresie ochrony informacji niejawnych. Usunięto zapis zawarty w art. 16 ust. 1 poprzedniej ustawy odnośnie kontroli „tajemnicy państwowej", jednoznacznie wskazując, iż ABW i SKW uprawnione są do kontroli ochrony informacji niejawnych oznaczonych wszystkimi klauzulami. Ponadto, z ust. 1 wykreślono zapis zawarty w art. 16 ust. 5 poprzedniej ustawy dotyczący żądania

od kierowników i pracowników kontrolowanych jednostek posiadanych przez nich informacji na temat działalności wywiadowczej albo terrorystycznej, skierowanej przeciwko RP.

Art. 12.

1. *W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych, upoważnieni pisemnie funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mają prawo do:*

   1) wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane;

   2) wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;

   3) żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji;

   4) przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;

   5) żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień;

   6) zasięgania w związku z przeprowadzaną kontrolą informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;

   7) powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;

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

2. *Jeżeli w czasie wykonywania kontroli, o której mowa w ust. 1, zostanie w znacznym stopniu uprawdopodobnione podejrzenie możliwości przetwarzania informacji niejawnych w systemach teleinformatycznych nieposiadających akredytacji bezpieczeństwa teleinformatycznego, funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mogą żądać udostępnienia do kontroli tych systemów, wyłącznie w celu i zakresie niezbędnym do ustalenia, czy przetwarzanie takie miało miejsce, oraz wyjaśnienia okoliczności z tym związanych.*

3. *Postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5, podlegają kontroli w zakresie prawidłowości ich realizacji. Kontrolę tę prowadzą:*

   1) Prezes Rady Ministrów - w odniesieniu do postępowań zrealizowanych przez ABW albo SKW;

   2) odpowiednio ABW lub SKW - w odniesieniu do postępowań zrealizowanych przez pełnomocników ochrony.

4. *Do czynności, o których mowa w ust. 1 i 3, dokonywanych przez ABW albo SKW albo przez Prezesa Rady Ministrów mają zastosowanie odpowiednio przepisy art. 30-39 ust. 2-4, art. 40 ust. 2-4, art. 41-49 ust. 2-6, art. 50 ust. 1-3, art. 64 ust. 1 i art. 98 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2007 r. Nr 231, poz. 1701 oraz z 2008 r. Nr 209, poz. 1315, Nr 225, poz. 1502 i Nr 227, poz. 1505), z tym że przewidziane w tej ustawie uprawnienia i obowiązki:*

   1) Najwyższej Izby Kontroli - wykonują odpowiednio ABW i SKW albo Kancelaria Prezesa Rady Ministrów;

2) Prezesa, Wiceprezesa i pracownika Najwyższej Izby Kontroli - wykonują odpowiednio Szef, zastępca Szefa i upoważniony funkcjonariusz ABW oraz Szef, zastępca Szefa i upoważniony funkcjonariusz lub żołnierz SKW albo Prezes Rady Ministrów lub upoważniony pracownik Kancelarii Prezesa Rady Ministrów.

5. *Czynności, o których mowa w ust. 1 pkt 1-5 i 8, dokonywane przez ABW w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej są wykonywane w uzgodnieniu odpowiednio z Marszałkiem Sejmu, Marszałkiem Senatu oraz Szefem Kancelarii Prezydenta Rzeczypospolitej Polskiej. Uzgodnienia dokonuje Prezes Rady Ministrów, a w przypadku braku uzgodnienia czynność nie może być wykonana.*
6. *Prezes Rady Ministrów określi, w drodze rozporządzenia:*

   1) sposób przygotowania oraz zakres i tryb przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych;

   2) tryb uzgadniania terminu kontroli, w tym czynności, o których mowa w ust. 1 pkt 1-5 i 8, wykonywanych w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej;

   3) zadania funkcjonariuszy ABW oraz funkcjonariuszy lub żołnierzy SKW nadzorujących i wykonujących czynności kontrolne;

   4) sposób dokumentowania czynności kontrolnych oraz sporządzania protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach kontroli.
7. *W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni potrzebę zapewnienia, aby zakres i sposób prowadzenia kontroli umożliwiał sprawne i obiektywne ustalenie stanu faktycznego zabezpieczenia informacji niejawnych w kontrolowanej jednostce organizacyjnej oraz jego rzetelne udokumentowanie.*

Niezwykle istotną zmianą jest nadanie ABW i SKW uprawnień do kontroli systemów teleinformatycznych nieposiadających akredytacji, choć możliwość taka została ograniczona tylko do przypadków prawdopodobieństwa, iż przetwarzane są w nich informacje niejawne (art. 12 ust. 2).

W art. 12 ust. 3 uregulowano kwestię związaną z kontrolą postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego. Całkowicie nowym rozwiązaniem jest poddanie postępowań prowadzonych przez ABW oraz SKW kontroli Prezesa Rady Ministrów. Dotychczas postępowania te pozostawały poza kontrolą podmiotów zewnętrznych (poza przypadkami podlegającymi postępowaniu odwoławczemu). Bez zmian pozostawiono uprawnienia ABW i SKW do kontroli postępowań realizowanych przez pełnomocników ochrony pozostałych jednostek organizacyjnych. Z przedmiotowej kontroli, realizowanej przez podmioty zewnętrzne, wyłączono postępowania prowadzone przez AW, CBA, BOR, Policję, Służbę Więzienną, SWW, SG, ŻW.

Wśród wymienionych w art. 12 ust. 4 ustawy przepisów o Najwyższej Izbie Kontroli[6], które mają zastosowanie przy realizacji czynności kontrolnych prowa-

[6] Dz.U. z 2007 r., Nr 231, poz. 1701 z późn. zm.

dzonych przez ABW, SKW oraz Prezesa Rady Ministrów, szczególną uwagę zwraca dodanie art. 98 ustawy o NIK, określającego odpowiedzialność karną za uchylanie się od kontroli, utrudnianie jej prowadzenia, bądź wprowadzanie w błąd co do wykonania wniosków pokontrolnych.

Bez zmian pozostawiono określenie odpowiedzialności kierownika jednostki organizacyjnej za ochronę informacji niejawnych oraz pełnomocnika ochrony za zapewnienie przestrzegania przepisów o ich ochronie. Doprecyzowano natomiast, że pełnomocnik ochrony jest zatrudniony przez kierownika jednostki (art. 14 ust. 2). Definicję zatrudnienia zawarto w art. 2 pkt 18 ustawy (słowniczek).

18) zatrudnieniem - jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

W art. 14 ust. 3 określono kryteria, jakie powinien spełniać pełnomocnik ochrony. Nowością jest wprowadzenie obowiązku posiadania przez niego wyższego wykształcenia (obowiązek ten dotyczy tylko pełnomocników zatrudnionych po wejściu w życie przepisów nowej ustawy). Ponadto uściślono, że powinien on posiadać zaświadczenie o stosownym przeszkoleniu przeprowadzonym przez ABW, SKW lub WSI (z uwagi na 5-letni okres ważności takiego zaświadczenia nie wpisano w tym miejscu Urzędu Ochrony Państwa, który został zlikwidowany 29.06.2002 r.).

3. Pełnomocnikiem ochrony może być osoba, która posiada:

1) obywatelstwo polskie;

2) wykształcenie wyższe;

3) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne;

4) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Doprecyzowano także budzący pewne wątpliwości dotychczasowy zapis (art. 18 ust. 2a poprzedniej ustawy) dotyczący powołania zastępcy pełnomocnika ochrony, w którym użyto liczby pojedynczej, co mogło wskazywać, że w jednostce organizacyjnej można powołać tylko jedną osobę na to stanowisko. Obecny zapis (art. 14 ust. 4) stanowi, iż kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony.

> *4. Kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony, z zastrzeżeniem spełnienia przez te osoby warunków, o których mowa w ust. 3.*

Nowym rozwiązaniem (art. 14 ust. 5) jest obowiązek określenia przez kierownika jednostki organizacyjnej szczegółowego zakresu czynności realizowanych przez zastępcę pełnomocnika ochrony.

> *5. Szczegółowy zakres czynności zastępcy pełnomocnika ochrony określa kierownik jednostki organizacyjnej.*

Uwagę zwraca zmiana polegająca na nałożeniu szczegółowych zadań związanych z ochroną informacji niejawnych w jednostce na pełnomocnika ochrony, a nie jak do tej pory (art. 18 ust. 4 poprzedniej ustawy) na pion ochrony. Projektodawcy kierowali się przede wszystkim potrzebą jasnego określenia indywidualnej odpowiedzialności za ochronę informacji niejawnych na poziomie podmiotów ustawy. Uznano także, iż nie w każdej jednostce organizacyjnej, w której przetwarzane są informacje niejawne, poza pełnomocnikiem ochrony musi być powołany także pion ochrony. W zakresie obowiązków pełnomocnika, w porównaniu do dotychczas obowiązujących przepisów, dokonano następujących zmian:

- wprowadzono zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie tego ryzyka (pojęcia te związane są z bezpieczeństwem teleinformatycznym; w przypadku środków bezpieczeństwa fizycznego obowiązuje określanie poziomu zagrożeń),
- doprecyzowano zapis dotyczący przeprowadzania okresowych kontroli ewidencji, materiałów i obiegu dokumentów poprzez wskazanie częstotliwości dokonywania tych czynności – tj. co najmniej raz na trzy lata,
- włączono zawarty w poprzedniej ustawie w innym rozdziale obowiązek prowadzenia przez pełnomocnika ochrony wykazu osób posiadających w jednostce organizacyjnej dostęp do informacji niejawnych oraz wykazu osób, którym cofnięto lub odmówiono wydania poświadczenia bezpieczeństwa oraz przekazywania tych danych do ewidencji ABW lub SKW. Wskazano przy tym szczegółowe dane (mniejszy zakres niż dotychczas), jakie taki wykaz powinien zawierać. Jednocześnie zrezygnowano z obowiązku sporządzania przez pełnomocnika ochrony wykazu stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych (art. 15 ust. 1).

Art. 15.

1. Do zadań pełnomocnika ochrony należy:

1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;

2) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;

3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;

4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;

5) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;

6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;

7) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;

8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto, obejmującego wyłącznie:

a) imię i nazwisko,

b) numer PESEL,

c) imię ojca,

d) datę i miejsce urodzenia,

e) adres miejsca zamieszkania lub pobytu,

f) określenie dokumentu kończącego procedurę, datę jego wydania oraz numer;

9) przekazywanie odpowiednio ABW lub SKW do ewidencji, o których mowa w art. 73 ust. 1, danych, o których mowa w art. 73 ust. 2, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt 8.

Pełnomocnika ochrony zwolniono także z obowiązku sporządzania odrębnego planu postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego (art. 18 ust. 8 poprzedniej ustawy). Stosowne procedury powinny być zawarte w planie ochrony informacji niejawnych i dotyczyć wszystkich informacji niejawnych pozostających w dyspozycji jednostki organizacyjnej.

Art. 10.

1. *ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ust. 2 i 3:*

   1) prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;

   2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;

   3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;

   4) zapewniają ochronę informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;

   5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

Przepisy dotyczące szkoleń w zakresie ochrony informacji niejawnych

Dopuszczenie do pracy lub służby związanej z dostępem do informacji niejawnych poprzedza odbycie stosownego szkolenia w zakresie ochrony tego typu informacji, któremu poświecono odrębny rozdział – czwarty – *Szkolenie w zakresie ochrony informacji niejawnych.* W art. 19 ust. 1 określono przedmiotowy zakres tego szkolenia. Zrezygnowano z części dotyczącej zagrożeń ze strony obcych służb specjalnych i organizacji terrorystycznych. Zdjęto w ten sposób obowiązek przeprowadzania tego typu szkoleń z pełnomocników ochrony, którzy nie dysponują odpowiednim przygotowaniem merytorycznym. Wprowadzono natomiast wymóg przeszkolenia inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu teleinformatycznego w zakresie zarządzania ryzykiem bezpieczeństwa informacji niejawnych, ze szczególnym uwzględnieniem szacowania ryzyka (art. 52 ust. 4 ustawy).

Art. 19.

1. *Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:*

   1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;

   2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka;

   3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.

W art. 19 ust. 2 ustawy określono natomiast zakres podmiotowy szkolenia. Zrezygnowano z obowiązku szkolenia szerokiego katalogu osób wymienionych w art. 27 ust. 3-8 poprzedniej ustawy. W zamian wprowadzono szkolenia prowadzone przez ABW lub SKW (wspólnie z pełnomocnikiem ochrony) dla kierowników jednostek organizacyjnych, ale tylko tych, w których przetwarzane są informacje niejawne o klauzulach „ściśle tajne" i „tajne". Dodatkowo w pkt 4. wskazano wprost ABW jako służbę właściwą do przeprowadzania szkoleń dla posłów i senatorów. Ustanowiono także nowy katalog osób szkolonych przez ABW lub SKW: są to przedsiębiorcy wykonujący działalność jednoosobowo oraz kierownicy przedsiębiorców, u których nie zatrudniono pełnomocnika ochrony (definicje wyżej wymienionych osób zawarto w art. 2 ustawy). Bez zmian pozostawiono obowiązek szkolenia przez ABW i SKW pełnomocników ochrony i ich zastępców, a także kandydatów na te stanowiska, oraz zapis dotyczący szkolenia przez pełnomocników ochrony pozostałych osób zatrudnionych w jednostce.

2. Szkolenie, o którym mowa w ust. 1:

1) przeprowadzają odpowiednio ABW lub SKW - dla pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska, przedsiębiorców wykonujących działalność jednoosobowo, a także dla kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony;

2) przeprowadzają odpowiednio ABW lub SKW, wspólnie z pełnomocnikiem ochrony - dla kierownika jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „ściśle tajne" lub „tajne";

3) organizuje pełnomocnik ochrony - dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej;

4) przeprowadza ABW - dla posłów i senatorów.

ABW i SKW przeprowadzają szkolenia w zakresie ochrony informacji niejawnych dla pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska, dla przedsiębiorców wykonujących działalność jednoosobowo (o czym mowa była wyżej), a także dla kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony. Natomiast pełnomocnik ochrony organizuje takie szkolenia dla osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej. Przy czym nie musi on osobiście prowadzić takiego szkolenia, omówienie niektórych zagadnień może zlecać osobom z odpowiednim wykształceniem i doświadczeniem (np. radcom prawnym). Musi jedynie podpisać się na zaświadczeniu, którego wzór został określony w rozporządzeniu Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. (Dz. U. Nr 258, poz. 1751) i odebrać oświadczenie, o którym mowa w art. 20 ust. 1 ustawy, tj. o zapoznaniu się z przepisami o ochronie informacji niejawnych.

W art. 19 ust. 4 i 5 uregulowano kwestię ponoszenia kosztów szkolenia z zakresu ochrony informacji niejawnych przez jednostki organizacyjne. Koszty szkolenia prowadzonego przez ABW lub SKW pokrywa jednostka organizacyj-

na, w której osoba szkolona jest zatrudniona bądź pełni służbę. Z obowiązku zwrotu kosztów wyłączono jedynie jednostki podległe Ministrowi Obrony Narodowej i przez niego nadzorowane, Policję oraz posłów i senatorów. Zmiany w projekcie przewidujące te wyłączenia zostały wprowadzone na etapie uzgodnień międzyresortowych.

> 4. *Koszty szkolenia przeprowadzonego przez ABW albo SKW, z wyłączeniem szkolenia, o którym mowa w ust. 2 pkt 4, oraz z zastrzeżeniem ust. 5, pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.*
>
> 5. *Jednostki organizacyjne, o których mowa w art. 1 ust. 2 pkt 2, oraz Policja nie pokrywają kosztów szkoleń przeprowadzonych przez ABW albo SKW.*

W ustawie zrezygnowano z zapisu dotyczącego instytucji *szkolenia uzupełniającego*, prowadzonego dotychczas dla pełnomocników ochrony i ich zastępców. Ujednolicono w ten sposób terminologię, ograniczając się do szkolenia w zakresie ochrony informacji niejawnych. Jednocześnie pozostawiono wymóg odbywania szkoleń w przedmiotowym zakresie nie rzadziej niż raz na 5 lat, obligując do tego wszystkie osoby posiadające dostęp do informacji niejawnych (dotychczas wymóg ten dotyczył wyłącznie pełnomocników ochrony i ich zastępców). Wskazano także wprost na uznawalność zaświadczeń o odbytym przeszkoleniu, uzyskanych od innego organu uprawnionego, z zachowaniem 5-letniego okresu ważności tego zaświadczenia.

W art. 19 ust. 6 do umowy dotyczącej szkolenia wprowadzono trzecią stronę – jednostkę organizacyjną, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.

> 6. *Wzajemne prawa i obowiązki podmiotu przeprowadzającego szkolenie, uczestnika szkolenia, o którym mowa w ust. 2 pkt 1 i 2, oraz jednostki organizacyjnej, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone, określa umowa zawarta między tym podmiotem, uczestnikiem szkolenia oraz jednostką organizacyjną.*

Dodano także obowiązek składania przez osoby przeszkolone pisemnych oświadczeń o zapoznaniu się z przepisami o ochronie informacji niejawnych (art. 20 ust. 1). Dotychczas taki obowiązek spoczywał jedynie na osobach, wobec których nie prowadzono postępowań sprawdzających.

Nowością jest określenie w akcie prawnym na poziomie ustawy górnej granicy kosztów szkolenia[7].

[7] Art. 20. 3.: W rozporządzeniu, o którym mowa w ust. 2, Prezes Rady Ministrów uwzględni odrębności wynikające z wydawania zaświadczeń przez ABW i SKW oraz pełnomocników ochrony oraz sposób ustalania kosztów na potrzeby ich rozliczania w ten sposób, że ich wysokość nie może przekroczyć 25% przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 *Ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich* (Dz.U. z 1998 r., Nr 108, poz. 685 z późn. zm.).

Art. 20.

1. Szkolenie, o którym mowa w art. 19 ust. 1, kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

Przepisy dotyczące bezpieczeństwa osobowego

Przepisy ustawy regulujące kwestie związane z bezpieczeństwem osobowym, tj. z zasadami upoważniania osób do dostępu do informacji niejawnych, w szczególności z prowadzeniem postępowań sprawdzających, zawarto w rozdziale 5 – *Bezpieczeństwo osobowe*. Zgodnie z przyjętym założeniem każdemu ze związanych tematycznie i funkcjonalnie z bezpieczeństwem osobowym zagadnień poświęcono osobną jednostkę redakcyjną. Spowodowało to, iż niektóre z artykułów są dużo obszerniejsze niż w poprzedniej ustawie. Merytoryczny zakres zmian nie jest natomiast co do swej istoty szeroki, ponieważ intencją ustawodawcy była przede wszystkim próba uporządkowania oraz sprecyzowania nie do końca jednoznacznych dotychczas przepisów.

Należy jeszcze raz zwrócić uwagę na fakt, iż niektóre kwestie związane z bezpieczeństwem osobowym – z uwagi na zasady techniki legislacyjnej (jako przepisy ogólne lub odrębne) – w rozdziale tym nie zostały ujęte. I tak np. kluczowa dla bezpieczeństwa osobowego definicja dawania rękojmi zachowania tajemnicy znajduje się w „słowniczku", a zasada *need-to-know*, zastrzegająca, że osoba posiadająca poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o określonej klauzuli tajności nie może posiadać „z urzędu" lub domagać się dostępu do każdej informacji o takiej bądź niższej klauzuli, ale tylko do tych informacji, które mają związek z wykonywanymi przez tę osobę obowiązkami służbowymi – w art. 4 ust. 1 (poprzednio w art. 3).

Szczególnie istotne znaczenie, o czym wspomniane było wcześniej, ma rozstrzygnięcie zawarte w art. 11 ustawy, zgodnie z którym Szef Agencji Bezpieczeństwa Wewnętrznego pełni funkcję krajowej władzy bezpieczeństwa.

Art. 11.

1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Jak wskazano, ustawodawca tak skonstruował przepisy rozdziału 5 art. 21- 34) omawianej ustawy, że każda jednostka redakcyjna stanowi wyczerpujący opis odrębnego zagadnienia. I tak, art. 21 określa ogólne warunki dostępu do informacji niejawnych, dotychczas opisane w kilku artykułach różnych rozdziałów. W stosunku do poprzednio obowiązujących rozwiązań zniesiono obowiązek posiadania poświadczenia

bezpieczeństwa (a tym samym prowadzenia postępowań sprawdzających) w przypadku ubiegania się o dostęp do informacji niejawnych o klauzuli „zastrzeżone" (a więc także adekwatnych im klauzulą informacji niejawnych organizacji międzynarodowych). Dostęp do tego typu informacji będzie następował na podstawie pisemnego upoważnienia kierownika jednostki organizacyjnej (jeżeli osoba nie będzie posiadać wydanego wcześniej poświadczenia bezpieczeństwa) oraz po przeszkoleniu w zakresie ochrony informacji niejawnych (art. 21 ust. 4).

4. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po:

1) pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa;

2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

Z katalogu okoliczności wyłączających dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne" (a także adekwatnych im klauzulą informacji niejawnych organizacji międzynarodowych) usunięto ukaranie prawomocnym wyrokiem za przestępstwa umyślne ścigane z oskarżenia publicznego, także popełnione za granicą. W nowej ustawie jest to przesłanka do odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa, ale tylko przy jednoczesnym wystąpieniu dwóch warunków – orzeczenia kary pozbawienia wolności oraz gdy czyn, za który nastąpiło skazanie, wywołuje ustawowe wątpliwości związane z oceną dawania rękojmi zachowania tajemnicy.

Ustawa wprowadza dwa (w miejsce dotychczasowych trzech) rodzaje postępowań sprawdzających (art. 22).

Art. 22.

1. W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej „osobą sprawdzaną", przeprowadza się:

1) zwykłe postępowanie sprawdzające - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne", z zastrzeżeniem pkt 2 lit. b-d;

2) poszerzone postępowanie sprawdzające:

a) przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne",

b) wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska,

c) wobec kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej,

d) wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską.

> 2. *Osobom wskazanym w ust. 1 pkt 2 lit. b-d wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana we wniosku lub poleceniu.*

W stosunku do poprzednio obowiązujących rozwiązań zniesiono instytucję specjalnych postępowań sprawdzających. Według generalnej zasady, w przypadku ubiegania się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli „poufne" będzie prowadzone zwykłe postępowanie sprawdzające, a w pozostałych przypadkach – tj. w przypadku ubiegania się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" oraz adekwatnych im klauzulą, np. *„Secret UE/EU secret", „Très secret UE/EU top secret", „NATO Secret", „Cosmic Top Secret"*, informacji niejawnych organizacji międzynarodowych – postępowanie poszerzone. Ponadto, postępowania poszerzone będą również prowadzone w przypadku kierowników jednostek organizacyjnych, pełnomocników ochrony, zastępców pełnomocników ochrony i kandydatów na te stanowiska oraz wobec osób ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych (wobec pełnomocników ochrony i ich zastępców oraz kandydatów na te stanowiska – także w przypadku konieczności uzyskania dostępu do informacji niejawnych jedynie o klauzuli „zastrzeżone"), jak również wobec osób ubiegających się o wydanie poświadczenia bezpieczeństwa organizacji międzynarodowej, upoważniającego do dostępu do informacji niejawnych o klauzuli adekwatnej do klauzuli „poufne", a więc np. *„Confidentiel UE/EU confidential" czy „NATO Confidential"*. W przypadku, gdy osoby te będą ubiegać się jedynie o dostęp do informacji niejawnych o klauzuli „poufne" i/lub adekwatnych im klauzulą (np. *„Confidentiel UE/EU confidential"* czy *„NATO Confidential"*), informacji niejawnych organizacji międzynarodowych – po przeprowadzeniu postępowania poszerzonego będzie wydawane poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych jedynie o klauzuli „poufne" lub *„Confidentiel UE/EU confidential"* czy *„NATO Confidential"*.

W art. 23 określono z kolei właściwość organów do prowadzenia postępowań sprawdzających[8]. W stosunku do poprzednio obowiązujących rozwiązań doprecyzowano, że ABW i SKW oraz inne służby upoważnione do prowadzenia postępowań wobec własnych pracowników prowadzą również postępowania wobec osób, które wykonują na ich rzecz czynności zlecone lub ubiegają się o wykonywanie takich czynności. Najistotniejszą zmianą merytoryczną w zakresie właściwo-

[8] W zależności od rodzaju postępowania: ogólna właściwość ABW i SKW w zakresie ochrony informacji niejawnych opisana jest w art. 10 ustawy, zaś uprawnienie tylko tych służb do prowadzenia postępowań przed wydaniem poświadczeń bezpieczeństwa organizacji międzynarodowych – w art. 11.

ści organów do prowadzenia postępowań sprawdzających jest upoważnienie Biura Ochrony Rządu do prowadzenia „samodzielnych" postępowań sprawdzających (tj. wobec własnych pracowników lub funkcjonariuszy oraz kandydatów do zatrudnienia lub podjęcia służby), a także upoważnienie ABW do prowadzenia postępowań sprawdzających wobec Szefów SKW, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Biura Ochrony Rządu, Komendantów Głównych Policji i Straży Granicznej oraz Dyrektora Generalnego Służby Więziennej oraz kandydatów na te stanowiska. Szef SKW został natomiast uprawniony do prowadzenia postępowań wobec Szefa ABW, Służby Wywiadu Wojskowego oraz Komendanta Głównego Żandarmerii Wojskowej, jak również kandydatów na te stanowiska. Taki zapis oznacza praktyczną realizację zasady wyłączenia pracownika organu od udziału w sprawie, w której jedną ze stron jest osoba pozostająca wobec niego w stosunku nadrzędności służbowej (art. 24 § 1 pkt 7 kpa). Podobnie jest w przypadku uprawnienia ABW i SKW do realizacji postępowań sprawdzających wobec kierowników jednostek organizacyjnych, nawet gdy ubiegają się oni o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych jedynie o klauzuli „poufne".

Art. 23.

1. *Pełnomocnik ochrony przeprowadza zwykłe postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej.*
2. *ABW albo SKW przeprowadzają poszerzone postępowania sprawdzające:*

   1) na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenia prac;

   2) wobec funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w ABW albo SKW;

   3) wobec osób wykonujących czynności zlecone lub ubiegających się o wykonywanie tych czynności na rzecz ABW albo SKW.
3. *ABW przeprowadza poszerzone postępowania sprawdzające wobec:*

   1) Szefa SKW, Szefa Agencji Wywiadu, zwanej dalej „AW", Szefa CBA, Szefa Biura Ochrony Rządu, Komendanta Głównego Policji, Dyrektora Generalnego Służby Więziennej, Komendanta Głównego Straży Granicznej oraz osób przewidzianych na te stanowiska;

   2) pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w SKW, AW, CBA, Biurze Ochrony Rządu, Policji, Służbie Więziennej oraz Straży Granicznej.
4. *SKW przeprowadza poszerzone postępowania sprawdzające wobec:*

   1) Szefa ABW, Szefa Służby Wywiadu Wojskowego, zwanej dalej „SWW", Komendanta Głównego Żandarmerii Wojskowej oraz osób przewidzianych na te stanowiska;

   2) pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w ABW, SWW oraz Żandarmerii Wojskowej.
5. *AW, CBA, Biuro Ochrony Rządu, Policja, Służba Więzienna, SWW, Straż Graniczna oraz Żandarmeria Wojskowa przeprowadzają samodzielnie postępowania sprawdzające oraz kontrolne postępowania sprawdzające odpowiednio wobec:*

1) własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy,

2) osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności

- z zastrzeżeniem ust. 3 i 4.

6. W zakresie postępowań sprawdzających oraz kontrolnych postępowań sprawdzających przeprowadzanych przez służby i instytucje, o których mowa w ust. 5, przysługują tym służbom i instytucjom uprawnienia ABW oraz SKW.

W przypadku pełnomocników ochrony w SKW, AW, CBA, BOR, SG, SW i w Policji, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska, przeprowadzenie postępowania sprawdzającego pozostaje we właściwości ABW, a wobec tej samej kategorii osób w ABW, SWW i ŻW – we właściwości SKW.

W art. 24 określono zasady prowadzenia postępowań sprawdzających. W stosunku do poprzednio obowiązujących rozwiązań poszczególne kategorie wątpliwości ustalane w toku postępowania pogrupowano hierarchicznie, zaczynając od zagrożenia najpoważniejszego dla bezpieczeństwa państwa, tj. prowadzenia działalności szpiegowskiej bądź terrorystycznej, poprzez zagrożenia ze strony obcych służb specjalnych w postaci prób dokonywania werbunku, aż po członkostwo w organizacjach ekstremistycznych.

Art. 24.

1. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

2. W toku postępowania sprawdzającego ustala się, czy istnieją uzasadnione wątpliwości dotyczące:

1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej;

2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu;

3) przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, albo współpracowała lub współpracuje z takimi partiami lub organizacjami;

4) ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego, zwanej dalej „ankietą", lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych;

5) wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;

6) niewłaściwego postępowania z informacjami niejawnymi, jeżeli:

a) doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym,

b) było to wynikiem celowego działania,

c) stwarzało to realne zagrożenie ich nieuprawnionym ujawnieniem i nie miało charakteru incydentalnego,

d) dopuściła się tego osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej.

3. W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące:

1) poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody;

2) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac, związanych z dostępem do informacji niejawnych;

3) uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

4. W razie niedających się usunąć wątpliwości, o których mowa w ust. 2 lub 3, interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami.

5. Organ prowadzący postępowanie sprawdzające, kierując się zasadami bezstronności i obiektywizmu, jest obowiązany do wykazania najwyższej staranności w toku prowadzonego postępowania sprawdzającego co do jego zgodności z przepisami ustawy.

6. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 3 miesięcy od dnia:

1) złożenia do pełnomocnika ochrony wypełnionej ankiety, lub

2) złożenia wniosku o przeprowadzenie postępowania sprawdzającego wraz z wypełnioną ankietą.

7. W przypadku niedotrzymania terminu, o którym mowa w ust. 6, organ prowadzący postępowanie informuje, na wniosek osoby sprawdzanej, o przewidywanym terminie zakończenia postępowania oraz - jeżeli nie naruszy to zasad ochrony informacji niejawnych - o powodach przedłużania się postępowania.

8. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć.

9. Zbieranie i przetwarzanie informacji o osobach trzecich, określonych w ankiecie, może odbywać się bez wiedzy i zgody tych osób, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Informacje o osobach trzecich mogą być zbierane i przetwarzane wyłącznie w zakresie określonym w ust. 2.

10. Ankieta po wypełnieniu stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego. Wzór ankiety wraz z instrukcją jej wypełnienia stanowi załącznik do ustawy.

Występującą wcześniej w jednym przepisie wątpliwość związaną z podawaniem w postępowaniu sprawdzającym nieprawdziwych informacji oraz z występowaniem okoliczności powodujących ryzyko podatności na szantaż lub wywieranie presji podzielono na dwie przesłanki. W praktyce realizacji postępowań bardzo często zdarzało się, że podatność na szantaż lub presję była podstawą do wydania decyzji o odmowie wydania poświadczenia bezpieczeństwa, bez związku z podawaniem w toku postępowania nieprawdziwych informacji. Takie przypadki mają

miejsce np. wtedy, gdy osoba sprawdzana wpada w spiralę zadłużenia (nie jest w stanie na bieżąco regulować zobowiązań finansowych, ponieważ jej miesięczne dochody są niższe od miesięcznych rat tych zobowiązań), albo gdy przedstawia jej się zarzut popełnienia przestępstwa np. o charakterze korupcyjnym.

Istotną zmianą jest sprecyzowanie, jakiego typu postępowanie osoby sprawdzanej z informacjami niejawnymi wywołuje niedające się usunąć wątpliwości (art. 24 ust. 2 pkt 6). Dotychczasowy przepis był na tyle ogólny, że za niewłaściwe postępowanie z informacjami niejawnymi można było uznać choćby jednokrotne naruszenie formalnych przepisów dotyczących ochrony informacji niejawnych. W przyjętym obecnie rozwiązaniu, aby można było stwierdzić występowanie wątpliwości dotyczących właściwego postępowania osoby sprawdzanej z informacjami niejawnymi, niezbędne jest spełnienie co najmniej jednego z czterech poniższych warunków: 1) bezpośrednie doprowadzenie do ujawnienia tych informacji osobom nieuprawnionym; 2) celowe działanie; 3) stworzenie realnego zagrożenia ich nieuprawnionego ujawnienia i nieincydentalny charakter; 4) dopuszczenie się nieuprawnionego ujawnienia informacji niejawnych przez osobę szczególnie zobowiązaną na podstawie ustawy do ochrony informacji niejawnych, tj. przez pełnomocnika ochrony, jego zastępcę lub kierownika kancelarii tajnej. Nowe rozwiązanie w większym stopniu gwarantuje osobom sprawdzanym, że ocena ich niewłaściwego postępowania z informacjami niejawnymi będzie dokonywana przez organ prowadzący postępowanie w oparciu o rzeczywisty wpływ uchybień na ochronę informacji niejawnych, a nie na podstawie formalnego naruszania tego typu przepisów. Nie oznacza to jednak, że formalne naruszanie przepisów nie będzie mogło w takim przypadku stanowić podstawy do odmowy wydania poświadczenia bezpieczeństwa. Jednakże będzie mogło do tego dojść dopiero wówczas, gdy dopuści się go osoba szczególnie zobowiązana do ochrony informacji niejawnych na podstawie ustawy (przy ocenie tego typu przypadków powinna być brana pod uwagę skala naruszeń).

Zastąpiono również nieprecyzyjny dotychczas zapis odnośnie ustalania w toku postępowania wątpliwości związanych z uzależnieniem od narkotyków na semantycznie szerszy – dotyczący ustalania wątpliwości związanych z uzależnieniem od alkoholu, środków odurzających lub substancji psychotropowych (art. 24 ust. 3 pkt 3).

Kolejną zmianą jest wprowadzenie jednego dla każdego rodzaju postępowań sprawdzających, trzymiesięcznego terminu ich realizacji, który nadal pozostaje terminem instrukcyjnym, co oznacza, że jego przekroczenie nie wywołuje skutków prawnych. Jednak przekroczenie terminu trzymiesięcznego musi być zawsze uzasadnione dobrem postępowania. Dodatkową gwarancją terminowej realizacji

postępowań sprawdzających jest wprowadzenie obowiązku – o ile zainteresowana osoba o to wystąpi – poinformowania jej przez organ prowadzący postępowanie o przyczynach niedotrzymania pierwotnego terminu oraz wskazania nowego (art. 24 ust. 7).

W art. 25 określono czynności podejmowane w toku zwykłych postępowań sprawdzających. W stosunku do poprzednio obowiązujących rozwiązań nastąpiły tu trzy fundamentalne zmiany. Pierwszą z nich jest ograniczenie obligatoryjnych sprawdzeń w ewidencjach, rejestrach i kartotekach (oprócz sprawdzenia w ewidencjach powszechnie niedostępnych, dokonywanego za pośrednictwem ABW lub SKW zgodnie z ich właściwością) do sprawdzenia tylko w Krajowym Rejestrze Karnym (dotychczas obowiązkowe było również sprawdzanie akt stanu cywilnego oraz dokonywanie sprawdzeń w Centralnym Zarządzie Służby Więziennej). Powyższe nie wyklucza dokonywania innych ustaleń, w tym w aktach stanu cywilnego oraz w CZSW, ale daje organowi prowadzącemu postępowanie większą swobodę w doborze czynności sprawdzających, które ten uzna za konieczne w ramach konkretnego postępowania.

Art. 25.

1. *Zwykłe postępowanie sprawdzające obejmuje:*

   1) sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy;

   2) sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

2. *Sprawdzenie, o którym mowa w ust. 1 pkt 2, jest prowadzone na pisemny wniosek pełnomocnika ochrony przez ABW albo SKW.*

3. *W toku sprawdzenia, o którym mowa w ust. 1 pkt 2, ABW albo SKW ma prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach.*

4. *ABW albo SKW przekazuje pełnomocnikowi ochrony pisemną informację o wynikach czynności, o których mowa w ust. 1 pkt 2 oraz w ust. 3.*

5. *Jeżeli jest to konieczne w wyniku uzyskanych informacji, zwykłe postępowanie sprawdzające obejmuje ponadto rozmowę z osobą sprawdzaną.*

6. *Jeżeli w toku zwykłego postępowania sprawdzającego wystąpią wątpliwości niepozwalające na ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, organ prowadzący postępowanie sprawdzające zapewnia osobie sprawdzanej w trakcie wysłuchania możliwość osobistego ustosunkowania się do informacji wywołujących te wątpliwości. Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem. Z przebiegu wysłuchania sporządza się protokół, który podpisują osoba prowadząca wysłuchanie, osoba wysłuchana oraz pełnomocnik, jeżeli w nim uczestniczył.*

7. *Organ prowadzący zwykłe postępowanie sprawdzające odstępuje od przeprowadzenia czynności, o której mowa w ust. 6, jeżeli:*

1) jej przeprowadzenie wiązałoby się z ujawnieniem informacji niejawnych;

2) postępowanie sprawdzające doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

Druga zmiana dotyczy możliwości weryfikacji w ramach postępowania sprawdzającego nie tylko, jak to było dotychczas, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie bezpieczeństwa osobowego, ale także innych informacji uzyskanych w toku postępowania sprawdzającego, jednakże tylko tych, które organ prowadzący to postępowanie uzna za niezbędne do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

Trzecią zasadniczą zmianą jest wprowadzenie do postępowania zwykłego obowiązku zapewnienia osobie sprawdzanej możliwości osobistego ustosunkowania się – w trybie wysłuchania – do informacji wywołujących wątpliwości niepozwalające na ustalenie, czy osoba ta daje rękojmię zachowania tajemnicy (dotychczas taka możliwość istniała tylko w przypadku postępowań poszerzonych i specjalnych). Dodano także obowiązek sporządzania protokołu z wysłuchania, który podpisują osoba wysłuchująca, osoba wysłuchiwana oraz jej pełnomocnik, jeżeli w wysłuchaniu uczestniczył. Od wysłuchania odstępuje się, jeśli miałoby ono doprowadzić do ujawnienia informacji niejawnych (wcześniej warunkiem odstąpienia od wysłuchania było tylko zagrożenie ujawnieniem osobie nieuprawnionej informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"), a zmiana w tym zakresie jest wynikiem zmiany definicji informacji niejawnych. Ponadto wprowadzono obowiązek odstąpienia od wysłuchania w sytuacji, gdy postępowanie doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

Jednocześnie upoważniono ABW i SKW do przekazywania pełnomocnikowi ochrony nie tylko informacji o wynikach sprawdzeń w ewidencjach powszechnie niedostępnych, ale także wyniku rozmowy z osobą sprawdzaną, jeżeli w toku postępowania prowadzonego przez pełnomocnika ABW lub SKW uznała ona, że przeprowadzenie takiej rozmowy jest konieczne.

W art. 26 zostały określone czynności podejmowane w toku poszerzonych postępowań sprawdzających. W stosunku do poprzednio obowiązujących rozwiązań wprowadzono możliwość bardziej elastycznego i racjonalnego, uwzględniającego z jednej strony zasadę rzetelnego dokumentowania, a z drugiej – zasadę ekonomiczności podejmowanych działań, doboru takiego zakresu podejmowanych czynności, jaki organ prowadzący postępowanie uzna w konkretnej sytuacji za niezbędny. Podobnie jak w przypadku postępowania zwykłego, obowiązkowe będzie

jedynie sprawdzenie w KRK oraz w ewidencjach powszechnie niedostępnych. Jeżeli organ uzna to za niezbędne (na podstawie uzyskanych wcześniej informacji), w toku postępowania poszerzonego będzie możliwe dokonywanie sprawdzeń w innych ewidencjach, rejestrach i kartotekach oraz przeprowadzenie rozmowy z osobą sprawdzaną lub – jeżeli jest to konieczne w związku z uzyskanymi informacjami – jej wysłuchanie.

Art. 26.

1. *Poszerzone postępowanie sprawdzające obejmuje czynności, o których mowa w art. 25 ust. 1, a ponadto, jeżeli jest to konieczne w wyniku uzyskanych informacji, postępowanie to obejmuje:*

   1) rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami;

   2) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej;

   3) sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa.

2. *Do czynności, o której mowa w ust. 1 pkt 2, przepisy ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego i wydane na jej podstawie przepisy dotyczące wywiadu środowiskowego stosuje się odpowiednio.*

3. *Czynności, o których mowa w ust. 1 pkt 3, są wykonywane zgodnie z art. 105 ust. 1 pkt 2 lit. k ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.9)). Przepisy art. 82 § 1 i 2, art. 182 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60, z późn. zm.10)) oraz art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65, z późn. zm.11)) stosuje się odpowiednio.*

4. *Do poszerzonego postępowania sprawdzającego przepisy art. 25 ust. 5-7 stosuje się odpowiednio.*

5. *W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli „ściśle tajne" poszerzone postępowanie sprawdzające obejmuje także, jeżeli jest to konieczne w wyniku uzyskanych wcześniej informacji, rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu uzyskania innych informacji mogących mieć znaczenie dla oceny dawania rękojmi zachowania tajemnicy.*

6. *W celu dokonania ustaleń, o których mowa w art. 24 ust. 3 pkt 2 i 3, organ prowadzący poszerzone postępowanie sprawdzające może zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań. Lekarzowi przeprowadzającemu to badanie udostępnia się dokumentację medyczną osoby sprawdzanej w zakresie dotyczącym wątpliwości, o których mowa w art. 24 ust. 3 pkt 2 i 3.*

W ramach postępowania poszerzonego nadal istnieje możliwość przeprowadzania rozmów z przełożonymi osoby sprawdzanej lub z innymi osobami, przeprowadzenia wywiadu w miejscu zamieszkania oraz sprawdzenia stanu i obrotów na rachunku bankowym osoby sprawdzanej oraz jej zadłużenia, w szczególności wobec Skarbu Państwa, jak również zobowiązania osoby sprawdzanej do poddania się specjalistycznym badaniom i udostępnienia wyników tych badań. W przypadku tej ostatniej czynności sprecyzowano, że lekarzowi przeprowadzającemu specjalistyczne badanie pod kątem stwierdzenia bądź wykluczenia choroby lub dolegli-

wości psychicznej albo uzależnienia od alkoholu, środków odurzających lub psychotropowych, może być udostępniona dokumentacja medyczna osoby sprawdzanej – oczywiście wyłącznie w zakresie dotyczącym wątpliwości, o których mowa w art. 24 ust. 3 pkt. 2 i 3 nowej ustawy.

Rozmowy z osobami polecającymi nie są – jak w poprzedniej ustawie – czynnością obligatoryjną. Przeprowadza się je bowiem *jeżeli jest to konieczne w wyniku uzyskanych informacji*. I tylko w przypadku, gdy osoba ubiega się o dostęp do informacji niejawnych o klauzuli „ściśle tajne" lub informacji niejawnych międzynarodowych o klauzuli odpowiedniej do klauzuli „ściśle tajne".

W nowej ustawie rozszerzono i doprecyzowano przepisy dotyczące instytucji zawieszenia postępowania sprawdzającego (art. 27). W stosunku do poprzednio obowiązujących rozwiązań do okoliczności umożliwiających zawieszenie postępowania dodano *brak możliwości przeprowadzenia skutecznego postępowania sprawdzającego z przyczyn niezależnych od organu je prowadzącego*[9]. Przepis ten można zastosować np. w sytuacji, gdy osoba objęta postępowaniem sprawdzającym odmawia kontaktu lub przekazania informacji organowi prowadzącemu postępowanie, ale formalnie nie cofa swojej zgody na jego przeprowadzenie. Z kolei dotychczasową podstawę do zawieszenia postępowania w postaci wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe uznano za szczególny przypadek sytuacji, gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia problemu przez inny organ (jest to nieco zmieniona formuła art. 97 § 1 pkt 4 kpa, mającego zastosowanie do postępowań sprawdzających). Ponadto sprecyzowano, że długotrwała choroba umożliwiająca zawieszenie postępowania to choroba dłuższa niż 30 dni.

Art. 27.

1. *Postępowanie sprawdzające może zostać zawieszone w przypadku:*

   1) trwającej powyżej 30 dni choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego;

   2) wyjazdu za granicę osoby sprawdzanej na okres przekraczający 30 dni;

   3) gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ, w szczególności w przypadku wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe;

   4) gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego.

[9] W brzemieniu poprzedniej ustawy obowiązującej od 1999 r. do nowelizacji w 2005 r., w art. 37 ust. 9, okoliczność taka stanowiła podstawę do odmowy wydania poświadczenia bezpieczeństwa.

> 2. *Zawieszone postępowanie sprawdzające zostaje podjęte, jeżeli:*
>
> *1) ustąpiły przyczyny uzasadniające zawieszenie postępowania;*
>
> *2) ujawniono okoliczności mogące stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego.*
>
> 3. *O zawieszeniu postępowania sprawdzającego oraz o jego podjęciu organ prowadzący postępowanie sprawdzające zawiadamia wnioskodawcę, pełnomocnika ochrony i osobę sprawdzaną.*
>
> 4. *Do zażalenia na postanowienie w sprawie zawieszenia postępowania sprawdzającego przepisy art. 35, art. 37 i art. 38 stosuje się odpowiednio.*

Do dotychczasowego obowiązku podjęcia przez organ prowadzący zawieszonego postępowania sprawdzającego (w przypadku ustąpienia przyczyn uzasadniających jego zawieszenie) wprowadzono dodatkowo możliwość podjęcia tego typu postępowania, gdy ujawniono okoliczności mogące stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego. Tak więc na przykład w sytuacji, gdy wnioskodawca postępowania wystąpi w stosunku do osoby sprawdzanej, wobec której prowadzone postępowanie sprawdzające zostało zawieszone z uwagi na przedstawienie jej zarzutów popełnienia przestępstwa o charakterze korupcyjnym, o umorzenie tego postępowania z uwagi na rezygnację z zamiaru obsadzenia tej osoby na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych, postępowanie takie będzie można umorzyć (oczywiście po jego uprzednim podjęciu).

Ponadto, na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego zawieszeniu oraz podjęciu nie tylko osoby sprawdzanej i wnioskodawcy, ale również pełnomocnika ochrony (o ile to sam pełnomocnik ochrony nie jest organem, który prowadzi to postępowanie).

Z punktu widzenia osób objętych postępowaniami niezwykle istotne jest sprecyzowanie trybu składania zażaleń na postanowienia o zawieszeniu i podjęciu zawieszonego postępowania sprawdzającego, które ma się odbywać według zasad właściwych dla odwołań od decyzji kończących postępowanie (o czym mowa będzie dalej). Dotychczas obowiązujące rozwiązanie przewidywało co prawda – – na podstawie ogólnego zapisu w art. 101 § 3 kpa – możliwość złożenia zażalenia na postanowienie o zawieszeniu postępowania, ale nie precyzowało, do kogo należy takie zażalenie składać.

W art. 28 ustawy określono formy zakończenia postępowania sprawdzającego. W stosunku do poprzednio obowiązujących rozwiązań uściślono, że efektem kończącym postępowanie sprawdzające jest nie tylko otrzymanie poświadczenia bezpieczeństwa lub decyzja o odmowie jego wydania, ale również decyzja o umorzeniu postępowania.

Art. 28.

Postępowanie sprawdzające kończy się:

1) wydaniem poświadczenia bezpieczeństwa;

2) odmową wydania poświadczenia bezpieczeństwa;

3) umorzeniem.

Poważne zmiany wprowadzono w przepisie dotyczącym poświadczeń bezpieczeństwa, w tym w szczególności okresów ważności oraz trybu i zasad ich wydawania i przekazywania (art. 29). W stosunku do poprzednio obowiązujących rozwiązań wskazano wprost, że poświadczenia bezpieczeństwa wydane w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5 (czyli przez AW, SWW, CBA, Policję, ŻW, SG, SW oraz BOR), zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.

Art. 29.

1. *Po zakończeniu postępowania sprawdzającego z wynikiem pozytywnym organ prowadzący postępowanie wydaje poświadczenie bezpieczeństwa i przekazuje osobie sprawdzanej, zawiadamiając o tym wnioskodawcę.*
2. *Poświadczenie bezpieczeństwa powinno zawierać:*

   1) numer poświadczenia;

   2) podstawę prawną;

   3) wskazanie wnioskodawcy postępowania sprawdzającego;

   4) określenie organu, który przeprowadził postępowanie sprawdzające;

   5) datę i miejsce wystawienia;

   6) imię, nazwisko i datę urodzenia osoby sprawdzanej;

   7) określenie rodzaju przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp;

   8) stwierdzenie, że osoba sprawdzana daje rękojmię zachowania tajemnicy;

   9) termin ważności;

   10) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.
3. *Poświadczenie bezpieczeństwa wydaje się na okres:*

   1) 10 lat - w przypadku dostępu do informacji niejawnych o klauzuli „poufne";

   2) 7 lat - w przypadku dostępu do informacji niejawnych o klauzuli „tajne";

   3) 5 lat - w przypadku dostępu do informacji niejawnych o klauzuli „ściśle tajne".
4. *Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności, odpowiednio przez okresy, o których mowa w ust. 3, także w odniesieniu do poświadczeń bezpieczeństwa organizacji międzynarodowych.*

5. *Poświadczenia bezpieczeństwa wydane w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5, zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.*
6. *Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory:*
   1) poświadczenia bezpieczeństwa;
   2) poświadczeń bezpieczeństwa organizacji międzynarodowych.
7. *W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni we wzorach poświadczeń bezpieczeństwa dane określone w ust. 2 oraz zapewni zróżnicowanie wzorów poświadczeń bezpieczeństwa wydawanych przez ABW, SKW, służby i instytucje określone w art. 23 ust. 5 oraz pełnomocników ochrony.*

Do tej samej kwestii nawiązuje również art. 34 ust. 1 nowej ustawy, zgodnie z którym *Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5.*

Art. 34.

1. *Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5.*

Bardzo ważną zmianą, której wprowadzenie poprzedzono konsultacjami z instytucjami odpowiedzialnymi w UE i NATO za ochronę informacji niejawnych, jest wdrożenie zasady „kaskadowej" ważności poświadczeń bezpieczeństwa, upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych. Zasada ta stosowana była dotychczas (choć dopiero od nowelizacji z 2005 roku) tylko w odniesieniu do poświadczeń upoważniających do dostępu do „krajowych" informacji niejawnych. Tak więc obecnie poświadczenie bezpieczeństwa, które będzie upoważniało do dostępu do informacji niejawnych o klauzuli *„Cosmic Top Secret"* na okres 5 lat, będzie jednocześnie upoważniało jego posiadacza do dostępu do informacji niejawnych o klauzuli *„NATO Secret"* przez kolejne 2 lata (tj. 7 lat od wydania poświadczenia), a o klauzuli *„NATO Confidential"* – przez kolejne 3 lata (10 lat od wydania poświadczenia). Podobna zasada będzie obowiązywała w przypadku poświadczeń bezpieczeństwa Unii Europejskiej. Należy jednak mieć na uwadze to, że wprowadzenie zasady „kaskadowej" ważności poświadczeń upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych będzie dotyczyło tylko tych postępowań, które zostaną wszczęte po wejściu w życie nowej ustawy (o czym stanowi przepis przejściowy w art. 182).

W art. 30 dotyczącym decyzji o odmowie wydania poświadczeń bezpieczeństwa, w tym w szczególności prawnych i faktycznych podstaw tych decyzji oraz trybu i zasad ich wydawania i przekazywania, zawarto przepisy, które w poprzedniej ustawie znajdowały się w wielu jednostkach redakcyjnych. Ponadto, w stosunku do obowiązujących dotychczas rozwiązań zmieniono zasady wyłączania dostepu do informacji niejawnych osobom sprawdzanym[10]. Oznacza to odejście od automatycznego uznawania, że osoba skazana np. za jazdę rowerem w stanie nietrzeźwym (art. 178a kk) albo ukarana za nieodprowadzanie składek ZUS za pracowników nie daje rękojmi zachowania tajemnicy w zakresie dostępu do informacji niejawnych o klauzuli „tajne" i „ściśle tajne". Ustawodawca uznał, że skazanie prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego (sprecyzowano, że chodzi tu także o umyślne przestępstwo skarbowe) będzie stanowić podstawę do wydania decyzji o odmowie wydania poświadczenia bezpieczeństwa tylko wtedy, gdy osoba sprawdzana zostanie skazana na karę pozbawienia wolności (trudno uwierzyć, że sądy mogą skazywać na taką karę za przestępstwa mniejszej wagi), choćby wykonanie tej kary warunkowo zawieszono. Poza tym, skazanie osoby sprawdzanej prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego będzie podstawą do odmowy wydania poświadczenia bezpieczeństwa tylko wówczas, gdy będzie wywoływać wątpliwości ustalane w toku postępowania (przy czym nie jest konieczne wykazanie, że wątpliwości te są niemożliwe do usunięcia).

Art. 30.

1. *Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli nie zostaną usunięte wątpliwości, o których mowa w art. 24 ust. 2, a także jeżeli w trakcie poszerzonego postępowania sprawdzającego nie zostaną usunięte wątpliwości, o których mowa w art. 24 ust. 3.*
2. *Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie, wywołuje wątpliwości, o których mowa w art. 24 ust. 2 i 3.*
3. *Decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać:*
   1) podstawę prawną oraz uzasadnienie faktyczne i prawne;
   2) wskazanie wnioskodawcy postępowania sprawdzającego;
   3) określenie organu, który przeprowadził postępowanie sprawdzające;

[10] Jeżeli osoba ubiegała się o dostęp do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", fakt skazania prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego, stanowił bezwzględną przesłankę wyłączenia dostępu do informacji niejawnych; w przypadkach klauzul „poufne" i „zastrzeżone" była to jedynie przesłanka fakultatywna.

4) datę i miejsce wydania;

5) imię, nazwisko i datę urodzenia osoby sprawdzanej;

6) określenie rodzaju przeprowadzonego postępowania sprawdzającego, ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp;

7) stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy;

8) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;

9) pouczenie o dopuszczalności i terminie wniesienia odwołania odpowiednio do Prezesa Rady Ministrów albo Szefa ABW lub Szefa SKW.

4. *Uzasadnienie faktyczne w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w niniejszej ustawie.*
5. *Po zakończeniu postępowania sprawdzającego z wynikiem negatywnym organ prowadzący postępowanie wydaje decyzję o odmowie wydania poświadczenia bezpieczeństwa i doręcza ją osobie sprawdzanej, zawiadamiając o tym wnioskodawcę oraz pełnomocnika ochrony.*
6. *Osoba uprawniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych, uniemożliwić dostęp do informacji niejawnych osobie, której odmowa dotyczy, z zastrzeżeniem art. 21 ust. 4.*
7. *Postępowanie sprawdzające wobec osoby, której odmówiono wydania poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po roku od daty doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa.*
8. *Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o odmowie wydania poświadczenia bezpieczeństwa.*
9. *W rozporządzeniu, o którym mowa w ust. 8, Prezes Rady Ministrów uwzględni we wzorze decyzji składniki określone w ust. 3 oraz zapewni zróżnicowanie wzorów decyzji wydawanych przez ABW, SKW, służby i instytucje określone w art. 23 ust. 5 oraz pełnomocników ochrony.*

Zmieniono również formułę dotyczącą zasad odstępowania od przekazywania przez organ prowadzący postępowanie faktycznego uzasadnienia decyzji o odmowie. W obecnym brzmieniu tego przepisu uzasadnienie faktyczne podlega ochronie na zasadach określonych w ustawie, co oznacza, że osoba nieposiadająca poświadczenia nie będzie mogła się z nim zapoznać, czyli że w praktyce będzie się odstępować od przekazywania takiego uzasadnienia (o ile będzie ono zawierać informacje niejawne).

Analogicznie do postanowień o zawieszeniu postępowania sprawdzającego, na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego zakończeniu decyzją o odmowie wydania poświadczenia bezpieczeństwa nie tylko wnioskodawcy, ale również pełnomocnika ochrony (o ile oczywiście to sam pełnomocnik ochrony nie jest organem, który wydał tę decyzję).

Pewne zmiany wprowadzono także w przepisie określającym zasady umarzania postępowań sprawdzających (art. 31). W stosunku do poprzednio obowiązujących rozwiązań do ustawy włączono wprost treść art. 105 § 1 kpa, mówiącego o tym, że postępowanie zostaje umorzone, gdy stało się bezprzedmiotowe (czyli np. w sytuacji, gdy wygasła właściwość organu do prowadzenia postępowania sprawdzającego). I analogicznie jak w przypadku postanowień o zawieszeniu postępowania sprawdzającego oraz zakończeniu postępowania decyzją o odmowie, na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego umorzeniu nie tylko wnioskodawcy, ale również pełnomocnika ochrony (o ile to pełnomocnik ochrony nie jest organem, który umorzył to postępowanie). Sprecyzowano też tryb składania odwołań od decyzji o umorzeniu postępowania sprawdzającego (tak jak w przypadku odwołań od decyzji o odmowie wydania poświadczenia bezpieczeństwa).

Art. 31.

1. *Umorzenie postępowania sprawdzającego następuje w przypadku:*

   1) śmierci osoby sprawdzanej;

   2) rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac, związanych z dostępem do informacji niejawnych;

   3) odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac, związanych z dostępem do informacji niejawnych;

   4) gdy postępowanie z innej przyczyny stało się bezprzedmiotowe.

2. *O umorzeniu postępowania sprawdzającego organ je prowadzący zawiadamia wnioskodawcę, pełnomocnika ochrony oraz, w przypadkach, o których mowa w ust. 1 pkt 2-4, osobę sprawdzaną.*

W art. 32 dotyczącym kolejnych postępowań sprawdzających wprowadzono możliwość przeprowadzenia „uproszczonego" postępowania sprawdzającego wobec osoby ubiegającej się o wydanie poświadczenia bezpieczeństwa organizacji międzynarodowych, która posiada ważne poświadczenie „krajowe", wydane przez ABW, SKW, AW lub SWW. W takim przypadku nie ma konieczności wypełniania ankiety, a poświadczenie upoważniające do dostępu do informacji niejawnych organizacji międzynarodowych wydaje się tylko na okres ważności poświadczenia „krajowego". Choć nie zapisano tego wprost, ze zbiegu przepisów ustawy (art. 32 ust. 2, art. 24 ust. 8) wynika jednak obowiązek uzyskania przez organ prowadzący takie „uproszczone" postępowanie odrębnej zgody osoby sprawdzanej na jego przeprowadzenie.

Art. 32.

1. *Na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska, złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa, właściwy organ przeprowadza kolejne postępowanie sprawdzające.*

2. *Do kolejnego postępowania sprawdzającego stosuje się przepisy ustawy odnoszące się do właściwego postępowania sprawdzającego, z uwzględnieniem ust. 3 i 4.*

3. *Kolejne postępowanie sprawdzające powinno być zakończone przed upływem terminu ważności poświadczenia bezpieczeństwa. Termin, o którym mowa w art. 24 ust.6, nie ma zastosowania.*

4. *Jeżeli wobec osoby posiadającej ważne poświadczenie bezpieczeństwa, wydane przez ABW, SKW, AW lub SWW, zostanie skierowany wniosek o przeprowadzenie postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej, wypełnienie ankiety nie jest wymagane, a poświadczenie bezpieczeństwa organizacji międzynarodowej jest wydawane jedynie na okres ważności posiadanego przez tę osobę poświadczenia bezpieczeństwa.*

Niezwykle istotną instytucją w przypadku bezpieczeństwa osobowego pozostaje kontrolne postępowanie sprawdzające (art. 33), w poprzedniej ustawie opisane w art. 45-47. W obecnie obowiązującej ustawie usankcjonowano możliwość dokonania *wstępnych czynności weryfikacyjnych* jeszcze przed wszczęciem postępowania kontrolnego. Pełnomocnik ochrony może dokonać sprawdzeń w ewidencjach i kartotekach, a ABW, SKW, AW, SWW, CBA, Policja, ŻW, SW, SG oraz BOR – dodatkowo w ewidencjach niedostępnych powszechnie. Czynności te należy rzetelnie dokumentować, a dokumentację tę włączyć do akt postępowania (kontrolnego – jeśli zostanie wszczęte – lub poprzedniego – jeżeli nie zostanie wszczęte).

Art. 33.

1. *W przypadku gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające. Osoba sprawdzana nie wypełnia nowej ankiety dla celów tego postępowania.*

2. *Postępowanie, o którym mowa w ust. 1, przeprowadza organ właściwy do przeprowadzenia kolejnego postępowania sprawdzającego, z zastrzeżeniem ust. 3.*

3. *W przypadkach uzasadnionych względami bezpieczeństwa państwa kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW albo SKW.*

4. *Przepisu ust. 3 nie stosuje się do kontrolnych postępowań sprawdzających prowadzonych wobec osób, które posiadają poświadczenie bezpieczeństwa wydane w wyniku przeprowadzenia postępowania sprawdzającego, o którym mowa w art. 23 ust. 5.*

5. *W celu weryfikacji informacji, o których mowa w ust. 1, właściwy organ może przeprowadzić niezbędne czynności sprawdzające. Pełnomocnik ochrony może przeprowadzić w tym trybie czynności, o których mowa w art. 25 ust. 1 pkt 1, a służby i instytucje uprawnione do prowadzenia poszerzonych postępowań sprawdzających także czynności, o których mowa w art. 25 ust. 1 pkt 2. Czynności te muszą być rzetelnie udokumentowane i prowadzone zgodnie z zasadami bezstronności, obiektywizmu i wykazania najwyższej staranności. Dokumentację tych czynności dołącza się do akt postępowania sprawdzającego.*

6. *O wszczęciu kontrolnego postępowania sprawdzającego zawiadamia się:*

1) kierownika jednostki organizacyjnej lub osobę uprawnioną do obsady stanowiska;

2) pełnomocnika ochrony w jednostce organizacyjnej;

3) osobę sprawdzaną.

7. *Po otrzymaniu zawiadomienia, o którym mowa w ust. 6, kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska uniemożliwia osobie sprawdzanej dostęp do informacji niejawnych.*

8. *Do kontrolnego postępowania sprawdzającego stosuje się przepisy art. 24 ust. 1-5 i 9, art. 25-27, art. 30, art. 31 ust. 1 pkt 1 i 4 oraz ust. 2.*

9. *Wszystkie czynności przeprowadzone w toku kontrolnych postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 6 miesięcy od dnia wszczęcia postępowania.*

10. *W szczególnie uzasadnionych przypadkach niezakończenia kontrolnego postępowania sprawdzającego w terminie, o którym mowa w ust. 9, organ prowadzący postępowanie jednorazowo przedłuża je o kolejne 6 miesięcy, zawiadamiając o tym osoby, o których mowa w ust. 6.*

11. *Kontrolne postępowanie sprawdzające kończy się:*

1) decyzją o cofnięciu poświadczenia bezpieczeństwa;

2) poinformowaniem osób wymienionych w ust. 6 o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem dalszej jej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa;

3) decyzją o umorzeniu postępowania, w przypadku gdy postępowanie to nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia.

12. *Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o cofnięciu poświadczenia bezpieczeństwa.*

13. *W rozporządzeniu, o którym mowa w ust. 12, Prezes Rady Ministrów uwzględni we wzorze decyzji składniki określone w art. 30 ust. 3 pkt 1 i 3-9 oraz zapewni zróżnicowanie wzorów decyzji wydawanych przez ABW, SKW, służby i instytucje określone w art. 23 ust. 5 oraz pełnomocników ochrony.*

W nowej ustawie sprecyzowano również, który organ jest właściwy do prowadzenia kontrolnego postępowania sprawdzającego. Zgodnie z nowym zapisem jest nim ten organ, który byłby właściwy w momencie wszczęcia tego postępowania do przeprowadzenia kolejnego postępowania sprawdzającego. Odstępstwem od tej reguły jest zapis, że w przypadkach uzasadnionych względami bezpieczeństwa państwa kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW albo SKW, z wyłączeniem osób, które posiadają poświadczenie wydane w wyniku postępowania, o którym mowa w art. 23 ust. 5.

Najpoważniejszą zmianą z punktu widzenia osoby sprawdzanej jest wprowadzenie zawitego terminu realizacji postępowania kontrolnego. Postępowanie tego typu powinno zakończyć się po upływie 6 miesięcy od momentu jego wszczęcia, jednakże w przypadkach szczególnie uzasadnionych organ prowadzący może je jednorazowo przedłużyć o kolejne 6 miesięcy. Po upływie tego drugiego terminu, a więc po upływie roku od wszczęcia postępowania kontrolnego, jeżeli nie zo-

stanie ono zakończone decyzją o cofnięciu poświadczenia bezpieczeństwa albo poinformowaniem o braku zastrzeżeń w stosunku do osoby, którą nim objęto, postępowanie to musi zostać umorzone.

Kolejna zmiana dotyczy trybu informowania o wszczęciu, przedłużeniu o kolejne 6 miesięcy oraz o zakończeniu postępowania kontrolnego. O tych faktach organ prowadzący zobowiązany jest poinformować nie tylko kierownika jednostki organizacyjnej, w której zatrudniona jest osoba objęta takim postępowaniem, ale także samą osobę sprawdzaną oraz pełnomocnika ochrony. Jednocześnie wyraźnie wskazano, że na potrzeby postępowania kontrolnego nie wypełnia się ankiety bezpieczeństwa osobowego. Wprowadzono również – m.in. ze względu na zmianę definicji informacji niejawnych – bezwzględną konieczność wyłączenia dostępu do informacji niejawnych osobie, wobec której wszczęto kontrolne postępowanie sprawdzające (dotychczas była jedynie możliwość ograniczenia tego dostępu).

W art. 34 opisano sytuacje, w których nie przeprowadza się postępowania sprawdzającego wobec osoby dopuszczanej do informacji niejawnych (do tej pory opisane m.in. w ustawie *Prawo o ustroju sądów powszechnych*[11]). W stosunku do poprzednio obowiązujących rozwiązań do katalogu osób, które z urzędu wyłączone są z konieczności poddawania się jakimkolwiek postępowaniom sprawdzającym (Prezydent RP, Prezes Rady Ministrów, Marszałek Sejmu, Marszałek Senatu), w tym prowadzonym w związku z koniecznością posiadania poświadczenia bezpieczeństwa organizacji międzynarodowych, dodano osobę wybraną na urząd Prezydenta (Prezydenta-elekta, tj. osobę ogłoszoną przez Państwową Komisję Wyborczą zwycięzcą wyborów prezydenckich, do momentu zaprzysiężenia przed Zgromadzeniem Narodowym).

Art. 34.

1. *Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5.*
2. *O zatrudnieniu na stanowisku, z którym może łączyć się dostęp do informacji niejawnych osoby, o której mowa w ust. 1, przedstawiającej odpowiednie poświadczenie bezpieczeństwa, kierownik jednostki organizacyjnej informuje w terminie 7 dni organ, który wydał poświadczenie bezpieczeństwa, oraz odpowiednio ABW lub SKW.*
3. *Od obowiązku określonego w ust. 2 są zwolnieni kierownicy jednostek organizacyjnych podmiotów, o których mowa w art. 23 ust. 5.*
4. *Jeżeli z ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych wynika obowiązek dopuszczenia do informacji niejawnych obywateli obcych państw mających*

[11] Na podstawie *Ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych* (Dz.U. z 2001 r., Nr 98, poz. 1070 z późn. zm.) z konieczności poddawania się procedurom sprawdzającym przed uzyskaniem dostępu do informacji niejawnych wyłączono sędziów (art. 85 § 4) i prokuratorów (art. 185 pkt 15).

wykonywać w Rzeczypospolitej Polskiej pracę w interesie innego państwa lub organizacji międzynarodowej, postępowania sprawdzającego nie przeprowadza się.

5. *Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu, Kancelarii Senatu lub Kancelarii Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli lub kierownik urzędu centralnego, a w przypadku ich braku ABW albo SKW, mogą:*

   1) w szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4 ust. 2, wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa;

   2) wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" osobie, wobec której wszczęto poszerzone postępowanie sprawdzające.

6. *W stanach nadzwyczajnych Prezydent Rzeczypospolitej Polskiej lub Prezes Rady Ministrów, każdy w swoim zakresie, może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.*

7. *W przypadkach, o których mowa w ust. 5 i 6, kopię zgody na udostępnienie informacji niejawnych lub odstąpienie od przeprowadzenia postępowania sprawdzającego przekazuje się odpowiednio do ABW lub SKW.*

8. *Obowiązek, o którym mowa w ust. 7, nie dotyczy służb i instytucji uprawnionych do przeprowadzania poszerzonych postępowań sprawdzających, o których mowa w art. 23 ust. 5.*

9. *Zgodę na udostępnienie informacji niejawnych o klauzuli „poufne" osobie, wobec której wszczęto postępowanie sprawdzające, może wyrazić, w formie pisemnej, kierownik jednostki organizacyjnej, w której ta osoba jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.*

10. *Postępowania sprawdzającego nie przeprowadza się, z zastrzeżeniem ust. 11-13, wobec:*

    1) Prezydenta Rzeczypospolitej Polskiej oraz osoby wybranej na ten urząd;

    2) Marszałka Sejmu;

    3) Marszałka Senatu;

    4) Prezesa Rady Ministrów;

    5) członka Rady Ministrów;

    6) Prezesa Narodowego Banku Polskiego;

    7) Prezesa Najwyższej Izby Kontroli;

    8) Rzecznika Praw Obywatelskich;

    9) Generalnego Inspektora Ochrony Danych Osobowych;

    10) członka Rady Polityki Pieniężnej;

    11) członka Krajowej Rady Radiofonii i Telewizji;

    12) Prezesa Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;

    13) Szefa Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów;

    14) posła i senatora;

    15) sędziego sądu powszechnego i sądu wojskowego, Sądu Najwyższego, sądów ad-

ministracyjnych i Naczelnego Sądu Administracyjnego, a także Trybunału Stanu i Trybunału Konstytucyjnego, ławnika sądu powszechnego i ławnika sądu wojskowego oraz prokuratora i asesora prokuratury pełniącego czynności prokuratorskie.

11. *W stosunku do osób zajmujących lub kandydujących na stanowiska albo pełniących funkcje, o których mowa w ust. 10 pkt 5-15, ubiegających się o dostęp do informacji niejawnych organizacji międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską, ABW albo SKW, przeprowadzają poszerzone postępowanie sprawdzające. Z wnioskiem o przeprowadzenie tego postępowania występuje osoba uprawniona do powołania na to stanowisko lub Marszałek Sejmu w stosunku do posłów lub jeżeli do powołania jest uprawniony Sejm albo Marszałek Senatu w stosunku do senatorów lub jeżeli do powołania jest uprawniony Senat.*
12. *W stosunku do kandydatów na stanowiska, o których mowa w ust. 10 pkt 6-13, oraz wobec posłów lub senatorów, których obowiązki poselskie bądź senatorskie wymagają dostępu do informacji niejawnych o klauzuli „ściśle tajne", ABW przeprowadza poszerzone postępowanie sprawdzające. Z wnioskiem o przeprowadzenie tego postępowania występuje osoba uprawniona do powołania na to stanowisko lub Marszałek Sejmu w stosunku do posłów lub jeżeli do powołania jest uprawniony Sejm albo Marszałek Senatu w stosunku do senatorów lub jeżeli do powołania jest uprawniony Senat.*
13. *Postępowanie sprawdzające, o którym mowa w ust. 12, w stosunku do osób kandydujących na stanowiska, o których mowa w ust. 10 pkt 6-13, powinno być zakończone przed upływem 14 dni od dnia złożenia wniosku o przeprowadzenie tego postępowania wraz z wypełnioną ankietą, o której mowa w art. 24 ust. 10.*
14. *W przypadku zakończenia postępowania sprawdzającego prowadzonego na wniosek Marszałka Sejmu albo Marszałka Senatu decyzją o odmowie wydania poświadczenia bezpieczeństwa, Prezes Rady Ministrów przedstawia informację o powodach tej decyzji odpowiednio Marszałkowi Sejmu lub Marszałkowi Senatu.*
15. *Prezydent Rzeczypospolitej Polskiej, Prezes Rady Ministrów oraz Marszałek Sejmu i Marszałek Senatu zapoznają się z przepisami o ochronie informacji niejawnych i składają oświadczenie o znajomości tych przepisów. Oświadczenie przechowuje się odpowiednio w Kancelariach Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, Sejmu albo Senatu.*

Postępowaniom sprawdzającym w związku z uzyskaniem dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej nie muszą poddawać się również ławnicy sądów powszechnych[12] i wojskowych, asesorzy prokuratury pełniący czynności prokuratorskie, sędziowie sądów powszechnych, wojskowych, Sądu Najwyższego, sądów administracyjnych i Naczelnego Sądu Administracyjnego, a także sędziowie Trybunału Stanu i Trybunału Konstytucyjnego (choć nadal nie są oni zwolnieni z konieczności poddawania się procedurom sprawdzającym, jeżeli zachodzi konieczność wydania im poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych).

Utrzymano funkcjonujący wcześniej 14-dniowy termin realizacji procedur wobec kandydatów na niektóre najważniejsze stanowiska w państwie. Jednak w przypadku wniosków o przeprowadzenie takiego postępowania (art. 34 ust. 13

[12] Na decyzję ustawodawcy w tej sprawie miała zapewne wpływ uchwała Sądu Najwyższego nr 1 KZP34/09 z dnia 24.02.2010 r., w której stwierdzono, iż przepisy dotyczące prowadzenia postępowań sprawdzających nie mają zastosowania do ławników sądów powszechnych.

ustawy), ABW nie będzie – jak to miało miejsce dotychczas – wydawała „opinii" (art. 27 ust. 7 poprzedniej ustawy), tylko poświadczenie bezpieczeństwa.

Obok istniejącego dotychczas obowiązku informowania (w ciągu 7 dni) organu, który wydał poświadczenie bezpieczeństwa o zatrudnieniu osoby posiadającej to poświadczenie na stanowisku związanym z dostępem do informacji niejawnych, wprowadzono także obowiązek informowania o tym fakcie także ABW bądź SKW, czyli służby właściwej dla danej „sfery" (cywilnej lub wojskowej), aby nie dochodziło do sytuacji, że w sferze „cywilnej" zatrudnia się osoby posiadające poświadczenie wydane przez SKW, a nadzorująca tę sferę ABW nie posiada na ten temat żadnej wiedzy. Podobny mechanizm działa także w drugą stronę, tzn. jeżeli w MON zostanie zatrudniona osoba posiadająca poświadczenie wydane przez ABW, to informację o tym fakcie uzyska nie tylko ABW, ale również SKW (jako służba realizująca zadania z zakresu ochrony informacji niejawnych w MON). Z obowiązku informowania, o którym mowa wyżej, zwolnieni są szefowie AW, SWW, CBA, Policji, ŻW, SW, SG oraz BOR, którzy w zakresie udostępniania informacji niejawnych swoim funkcjonariuszom, żołnierzom czy pracownikom dysponują daleko posuniętą autonomią (tj. prawem do realizowania „samodzielnych" postępowań sprawdzających).

Ustawa sprecyzowała także tryb udostępniania informacji niejawnych osobom nieposiadającym poświadczenia bezpieczeństwa w stanach nadzwyczajnych. W takich sytuacjach – podobnie jak dotychczas – prezydent lub premier wydają zgodę na udostępnienie informacji niejawnych osobie nieposiadającej poświadczenia, ale kopie takiej zgody muszą przekazać do ABW lub SKW. Obowiązek ten nie dotyczy sytuacji, gdy osoba nieposiadająca poświadczenia bezpieczeństwa ma uzyskać dostęp do informacji niejawnych w związku z zatrudnieniem lub wykonywaniem prac na rzecz ABW, SKW, AW, SWW, CBA, Policji, ŻW, SW, SG oraz BOR.

Bezpośrednio do zagadnień związanych z postępowaniami sprawdzającymi odnosi się również rozdział 6 przedmiotowej ustawy – *Postępowanie odwoławcze i skargowe, wznowienie postępowania*, funkcjonujący wcześniej (od nowelizacji z 2001 roku) także jako odrębny rozdział 5a ustawy. Art. 35 tego rozdziału dotyczy trybu i zasad składania odwołań do Prezesa Rady Ministrów. W stosunku do poprzednio obowiązujących rozwiązań doprecyzowano, że od wszystkich decyzji o odmowie wydania i cofnięciu poświadczenia bezpieczeństwa, będących rezultatem postępowań sprawdzających prowadzonych przez ABW, SKW, AW, SWW, CBA, Policję, ŻW, SW, SG oraz BOR (nawet, gdy będą to zwykłe postępowania sprawdzające realizowane przez pełnomocników ochrony w tych służbach lub w ich jednostkach organizacyjnych), osobom sprawdzanym przysługuje odwoła-

nie do premiera. Ustalono również, że ten sam tryb (składania odwołań) odnosi się do odwołań od decyzji o umorzeniu postępowania, jak również do zażaleń na postanowienie o zawieszeniu lub podjęciu zawieszonego postępowania sprawdzającego. Dodano także, że wniesienie odwołania nie wstrzymuje wykonania decyzji.

Art. 35.

1. *Od decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, wydanej przez podmiot, o którym mowa w art. 23 ust. 2 i 5, osobie sprawdzanej przysługuje odwołanie do Prezesa Rady Ministrów. Odwołanie nie wymaga uzasadnienia.*
2. *Odwołanie wnosi się w terminie 14 dni od dnia doręczenia osobie sprawdzanej decyzji, o której mowa w ust. 1, za pośrednictwem podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające.*
3. *Podmiot, o którym mowa w art. 23 ust. 2 i 5, jest obowiązany przesłać odwołanie wraz z aktami postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym otrzymał odwołanie.*
4. *Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania.*
5. *Wniesienie odwołania nie wstrzymuje wykonania decyzji.*

W art. 36, który dotyczy rozstrzygnięć postępowań odwoławczych, poszerzono katalog możliwych rozstrzygnięć postępowania odwoławczego, dodając uchylenie decyzji o cofnięciu poświadczenia bezpieczeństwa, uchylenie decyzji i przekazanie sprawy do ponownego rozpatrzenia oraz stwierdzenie nieważności decyzji[13]. Wskazano, że zlecenie dodatkowych czynności w postępowaniu odwoławczym może dotyczyć w szczególności ponownego przeprowadzenia specjalistycznych badań medycznych (pod kątem stwierdzenia występowania wątpliwości związanych z chorobą lub dolegliwością psychiczną oraz uzależnieniem od alkoholu lub środków odurzających albo psychotropowych), które powinny być wykonane przez innego specjalistę niż w postępowaniu sprawdzającym.

Art. 36.

1. *Prezes Rady Ministrów stwierdza, w drodze postanowienia:*
   1) niedopuszczalność odwołania;
   2) uchybienie terminowi do wniesienia odwołania.
2. *Postanowienie w tej sprawie jest ostateczne i powinno zawierać w szczególności:*
   1) oznaczenie organu;

[13] W praktyce jest to wpisanie wprost do ustawy niektórych przepisów kpa, m.in. z art. 138 i art. 156 (ten ostatni jest wpisany do art. 3 *Ustawy o ochronie informacji niejawnych* jako mający zastosowanie w postępowaniach sprawdzających).

2) datę wydania;

3) oznaczenie osoby sprawdzanej;

4) powołanie podstawy prawnej;

5) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;

6) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego;

7) podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego, osoby upoważnionej do jego wydania.

3. Prezes Rady Ministrów może na żądanie osoby sprawdzanej lub z urzędu zlecić właściwemu podmiotowi przeprowadzenie dodatkowych czynności, w tym specjalistycznych badań, o których mowa w art. 26 ust. 6, w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym lub kontrolnym postępowaniu sprawdzającym. W przypadku, gdy zlecenie przeprowadzenia dodatkowych czynności dotyczy ponownego przeprowadzenia specjalistycznych badań, badania te powinny być wykonane przez innego specjalistę niż badania przeprowadzone w ramach postępowania sprawdzającego zakończonego wydaniem decyzji, od której odwołanie jest rozpatrywane.

4. Prezes Rady Ministrów wydaje decyzję, w której:

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

2) uchyla decyzję podmiotu, który przeprowadził kontrolne postępowanie sprawdzające zakończone 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.

5. Decyzja powinna zawierać w szczególności:

1) oznaczenie organu;

2) datę wydania;

3) oznaczenie osoby sprawdzanej;

4) powołanie podstawy prawnej;

5) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;

6) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego;

7) podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do jej wydania.

6. Po wydaniu decyzji lub postanowienia Prezes Rady Ministrów niezwłocznie zwraca właściwemu podmiotowi akta postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego.

7. Decyzje i postanowienia doręcza się na piśmie osobie sprawdzanej i właściwemu podmiotowi, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę uprawnioną do obsady stanowiska.

8. Do postępowania odwoławczego przepisy art. 27, art. 30 ust. 4 oraz art. 31 stosuje się odpowiednio.

Istotną zmianą jest wprowadzenie instytucji wznowienia postępowania. Ponieważ nie było możliwe zastosowanie przepisów kpa wprost, zdecydowano się na rozwiązanie kompromisowe: opierając się na przepisach dotyczących wznowień postępowań administracyjnych, wprowadzono taką możliwość w odniesieniu do postępowań sprawdzających (i odwoławczych), ale wdrażając procedury właściwe dla specyfiki tych postępowań (art. 39).

Art. 39.

1. *Prezes Rady Ministrów, pełnomocnicy ochrony lub podmioty wymienione w art. 23 ust. 2 i 5 wznawiają postępowanie sprawdzające lub kontrolne postępowanie sprawdzające, zakończone decyzją ostateczną, odpowiednio o odmowie wydania albo o cofnięciu poświadczenia bezpieczeństwa, jeżeli decyzja została wydana wyłącznie 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, a postępowanie karne zostało następnie umorzone lub zakończone uniewinnieniem osoby sprawdzanej.*
2. *Wznowienie postępowania następuje z urzędu lub na wniosek osoby sprawdzanej.*
3. *Wniosek o wznowienie postępowania wnosi się do podmiotu, który wydał w sprawie decyzję w pierwszej instancji, w terminie 30 dni od dnia, w którym osoba sprawdzana dowiedziała się o okoliczności stanowiącej podstawę do wznowienia postępowania.*
4. *Rozpatrzenie wniosku powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania.*
5. *Podmiot właściwy do wznowienia postępowania stwierdza, w drodze postanowienia, uchybienie terminowi do złożenia wniosku o wznowienie postępowania.*
6. *Postanowienie, o którym mowa w ust. 5, jest ostateczne i powinno zawierać:*
   1) oznaczenie podmiotu;
   2) datę wydania;
   3) oznaczenie osoby sprawdzanej;
   4) powołanie podstawy prawnej;
   5) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne;
   6) pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego;
   7) podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do jego wydania.
7. *Wznowienie postępowania następuje w drodze postanowienia.*
8. *Postanowienie stanowi podstawę do przeprowadzenia przez właściwy podmiot postępowania co do przyczyn wznowienia oraz rozstrzygnięcia co do istoty sprawy.*
9. *Odmowa wznowienia postępowania następuje w drodze decyzji.*

Postępowanie wznawia się (może to zrobić albo organ odwoławczy, albo pierwszoinstancyjny – z urzędu lub na wniosek osoby sprawdzanej), jeżeli zostało ono zakończone odmową wydania poświadczenia bezpieczeństwa lub jego cofnię-

ciem na podstawie przedstawienia osobie sprawdzanej zarzutu popełnienia przestępstwa, postawienia jej w stan oskarżenia lub skazania za przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe, a postępowanie karne zostało następnie umorzone lub zakończone uniewinnieniem osoby sprawdzanej. Taka konstrukcja tego przepisu (wznowienie postępowań zakończonych odmową wydania poświadczenia bezpieczeństwa z uwagi na fakt toczącego się postępowania karnego) jest niezwykle istotna dla pragmatyki postępowań sprawdzających, ponieważ sankcjonuje od dawna praktykowaną i wielokrotnie potwierdzoną rozstrzygnięciami organów odwoławczych oraz sądu administracyjnego zasadę, że w szczególnych okolicznościach, przy spełnieniu określonych warunków, fakt toczącego się wobec osoby sprawdzanej postępowania karnego (a więc od momentu przedstawienia zarzutów do uprawomocnienia się wyroku sądu lub postanowienia prokuratury) może stanowić podstawę nie tylko do zawieszenia toczącego się postępowania, ale i do decyzji o odmowie wydania bądź cofnięcia poświadczenia bezpieczeństwa.

Wniosek o wznowienie postępowania wnosi się do organu pierwszoinstancyjnego w terminie 30 dni od dnia, w którym osoba sprawdzana dowiedziała się o okoliczności stanowiącej podstawę wznowienia (w przypadku uchybienia tego terminu organ w drodze postanowienia stwierdza jego uchybienie, które jest ostateczne), a jego rozpatrzenie powinno nastąpić w terminie 3 miesięcy od otrzymania wniosku. Wznowienie postępowania następuje w drodze postanowienia, a jego odmowa – w drodze decyzji (od której można się odwołać na podstawie przepisów przewidzianych dla odwołania od decyzji o odmowie wydania poświadczenia bezpieczeństwa).

Wznowione postępowanie może zostać zakończone:

1) odmową uchylenia pierwotnej decyzji,
2) uchyleniem pierwotnej decyzji i wydaniem nowej,
3) uchyleniem pierwotnej decyzji i przekazaniem sprawy do ponownego rozpatrzenia,
4) uchyleniem pierwotnej decyzji o cofnięciu poświadczenia i/lub o utrzymaniu w mocy cofnięcia (art. 40 ustawy).

Od rozstrzygnięć zapadłych w wyniku wznowienia postępowania przysługuje prawo do wniesienia odwołania. Zasady odwołań są takie same, jak w przypadku odmów, o ile wznowione postępowanie było prowadzone przez organ pierwszoinstancyjny. Jeżeli zatem decyzję w pierwszej instancji wydały ABW, SKW, AW, SWW, CBA, Policja, ŻW, SW, SG oraz BOR, w tym pełnomocnicy ochrony

w tych instytucjach, odwołanie wnosi się do premiera. Jeżeli zaś tego typu decyzję wydali pełnomocnicy ochrony spoza tych instytucji – odwołanie wnosi się odpowiednio do Szefa ABW lub SKW.

Jeżeli natomiast wznowione zostało postępowanie odwoławcze, to od takiej decyzji nie można się odwołać, ale *osoba niezadowolona z decyzji* może zwrócić się do organu, który wydał decyzję we wznowionym postępowaniu odwoławczym, o ponowne rozpatrzenie sprawy.

Dla zagadnień dotyczących bezpieczeństwa osobowego istotne znaczenie mają także przepisy zawarte w rozdziale 11 nowej ustawy, zatytułowanym *Zmiany w przepisach obowiązujących*. Uwagę zwraca tu przede wszystkim nadanie uprawnień dotychczasowych służb ochrony państwa (ABW i SKW) wszystkim służbom i organom uprawnionym do prowadzenia „samodzielnych" postępowań sprawdzających, tj. AW, SWW, CBA, Policji, ŻW, SG, SW oraz BOR, co związane jest z prawem do występowania o przekazanie niezbędnych informacji i udostępnianie dokumentów[14].

Równie ważne w tym kontekście regulacje znajdują się w ostatnim rozdziale ustawy (*Przepisy przejściowe i końcowe*). W art. 182 wskazano, że poświadczenia bezpieczeństwa wydane na podstawie dotychczasowych przepisów zachowują ważność przez okres wskazany w tych przepisach. Oznacza to, że dla poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych, wydanych przed wejściem w życie nowej ustawy, nie będzie obowiązywała „kaskada" ważności. Jest to odmienne uregulowanie kwestii związanych z okresem przejściowym w stosunku do nowelizacji poprzedniej ustawy, dokonanej w 2005 roku, gdzie uznano, że poświadczenia bezpieczeństwa wydane przed dniem wejścia w życie ustawy, ważne w tym dniu, zachowują ważność w zakresie i okresie określonym *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, w brzmieniu nadanym nowo wprowadzoną w 2005 r. ustawą[15].

---

[14] Dotyczy to następujących ustaw: 1) *Ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa* (Dz.U. z 2005 r., Nr 8, poz. 60 z późn. zm.) – art. 119 pkt 8 i 9, zmieniające odpowiednio art. 297 § 1 pkt 7 oraz art. 298 pkt 5a ustawy Ordynacja Podatkowa; 2) *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (Dz.U. z 2002 r., Nr 72, poz. 665 z późn. zm.) – art. 120 pkt 1 i 2 nowej ustawy, zmieniające odpowiednio art. 105 ust. 1 pkt 2 lit. k oraz art. 110 pkt 6 ustawy Prawo bankowe; 3) *Ustawy z dnia 26 października 2000 r. o giełdach towarowych* (Dz.U. z 2010 r., Nr 48, poz. 284 z późn zm.) – art. 128 nowej ustawy, zmieniający w art. 54 w ust. 1 pkt 6 ustawy o giełdach towarowych; 4) *Ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych* (Dz.U. z 2004 r., Nr 146, poz. 1546 z późn. zm.) – art. 153 nowej ustawy, zmieniający w art. 281 w ust. 1 pkt 8 ustawy o funduszach inwestycyjnych; oraz 5) *Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi* (Dz.U. z 2005 r., Nr 183, poz. 1538 z późn. zm.) – art. 162 nowej ustawy, zmieniający w art. 149 pkt 7 ustawy o obrocie instrumentami finansowymi.

[15] Art. 8 *Ustawy z 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw* (Dz.U. z 2005 r., Nr 85, poz. 727).

Art. 182.

Poświadczenia bezpieczeństwa wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.

Również odmiennie niż w 2005 roku[16], w art. 188 uregulowano kwestię stosowania nowych przepisów do postępowań rozpoczętych przed wejściem w życie ustawy.

Przyjęto rozwiązanie, że do tych postępowań będą stosowane przepisy dotychczasowe (tj. wcześniejsze, z *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* wraz ze zmianami do niej), co oznacza, że przez pewien okres przejściowy (tj. do momentu zakończenia postępowań sprawdzających wszczętych przed wejściem w życie nowej ustawy), w postępowaniach sprawdzających stosowane będą podwójne standardy dotyczące przede wszystkim zakresu i czynności sprawdzających, jak również podstaw decyzji o odmowie wydania poświadczenia bezpieczeństwa.

Art. 188.

Do postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

Art. 189.

1. *Dotychczasowe przepisy wykonawcze wydane na podstawie art. 14 ust. 4, art. 17 ust. 2, art. 18a ust. 2, art. 23 ust. 3, art. 36 ust. 3, art. 53 ust. 1-4, art. 55, art. 62 ust. 1, art. 63 ust. 4, art. 74 i art. 74a ust. 2 ustawy, o której mowa w art. 190, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 6 ust. 9, art. 12 ust. 6, art. 13 ust. 4, art. 18 ust. 1, art. 20 ust. 2, art. 29 ust. 6, art. 30 ust. 8, art. 33 ust. 12, art. 47 ust. 1, 3 i 5, art. 49 ust. 9, art. 53 ust. 4, art. 61 ust. 2 i art. 68 ust. 1 niniejszej ustawy, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.*
2. *Dotychczasowe przepisy wykonawcze wydane na podstawie art. 17 ust. 3 ustawy, o której mowa w art. 84, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 17 ust. 3 tej ustawy w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.*
3. *Dotychczasowe przepisy wykonawcze wydane na podstawie art. 7 ust. 2 ustawy, o której mowa w art. 91, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na postawie art. 7 ust. 2 tej ustawy w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.*

[16] Art. 7 wyżej wymienionej ustawy: *Do postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy tej ustawy.*

Integralną częścią ustawy (jako załącznik do niej) pozostaje wzór ankiety bezpieczeństwa osobowego. Najbardziej zauważalną zmianą jest kompletna zmiana jej formy, upodabniająca ją do deklaracji podatkowej PIT. Jest to rezultat przygotowań do wprowadzenia w przyszłości możliwości wypełniania i przesyłania ankiety do organu mającego prowadzić postępowanie w wersji elektronicznej. Formularz elektroniczny miał w założeniach zdecydowanie upraszczać ankietę i uzależniać jej obszerność („otwarcie" poszczególnych fragmentów i pytań) od odpowiedzi. W związku z tym wprowadzono pytania alternatywne (odpowiedź „TAK" lub „NIE"). Mimo zmiany formy, nowy formularz ankiety w ogromnej większości zawiera te same pytania, co poprzedni, choć część z nich – dla uzyskania bardziej precyzyjnych odpowiedzi – jest rozdzielona na pytania uszczegóławiające, na które należy odpowiadać tylko w sytuacji, gdy zaznaczy się stosowną odpowiedź (najczęściej „TAK") w pytaniu „głównym".

Z punktu widzenia osoby wypełniającej ankietę, ale także osób odpowiedzialnych za jej przekazanie lub przesłanie do organu mającego prowadzić postępowanie, istotne jest ograniczenie obowiązku podpisywania ankiety tylko do osoby, która ma być objęta postępowaniem. Oznacza to, że ankieta nie musi – jak to było dotychczas – być udostępniana pełnomocnikowi ochrony i kierownikowi jednostki organizacyjnej. W instrukcji zapisano, że osoba wypełniająca ankietę na potrzeby postępowania poszerzonego może włożyć ją do koperty, a kopertę zakleić.

Inną ważną zmianą formalną jest odejście od obowiązku nadawania ankiecie klauzuli tajności. Taka możliwość oczywiście będzie istniała, ale nie „z urzędu", tylko zgodnie z ogólnymi przepisami dotyczącymi ochrony informacji niejawnych (tj. w sytuacji, gdy będzie zawierać informacje spełniające kryteria definicji informacji niejawnych). Ankieta będzie natomiast chroniona na podstawie zasad ochrony informacji niejawnych o klauzuli „poufne" (w przypadku postępowania poszerzonego) lub „zastrzeżone" (w przypadku postępowania zwykłego). Należy jednak pamiętać, że *ochrona według zasad ochrony informacji niejawnych o klauzuli „poufne" lub „zastrzeżone"* nie oznacza obowiązku nadania ankiecie jednej z tych klauzul, a odnosi się raczej do zasad fizycznej ochrony tego dokumentu.

Zasadniczą zmianą graficzną i formalną w ankiecie jest pogrupowanie „rozrzuconych" dotychczas pytań w „bloki tematyczne". Formularz nowej ankiety podzielono na 7 części:

- część I – *Dane osobowe* – zawierającą podstawowe dane o osobie, wpisywane dotychczas do pkt. 1a-1p ankiety wypełnianej w przypadku ubiegania się o dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne", stanowiącej załącznik nr 2c do poprzedniej ustawy,

- część II – *Dane osobowe członków rodziny* – zawierającą podstawowe dane dotyczące członków rodziny oraz współmieszkańców osoby sprawdzanej, wpisywane dotychczas do pkt. 2-9 oraz 28 poprzedniej ankiety,

- część III – *Dane dotyczące historii życia zawodowego i osobistego* – zawierającą dane (dotyczące okresu po ukończeniu 18 roku życia) odnośnie:

  1) historii zatrudnienia,

  2) dostępu do informacji niejawnych,

  3) ostatniej ukończonej szkoły, wszystkich szkół ukończonych po 18 roku życia, a także kursów zagranicznych i posiadanego wykształcenia oraz tytułów naukowych,

  4) członkostwa w partiach politycznych, stowarzyszeniach, organizacjach społecznych oraz we władzach fundacji,

  5) adresów zamieszkania dłuższych niż 30 dni; wpisywane dotychczas do pkt. 19, 24, 30, 32 i 27 poprzedniej ankiety,

- część IV – *Dane dotyczące bezpieczeństwa* – zawierającą pytania o:

  1) współpracę lub pracę w organach bezpieczeństwa PRL,

  2) karalność za przestępstwa,

  3) toczące się aktualnie postępowania karne,

  4) toczące się aktualnie postępowania dyscyplinarne związane z naruszeniem przepisów dotyczących ochrony informacji niejawnych,

  5) zainteresowania ze strony obcych służb specjalnych i/lub grup przestępczych, (także wobec członków rodziny i/lub współmieszkańców),

  6) wypytywania przez obce władze na tematy związane z bezpieczeństwem i obronnością RP (także wobec członków rodziny i/lub współmieszkańców),

  7) pobyty zagraniczne (także partnera) dłuższe niż 30 dni,

  8) kontakty (także partnera) z obywatelami innych państw; wpisywane dotychczas do pkt. 11-12, 15, 14, 35, 34, 25 i 31 poprzedniej ankiety,

- część V – *Dane dotyczące stanu zdrowia* – zawierającą rozbudowane i bardziej sprecyzowane w stosunku do poprzedniej ankiety pytania o:

  1) kategorię zdrowia (stwierdzoną w wyniku badania np. w wojsku),

  2) przebyte lub aktualne choroby psychiczne,

  3) przebyte lub aktualne dolegliwości psychiczne,

  4) zażywanie środków odurzających i psychotropowych,

  5) spożywanie alkoholu w ilościach powodujących utratę świadomości,

  6) problemy w pracy lub życiu prywatnym spowodowane spożywaniem alkoholu,

  7) leczenie się w związku ze spożywaniem alkoholu; wpisywane dotychczas do pkt pkt 16-18 poprzedniej ankiety,

- część VI – *Dane dotyczące sytuacji majątkowo-finansowej* – zawierającą rozbudowane i bardziej sprecyzowane w stosunku do poprzedniej ankiety pytania dotyczące:

  1) wynagrodzenia,

  2) innych dochodów,

  3) łącznych dochodów za poprzedni rok,

  4) składania oświadczeń o stanie majątkowym,

  5) osób prowadzących wspólne gospodarstwo domowe z osobą sprawdzaną (w tym numery PESEL i NIP tych osób oraz zestawienia ich rocznych dochodów),

  6) liczby osób na utrzymaniu osoby sprawdzanej,

  7) posiadanych nieruchomości (także innych osób ze wspólnego gospodarstwa domowego),

  8) posiadanych firm lub udziałów w firmie,

9) posiadanych ruchomości, których koszt nabycia był wyższy niż 20 000 zł,

10) posiadanych rachunków bankowych,

11) zadłużenia i innych zobowiązań finansowych,

12) problemów związanych z grami hazardowymi; wpisywanych dotychczas do pkt. 1p-1r i pkt. 20-23 poprzedniej ankiety,

- część VII – *Osoby polecające* – zawierającą podstawowe dane o trzech osobach polecających; wpisywane dotychczas do pkt. 33 poprzedniej ankiety.

W przypadku postępowań zwykłych nie wypełnia się części V – VI, a część VII wypełniają tylko osoby ubiegające się o dostęp do informacji niejawnych o klauzuli „ściśle tajne".

W części I ankiety (*Dane osobowe*) nowością jest wymóg dołączenia kolorowego zdjęcia osoby sprawdzanej, wprowadzenie pytania o inne posiadane przez tę osobę paszporty oraz o daty dotyczące posiadanych obywatelstw. Dodano też pytanie o numer telefonu kontaktowego, a pytania dotyczące dochodów przesunięto do części VI.

W części II (*Dane osobowe członków rodziny*) zrezygnowano z pytań odnośnie danych osobowych dzieci osoby sprawdzanej poniżej 15 roku życia (w postępowaniach poszerzonych osoba sprawdzana ma jedynie wskazać w części finansowej, dotyczącej osób na utrzymaniu liczbę tych dzieci) oraz jej rodziców, rodzeństwa i dzieci partnera/partnerki – jeśli osoby te nie mieszkają razem z osobą sprawdzaną (jeżeli mieszkają – musi je wykazać w rozbudowanym punkcie *Współmieszkańcy*, który nie dotyczy osób poniżej 15 roku życia). W przypadku braku rodziny wypełnienie tego punktu ograniczy się do danych personalnych rodziców oraz zaznaczenia odpowiednich odpowiedzi „NIE" w pytaniach „głównych", dotyczących posiadania rodzeństwa, dzieci, małżonka czy partnera. W ankiecie wprowadzono rozdzielenie pomiędzy małżonkiem i partnerem osoby sprawdzanej, ponieważ osoba sprawdzana może pozostawać formalnie w małżeństwie, ale w praktyce posiadać innego partnera życiowego. Pytanie dotyczące małżonka i partnera osoby sprawdzanej rozbudowano o posiadane paszporty i obywatelstwa (wraz z datami ich utraty/nabycia). Do punktu odnośnie rodzeństwa dodano pytania o uprzednio posiadane obywatelstwa, ale całe pytanie ograniczono jedynie do rodzeństwa powyżej 15 roku życia. Podobnie do punktu dotyczącego dzieci osoby sprawdzanej oraz współmieszkańców dodano pytania o obecnie i uprzednio posiadane obywatelstwa, ale całe pytanie ograniczono do rodzeństwa (współmieszkańców) po-

wyżej 15 roku życia. Znacznie rozbudowano pytanie o współmieszkańców osoby sprawdzanej (analogicznie do pytań o członków rodziny) i zrezygnowano z pytania o właściciela zajmowanego przez osobę sprawdzaną mieszkania.

W części III ankiety (*Dane dotyczące historii życia zawodowego i osobistego*) zrezygnowano z osobnego pytania odnośnie pracy za granicą, ponieważ osoba sprawdzana i tak musi podać powód tego pobytu w pytaniu dotyczącym przebywania na terytorium innego państwa, jeżeli był dłuższy niż 30 dni (dane o pracy w krótszych okresach są z reguły nieistotne z punktu widzenia oceny dawania rękojmi zachowania tajemnicy), lub w pytaniu o wcześniejszy dostęp do informacji niejawnych (w którym należy wskazać miejsce pracy, także za granicą).

W pytaniu o ukończone szkoły ograniczono się do pytania tylko o: 1) ostatnią ukończoną szkołę, 2) szkoły ukończone po 18 roku życia, 3) kursy zagraniczne – dane o szkołach podstawowych i średnich ukończonych przez osoby posiadające wykształcenie wyższe uznano za nieistotne z punktu widzenia oceny dawania rękojmi zachowania tajemnicy. Pytanie o członkostwo w partiach politycznych również ograniczono do okresu po ukończeniu 18 roku życia. Wprowadzono też konieczność podawania informacji o członkostwie w radach nadzorczych fundacji. Zmieniono zakres pytania o adresy zamieszkania (obecnie należy podawać tylko dane o zamieszkiwaniu powyżej 30 dni w okresie po ukończeniu 18 roku życia, a nie przez ostatnie 10 lat, wliczając nawet krótkie pobyty).

W części IV ankiety (*Dane dotyczące bezpieczeństwa*), w pytaniu o współpracę z organami bezpieczeństwa usunięto odpowiedź „NIE DOTYCZY" (bo albo ktoś był współpracownikiem, albo nie, *tertium non datum*) i wskazano, że przy odpowiedzi w tym punkcie tracą znaczenie wcześniejsze zobowiązania do zachowania tego faktu w tajemnicy (w instrukcji do ankiety zapisano, że punkt ten wypełniają tylko osoby urodzone przed 1 sierpnia 1972 roku). Usunięto pytanie o karalność za wykroczenia i toczące się aktualnie postępowania o wykroczenia (uznano to za nieistotne z punktu widzenia oceny dawania rękojmi zachowania tajemnicy) oraz usunięto pytanie dotyczące wcześniejszej karalności dyscyplinarnej za naruszenie przepisów o ochronie informacji niejawnych z uwagi na to, że kary za przewinienia dyscyplinarne zacierają się po pół roku od ich wykonania, a więc osoba sprawdzana i tak nie musiałaby ich podawać. Jeżeli zaś te „naruszenia" były poważne, to powinny być karane zgodnie z przepisami kodeksu karnego. Zmieniono zakres pytania o pobyty zagraniczne (osoba sprawdzana będzie zobowiązana podać jedynie dane o trwających powyżej 30 dni pobytach jej samej oraz jej partnera/małżonka za granicą po ukończeniu przez nich 18 lat) i dostosowano go do zmian społeczno-politycznych ostatnich lat (integracja z UE). Natomiast kontakty dalszej rodziny, w szczególności powinowatych osoby sprawdzanej, i tak nie mogły mieć

znaczenia dla oceny dawania przez nią rękojmi zachowania tajemnicy. W podobny sposób i na podstawie tych samych przesłanek zmieniono zakres pytania o kontakty z obywatelami innych państw (w obecnie obowiązującej ankiecie pozostawiono tylko pytania o kontakty osoby sprawdzanej i jej partnera/małżonka).

W części V (*Dane dotyczące stanu zdrowia*) dodano pytanie o to, czy osoba sprawdzana stawała przed komisją wojskową (lub inną komisją służb mundurowych) w celu określenia stanu zdrowia, a jeśli tak, to jaki był tego rezultat. Pytanie o choroby psychiczne oddzielono od pytania o dolegliwości psychiczne. Złożone pytania o leczenie rozdzielono na krótkie precyzyjne pytania dodatkowe. Pytanie o zażywanie narkotyków zmieniono na pytanie o zażywanie środków odurzających lub substancji psychotropowych (i to bez zastrzeżenia, że pytanie nie dotyczy przypadków zażywania wyżej wymienionych środków z przepisu lekarza). Zmieniono redakcję punktu dotyczącego spożywania alkoholu – usunięto pytanie o przypadki zaburzeń świadomości (pozostawiono jedynie pytanie o przypadki utraty świadomości), przy czym określono, że chodzi o wszystkie przypadki po ukończeniu 18 roku życia, a nie tylko w okresie ostatnich 10 lat (w tym w okresie do ukończenia 18 roku życia). Zmieniono także brzmienie punktu odnośnie problemów związanych ze spożywaniem alkoholu – sprecyzowano, że chodzi tu tylko o przypadki, które miały miejsce po ukończeniu 18 roku życia. Dodano również pytanie o leczenie odwykowe związane z chorobą alkoholową.

Do części VI ankiety (*Dane dotyczące sytuacji majątkowo-finansowej*) z części odnoszących się do danych osobowych przesunięto pytanie o miesięczne wynagrodzenie oraz inne dochody i dodano pytanie o to, czy osoba sprawdzana składała oświadczenia o stanie majątkowym, a jeśli tak, to kiedy i komu. Wpisano również obowiązek wskazania danych osoby prowadzącej z osobą sprawdzaną wspólne gospodarstwo domowe (imię, nazwisko, PESEL, NIP, dochody roczne) oraz podania liczby osób pozostających na utrzymaniu osoby sprawdzanej. Rozdzielono punkt dotyczący posiadanych nieruchomości oraz firm i udziałów w firmach. W oddzielnym pytaniu o posiadane nieruchomości wprowadzono konieczność wskazania:

1) imienia i nazwiska właściciela nieruchomości,

2) nazwy i adresu nieruchomości,

3) nazwy dokumentu potwierdzającego nabycie nieruchomości,

4) udziału procentowego we własności nieruchomości,

5) źródła finansowania nabycia nieruchomości,

6) sposobu, daty i ceny nabycia nieruchomości.

W pytaniu o posiadane firmy lub udziały (akcje) firmy wprowadzono konieczność wskazania:

1) imienia i nazwiska właściciela firmy lub udziałów (akcji) firmy,

2) nazwy firmy,

3) udziału procentowego we własności firmy lub udziałach (akcjach) firmy,

4) źródła finansowania nabycia firmy lub udziałów (akcji) firmy,

5) sposobu, daty i ceny nabycia firmy lub udziałów (akcji) firmy,

6) obecnej szacunkowej wartości firmy lub udziałów.

Jednocześnie dodano pytania o posiadane ruchomości, których koszt nabycia wyniósł powyżej 20 000 złotych – według schematu szczegółowych pytań dotyczących nieruchomości – oraz o posiadane rachunki bankowe (także te, których osoba sprawdzana jest jedynie współposiadaczem). Pytanie w szczególności dotyczy nazwy i adresu banku oraz numeru rachunku. W pytaniu o zadłużenie wprowadzono konieczność wskazania:

1) imienia i nazwiska osoby posiadającej zobowiązanie,

2) nazwy zobowiązania,

3) nazwy dokumentu, na podstawie którego powstało zobowiązanie,

4) nazwy lub imienia i nazwiska wierzyciela,

5) całkowitej kwoty zobowiązania,

6) kwoty pozostałej do spłaty,

7) wysokości miesięcznej raty,

8) liczby rat pozostałych do spłaty,

9) daty powstania zobowiązania,

10) przewidywanego terminu spłaty zobowiązania.

Dodano także pytanie o problemy związane z udziałem w grach hazardowych po ukończeniu 18 roku życia.

W części VII ankiety (*Osoby polecające*) wpisano konieczność wskazania numeru PESEL, numeru telefonu kontaktowego oraz stanowiska zajmowanego przez osoby polecające.

Przepisy dotyczące kancelarii tajnych oraz środków bezpieczeństwa fizycznego

Kierownik jednostki organizacyjnej (a nie jak dotychczas jednostka organizacyjna), w której są przetwarzane informacje niejawne o klauzuli „tajne" lub „ściśle tajne", ma obowiązek utworzenia kancelarii tajnej (art. 42 ust. 1 ustawy).

Art. 42.

1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „tajne" lub „ściśle tajne", tworzy kancelarię, zwaną dalej „kancelarią tajną", i zatrudnia jej kierownika.

O utworzeniu lub likwidacji kancelarii tajnej, z podaniem klauzuli tajności przetwarzanych w niej informacji niejawnych, zgodnie z właściwością informuje się ABW lub SKW (art. 42 ust. 6).

6. Kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych.

Z obowiązku utworzenia kancelarii tajnej wyłączono jednostki, które przetwarzają materiały do poziomu „poufne". Dodatkowo zobowiązano kierownika jednostki organizacyjnej, w której przetwarzane są informacje niejawne o klauzuli „ściśle tajne" lub „tajne" do zatrudnienia kierownika kancelarii tajnej (art. 42 ust. 1).

W art. 42 ust. 3 wprowadzono nowe rozwiązanie polegające na możliwości, za zgodą ABW lub SKW, zorganizowania kancelarii tajnej obsługującej dwie

jednostki organizacyjne lub więcej. Powyższe rozwiązanie ma służyć przedsiębiorcom, którzy prowadzą więcej niż jeden podmiot gospodarczy oraz jednostkom, które posiadają niewielką liczbę dokumentów niejawnych. Warunkiem korzystania z kancelarii tajnej innego podmiotu będzie podpisanie stosowanego porozumienia pomiędzy kierownikami zainteresowanych jednostek organizacyjnych, regulującego podległość, obsadę i zasady finansowania takiej kancelarii.

> *3. W uzasadnionych przypadkach, za zgodą odpowiednio ABW lub SKW, można utworzyć kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych. Podległość, obsada i zasady finansowania takiej kancelarii zostaną określone przez właściwych kierowników jednostek organizacyjnych.*

Zwraca uwagę nowa redakcja definicji kancelarii tajnej (art. 42 ust. 4), która podkreśla, iż stanowi ona wyodrębnioną komórkę organizacyjną, a nie, jak dotąd przyjmowano, odpowiednio zabezpieczone pomieszczenie i komórkę organizacyjną.

> *4. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną, w zakresie ochrony informacji niejawnych podległą pełnomocnikowi ochrony, obsługiwaną przez pracowników pionu ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.*

Oczywiste jest, że kancelaria tajna, jako komórka organizacyjna odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom, musi być zlokalizowana w odpowiedniej strefie ochronnej (o której mowa w art. 46 pkt. 1 nowej ustawy). Środki bezpieczeństwa fizycznego odnosić się będą wówczas do zabezpieczania stref ochronnych, a nie kancelarii tajnej.

> **Art. 46.**
>
> *W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej należy w szczególności:*
>
> *1) zorganizować strefy ochronne;*
>
> *2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;*
>
> *3) określić uprawnienia do przebywania w strefach ochronnych;*
>
> *4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.*

W art. 42 ust. 5 zawarto przeniesiony z *Rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii*

tajnych (§ 10 ust. 3) zapis dotyczący możliwości przetwarzania w kancelarii tajnej, za zgodą kierownika jednostki organizacyjnej, informacji niejawnych o klauzuli „zastrzeżone" i – odtąd – „poufne".

> 5. *Kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne" lub „zastrzeżone".*

Bez zmian pozostawiono wymóg takiego zorganizowania pracy kancelarii tajnej, która umożliwi jednoznaczne ustalenie, gdzie dany dokument „tajny" lub „ściśle tajny" się znajduje (art. 43 ust. 1). Analogiczne wymogi wprowadzono dla dokumentów niejawnych o klauzuli „poufne", które będą przetwarzane poza kancelarią tajną, np. w punktach kancelaryjnych (art. 43 ust. 2).

> **Art. 43.**
>
> 1. *Organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne" lub „ściśle tajne" pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.*
> 2. *Przepis ust. 1 stosuje się odpowiednio do organizacji pracy innych niż kancelaria tajna komórek, w których są rejestrowane materiały o klauzuli „poufne".*
> 3. *Kierownik jednostki organizacyjnej zatwierdza, opracowany przez pełnomocnika ochrony sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych.*
> 4. *Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, zatwierdza opracowaną przez pełnomocnika ochrony dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.*
> 5. *Kierownik jednostki organizacyjnej zatwierdza, opracowaną przez pełnomocnika ochrony, instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.*
> 6. *Kancelaria tajna lub komórka, o której mowa w ust. 2, odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.*

Przepisy ustawy obligują pełnomocnika ochrony do opracowania, a kierownika jednostki do zatwierdzenia, dokumentacji regulującej kwestię sposobu i trybu przetwarzania informacji niejawnych o klauzulach „zastrzeżone" i „poufne" (art. 43 ust. 3 i 5). Jednocześnie wprowadzono nowe pojęcie środki bezpieczeństwa fizycznego, które zastąpiło pojęcie środki ochrony fizycznej, funkcjonujące w poprzedniej ustawie.

Szczególne znaczenie ma wprowadzone w art. 43 ust. 4 nowe pojęcie – p o z i o m z a g r o ż e ń. Na bazie nowych uregulowań kierownicy jednostek organizacyjnych, w których przetwarzane są informacje niejawne od klauzuli „pouf-

ne", będą mieli obowiązek określenia poziomu zagrożenia związanego z nieuprawnionym dostępem do informacji niejawnych lub ich utratą. Dopiero w zależności od określenia tego poziomu oraz od klauzuli posiadanych informacji, zostaną dobrane odpowiednie środki bezpieczeństwa fizycznego. Szczegółowy sposób określania poziomu zagrożenia oraz doboru środków bezpieczeństwa fizycznego zostanie przedstawiony w akcie wykonawczym.

W art. 44 ustawy (podobnie jak w art. 52a poprzedniej ustawy) dopuszczono możliwość organizowania w niektórych jednostkach organizacyjnych (przy czym katalog podmiotów zwiększono), innych niż kancelaria tajna, komórek odpowiedzialnych za przetwarzanie materiałów niejawnych. Jednocześnie w uzasadnionych przypadkach umożliwiono przejmowanie przez kierownika takiej komórki obowiązków pełnomocnika ochrony, z wyłączeniem możliwości prowadzenia postępowań sprawdzających. Powyższe rozwiązania wprowadzono głównie na potrzeby placówek zagranicznych podległych MSZ, ponieważ pełnomocnik ochrony MSZ, na podstawie dotychczas obowiązujących przepisów, nie miał realnego wpływu na zapewnienie przestrzegania regulacji dotyczących ochrony informacji niejawnych w placówkach zagranicznych.

Art. 44.

1. *W jednostkach organizacyjnych, o których mowa w art. 47 ust. 3, dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych. W uzasadnionych przypadkach obowiązki pełnomocnika ochrony, z wyłączeniem prowadzenia postępowań sprawdzających, może przejąć kierownik tej komórki organizacyjnej.*
2. *Do komórek organizacyjnych, o których mowa w ust. 1, przepisy art. 46 stosuje się odpowiednio.*

W art. 45 nowej ustawy, jak było wspomniane wyżej, powielono zapisy art. 56 poprzedniej ustawy z uwzględnieniem zmiany nazewnictwa ze środki ochrony fizycznej na środki bezpieczeństwa fizycznego. Jednocześnie w ust. 2 wskazano, iż zakres stosowania wyżej wymienionych środków uzależniony jest od poziomu zagrożenia. Z kolei w art. 45 ust. 3 wskazano, jakiego rodzaju elementy należy brać pod uwagę przy określaniu poziomu zagrożenia. Poza tym, ABW i SKW przyznano możliwość wpływania w uzasadnionych przypadkach na określanie poziomu zagrożenia danej jednostki. Powyższe uprawnienie jest szczególnie ważne w przypadku jednostek organizacyjnych o znaczeniu strategicznym dla bezpieczeństwa państwa. W związku z powyższym, ABW lub SKW będą mogły wskazywać dodatkowe czynniki, np. nieuwzględnione przez pełnomocnika ochrony, w istotny sposób wpływające na określenie poziomu zagrożenia, a tym samym determinujące zastosowanie odpowiednich środków bezpieczeństwa fizycznego.

Art. 45.

1. *Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:*

   1) działaniem obcych służb specjalnych;

   2) zamachem terrorystycznym lub sabotażem;

   3) kradzieżą lub zniszczeniem materiału;

   4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;

   5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

2. *Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.*

3. *Przy określaniu poziomu zagrożeń, o którym mowa w ust. 2, uwzględnia się w szczególności występujące rodzaje zagrożeń, klauzule tajności i liczbę informacji niejawnych. W uzasadnionych przypadkach przy określaniu poziomu zagrożeń uwzględnia się wskazania odpowiednio ABW lub SKW.*

Minimalne wymagania, jakie należy spełnić w celu zabezpieczenia dokumentów od klauzuli „poufne" wzwyż przed nieuprawnionym dostępem, określono w art. 46 ustawy. Zasadnicza zmiana w stosunku do przepisów obowiązujących polega na likwidacji stref administracyjnej oraz bezpieczeństwa. W zamian wprowadzono pojęcie *stref ochronnych.* Szczegółowy opis ich zabezpieczeń określi akt wykonawczy. Bez zmian pozostawiono zapisy dotyczące obowiązku wprowadzenia systemu kontroli wejść i wyjść ze stref ochronnych oraz określenia uprawnień do przebywania w tych strefach.

Ponadto, w punkcie 4 wykreślono zapis dotyczący świadectw kwalifikacyjnych. Powyższe wynika z rezygnacji wydawania tego typu dokumentów przez podmioty uprawnione. Aktualnie wydawane będą certyfikaty na wykorzystywanie urządzeń służących ochronie informacji niejawnych.

Art. 46.

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej należy w szczególności:

1) zorganizować strefy ochronne;

2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;

3) określić uprawnienia do przebywania w strefach ochronnych;

4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

W przepisach ustawy nie zawarto odpowiednika art. 58 poprzedniej ustawy. W związku z tym zrezygnowano z możliwości zorganizowania specjalnej strefy bezpieczeństwa. Odpowiednikiem tej strefy w nowych przepisach będzie wskazana i opisana jedna ze stref ochronnych.

Wśród przepisów dotyczących delegacji ustawowej do wydawania rozporządzeń w sprawie m.in. *organizacji i funkcjonowania kancelarii tajnych oraz przewożenia materiałów niejawnych* (art. 47) uwagę zwraca zawarte w ust. 4 uprawnienie ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego do wydawania zarządzeń dla archiwów państwowych, określających szczególny sposób i tryb przetwarzania informacji niejawnych przechowywanych w zasobie archiwalnym tych archiwów, dobór i stosowanie środków bezpieczeństwa fizycznego oraz organizację komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych.

Art. 47.

1. *Rada Ministrów określi, w drodze rozporządzenia:*

   1) podstawowe kryteria i sposób określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;

   2) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych;

   3) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;

   4) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;

   5) zakres stosowania środków bezpieczeństwa fizycznego;

   6) kryteria tworzenia stref ochronnych;

   7) strukturę organizacyjną kancelarii tajnej, z uwzględnieniem możliwości tworzenia jej oddziałów;

   8) podstawowe zadania kierownika kancelarii;

   9) sposób i tryb przetwarzania informacji niejawnych;

   10) wzór karty zapoznania się z dokumentem;

   11) wzory dzienników ewidencji.

2. *W rozporządzeniu, o którym mowa w ust. 1, Rada Ministrów uwzględni potrzebę racjonalizacji nakładów ponoszonych przez jednostki organizacyjne w zakresie tworzenia systemu bezpieczeństwa fizycznego informacji niejawnych, zgodnie z zasadami określonymi w ustawie.*

3. *Ministrowie właściwi do spraw wewnętrznych, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, Minister Obrony Narodowej, Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Pierwszy Prezes Sądu Najwyższego, Prokurator Generalny, Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego, Szef Cen-*

tralnego Biura Antykorupcyjnego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, a także Prezes Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, określą, w drodze zarządzenia, każdy w zakresie swojego działania, szczególny sposób organizacji i funkcjonowania kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 44 ust. 1, sposób i tryb przetwarzania informacji niejawnych oraz dobór i stosowanie środków bezpieczeństwa fizycznego.

4. *Minister właściwy do spraw kultury i ochrony dziedzictwa narodowego określi, w drodze zarządzenia, dla archiwów państwowych szczególny sposób i tryb przetwarzania informacji niejawnych wchodzących w skład zasobu archiwalnego tych archiwów, dobór i stosowanie środków bezpieczeństwa fizycznego oraz organizację komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych.*

5. *Prezes Rady Ministrów określi, w drodze rozporządzenia:*

   1) tryb i sposób nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów;

   2) sposób postępowania nadawców przesyłek zawierających informacje niejawne oraz wymogi, jakie muszą spełniać te przesyłki;

   3) sposób postępowania podmiotów, które wykonują zadania przewoźników tych materiałów, z przesyłkami zawierającymi informacje niejawne;

   4) sposób dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy;

   5) warunki ochrony i sposoby zabezpieczenia przesyłek przez przewoźnika oraz warunki, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby;

   6) sposób postępowania w przypadku zaistnienia nieprzewidzianych okoliczności mogących mieć wpływ na bezpieczeństwo przesyłki;

   7) warunki przewożenia materiałów poza granicami Rzeczypospolitej Polskiej.

6. *W rozporządzeniu, o którym mowa w ust. 5, Prezes Rady Ministrów uwzględni potrzebę zabezpieczenia materiałów przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem oraz szczególne warunki ochrony ze względu na rozmiary lub charakter materiału*

Przepisy dotyczące bezpieczeństwa przemysłowego

Zmiany dotyczące niezwykle istotnego obszaru systemu ochrony informacji niejawnych, jakim są procedury dotyczące przedsiębiorców, wprowadzono już w przepisach ogólnych – w art. 1 i art. 2 – i zostały omówione wcześniej. Zasadnicze znaczenie ma także dokonany w art. 10 podział właściwości między Agencję Bezpieczeństwa Wewnętrznego i Służbę Kontrwywiadu Wojskowego, w wyniku którego zdecydowanie ograniczono kompetencje SKW w ramach gwarantowania bezpieczeństwa przemysłowego. Obecnie SKW będzie realizować zadania wyłącznie wobec przedsiębiorców nadzorowanych przez MON i jednostki organizacyjne podległe ministrowi obrony narodowej lub przez niego nadzorowane, natomiast wobec wykonawców lub podwykonawców umów zlecanych przez te jednostki – nie będzie. Tym samym zwiększy się liczba wniosków kierowanych przez

przedsiębiorców do ABW, na której będzie spoczywała również odpowiedzialność za przeprowadzanie postępowań bezpieczeństwa przemysłowego wobec przedsiębiorców prowadzących działalność w sferze wojskowej.

W rozdziale 9 – *Bezpieczeństwo przemysłowe* (od art. 54 do 71) na uwagę zasługuje szczególnie zmiana zawarta w art. 54 ust. 2.

> 2. *Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej jest świadectwo bezpieczeństwa przemysłowego, zwane dalej „świadectwem", wydawane przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.*

W związku z odstąpieniem od dotychczasowego podziału informacji niejawnych na tajemnicę służbową i państwową, przy jednoczesnym nadaniu wyższej rangi informacjom o klauzuli „poufne", wprowadzono obowiązek uzyskiwania świadectwa bezpieczeństwa przemysłowego przez podmioty zamierzające realizować umowy lub zadania związane z dostępem do informacji niejawnych oznaczonych właśnie klauzulą „poufne" lub wyższą. Jest to rozwiązanie analogiczne do uregulowań stosowanych przez NATO i Unię Europejską. Przedsiębiorcy, którzy rozpoczęli realizację umów z dostępem do informacji niejawnych przed wejściem w życie ustawy i będą ją nadal realizować w okresie obowiązywania nowej ustawy, a nie posiadają świadectwa, są zobligowani do dnia 2 stycznia 2012 r. (art. 187).

> **Art. 187.**
>
> *Przedsiębiorcy wykonujący umowy związane z dostępem do informacji niejawnych o klauzuli „poufne", nieposiadający w dniu wejścia w życie ustawy ważnego świadectwa bezpieczeństwa przemysłowego powinni uzyskać takie świadectwo w terminie 12 miesięcy od dnia wejścia w życie ustawy.*

Istotną zmianą jest także odstąpienie od wymogu posiadania świadectwa bezpieczeństwa przemysłowego przez osoby fizyczne prowadzące działalność gospodarczą jednoosobowo i osobiście. Tego typu przedsiębiorcy zobowiązani są jedynie poddać się prowadzonemu przez ABW lub SKW postępowaniu sprawdzającemu, zmierzającemu do wydania poświadczenia bezpieczeństwa oraz do odbycia organizowanego przez te służby szkolenia w zakresie ochrony informacji niejawnych (art. 54 ust. 3).

> 3. *W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, wydawane przez ABW albo SKW, i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych wydawane przez ABW albo SKW.*

Wyjątek stanowią sytuacje, kiedy obowiązek uzyskania świadectwa bezpieczeństwa przemysłowego wynika z przepisów międzynarodowych. Taki zapis umożliwia elastyczne dostosowywanie się do wymogów zawartych w umowach bilateralnych lub przepisach organizacji międzynarodowych: jeżeli formułują one bezwzględny wymóg posiadania świadectwa bezpieczeństwa przemysłowego przez każdego bez wyjątku przedsiębiorcę, ABW lub SKW będzie przeprowadzała postępowanie bezpieczeństwa przemysłowego.

> *4. Przepisu ust. 3 nie stosuje się, jeżeli obowiązek uzyskania świadectwa wynika z ratyfikowanej przez Rzeczpospolitą Polską umowy międzynarodowej lub prawa wewnętrznego strony zawierającej umowę.*

Obowiązek posiadania świadectwa bezpieczeństwa przemysłowego dotyczy przedsiębiorców mających uzyskać dostęp do informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą. Nie wydaje się natomiast świadectw do poziomu „zastrzeżone". Przedsiębiorca uzyskujący dostęp do informacji oznaczonych klauzulą „zastrzeżone" jest zobowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych oznaczonych tą klauzulą, ale nie jest zobowiązany (tak jak to było dotychczas) do powoływania pełnomocnika ochrony w przypadku gdy wykonuje umowę związaną z dostępem do informacji niejawnych, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach (art. 54 ust. 9-10).

> *9. W przypadku gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", świadectwo nie jest wymagane.*
>
> *10. Przedsiębiorca, o którym mowa w ust. 9, jest obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone", z wyjątkiem wymogu zatrudnienia pełnomocnika ochrony, jeżeli wykonuje umowę związaną z dostępem do tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.*

Przepisy ustawy pozostawiają bez zmian trzy stopnie świadectw bezpieczeństwa przemysłowego. Przeredagowano (skrócono) natomiast definicje każdego ze stopni, ponieważ definicje: przedsiębiorcy, przetwarzania informacji niejawnych oraz systemów teleinformatycznych zostały zawarte w art. 2. Nowością jest przyjęcie funkcjonującego w postępowaniach osobowych modelu „kaskadowej" ważności uprawnień w zakresie ochrony informacji niejawnych. Oznacza to, że ważność tego samego świadectwa potwierdzającego zdolność do ochrony informacji niejawnych oznaczonych wyższą klauzulą jest odpowiednio dłuższa dla klauzul niższych. Zgodnie z przepisami poprzedniej ustawy

przedsiębiorca po upływie daty ważności określonej w świadectwie bezpieczeństwa przemysłowego zobowiązany był do ponownego ubiegania się o nie, nawet jeżeli zostało ono wydane do klauzuli „ściśle tajne", a podmiot nie zamierza realizować umów o klauzuli wyższej niż „tajne". Przedsiębiorca taki, zgodnie z przepisami nowej ustawy, nie będzie musiał występować z kolejnym wnioskiem o wydanie świadectwa przez okres kolejnych dwóch lat dla klauzuli „tajne" lub pięciu dla klauzuli „poufne" (art. 55 ust. 1 i 2).

Art. 55.

1. *W zależności od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej wydaje się świadectwo odpowiednio:*

   1) pierwszego stopnia - potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji;

   2) drugiego stopnia - potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;

   3) trzeciego stopnia - potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

2. *Świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli:*

   1) „ściśle tajne" potwierdza zdolność do ochrony informacji niejawnych o klauzuli:

   a) „ściśle tajne" - przez okres 5 lat od daty wystawienia,

   b) „tajne" - przez okres 7 lat od daty wystawienia,

   c) „poufne" - przez okres 10 lat od daty wystawienia;

   2) „tajne" potwierdza zdolność do ochrony informacji niejawnych o klauzuli:

   a) „tajne" - przez okres 7 lat od daty wystawienia,

   b) „poufne" - przez okres 10 lat od daty wystawienia;

   3) „poufne" potwierdza zdolność do ochrony informacji niejawnych o tej klauzuli przez okres 10 lat od daty wystawienia.

3. *ABW albo SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych o klauzuli stanowiącej zagraniczny odpowiednik klauzuli „tajne" lub „poufne", stosowany przez organizacje międzynarodowe. Przepis ust. 2 stosuje się odpowiednio.*

4. *Świadectwo wygasa, jeżeli:*

   1) upłynął okres jego ważności, o którym mowa w ust. 2;

   2) przedsiębiorca zrzekł się uprawnień określonych w świadectwie;

   3) przedsiębiorca został przejęty przez inny podmiot lub zlikwidowany.

„Kaskadę" ważności wprowadzono także dla świadectw wydanych na podstawie przepisów poprzedniej ustawy, ważnych w dniu wejścia w życie nowej ustawy (art. 186).

Art. 186.

1. *Świadectwa bezpieczeństwa przemysłowego wydane na podstawie przepisów dotychczasowych, ważne w dniu wejścia w życie ustawy, potwierdzające zdolność do ochrony informacji niejawnych:*

   1) o klauzuli „ściśle tajne" - potwierdzają także zdolność do ochrony informacji niejawnych o klauzuli „tajne" i „poufne" w okresie wskazanym w niniejszej ustawie;

   2) o klauzuli „tajne" - potwierdzają także zdolność do ochrony informacji niejawnych o klauzuli „poufne" w okresie wskazanym w niniejszej ustawie.

2. *Okresy ważności świadectw, o których mowa w ust. 1, liczone są od daty wydania świadectwa.*

Przepisy ustawy określają wprost, że w przypadku przedsiębiorców zamierzających uzyskać dostęp do informacji niejawnych organizacji międzynarodowych (np. NATO i Unii Europejskiej) oznaczonych odpowiednikiem klauzuli „poufne" lub „tajne" wydawane są świadectwa odrębne. Dotychczasowe przepisy wskazywały na to pośrednio – w rozporządzeniu w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectw bezpieczeństwa przemysłowego oraz decyzji o odmowie i cofnięciu świadectwa występują odrębne wzory świadectw potwierdzających zdolność do ochrony informacji niejawnych Unii Europejskiej i NATO (art. 55 ust. 3).

Zgodnie z art. 55 ust. 4 ustawy w przypadku połączenia dwóch podmiotów, np. spółek prawa handlowego poprzez przejęcie podmiotu przejmowanego przez podmiot przejmujący, świadectwo nie przechodzi na podmiot przejmujący (odmiennie niż np. w przypadku zezwoleń i koncesji posiadanych przez podmiot przejmowany, które zgodnie z odrębnymi przepisami przechodzą na podmiot przejmujący). Do wygaśnięcia świadectwa dochodzi również wtedy, gdy przedsiębiorca zrzeka się uprawnień określonych w tym świadectwie lub zostaje zlikwidowany albo upływa okres ważności, z uwzględnieniem ważności „kaskadowej".

Tryb wnioskowania o przeprowadzenie postępowania bezpieczeństwa przemysłowego nie uległ zasadniczej zmianie. Wniosek składa we własnym imieniu przedsiębiorca. Przepisy ustawy wskazują jednak wprost, że wniosek nie musi zawierać uzasadnienia. Ważniejszą zmianą jest wprowadzenie 30-dniowego terminu (licząc od dnia otrzymania wezwania) na usunięcie ewentualnych braków formalnych we wniosku i jego załącznikach (art. 56 ust. 4). Powyższy termin jest dłuższy niż określone w kodeksie postępowania administracyjnego 7 dni, dzięki czemu przedsiębiorca wnioskujący o wszczęcie postępowania bezpieczeństwa przemysłowego będzie miał więcej czasu na przekazanie brakujących danych. W dalszym ciągu oczywiście, na podstawie art. 3 ustawy, który odwołuje się do wybranych przepisów kodeksu postępowania administracyjnego, przedsiębiorca może wnosić o przywrócenie terminu, jeżeli uprawdopodobni, że jego niedotrzymanie nie wynikało z jego winy.

Ustawa wskazuje jednoznacznie, że postępowanie bezpieczeństwa przemysłowego to nie tylko sprawdzenia przedsiębiorcy, ale również postępowania sprawdzające wobec osób objętych wnioskiem przedsiębiorcy (art. 57 ust. 1). Ważną zmianą jest także wyraźne wskazanie, że postępowania sprawdzające przeprowadza się nie tylko w trakcie postępowania bezpieczeństwa przemysłowego, ale również w okresie ważności świadectwa (zgodnie z poprzednią ustawą postępowania sprawdzające prowadzone były tylko w ramach postępowania bezpieczeństwa przemysłowego).

Art. 57.

1. *Postępowanie bezpieczeństwa przemysłowego obejmuje sprawdzenie przedsiębiorcy i postępowania sprawdzające wobec osób wymienionych w ust. 3.*
2. *Sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, obejmuje:*

   1) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową;

   2) strukturę organizacyjną;

   3) system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego;

   4) wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia;

   5) w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa.
3. *W toku postępowania bezpieczeństwa przemysłowego oraz w okresie ważności świadectwa przeprowadza się postępowania sprawdzające wobec osób nieposiadających odpowiednich poświadczeń bezpieczeństwa lub kolejne postępowania sprawdzające wobec:*

   1) kierownika przedsiębiorcy;

   2) pełnomocnika ochrony i jego zastępcy;

   3) osób zatrudnionych w pionie ochrony;

   4) administratora systemu teleinformatycznego;

   5) pozostałych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych.
4. *W stosunku do osób, o których mowa w ust. 3 pkt 1-4, odpowiednie poświadczenie bezpieczeństwa oznacza poświadczenie upoważniające do dostępu do informacji niejawnych o klauzuli nie niższej niż wskazana we wniosku przedsiębiorcy o wydanie świadectwa.*

Uwagę zwraca także poszerzenie katalogu osób, wobec których przeprowadza się postępowania sprawdzające: dodano do niego pełnomocnika ochrony oraz jego zastępcę. Zrezygnowano natomiast z dość nieczytelnego rozróżnienia na osoby uczestniczące w czynnościach zmierzających do zawarcia umowy oraz osoby mające kierować wykonaniem umowy lub zadania albo uczestniczyć w ich bez-

pośredniej realizacji. Zamiast tych dwóch kategorii osób pojawia się ogólny zapis wskazujący inne osoby, wymienione w kwestionariuszu bezpieczeństwa przemysłowego jako te, które powinny mieć dostęp do informacji niejawnych (art. 57 ust. 3).

Istotną zmianą jest doprecyzowanie, jaka klauzula tajności powinna być określona w poświadczeniu bezpieczeństwa osób pełniących funkcje związane z ochroną informacji niejawnych (kierownik przedsiębiorcy, pełnomocnik ochrony i jego zastępca, pracownik pionu ochrony, administrator systemu teleinformatycznego). Nowy zapis mówi, że nie może być ona niższa od klauzuli tajności określonej w świadectwie bezpieczeństwa przemysłowego (art. 57 ust. 4).

Równie ważna jest modyfikacja zawarta w art. 58 ust. 1 – tj. uwzględnienie możliwości prowadzenia sprawdzeń na podstawie informacji innych niż dane zawarte w kwestionariuszu bezpieczeństwa przemysłowego. W ten sposób prawnie usankcjonowano sprawdzenia oparte np. na informacjach uzyskanych ze źródeł otwartych, które mogą mieć znaczenie z punktu widzenia oceny zdolności podmiotu do ochrony informacji niejawnych (np. informacje mogące wskazywać na pogorszenie się sytuacji finansowej podmiotu, powstanie zobowiązań finansowych, wszczęcie postępowań karnych).

Korzystne dla przedsiębiorców rozwiązanie przyniosła zmiana wprowadzona w art. 60 ust. 1, zgodnie z którym w przypadku ubiegania się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia (przedsiębiorca nie będzie przetwarzał informacji niejawnych we własnych obiektach) nie ma obowiązku powoływania pełnomocnika ochrony ani tworzenia pionu ochrony. Wyjątkiem jest ubieganie się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne" lub „poufne", stosowanym przez organizacje międzynarodowe (np. NATO i Unię Europejską).

Art. 60.

1. *W przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa, o którym mowa w art. 55 ust. 1 pkt 3, zatrudnienie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne" lub „poufne", stosowanym przez organizacje międzynarodowe.*

Przepisy ustawy umożliwiają (podobnie jak to było poprzednio) przeprowadzanie przez pełnomocników ochrony jednostek zlecających wykonanie umów lub zadań postępowań sprawdzających do poziomu „poufne" wobec pracowników przedsiębiorcy posiadającego świadectwo trzeciego stopnia oraz szkolenie tych

osób w zakresie ochrony informacji niejawnych. Należy jednak zwrócić uwagę, że jest to możliwość, a nie obowiązek, dlatego też przedsiębiorca posiadający świadectwo trzeciego stopnia, mimo iż nie jest zobowiązany powoływać pełnomocnika ochrony, w sytuacji, gdy jednostka zlecająca wykonanie umowy odmówi przeprowadzenia postępowań sprawdzających, i tak będzie zmuszony do powołania takiego pełnomocnika. Dotychczas w praktyce możliwość przeprowadzania postępowań przez pełnomocnika ochrony jednostki zlecającej umowę dotyczyła tylko okresu poprzedzającego rozpoczęcie faktycznej realizacji umowy przez przedsiębiorcę (zamiar ubiegania się lub ubieganie się o realizację umowy). Zgodnie z przepisami nowej ustawy możliwość ta istnieje na każdym etapie działań związanych z umową, począwszy od momentu jej podpisania lub podpisania wstępnego porozumienia o jej zawarciu, aż do zakończenia jej realizacji.

Przepisy ustawy utrzymały zasadę odpłatności za podejmowane przez ABW lub SKW czynności, tj. za przeprowadzanie postępowań bezpieczeństwa przemysłowego oraz postępowań sprawdzających wobec osób – pracowników podmiotu sprawdzanego lub posiadającego ważne świadectwo bezpieczeństwa przemysłowego. Silniej jednak zaakcentowano związek tej odpłatności z kosztami ponoszonymi przez ABW lub SKW na przeprowadzanie czynności w ramach realizacji postępowań sprawdzających (termin *opłata* zastąpiono terminem *zwrot zryczałtowanych kosztów przeprowadzenia czynności* – art. 61[17]). Ważną zmianą jest wskazanie, iż dodatkowej odpłatności nie podlegają postępowania wobec osób posiadających ważne poświadczenia bezpieczeństwa wydane przez ABW i SKW, w przypadku których skierowano wniosek o przeprowadzenie postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej. W tego rodzaju sytuacji poświadczenie bezpieczeństwa organizacji międzynarodowej wydawane jest na okres ważności już posiadanego poświadczenia (art. 61 ust. 1). Opłacie nie podlega również przeprowadzenie postępowania kontrolnego wszczynanego po stwierdzeniu faktów mogących wskazywać na to, że osoba posiadająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy (dotychczasowe przepisy nie były w tej materii jednoznaczne, aczkolwiek interpretowano je właśnie w powyższy sposób).

Art. 61.

1. Za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających wo-

[17] Wysokość zryczałtowanych kosztów nie powinna przekroczyć 7-krotności kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 *Ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich.*

bec osób wymienionych w art. 57 ust. 3, z wyjątkiem postępowań sprawdzających, o których mowa w art. 32 ust. 4 i art. 33 ust. 1, ABW albo SKW przysługuje zwrot zryczałtowanych kosztów przeprowadzenia czynności przy sprawdzeniach przedsiębiorcy oraz postępowań sprawdzających.

2. *Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość zryczałtowanych kosztów, o których mowa w ust. 1, oraz tryb ich zwrotu, uwzględniając, że wysokość kosztów nie powinna przekroczyć 7-krotności kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich.*

Przepisy poprzedniej ustawy – poprzez odesłanie w art. 1 ust. 4 do art. 105 kpa – umożliwiały umorzenie przez ABW lub SKW postępowania bezpieczeństwa przemysłowego w przypadku, gdy wystąpiła o to strona, na której żądanie (wniosek) postępowanie zostało wszczęte (umorzenie na wniosek – art. 105 § 2 kpa) oraz w przypadku, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe (umorzenie z urzędu – art. 105 § 1 kpa). Obecnie obowiązująca ustawa określa w art. 62 ustawy przesłanki umorzenia postępowania tj.:

- wycofanie wniosku o wydanie świadectwa przez przedsiębiorcę (rezygnacja z ubiegania się o świadectwo bezpieczeństwa przemysłowego),

- wydanie orzeczenia o zakazie prowadzenia przez przedsiębiorcę działalności gospodarczej (zakaz taki może być wydany m.in. przez sąd za popełnienie przestępstwa skarbowego; w przypadku działalności regulowanej zakaz wydaje właściwy podmiot prowadzący rejestr tej działalności, np. UKE w stosunku do operatorów telekomunikacyjnych, zaś w przypadku oddziałów lub przedstawicielstw przedsiębiorcy zagranicznego – minister właściwy do spraw gospodarki),

- przejęcie lub likwidacja przedsiębiorcy (podmiot przejmujący nie może zatem żądać kontynuowania postępowania bezpieczeństwa przemysłowego prowadzonego do chwili przejęcia wobec spółki przejmowanej).

Wprowadzono obowiązek zawieszenia, a następnie podjęcia, postępowania przemysłowego na wniosek strony (art. 63). Jednocześnie ustanowiono katalog okoliczności, przy wystąpieniu których ABW lub SKW może zawiesić prowadzone postępowanie. Jest to korzystne dla przedsiębiorcy ubiegającego się o świadectwo bezpieczeństwa przemysłowego, ponieważ umożliwia zawieszenie postępowania w sytuacjach, gdy jednoznaczna ocena zdolności do ochrony informacji niejawnych nie jest w danym momencie możliwa (np. w sytuacjach: wydania przez

inny organ decyzji nakazującej przedsiębiorcy wstrzymanie prowadzenia działalności gospodarczej, wszczęcia postępowania upadłościowego wobec przedsiębiorcy, nieuregulowania w terminie zobowiązań publicznoprawnych, uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd).

Art. 63.

1. *ABW albo SKW zawiesza lub podejmuje postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3, na wniosek przedsiębiorcy.*
2. *ABW albo SKW może z urzędu zawiesić postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3, w przypadku:*

   1) wydania przez inny organ decyzji nakazującej przedsiębiorcy wstrzymanie prowadzenia działalności gospodarczej;

   2) wszczęcia postępowania upadłościowego wobec przedsiębiorcy;

   3) nieuregulowania w terminie zobowiązań publicznoprawnych;

   4) uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd.
3. *ABW albo SKW podejmuje z urzędu postępowanie bezpieczeństwa przemysłowego, w tym postępowania sprawdzające wobec osób wymienionych w art. 57 ust. 3, zawieszone na podstawie ust. 2, po ustaniu przyczyn zawieszenia.*

Przepisy poprzedniej ustawy stanowiły, że świadectwo bezpieczeństwa przemysłowego wydawane jest w przypadku pozytywnego wyniku postępowania bezpieczeństwa przemysłowego. Korzystając z tego samego przepisu, na zasadzie wnioskowania *a contrario*, wyprowadzano zapis, że negatywny wynik postępowania pociąga za sobą wydanie decyzji o odmowie wydania świadectwa. Jednocześnie jako przesłankę fakultatywną do wydania decyzji o odmowie wydania świadectwa przyjęto świadome podanie nieprawdziwych danych lub ich zatajenie w kwestionariuszu albo niewywiązanie się z tzw. obowiązków informacyjnych wobec służby prowadzącej postępowanie bezpieczeństwa przemysłowego.

Nowa ustawa enumeratywnie wymienia sytuacje, w jakich postępowanie bezpieczeństwa przemysłowego kończy się wydaniem decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, w tym między innymi brak poświadczenia bezpieczeństwa (wynikające z odmowy jego wydania lub cofnięcia) przez kierownika przedsiębiorcy, brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych (np. w przypadku spółek finansowanych przez podmioty zagraniczne). Podstawą do odmowy wydania świadectwa będzie również podanie w kwestionariuszu nieprawdziwych danych albo ich zatajenie, ale również – co stanowi racjonalne uzupełnienie – podanie nieprawdziwych danych

o zmianach zawartych w kwestionariuszu. ABW lub SKW może również odmówić przedsiębiorcy wydania świadectwa pierwszego lub drugiego stopnia, jeżeli nie zorganizuje on w terminie 6 miesięcy od daty wszczęcia postępowania kompleksowego systemu ochrony informacji niejawnych (w praktyce przedsiębiorcy częstokroć ubiegali się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych przetwarzanych w ich obiektach, nie posiadając systemu fizycznej ochrony informacji niejawnych, wskutek czego zakończenie postępowania w znacznym stopniu opóźniało się z winy wnioskodawcy).

Istotną modyfikacją odnoszącą się do przesłanek fakultatywnych wydania decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego jest wprowadzenie możliwości wydania takiej decyzji w przypadku niedających się usunąć wątpliwości dotyczących osób wchodzących w skład organów zarządzających, kontrolnych lub osób działających z ich upoważnienia, w zakresie:

- uczestnictwa, współpracy lub popierania przez te osoby działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej,
- zagrożenia tych osób ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nimi kontaktu,
- przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim ustalenia, czy osoby te uczestniczyły lub uczestniczą w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, albo współpracowały lub współpracują z takimi partiami lub organizacjami,
- wystąpienia związanych z tymi osobami okoliczności powodujących ryzyko ich podatności na szantaż lub wywieranie presji.

Wydaniem decyzji o odmowie wydania świadectwa może również skutkować niepowiadomienie w terminie 30 dni (ustalono termin na wniesienie powiadomienia, zastępując nim nie do końca precyzyjne określenie „niezwłoczne informowanie") o zmianach danych zawartych w kwestionariuszu bezpieczeństwa przemysłowego (art. 64 ust. 3).

2. ABW albo SKW odmawia wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych, z powodu:

1) odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom,

które zajmują stanowisko kierownika przedsiębiorcy;

2) braku możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;

3) niezorganizowania, w terminie 6 miesięcy od daty wszczęcia postępowania, kompleksowego systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia;

4) zatajenia danych w kwestionariuszu lub podania w nim danych nieprawdziwych;

5) podania nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu.

3. ABW albo SKW może odmówić wydania świadectwa, stwierdzając brak zdolności do ochrony informacji niejawnych, z powodu:

1) ujawnienia, w wyniku sprawdzenia osób wymienionych w art. 57 ust. 2 pkt 4, w toku postępowania bezpieczeństwa przemysłowego niedających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1–3 lub 5 lub w art. 24 ust. 3;

2) niepowiadomienia w terminie 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania bezpieczeństwa przemysłowego.

Utrzymana została możliwość przeprowadzenia z urzędu wybranych sprawdzeń lub sprawdzenia w pełnym zakresie przedsiębiorcy posiadającego ważne świadectwo bezpieczeństwa przemysłowego. Wprowadzono jednak zmianę dotyczącą możliwości zainicjowania sprawdzeń lub przeprowadzenia kontroli podmiotu posiadającego świadectwo na wniosek służby, która nie wydała świadectwa oraz uczestniczenia jej funkcjonariuszy lub żołnierzy w tych czynnościach. SKW może wnioskować o przeprowadzenie kontroli lub sprawdzeń w przypadku podmiotu posiadającego ważne świadectwo wydane przez ABW, jeżeli w związku z realizacją przez ten podmiot umowy (umów) na rzecz jednostki (jednostek) organizacyjnej podległej ministrowi obrony narodowej lub przez niego nadzorowanej, ujawni fakty wskazujące na możliwość utraty zdolności do ochrony informacji niejawnych. Analogicznie ABW może wystąpić z wnioskiem o przeprowadzenie przez SKW sprawdzeń lub kontroli w przypadku podmiotu posiadającego świadectwo wydane przez SKW, który realizuje umowę (umowy) na rzecz jednostek organizacyjnych, które nie podlegają ministrowi obrony narodowej ani nie są przez niego nadzorowane. Funkcjonariusze ABW lub żołnierze i funkcjonariusze SKW mogą zapoznać się, w zakresie dotyczącym sprawdzeń lub kontroli, z aktami postępowania bezpieczeństwa przemysłowego prowadzonego wobec tego podmiotu przez drugą ze służb.

Wprowadzając przesłanki do wydania decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, w pierwszej kolejności wskazano na wyniki sprawdzeń podejmowanych z urzędu lub na wyniki przeprowadzonej kontroli (art. 66 ust. 1).

Art. 66.

1. Wyniki sprawdzenia przedsiębiorcy z urzędu lub ustalenia kontroli ochrony informacji niejawnych mogą stanowić podstawę wydania decyzji o cofnięciu świadectwa.

Ponadto, podstawę takiej decyzji stanowić mogą: ujawnienie w wyniku sprawdzeń osób wymienionych w art. 57 ust. 2 pkt 4, w toku postępowania bezpieczeństwa przemysłowego, nie dających się usunąć wątpliwości dotyczących dawania rękojmi zachowania tajemnicy oraz niewykonanie przez przedsiębiorcę obowiązku, o którym mowa w art. 70 ust. 1. Warto przy tym zwrócić uwagę, że wyżej wymienione przepisy wskazują na możliwość, a nie na konieczność, wydania takiej decyzji. Jako przesłanki obligatoryjnie skutkujące decyzją o cofnięciu świadectwa bezpieczeństwa przemysłowego wskazano brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy, utratę funkcjonalności systemu ochrony informacji niejawnych oraz podanie nieprawdziwych danych lub ich zatajenie w ramach przekazywanych ABW albo SKW informacji o zmianach danych zawartych w kwestionariuszu.

Art. 70.

1. Przedsiębiorca, w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa, ma obowiązek informowania w terminie 30 dni odpowiednio ABW lub SKW o:

1) zmianach danych zawartych w kwestionariuszu, ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formie zakończenia przez nią działalności, wypowiedzeniu umowy oraz zakończeniu wykonywania umowy;

2) zawarciu umowy związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, ze szczególnym uwzględnieniem nazwy i adresu jednostki organizacyjnej zawierającej umowę, przedmiotu umowy oraz najwyższej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy, wypowiedzeniu tej umowy oraz zakończeniu jej wykonywania;

3) zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, wypowiedzeniu tej umowy oraz zakończeniu jej wykonywania.

Zasadniczą zmianą dotyczącą danych, które powinny zostać zawarte w świadectwie, decyzji o odmowie wydania lub o cofnięciu świadectwa, jest wymóg podania numerów KRS i REGON sprawdzanego podmiotu, przy czym konieczność podania numeru KRS dotyczy oczywiście tych podmiotów, które z mocy prawa podlegają obowiązkowi wpisu do właściwego rejestru prowadzonego w ramach

KRS. Te dodatkowe informacje pozwalają jednoznacznie identyfikować podmiot wymieniony w świadectwie, nawet w przypadku zmiany firmy, pod jaką przedsiębiorca prowadzi działalność, która to nastąpiła po wydaniu dokumentu (art. 67).

Art. 67.

1. *Świadectwo, decyzja o odmowie wydania świadectwa oraz decyzja o cofnięciu świadectwa powinny zawierać:*

   1) oznaczenie organu, który wydał, odmówił wydania bądź cofnął świadectwo;

   2) wskazanie miejsca i daty wystawienia;

   3) nazwę podmiotu, adres jego siedziby, numer w Krajowym Rejestrze Sądowym i numer REGON;

   4) podstawę prawną;

   5) stwierdzenie wydania świadectwa, odmowy wydania lub jego cofnięcia;

   6) w przypadku wydania świadectwa - jego stopień, klauzulę tajności oraz termin ważności;

   7) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW.

2. *Decyzja o odmowie wydania oraz decyzja o cofnięciu świadectwa powinny zawierać uzasadnienie faktyczne i prawne oraz pouczenie o dopuszczalności i terminie wniesienia:*

   1) odwołania do Prezesa Rady Ministrów;

   2) skargi do sądu administracyjnego.

3. *Uzasadnienie faktyczne w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w niniejszej ustawie.*

W przypadku decyzji o odmowie wydania świadectwa lub o jego cofnięciu zmianie ulega regulacja odnosząca się do uzasadnienia faktycznego decyzji (art. 67 ust. 2). W poprzedniej ustawie można było odstąpić od tego typu uzasadnienia lub je ograniczyć do zakresu, w jakim jego udostępnienie nie mogłoby spowodować zagrożenia dla podstawowych interesów RP dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych. Powyższe przesłanki uzasadniające odstąpienie od uzasadnienia lub jego ograniczenie nawiązywały wprost do definicji tajemnicy państwowej określonej w art. 2 pkt 1 poprzedniej ustawy. Obecnie uzasadnienie decyzji, które w całości lub w części zawiera informacje niejawne, nie będzie w tej decyzji zamieszczane.

Postępowania bezpieczeństwa przemysłowego wszczęte i niezakończone przed wejściem w życie ustawy będą prowadzone na podstawie przepisów poprzedniej ustawy (art. 188).

Art. 188.

Do postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

Przepisy dotyczące ewidencji i udostępniania danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

Podstawowa zmiana w ustawie dotycząca postępowania z materiałami i danymi zgromadzonymi w związku z postępowaniami sprawdzającymi i kontrolnymi postępowaniami sprawdzającymi oraz postępowaniami bezpieczeństwa przemysłowego polega na tym, że zagadnienia te zgromadzono w jednym, wyodrębnionym rozdziale 10 – *Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego.* W przypadku poprzedniej ustawy przedmiotowe kwestie umieszczono w różnych rozdziałach, w odległych od siebie jednostkach redakcyjnych[18].

W znowelizowanej ustawie omawiane problemy ujęto w dwóch artykułach, przy czym art. 72 w sposób kompleksowy określa sposób postępowania z aktami procedur przeprowadzonych wobec osób i przedsiębiorców, natomiast art. 73 – kwestie związane z prowadzeniem przez ABW i SKW ewidencji z zakresu bezpieczeństwa osobowego.

Art. 72.

1. *Akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez służby i instytucje uprawnione do prowadzenia poszerzonych postępowań sprawdzających i akta postępowań bezpieczeństwa przemysłowego są udostępniane do wglądu lub przekazywane wyłącznie na pisemne żądanie:*

   1) sądowi lub prokuratorowi dla celów postępowania karnego;

   2) służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego wobec tej samej osoby;

   3) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5;

   4) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia;

   5) sądowi administracyjnemu w związku z rozpatrywaniem skargi.

[18] Art. 42 ust. 2-8 oraz art. 75 poprzedniej ustawy.

2. *Przepisu ust. 1 pkt 2 nie stosuje się w odniesieniu do akt postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez AW, ABW, SKW lub SWW. Akta tych postępowań mogą być udostępnione do wglądu wyłącznie dla celów postępowania sprawdzającego prowadzonego przez tę samą służbę wobec tej samej osoby.*

3. *Akta zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających, mogą być udostępnione do wglądu i przekazane w przypadkach określonych w ust. 1 oraz dla celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego wobec tej samej osoby.*

4. *Akta zakończonych zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających, mogą być udostępnione do wglądu osobie sprawdzanej, z wyłączeniem danych dotyczących osób trzecich.*

5. *Po wykorzystaniu akta są niezwłocznie zwracane.*

6. *Po zakończeniu postępowania sprawdzającego, kontrolnego postępowania sprawdzającego lub postępowania bezpieczeństwa przemysłowego akta tych postępowań są przechowywane przez co najmniej 20 lat, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2006 r. Nr 97, poz. 673, z późn. zm.13)) oraz aktów wykonawczych wydanych na jej podstawie:*

   1) jako wyodrębniona część w archiwach służb i instytucji, które przeprowadziły te postępowania;

   2) przez pełnomocnika ochrony lub w pionie ochrony - w przypadku akt zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających przeprowadzonych przez tego pełnomocnika.

7. *W przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej akta, o których mowa w ust. 6, przejmuje następca prawny, a w przypadku jego braku - ABW albo SKW.*

Art. 73.

1. *ABW i SKW prowadzą ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej oraz ewidencję osób, którym odmówiono wydania poświadczenia bezpieczeństwa, a także osób, wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w podmiotach, o których mowa w art. 23 ust. 5.*

2. *Dane z ewidencji, o których mowa w ust. 1, mogą obejmować wyłącznie:*

   1) imię i nazwisko;

   2) numer PESEL;

   3) imię ojca;

   4) datę i miejsce urodzenia;

   5) adres miejsca zamieszkania lub pobytu;

   6) nazwę jednostki organizacyjnej;

   7) określenie dokumentu kończącego procedurę, datę wydania oraz numer.

3. *Dane z ewidencji, o których mowa w ust. 1, oraz wykazów, o których mowa w art. 15 ust. 1 pkt 8, są udostępniane na pisemne żądanie wyłącznie w przypadkach określonych w art. 72 ust. 1 pkt 1 i 3-5 oraz służbom i instytucjom uprawnionym do realizacji poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego oraz postępowania bezpieczeństwa przemysłowego.*

Zgodnie z przyjętymi rozwiązaniami zarówno akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez organy i służby uprawnione do prowadzenia poszerzonych postępowań sprawdzających, jak i akta postępowań bezpieczeństwa przemysłowego przeprowadzonych przez ABW i SKW udostępniane są do wglądu lub przekazywane wyłącznie na pisemne żądanie wskazanych podmiotów w pięciu określonych przypadkach (zamknięty katalog):

1) sądowi lub prokuratorowi dla celów postępowania karnego,

2) służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających wobec tej samej osoby,

3) właściwemu organowi, w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5,

4) właściwemu organowi, w celu rozpatrzenia odwołania lub zażalenia,

5) sądowi administracyjnemu, w związku z rozpatrywaniem skargi.

W stosunku do dotychczasowego stanu prawnego wprowadzono także szereg innych zmian. Ustawodawca zastrzegł, że dokumenty mogą być albo udostępniane do wglądu albo przekazane (do tej pory stosowano jedynie pojęcie udostępnienia − w przypadku akt procedur zrealizowanych przez służby, określone w art. 30 poprzedniej ustawy lub udostępnienie do wglądu − w przypadku akt postępowań przeprowadzonych przez pełnomocników ochrony). W praktyce pojawiły się wątpliwości, czy pojęcie udostępnienia zawiera w sobie także znaczenie *przesłania akt do innej jednostki organizacyjnej w celu dokonania tamże ich przeglądu*.

Ponadto, określając przypadki uzasadniające udostępnienie do wglądu lub przekazanie akt zrezygnowano z zastrzeżenia, że dotyczy to procedur „zakończonych". W ustawie przyjęto także, że akta postępowań bezpieczeństwa przemysłowego (do których realizacji uprawnione są nadal wyłącznie ABW i SKW) udostępniane są w przypadku zaistnienia tych samych okoliczności i w tym samym trybie, co akta postępowań sprawdzających i kontrolnych postępowań sprawdzających. Oznacza to m.in., że ustawodawca nie uznał za stosowne utrzymanie występującego w poprzedniej ustawie uprawnienia Prezydenta RP i Prezesa Rady Ministrów do zapoznawania się z aktami postępowań bezpieczeństwa przemysłowego gdy wymaga tego *istotny interes Rzeczypospolitej Polskiej*.

Rozszerzenie katalogu przypadków, w których może nastąpić udostępnienie do wglądu lub przekazanie akt postępowań sprawdzających, kontrolnych po-

stępowań sprawdzających i akt postępowań bezpieczeństwa przemysłowego o sytuacje związane z przeprowadzeniem kontroli prawidłowości postępowania oraz z rozpatrywaniem zażalenia wynika z wprowadzenia do ustawy tych instytucji[19].

Co istotne, w art. 72 ust. 1 pkt 3 ustawy wskazano (normę tę wprowadzono w art. 12 ust. 3 ustawy), że spod kontroli prawidłowości przeprowadzonego postępowania, a co za tym idzie – z prawa do wglądu na tej podstawie – wyłączone są akta postępowań przeprowadzonych przez organy i służby wymienione w art. 23 ust. 5 ustawy (tj. AW, CBA, BOR, Policję, Służbę Więzienną, SWW, Straż Graniczną oraz Żandarmerię Wojskową).

Szczególnie ważne zastrzeżenie zawarto w art. 72 ust. 2, który stanowi wprost, że akta postępowań sprawdzających i kontrolnych postępowań sprawdzających przeprowadzonych przez AW, ABW, SKW lub SWW mogą być udostępnione *wyłącznie dla celów postępowania sprawdzającego prowadzonego przez tę samą służbę wobec tej samej osoby*. Oznacza to, że żadna inna służba nie będzie miała dostępu do akt postępowania przeprowadzonego przez wyżej wymienione służby.

Dwie poważne zmiany znalazły się po za tym w przepisach odnoszących się do udostępniania do wglądu lub przekazywania akt zwykłych postępowań sprawdzających i kontrolnych postępowań sprawdzających zrealizowanych przez pełnomocników ochrony. Przede wszystkim uznano, że z przedmiotowymi aktami, poza przypadkami określonymi w art. 72 ust. 1, można zapoznać się także dla celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, ale dotyczy to tylko postępowania prowadzonego wobec tej samej osoby.

Chociaż utrzymano możliwość zapoznania się przez osobę sprawdzaną z aktami przeprowadzonego wobec niej przez pełnomocnika ochrony zwykłego postępowania sprawdzającego, to wprowadzono ograniczenie, że prawo to nie dotyczy *danych dotyczących osób trzecich*. Przepis ten należy traktować jako kolejne wyrażenie ogólnej intencji projektodawców, aby zabezpieczyć prawa osób trzecich, których dane gromadzone są w ramach procedur określonych w ustawie (vide także art. 24 ust. 9 nowej ustawy).

Za niezwykle istotne należy uznać określenie przez ustawodawcę w art. 72 ust. 6 minimalnego okresu przechowywania akt zakończonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa

[19] Zażalenie na postanowienie o zawieszeniu postępowania – art. 27 ust. 4 znowelizowanej ustawy o ochronie informacji niejawnych; kontrola w zakresie prawidłowości postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego – art. 12 ust. 3 wyżej wymienionej ustawy.

przemysłowego (20 lat) oraz wskazanie na zastosowanie w tym zakresie przepisów ustawy o narodowym zasobie archiwalnym. Powinno to jednoznacznie wykluczyć odnotowywane w ostatnich latach sytuacje sprzecznego z prawem brakowania przez niektórych pełnomocników ochrony akt postępowań sprawdzających po zakończeniu pracy danej osoby w jednostce organizacyjnej lub po upływie ważności poświadczenia bezpieczeństwa wydanego po przeprowadzeniu zwykłego postępowania sprawdzającego.

Dodano także, że akta zakończonych zwykłych postępowań sprawdzających mogą być przechowywane nie tylko przez pełnomocnika ochrony (jak to było do tej pory), ale także w pionie ochrony, co umożliwia racjonalne postępowanie z aktami, zwłaszcza w dużych jednostkach, w których do informacji niejawnych o klauzuli „poufne" dopuszczonych zostaje kilkaset osób. Zdarzało się bowiem, że na stanie ewidencyjnym pełnomocnika ochrony pozostawało kilkanaście tysięcy dokumentów tylko dlatego, że to jedynie on mógł – zgodnie z art. 42 ust. 3 poprzedniej ustawy – przechowywać akta zwykłych postępowań sprawdzających przeprowadzonych wobec osób z danej jednostki organizacyjnej. Z tych względów rozliczanie takiego pełnomocnika związane z jego odejściem ze stanowiska było niejednokrotnie bardzo czaso- i pracochłonne.

W nowej ustawie utrzymano przepis nakładający na ABW i SKW obowiązek przejmowania – w przypadku braku następcy prawnego – akt postępowań sprawdzających z jednostek organizacyjnych, które uległy rozwiązaniu, zniesieniu, likwidacji, przekształceniu i reorganizacji (art. 72 ust. 7).

Odmiennie uregulowano natomiast zasady prowadzenia przez ABW i SKW ewidencji osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub którym je cofnięto.

Przede wszystkim przesądzono, że ABW i SKW prowadzą – każda we własnym zakresie – jedną ewidencję dotyczącą bezpieczeństwa osobowego, niezależnie od podstawy dostępu lub braku dostępu do informacji niejawnych. Wcześniej obowiązek gromadzenia niezbędnych danych wynikał z dwóch przepisów: art. 42 ust. 5 (dotyczącego wydanych poświadczeń bezpieczeństwa i odmów wydania poświadczeń bezpieczeństwa) oraz art. 49 ust. 1 (dotyczącego wydanych zgód na udostępnienie informacji).

Do ewidencji prowadzonych przez ABW i SKW pełnomocnicy ochrony powinni przekazywać dane dotyczące osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają

uprawnienia do dostępu do informacji niejawnych na podstawie przepisów ustawy, tzn. osób:

- wobec których przeprowadzono postępowanie sprawdzające i wydano poświadczenie bezpieczeństwa,

- które przedstawiły w nowym miejscu pracy, pełnienia służby lub wykonywania czynności zleconych ważne, aktualne i odpowiednie poświadczenie bezpieczeństwa zgodnie z art. 34 ust. 1 ustawy,

- które uzyskały dostęp do informacji niejawnych o klauzuli „poufne" i wyższej na podstawie zgody właściwego organu zgodnie z art. 34 ust. 5, 6 i 9 ustawy.

Art. 73.

1. ABW i SKW prowadzą ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej oraz ewidencję osób, którym odmówiono wydania poświadczenia bezpieczeństwa, a także osób, wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w podmiotach, o których mowa w art. 23 ust. 5.

Art. 15.

1. Do zadań pełnomocnika ochrony należy:

(…)

8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto, obejmującego wyłącznie:

a) imię i nazwisko,

b) numer PESEL,

c) imię ojca,

d) datę i miejsce urodzenia,

e) adres miejsca zamieszkania lub pobytu,

f) określenie dokumentu kończącego procedurę, datę jego wydania oraz numer;

9) przekazywanie odpowiednio ABW lub SKW do ewidencji, o których mowa w art. 73 ust. 1, danych, o których mowa w art. 73 ust. 2, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt 8.

Należy podkreślić, że na podstawie ustawy, do dostępu do informacji niejawnych uprawniają nie tylko poświadczenia bezpieczeństwa, ale także zgody właściwego organu wydane zgodnie z art. 34 ust. 5, 6 i 9 ustawy. Ponadto słowa *aktualnego wykazu* oznaczają, że mają być w tym wykazie także osoby, które pojawiły

się w nowej jednostce organizacyjnej z poświadczeniem wydanym w poprzednim miejscu pracy. Zgodnie zaś z art. 34 ust. 2 o tym fakcie informowane są w terminie 7 dni: organ, który wydał poświadczenie bezpieczeństwa oraz odpowiednio ABW lub SKW.

W art. 73 ust. 1 omawianej ustawy jednoznacznie wskazano, że ewidencja, o której mowa wyżej, nie dotyczy osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w podmiotach, których dotyczy art. 23 ust. 5 ustawy. Należy pamiętać, że rozwiązanie to stanowi jeden z elementów nowego, jednoznacznego określenia odpowiedniości poświadczeń wydanych w trybie art. 23 ust. 5, które są odpowiednie wyłącznie w ramach pracy, służby lub wykonywania prac zleconych tylko w podmiocie, który przeprowadził postępowanie i wydał poświadczenie.

Ustawodawca zdecydował ponadto o ograniczeniu danych, które ABW i SKW mogą gromadzić w ramach ewidencji, o której mowa w przytaczanym art. 73 ust. 1 ustawy. Zrezygnowano m.in. z podawania „sygnatury postępowania", co było niezbędne z uwagi na fakt, iż żaden przepis nowej ustawy (podobnie jak i poprzedniej) nie nakazuje stosowania sygnatury, a poza tym brak jest definicji tego pojęcia. Informacje na temat daty wydania i numeru poświadczenia bezpieczeństwa zastąpiono danymi dotyczącymi określenia dokumentu kończącego procedurę oraz daty jego wydania i numeru, co było niezbędne, gdyż ewidencja zawiera nie tylko dane dotyczące wydanych poświadczeń bezpieczeństwa, ale także decyzji o odmowie wydania bądź cofnięciu poświadczenia bezpieczeństwa.

Rezygnacja z niektórych innych danych, takich jak *data objęcia stanowiska i określenie, z dostępem do jakich informacji niejawnych łączy się to stanowisko* stanowi wprost konsekwencję ostatecznego odejścia w ustawie od powiązania zasady *need to know* ze stanowiskiem służbowym, które musiało być wskazane w wykazie określonym przez kierownika jednostki organizacyjnej, aby dana osoba mogła mieć dostęp do informacji niejawnych[20].

Na takim samym poziomie utrzymano ochronę danych gromadzonych w omawianych ewidencjach. Udostępnianie danych z ewidencji prowadzonych

[20] Związek taki w poprzedniej ustawie wynikał z obowiązku zawartego w art. 26:
Art. 26. 1. Kierownik jednostki organizacyjnej określi, z zastrzeżeniem ust. 2, stanowiska lub rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności.
2. Rada Ministrów określi, w drodze rozporządzenia, stanowiska i rodzaje prac zleconych w organach administracji rządowej, których wykonywanie w tych organach może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową (art. 26 ust. 2 został uchylony w 2005 r. – Dz.U. z 2005 r., Nr 85, poz. 727).

przez ABW i SKW oraz z wykazów prowadzonych przez pełnomocników ochrony na podstawie art. 15 ust. 1 pkt 8 ustawy, ograniczono do przypadków analogicznych do przesłanek udostępniania do wglądu lub przekazania akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego.

Przepisy dotyczące zagadnień z zakresu bezpieczeństwa teleinformatycznego

Wraz z wejściem w życie nowej ustawy o ochronie informacji niejawnych istotnym zmianom uległ cały system ochrony tego typu informacji. Nowelizacja objęła także obszar bezpieczeństwa teleinformatycznego, wprowadzając zasadnicze zmiany w stosunku do stanu poprzedniego.

W pierwszej kolejności należy przypomnieć, że ustawodawca, wprowadzając nową ustawę o ochronie informacji niejawnych, dokonał w niej zmian terminologicznych. Działanie to, mające na celu ujednolicenie stosowanych w całym systemie prawa pojęć, należy ocenić jako zasadne z uwagi na konieczność funkcjonowania każdej grupy przepisów w szerszym kontekście systemu prawa – przede wszystkim krajowego, ale także międzynarodowego. Najistotniejszą nowością w tym zakresie jest zmiana definicji systemu teleinformatycznego. Aktualnie więc posługujemy się określeniem s y s t e m t e l e i n f o r m a t y c z n y w znaczeniu zdefiniowanym w art. 2 pkt 6 ustawy poprzez odesłanie do przepisów innej ustawy, a mianowicie do art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[21]. Przyjętym rozwiązaniem inkorporowano do systemu ochrony informacji niejawnych definicję systemu teleinformatycznego, która została zastosowana w jednej z podstawowych z punktu widzenia prawa informatycznego polskich ustaw. Ponadto należy zaznaczyć, że definicja ta jest także zbieżna z definicją przyjętą w *Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*[22], co łącznie oznacza dostosowanie siatki terminologicznej ustawy do pozostałych ustaw. Poniżej – aktualne brzmienie omawianej definicji: *System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne*[23].

[21] Dz.U. z 2002 r., Nr 144, poz. 1204 z późn. zm.

[22] Dz.U. z 2005 r., Nr 64, poz. 565.

[23] Art. 2 pkt 6 *Ustawy o ochronie informacji niejawnych*, Dz.U. z 2002 r., Nr 144, poz. 1204 z późn. zm.

Analizując różnice pomiędzy nową a dawną definicją, należy podkreślić dwie rzeczy: po pierwsze, nowa definicja systemu zawiera w sobie desygnaty terminu s i e ć t e l e i n f o r m a t y c z n a, który został z ustawy usunięty. W nowym stanie prawnym posługiwanie się określeniem s i e c i t e l e i n f o r m a t y c z n e stanowi więc błąd posługiwania się pojęciami pozaprawnymi. Zmiana ta odzwierciedlona została w tytule rozdziału poświęconego problematyce bezpieczeństwa teleinformatycznego, który w obecnej ustawie nosi nazwę *Bezpieczeństwo teleinformatyczne*. Po drugie zaś, przyjęta definicja nie wymienia metod ani procedur postępowania, skupiając się jedynie na technicznym aspekcie pojęcia.

Omawiając kwestie terminologiczne, nie sposób pominąć także niezwykle istotnej zmiany w regulacji sfery bezpieczeństwa teleinformatycznego, jaką jest wprowadzenie do tego obszaru zasad zarządzania ryzykiem, stanowiących aktualnie podstawę oceny zagrożeń dla budowanych systemów oraz w efekcie – podstawę doboru określonych zabezpieczeń (problematyka ta zostanie omówiona szerzej w dalszej części opracowania; w tym miejscu zaś skupiono się jedynie na kwestiach terminologicznych). Samo pojęcie r y z y k a zostało zdefiniowane w art. 2 pkt 15 nowej ustawy w następujący sposób:

ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji (…)

Dwa kolejne, zasadnicze w poruszanym temacie, pojęcia zdefiniowano w art. 2 pkt. 16 i 17 ustawy w następujący sposób: s z a c o w a n i e m r y z y k a *– jest całościowy proces analizy i oceny ryzyka* (…)*; zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka* (…)

Powyższe definicje, jak też regulacje materialne w tym zakresie, zostały oparte na postanowieniach polskiej normy PN-ISO/IEC 27005.

Słowniczek ustawowy został ponadto uzupełniony o definicje dokumentu szczególnych wymagań bezpieczeństwa oraz dokumentu procedur bezpiecznej eksploatacji systemu teleinformatycznego (odpowiednio w art. 2 pkt. 7 i 8 ustawy), co stanowi głównie zabieg legislacyjny, mający na celu uproszczenie konstrukcji ustawy, oraz o definicję certyfikacji, której wprowadzenie wiąże się z rozbudowaniem procesów certyfikacji urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych. Kwestie związane z procesem certyfikacji zostały rozwinięte w dalszej części opracowania.

Przechodząc do części merytorycznej ustawy, w pierwszej kolejności należy przypomnieć o tym, co zostało stwierdzone na wstępie, tj. że zmianom uległy praktycznie wszystkie obszary regulacji przedmiotowej ustawy. Rozdział poświęcony zagadnieniom bezpieczeństwa teleinformatycznego jest tylko częścią całego aktu normatywnego, ściśle powiązaną z pozostałymi jego regulacjami. Opracowanie wydzielonej materii dotyczącej przedmiotowego zagadnienia nie powinno być czytane i odbierane w oderwaniu od regulacji ogólnych w sprawie innych zakresów tematycznych ustawy.

Zakres, który w ustawie poprzedzającej był regulowany w rozdziale 10. zatytułowanym *Bezpieczeństwo systemów i sieci teleinformatycznych* (art. 60. i następne) obecnie znajduje się w rozdziale 8. (art. 48 i następne) – *Bezpieczeństwo teleinformatyczne.* Dla sprawniejszego przeprowadzenia analizy zamiast ścisłego trzymania się kolejności redakcyjnej przepisów, przyjęto problemowe ujęcie zagadnień.

O ile w obu ustawach, tj. poprzedzającej oraz aktualnej, przepis otwierający rozdział poświęcony problematyce bezpieczeństwa teleinformatycznego konstytuuje zasadę przetwarzania informacji niejawnych wyłącznie w akredytowanych systemach teleinformatycznych, o tyle reguły i warunki akredytacji uległy istotnej modyfikacji. Obowiązująca ustawa wprowadziła przede wszystkim podział kompetencji pomiędzy ABW lub SKW z jednej strony, a kierownika jednostki organizacyjnej, w której tworzony jest dany system, z drugiej. Zgodnie z art. 48 ust. 9 w obecnym stanie prawnym akredytacji bezpieczeństwa teleinformatycznego systemom przeznaczonym do przetwarzania informacji niejawnych wyłącznie o klauzuli „zastrzeżone" udziela kierownik tej jednostki, choć przy udziale odpowiedniej służby, która może przedstawiać kierownikowi zalecenia wprowadzenia określonych zmian w organizacji systemu. Do tej pory podmiotami właściwymi do udzielania akredytacji w zakresie wszystkich klauzul były wyłącznie ABW i SKW, każda w zakresie swojej właściwości, określonej obecnie w art. 10 ustawy (w uproszczeniu – podział na sferę cywilną i wojskową).

> 9. *Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.*

Z drugiej strony nowa ustawa zaostrzyła jednak warunki uzyskiwania akredytacji systemów mających przetwarzać informacje oznaczone klauzulą „poufne" oraz wyższymi.

> *6. Świadectwo, o którym mowa w ust. 5, wydaje się na podstawie:*
>
> *1) zatwierdzonej przez ABW albo SKW dokumentacji bezpieczeństwa systemu teleinformatycznego;*
>
> *2) wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez ABW albo SKW.*

Zgodnie z przepisem art. 48 ust. 6 dla udzielenia akredytacji w tych przypadkach, dokonywanej poprzez wydanie stosownego świadectwa (zwanego w poprzedniej ustawie *certyfikatem* – art. 60 ust. 5), niezbędne jest zatwierdzenie przez właściwą służbę dokumentacji bezpieczeństwa systemu oraz przeprowadzenie audytu bezpieczeństwa mającego na celu zweryfikowanie funkcjonowania systemu zgodnie z tą dokumentacją. Na gruncie wcześniejszych przepisów powyższe zasady obowiązywały przy systemach mających służyć do przetwarzania informacji niejawnych o klauzulach „tajne" lub „ściśle tajne", ponieważ w przypadku dwóch niższych klauzul, obejmujących informacje nazywane dotąd „tajemnicą służbową", dokumentacja nie wymagała wyraźnego zatwierdzenia (była natomiast aprobowana poprzez niewnoszenie zastrzeżeń w terminie 30 dni). Powyższą zmianę należy oceniać w kontekście przyjętego kierunku obniżania klauzul, jako konsekwencję tego procesu, oraz mając na uwadze rosnące znaczenie przetwarzania informacji zapisanych w postaci dokumentów elektronicznych. Ostatecznie ustawodawca uznał, że przyjęcie w nowej ustawie właśnie klauzuli „poufne" jako cezury dla akredytacji dokonywanej przez służby ustala stosowną równowagę pomiędzy wymaganym nadzorem nad przetwarzaniem informacji niejawnych ze strony państwa, a elastycznością systemu ochrony tych informacji. W tym miejscu należy także wskazać, że na mocy postanowień art. 48 ust. 8 przedmiotowej ustawy ABW lub SKW mogą odstąpić od przeprowadzania audytu bezpieczeństwa w przypadku tworzenia systemu przeznaczonego do przetwarzania informacji niejawnych oznaczonych klauzulą „poufne", co stanowi pozytywny przejaw uwzględniania wymagań praktyki w obowiązujących przepisach. Takie podejście zaowocowało m.in. usankcjonowaniem przyjętej już na gruncie poprzedzającego aktu zasady, choć niesformalizowanej wyraźnie w przepisie, przyjmującej zakaz łączenia funkcji inspektora bezpieczeństwa teleinformatycznego z funkcją administratora systemu (art. 52 ust. 1 pkt. 1 i 2 ustawy).

Istotną nowością wprowadzoną do procesu akredytacji jest w dalszej kolejności wyraźne wyznaczenie ustawowych terminów jej udzielania. W przypadku akredytacji udzielanej przez ABW lub SKW termin ten wynosi 6 miesięcy, choć, jeśli jest to uzasadnione (np. skomplikowanie systemu), termin ten może być przedłużony o kolejne 6 miesięcy (art. 48 ust. 4 ustawy). Ustawa wskazuje ponadto na termin dokonania samego zatwierdzenia dokumentacji bezpieczeństwa (w ramach wyżej wymienionych okresów), które powinno odbyć się w ciągu 30 dni

od otrzymania kompletu dokumentów oraz może być przedłużone o kolejne 30 dni, z przyczyn analogicznych jak wyżej (art. 49 ust. 8 ustawy). Przy akredytacji dokonywanej przez kierownika jednostki organizacyjnej (a więc tylko w odniesieniu do informacji „zastrzeżonych") służby dokonują natomiast oceny dokumentacji zatwierdzonej przez tego kierownika, na co ustawa wyznacza im 30-dniowy termin; również kierownik jednostki ma na przesłanie dokumentacji do ABW lub SKW 30 dni od momentu jej zatwierdzenia (art. 48 ust. 11 i 12 ustawy). W przypadku zgłoszenia przez jedną ze służb stosownych zaleceń, kierownik w ciągu kolejnych 30 dni udziela informacji o sposobie ich wdrożenia. Pewnym hamulcem bezpieczeństwa, niezbędnym do zapewnienia poprawnej kontroli udzielania akredytacji przez samych kierowników jednostek organizacyjnych, jest możliwość nakazania przez ABW lub SKW, w szczególnie uzasadnionych przypadkach, wstrzymania przetwarzania informacji niejawnych w systemie.

Kolejną zmianą wprowadzoną przez nową ustawę w zakresie terminów jest zasada udzielania akredytacji na czas określony, tj. maksymalnie na 5 lat (art. 48 ust. 2). W poprzedzającej ustawie akredytacje co do zasady udzielane były bezterminowo; wyjątkiem było udzielenie czasowej akredytacji systemowi nie spełniającemu wszystkich wymagań ustawowych, którego funkcjonowanie było jednak niezbędne z punktu widzenia potrzeb społecznych, obronności, bezpieczeństwa albo interesów międzynarodowych państwa (art. 60 ust. 7 dawnej ustawy).

> *2. Akredytacji, o której mowa w ust. 1, udziela się na czas określony, nie dłuższy niż 5 lat.*

Przechodząc do zagadnień związanych z budową systemów teleinformatycznych oraz ze sporządzaniem dokumentacji bezpieczeństwa, nie sposób nie zacząć omawiania zmian w tym zakresie od wskazania na wprowadzone do tego obszaru nowe zasady projektowania oraz konstruowania systemów, opierające się na procesie zarządzania ryzykiem. Celem nowej regulacji jest wdrożenie elastycznych zasad doboru zabezpieczeń systemu, zamiast, jak to było do tej pory, określania bezwzględnego katalogu wymagań, które każdy system musi spełnić. Jak można przeczytać w uzasadnieniu do projektu ustawy, stosowanie zarządzania ryzykiem przy określaniu wymogów bezpieczeństwa fizycznego i teleinformatycznego ma na celu umożliwienie istotnego ograniczenia nadmiernych i anachronicznych wymagań oraz związanych z nimi wydatków przez dopasowanie stosowanych środków ochrony do liczby i wagi chronionych informacji oraz rzeczywistego poziomu zagrożeń dla nich. Poza tym, wprowadzenie do zasad projektowania systemów obowiązku dokonywania analizy ryzyka powinno ułatwić akredytację systemów teleinformatycznych przygotowanych do przekazywania i przetwarzania

informacji niejawnych, co będzie miało kluczowe znaczenie w okresie prezydencji Polski w Unii Europejskiej (ma więc również wymiar praktyczny). Z całą stanowczością należy poprzeć projektodawców ustawy także w kolejnym stwierdzeniu, pochodzącym z uzasadnienia ustawy, że ideą omawianych w tym miejscu zmian nie jest obniżenie standardów ochrony, ale ich adekwatne i efektywne stosowanie na rzecz odejścia od konieczności aplikowania sztywnych wymogów formalnych. Podkreślenia wymaga przy tym fakt, że proces zarządzania ryzykiem, w tym prowadzone w jego ramach szacowanie ryzyka, stał się obecnie głównym elementem bezpieczeństwa teleinformatycznego. Wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym stały się aktualnie, zgodnie z postanowieniami art. 49 ust. 1 ustawy, jednym z najważniejszych elementów dokumentu szczególnych wymagań w zakresie bezpieczeństwa systemu teleinformatycznego, stanowiącym punkt wyjścia dla oceny bezpieczeństwa tego systemu. Szacowanie ryzyka stało się zaś tym samym podstawowym działaniem, jakie należy przeprowadzić przed przystąpieniem do sporządzenia dokumentacji odnośnie bezpieczeństwa. Należy jednak mieć świadomość, że aby oceny były zawsze aktualne, czynność ta powinna być przeprowadzana.

Art. 49.

1. *Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.*

Zgodnie z postanowieniami art. 51 ustawy obowiązkowi akredytacji nie podlegają systemy teleinformatyczne znajdujące się poza strefami ochronnymi oraz bezpośrednio służące do pozyskiwania i przekazywania w sposób niejawny informacji, a także do utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty. Regulacja ta jest swego rodzaju rozwinięciem i uściśleniem brzmienia art. 60 ust. 8 poprzedniej ustawy.

Art. 51.

1. *Obowiązkowi akredytacji, o którym mowa w art. 48 ust. 1, nie podlegają systemy teleinformatyczne znajdujące się poza strefami ochronnymi oraz służące bezpośrednio do pozyskiwania i przekazywania w sposób niejawny informacji oraz utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez*

uprawnione do tego podmioty. Wyłączenie obowiązku akredytacji nie obejmuje interfejsów, o których mowa w art. 179 ust. 4a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.12)), oraz systemów z nimi współpracujących.

2. *Obowiązkowi akredytacji, o którym mowa w art. 48 ust. 1, oraz badań i oceny bezpieczeństwa w ramach procesów certyfikacji prowadzonych przez ABW albo SKW nie podlegają systemy teleinformatyczne, urządzenia lub narzędzia kryptograficzne wykorzystywane przez AW lub SWW do uzyskiwania lub przetwarzania informacji niejawnych podczas wykonywania czynności operacyjno-rozpoznawczych poza granicami Rzeczypospolitej Polskiej oraz wydzielone stanowiska służące wyłącznie do odbierania i przetwarzania tych informacji na terytorium Rzeczypospolitej Polskiej.*

W art. 51 nowej ustawy wprowadzono dodatkowo zwolnienie z obowiązku akredytacji oraz dokonywania badań i oceny bezpieczeństwa w ramach procesów certyfikacji (opisanych poniżej) dotyczące systemów teleinformatycznych oraz urządzeń i narzędzi kryptograficznych wykorzystywanych przez Agencję Wywiadu oraz Służbę Wywiadu Wojskowego do uzyskiwania lub przetwarzania informacji niejawnych podczas wykonywania czynności operacyjno-rozpoznawczych poza granicami Rzeczypospolitej Polskiej, a także wydzielonych stanowisk służących wyłącznie do odbierania i przetwarzania tych informacji na terytorium RP. Przyjęcie tego rozwiązania nakłada na AW i SWW ogromną odpowiedzialność za właściwe zabezpieczanie informacji o szczególnym znaczeniu dla bezpieczeństwa państwa.

Projektując nową ustawę, dokonano także uporządkowania zagadnienia certyfikacji środków ochrony informacji niejawnych stosowanych w systemach teleinformatycznych. Dla wyraźnego odróżnienia tego zagadnienia od procesu akredytacji systemów teleinformatycznych, terminu c e r t y f i k a c j a w ustawie używa się wyłącznie wobec prowadzenia badań oraz wydawania certyfikatów dla określonych rozwiązań technicznych, natomiast odnosząc się do systemów teleinformatycznych ustawa posługuje się wyłącznie terminem a k r e d y t a c j a. Powyższe miało na celu ujednolicenie terminologii oraz usunięcie wątpliwości związanych z funkcjonującym w poprzedniej ustawie terminem certyfikat a k r e d y t a c j i. Regulacja tej sfery bezpieczeństwa teleinformatycznego została zawarta w art. 50 ustawy, wprowadzając certyfikację środków ochrony elektromagnetycznej przeznaczonych do ochrony informacji o klauzuli „poufne" lub wyższej, urządzeń i narzędzi kryptograficznych chroniących informacje o wszystkich klauzulach tajności oraz urządzeń lub narzędzi służących do realizacji zabezpieczeń teleinformatycznych. Wprowadzenie zasady generalnej certyfikacji kryptografii (do wszystkich klauzul) stanowi kolejną różnicę w stosunku do wcześniejszego stanu prawnego, w którym kryptografia była certyfikowana na potrzeby wykorzystania jej w systemach przetwarzających informacje o klauzuli co najmniej „poufne" (art. 60 ust. 3 dawnej ustawy). Zatwierdzenie certyfikatów dla środków ochrony elektro-

magnetycznej oraz omówiona zmiana w certyfikacji kryptografii pozwalają nie tylko na usprawnienie całego procesu akredytacji systemów, ale umożliwiają także polskim przedsiębiorcom uzyskiwanie certyfikatów niezbędnych do wprowadzania oferowanych produktów do wykorzystania w ramach struktur NATO i Unii Europejskiej. Certyfikaty wydawane są czasowo, jednak na okres nie krótszy niż 3 lata (art. 50 ust. 4).

Art. 50.

1. *Środki ochrony elektromagnetycznej przeznaczone do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.*
2. *Urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.*
3. *ABW albo SKW, na wniosek zainteresowanego podmiotu, przeprowadza certyfikację urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego, przeznaczonego do ochrony informacji niejawnych.*
4. *Pozytywne wyniki ocen bezpieczeństwa uzyskane na podstawie wyników badań prowadzonych w ramach certyfikacji, o których mowa w ust. 1-3, stanowią podstawę do wydania przez ABW albo SKW certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa teleinformatycznego. Certyfikaty są wydawane, w zależności od wyników ocen bezpieczeństwa, na okres nie krótszy niż 3 lata. Od odmowy wydania certyfikatu nie służy odwołanie.*
5. *Certyfikacje, o których mowa w ust. 1-3, są prowadzone przez ABW albo SKW z pominięciem właściwości, o której mowa w art. 10 ust. 2 i 3.*
6. *Szef ABW albo Szef SKW może zlecić podmiotowi zewnętrznemu badanie urządzenia lub narzędzia służącego do ochrony informacji niejawnych, na zasadach, warunkach i w zakresie przez siebie określonych.*
7. *Bez konieczności przeprowadzania badań i oceny Szef ABW albo Szef SKW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa państwa będącego członkiem NATO lub Unii Europejskiej lub inny uprawniony organ w NATO lub w Unii Europejskiej*

Niezwykle ważką zmianą, która eliminuje konieczność dokonywania a priori oceny przeznaczenia danego środka, urządzenia lub narzędzia do wykorzystania w jednej ze sfer – wojskowej lub cywilnej – jest pominięcie ogólnej właściwości ABW i SKW w kwestii wydawania certyfikatów (art. 50 ust. 5). Słusznie w trakcie prac legislacyjnych zwracano uwagę, że niektóre rozwiązania techniczne mogą służyć zarówno ochronie informacji przetwarzanych przez wojsko, jak i przez instytucje cywilne. Z uwagi na powyższe, przedmiotowe rozwiązanie należy oceniać pozytywnie. Ponieważ proces certyfikacji wiąże się jednak z koniecznością dokonywania szeroko zakrojonych badań danego produktu, które niejednokrotnie są czasochłonne, ustawodawca, idąc śladem rozwiązań przyjmowanych w innych krajach, wprowadził do nowej ustawy możliwość zlecania przez

Szefów ABW i SKW takich badań podmiotom zewnętrznym na zasadach, warunkach i w zakresie określonym przez szefa służby dokonującej certyfikacji. Stanowi to kolejny element usprawniający procedury prowadzone w zakresie bezpieczeństwa teleinformatycznego, otwierając jednocześnie nowe możliwości dokonywania szczegółowych, wysoko specjalistycznych badań.

Zmiany wprowadzone przez nową ustawę dotyczą także szkoleń specjalistycznych z zakresu bezpieczeństwa teleinformatycznego, choć odnoszą się jedynie do ich strony organizacyjnej. Nowa ustawa wprowadziła konieczność zawierania trójstronnych umów o przeprowadzenie tego typu szkoleń pomiędzy podmiotem przeprowadzającym szkolenie (ABW lub SKW w zakresie ogólnej właściwości), jego uczestnikiem oraz jednostką organizacyjną, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone (art. 52 ust. 7 ustawy). Z pokrywania kosztów za przeprowadzenie szkolenia zwolniono wyłącznie Policję oraz jednostki organizacyjne podległe ministrowi obrony narodowej lub przez niego nadzorowane. Podobne zwolnienia zastosowano w przypadku osób ubiegających się o dostęp do informacji niejawnych.

> 7. *Wzajemne prawa i obowiązki podmiotu przeprowadzającego szkolenie, uczestnika szkolenia, o którym mowa w ust. 4, oraz jednostki organizacyjnej, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone, określa umowa zawarta między tym podmiotem, uczestnikiem szkolenia oraz jednostką organizacyjną.*

Justyna Strużewska-Smirnow

Ochrona informacji niejawnych po 1989 r. – – przekrój podstaw prawnych

Ochrona informacji niejawnych w polskim systemie prawnym po 1989 r. była zawsze uregulowana w akcie rangi ustawowej. Chociaż unormowania te mają zasadnicze znaczenie dla bezpieczeństwa publicznego, obronności, sytuacji ekonomicznej oraz stosunków międzynarodowych, nie wpływają jednak w szczególny sposób na codzienne życie obywateli. Analiza kolejnych ustaw dotyczących ochrony informacji o kluczowym znaczeniu dla interesów państwa pozwala natomiast zaobserwować, jak zmiany społeczne oraz rozwój technologii powodowały konieczność wielokrotnych nowelizacji obowiązującego prawa.

Pierwszym aktem prawnym regulującym zagadnienia związane z ochroną informacji niejawnych była *Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej*. Gdy w 1989 r. rozpoczęły się w Polsce zmiany związane z transformacją ustrojową, modernizacji wymagała większość istotnych dziedzin życia publicznego. Prace legislacyjne zostały skoncentrowane przede wszystkim na sferach związanych z ekonomicznym aspektem funkcjonowania państwa oraz sferze swobód obywatelskich. Dostrzegano także potrzebę aktualizacji licznych aktów prawnych regulujących inne zagadnienia, w tym m.in. uchwalenie nowej ustawy o ochronie tajemnicy państwowej i służbowej. Obowiązującej ustawie z 1982 r. zarzucano, iż była niedemokratyczna, przestarzała, a przede wszystkim powstała w okresie stanu wojennego[1]. Prace nad nowym aktem prawnym zostały podjęte przez rząd Tadeusza Mazowieckiego, jednak projekt nie został uchwalony ze względu na upływ kadencji Sejmu[2]. Mimo iż prace nad kolejnymi projektami były kontynuowane, *Ustawa z 1982 r. o ochronie tajemnicy państwowej i służbowej* funkcjonowała aż do 1999 r. Warto zatem nieco przybliżyć zakres tej regulacji.

Ustawa z 1982 r. regulowała zbiorczo zasady i sposób postępowania z informacjami stanowiącymi tajemnicę państwową i służbową. Formułując definicje wiadomości, dla których przewidziano trzy rodzaje klauzul tajności, zobowiązywała równocześnie organy administracji państwowej oraz inne podmioty niepaństwowe do ustalania wykazów rodzajów informacji, które nierzadko same miały

[1] S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, LexisNexis, s. 14.

[2] Tamże, s. 15

klauzule tajności lub poufności. Co więcej, akty wykonawcze do ustawy również oznaczone były klauzulami tajności bądź w ogóle nie były publikowane. Tworzyło to sytuację, w której realizacja powszechnego, ustawowego obowiązku ochrony tajemnicy państwowej i służbowej była utrudniona z uwagi na limitowany klauzulami dostęp do przepisów wykonawczych[3].

Omawiane rozwiązania ustawowe przewidywały również instytucję *upoważnienia do dostępu do wiadomości stanowiących tajemnicę państwową lub służbową*, dość enigmatycznie określając warunki wydania takiego upoważnienia. Równocześnie omawiana ustawa zawierała delegację dla Marszałka Sejmu, Prezydenta Rzeczypospolitej Polskiej oraz Prezesa Rady Ministrów do określenia wykazów stanowisk i funkcji w podległych bądź nadzorowanych przez nich organach, których pełnienie uprawniało do dostępu do wiadomości stanowiących tajemnicę państwową bez potrzeby uzyskiwania stosownych upoważnień. W praktyce zatem duża grupa funkcjonariuszy i urzędników państwowych z mocy prawa miała dostęp do wiadomości tajnych[4].

Kwestie takie, jak ochrona informacji niejawnych w systemach i sieciach teleinformatycznych czy też ochrona informacji przekazywanych podmiotom gospodarczym w związku z realizacją umów na dostawę produktów lub usług były uregulowane fragmentarycznie i poza ustawą.

Warto zaznaczyć, iż niektóre przepisy ustawy z 1982 r. stały się przedmiotem wykładni Trybunału Konstytucyjnego (uchwała z 13 czerwca 1994 r. W 3/94, OTK 1994/1/26). Trybunał zajął się m.in. wykładnią zawartego w art. 2 ust. 1 pkt. 2 ustawy określenia dane identyfikujące funkcjonariuszy tych organów i osoby współdziałające z organami ochrony bezpieczeństwa publicznego, wykonujące zadania z zakresu wywiadu i kontrwywiadu. W ocenie TK określenie to odnosiło się nie do wszystkich funkcjonariuszy organów ochrony porządku i bezpieczeństwa publicznego i osób współdziałających z organami bezpieczeństwa publicznego, lecz jedynie do tych, którzy wykonywały zadania z zakresu wywiadu lub kontrwywiadu[5].

W tym kontekście TK wyjaśnił także, iż pojęcie tajemnicy państwowej, o której mowa w art. 2 ust. 1 pkt 2 cytowanej ustawy, nie obejmowało danych identyfikacyjnych osób, które w przeszłości były funkcjonariuszami organów ochrony porządku i bezpieczeństwa publicznego albo które z tymi organami współdziała-

[3] Uzasadnienie do projektu ustawy z 22 stycznia 1999 r. o ochronie informacji niejawnych (materiały własne, zgromadzone w toku pracy zawodowej).

[4] Tamże.

[5] Uchwała Trybunału Konstytucyjnego z 13 czerwca 1994 r., W 3/94, OTK 1994/1/26.

ły, chyba, że osoby te wykonywały zadania z zakresu wywiadu lub kontrwywiadu, a ujawnienie ich danych mogłoby narazić na szkodę obronność, bezpieczeństwo lub inny ważny interes Rzeczypospolitej Polskiej[6].

Ponadto, rozpatrując wniosek Pierwszego Prezesa Sądu Najwyższego, Trybunał Konstytucyjny w postanowieniu z 13 czerwca 1994 r. (S 1/94, OTK 1994/1/28) zasygnalizował Sejmowi RP lukę w prawie polegającą na:

1) braku określenia w przepisach ustawowych zasad zwalniania z obowiązku zachowania tajemnicy państwowej w postępowaniu przed sądami i innymi organami, o których mowa w art. 5 ust. 2 cyt. ustawy oraz właściwej w tym względzie procedury,

2) nieuwzględnieniu w art. 7 ust. 6 cyt. ustawy kompetencji organów sądowych (Pierwszego Prezesa Sądu Najwyższego, Prezesa Naczelnego Sądu Administracyjnego i Prezesa Trybunału Konstytucyjnego) do ustalania wykazu stanowisk i funkcji, których pełnienie uprawnia do dostępu do wiadomości stanowiących tajemnicę państwową bez potrzeby uzyskiwania upoważnień,

3) nieokreśloności i systemowej niespójności konstrukcji prawnej tajemnicy państwowej, zwłaszcza art. 6 ust. 1, 4 i 5 cytowanej ustawy, przekazującego uszczegółowienie i aktualizację wiadomości objętych tą tajemnicą do uregulowania aktem niższej rangi niż ustawa oraz wyłączenie spod publikacji wykazów dotyczących obronności sił zbrojnych i bezpieczeństwa państwa,

4) braku spójności przepisów cyt. wyżej ustawy, a w szczególności jej art. 6, z rt. 1 pozostawionych w mocy przepisów konstytucyjnych,

5) nieokreśleniu procedury ujawnienia wiadomości stanowiących tajemnicę państwową, co powoduje niespójność z obowiązującym w RP systemem prawnym, a w szczególności z art. 1 i 56 pozostawionych w mocy przepisów konstytucyjnych[7].

Mimo konieczności dostosowania przepisów ustawy z 1982 r. do warunków demokratycznego systemu prawnego, prace nad kolejnymi projektami były przerywane.

W konsekwencji postępujących zmian społeczno-gospodarczych i politycznych Polska wyraziła chęć przystąpienia do Sojuszu Północnoatlantyckiego. Roz-

[6] Tamże.

[7] Postanowienie Trybunału Konstytucyjnego z 13 czerwca 1994 r., S 1/94, OTK 1994/1/28.

poczęły się także starania o przystąpienie do Wspólnoty Europejskiej. W związku z udziałem naszego państwa w Partnerstwie dla Pokoju 3 listopada 1994 r. Polska zawarła z NATO *Umowę o bezpieczeństwie* i tym samym zobowiązała się do przestrzegania m.in. zachodnich standardów w dziedzinie ochrony tajemnicy, które zostały przedstawione przez Biuro Bezpieczeństwa NATO przedstawicielom polskiego rządu. W tym samym roku Rzeczpospolita Polska zawarła także umowę o bezpieczeństwie z Unią Zachodnioeuropejską – jej celem była ochrona informacji wymienianych z tą organizacją[8]. Otwarcie Polski na zachodnich sojuszników zaowocowało także podpisaniem umów o randze resortowej, które dotyczyły m.in. wymiany wojskowych informacji niejawnych w dziedzinie obronności. Należy podkreślić, iż w umowach tych określona została między innymi wzajemna odpowiedniość klauzul tajności.

Warto wyjaśnić, iż wiele z państw wchodzących w skład Sojuszu Północnoatlantyckiego było związanych nie tylko umowami sojuszniczymi, określającymi zasady wzajemnej ochrony informacji niejawnych w ramach NATO oraz Unii Zachodnioeuropejskiej, lecz także zawierały pomiędzy sobą liczne umowy bilateralne mające istotne znaczenie zwłaszcza dla współpracy w zakresie obronności, gospodarki, polityki oraz bezpieczeństwa wewnętrznego (zwłaszcza współpracy w zwalczaniu najgroźniejszych form przestępczości). Rozwiązania przyjęte w tych umowach odnosiły się nie tylko do organów władzy publicznej (do których były przede wszystkim skierowane), ale także do przedsiębiorców realizujących kontrakty z wykorzystaniem informacji niejawnych oraz osób fizycznych – w zakresie przyznanego im prawa dostępu do informacji niejawnych i wykonywanych obowiązków służbowych. Brak nowoczesnej regulacji ustawowej w Polsce dotyczącej ochrony informacji niejawnych, w której uwzględnione były standardy wyznaczane przez Sojusz Północnoatlantycki, spowodował, iż do 1999 r. rządową umowę o wzajemnej ochronie informacji niejawnych z Polską zawarła jedynie Republika Federalna Niemiec.

Z uwagi na konieczność przygotowania do przyjęcia rozwiązań stosowanych w państwach NATO 27 sierpnia 1997 r., z inicjatywy rządu, Sejm uchwalił ustawę o zmianie ustawy o ochronie tajemnicy państwowej i służbowej. W nowelizacji zawarto przepisy umożliwiające wymianę informacji stanowiących tajemnicę państwową lub służbową na podstawie umów międzynarodowych, a także podstawowe zapisy dotyczące ochrony informacji stanowiących tajemnicę państwową lub służbową przekazywanych podmiotom gospodarczym w związku z realizacją umów na dostawę produktów lub usług. W nowelizacji zarysowany został także podział na sferę cywilną i wojskową.

---

[8] S. Hoc, *Ustawa o ochronie*..., s. 16-17.

Należy jednak zauważyć, iż mimo opisanych powyżej zmian ustawa z 1982 r. w dalszym ciągu nie regulowała kwestii dotyczących sprawdzeń osób, które mają mieć dostęp do tajemnicy państwowej o *szczególnym znaczeniu dla obronności Państwa, Sił Zbrojnych i bezpieczeństwa Państwa*. Ponadto, w świetle przyjętej w 1997 r. Konstytucji Rzeczypospolitej Polskiej, odesłanie w kwestii przedmiotu i zakresu takich sprawdzeń do regulacji w akcie wykonawczym było rozwiązaniem wątpliwym[9].

W uzasadnieniu do projektu kolejnej ustawy o ochronie informacji niejawnych, która weszła w życie 22 stycznia 1999 r., jako bezwzględną potrzebę jej uchwalenia przywołano zarówno brak nowoczesnego i uwzględniającego interes bezpieczeństwa państwa demokratycznego systemu ochrony informacji niejawnych, jak i finalizowany proces przystąpienia Rzeczypospolitej Polskiej do Organizacji Traktatu Północnoatlantyckiego oraz związane z tym sformalizowane wymagania Sojuszu dotyczące ochrony informacji tajnych przez każde z państw członkowskich.

W myśl założeń uzasadnienia ustawa z 1999 r. nie stanowiła prostej negacji rozwiązań przyjętych w ustawie z 1982 r. Była jednak oparta na innych założeniach – uwzględniała standardy NATO i Unii Europejskiej w zakresie bezpieczeństwa informacji klasyfikowanych, niejednokrotnie nawet poza nie wykraczając. Podstawowym elementem odróżniającym ustawę z 1999 r. od poprzedniej regulacji było założenie, iż problem ochrony informacji niejawnych ma charakter ponadresortowy, co oznacza nałożenie obowiązków i określenie odpowiedzialności za tę ochronę na każdą osobę uprawnioną do dostępu do nich.

Kolejne założenie projektodawców wynikało z konieczności dostosowania podstaw prawnych oraz organizacji i funkcjonowania systemu ochrony informacji niejawnych do obowiązujących w tym zakresie wymagań Sojuszu Północnoatlantyckiego. Wymagania te zostały określone w Umowie pomiędzy Stronami Traktatu Północnoatlantyckiego o ochronie informacji z 6 marca 1997 r. (umowa weszła w życie w stosunku do Rzeczypospolitej Polskiej 21 października 1999 r.) oraz w przyjętym przez Radę Północnoatlantycką dokumencie dotyczącym minimalnych wymagań w zakresie bezpieczeństwa informacji klasyfikowanych NATO (dokument C-M/55/15/Wersja ostateczna). Założenie to można wyrazić tezą, że niezależnie od zobowiązań międzynarodowych, narodowy system ochrony informacji niejawnych nie może być słabszy od systemu ochrony takich informacji, które są wymieniane z NATO.

Ustawa z 1999 r. stworzyła nowy kompleksowy system, który został opisany w 11 rozdziałach. Przede wszystkim w ustawie została wyrażona jedna z funda-

[9] Uzasadnienie do projektu ustawy z 22 stycznia 1999 r.

mentalnych zasad dla ochrony informacji niejawnych w krajach Sojuszu Północnoatlantyckiego. Zawiera ona dwa podstawowe wymagania odnośnie dostępu do informacji klauzulowanych:

1) jest on możliwy wyłącznie dla osoby dającej rękojmię zachowania tajemnicy, co oznacza, że spełnia ona ustawowe wymagania dla zapewnienia ochrony tajemnicy przed nieuprawnionym ujawnieniem,
2) dostęp jest możliwy tylko w takim zakresie, jaki jest niezbędny do wykonania przez tę osobę pracy lub obowiązków służbowych na zajmowanym stanowisku albo innej pracy zleconej.

Opisana zasada, zwana „zasadą ograniczonego dostępu" (ang. *need to know*), to podstawowy standard NATO[10].

Początkowo przepisy określające organizację ochrony informacji tajnych wyznaczały trzy podstawowe poziomy. Pierwszy obejmował działający przy Radzie Ministrów Komitet Ochrony Informacji Niejawnych jako organ odpowiedzialny za kształtowanie polityki państwa w zakresie ochrony informacji niejawnych.

Na drugim poziomie zostały utworzone krajowe władze bezpieczeństwa (w sierpniu 1997 r. rząd RP poinformował NATO, że funkcje te będą spełniać: Wojskowe Służby Informacyjne – w zakresie obronności i Urząd Ochrony Państwa – w sprawach z nią nie związanych[11]), które zgodnie ze standardami Sojuszu Północnoatlantyckiego odpowiadały za kontrolę przestrzegania przepisów o ochronie informacji niejawnych, ochronę informacji niejawnych wymienianych przez Polskę z innymi krajami oraz organizacjami międzynarodowymi. Szkolenie i doradztwo w zakresie ochrony informacji niejawnych, a także prowadzenie postępowania sprawdzającego dla ustalenia, czy osoby mające mieć dostęp do informacji niejawnych dają rękojmię ich ochrony przed nieuprawnionym ujawnieniem.

Na trzecim poziomie usytuowane zostało podstawowe ogniwo systemu ochrony informacji niejawnych – kierownicy jednostek organizacyjnych, w których takie informacje były wytwarzane, przetwarzane, przekazywane lub przechowywane i powoływani byli obligatoryjnie pełnomocnicy ds. ochrony informacji niejawnych oraz podlegające im wyspecjalizowane komórki organizacyjne zwane „pionami ochrony". To właśnie na nich, stanowiących podstawę całego systemu, spoczywają obowiązki i odpowiedzialność związana z kompleksową ochroną informacji niejawnych, w myśl zasady, że tak silny jest cały system, jak silne jest jego najsłabsze ogniwo[12].

---

[10] Tamże.

[11] S. Hoc, *Ustawa o ochronie*..., s. 17.

[12] Uzasadnienie do projektu ustawy z 22 stycznia 1999 r.

Projektodawcy uznali, iż skuteczne funkcjonowanie systemu ochrony informacji niejawnych zależy także od utworzenia mechanizmu przekazywania sygnałów o podstawowych zagrożeniach dla bezpieczeństwa takich informacji, ich gromadzenia oraz analizy przez krajowe organy bezpieczeństwa.

Wychodząc naprzeciw standardom NATO wprowadzono cztery klauzule tajności. Wprowadzono również upoważnienie dla ministra właściwego do spraw wewnętrznych i ministra obrony narodowej, stwarzające możliwość określenia w drodze rozporządzenia dodatkowych oznaczeń dokumentów, które mogą poprzedzać przyznane im klauzule tajności (w NATO takimi oznaczeniami są *„COSMIC”* i *„ATOMAL”*).

Kluczowe znaczenie miała treść rozdziału piątego ustawy z 1999 r. pt. *Dostęp do informacji niejawnych. Postępowanie sprawdzające*. Zawiera on rozwiązania prawne zupełnie odmienne od przyjętych w tym przedmiocie w ustawie z 1982 r.

Punktem wyjścia dla wyznaczenia zakresu uprawnień do dostępu do informacji niejawnych stało się określenie przez kierownika jednostki organizacyjnej stanowisk lub prac zleconych, z którymi łączy się dostęp do dokumentów o określonej klauzuli tajności, a przez Radę Ministrów w odniesieniu do stanowisk i prac zleconych w organach administracji rządowej. Dopuszczenie do pracy lub pełnienia służby na takim stanowisku albo zlecenie określonej pracy oznaczało przyznanie uprawnienia do dostępu do dokumentów zawierających informacje niejawne. Warunkiem było jednak przeprowadzenie postępowania sprawdzającego, przy akceptacji i wiedzy osoby sprawdzanej co do zakresu i podmiotu postępowania, w celu ustalenia, czy daje ona rękojmię zachowania tajemnicy oraz przeszkolenie tej osoby w zakresie ochrony informacji niejawnych[13].

W ustawie zawarto także przepisy wyłączające lub ograniczające przeprowadzenie postępowania sprawdzającego w pełnym zakresie wobec osób zajmujących najwyższe urzędy w państwie. Ustawa określiła również zasadę ścisłego wyodrębnienia akt postępowań sprawdzających i ograniczyła możliwości ich wykorzystania dla celów innych niż wspomniane postępowania. Zakończeniem postępowania sprawdzającego było wydanie poświadczenia bezpieczeństwa (w zależności od klauzuli tajności na 3, 5 lub 10 lat) bądź odmowa wydania takiego poświadczenia.

W ustawie znalazły się także uregulowania dotyczące kancelarii tajnych i obiegu dokumentów, dla których uzasadnieniem był fakt, iż w obręb funkcjono-

[13] Tamże.

wania systemu ochrony informacji niejawnych weszły także podmioty gospodarcze oraz osoby fizyczne zatrudnione poza szeroko rozumianym aparatem państwowym.

Z tych samych przyczyn w ustawie uregulowano zasady dotyczące środków fizycznej i technicznej ochrony informacji niejawnych. Przepisy ustawy z 1999 r. wprowadziły obowiązek stosowania tego rodzaju środków w celu uniemożliwienia osobom nieupoważnionym dostępu do materiałów niejawnych oraz określono katalog podstawowych środków ochrony fizycznej. Uregulowano także kwestie związane z wydzieleniem specjalnych stref bezpieczeństwa (ochrona dokumentów zawierających tajemnicę państwową), a także rozmów i spotkań, których przedmiotem są informacje o takim charakterze[14].

Niezwykle istotne znaczenie miało po raz pierwszy unormowanie problematyki bezpieczeństwa systemów i sieci teleinformatycznych, za których pośrednictwem przekazywane są informacje niejawne. Sformułowanie takich wymagań było jednym z podstawowych warunków dostosowania i tworzenia w Polsce bezpiecznych systemów i sieci teleinformatycznych do bardzo surowych w tym zakresie standardów NATO. Wprowadzono instytucję certyfikatu, od którego uzyskania uzależnione było dopuszczenie do funkcjonowania bezpiecznych, z punktu widzenia ochrony informacji niejawnych, sieci i systemów teleinformatycznych[15].

Nowością było także ujęcie w przepisach podstawowych zagadnień z zakresu bezpieczeństwa przemysłowego. Określone zostały warunki i obowiązki podmiotów gospodarczych związanych z zawieraniem umów, jeżeli wiązało się to z koniecznością dostępu do informacji niejawnych. Ich zdolność do zapewnienia ochrony informacji niejawnych oceniana była w toku specjalnego postępowania, do którego stosowano także przepisy dotyczące postępowania sprawdzającego wobec osób. Pozytywna ocena zdolności podmiotu gospodarczego do zapewnienia ochrony informacji niejawnych skutkowała wydaniem przez właściwy organ bezpieczeństwa świadectwa bezpieczeństwa przemysłowego[16].

Nie bez znaczenia były także przepisy przejściowe i końcowe. Miały one istotny walor porządkujący. Przyjęto, za ustawą z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, cezurę 10 maja 1990 r., jako odnośnik do objęcia ochroną dokumentów niejawnych wytworzonych po tej dacie i określono sposób postępowania z dokumentami wytworzonymi wcześniej. W stosunku do dokumentacji wytworzonej po 10 maja 1990 r. narzucono obowiązek dokonania w terminie 36 miesięcy ich

[14] Tamże.

[15] Tamże.

[16] Tamże.

przeglądu w celu dostosowania ich dotychczasowych klauzul do klauzul wynikających z ustawy. Wyznaczono także sześciomiesięczny termin na dostosowanie funkcjonowania jednostek organizacyjnych, w których przetwarzane były informacje niejawne, do nowych przepisów oraz przyjęto przepisy dotyczące ważności wydanych na podstawie ustawy z 1982 r. upoważnień do dostępu do wiadomości stanowiących tajemnicę państwową lub służbową.

Z perspektywy czasu należy docenić wielkość przedsięwzięcia, jakim było utworzenie na gruncie ustawy z 1999 r. całkowicie nowego systemu ochrony informacji niejawnych. Trzeba także zwrócić uwagę na stosunkowo krótki okres, jaki ustawodawca wyznaczył na wdrożenie nowych przepisów. Wprawdzie można spotkać opinie, iż ustawa z 1999 r. była aktem niespójnym i niekonsekwentnym[17], jednak wydaje się, iż pierwotne brzmienie ustawy z 1999 r. przeczy takim ocenom. Akt ten był sporządzony na podstawie przepisów wynikających z długoletniej praktyki w zakresie ochrony informacji niejawnych Sojuszu Północnoatlantyckiego. Jednocześnie musiały być w nim uwzględnione rzeczywiste możliwości egzekwowania nowych regulacji a także sprawność aparatu urzędniczego. Pozytywną rolę odgrywało również zawarcie w akcie rangi ustawowej przekrojowej wiedzy dotyczącej ochrony informacji niejawnych. Ustawa ta oraz akty wykonawcze do niej były bowiem podstawowym źródłem wiedzy dla tworzącej się kadry pionów ochrony. Stąd też być może nieco zbyt kazuistyczne zapisy były w tym wypadku celowe i użyteczne[18].

Natomiast liczne nowelizacje ustawy, choć niezbędne z punku widzenia zgodności z Konstytucją oraz wynikające z rozwoju technologii i relacji międzynarodowych, niewątpliwie osłabiły jej wewnętrzną spójność.

Pierwsza istotna nowelizacja wynikała z orzeczenia Trybunału Konstytucyjnego, który w wyroku z 10 maja 2000 r. orzekł o niezgodności niektórych przepisów ustawy z Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności oraz Konstytucją RP, przez to, że osoba sprawdzana pozbawiona była jakiegokolwiek skutecznego środka odwoławczego w wypadku odmowy wydania poświadczenia bezpieczeństwa. W wyniku tej nowelizacji wprowadzono do ustawy przede wszystkim nowy rozdział 5a *Postępowanie odwoławcze i skargowe*[19].

W 2002 r. z ustawy wykreślono cały rozdział 2 dotyczący Komitetu Ochrony Informacji Niejawnych. W ten sposób system, wbrew pierwotnym założeniom, przestał być trójpoziomowy.

---

[17] S. Hoc, *Ustawa o ochronie*..., s. 23.

[18] Tamże s. 20.

[19] Tamże

W tym samym roku ponownie podjęto działania zmierzające do dalszej nowelizacji ustawy z 1999 r. Wynikiem tych działań było uchwalenie licznych poprawek, a tekst jednolity ustawy wszedł w życie 16 czerwca 2005 r. Była to największa, od początku obowiązywania ustawy, reforma systemu ochrony informacji niejawnych. Objęła ona blisko jedną trzecią artykułów. Lata praktyki ujawniły nieco zbyt rygorystyczny charakter niektórych zapisów. Ponadto nie bez znaczenia było doświadczenie zdobyte przez krajowe władze bezpieczeństwa w kontaktach międzynarodowych: udział w pracach organów Sojuszu Północnoatlantyckiego, przygotowania do akcesji do Unii Europejskiej. Duże znaczenie miał również kontakt z partnerami zagranicznymi w ramach negocjacji bilateralnych umów rządowych o wzajemnej ochronie informacji niejawnych, które po wejściu w życie ustawy z 1999 r. były sukcesywnie zawierane z zagranicznymi partnerami. Natomiast praktyka funkcjonowania pionów ochrony w różnych jednostkach organizacyjnych oraz zastrzeżenia zgłaszane przez środowisko pełnomocników ds. ochrony informacji niejawnych pozwoliły na wyznaczenie zasadniczego kierunku zmian, jakie musiały zostać wdrożone w systemie ochrony informacji niejawnych.

Znaczące było wpisanie do ustawy z 2005 r. przepisów kodeksu postępowania administracyjnego, które od tego czasu mają wprost zastosowanie do procedur przewidzianych ustawą. Praca pionów ochrony została uelastyczniona przez wprowadzenie możliwości powoływania zastępców pełnomocników ds. ochrony informacji niejawnych, a także powierzenie pełnomocnikowi ochrony wykonywania innych zadań, o ile ich realizacja nie naruszy prawidłowego wykonywania zadań ustawowych. Pojawiły się także zapisy świadczące o zintensyfikowaniu współpracy międzynarodowej związanej z wymianą i wzajemną ochroną informacji niejawnych.

Zasadniczych zmian dokonano w zakresie postępowania sprawdzającego, m.in. przejęto instytucje z kodeksu postępowania administracyjnego – umorzenie oraz zawieszenie postępowania sprawdzającego, wydłużono okresy ważności poświadczeń bezpieczeństwa (odpowiednio do 5, 7, i 10 lat) oraz wprowadzono zasadę „kaskady", która oznaczała, iż poświadczenia bezpieczeństwa upoważniające do dostępu do informacji oznaczonych klauzulą „ściśle tajne" uprawniały do dostępu do informacji oznaczonych niższymi klauzulami − odpowiednio przez 7 lat do „tajne" i 10 lat do tajemnicy służbowej, licząc od daty jego wystawienia. Podobnie w odniesieniu do tajemnicy służbowej przedłużanie uprawnień następowało w przypadku legitymowania się poświadczeniem upoważniającym do dostępu do informacji oznaczonych klauzulą „tajne"[20]. Ponadto znaczna część przepisów dotyczących procedury sprawdzeniowej została uszczegółowiona i rozbudowana (np. zasady odnoszące się do kontrolnego postępowania sprawdzającego).

[20] D. Jęda, M. Witkowski, *Ochrona informacji niejawnych – nowe rozwiązania*, Warszawa 2007, Wydawnictwo Ubezpieczeń, s. 48.

Natomiast rozdział dotyczący bezpieczeństwa systemów i sieci teleinformatycznych, ze względu na wielość zmian, został napisany na nowo. Pojawiły się w nim liczne rozwiązania, a także spisano procedury wypracowane w toku obowiązywania ustawy w dotychczasowym brzmieniu. Określono, iż bezpieczeństwo systemów i sieci teleinformatycznych zapewnia się przez spełnienie standardów wynikających z akredytacji bezpieczeństwa teleinformatycznego oraz badań i certyfikacji urządzeń i narzędzi kryptograficznych. Efektem tych czynności były wydawane przez służby ochrony państwa certyfikaty akredytacji bezpieczeństwa teleinformatycznego oraz certyfikaty ochrony kryptograficznej[21]. Ponadto doprecyzowano pojęcie dokumentów szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej.

Podobnie jak w przypadku zagadnień związanych z bezpieczeństwem teleinformatycznym, również rozdział dotyczący bezpieczeństwa przemysłowego został napisany od nowa. Wprowadzone zmiany miały charakter rewolucyjny. Przyczyną ich wdrożenia była duża różnorodność podmiotów gospodarczych ubiegających się o udział w rynku usług związanych z ochroną informacji niejawnych powiększającym się stopniowo od 1999 r. Jako najważniejsze należy wymienić wprowadzenie trzech kategorii świadectw bezpieczeństwa przemysłowego, a koszty ponoszone przez pracodawcę w związku z uzyskaniem odpowiedniego świadectwa uzależnione były m.in. od stopnia zdolności do ochrony informacji niejawnych. Postulatem przedsiębiorców, zrealizowanym w nowelizacji, było także wprowadzenie okresów ważności świadectwa bezpieczeństwa przemysłowego w zależności od klauzuli tajności (odpowiednio jak przy bezpieczeństwie osobowym). Należy podkreślić, iż zmiana ta istotnie wzmacniała pozycję przedsiębiorców. Do nowelizacji bowiem musieli oni ubiegać się o świadectwo bezpieczeństwa przemysłowego ilekroć przystępowali do umowy związanej z dostępem do informacji niejawnych. Innymi słowy wcześniej było ono dokumentem wydawanym jednorazowo.

Uwzględniając zapisy międzynarodowych umów o wzajemnej ochronie informacji niejawnych, a także przystąpienie do wspólnego rynku europejskiego, w związku z akcesją Polski do Unii Europejskiej w 2004 r. wprowadzono również zapis odnoszący się do zagranicznych podmiotów gospodarczych. Postępowanie bezpieczeństwa przemysłowego, sprawdzające zdolność do ochrony informacji niejawnych stanowiących tajemnicę służbową, przeprowadzane było wobec przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych tylko wtedy, gdy obowiązek uzyskania świadectwa bezpieczeństwa przemysłowego, upoważniającego do wykonywania umów związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne" lub jej zagranicznym odpowiednikiem, wy-

[21] T. Szewc, *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007, CH BECK, s. 60.

nikał z umów międzynarodowych zawartych przez Polskę lub z prawa wewnętrznego strony zlecającej umowę. W stosunku do podmiotów krajowych przeprowadzane było jedynie postępowanie w celu stwierdzenia zdolności do ochrony tajemnicy państwowej.

Z uwagi na liczne zmiany, które w okresie od 1999 r. zostały wprowadzone do ustawy, w przepisach przewidziano także szkolenie uzupełniające dla pełnomocników ochrony i ich zastępców, przeprowadzane nie rzadziej niż co 5 lat.

W założeniu nowelizacja miała przyczynić się do uelastycznienia procedur opisanych w ustawie z 1999 r. Przede wszystkim zaś wzmocnić pracę pionów ochrony oraz umożliwić ściślejszą współpracę międzynarodową nie tylko militarną i bezpieczeństwa, jak to miało to miejsce w związku z przystąpieniem do NATO, ale także współpracę gospodarczą, dynamicznie rozwijającą się po przystąpieniu Polski do Wspólnoty Europejskiej.

Niestety, praktyka stosowania przepisów wykazała, iż kolejne zmiany osłabiły wewnętrzną logikę ustawy, co wiązało się z trudnościami interpretacyjnymi i wątpliwościami prawnymi. Zwłaszcza dopuszczenie stosowania wprost przepisów kodeksu postępowania administracyjnego do procedur przewidzianych znowelizowaną ustawą powodowało konieczność interpretowania konkretnych przypadków w kontekście prawa administracyjnego. Na gruncie doktryny pojawił się wówczas termin p r o c e d u r a q u a s i - a d m i n i s t r a c y j n a, który miał zastosowanie zwłaszcza w odniesieniu do postępowań sprawdzających. Nowe pojęcie wynikało z faktu, iż niektóre zasady postępowania administracyjnego doznawały ograniczenia w toku procedury sprawdzeniowej, jako że interes ochrony informacji niejawnych miał znaczenie nadrzędne. Przykładowo, z przepisów dotyczących zasad ogólnych postępowania administracyjnego w znowelizowanej ustawie nie zostały wymienione artykuły gwarantujące udzielanie informacji (art. 9 kpa) lub wyjaśnienie zasadności przesłanek (art. 11 kpa).

Z jednej więc strony znowelizowana ustawa wychodziła naprzeciw zmianom, jakie już w praktyce przyniosła akcesja do struktur europejskich i północnoatlantyckich oraz łagodziła nadmierny rygoryzm przepisów wdrożonych w 1999 r., uwzględniając przy tym sprawdzone zasady kodeksu postępowania administracyjnego. Z drugiej, brak wewnętrznej spójności aktu prawnego oraz konieczność przystosowania przewidzianych ustawą postępowań do stosowania wprost przepisów administracyjnych, stanowiły istotną trudność dla wszystkich szczebli systemu ochrony informacji niejawnych.

Problematyczne było także stosowanie załącznika nr 1 do ustawy, w którym od 1999 r. określono wykaz informacji stanowiących tajemnicę państwową. Z uwagi na postęp technologiczny, np. korzystanie z bardzo szczegółowych zdjęć satelitarnych także przez podmioty gospodarcze (np. portal internetowy www.zumi.pl), pod znakiem zapytania stawiało możliwość zapewnienia rzeczywistej ochrony (przez nadanie klauzuli „tajne" zgodnie z cz. II zał. nr 1 pkt 14) fotogrametrycznym zobrazowaniom lotniczym lub naziemnym, zarejestrowanym na dowolnym nośniku, oraz wysokorozdzielczym zdjęciom satelitarnym zawierającym obrazy obiektów na terenach zamkniętych. W praktyce więc umieszczenie jakiegoś rodzaju informacji w załączniku i ustawowy wymóg przyznawania jej określonej klauzuli tajności nie gwarantował bezpieczeństwa takiej informacji. W obliczu powyższych trudności zgłoszono postulat podjęcia kompleksowych prac legislacyjnych w tym zakresie[22].

Wynikiem podjętych działań jest obowiązująca *Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych*. W uzasadnieniu do jej projektu doceniono, iż poprzednia ustawa pozwoliła stworzyć współczesny system ochrony informacji niejawnych oraz odegrała istotną rolę w okresie akcesji Polski do Sojuszu Północnoatlantyckiego. Zauważono jednak, iż rozwiązania zawarte w ustawie i aktach wykonawczych, zwłaszcza w zakresie bezpieczeństwa teleinformatycznego i fizycznego, odstają od aktualnego poziomu technologicznego. Wskazano także, iż zmianie uległy przepisy międzynarodowe regulujące politykę bezpieczeństwa. Zamiast wspomnianego wcześniej dokumentu C-M(55)15/Wersja ostateczna w 2002 r. przyjęto nowy dokument C-M(2002)49, który wprowadził zasady znacznie bardziej elastyczne i umożliwił szerokie stosowanie zarządzania ryzykiem zamiast dawniej obowiązujących standardów minimalnych. Dlatego też w nowej ustawie uwzględniono nie tylko potrzeby polskich instytucji i podmiotów stosujących ustawę, ale także standardy aktualnie stosowane przez NATO i UE.

W uzasadnieniu argumentowano, że istotą nowej ustawy jest takie unormowanie systemu ochrony informacji niejawnych, aby był on maksymalnie efektywny zarówno w sferze krajowej, jak i zagranicznej, przy jednoczesnej prostocie i elastyczności funkcjonowania, ale bez uszczerbku dla bezpieczeństwa informacji niejawnych. Działania te są szczególnie istotne z uwagi na objęcie przez Polskę przewodnictwa w Radzie Unii Europejskiej w 2011 r. W ocenie projektodawców brak zmiany przepisów z pewnością utrudniłby, a w wielu przypadkach wręcz uniemożliwiłby realizację zadań związanych z prezydencją. Dotyczy to szczególnie przewidzianej aktualnie możliwości znacznie bardziej elastycznego traktowania zasad ochrony informacji o niskich klauzulach tajności, co w strukturach unijnych umożliwia szybkie, bieżące wykorzystywanie tych informacji w pracy grup roboczych oraz ich sprawne przetwarzanie w systemach teleinformatycznych.

[22] S. Hoc, *Ustawa o ochronie* ..., s. 24.

Warto wyróżnić niektóre z kluczowych zasad, zaczerpniętych z systemu ochrony informacji niejawnych wspomnianych wyżej organizacji międzynarodowych, które stały się podstawą zasadniczych zmian w systemie krajowym. Przede wszystkim zrezygnowano z podziału informacji niejawnych na tajemnicę państwową i służbową. Jak argumentowano w uzasadnieniu do projektu ustawy, dziesięcioletnia praktyka funkcjonowania tego podziału wskazywała, że był on sztuczny i nie miał większego sensu praktycznego. Kolejnym jakościowym założeniem merytorycznym jest odejście od rozbudowanych formalnie wykazów informacji niejawnych na rzecz jednoznacznego zobowiązania wytwórców informacji do kierowania się nowymi definicjami poszczególnych klauzul. Zwrócono uwagę na fakt, iż zawieranie w ustawie wykazu informacji niejawnych nie jest standardowym rozwiązaniem w państwach o długoletniej tradycji demokratycznej.

W uzasadnieniu podniesiono też, iż duże znaczenie dla uproszczenia systemu ochrony informacji niejawnych powinna mieć rezygnacja z traktowania informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych jako informacji niejawnych. Inną ważną zmianą, którą wyraźnie określono w projekcie ustawy, a z czasem zostanie ona szczegółowo unormowana w aktach wykonawczych, jest umożliwienie stosowania zarządzania ryzykiem przy określeniu wymogów bezpieczeństwa fizycznego i teleinformatycznego. Umożliwi to istotne ograniczenie nadmiernych i anachronicznych wymagań oraz związanych z nimi wydatków przez dopasowanie stosowanych środków ochrony do liczby i znaczenia chronionych informacji oraz rzeczywistego poziomu istniejących dla nich zagrożeń.

Z punktu widzenia skuteczności polskiej prezydencji bardzo ważna jest – – w ocenie projektodawców – propozycja dotycząca rezygnacji ze ścisłej kontroli obiegu dokumentów o niższych klauzulach, a zwłaszcza o klauzuli „zastrzeżone". Zniesiono także istniejący do tej pory obowiązek prowadzenia postępowań sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone". W ten sposób został wprowadzony system obowiązujący w większości krajów Europy oraz w NATO i UE zakładający, że poświadczenie bezpieczeństwa obowiązuje do poziomu „poufne" i wzwyż, a podstawą do udostępnienia informacji o najniższej klauzuli tajności jest potrzeba wynikająca z wykonywania określonych obowiązków służbowych. Dostęp do informacji niejawnych o klauzuli „zastrzeżone" jest obecnie możliwy na podstawie pisemnego upoważnienia kierownika jednostki organizacyjnej, po odbyciu stosownego przeszkolenia[23].

Istotną zmianę stanowi także wprowadzenie jednej krajowej władzy bezpieczeństwa odpowiedzialnej za ochronę informacji niejawnych wymienianych z NATO i Unią Europejską. Zdaniem projektodawców nowy model powinien sku-

23 Uzasadnienie do projektu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 r.

tecznie zlikwidować mankamenty dotychczasowego rozwiązania polegającego na równoległym pełnieniu funkcji krajowej władzy bezpieczeństwa przez Szefów ABW i SKW, związane z funkcjonowaniem odmiennych standardów ochrony tych informacji w sferze cywilnej i wojskowej, na co niejednokrotnie zwracały uwagę inspekcje struktur bezpieczeństwa NATO i UE[24].

Zrozumiałe, iż tak rewolucyjne zmiany znalazły odzwierciedlenie także w nowelizacji dużej liczby innych obowiązujących aktów prawnych, co zostało uwzględnione w przepisach.

W ocenie skutków regulacji dostrzeżono, iż istnieje ryzyko obniżenia bezpieczeństwa niektórych informacji w wyniku zmiany zakresu definicji poszczególnych klauzul oraz obniżenia wymogów dotyczących ochrony informacji o niskich klauzulach. Zauważono także możliwość obniżenia bezpieczeństwa informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych, które przestaną być chronione na podstawie ustawy o ochronie informacji niejawnych. Podkreślono jednak, że ustawa wyznacza granicę między dostępem do informacji publicznej a nakazem ochrony informacji i obowiązkiem zachowania tajemnicy. Granica ta, będąca konsekwencją zmian w definicjach poszczególnych klauzul tajności, zostaje przesunięta, powiększając zakres informacji publicznej. Regulacja – zgodnie z założeniami projektodawców – może wpłynąć na zwiększenie jawności życia publicznego i ułatwić dostęp do informacji publicznej. Tym samym ustawa poszerzy sferę wolności i praw jednostek, zmniejszając ograniczenie prawa do informacji o działalności organów władzy publicznej[25].

Z uwagi na fakt, iż od momentu uchwalenia tekstu ustawy ukazało się wiele publikacji poświęconych omówieniu szczegółowych jej rozwiązań (artykuły były zamieszczane także w „Przeglądzie Bezpieczeństwa Wewnętrznego"), zaznaczono jedynie podstawowe zmiany systemowe. Nowatorskich rozwiązań w ustawie jest znacznie więcej. Doceniając całokształt pracy, trzeba jednak wspomnieć, że nie wszystkie z postulowanych zmian znalazły odzwierciedlenie w nowej ustawie.

Warto chociażby zaznaczyć, że w związku z liberalizacją dostępu do informacji niejawnych o klauzuli „zastrzeżone" pierwotnie postulowano, aby w jednostkach organizacyjnych, w których przetwarzane są informacje tylko o tej klauzuli, nie było obowiązku powoływania pełnomocnika ds. ochrony informacji niejawnych oraz pionu ochrony. Odpowiedzialność za ochronę informacji niejawnych spoczywałaby wówczas na kierowniku jednostki organizacyjnej. Ostatecznie jednak rozwiązanie to nie zostało przyjęte.

---

[24] Tamże.

[25] Ocena skutków regulacji do projektu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 r.

Ustawa z 2010 r. o ochronie informacji niejawnych obowiązuje od 2 stycznia 2011 r. Dotychczasowa praktyka ujawniła drobne trudności interpretacyjne związane m.in. z nową definicją klauzul tajności oraz pojęciem rękojmi zachowania tajemnicy w odniesieniu do zgody kierownika jednostki organizacyjnej wydawanej pracownikom w związku z dostępem do informacji niejawnych o klauzuli „zastrzeżone". Sytuacje problemowe powstają także w związku z postępowaniami odwoławczymi i skargowymi, w przypadku decyzji wydanych jeszcze na podstawie przepisów ustawy z 2005 r. Warto zauważyć, iż przed wejściem w życie ustawy w pionie ochrony informacji niejawnych Agencji Bezpieczeństwa Wewnętrznego dokonano analizy nowych przepisów, mając na względzie ewentualne trudności interpretacyjne lub potrzebę wyjaśnienia wprost nowych rozwiązań. Wyniki tej pracy zostały zamieszczone na stronie internetowej ABW i są stale uzupełniane o nowe komentarze i oficjalne interpretacje przepisów.

Czy zatem po latach praktyki udało się stworzyć system zupełny? Rozważając ten problem trzeba zauważyć, że przyczyną, dla której stosowanie aktualnie obowiązujących przepisów nie niesie za sobą na razie poważnych trudności jest niewątpliwie fakt, iż podstawowy ciężar ochrony informacji wrażliwych spoczywa na pionach ochrony, których praktyka sięga już 12 lat. Ponadto nie bez znaczenia pozostaje treść przepisów przejściowych, zgodnie z którymi przewidziano odpowiednio długie okresy na dostosowanie funkcjonowania jednostek organizacyjnych do nowych regulacji. W art. 181 ustawy określono długi – bo aż 36-miesięczny termin na dokonanie przeglądu w jednostkach organizacyjnych materiałów niejawnych z uwagi na ewentualną potrzebę zmiany lub zniesienia klauzuli tajności. Zgodnie z art. 188 procedury wszczęte i niezakończone przed dniem wejścia w życie nowej ustawy dokonywane są na podstawie przepisów starej ustawy. Przewidziano także 12-miesięczny termin na uzyskanie świadectw bezpieczeństwa przemysłowego przez przedsiębiorców wykonujących umowy związane z dostępem do informacji o klauzuli „poufne", którzy na mocy dotychczasowych przepisów nie byli zobligowani do posiadania takich świadectw.

Przede wszystkim jednak nadal trwają prace nad kluczowymi dla funkcjonowania nowej ustawy rozporządzeniami m.in. o kancelariach tajnych oraz o oznaczaniu materiałów. Te przyczyny powodują, że system nie jest jeszcze komplementarny, a praktyka funkcjonuje nadal w dużym stopniu opierając się na sprawdzonych schematach. A zatem skuteczność nowego systemu podmioty ustawy będą w stanie zweryfikować dopiero wtedy, gdy praktyka ochrony informacji niejawnych zostanie całkowicie dostosowana do nowych przepisów.

Oceniając przepisy ustawy z 2010 r., należy pamiętać, że prawo nie nadąża często za przemianami, jakim ulegają stosunki międzyludzkie. Ustawodawca, tworząc przepisy, nie jest w stanie przewidzieć wszystkich ewentualności. W rezulta-

cie zachodzą sytuacje, których obowiązujące prawo nie normuje, mimo że potrzeba regulacji jest oczywista. Zdarza się też, że ustawodawca celowo pozostawia lukę w tworzonych przepisach. Zwłaszcza gdy odnoszą się one do nowych dziedzin. Dopiero po pewnym czasie, gdy działalność organów stosujących prawo dostarczy praktycznych doświadczeń, wypełnia się tę lukę poprzez wydanie odpowiedniego aktu[26].

Dokonując przeglądu przepisów regulujących ochronę informacji klasyfikowanych, warto także zastanowić się, dlaczego ustawa o ochronie informacji niejawnych była nowelizowana wielokrotnie. Czy świadczy to o słabości tworzonego prawa? Wydaje się, iż główną przyczyną, dla której materia związana z bezpieczeństwem informacji niejawnych musi być w miarę możliwości jak najczęściej aktualizowana jest zarówno szybki rozwój technologii, jak też dynamika zmian społecznych. Te czynniki wymuszają wprowadzanie częstych zmian, aby zapewnić właściwy poziom zabezpieczenia informacji niezwykle istotnych dla stabilności państwa i bezpieczeństwa obywateli.

Czas obowiązywania nowej ustawy jest na tyle krótki, iż nie sposób przewidzieć, w jakim kierunku system ochrony informacji niejawnych będzie dalej ewoluował. Niewątpliwie prezydencja Polski w Unii Europejskiej pozwoli docenić najnowsze zmiany, które mają szczególny wpływ na ochronę międzynarodowych informacji niejawnych. Należy się jednak spodziewać, iż stosowanie przepisów o ochronie informacji niejawnych ukaże również wady opracowanych rozwiązań. Nie można zatem wykluczyć, iż w najbliższych latach ponownie zajdzie potrzeba kompleksowej nowelizacji ustawy o ochronie informacji niejawnych. Przykładowo − kolejnym wyzwaniem, jakie z pewnością zrewolucjonizuje administrację publiczną, jest jej informatyzacja. Uchwalona 17 lutego 2005 r. ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z przepisami wykonawczymi, została w 2010 r. znowelizowana. W jej ramach zmieniono także inne ustawy. Przepisy tej ustawy normują trzy obszary tematyczne:

1) instytucje wspierające informatyzację (zarówno materialnie jak i ustrojowo),

2) rozwiązania dotyczące zasad stosowania technik telekomunikacyjnych i informatycznych w podmiotach publicznych,

3) określone w ustawach szczególnych (materialnych i proceduralnych) do rozwiązań przewidzianych w ustawie o informatyzacji[27].

---

[26] A. Breczko, A. Jamróz, S. Oliwniak, *Wstęp do nauk prawnych*, Białystok 1997, Temida 2, s. 128.

[27] G. Sibiga, *Informatyzacja administracji publicznej w Polsce*, „Edukacja Prawnicza" 2011, nr 3(123).

W ostatniej grupie przepisów zmianie uległy ustawy procesowe, w tym m.in. kodeks postępowania administracyjnego, którego przepisy mają kluczowe znaczenie dla funkcjonowania ustawy o ochronie informacji niejawnych. Chociażby zmiana dotychczasowego brzmienia art. 14 § 1 kpa, zgodnie z którą sprawa administracyjna może zostać załatwiona w formie pisemnej lub w formie dokumentu elektronicznego, co pociąga za sobą daleko idące konsekwencje, otwierając drogę do dalszej informatyzacji procedury administracyjnej. Dla obywatela szczególnego znaczenia nabiera możliwość załatwienia sprawy indywidualnej z wykorzystaniem komunikacji elektronicznej. Warto zauważyć, iż aktualnie kpa przewiduje alternatywne sposoby identyfikacji składającego podanie, będące jednocześnie wymogami co do treści podania:

1) kwalifikowany podpis elektroniczny,

2) podpis potwierdzony profilem zaufanym Elektronicznej Platformy Usług Administracji Publicznej,

3) inne technologie identyfikacji użytkownika, które spełniają warunki techniczne i organizacyjne określone w rozporządzeniu wydanym na podstawie art. 20a ust. 3 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (rozporządzenie nie zostało dotychczas opracowane),

4) podpis osobisty nowego dowodu osobistego[28].

Opisana powyżej zmiana odzwierciedla praktyczne zastosowanie zaledwie jednej ze znowelizowanych jednostek redakcyjnych kpa. Całość zmian, które będą dopiero wdrażane, ma naprawdę rewolucyjny charakter, a ich realizacja w praktyce przyczyni się do przekształcenia państwa analogowego w cyfrowe. Ochrona informacji niejawnych także będzie musiała sprostać nowym wymaganiom.

[28] Tamże.

Stanisław Smykla

Zmiany w przepisach dotyczących ogólnych zasad systemu oraz klasyfikowania informacji niejawnych

Przepisy każdej ustawy, umiejscowione w rozdziale zatytułowanym *Przepisy ogólne*, mają szczególne znaczenie dla całego aktu prawnego. Zawarte w nich są bowiem nie tylko wskazania co do obszaru uregulowanych spraw, właściwych podmiotów, objaśnienia użytych pojęć, ale również *postanowienia wspólne dla wszystkich albo dla większości przepisów merytorycznych zawartych w ustawie*[1]**.** Nie inaczej jest w przypadku rozdziału 1 − *Przepisy ogólne Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[2], zwanej w dalszej części artykułu „ustawą".

Przede wszystkim należy zauważyć, że dokonano zasadniczej zmiany w zakresie określenia przedmiotu ustawy. W art. 1 ust. 1, w którym wymieniono zasady ochrony informacji niejawnych, zastosowany zwrot *to jest zasady* świadczy de facto o ich zamkniętym katalogu. Dotychczas wykaz ten − dzięki użyciu zwrotu *a w szczególności* − był otwarty. Jest to o tyle ważne, że wśród podanych zasad nie zostały wymienione ani kwestie związane z prowadzeniem ewidencji i udostępnianiem danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego, które zostały uregulowane w rozdziale 10 ustawy, ani kwestie dotyczące szkoleń z zakresu ochrony informacji niejawnych, którym poświęcono rozdział 4. Taki nieprecyzyjny zapis, mimo, że nie było to intencją projektodawców[3], może − w ocenie autora − budzić wątpliwości co do traktowania przedmiotowych zagadnień na równi z innymi zasadami dotyczącymi systemu ochrony informacji niejawnych.

Użycie w art. 1 ust. 3 sformułowania *z zastrzeżeniem art. 5* (którego brak w analogicznym art. 1 ust. 3 poprzedniej ustawy[4]) ma wskazywać, że informacje chronione jako *tajemnica zawodowa* lub *inna tajemnica prawnie chroniona* nie są regulowane przepisami ustawy o ochronie informacji niejawnych, chyba, że zacho-

---

[1] *Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (Dz.U. z 2002 r., Nr 100, poz. 908).

[2] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228).

[3] Zapis ten stanowi efekt przyjęcia stosownej poprawki Senatu, zaproponowanej przez legislatorów tej izby (www.senat.gov.pl/k7/kom/kstap/2010/184stap.htm).

[4] *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (tekst jednolity Dz.U. z 2005 r., Nr 196, poz. 1631 z późn. zm.).

dzą przesłanki określone w art. 5[5]. Rozwiązanie to powinno w zdecydowany sposób zmniejszyć ilość wytwarzanych informacji o klauzulach „poufne" i „zastrzeżone" i wyłączyć z systemu ochrony informacji niejawnych inne informacje prawnie chronione, np. dotyczące danych osobowych[6].

Z pozoru istotne, choć w rzeczywistości raczej porządkowe zmiany zostały dokonane także w art. 1 ust. 2, w którym wymieniono podmioty ustawy. Przede wszystkim, poza organami jednostek samorządu terytorialnego, wymienionymi w art. 1 ust. 2 pkt 1 lit. d, podmiotami ustawy są *inne podległe im jednostki organizacyjne lub przez nie nadzorowane*. Uproszczono ponadto nazewnictwo sfery wojskowej, ograniczając się do terminu funkcjonującego w innych ustawach (*jednostki podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane* − art. 1 ust. 2 pkt 2). Z katalogu podmiotów ustawy (z mocy prawa) wyłączono banki państwowe (w art. 1 ust. 2 pkt 3), które jako przedsiębiorcy mogą być podmiotami ustawy na podstawie art. 1 ust. 2 pkt 6. Najistotniejsza zmiana dotycząca określenia podmiotów ustawy została dokonana w art. 1 ust. 2 pkt 6, z którego wykreślono *jednostki naukowe lub badawczo-rozwojowe*. Związane jest to z zastosowaniem w ustawie definicji p r z e d s i ę b i o r c y sensu largo, którym jest każda inna jednostka organizacyjna, niezależnie od formy własności, która w ramach prowadzonej działalności gospodarczej zamierza realizować lub realizuje związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa (art. 2 pkt 13).

Poza pojęciem przedsiębiorcy dodano nowe określenia, np.: *przetwarzanie informacji niejawnych, kierownik przedsiębiorcy* oraz *zatrudnienie*. Najwięcej, bo aż 10 pojęć użytych w art. 2 odnosi się do zagadnień uregulowanych w rozdziale 8 − *Bezpieczeństwo teleinformatyczne*.

Na szczególną uwagę zasługują zmiany w art. 3 dotyczącym stosowania przepisów kodeksu postępowania administracyjnego do procedur opisanych w ustawie. Przede wszystkim wybrane przepisy kodeksu mają mieć zastosowanie do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego. W przeciwieństwie do poprzedniej ustawy[7] nie wymieniono w tym kontekście postępowań odwoławczych. Rozwiąza-

[5] W tej jednostce redakcyjnej zdefiniowano właśnie informacje o klauzuli „ściśle tajne", „tajne", „poufne" i zastrzeżone".

[6] Stosowne zmiany polegające na rezygnacji z klauzuli „zastrzeżone" na dokumentach stosowanych w ramach procedur alimentacyjnych zostały już wprowadzone poprzez *Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 25 stycznia 2011 r. w sprawie rodzinnego wywiadu środowiskowego* (Dz.U. z 2011 r., Nr 27, poz. 138) oraz *Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 23 marca 2011 r. w sprawie wzoru kwestionariusza wywiadu alimentacyjnego oraz wzoru oświadczenia majątkowego dłużnika alimentacyjnego* (Dz.U. z 2011 r., Nr 73, poz. 395).

[7] Art. 1 ust. 4 *Ustawy z dnia 22 stycznia 1999 r. o ochronie...* .

nie to może zostać ocenione jako swego rodzaju niekonsekwencja ustawodawcy, który znacznie rozszerzył uprawnienia strony (osoby sprawdzanej) w trakcie postępowania sprawdzającego (np. art. 24 ust. 7 ustawy) i kontrolnego postępowania sprawdzającego (art. 33 ust. 9-10 ustawy), jednocześnie ograniczając je (poprzez wyłączenie zastosowania przepisów kpa) w postępowaniu odwoławczym. Można polemizować z twórcami uzasadnienia, w którym wyjaśniono tę kwestię w następujący sposób: „pominięcie postępowań odwoławczych w tym artykule ma charakter jedynie porządkujący, gdyż postępowania odwoławcze nie są odrębnym rodzajem postępowań obok postępowań sprawdzających w zakresie bezpieczeństwa osobowego lub bezpieczeństwa przemysłowego, tak więc wskazane w art. 3 przepisy kpa będą miały do postępowań odwoławczych takie samo zastosowanie, jak do wcześniejszych etapów postępowań sprawdzających i będzie to przedmiotem oceny sądów administracyjnych w postępowaniu skargowym”[8]. Wydaje się bowiem, że postępowania odwoławcze są jednak, skoro poświęcono im oddzielny rozdział, odrębnym rodzajem postępowań. Dokumentacja takich postępowań nie jest włączana do akt postępowania sprawdzającego, a procedury odwoławcze kończą się decyzją administracyjną. Jakie skutki będzie mieć nowa redakcja art. 3, pokaże oczywiście praktyka. Należy jednak zauważyć, że wątpliwości tych nie podzielają twórcy doktryny, ponieważ zmiana nie została skomentowana[9].

Odnośnie nowych przepisów kpa, które mają zastosowanie do wymienionych postępowań, rozszerzono ich katalog głównie o te przepisy, które usprawniają realizację procedur[10]. Zmiany nie są zatem radykalne i stanowią de facto usankcjonowanie praktyki i tak już stosowanej w ostatnich latach.

Przepisy zawarte w art. 4 ustawy kończącym rozdział 1, dotyczące zasady *need to know* oraz zasad związanych ze zwalnianiem z obowiązku zachowania tajemnicy oraz kontroli, w tym dostępu do pomieszczeń i materiałów na podstawie innych ustaw, zostały wprost przejęte z art. 3 oraz art. 4 poprzedniej ustawy.

Zasadnicze zmiany wprowadza za to ustawa w zakresie definicji informacji niejawnych oraz ochrony i znoszenia klauzul tajności w rozdziale 2 zatytułowanym *Klasyfikowanie informacji niejawnych*. Przede wszystkim, utrzymując dotychczasowe nazwy klauzul tajności („ściśle tajne”, „tajne”, „poufne” i „zastrze-

[8] Uzasadnienie do projektu ustawy przesłanego do Sejmu (http://orka.sejm.gov.pl/Druki6ka.nsf/wgdrukuj/2791).

[9] S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010 , Wydawnictwo LexisNexis, s. 81-83.

[10] Art. 50 kpa − możliwość składania wyjaśnień przez pełnomocnika lub na piśmie, art. 55 kpa − ułatwienie komunikowania się ze stroną, np. telefonicznie, art. 65 kpa – brak negatywnych konsekwencji w kontekście zachowania terminu w przypadku wniesienia podania do niewłaściwego organu, art. 103 kpa − wstrzymanie biegu terminów w przypadku zawieszenia postępowania.

żone"), zrezygnowano z podziału informacji niejawnych na tajemnicę państwową i tajemnicę służbową. Co więcej, w art. 5 zawarto nowe definicje informacji niejawnych oznaczonych poszczególnymi klauzulami, zastępujące dotychczasowe − w ocenie projektodawców − bardzo ogólne definicje tajemnicy państwowej i służbowej oraz wykazy informacji niejawnych w załączniku do ustawy. Zrezygnowano zatem z definicji, na którą w przypadku informacji o klauzulach „ściśle tajne" i „tajne" składała się przesłanka formalna (potencjalna szkoda w przypadku nieuprawnionego ujawnienia) i materialna (odesłanie do wykazu stanowiącego załącznik do ustawy). Nie mniejsze zmiany dotyczą dotychczasowej „tajemnicy służbowej", ponieważ zrezygnowano z oznaczania klauzulami „poufne" lub „zastrzeżone" informacji chronionych na podstawie innych ustaw, a definicje tych klauzul, podobnie jak w przypadku informacji o klauzulach „ściśle tajne" i „tajne", odniesiono jedynie do ewentualnych szkód, jakie ujawnienie informacji mogłoby przynieść dla bezpieczeństwa i interesów Rzeczypospolitej Polskiej.

W związku z powyższym wydaje się, że osiągnięto wyznaczony cel, jaki przyświecał autorom w momencie przekazywania projektu do akceptacji Rady Ministrów: „dotychczasowe informacje stanowiące tajemnicę państwową lub służbową zostaną ograniczone do informacji niejawnych zawierających w pewnym sensie „tajemnicę państwową o czterech klauzulach, przy czym znaczna część informacji do tej pory „ściśle tajnych" powinna być klauzulowana jako „tajne" lub „poufne", „tajnych" jako „poufne" lub „zastrzeżone", a większość informacji stanowiących tajemnicę służbową, z wyjątkiem odnoszących się do interesu państwa, powinna przestać być chroniona na podstawie ustawy o ochronie informacji niejawnych".

Tym samym w przypadku informacji o klauzulach „ściśle tajne", „tajne" i „poufne" muszą być spełnione łącznie dwie przesłanki:

- nieuprawnione ujawnienie tych informacji musi zagrażać wymienionym enumeratywnie (zróżnicowanym adekwatnie do klauzuli) dobrom,

- nieuprawnione ujawnienie tych informacji spowoduje dla Rzeczypospolitej Polskiej – w przypadku „ściśle tajnych" – „szkodę wyjątkowo poważną", „tajne" – „szkodę poważną", „poufne" – „szkodę".

Informacjom niejawnym nadaje się natomiast klauzulę „zastrzeżone", *jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej*.

Nie rozstrzygając kwestii, czy wprowadzone nowe definicje są bardziej, czy mniej ogólne od poprzednich, należy zwrócić uwagę, że przynajmniej w zakresie uznania danych osobowych funkcjonariuszy, żołnierzy lub pracowników operacyjnych za informacje niejawne o klauzuli „ściśle tajne" można mówić o zdecydowanym uściśleniu w stosunku do obowiązującego do tej pory stanu prawnego. Najwyższą klauzulę tajności nadaje się bowiem informacjom niejawnym, których nieuprawnione ujawnienie spowoduje wyjątkową szkodę dla RP poprzez to, że *doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie*. Zgodnie zaś z obowiązującą wcześniej definicją klauzula „ściśle tajne" powinna być nadawana danym identyfikującym lub mogącym doprowadzić do identyfikacji funkcjonariuszy i żołnierzy służb, o których mowa w załączniku nr 1, pkt 16 poprzedniej ustawy[11], realizujących czynności operacyjno-rozpoznawcze (art. 2 pkt 1 w zw. z punktem I.18 załącznika nr 1).

Bez wątpienia nowe definicje informacji niejawnych mogą wywoływać wiele wątpliwości zarówno u pracowników jednostek będących podmiotami ustawy, jak też u przedstawicieli środowisk (np. dziennikarskich, organizacji pozarządowych), których problem ten dotyczy w sposób pośredni. Wątpliwościom, na które zwracano uwagę już na etapie przekazania przez Kancelarię Prezesa Rady Ministrów projektu ustawy do konsultacji międzyresortowych, sprowadzającym się głównie do tego, że *przyznawanie klauzuli tajności materiałom wyłącznie na podstawie mało precyzyjnej definicji ustawowej utrudni właściwe klasyfikowanie informacji niejawnych oraz spowoduje, że tym samym informacjom w poszczególnych jednostkach organizacyjnych będą nadawane różne klauzule tajności*, nie można odmówić racjonalności. Należy jednak pamiętać, że koncepcja nowego zdefiniowania informacji niejawnych wynikała także z docierających do KPRM opinii, że dotychczasowe przepisy w tym zakresie są niedoskonałe. Oceny te formułowały często te same podmioty, które później negowały założenia nowej koncepcji. Wydaje się, że zasób zdobytych doświadczeń, wynikający z przeszło jedenastu lat stosowania przepisów poprzedniej ustawy, powinien pomóc we właściwym stosowaniu przepisów i określaniu klauzul tajności, a co za tym idzie − ochronie informacji niejawnych. Należy się w tym kontekście spodziewać częstego stosowania instytucji „rozstrzygania sporu", w trybie art. 9, o którym będzie mowa w dalszej części artykułu.

[11] Tj. o Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego oraz byłego Urzędu Ochrony Państwa i byłych Wojskowych Służb Informacyjnych.

Zasadnicze zmiany zostały też wprowadzone jeśli chodzi o zniesienie lub zmianę nadanej klauzuli tajności, których głównym przejawem jest odejście od ustawowo określonych terminów obowiązywania klauzul na rzecz możliwości zniesienia lub zmiany klauzuli w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Oczywiście nie oznacza to, iż nadanie dokumentowi np. klauzuli tajności „zastrzeżone" spowoduje jego ochronę przez kilkadziesiąt lat. Powstawaniu ewentualnych nieracjonalnych sytuacji zapobiegnie obowiązek przeglądu wszystkich wytworzonych dokumentów niejawnych raz na pięć lat w celu określenia, czy informacje te spełniają nadal ustawowe przesłanki, które były podstawą nadania im klauzuli tajności (art. 6 ust. 4 ustawy). Jeżeli przegląd wykaże brak przesłanek do dalszej ochrony tych informacji na określonym poziomie, to nastąpi zmiana lub zniesienie nadanej klauzuli. Ponadto w przepisach przejściowych i końcowych (art. 181 ustawy) nałożono na kierowników jednostek organizacyjnych obowiązek przeprowadzenia w terminie 36 miesięcy od dnia wejścia w życie ustawy przeglądu wytworzonych w podległych im jednostkach materiałów w celu ustalenia, czy spełniają przesłanki ochrony zgodne z nowymi definicjami informacji niejawnych wprowadzonymi przez ustawę.

Na większą elastyczność systemu wskazuje także możliwość określenia z góry (niezależnie od klauzuli) daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności oraz nadawania odrębnie klauzul tajności poszczególnym częściom jednego materiału (art. 6 ust. 2 i 8 ustawy).

Warto także zwrócić uwagę na modyfikację samej decyzji dotyczącej zniesienia lub zmiany klauzuli tajności. Nadal upoważnienie w tym zakresie posiada osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, ale normą ustawową stał się obowiązek *wyrażenia pisemnej zgody* (dotychczas kwestię tę regulowały przepisy odpowiedniego rozporządzenia). Przepis ten (art. 6 ust. 3) wraz z zastrzeżeniem, że decyzja taka może zostać wyrażona wyłącznie *w przypadku ustania lub zmiany ustawowych przesłanek ochrony* powinien skutecznie zabezpieczyć informacje niejawne przed nieuzasadnionym znoszeniem lub zmianą klauzul tajności. Szczególnej ochronie ustawodawca poddał informacje o klauzuli „ściśle tajne", w przypadku których decyzję o zmianie lub jej zniesieniu podjąć może wyłącznie kierownik jednostki organizacyjnej, a więc osoba, która na podstawie art. 14 ustawy ponosi w największym stopniu odpowiedzialność za ochronę informacji niejawnych w danej jednostce organizacyjnej.

Możliwość dokonania zmian i zniesienia klauzul (o której mowa w art. 6 ustawy) nie dotyczy jednak wszystkich kategorii informacji niejawnych. Wyłączeniu w tym zakresie podlegają informacje wskazane w art. 7 ust. 1 ustawy, które mają podlegać ochronie bez względu na upływ czasu, czyli informacje mogące

identyfikować funkcjonariuszy, żołnierzy lub pracowników służb i instytucji wykonujących czynności operacyjno-rozpoznawczych, a także osoby udzielające pomocy w wykonywaniu tych czynności. Należy zauważyć, że przepis ten nie jest prostym powtórzeniem art. 25 ust. 2 poprzedniej ustawy. Zgodnie bowiem z poprzednim stanem prawnym ochronie bez względu na upływ czasu podlegać miały dane identyfikujące funkcjonariuszy i żołnierzy, ale tylko ABW, AW, SKW, SWW i CBA oraz byłego UOP i byłych WSI (czyli służb specjalnych) wykonujących czynności operacyjno-rozpoznawcze. Obecnie szczególnej ochronie podlegać mają także dane np. funkcjonariuszy Policji, Straży Granicznej czy pracowników wywiadu skarbowego spełniających kryteria, o których mowa w art. 7 ust. 1 ustawy.

Bardzo ważnym elementem założonego przez autorów projektu ustawy uszczelniania systemu jest wprowadzona w art. 9 ustawy możliwość *odwołania się* od decyzji wytwórcy dotyczącej nadania klauzuli tajności do ABW lub SKW, a w przypadku sporu z jedną z tych służb − do Prezesa Rady Ministrów. W dotychczasowym systemie odbiorca mógł tylko apelować do wytwórcy o zmianę nieprawidłowej klauzuli. Nowa regulacja może przyczynić się do znacznego ograniczenia liczby przypadków bezpodstawnego zawyżania lub zaniżania klauzul tajności.

Istotne znaczenie, jako z jednej strony swego rodzaju podsumowanie ogólnych zasad dotyczących ochrony informacji, z drugiej zaś wprowadzenie do szczegółowych przepisów dotyczących bezpieczeństwa osobowego, bezpieczeństwa fizycznego oraz bezpieczeństwa teleinformatycznego, ma art. 8 ustawy, zgodnie z którym informacje niejawne, którym nadano określoną klauzulę tajności:

1) mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności,

2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności,

3) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Przedstawione wyżej zasady zostały sprecyzowane w poszczególnych rozdziałach ustawy. Zgodnie z założeniami projektodawców przepisy miały zostać

uaktualnione, by doprowadzić do uproszczenia systemu ochrony informacji niejawnych. Przy tworzeniu konkretnych rozwiązań korzystano przede wszystkim z dotychczas obowiązujących rozwiązań.

W niektórych przypadkach regulacje zostały wprost przeniesione z *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, a w innych wykorzystano stosowane już rozwiązania, jeśli przepisy nowej ustawy na to pozwalały. Znaleźć można także wiele oryginalnych, znacznie odbiegających od dotychczasowych, rozstrzygnięć, które zostaną dopiero sprawdzone w działaniu. Na ile ustawa spełni oczekiwania projektodawców i innych jej podmiotów oraz cele ustawodawcy, pokaże praktyka.

Sylwia Stefaniak

„Klucz kodowy" zmian w obowiązujących przepisach wprowadzonych nową ustawą o ochronie informacji niejawnych

Niniejszy artykuł odnosi się do zmian aż w 107 przepisach obowiązujących aktów prawnych, które wprowadza nowa ustawa o ochronie informacji niejawnych z 5 sierpnia 2010 r.[1] Za pomocą swoistego „klucza kodowego" wskazano obszary merytoryczne nowelizowanych aktów normatywnych, uwzględniając wpływ danych regulacji na funkcjonowanie społeczeństwa w różnych dziedzinach oraz na ich powiązanie z systemem ochrony informacji niejawnych.

Tworząc przedmiotową klasyfikację, skoncentrowano się na określeniu celu oraz zakresie omawianych zmian.

Wprowadzenie

Dla prawidłowego funkcjonowania państwa, a zwłaszcza instytucji państwowych i przedsiębiorców, niezbędne jest ograniczenie dostępu do niektórych istotnych informacji. W tym celu nieuniknione staje się stworzenie systemu ochrony informacji niejawnych, który będzie zapobiegał powstawaniu szkód w trakcie wykonywania przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie ochrony obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczpospolitej Polskiej.

Dotychczas zasady systemu ochrony informacji niejawnych określała *Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych*[2], zwana w dalszej części artykułu „poprzednią UOIN", która obowiązywała do 1 stycznia 2011 r.

Niestety z uwagi na zbyt pośpieszne tworzenie tego aktu normatywnego, co było spowodowane koniecznością spełnienia wymagań przystąpienia Rzeczpospolitej Polskiej do Traktatu Północnoatlantyckiego[3], zawierał on niespójności i nielogiczności, a w niektórych miejscach brakowało związku przyczynowo-skutkowego pomiędzy poszczególnymi przepisami.

---

[1] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228).

[2] *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. z 2005 r., Nr 196, poz. 1631).

[3] Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. wraz z protokołem do Traktatu o akcesji Rzeczypospolitej Polskiej, podpisanym w Brukseli dnia 16 grudnia 1997 r. (Dz.U. z 2000 r., Nr 87, poz. 970).

Niespójności kodyfikacyjne usiłowano uzupełniać licznymi nowelizacjami − w sumie było ich 24 − w tym najważniejsza z 15 kwietnia 2005 r.[4], najbardziej wpływająca na zmianę pierwotnego tekstu. Niestety mnogość noweli często ograniczała klarowność przekazu poprzedniej UOIN, a wciąż pojawiały się zagadnienia problematyczne wynikające z praktycznego stosowania przepisów.

Co więcej, zarówno przy wprowadzaniu poprzedniej UOIN, jak i licznych nowelizacji do niej, nie dokonano wnikliwego przeglądu innych aktów prawnych, na które ona oddziaływała, co wiązało się z powstawaniem wielu niekonsekwencji oraz częstego nieuzasadnionego stosowania zaostrzonego rygoru wobec danych, które w rzeczywistości nie spełniały przesłanek określonych przedmiotową regulacją i nie można ich było zaklasyfikować jako informacje niejawne.

Niezbędna stała się zatem zmiana treści całej poprzedniej ustawy, tak aby była ona bardziej precyzyjna, przejrzysta i maksymalnie uproszczona. Aby jednak sztucznie nie nakładać nowej kodyfikacji na poprzednie rozwiązania, zdecydowano o rozpoczęciu procesu legislacyjnego nad nowym aktem prawnym, który korzystałby z wcześniejszego dorobku.

Rezultatem podjętych prac jest uchwalenie przez parlament Rzeczpospolitej Polskiej *Ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych*[5], zwanej dalej „nową UOIN", która została podpisana przez Prezydenta Rzeczpospolitej Polskiej 30 sierpnia 2010 r. i wdrożona 2 stycznia 2011 r. z wyjątkiem art. 131, który wejdzie w życie 1 stycznia 2013 r.

W odróżnieniu od obowiązującej wcześniej ustawy w rozdziale 11. nowej UOIN uwzględniono szeroki zakres zmian w innych przepisach, gdyż odwołano się aż do 107 obowiązujących aktów prawnych, wobec których stosowano zasady systemu ochrony informacji niejawnych lub będzie się stosowało zmodyfikowane zasady systemu ochrony informacji niejawnych.

Ponieważ obszar tematyczny nowelizowanych aktów normatywnych odnosi się do wielu dziedzin życia społecznego, w celu stworzenia bardziej klarownego przekazu postanowiono utworzyć swoisty „klucz kodowy", który ułatwi zapoznanie się z ich treścią. „Klucz kodowy" jest bowiem dokumentem upraszczającym czy też uogólniającym zagadnienia, co umożliwia ich analizę i interpretację. Co ważne, jest to także sposób scalania podobnych kwestii we wspólne grupy, co tworzy wewnętrzną strukturę pozwalającą dostrzec cele i rodzaje wprowadzanych zmian.

---

[4] *Ustawa z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw* (Dz.U. z 2005 r., Nr 85, poz. 727) weszła w życie 16 czerwca 2005 r.

[5] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji...* .

Tworząc przedmiotowy „klucz kodowy", bazowano głównie na klasyfikacji działów administracji rządowej[6] oraz na podziale instytucji państwowych zawartym w Konstytucji Rzeczpospolitej Polskiej[7], gdyż najbardziej odpowiadają one zagadnieniom regulowanym w nowelizowanych ustawach (np. finanse publiczne, zdrowie, zabezpieczenie społeczne czy sądy i trybunały). Dodano również inne kategorie uwzględniające specyfikę regulacji o ochronie informacji niejawnych, np. służby i instytucje upoważnione do przeprowadzania postępowań sprawdzających.

Dokonane zmiany w treści przedmiotowych regulacji prawnych mają albo charakter porządkowy, czyli polegają jedynie na zmianie stosowanego dotychczas nazewnictwa i uaktualniają powoływane przepisy prawne, albo zmieniają zakres informacji traktowanych jako tajemnice prawnie chronione, albo też istotnie wpływają na treść obowiązujących aktów normatywnych poprzez wprowadzanie nowych rozwiązań lub nawet rezygnację z odwoływania się do systemu ochrony informacji niejawnych.

Kategorie klasyfikacyjne w „kluczu kodowym"

Przyjęte w „kluczu kodowym" kryteria klasyfikacyjne, ujmujące zagadnienia zmienione nową UOIN, wyodrębniono, opierając się na odpowiednio zmodyfikowanych działach administracji rządowej oraz podziałach instytucji wyszczególnionych w Konstytucji RP takich jak:

1. Obrona narodowa i wojskowość,
2. Służby i inspekcje,
3. Sądy, trybunały oraz prokuratura,
4. Organy kontroli państwowej i ochrony prawa,
5. Parlamentarzyści,
6. Przekazywanie informacji,
7. Finanse publiczne,
8. Gospodarka i prowadzenie działalności gospodarczej,

[6] *Ustawa z dnia 4 września 1997 r. o działach administracji rządowej* (Dz.U. z 2007 r., Nr 65, poz. 437 z późn. zm.).

[7] Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., Nr 78, poz. 483 z późn. zm.), zwana dalej „Konstytucją RP".

9. Gospodarka morska i wodna,

10. Geodezja i budownictwo,

11. Nauka i umiejętności,

12. Praca,

13. Zabezpieczenie społeczne,

14. Zdrowie,

15. Środowisko.

Ponadto, z uwagi na częstość występowania pewnych grup zagadnień, uwzględniono także dodatkowe kategorie: *Korpus urzędniczy, Kodeksy* oraz *Służby i instytucje upoważnione do przeprowadzania postępowań sprawdzających.*

Wyróżniono również kategorie *Inne*, do której będą klasyfikowane przepisy niezaliczające się do żadnych z powyższych kategorii.

Przedmiotowy „klucz kodowy" zbudowany jest z 19 kategorii tematycznych, odpowiadających głównym zagadnieniom. Właściwe zatem staje się przedstawienie, jakie konkretnie nowelizowane akty normatywne zostały zaklasyfikowane do poszczególnych kategorii, a także czym kierował się ustawodawca dokonując w ich treści zmian.

1. Obrona narodowa i wojskowość

Do tej kategorii zaliczono zagadnienia związane z wojskowością, czyli powszechny obowiązek obrony Rzeczypospolitej Polskiej, służba wojskowa żołnierzy zawodowych, zakwaterowanie Sił Zbrojnych, wyroby przeznaczone na potrzeby obronności i bezpieczeństwa państwa oraz broń chemiczna.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *w przepisach ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r., Nr 196, poz. 1631, z późn. zm.)* określeniem *przepisy o ochronie*

informacji niejawnych − art. 78 i art. 135 nowej UOIN (wszystkie przytaczane w wyliczeniu artykuły odnoszą się do nowej UOIN – przyp. red.),

- uaktualniono stan prawny i zastąpiono określenie *w przepisach ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* na określenie *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* – art. 151 pkt 2, art. 169,

- uaktualniono nazwy pojęć ustawowych, rezygnując z określenia *specjalne postępowania sprawdzające* oraz *służby ochrony państwa* – art. 78 i art. 169,

- dokonano porządkowej zmiany, zastępując określenie *tajemnica ustawowo chroniona* na określenie *tajemnica prawnie chroniona* – art. 102,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa lub tajemnica służbowa* − art. 151 pkt 3;

b) wprowadzenie nowej regulacji:

- dodano, iż zwykłe postępowanie sprawdzające przeprowadza właściwy wojskowy komendant uzupełnień − art. 78 pkt;

c) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez żołnierzy zawodowych, z zastrzeżeniem, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla klauzuli „zastrzeżone" nie stanowiąc de facto i de iure informacji niejawnej – art. 151 pkt 1.

2. Służby i instytucje umocowane do przeprowadzania postępowań sprawdzających

Do tej kategorii zaliczono służby i instytucje wymienione w art. 23 ust. 2 i 5 nowej UOIN, czyli Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Agencję Wywiadu, Centralne Biuro Antykorupcyjne, Biuro Ochrony Rządu, Policję, Służbę Więzienną, Służbę Wywiadu Wojskowego, Straż Graniczą oraz Żandarmerię Wojskową, które uprawnione są do przeprowadzania postępowań sprawdzających.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *w ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r., Nr 196, poz. 1631, z późn. zm.)* określeniem *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* − art. 92 pkt 1, art. 93 pkt 1, art. 133 pkt. 2 i 3, art. 141 pkt 1, art. 144 pkt 5, art. 165 pkt 2 i 4-6 i art. 178 pkt 2,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 92 pkt 2 i 5, art. 93 pkt 3, art. 105, art. 141 pkt 5, art. 144 pkt 1 lit. a, pkt 2, 3, 4, 6, 7, 9, 11 i 12, art. 164 pkt 1-4 i pkt 6-7, art. 165 pkt 3-4, 7-8, art. 166 i art. 178 pkt 1,

- zrezygnowano z określenia ABW jako *służby ochrony państwa* i zastąpiono je określeniem, iż wykonuje ona *zadania związane z ochroną informacji niejawnych* − art. 144 pkt 1 lit. b,

- zrezygnowano z określenia SKW jako *służby ochrony państwa*, ale też w żaden sposób nie podkreślono, iż będzie ona nadal wykonywała *zadania związane z ochroną informacji niejawnych* − art. 165 pkt 1,

- w przepisach dotyczących postępowania w razie odmowy zwolnienia funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych od obowiązku zachowania tajemnicy albo odmowy zezwolenia na udostępnienie dokumentów lub materiałów objętych tajemnicą pomimo żądania prokuratora lub sądu wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 105, art. 141 pkt 2-4, art. 144 pkt 8, art.164 pkt 5, art. 165 pkt 9;

b) wprowadzenie nowej regulacji:

- dodano funkcjonariuszy Biura Ochrony Rządu do podmiotów, którym minister właściwy do spraw wewnętrznych zezwala na udzielenie wiadomości stanowiącej informacje niejawne określonej osobie lub instytucji – art. 105. Warte podkreślenia jest, iż w zmienianym akcie prawnym nie wymienia się już żołnierzy jednostek, wcześniej podporządkowanych

lub nadzorowanych przez ministra właściwego do spraw wewnętrznych,

- dodano *prokuratora Biura Lustracyjnego Instytutu Pamięci Narodowej* − art. 105;

c) zmianę treści składanych ślubowań poprzez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez podejmującego służbę w Policji, Straży Granicznej, Biurze Ochrony Rządu oraz w Służbie Więziennej, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *strzec tajemnicy państwowej i służbowej* wprowadzono *strzec tajemnic związanych ze służbą* – art. 92 pkt 3, art. 93 pkt 4, art. 133 pkt 1 i art. 178 pkt 3,

- uwzględniono zmianę w treści ślubowania składanego przez podejmującego służbę w ABW, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *strzec tajemnicy państwowej i służbowej* wprowadzono *strzec tajemnicy prawnie chronionej* − art. 144 pkt 10;

d) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez policjantów i strażników granicznych, z zastrzeżeniem, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla klauzuli „zastrzeżone", nie stanowiąc de facto i de iure informacji niejawnej – art. 92 pkt 4 i art. 93 pkt 5.

3. Służby i inspekcje

Do tej kategorii zaliczono służby i inspekcje zajmujące się głównie sprawami wewnętrznymi, a często porządkowymi, takie jak: służba celna, straż pożarna, straż gminna i państwowa inspekcja sanitarna.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego:

- uaktualniono stan prawny i zastąpiono określenie *przepisów o tajemnicy celnej nie stosuje się do informacji podlegających ochronie na podstawie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* określeniem *przepisów o tajemnicy celnej nie stosuje się do informacji podlegających ochronie na podstawie przepisów o ochronie informacji niejawnych* – art. 177 pkt 1,

- wprowadzono określenie *informacje niejawne* zamiast pojęcia *tajemnica państwowa lub służbowa* – art. 105,

- w przepisach dotyczących postępowania w razie odmowy zwolnienia funkcjonariusza, pracownika lub osoby udzielającej im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych od obowiązku zachowania tajemnicy albo odmowy zezwolenia na udostępnienie dokumentów lub materiałów objętych tajemnicą, pomimo żądania prokuratora lub sądu, wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 105;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- uzyskane przez organy Państwowej Inspekcji Sanitarnej w trakcie kontroli informacje, dokumenty i inne dane stanowiące tajemnicę kontrolowanego nie są objęte tajemnicą służbową, ale traktowane jako *tajemnica prawnie chroniona* – art. 86,

- określono, iż do obowiązków strażnika gminnego należy *zachowanie tajemnicy prawnie chronionej*, a nie jak wcześniej *tajemnicy państwowej i służbowej* – art. 117;

c) zmianę treści składanych ślubowań poprzez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez podejmującego służbę w Państwowej Straży Pożarnej, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *strzec tajemnicy państwowej i służbowej* lub *dochować tajemnicy państwowej i służbowej* wprowadzono *strzec tajemnic związanych ze służbą* − art. 97 pkt 1;

d) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez strażaków oraz przez funkcjonariuszy Służby Celnej, z zastrzeżeniem jednak, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla klauzuli „zastrzeżone" nie stanowiąc de facto i de iure informacji niejawnej − art. 97 pkt 2 i art. 177 pkt 2.

4. Korpus urzędniczy

Do tej kategorii zaliczono pracowników urzędów państwowych.

Wprowadzona zmiana polega na określeniu, iż do obowiązków urzędnika państwowego należy *dochowanie tajemnicy związanej z wykonywaniem obowiązków*, a nie jak wcześniej *tajemnicy państwowej i służbowej* – art. 82.

5. Parlamentarzyści

Do tej kategorii zaliczono zagadnienia związane z posłami i senatorami.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego:

- wprowadzenie określenia *informacje niejawne* zamiast pojęcia *tajemnica państwowa lub służbowa* – art. 104,

- wprowadzenie określenia *tajemnica informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne"* zamiast pojęcia *tajemnica państwowa* – art. 125 pkt 1 i 2;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- określono, iż wiadomości uzyskane w toku przesłuchań przez sejmową komisję śledczą stanowią *tajemnicę prawnie chronioną*, a nie jak wcześniej *tajemnicę służbową* – art. 125 pkt 3;

c) wprowadzenie nowej regulacji:

- dodano, iż posłowie i senatorowie w ramach wykonywanego mandatu mają prawo wstępu do pomieszczeń, w których znajdują się informacje i materiały, z zachowaniem przepisów o tajemnicy prawnie chronionej – – art. 104;

d) usunięcie regulacji:

- uchylenie przepisów dotyczących dostępu posłów i senatorów do *wiadomości stanowiących tajemnicę państwową o szczególnie ważnym znaczeniu dla obronności Państwa, Sił Zbrojnych i bezpieczeństwa Państwa, oznaczonych klauzulą „tajne specjalnego znaczenia"* – art. 89.

6. Sądy, trybunały oraz prokuratura

Do tej kategorii zaliczono zagadnienia związane z funkcjonowaniem sądów powszechnych, wojskowych i administracyjnych, Trybunału Stanu i Trybunału Konstytucyjnego oraz prokuratury, ale także kwestie dotyczące aplikantów w Krajowej Szkole Sądownictwa i Prokuratury, komorników sądowych i kuratorów sądowych oraz pracowników sądów i prokuratury. Ponadto w tej kategorii ujęto Instytut Pamięci Narodowej, który w swej strukturze organizacyjnej ma prokuratorów. Dołączono też notariuszy, którzy uwzględniani są w wymiarze sprawiedliwości.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r., Nr 196, poz. 1631, z późn. zm.)* określeniem *w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* − − art. 139 pkt 2,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 80 pkt 1 i 2, art. 112, art. 123 pkt 1 i 2, art. 146,

- w przepisach dotyczących postępowania dyscyplinarnego w przypadku ujawnienia informacji z postępowania karnego stanowiących tajem-

nicę wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 88 pkt 3,

- w przepisach dotyczących możliwości wyłączenia jawności rozpraw toczących się przed Trybunałem Stanu oraz Trybunałem Konstytucyjnym wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* – art. 80 pkt 3 i art. 112,

- w przepisach dotyczących zastrzeżenia dostępu do określonych dokumentów przechowywanych w Instytucie Pamięci Narodowej wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* – art. 123 pkt 3;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- określono, iż do obowiązków pracowników sądów i prokuratury należy *zachowanie tajemnicy prawnie chronionej*, a nie jak wcześniej *tajemnicy państwowej i służbowej* – art. 124;

c) rezygnację z dotychczasowej regulacji:

- zrezygnowano z uwzględniania w dotychczas składanym przez notariusza ślubowaniu, iż dochowuje on *tajemnicy państwowej i zawodowej* i pozostawiono określenie *tajemnica zawodowa*;

d) zmianę treści składanych ślubowań przez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez prokuratora, radcę i starszego radcę Prokuratorii Generalnej, sędziów sądów wojskowych, sądów powszechnych oraz Sądu Najwyższego, referendarza sądowego, ławników, aplikanta w Krajowej Szkole Sądownictwa i Prokuratury, komornika sądowego oraz kuratora sądowego, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *dochować tajemnicy państwowej i służbowej* lub *dochować tajemnicy służbowej*, lub *dochować tajemnicy państwowej* wprowadzono *dochować tajemnicy prawnie chronionej* − art. 88 pkt 1, art. 118 pkt 1, art. 138, art. 139 pkt 1, art. 139 pkt 4-5, art. 147, art. 161 i art. 175;

e) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez prokuratora i sędziów sądów wojskowych oraz sądów powszechnych, komornika sądowego z zastrzeżeniem jednak, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla klauzuli „zastrzeżone", nie stanowiąc de facto i de iure informacji niejawnej – art. 88 pkt 2, art. 113, art. 118 pkt 2, art. 139 pkt 3.

7. Kodeksy

Do tej kategorii zaliczono zmiany wprowadzane w kodeksie postępowania administracyjnego, kodeksie postępowania cywilnego, kodeksie postępowania karnego, kodeksie karnym, kodeksie karnym wykonawczym oraz kodeksie pracy. Dodatkowo do tej kategorii włączono przepisy ściśle powiązane z prawem karnym, czyli ustawę o świadku koronnym oraz o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Wśród wprowadzonych zmian znalazły się:

a) aktualizacja stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 75 pkt 2, art. 77 pkt 1 i 2, art. 108 pkt 4, 6-7, art. 111 i art. 129,

- w przepisach dotyczących wyłączenia prawa do przeglądu akt, ale też sporządzania odpisów i kserokopii, wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 75 pkt 1, art. 108 pkt 1,

- w przepisach dotyczących wyłączenia możności bycia świadkiem przez wojskowych i urzędników wprowadzono doprecyzowanie klauzul tajności „zastrzeżone" i „poufne" zamiast dotychczasowego określenia *tajemnica służbowa* − art. 77 pkt 3,

- w przepisach określających przestępstwa przeciwko ochronie informacji niejawnych wprowadzono doprecyzowanie klauzul tajności „zastrzeżone" i „poufne" zamiast dotychczasowego określenia *tajemnica służbo-*

wa oraz klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 107,

- w przepisach dotyczących przesłuchania osób obowiązanych do zachowania tajemnicy wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* oraz klauzul tajności „zastrzeżone" i „poufne" zamiast dotychczasowego określenia *tajemnica służbowa* − art. 108 pkt 2 i art. 140 pkt 1,

- w przepisach dotyczących świadka anonimowego wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 108 pkt 5,

- w przepisach dotyczących przekazania informacji uzyskanych podczas zatrzymania rzeczy lub podczas przeszukania wprowadzono doprecyzowanie klauzul tajności „zastrzeżone" i „poufne" zamiast dotychczasowego określenia *tajemnica służbowa* – art. 108 pkt 6,

- w przepisach dotyczących kontroli i utrwalania rozmów wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 108 pkt 8,

- w przepisach dotyczących doręczenia oskarżonemu odpisu aktu oskarżenia bez uzasadnienia oraz wniesienia apelacji przez prokuratora, obrońcę lub pełnomocnika wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 108 pkt 9 i 11,

- w przepisach dotyczących wyłączenia jawności postępowania karnego oraz postępowania w sprawach o wykroczenia wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 108 pkt 10 i art. 140 pkt 2,

- w przepisach dotyczących kierowania przez sąd orzeczenia do wykonania wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 109;

b) nowa regulacja:

- dodano, iż wzajemne zobowiązania wynikające z układu zbiorowego pracy nie naruszają przepisów o ochronie informacji niejawnych – art. 79.

8. Organy kontroli państwowej i ochrony państwa

Do tej kategorii zaliczono organy kontroli państwowej i ochrony państwa wymienione w Konstytucji RP, czyli Rzecznika Praw Obywatelskich, Najwyższą Izbę Kontroli, oraz kwestie związane z radiofonią i telewizją. Ponadto uwzględniono także Rzecznika Praw Dziecka.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 99,

- w przepisach dotyczących prowadzonego przez Rzecznika Praw Obywatelskich postępowania wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − art. 90 pkt 2,

- w przepisach dotyczących przesłuchania osób obowiązanych do zachowania tajemnicy wprowadzono doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* oraz klauzul tajności „zastrzeżone" i „poufne" zamiast dotychczasowego określenia *tajemnica służbowa* − art. 101 pkt 3,

- wprowadzono zmianę nieaktualnego nazewnictwa klauzuli tajności z określenia „tajne specjalnego znaczenia" na określenie „ściśle tajne" – – art. 101 pkt 1;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- określono, iż odmowa udzielenia wyjaśnień kontrolerom Najwyższej Izby Kontroli może nastąpić jedynie w przypadkach, gdy kontroler nie posiada właściwego upoważnienia, a wyjaśnienia mają dotyczyć *tajemnicy prawnie chronionej*, a nie jak wcześniej *tajemnicy ustawowo chronionej innej niż tajemnica służbowa* – art. 101 pkt 2;

c) zmianę treści składanych ślubowań poprzez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez Rzecznika Praw Obywatelskich i Rzecznika Praw Dziecka, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *dochować tajemnicy państwowej i służbowej* wprowadzono *dochować tajemnicy prawnie chronionej* − − art. 90 pkt 1, art. 126.

9. Przekazywanie informacji

Do tej kategorii zaliczono przekazywanie informacji publicznych, kryminalnych, danych osobowych, informacji o dokumentach organów bezpieczeństwa państwa oraz informacji gospodarczych, a także o prawie prasowym oraz informatyzacji działalności podmiotów realizujących zadania publiczne, oraz o podpisie elektronicznym.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* na określenie *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* − − art. 136 pkt 1, art. 143 pkt 2, art. 159 pkt 1, art. 179,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 121, art. 136 pkt 2, art. 142, art. 159 pkt 2, art. 168,

- w przepisach dotyczących przekazywania informacji kryminalnych za granicę zrezygnowano z określenia *właściwa służba ochrony państwa* na rzecz określenia *krajowa władza bezpieczeństwa* oraz odstąpiono od powoływania się na nieaktualną *ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* na rzecz określenia *przepisy o ochronie informacji niejawnych* – art. 136 pkt 3,

- w przepisach dotyczących wydawania certyfikatów urządzeń zrezygnowano z określenia *służba ochrony państwa* na rzecz określenia *Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego* – art. 143 pkt 1,

- w przepisach dotyczących kontroli zgodności przestrzegania ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne wprowadzono doprecyzowanie klauzul tajności. Co ważne, poszerzono je o dostęp do klauzuli „poufne" – art. 159 pkt 3;

b) rezygnację z dotychczasowych regulacji:

- zrezygnowano z określenia, iż *dziennikarz nie może opublikować informacji, jeżeli osoba udzielająca jej zastrzegła to ze względu na tajemnicę służbową*, pozostawiając tylko *tajemnicę zawodową* – art. 85.

10. Finanse publiczne

Do tej kategorii zaliczono kwestie związane z podatkami, kontrolą skarbową, giełdą towarową oraz prawem bankowym.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* na określenie *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* − art. 176,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 103, art. 119 pkt 1 i 3-6, art. 158,

- wskazując podmioty uprawnione do uzyskiwania informacji i przeglądu akt, zastosowano nowe nazewnictwo ustawowe, w którym rezygnuje się z określenia *służby ochrony państwa* na rzecz *Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego* − art. 98 pkt 2, art. 119 pkt 8-9 oraz art. 120,

- wśród podmiotów, którym udzielone są informacje wymieniono organy i służby z art. 23 ust. 5 nowej UOIN uprawnione do przeprowadzania postępowań sprawdzających − art. 98 pkt 2, art. 119 pkt 8-9, art. 120, art. 128 i art. 162;

b) wprowadzenie nowych regulacji:

- wskazano, iż Prezes Rady Ministrów będzie określał, ze względu na ochronę informacji niejawnych, w drodze zarządzenia, odrębny tryb poboru podatku dochodowego, tryb składania informacji i zeznań podatkowych, a także dodatkowe zadania płatników związane z obowiązkiem rozliczania rocznego podatków − art. 96,

- dodano, iż informacje należy przechowywać nie tylko w kasach pancernych lub szafach pancernych, ale także w urządzeniach służących ochronie informacji niejawnych o klauzuli „poufne", którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne − art. 119 pkt 7,

- doprecyzowano, iż przekazywanie informacji oznaczonych klauzulą *Tajemnica skarbowa* następuje w trybie przewidzianym dla dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone", a nie jak wcześniej *tajemnicę służbową*, co wskazywało, iż mogło być oznaczone zarówno klauzulą „zastrzeżone", jak i „poufne" − art. 98 pkt 1 i art. 119 pkt 2.

11. Gospodarka i prowadzenie działalności gospodarczej

Do tej kategorii zaliczono zagadnienia związane z prowadzeniem działalności gospodarczej, własnością przemysłową, handlem oraz zamówieniami publicznymi.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* na określenie *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* − art. 127 pkt 2, art. 170,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 106, art. 152 i art. 156,

- wśród podmiotów, którym udziela się informacji wymieniono organy i służby z art. 23 ust. 5 nowej UOIN uprawnione do przeprowadzania postępowań sprawdzających − art. 153,

- w przepisach dotyczących zakazu wykonywania działalności gospodarczej przez przedsiębiorcę zagranicznego oraz odmowie wpisu do rejestru wprowadzono określenie *informacje niejawne* zamiast dotychczasowego określenia *tajemnica państwowa* oraz wprowadzono doprecyzowanie klauzuli tajności „poufne", co rozszerza zakres informacji, które mogą być zagrożone − art. 154 pkt 3-5;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- zrezygnowano ze wskazywania na *ochronę tajemnicy państwowej* jako przyczynę odmowy wydania zezwolenia na prowadzenie działalności – art. 81,

- zrezygnowano z obejmowania wynalazku tajnego dotychczasową *tajemnicą państwową* i objęto go *tajemnicą prawnie chronioną* – art. 127 pkt 1,

- zrezygnowano z określenia, iż ekspert w Urzędzie Patentowym jest zobowiązany dochować *tajemnicy państwowej i służbowej* i zastąpiono je określeniem *dochować tajemnicy prawnie chronionej* − art. 127 pkt 4,

- zrezygnowano z określenia informacji uzyskanych podczas kontroli przez Inspekcję Handlową dotyczących tajemnicy handlowej jako *tajemnicy służbowej* i objęto je *tajemnicą prawnie chronioną* – art. 130;

c) wprowadzenie zmian porządkowych:

- zmiana spójników z *i* na *lub* – art. 154,

- zmiana numeracji z *art. 60 ust. 1a* na *art. 60a ust. 1a* – art. 180;

d) zmianę treści składanych ślubowań poprzez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez eksperta w Urzędzie Patentowym oraz przez syndyka, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji

niejawnych, i tak zamiast stwierdzenia *dochować tajemnicy państwowej i służbowej* lub *dochować tajemnicy państwowej* wprowadzono *dochować tajemnicy prawnie chronionej* − art. 127 pkt 3, art. 172;

e) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez osoby pełniące funkcje publiczne, z zastrzeżeniem, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla klauzuli „zastrzeżone", nie stanowiąc de facto i de iure informacji niejawnej − art. 114.

12. Gospodarka morska i wodna

Do tej kategorii zaliczono zagadnienia związane z izbami morskimi, rybactwem, żeglugą oraz prawem wodnym.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 76, art. 131 i art. 137,

- w przepisach dotyczących uprawnień strażników Państwowej Straży Rybackiej, wprowadzono doprecyzowanie klauzuli tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* − − art. 87.

13. Geodezja i budownictwo

Do tej kategorii zaliczono zagadnienia związane z geodezją oraz budownictwem.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa*, *tajemnica państwowa lub tajemnica służbowa* albo *klauzula „poufne"* − art. 91 i art. 163,

- w przepisach dotyczących umów, do których nie ma zastosowania ustawa o koncesjach na roboty budowlane lub usługi, wprowadzono określenie *informacje niejawne* zamiast dotychczasowego określenia *tajemnica państwowa* oraz wprowadzono doprecyzowanie klauzuli tajności „poufne", co rozszerza zakres informacji ujętych w umowach, do których nie będzie miała zastosowania ustawa − art. 174.

14. Nauka i umiejętności

Do tej kategorii zaliczono zagadnienia związane z nadawaniem stopni naukowych oraz z uprawnieniami tłumacza przysięgłego.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa*, *tajemnica państwowa lub tajemnica służbowa* − art. 148;

b) zmianę treści składanych ślubowań przez zmianę zakresu tajemnic podlegających ochronie:

- uwzględniono zmianę w treści ślubowania składanego przez tłumacza przysięgłego, w którym rozszerzono zakres chronionych tajemnic, bez ścisłego odwoływania się do informacji niejawnych, i tak zamiast stwierdzenia *dochowując tajemnicy państwowej* ograniczono do określenia *dochować tajemnicy prawnie chronionej* − art. 157.

15. Praca

Do tej kategorii zaliczono zagadnienia związane z pracą, w tym ze społeczną inspekcją pracy oraz Państwową Inspekcją Pracy.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa*, *tajemnica państwowa lub tajemnica służbowa* − art. 83, art. 171 pkt 2;

b) rezygnację z klasyfikowania danych jako informacji niejawnych:

- w przepisach dotyczących postępowania kontrolnego prowadzonego przez inspektorów pracy z Państwowej Inspekcji Pracy zrezygnowano z określania postanowień w sprawie zachowania w tajemnicy uzyskanych danych osobowych *tajemnicą służbową* – art. 171 pkt 1-2.

16. Zabezpieczenie społeczne

Do tej kategorii zaliczono zagadnienia związane ze świadczeniami socjalnymi i emerytalnymi oraz ubezpieczeniem społecznym.

Wśród wprowadzonych zmian wyróżnia się:

a) rezygnację z klasyfikowania danych jako informacji niejawnych i ujęcie ich jako tajemnic prawnie chronionych:

- w przepisach dotyczących danych przetwarzanych przez Zakład Ubezpieczeń Społecznych zrezygnowano z obejmowania ich dotychczasową *tajemnicą służbową* na rzecz określania ich *tajemnicą prawnie chronioną Zakładu* – art. 122,

- w przepisach dotyczących przetwarzania danych osobowych osób uprawnionych do renty socjalnej oraz zasiłku pogrzebowego zrezygnowano z obejmowania tych informacji dotychczasową *tajemnicą służbową* – art. 150;

b) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym:

- odstąpiono od nadawania klauzuli tajności oświadczeniom majątkowym składanym przez członków zarządu powszechnego towarzystwa emerytalnego, z zastrzeżeniem, iż informacje zawarte w przedmiotowych oświadczeniach stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji niejawnych o klauzuli „zastrzeżone". Podlegają one zatem ochronie przewidzianej dla tej klauzuli, nie stanowiąc de facto i de iure informacji niejawnej − art. 116.

17. Zdrowie

Do tej kategorii zaliczono zagadnienia związane z ochroną zdrowia, w tym ochroną zdrowia psychicznego, świadczeniami opieki zdrowotnej oraz pobieraniem, przechowywaniem i przeszczepianiem komórek, tkanek i narządów oraz z substancjami i preparatami chemicznymi.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* − art. 155,
- wśród podmiotów, którym udzielone są informacje wymieniono organy i służby z art. 23 ust. 5 nowej UOIN uprawnione do przeprowadzania postępowań sprawdzających − art. 100;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i objęcie ich inną tajemnicą prawnie chronioną:

- określono, iż szczegółowy skład chemiczny preparatu stanowi *tajemnicę prawnie chronioną*, a nie jak wcześniej *tajemnicę służbową* – art. 132,
- określono, iż dane dawców i biorców komórek, tkanek i narządów stanowią *tajemnicę prawnie chronioną*, a nie jak wcześniej *tajemnicę służbową* – art. 160.

18. Środowisko

Do tej kategorii zaliczono przepisy dotyczące ochrony środowiska, w tym Inspekcji Ochrony Środowiska.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizacja stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* określeniem *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)* – art. 134 i art. 173,

- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* albo *tajemnica państwowa lub tajemnica służbowa* − art. 95.

19. Inne

Do tej kategorii zaliczono zagadnienia, które nie spełniały kryteriów żadnej z powyższych kategorii. Znajdują się tu kwestie dotyczące ruchu drogowego, lotnictwa, prawa pocztowego, ochrony osób i mienia, bezpieczeństwa żywności, cmentarzy oraz archiwum.

Wśród wprowadzonych zmian wyróżnia się:

a) aktualizację stanu prawnego i nazewnictwa:

- uaktualniono stan prawny i zastąpiono określenie *przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.)* określeniem *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228)* – art. 115, art. 145 i art. 149,
- wprowadzono określenie *informacje niejawne* zamiast pojęć *tajemnica państwowa* − art. 84,
- w przepisach dotyczących blankietów dowodów rejestracyjnych, pozwoleń czasowych, nalepek kontrolnych i innych dokumentów wymaganych do rejestracji oraz tablic rejestracyjnych wprowadzano doprecyzowanie klauzul tajności „ściśle tajne" i „tajne" zamiast dotychczasowego określenia *tajemnica państwowa* – art. 110;

b) rezygnację z klasyfikowania danych jako informacji niejawnych i określanie ich jako tajemnicy prawnie chronionej:

- w przepisach dotyczących uzyskanych przez organy urzędowej kontroli żywności − w trakcie kontroli − informacji, dokumentów i innych danych stanowiących tajemnicę przedsiębiorcy zrezygnowano z obejmowania ich dotychczasową *tajemnicą służbową* − art. 167,
- określono, iż dane dotyczące stwierdzenia zgonu stanowią *tajemnicę prawnie chronioną*, a nie jak wcześniej *tajemnicę służbową* – art. 74.

Podsumowanie

Przedstawienie zmian w przepisach obowiązujących w formie swoistego „klucza kodowego" niewątpliwie umożliwiło uporządkowanie rozległych tematycznie zagadnień.

Co więcej, pozwoliło ono na wyszczególnienie grup zmian, do których należy:

a) aktualizacja stanu prawego i nazewnictwa,

b) rezygnacja z klasyfikowania danych jako informacji niejawnych i określenie ich jako tajemnicy prawnie chronionej, w czym zawiera się też rezygnacja z określania pewnych danych jako tajemnic,

c) rezygnacja z dotychczasowych regulacji,

c) wprowadzenie nowych regulacji prawnych,

d) zmiany w treści ślubowań poprzez zmianę zakresu tajemnic podlegających ochronie,

e) odstąpienie od nadawania klauzuli tajności oświadczeniom majątkowym,

f) wprowadzenie zmian porządkowych,

g) usunięcie regulacji z bytu prawnego.

Istotne jest, iż ustawodawca, często rezygnując ze stosowania dotychczasowego określenia *tajemnica państwowa lub tajemnica służbowa*, zadecydował o objęciu takich danych tajemnicą prawnie chronioną, w której zakresie semantycznym zawierają się również informacje niejawne. Wydaje się, iż takie ujęcie powoduje de facto rozszerzenie katalogu informacji, do których zachowania w tajemnicy są zobowiązane różne podmioty.

Ważne jest także, iż ustawodawca w wielu przedstawionych przypadkach zrezygnował z klasyfikowania pewnych danych jako informacji niejawnych, w szczególności odstępując od traktowania w ten sposób danych osobowych, tajemnicy przedsiębiorstwa czy wiadomości uzyskanych podczas kontroli.

Warte podkreślenia jest także, iż ustawodawca zrezygnował z obowiązku nadawania klauzuli tajności oświadczeniom majątkowym, przy jednoczesnym zapewnieniu im ochrony, jakby były takimi informacjami. Tak więc formalnie oświadczeniom o stanie majątkowym nie będzie nadawana klauzula tajności, ale będą chronione tak jak informacje niejawne oznaczone klauzulą „zastrzeżone".

Dokonane zmiany dotyczą aktów normatywnych w randze ustawy, co w konsekwencji będzie prowadziło do konieczności wprowadzenia zmian także w aktach wykonawczych wydanych na podstawie tych ustaw. Nowa ustawa o ochronie informacji niejawnych wywrze zatem silny wpływ na stan prawny w Polsce.

Na koniec warto jednak zauważyć, iż mimo ogromnego zakresu zmian, wciąż pewne dane są uznawane za informacje niejawne, choć w rzeczywistości nie spełniają one przesłanek ustawowych określonych w definicjach klauzul tajności, np. nadawanie klauzul tajności dokumentom o nadaniu orderu lub odznaczenia[8].

Wydaje się więc, iż w takich przypadkach częste zastosowanie będzie znajdował art. 9 nowej UOIN, zgodnie z którym w przypadku stwierdzenia zawyżenia klauzuli tajności, a więc bezpodstawnego nadania klauzuli tajności, będzie można zwracać się z wnioskiem o dokonanie stosownej zmiany. W rezultacie może to przyczynić się do nowelizacji jeszcze innych aktów prawnych niż tylko tych wymienionych od art. 74 do art. 180 „nowej UOIN".

Należy pamiętać, iż nazwanie pewnych danych informacjami niejawnymi i nadanie im klauzuli tajności w sposób przewidziany odpowiednimi przepisami nie uprawnia jeszcze do wniosku, że są one takimi informacjami w rozumieniu ustawy o ochronie informacji niejawnych.

[8] *Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 15 grudnia 2004 r. w sprawie szczegółowego trybu postępowania w sprawach o nadanie orderów i odznaczeń oraz wzorów odpowiednich dokumentów* (Dz.U. z 2004, Nr 277, poz. 2743 z późn. zm.).

Jolanta Frąckiewicz

Zmiany w zakresie organizacji ochrony informacji niejawnych

Wypracowany po 1990 r. system ochrony informacji niejawnych, po dziesięciu latach obowiązywania *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, uległ zmianie. W nowej ustawie zamieszczono wiele rozwiązań mających na celu wyeliminowanie przepisów przestarzałych, niefunkcjonalnych lub niespójnych z uwagi na wielokrotne nowelizacje ustawy. Dalsze wprowadzanie cząstkowych zmian nie było już w stanie doprowadzić do stworzenia jednolitego, przejrzystego aktu prawnego, dostosowanego do standardów międzynarodowych. Zwłaszcza w perspektywie naszego przywództwa w Radzie Unii Europejskiej nowelizacja krajowych uregulowań w zakresie budowy systemu ochrony informacji niejawnych stała się koniecznością.

Dziesięcioletnie doświadczenia ABW jako służby ochrony państwa razem z SKW, wykonującej ustawowe zadania w zakresie budowy i funkcjonowania polskiego systemu ochrony informacji niejawnych, pozwoliły wypracować strategiczne kierunki zmierzające do konstrukcji nowych uregulowań w tej sferze.

Zmieniono wiele, począwszy od zasad klasyfikowania informacji niejawnych, zakresu szkoleń, stosowania środków bezpieczeństwa fizycznego po akredytację systemów teleinformatycznych włącznie. Nie zmieniono jednak podstaw, na których oparty jest system ochrony informacji niejawnych, tj.:

- bezpieczeństwo osobowe – poprzez sprawdzanie osób, którym udostępniane są informacje niejawne, a także szkolenie z ochrony takich informacji,

- bezpieczeństwo fizyczne – poprzez stosowanie odpowiednich środków bezpieczeństwa fizycznego służących do ochrony informacji niejawnych,

- bezpieczeństwo teleinformatyczne – poprzez akredytację systemów wykorzystywanych do przetwarzania informacji niejawnych.

Dotychczasowe przepisy uległy zmianom, modyfikacji lub uzupełnieniu w taki sposób, aby doprowadzić do:

- ograniczenia ilości informacji podlegających zasadom bezpieczeństwa przewidzianym w przepisach o ochronie informacji niejawnych,

- zapewnienia ochrony informacjom niejawnym w okresie, kiedy rzeczywiście spełniają przesłanki ustawy,

- stosowania środków bezpieczeństwa fizycznego adekwatnych do liczby i klauzuli tajności informacji przetwarzanych w jednostkach organizacyjnych.

Jednocześnie uzupełniono lub doprecyzowano przepisy mające wpływ na podniesienie bezpieczeństwa informacji niejawnych, szczególnie oznaczonych najwyższą klauzulą tajności. Zmianom nie uległy natomiast podmioty odpowiedzialne w naszym kraju za nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych, a są to dwie służby specjalne: Agencja Bezpieczeństwa Wewnętrznego (w tzw. sferze cywilnej) i Służba Kontrwywiadu Wojskowego (w tzw. sferze wojskowej). W jednostce organizacyjnej osobą odpowiedzialną za zorganizowanie i zapewnienie funkcjonowania ochrony informacji niejawnych jest kierownik jednostki organizacyjnej, którego wspiera pełnomocnik do spraw ochrony informacji niejawnych (zwany pełnomocnikiem ochrony) – odpowiedzialny za zapewnienie przestrzegania przepisów.

Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego

Nadzór nad bezpieczeństwem informacji niejawnych w Polsce sprawują dwie służby – Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego (ustawodawca zrezygnował z pojęcia służby ochrony państwa). Dotychczasowa funkcja nadzorcza została wyraźnie sformułowana w art. 10 ust. 1 nowej ustawy. Ustawodawca, po raz pierwszy i to w sposób wyraźny, określił właściwość obu służb, wskazując, że SKW realizuje zadania w odniesieniu do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych i nadzorowanych przez MON, ataszatów obrony w placówkach zagranicznych oraz żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe poza tymi podmiotami, natomiast ABW realizuje zadania w odniesieniu do pozostałych podmiotów (art. 10 ust. 2-3).

Nie zmienił się także zakres zadań realizowanych przez obie służby, co oznacza, że ABW lub SKW są właściwe do:

- prowadzenia kontroli ochrony informacji niejawnych,

- prowadzenia postępowań sprawdzających, postępowań bezpieczeństwa przemysłowego,

- akredytacji systemów teleinformatycznych,

- zapewnienia ochrony informacji niejawnych wymienianych pomiędzy Polską a innymi państwami lub organizacjami międzynarodowymi,

- prowadzenia szkoleń, w tym przede wszystkim dla kandydatów na pełnomocników ochrony oraz osób pełniących już te funkcje, oraz prowadzenia doradztwa w zakresie ochrony informacji niejawnych.

Z punktu widzenia sprawowania przez ABW i SKW nadzoru nad funkcjonowaniem systemu ochrony informacji niejawnych, ważnym obowiązkiem kierowników jednostek organizacyjnych jest informowanie tych służb o utworzeniu lub likwidacji kancelarii tajnej, z określeniem klauzul tajności przetwarzanych w niej informacji niejawnych (art. 42 ust. 6). Ustawodawca zobligował kierowników jednostek, w których funkcjonują już kancelarie tajne, aby w terminie 3 miesięcy od daty wejścia w życie ustawy poinformowali o tym fakcie odpowiednio ABW lub SKW (art. 184). Taki zapis będzie sprzyjał prawidłowemu obiegowi informacji niejawnych, ponieważ przed wysłaniem dokumentu oznaczonego klauzulą „ściśle tajne" lub „tajne" możliwe będzie ustalenie, czy adresat jest przygotowany do przyjęcia niejawnej przesyłki, tzn. czy w jednostce funkcjonuje kancelaria tajna oraz do jakiej klauzuli tajności zorganizowano system ochrony.

ABW lub SKW, w ramach nadzoru nad bezpieczeństwem informacji niejawnych, jest właściwą służbą do prowadzenia kontroli stanu zabezpieczenia takich informacji, a w przypadku stwierdzenia nieprawidłowości − do wskazywania zaleceń kierownikom jednostek kontrolowanych, w tym do podjęcia konkretnych działań w celu usunięcia nieprawidłowości.

Dotychczasowe uprawnienia kontrolne służb, określone w art. 16 i art. 17 ustawy z dnia 22 stycznia 1999 r., zostały zachowane, co oznacza, że ABW lub SKW będą prowadziły kontrole ochrony informacji niejawnych i przestrzegania przepisów wydanych w tym zakresie, z uwzględnieniem prawidłowości zwykłych postępowań sprawdzających prowadzonych przez pełnomocników ochrony, którzy wydają poświadczenia umożliwiające dostęp do informacji o klauzuli „poufne".

Nie podlegają kontroli akta postępowań prowadzonych przez podmioty, które samodzielnie prowadzą postępowania sprawdzające (zwykłe lub poszerzone) wobec własnych funkcjonariuszy, żołnierzy lub pracowników, tzn. realizowane przez pełnomocników ochrony w AW, CBA, Policji, Służby Więziennej, SWW, Straży Granicznej, Żandarmerii Wojskowej oraz (od tego roku) BOR (art. 23 ust. 5 ustawy). Nowa ustawa nie wprowadziła więc zmian w stosunku do obowiązujących dotychczas przepisów w zakresie kontroli akt postępowań sprawdzających.

Dość istotne zmiany z punktu widzenia kontrolującego zaszły natomiast w zakresie uprawnień do kontroli systemów teleinformatycznych. Dotychczasowy przepis stanowiący, że *funkcjonariusze realizujący kontrolę mają prawo do żądania udostępnienia do kontroli sieci lub systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania tych informacji* budził wątpliwości co do możliwości poddania kontroli nieakredytowanych systemów (tj. niesłużących do przetwarzania informacji niejawnych). Kierownicy jednostek kontrolowanych stali na stanowisku, że przepis wyklucza możliwość kontroli innych systemów niż akredytowane (tj. służących do przetwarzania informacji niejawnych). Z punktu widzenia bezpieczeństwa informacji niejawnych niezwykle istotne było sprawdzenie, czy informacje niejawne są rzeczywiście przetwarzane tylko w systemach akredytowanych, a nie na przykład w systemach podłączonych do ogólnodostępnej sieci internet. Po wejściu w życie ustawy funkcjonariusze mogą żądać udostępnienia do kontroli systemów teleinformatycznych nieposiadajacych akredytacji bezpieczeństwa teleinformatycznego, pod warunkiem podejrzewania możliwości przetwarzania w nich informacji niejawnych (art. 12 ust. 2). W praktyce oznacza to, że jeśli w toku kontroli zostanie uprawdopodobnione podejrzenie przetwarzania informacji niejawnych poza akredytowanym system, to kontrolerowi należy udostępnić inne (wskazane przez niego) systemy teleinformatyczne w celu ustalenia, czy takie przetwarzanie miało miejsce. Warto przy tym wskazać jeszcze jedną zmianę, a mianowicie w zakres czynności kontrolerskich włączony został art. 98 *Ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli,* który dotyczy zakresu odpowiedzialności osób utrudniających prowadzenie kontroli.

Zupełnie nowym rozwiązaniem, budzącym (głównie organizacyjne) wątpliwości, jest możliwość zarządzenia „wspólnej" kontroli, tj. prowadzonej przez ABW i SKW u przedsiębiorców realizujących umowy związane z dostępem do informacji niejawnych (art. 65 ust. 2-3). Taka sytuacja będzie mogła zaistnieć w przypadku, gdy przedsiębiorca realizuje umowę w podmiocie nie nadzorowanym przez służbę, która wydała świadectwo bezpieczeństwa przemysłowego. Oznacza to, że jeśli przedsiębiorca, który otrzymał świadectwo bezpieczeństwa przemysłowego od ABW, a realizuje umowę na rzecz podmiotów nadzorowanych przez SKW (art. 10 ust. 2) i w toku realizacji tej umowy zostaną ujawnione fakty wskazujące na możliwość utraty przez przedsiębiorcę zdolności do ochrony informacji niejawnych – to w takim przypadku Szef SKW może wystąpić do Szefa ABW o zarządzenie kontroli. W kontroli będą uczestniczyć zarówno funkcjonariusze ABW, jak też funkcjonariusze lub żołnierze SKW. Ustawodawca przewidział też sytuację odwrotną, tj. gdy przedsiębiorca realizuje umowę na rzecz podmiotu nadzorowanego przez ABW (art. 10 ust. 3), a świadectwo bezpieczeństwa przemysłowego otrzy-

mał od SKW. Taka „wspólna" kontrola będzie zarządzana w trybie doraźnym, tzn. poza rocznymi planami kontroli zatwierdzanymi przez Szefów ABW i SKW oraz bez konieczności uzyskiwania opinii Kolegium do Spraw Służb Specjalnych.

Zasadniczą zmianą, ważną z punktu widzenia stosunków międzynarodowych, jest powierzenie Szefowi Agencji Bezpieczeństwa Wewnętrznego funkcji krajowej władzy bezpieczeństwa (art. 11 ust. 1 ustawy). Dotychczas funkcję tę pełnili wspólnie Szefowie *służb ochrony państwa* (tj. Szef ABW i Szef SKW). W nowej ustawie ustawodawca zobligował jednak Szefa ABW do współdziałania z Szefem SKW w zakresie pełnienia funkcji krajowej władzy bezpieczeństwa (art. 11 ust. 5 ustawy). Szef ABW pełniący funkcję krajowej władzy bezpieczeństwa nadzoruje system ochrony informacji niejawnych w stosunkach Polski z innymi państwami lub organizacjami międzynarodowymi, a także jest uprawniony do wydawania dokumentów upoważniających do dostępu do informacji niejawnych m.in. Organizacji Traktatu Północnoatlantyckiego czy Unii Europejskiej (art. 11 ust. 2 ustawy).

Kierownik jednostki organizacyjnej

Za bezpieczeństwo informacji niejawnych w jednostkach organizacyjnych odpowiada kierownik tej jednostki. Jednakże dotychczasowy przepis (art. 18 ust. 1 ustawy z dnia 22 stycznia 1999 r.) został doprecyzowany przez wskazanie, że kierownik jednostki odpowiada *w szczególności za zorganizowanie i zapewnienie funkcjonowania ochrony informacji niejawnych* (art. 14 ust. 1 ustawy). Kierownik jednostki organizacyjnej będzie zobligowany m.in. do:

- utworzenia kancelarii tajnej, jeśli jednostka przetwarza informacje oznaczone klauzulą „ściśle tajne" lub „tajne",
- zatrudnienia kierownika kancelarii tajnej oraz pełnomocnika ochrony (także inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu, jeśli jednostka posiada systemy przeznaczone do przetwarzania informacji niejawnych),
- opracowania dokumentacji dotyczącej sposobu i trybu przetwarzania informacji niejawnych, w tym dokumentacji bezpieczeństwa systemu teleinformatycznego,
- współdziałania ze służbami i instytucjami uprawionymi do prowadzenia poszerzonych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego,

- informowania (w terminie 7 dni) organu, który wydał poświadczenie bezpieczeństwa, a także ABW lub SKW o zatrudnieniu osoby przedstawiającej takie poświadczenie,
- przeprowadzania, nie rzadziej niż raz na 5 lat, przeglądu materiałów w celu ustalenia, czy spełniają one ustawowe przesłanki ochrony.

W nowej ustawie znaczenia nabiera kwestia szkolenia osób mających dostęp do informacji niejawnych. Wszystkie osoby mające do czynienia z informacjami niejawnymi, bez względu na zajmowane stanowisko lub pełnioną funkcję, powinny zostać zapoznane z przepisami o ochronie takich informacji (osoby sprawujące najważniejsze urzędy w naszym kraju, a także sędziowie i prokuratorzy składają stosowne oświadczenia, pozostałe osoby powinny zostać przeszkolone). Dotychczas szkolenia wobec osób zatrudnionych w jednostkach organizacyjnych prowadzili pełnomocnicy ochrony (wszystkich pełnomocników ochrony lub osoby przewidziane na te stanowiska szkoliły służby ochrony państwa). Obecnie ustawodawca zobligował ABW i SKW do przeszkolenia kierowników jednostek organizacyjnych, w których przetwarzane są informacje o klauzuli „ściśle tajne" lub „tajne", oraz wszystkich przedsiębiorców wykonujących działalność jednoosobowo (działalność związaną oczywiście z dostępem do informacji niejawnych), a także kierowników przedsiębiorców, u których nie zatrudniono pełnomocnika ochrony. Z tym że w sytuacji, gdy jednostka przetwarza informacje niejawne o najwyższych klauzulach tajności i zatrudnia pełnomocnika ochrony, to szkolenia wobec kierownika tej jednostki prowadzi ABW lub SKW wspólnie z pełnomocnikiem (art. 19 ust. 2 pkt 2). Szkolenie prowadzone przez służbę i pełnomocnika ochrony w podmiotach przetwarzających informacje „ściśle tajne" lub „tajne" ma na celu kompleksowe przedstawienie kierownikowi jednostki (odpowiedzialnemu za ochronę istotnych dla bezpieczeństwa państwa informacji niejawnych) zasad ochrony takich informacji oraz zapoznanie z uprawnieniami i obowiązkami wynikającymi z racji pełnionej funkcji.

Kierowników jednostek, w których występują informacje niejawne o klauzuli „poufne" lub „zastrzeżone" szkolić będą pełnomocnicy ochrony zatrudnieni w tych jednostkach. Wszystkie szkolenia w zakresie ochrony informacji niejawnych, zarówno te prowadzone przez ABW lub SKW, jak i pełnomocników ochrony, powinny być organizowane nie rzadziej niż raz na 5 lat, a każda osoba przeszkolona powinna złożyć pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych (art. 20 ust. 1). Częstotliwość szkoleń oraz składanie oświadczeń są nowymi rozwiązaniami − dotychczas obowiązek cyklicznych szkoleń dotyczył tylko pełnomocników ochrony i ich zastępców, a oświadczenia nie były wymagane.

Warto zwrócić także uwagę na nowe uprawnienia kierownika jednostki, a takim jest z pewnością wydawanie upoważnień osobom, które z racji wykonywanych zadań powinny mieć dostęp do informacji niejawnych o najniższej klauzuli tajności, czyli oznaczonymi klauzulą „zastrzeżone". Dotychczas osoba ubiegająca się o dostęp do informacji niejawnych, bez względu na klauzulę tajności, zobowiązana była do poddania się procedurze postępowania sprawdzającego (specjalnego, poszerzonego lub zwykłego). Dopiero po uzyskaniu poświadczenia bezpieczeństwa, wydanego przez służbę ochrony państwa lub pełnomocnika ochrony, mogła zapoznawać się z informacjami niejawnymi (oczywiście po przeszkoleniu). Obecnie dokumentem wystarczającym do zapoznania się z informacją niejawną o klauzuli „zastrzeżone" będzie pisemne upoważnienie kierownika jednostki organizacyjnej, w której osoba jest zatrudniona. Warunkiem dopuszczenia do pracy związanej z dostępem do informacji niejawnych o najniżej klauzuli tajności będzie zatem pisemne upoważnienie wydane przez kierownika jednostki organizacyjnej (art. 21 ust. 4 pkt 1), chyba, że osoba posiada ważne poświadczenie bezpieczeństwa, oraz przeszkolenie w zakresie ochrony informacji niejawnych, potwierdzone zaświadczeniem wydanym przez pełnomocnika ochrony.

Nowym uprawnieniem kierownika jednostki organizacyjnej jest także udzielanie akredytacji dla systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" (art. 48 ust. 9). Do tej pory akredytacji systemów teleinformatycznych udzielały służby ochrony państwa, które zatwierdzały dokumentację bezpieczeństwa teleinformatycznego, w tym także dla systemów przetwarzających informacje o najniższej klauzuli tajności. Obecnie dokumentację bezpieczeństwa teleinformatycznego dla systemu, w którym będą przetwarzane informacje „zastrzeżone" będzie zatwierdzał kierownik jednostki organizacyjnej, który jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego (art. 49 ust. 7). Ustawodawca zobligował jednak kierownika jednostki organizacyjnej do przekazania zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego odpowiednio do ABW lub SKW − służbom, które mogą zgłosić zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych, a w szczególnie uzasadnionych przypadkach nawet nakazać wstrzymanie przetwarzania informacji w tych systemach (art. 48 ust. 12).

Jak już wspomniano kierownik jednostki organizacyjnej odpowiada za ochronę informacji niejawnych przetwarzanych w jednostce, przede wszystkim w zakresie zorganizowania właściwego systemu ochrony tych informacji, a do realizacji tych zadań niezbędny jest pełnomocnik ochrony.

Pełnomocnik ochrony

Pełnomocnik ochrony, tak jak dotychczas, podlega bezpośrednio kierownikowi jednostki organizacyjnej i odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych (art. 14 ust. 2). Nie uległ zasadniczym zmianom zakres zadań przewidzianych na tym stanowisku, które zostały określone w art. 15. Tu też znajduje się zapis dotyczący możliwości powierzenia pełnomocnikowi przez kierownika jednostki organizacyjnej innych zadań, jeśli ich realizacja nie naruszy prawidłowego wykonywania zadań ustawowych. Do ustawowych zadań pełnomocnika ochrony należy w szczególności:

- prowadzenie zwykłych postępowań sprawdzających wobec pracowników mających dostęp do informacji niejawnych o klauzuli „poufne" (z wyłączeniem kierownika jednostki organizacyjnej),
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych,
- prowadzenie kontroli ewidencji, materiałów i obiegu dokumentów niejawnych (co najmniej raz na 3 lata),
- zapewnienie ochrony systemów teleinformatycznych, w których przetwarzane są informacje niejawne,
- zapewnienie ochrony informacjom niejawnym, w tym stosowanie środków bezpieczeństwa fizycznego.

Do zadań pełnomocnika ochrony należy także (podobnie jak dotychczas) opracowanie planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji (art. 15 ust. 1 pkt 5). Zmiany w przepisach dotyczą konieczności aktualizowania planu ochrony oraz każdorazowego akceptowania go przez kierownika jednostki organizacyjnej. Podstawowe elementy, które powinien zawierać plan ochrony zostaną zawarte w rozporządzaniu Rady Ministrów, wydanym w trybie art. 47 ust. 1 ustawy. Jest to istotny zapis, gdyż dziesięcioletnie doświadczenia ABW pokazały, że pełnomocnicy ochrony mieli trudności z opracowaniem takiego dokumentu. *Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych* oraz zmieniające je rozporządzenie z dnia 1 czerwca 2010 r. wskazuje tylko jeden element, który powinien zawierać plan ochrony, tj. zasady i spo-

sób zdawania, przechowywania oraz wydawania kluczy do pomieszczeń i szaf służących do przechowywania informacji niejawnych.

Pełnomocnik ochrony będzie także zobligowany do prowadzenia kontroli ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, zwłaszcza do prowadzenia okresowych, co najmniej raz na 3 lata, kontroli ewidencji, materiałów i obiegu dokumentów. Po raz pierwszy w ustawie pojawia się termin odnoszący się do „częstotliwości" prowadzenia przez pełnomocnika ochrony okresowych kontroli ewidencji i obiegu dokumentów. Taki zapis z pewnością będzie sprzyjał realizacji ustawowych zadań przewidzianych dla kancelarii tajnej, a mianowicie sprawowaniu kontroli nad obiegiem i przechowywaniem materiałów niejawnych.

Kancelaria tajna, podobnie jak dotychczas, będzie obsługiwana przez pracowników pionu ochrony i będzie podlegała pełnomocnikowi ochrony. Powinna być ona zorganizowana w taki sposób, aby zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „ściśle tajne" lub „tajne" pozostający w dyspozycji jednostki oraz kto z tym materiałem się zapoznał (art. 43 ust. 1). Wymagania w zakresie organizacji i funkcjonowania kancelarii tajnej oraz podstawowe zadania kierownika kancelarii zostaną określone w drodze rozporządzenia Rady Ministrów, wydanego na podstawie art. 47 ust. 1 ustawy.

Bez wątpienia zarówno pełnomocnik ochrony, jak też kierownik kancelarii tajnej czy inny pracownik pionu ochrony w sposób szczególny odpowiadają za ochronę informacji niejawnych. Wszelkie nieprawidłowości związane z wykonywaniem zadań powinny być wyjaśniane, a naruszenia przepisów zgłaszane odpowiednim organom. Ustawodawca doprecyzował zapis dotyczący czynności, które powinien wykonać pełnomocnik ochrony w razie stwierdzenia naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne" lub wyższą. Poza dotychczasowym zapisem, zobowiązującym pełnomocnika ochrony do powiadomienia o tym fakcie kierownika jednostki organizacyjnej i służbę ochrony państwa oraz podjęciem działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów, został on zobligowany do ograniczenia negatywnych skutków naruszenia przepisów. Warto także zwrócić uwagę, że pełnomocnik ochrony został zobligowany także do **niezwłocznego** informowania o fakcie naruszenia przepisów odpowiednio ABW lub SKW. Wyeliminuje to przypadki zwlekania z informowaniem służb nadzorujących system ochrony informacji niejawnych o naruszeniu przepisów dotyczących informacji oznaczonych klauzulą „ściśle tajne", „tajne" lub „poufne".

Nowością jest podejście do zabezpieczenia informacji niejawnych w środki bezpieczeństwa fizycznego. Do zadań pełnomocnika ochrony włączono − dotychczas w ogóle niewystępujący − obowiązek sporządzenia dokumentacji określającej poziom zagrożenia nieuprawnionego ujawnienia lub utraty informacji niejawnych. Pełnomocnik ochrony będzie odpowiadał także za dobór adekwatnych do poziomu zagrożenia środków bezpieczeństwa fizycznego oraz klauzuli tajności przetwarzanych informacji.

Powyższe zadania pełnomocnik ochrony może realizować przy pomocy wyodrębnionej komórki organizacyjnej do spraw ochrony informacji niejawnych, zwaną *pionem ochrony*, jeśli taka będzie utworzona w jednostce organizacyjnej (art. 15 ust. 2). Ustawodawca dopuszcza brak takiej komórki organizacyjnej w jednostkach dysponujących informacjami niejawnymi o klauzulach „zastrzeżone" lub „poufne", ale nieprzetwarzających ich w systemach teleinformatycznych.

Zmianom uległy warunki, jakie powinien spełniać kandydat na pełnomocnika ochrony, a mianowicie od stycznia 2011 r. o funkcję pełnomocnika do spraw ochrony informacji niejawnych może ubiegać się osoba z wyższym wykształceniem – dotychczas wystarczające było legitymowanie się średnim wykształceniem (wymóg wyższego wykształcenia nie dotyczy pełnomocników ochrony zatrudnionych przed 1 stycznia 2011 r. – art. 183). Zmiana dotycząca posiadania wyższego wykształcenia (art. 14 ust. 3 pkt 2) nie jest jedyną jeśli chodzi o warunki, jakie powinien spełniać kandydat na pełnomocnika ochrony. Zgodnie z nową ustawą, aby móc pełnić tę funkcję, należy posiadać nie tylko odpowiednie i ważne poświadczenie bezpieczeństwa wydane przez ABW lub SKW (także przez były UOP lub byłe WSI), ale też odpowiednie, tj. wydane przez ABW lub SKW (także WSI), zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych (art. 14 ust. 3 pkt 4). Co prawda na zaświadczeniu o przeszkoleniu nie ma daty jego ważności, niemniej jednak zaświadczenie takie jest ważne 5 lat od daty jego wystawienia (zaświadczenia wydane przez UOP są już zatem nieważne). Dotychczas, aby ubiegać się o funkcję pełnomocnika ochrony, wystarczyło legitymować się zaświadczeniem o przeszkoleniu wydanym przez służbę ochrony państwa – data wydania nie miała znaczenia.

Nowością jest także składanie pisemnych oświadczeń potwierdzających zapoznanie się z przepisami o ochronie informacji niejawnych przez kandydatów na pełnomocników ochrony oraz pełnomocników ochrony (oświadczenie będą składane po odbyciu przeszkolenia prowadzonego przez ABW lub SKW i będą przechowywane przez te służby). Bez zmian pozostają natomiast wymagania stawiane kandydatom na pełnomocnika ochrony dotyczące posiadania polskiego oby-

watelstwa. Podsumowując, funkcję pełnomocnika ochrony nadzorującego pracę kancelarii tajnej może pełnić osoba posiadająca:

- polskie obywatelstwo,
- wyższe wykształcenie,
- odpowiednie i ważne poświadczenie bezpieczeństwa wydane przez ABW lub SKW (także przez były UOP lub byłe WSI),
- aktualne zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych, wydane przez ABW lub SKW (także przez byłe WSI).

Wszystkie te warunki stawiane są także kandydatom na zastępców pełnomocnika ochrony. Bez zmian natomiast pozostają wymagania wobec pracowników pionu ochrony, którzy powinni posiadać:

- polskie obywatelstwo (z wyjątkiem osób zatrudnionych u przedsiębiorców),
- odpowiednie poświadczenie bezpieczeństwa (tj. do najwyższej klauzuli tajności przetwarzanych w jednostce informacji niejawnych),
- zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

Podsumowując, za bezpieczeństwo informacji niejawnych w Polsce odpowiadają Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego − dwie służby nadzorujące funkcjonowanie systemu ochrony informacji niejawnych; kierownicy jednostek organizacyjnych, odpowiadający za zorganizowanie systemu ochrony informacji niejawnych w swoich jednostkach oraz pełnomocnicy ochrony odpowiedzialni za zapewnienie przestrzegania przepisów. W stosunkach międzynarodowych nadzór nad systemem ochrony informacji niejawnych sprawuje Szef Agencji Bezpieczeństwa Wewnętrznego pełniący funkcję krajowej władzy bezpieczeństwa.

Jolanta Frąckiewicz

Zmiany w zakresie organizacji kancelarii tajnej i stosowania środków bezpieczeństwa fizycznego

Patrząc na zmiany, jakie wprowadziła *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, uwagę zwracają nowe uregulowania dotyczące kancelarii tajnych i stosowania środków służących do ochrony informacji niejawnych. Zmiany mają na celu przede wszystkim wprowadzenie zasad racjonalnego stosowania metod i środków służących ochronie informacji niejawnych oraz adekwatności rozwiązań dla określonych klauzul tajności. Zmiany mają też na celu złagodzenie wymagań dla podmiotów dysponujących informacjami o niskich klauzulach tajności, pozostawiając wysokie lub bardzo wysokie wymagania przy zabezpieczaniu informacji oznaczonych klauzulą „ściśle tajne" lub „tajne". W pracach nad przyjęciem nowych przepisów w zakresie organizacji kancelarii tajnych, a przede wszystkim stosowania środków służących do ochrony informacji niejawnych, oparto się z jednej strony na dziesięcioletnim doświadczeniu służb ochrony państwa (ABW lub SKW), które sprawują nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych w Polsce, z drugiej zaś na sposobach przyjętych w innych państwach Unii Europejskiej. Przy konstruowaniu niektórych przepisów, szczególnie dotyczących obiegu i zabezpieczenia informacji niejawnych o najniższej klauzuli tajności, brano pod uwagę to, że 1 lipca 2011 r. Polska obejmie Przewodnictwo w Radzie Unii Europejskiej. Na potrzebę stworzenia nowych rozwiązań wpłynął także znaczny postęp technologiczny.

Podstawowe zasady w zakresie organizacji kancelarii tajnej i zabezpieczenia informacji niejawnych, które dotychczas umieszczone były w dwóch rozdziałach: 7. − *Kancelarie tajne. Kontrola obiegu dokumentów* oraz w 9. − *Środki ochrony fizycznej informacji niejawnych* zostały scalone w rozdziale 7. nowej ustawy pt. *Kancelarie tajne. Środki bezpieczeństwa fizycznego*. Szczegółowe wymagania dotyczące organizacji i funkcjonowania kancelarii tajnych, struktury organizacyjnej oraz zadań przewidzianych na stanowisku kierownika kancelarii zostaną określone w rozporządzeniu Rady Ministrów (art. 47 ust. 1). Należy przy tym wskazać, że 1 stycznia 2011 r. weszło w życie *Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych* (Dz.U. z 2010 r., Nr 114, poz. 765)[1], wydane na podstawie *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, które będzie obowiązywało do czasu wydania nowego rozporządzenia − nie dłużej jednak niż do końca 2011 r.

[1] Przepisy rozporządzenia nie mają zastosowania do podmiotów wymienionych w art. 53 ust. 2 *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.*

Organizacja kancelarii tajnej

Podstawowym kryterium, jakie przyjęto przy opracowywaniu rozdziału 7. ustawy było wskazanie, że k a n c e l a r i a t a j n a to komórka organizacyjna odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom (art. 42 ust. 4), a nie jak dotychczas − jednocześnie *komórka organizacyjna* i *pomieszczenie* odpowiednio zabezpieczone w środki ochrony fizycznej. Dokumenty niejawne mogą być przechowywane w różnych pomieszczeniach służbowych (odpowiednio zabezpieczonych), a kancelaria tajna − jako wyodrębniona komórka organizacyjna – powinna sprawować nadzór nad prawidłowym oznaczaniem, obiegiem i zabezpieczeniem dokumentów niejawnych w jednostce organizacyjnej.

Organizacja pracy kancelarii tajnej powinna zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „ściśle tajne" lub „tajne", a także zapewniać, aby z informacjami niejawnymi zapoznawały się wyłącznie osoby do tego uprawnione. Warto przy tym wskazać, że ustawodawca powtórzył zapis z ustawy z 22 stycznia 1999 r. dotyczący odmowy udostępniania lub wydawania materiałów niejawnych osobom nieuprawnionym (art. 43 ust. 6), tzn. bez poświadczeń bezpieczeństwa lub upoważnionych w innym trybie. Trzeba przy tym pamiętać, że samo poświadczenie bezpieczeństwa nie jest podstawą do udostępniania informacji niejawnych – poświadczenie bezpieczeństwa jest „jedynie" dokumentem potwierdzającym, że osoba daje rękojmię zachowania tajemnicy i mogą być jej powierzane określone tajemnice. Warunkiem niezbędnym do udostępnienia informacji niejawnej (bez względu na klauzulę tajności) jest tzw. zasada ograniczonego dostępu wyrażona w art. 4 ust. 1 ustawy, zgodnie z którym informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy. W praktyce oznacza to, że z dokumentem niejawnym zapoznaje się adresat pisma (posiadający odpowiednie poświadczenie lub upoważnienie) lub osoba przez niego wskazana − najlepiej w formie dekretacji na piśmie. Oczywiście poza tymi warunkami niezbędne jest także odbycie przeszkolenia w zakresie ochrony informacji niejawnych i legitymowanie się odpowiednim zaświadczeniem.

Odnośnie zapisu dotyczącego organizacji kancelarii tajnej w sposób umożliwiający ustalenie w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „ściśle tajne" lub „tajne", pozostający w dyspozycji jednostki organizacyjnej, oraz kto z tym materiałem się zapoznał (art. 43 ust. 1), warto przypomnieć, że nie jest to nowy zapis. Zarówno w poprzedniej ustawie (w art. 52 ust. 1 i 4), jak i obecnej zapis ten jest niezwykle ważny. Po pierwsze: kancelaria tajna nie może dopuścić do sytuacji, w której traci kontrolę nad dokumentem. W realizacji tego zada-

nia niezbędne jest rzetelne i staranne prowadzenie urządzeń ewidencyjnych, przede wszystkim dziennika ewidencji. Od 2011 r. dokumenty niejawne powinny być rejestrowane tylko w takim urządzeniu, ponieważ zniesiono prowadzenie dziennika ewidencji wykonanych dokumentów (tzw. DEWD). Do nowych zasad oznaczania i rejestrowania dokumentów odnoszą się dwa nowe rozporządzenia (mimo że wydane na podstawie poprzedniej ustawy), tj. *Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych* oraz *Rozporządzenie Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności* (Dz.U. z 2010 r., Nr 159, poz. 1069); oba akty prawne zostaną zastąpione nowymi, wydanym na podstawie aktualnie obowiązującej ustawy. Po drugie, zadaniem kancelarii tajnej jest także dopilnowanie, aby fakt zapoznania się z materiałem „ściśle tajnym" lub „tajnym" przez każdą uprawnioną osobę był odnotowywany. W poprzedniej ustawie wskazano wprost, że fakt zapoznania się z dokumentem zawierającym tajemnicę państwową podlega odnotowaniu w „karcie zapoznania się z dokumentem". W obecnej ustawie nie ma zapisu dotyczącego obowiązku zakładania „kart zapoznania", jednakże w rozporządzeniu Rady Ministrów, które zostanie wydane w trybie art. 47 ust. 1 ustawy, zostanie określony wzór takiej karty i z pewnością określone zostaną zasady jej stosowania. Pamiętać przy tym trzeba, że w obecnie obowiązującym rozporządzeniu o funkcjonowaniu kancelarii tajnej (nie dotyczy wszystkich podmiotów) jest zapis dotyczący obowiązku zakładania kart zapoznania się z dokumentem oznaczonym klauzulą „ściśle tajne" lub „tajne".

Ustawodawca zawęził listę podmiotów zobligowanych do utworzenia kancelarii tajnej. Dotychczas kierownicy jednostek organizacyjnych, w których przetwarzane były informacje o klauzuli „poufne", mieli obowiązek zorganizowania kancelarii tajnej. Obecnie ustawodawca nakłada ten obowiązek na kierowników jednostek, w których przetwarzane są informacje o klauzuli „ściśle tajne" lub „tajne" (art. 42 ust. 1). Trzeba jednak zaznaczyć, że zmianie uległy zasady klasyfikowania informacji niejawnych. W nowej ustawie nie ma podziału na tajemnicę państwową i służbową – są po prostu informacje niejawne oznaczone klauzulami: „ściśle tajne", „tajne", „poufne" i „zastrzeżone". Nie ma również wykazu rodzajów informacji, które mogą być oznaczone klauzulą „ściśle tajne" lub „tajne". Klasyfikowanie informacji niejawnych oznacza przyznanie odpowiedniej klauzuli tajności, zgodnie z treścią art. 5 ustawy. Informacje oznaczone klauzulą „ściśle tajne" lub „tajne" charakteryzuje poważna lub wyjątkowo poważna szkoda dla Rzeczypospolitej Polskiej w przypadku ich nieuprawnionego ujawnienia (dot. m.in. niepodległości, suwerenności, integralności terytorialnej, stosunków międzynarodowych, funkcjonowania Sił Zbrojnych). Może zatem okazać się, że wiele podmiotów, które

dotychczas dysponowały materiałami stanowiącymi tajemnicę państwową, po wejściu w życie ustawy z 5 sierpnia 2010 r., nie będą już przetwarzały informacji oznaczonych klauzulą „ściśle tajne" lub „tajne", albowiem nie będą one spełniały ustawowych przesłanek ochrony na podstawie cytowanej ustawy. Takie rozwiązanie powinno ograniczyć liczbę informacji o najwyższej klauzuli tajności rzeczywiście tylko do tych, których nieuprawnione ujawnienie spowoduje nieodwracalne i poważne skutki dla podstawowych interesów Rzeczypospolitej Polskiej. Zgodnie z obowiązującą ustawą kancelarie tajne będą funkcjonowały w jednostkach organizacyjnych, które będą przetwarzały informacje niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" − spełniające przesłanki ustawy z dnia 5 sierpnia 2010 r.

Jednostki organizacyjne, które w dniu wejścia w życie ustawy dysponowały informacjami niejawnymi oznaczonymi klauzulą „ściśle tajne" lub „tajne", zaklasyfikowanymi według przepisów *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, powinny dokonać przeglądu materiałów pod kątem ustalenia, czy spełniają one ustawowe przesłanki ochrony na podstawie nowej ustawy i w razie potrzeby dokonać zmiany lub zniesienia klauzuli tajności. Kierownicy jednostek organizacyjnych mają 3 lata na dokonanie przeglądu materiałów niejawnych, wytworzonych w podległych jednostkach organizacyjnych, i dostosowanie klauzul tajności do przesłanek określonych w nowej ustawie. Obowiązek przeglądu materiałów nie dotyczy zbiorów materiałów spraw zakończonych oraz kartotek ewidencyjnych, zwłaszcza stanowiących materiał archiwalny przekazany do właściwych archiwów na podstawie odrębnych przepisów (art. 181). Kierownicy jednostek organizacyjnych, w których w dniu wejścia w życie ustawy funkcjonowały kancelarie tajne, powinni poinformować o tym fakcie odpowiednio ABW lub SKW, podając także klauzulę tajności przetwarzanych informacji (obowiązek należało zrealizować w ciągu 3 miesięcy od daty wejścia ustawy w życie). Jeśli w wyniku przeglądu materiałów okaże się, że jednostka organizacyjna nie dysponuje już informacjami o klauzuli „ściśle tajne" lub „tajne", to kierownik jednostki organizacyjnej powinien poinformować odpowiednio ABW lub SKW o likwidacji kancelarii tajnej.

Jeśli jednostka organizacyjna będzie dysponentem materiałów oznaczonych maksymalnie klauzulą „poufne", funkcję kancelarii tajnej może spełniać inna komórka organizacyjna, pod warunkiem, że zostanie zapewniona możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji jednostki organizacyjnej. W tym przypadku o sposobie i trybie przetwarzania informacji niejawnych w podległej jednostce organizacyjnej zadecyduje kierownik tej jednostki, zatwierdzając sporządzone przez pełnomocnika ochrony stosowne dokumenty zawierające procedury postępowania (art. 43 ust. 3).

Jedną z ciekawszych zmian w ustawie, uwzględniającą postulaty jednostek organizacyjnych dysponujących niewielką liczbą informacji niejawnych, jest możliwość utworzenia jednej kancelarii tajnej dla kilku jednostek organizacyjnych (art. 42 ust. 3). Takie rozwiązanie wychodzi naprzeciw oczekiwaniom tych jednostek, które z przyczyn od siebie niezależnych nie mogły zapewnić kancelarii tajnej środków ochrony fizycznej przewidzianych dla takich pomieszczeń. Wiele jednostek organizacyjnych ma swoje siedziby bądź wynajmuje pomieszczenia w budynkach zabytkowych lub o lekkich konstrukcjach, w których zamontowanie krat (lub innego zabezpieczenia chroniącego przed włamaniem) czy postawienie ciężkiej szafy metalowej wymagało wysokich nakładów finansowych (np. wzmocnienia stropów) lub było niemożliwe z innych powodów (np. braku zgody konserwatora zabytków). Nie bez znaczenia były także argumenty przedstawiane przez kierowników jednostek organizacyjnych dysponujących niewielką liczbą dokumentów niejawnych związane z kosztami ponoszonymi w związku z organizacją i funkcjonowaniem kancelarii tajnej. Kierownicy jednostek organizacyjnych wskazywali na nieadekwatność przewidzianych przepisami rozwiązań i środków bezpieczeństwa w stosunku do liczby przechowywanych dokumentów niejawnych. Zmiana ustawy daje możliwość utworzenia kancelarii tajnej obsługującej wiele podmiotów, ale pod jednym warunkiem. Otóż z uwagi na to, że pracownicy kancelarii tajnej będą mieli do czynienia z informacjami niejawnymi o najwyższych klauzulach tajności („ściśle tajne" lub „tajne"), zgodę na utworzenie takiej wspólnej kancelarii musi wyrazić odpowiednio ABW lub SKW (art. 42 ust. 3), tj. służby odpowiedzialne za nadzór nad systemem ochrony informacji niejawnych. Służby, każda w zakresie swojej właściwości, dokona oceny wniosku zainteresowanych podmiotów na utworzenie „wspólnej" kancelarii tajnej i podejmie decyzję w przedmiocie udzielenia bądź odmowy zgody, o której mowa w art. 42 ust. 3. Warto zwrócić uwagę na treść tego artykułu, który stanowi, że w uzasadnionych przypadkach można utworzyć kancelarię tajną obsługującą dwie jednostki organizacyjne lub więcej − zatem normą jest tworzenie kancelarii tajnej w każdej jednostce przetwarzającej informacje o klauzuli „ściśle tajne" lub „tajne".

Bez zmiany natomiast pozostaje możliwości obsługi przez kancelarię tajną materiałów niejawnych o niższych klauzulach tajności – zgoda w tym zakresie leży w gestii kierownika jednostki organizacyjnej (art. 42 ust. 5). Kierownik jednostki organizacyjnej może także utworzyć więcej niż jedną kancelarię tajną, jeśli przemawiają za tym względy organizacyjne (art. 42 ust. 2).

Jak już wspomniano, kancelaria tajna jest wyodrębnioną komórką organizacyjną odpowiedzialną za prawidłowy obieg materiałów niejawnych. W strukturze organizacyjnej jednostki kancelaria tajna powinna podlegać pełnomocnikowi ochrony i być obsługiwana przez pracowników pionu ochrony (art. 42 ust. 4). Po-

dobnie jak w ustawie z dnia 22 stycznia 1999 r., ustawodawca wskazał pełnomocnika ochrony jako osobę odpowiedzialną w jednostce organizacyjnej za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. W nowej ustawie dokonano zmian polegających na tym, że zadania, które dotychczas należały do obowiązków „pionu ochrony", czyli komórki organizacyjnej (m.in. zapewnienie ochrony informacji niejawnych, w tym systemów teleinformatycznych, a także prowadzenie okresowych kontroli czy opracowywanie planu ochrony) zostały powierzone pełnomocnikowi ochrony. Ustawodawca wskazał zatem konkretną osobę, która powinna m.in. sporządzić plan ochrony, dokumentację określającą poziom zagrożenia nieuprawnionego ujawnienia lub utraty informacji niejawnych (nowość) czy też instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone". Podobnie doprecyzowano zadania kierownika jednostki organizacyjnej, np. poprzez nałożenie obowiązku zatwierdzania powyższej dokumentacji sporządzanej przez pełnomocnika ochrony.

Ustawodawca doprecyzował także − budzący pewne wątpliwości dotychczasowy zapis (art. 18 ust. 2a) − dotyczący powołania zastępcy pełnomocnika ochrony. Liczba pojedyncza mogła wskazywać, że w jednostce organizacyjnej można powołać tylko jedną osobę na to stanowisko. Obecny zapis (art. 14 ust. 4) stanowi, że kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony. Nowością jest art. 14 ust. 5, zgodnie z którym w odniesieniu do zastępcy pełnomocnika ochrony, jego szczegółowy zakres czynności będzie określał kierownik jednostki organizacyjnej.

Pion ochrony, a co za tym idzie kancelaria tajna i pracownicy pionu ochrony podlegają pełnomocnikowi ochrony. Kierownik jednostki organizacyjnej może powierzyć zarówno pełnomocnikowi ochrony, jak też pracownikom pionu ochrony wykonywanie innych zadań, ale pod warunkiem, że ich realizacja nie naruszy prawidłowego wykonywania zadań określonych w ustawie o ochronie informacji niejawnych (art. 15 ust. 4).

Środki bezpieczeństwa fizycznego

W rozdziale 7 ustawy zostały wprowadzone nowe terminy dotychczas niewystępujące ani w *Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, ani w aktach wykonawczych do tej ustawy (m.in. w rozporządzeniu o organizacji i funkcjonowania kancelarii tajnych). W nowej ustawie pełnomocnik ochrony został zobligowany do opracowania *dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą* (43 ust. 4). Przy określaniu poziomu zagrożenia uwzględnia się przede wszystkim rodzaje zagrożeń, liczbę dokumentów niejawnych będących w dyspozycji jed-

nostki oraz klauzule tajności tych dokumentów. Ustawodawca zastrzegł przy tym, że w uzasadnionych przypadkach przy określaniu poziomu zagrożenia uwzględnia się wskazania odpowiednio ABW lub SKW (art. 45 ust. 3). Uprawnienie powyższe jest istotne w przypadku jednostek organizacyjnych o znaczeniu strategicznym dla bezpieczeństwa państwa. ABW lub SKW będą mogły wskazać w takim przypadku dodatkowe czynniki, np. nieuwzględnione przez pełnomocnika ochrony, wpływające w sposób istotny na określenie poziomu zagrożenia, a tym samym determinujące zastosowanie odpowiednich środków bezpieczeństwa fizycznego.

Dopiero w zależności od określonego poziomu zagrożenia będą dobierane odpowiednie i adekwatne do zagrożeń środki bezpieczeństwa fizycznego (wskazane w rozporządzeniu, które zostanie wydane w trybie art. 47 ust. 1). Takie rozwiązanie pozwoli na racjonalne stosowanie środków służących do ochrony informacji niejawnych, a także ich dobór uwzględniający specyfikę jednostki organizacyjnej. Zgodnie z zapisem w art. 45 ustawy zakres stosowania środków bezpieczeństwa fizycznego dla materiałów oznaczonych klauzulami „poufne", „tajne" i „ściśle tajne" uzależnia się od poziomu rzeczywistych zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utraty w danej jednostce. Warto zwrócić uwagę, że ustawodawca zadecydował o konieczności określenia poziomu zagrożeń nie tylko dla informacji oznaczonych klauzulą „ściśle tajne" i „tajne", ale także dla informacji oznaczonych niższą klauzulą, tj. „poufne". Należy bowiem pamiętać o tym, że zgodnie z art. 5 ust. 3 ustawy informacjom nadaje się klauzulę „poufne", jeśli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej (np. utrudni prowadzenie polityki zagranicznej, realizację przedsięwzięć obronnych) czy też zakłóci porządek publiczny.

Ocena poziomu zagrożenia będzie dokonywana indywidualnie w każdej jednostce organizacyjnej i będzie podstawą do zastosowania środków bezpieczeństwa fizycznego adekwatnych do istniejących zagrożeń. W celu ujednolicenia kryteriów określenie poziomu zagrożeń oraz katalog środków ochrony fizycznej, odpowiedni do poszczególnych poziomów zagrożenia, zostaną wskazane w rozporządzeniu wydanym na podstawie delegacji art. 47 ust. 1 ustawy. W rozporządzeniu tym zostaną określone m.in. podstawowe kryteria i sposób określania poziomu zagrożeń, dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń, rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń oraz zakres stosowania środków bezpieczeństwa fizycznego. W rozporządzeniu Rada Ministrów uwzględni potrzebę racjonalizacji nakładów ponoszonych przez jednostki organizacyjne − co wskazuje, że zakres stosowanych środków bezpieczeństwa fizycznego będzie różnił się w poszczególnych jednostkach, w zależności od określonego poziomu zagrożenia i klauzuli tajności przetwarzanych informacji.

Na uwagę zasługuje także nowy termin, który pojawił się w tym rozdziale ustawy, a mianowicie strefa ochronna – kryteria tworzenia takich stref zostaną określone w cytowanym rozporządzeniu. Strefa ochronna, a właściwie strefy ochronne, w pewnym stopniu zastępują dotychczasowe terminy: strefa administracyjna i strefa bezpieczeństwa. Celem tworzenia stref, zarówno na podstawie ustawy z dnia 22 stycznia 1999 r., jak też ustawy z dnia 5 sierpnia 2010 r., jest wydzielenie obszarów, które podlegają szczególnej kontroli – uniemożliwiającej dostęp do informacji niejawnych osobom nieuprawnionym. Podobnie jak w ustawie z 22 stycznia 1999 r., ustawodawca nakazał zorganizowanie stref ochronnych oraz wprowadzenie systemu kontroli wejść i wyjść, a także określenie uprawnień do przebywania w tych strefach (art. 46 pkt. 2-3). Strefy ochronne powinny zostać zorganizowane zarówno w podmiotach, w których funkcjonują kancelarie tajne, jak też w podmiotach dysponujących informacjami oznaczonymi klauzulą „poufne".

W bezpieczeństwie fizycznym funkcjonowanie stref ochronnych (wcześniej strefy bezpieczeństwa) ma istotne znaczenie dla ochrony informacji niejawnych przed nieuprawnionym dostępem, ponieważ:

- dobrze zorganizowana strefa ochronna umożliwia identyfikację wszystkich osób poruszających się w obszarze, gdzie przetwarzane są informacje niejawne,
- zastosowane środki bezpieczeństwa (czujki, systemy alarmowe, a także szafy metalowe) powinny pozwolić na podjęcie skutecznych działań w celu uniemożliwienia dostępu osobom, które w sposób siłowy będą próbowały dotrzeć do informacji niejawnych.

Przy okazji warto również zwrócić uwagę, że w ustawie zmieniono inne pojęcie – zamiast dotychczasowych środków ochrony fizycznej są środki bezpieczeństwa fizycznego, w tym jednak przypadku zmiana dotyczy wyłącznie nazwy. Zmianie nie uległy natomiast przepisy dotyczące stosowania jedynie certyfikowanych urządzeń wykorzystywanych do zabezpieczania pomieszczeń, w których przetwarzane są informacje niejawne. W celu uniemożliwienia dostępu do informacji niejawnych osobom nieuprawnionym należy stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty (art. 46 pkt 4). Przy wyposażaniu kancelarii tajnej w szafy metalowe, w których będą przechowywane informacje niejawne, należy pamiętać, że powinny one odpowiadać odpowiedniej klasie, wskazanej w aktach wykonawczych.

Na zakończenie warto dodać, że sposób i tryb przetwarzania informacji niejawnych oraz dobór i stosowanie środków bezpieczeństwa fizycznego w podmiotach wymienionych w art. 47 ust. 3 (m.in. w Kancelarii Prezydenta Rzeczypospoli-

tej Polskiej, Kancelarii Sejmu, Senatu oraz Prezesa Rady Ministrów, Ministerstwie Sprawiedliwości, Narodowym Banku Polskim, Najwyższej Izbie Kontroli, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Centralnym Biurze Antykorupcyjnym, Policji, Straży Granicznej, Biurze Ochrony Rządu) określą, w drodze zarządzenia, kierownicy tych podmiotów − każdy w zakresie swojego działania. Natomiast wszystkie podmioty zobligowane do stosowania przepisów nowej ustawy, w tym także te wymienione w art. 47 ust. 3, mają obowiązek stosowania środków bezpieczeństwa fizycznego (odpowiednich do poziomu zagrożeń) w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji. Zastosowane środki bezpieczeństwa fizycznego mają chronić m.in. przed kradzieżą lub zniszczeniem materiału, próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne, lub przed nieuprawnionym dostępem do informacji o wyższej klauzuli tajności osób nieposiadających odpowiednich uprawnień (art. 45 ust.1). Rozporządzenie, które zostanie wydane w trybie art. 47 ust. 1, powinno uwzględnić możliwość przechowywania materiałów niejawnych w wielu pomieszczeniach (strefach ochronnych), zaopatrzone w środki bezpieczeństwa fizycznego adekwatne do klauzuli tajności przechowywanych materiałów i poziomu zagrożenia nieuprawnionego ich ujawnienia bądź utraty.

Tomasz Gołębiewski

Zmiany w zakresie bezpieczeństwa osobowego, wprowadzone nową ustawą o ochronie informacji niejawnych

Uchwalenie 5 sierpnia 2010 r. przez Sejm RP nowej ustawy o ochronie informacji niejawnych – zamiast kolejnej nowelizacji funkcjonującej od marca 1999 r. *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, która powstała w związku z integracją Polski z NATO – jest wynikiem obszerności zakresu proponowanych zmian, co spowodowało, że koniecznością stało się nie tylko kolejne sprecyzowanie, dodanie i usunięcie niektórych przepisów, ale przede wszystkim uporządkowanie redakcyjne i merytoryczne tekstu ustawy. Nałożenie się nowych rozwiązań na poprzednio obowiązującą ustawę doprowadziłoby do powstania niejasnego i niespójnego aktu prawnego, bardzo rozbieżnego od tekstu pierwotnego z 1999 r., z nienaturalną numeracją poszczególnych jednostek redakcyjnych.

Powyższe uwagi odnoszą się w szczególności do przepisów ustawy regulujących kwestie związane z tzw. bezpieczeństwem osobowym, tj. zasadami upoważniania osób do dostępu do informacji niejawnych, w tym z trybem i zasadami prowadzenia postępowań sprawdzających. Dotychczasowa redakcja rozdziału 5. (*Dostęp do informacji niejawnych. Postępowania sprawdzające*) poprzedniej ustawy była niespójna, te same kwestie poruszano w kilku różnych jednostkach redakcyjnych (np. wyjątki od konieczności poddania się postępowaniu sprawdzającemu), a pomiędzy poszczególnymi przepisami brakowało częstokroć związku przyczynowo-skutkowego – np. dopiero po opisie zasad dotyczących okresów ważności poświadczeń określano zasady prowadzenia postępowań sprawdzających, których te poświadczenia są wynikiem.

Przyjęta przez parlament 5 sierpnia 2010 r. nowa ustawa porządkuje sprawy związane z bezpieczeństwem osobowym w rozdziale 5. (pt. *Bezpieczeństwo osobowe*). Ustawa ta grupuje związane z bezpieczeństwem osobowym zagadnienia tematycznie i funkcjonalnie, każdemu z nich poświęca osobną jednostkę redakcyjną. Merytoryczny zakres zmian nie jest natomiast – co do swej istoty – szeroki, ponieważ intencją ustawodawcy była przede wszystkim próba uporządkowania oraz sprecyzowania nie do końca jednoznacznych dotychczas przepisów.

Przed szczegółowym opisem wprowadzonych nową ustawą zmian w rozdziale 5 należy odnieść się najpierw do kwestii związanych z bezpieczeństwem osobowym, które – z uwagi na zasady techniki legislacyjnej (jako przepisy ogólne lub odrębne) – w rozdziale tym nie zostały ujęte. I tak kluczowa dla bezpie-

czeństwa osobowego definicja dawania rękojmi zachowania tajemnicy znajduje się w „słowniczku" (rozdział 1. *Przepisy ogólne*, art. 2 pkt 2 nowej ustawy, poprzednio w art. 2 pkt 4), a zasada *need-to-know* (zastrzegająca, że osoba posiadająca poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o określonej klauzuli tajności nie może posiadać „z urzędu" lub domagać się dostępu do każdej informacji o takiej – bądź niższej – klauzuli, ale tylko do tych informacji, które mają związek z wykonywanymi przez tę osobę obowiązkami służbowymi) – w art. 4 ust. 1 (poprzednio w art. 3).

W art. 3 nowej ustawy (poprzednio w art. 1 ust. 4) wskazano konkretne przepisy kodeksu postępowania administracyjnego, które mają zastosowanie do postępowań sprawdzających (a także do postępowań bezpieczeństwa przemysłowego). W nowej ustawie nieznacznie rozszerzono zakres stosowania kpa, czy to poprzez wskazanie tych przepisów w art. 3 ustawy, czy to poprzez włączenie tej samej albo zmodyfikowanej treści przepisów kpa bezpośrednio do ustawy. Poszerzenie zakresu stosowania przepisów kpa ogranicza się wyłącznie do kwestii proceduralnych, w praktyce i tak dotychczas stosowanych (zgodnie z obowiązkiem rzetelnego dokumentowania czynności sprawdzających), ułatwiających organom prowadzącym postępowania ich sprawniejszą realizację, a z punktu widzenia osoby sprawdzanej – szybsze uzyskanie poświadczenia bezpieczeństwa. W nowej ustawie rozszerzono stosowanie kpa o następujące przepisy: art. 50 (wezwanie do udziału w czynnościach, przyjmowanie wyjaśnień), art. 55 (telefoniczne załatwianie spraw), art. 65 (przekazanie sprawy do właściwego organu za postanowieniem), art. 72 (utrwalanie rezultatów czynności w formie adnotacji), art. 75 § 1 (dopuszczanie wszelkich dowodów), art. 77 § 1 (wyczerpujące zebranie i ocena dowodów), art. 103 (wstrzymanie biegu terminów w okresie zawieszenia), art. 109 § 1 (decyzje w formie pisemnej) oraz 125 § 1 (postanowienia w formie pisemnej). Usunięto natomiast z tej listy art. 105 § 1 (umorzenie postępowania z uwagi na bezprzedmiotowość) – treść tego przepisu włączono bezpośrednio do ustawy – oraz art. 113 § 2-3 (pisemne wyjaśnianie – w formie postanowienia – wątpliwości strony co do treści decyzji oraz prawo do składania zażaleń na takie postanowienia). Ten ostatni przepis nie będzie obowiązywał ze względu na teoretyczne wątpliwości związane z brakiem możliwości jego faktycznej realizacji – przekazywanie wyjaśnienia decyzji mogłoby okazać się niemożliwe z uwagi na ochronę informacji niejawnych.

Kolejne przepisy regulujące kwestie związane z realizacją postępowań sprawdzających, a niewłączone do rozdziału 5, zostały umieszczone w rozdziale 3. (*Organizacja ochrony informacji niejawnych*). W art. 10 nowej ustawy określono szczegółową właściwość Służby Kontrwywiadu Wojskowego oraz Agencji Bezpieczeństwa Wewnętrznego do realizacji zadań związanych z funkcjonowaniem syste-

mu ochrony informacji niejawnych (nieformalny podział na „sferę cywilną" i „sferę wojskową"), w tym także do prowadzenia postępowań sprawdzających. Funkcjonujący w dotychczasowej ustawie w rozdziale 5 – w art. 29 – podział kompetencji pomiędzy ABW i SKW dotyczył wyłącznie postępowań sprawdzających i dopiero na tej podstawie, przez analogię, stosowano go również w odniesieniu do innych obszarów związanych z ochroną informacji niejawnych. W art. 10 ust. 2 nowej ustawy zakres kompetencji SKW opisano odmiennie niż w obowiązujących wcześniej przepisach, ograniczając realizowanie zadań SKW jedynie do: Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych[1], ataszatów obrony w placówkach zagranicznych oraz żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w punktach 1-2. Zasadniczą zmianą w stosunku do obowiązujących dotychczas przepisów jest przeniesienie wyłącznie na ABW kompetencji do prowadzenia postępowań bezpieczeństwa przemysłowego (a w jego ramach – postępowań sprawdzających) w odniesieniu do przedsiębiorców realizujących produkcję lub usługi, ze względu na obronność państwa i na potrzeby Sił Zbrojnych, z którymi to usługami jest związany dostęp do informacji niejawnych, jeżeli nie jest to przedsiębiorca podległy bądź nadzorowany przez ministra obrony narodowej. Wyłączna właściwość ABW do prowadzenia tych postępowań wynika z treści ust. 3 cytowanego przepisu, w którym wskazano, że ABW jest właściwa do realizacji zadań do wszystkich innych podmiotów ustawy, które nie zostały wskazane w ust. 2 (jako te, które pozostają we właściwości SKW).

Na podstawie art. 11 nowej ustawy jedynie Szef ABW pełni funkcję krajowej władzy bezpieczeństwa, czyli nadzoruje system ochrony informacji niejawnych w relacjach międzynarodowych, zwłaszcza z NATO i UE (dotychczas funkcję tę pełnił zarówno Szef ABW, jak i Szef SKW[2]). Natomiast zarówno ABW, jak i SKW (w odniesieniu do sfery wojskowej) są upoważnione do wydawania poświadczeń bezpieczeństwa NATO i UE (a więc także w przypadku, gdy poświadczenie takie będzie niezbędne do wykonywania zadań np.: policjantowi, funkcjonariuszowi CBA bądź żołnierzowi Żandarmerii Wojskowej). Chociaż sprecyzowanie szczegółowych rozwiązań w tym zakresie nastąpi dopiero po wejściu w życie rozporządzenia o współdziałaniu Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW, można jednak założyć, że na

[1] Ich wykaz zawiera załącznik do *Decyzji Nr 246/MON Ministra Obrony Narodowej z dnia 7 lipca 2010 r. w sprawie bezpośredniego podporządkowania jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych* (Dz. Urz. MON, Nr 14, poz. 184).

[2] W poprzedniej ustawie kwestię krajowej władzy bezpieczeństwa, na poziomie bardzo ogólnym, regulował art. 15.

potrzeby osób zatrudnionych w instytucjach międzynarodowych lub przedsiębiorców kooperujących z podmiotami zagranicznymi, niezbędne będzie dodatkowe potwierdzenie tego faktu przez ABW w postaci zaświadczenia, mimo posiadania poświadczenia bezpieczeństwa NATO czy UE wydanego przez ABW lub SKW (zgodnie ze wzorem określonym w rozporządzeniu Prezesa Rady Ministrów[3]).

Nowością w stosunku do dotychczas obowiązujących przepisów jest poddanie kontroli Prezesa Rady Ministrów prowadzonych przez ABW i SKW postępowań sprawdzających (a także postępowań bezpieczeństwa przemysłowego) w zakresie prawidłowości ich realizacji (art. 12 ust. 3 pkt 1 nowej ustawy). Z jednej strony jest to dodatkowa gwarancja dla obywateli, że służby prowadzące wobec nich postępowania sprawdzające realizują je zgodnie z przepisami ustawy, a przede wszystkim kierują się zasadą bezstronności, szczególnej staranności oraz działania bez zbędnej zwłoki (ta ostatnia zasada wynika z art. 12 kpa mającego zastosowanie w ustawie o ochronie informacji niejawnych), z drugiej – konsekwencja wskazanego literalnie w nowej ustawie nieuznawania za ważne poza miejscem aktualnego zatrudnienia poświadczeń wydawanych przez Agencję Wywiadu, Służbę Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, Policję, Żandarmerią Wojskową, Straż graniczną, Służbę Więzienną oraz Biuro Ochrony Rządu (postępowania prowadzone prze te podmioty nie będą podlegać takiej kontroli). W tym samym artykule zapisano funkcjonujące dotychczas prawo ABW (lub SKW – w zakresie jej właściwości) do kontroli postępowań sprawdzających prowadzonych przez pełnomocników ochrony, z wyjątkiem postępowań sprawdzających prowadzonych przez pełnomocników ochrony w służbach upoważnionych do prowadzenia postępowań wobec własnych pracowników.

Podobnie jak wcześniej, poza rozdziałem 5 (w art. 13 nowej ustawy, poprzednio w art. 14) pozostaje obowiązek współdziałania kierowników jednostek organizacyjnych ze służbami uprawnionymi do prowadzenia postępowań sprawdzających, a w szczególności udostępniania dokumentów i informacji oraz udzielania niezbędnej pomocy. Tak jak dotychczas służby upoważnione do prowadzenia postępowań wobec własnych pracowników udostępniają informacje tylko w przypadku, gdy same stwierdzą, że osoba objęta postępowaniem nie daje rękojmi zachowania tajemnicy. Istotną zmianą jest natomiast rozszerzenie obowiązku współdziałania na wszystkie służby, które prowadzą „samodzielne" postępowania sprawdzające wobec własnych pracowników (dotychczas funkcjonował wyłącznie obowiązek współdziałania ze „służbami ochrony państwa", czyli tylko ABW i SKW). Ta zmiana ma też odzwierciedlenie w wydanym na podstawie art. 13 *Rozporządzeniu Prezesa*

[3] Wzór poświadczenia bezpieczeństwa NATO i UE określa załącznik nr 3 do *Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa* (Dz.U. z 2010 r., Nr 258, poz. 1752).

Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego (Dz.U. z 2010 r., Nr 258, poz. 1750). Dodatkowo, w ramach tej współpracy, służby prowadzące postępowania mogą weryfikować nie tylko dane z ankiety, ale również inne informacje uzyskane w toku postępowania (analogiczna zmiana dotyczy czynności podejmowanych w toku postępowań sprawdzających, vide art. 25 ust. 1 nowej ustawy).

Sformułowanie dotyczące współdziałania kierowników jednostek organizacyjnych *ze służbami uprawnionymi do prowadzenia postępowań sprawdzających* jest jedną z konsekwencji odejścia od niejednoznacznego terminu służba ochrony państwa, określającego w poprzedniej ustawie ABW i SKW. Skutkiem tego jest nadanie wszystkim wskazanym wyżej służbom dotychczasowych uprawnień do podejmowania czynności w postępowaniach sprawdzających przysługujących jedynie *służbom ochrony państwa*, co dotychczas – przez niejednoznaczność zapisu w art. 30 – powodowało nierzadko pewne utrudnienia w egzekwowaniu przysługujących służbom innym niż ABW i SKW uprawnień, np. związanych ze sprawdzeniami historii i obrotów na rachunkach bankowych osób sprawdzanych[4]. Konsekwentnie zmianę tę uwzględnia również rozporządzenie o współpracy i udzielaniu niezbędnej pomocy w postępowaniach sprawdzających. „Zrównanie" ABW i SKW z innymi służbami uprawnionymi do prowadzenia postępowań sprawdzających wobec własnych pracowników nie jest jednak pełne – nie dotyczy wydawanych przez nie poświadczeń bezpieczeństwa oraz udostępniania akt postępowań sprawdzających. W nowej ustawie sprecyzowano, że poświadczenia wydawane przez służby i organy upoważnione do prowadzenia postępowań wobec własnych pracowników nie będą – w przeciwieństwie do poświadczeń wydanych przez ABW lub SKW (także wobec własnych pracowników) – ważne poza służbą, która wydała to poświadczenie. Z kolei akta postępowań sprawdzających prowadzonych przez służby o charakterze kontrwywiadowczym (ABW i SKW) oraz wywiadowczym (AW i SWW) nie będą udostępniane innej służbie (czyli akta postępowania prowadzonego przez AW nie będą udostępniane np. SKW i vice versa).

Inne przepisy związane z bezpieczeństwem osobowym, pozostawione poza rozdziałem 5, dotyczące odwołań i skarg oraz wznowienia postępowania, jak również ewidencji i udostępniania danych oraz akt postępowań sprawdzających, zostały wyodrębnione do osobnych rozdziałów (odpowiednio – 6. i 10.) i zostaną opisane po omówieniu zmian w rozdziale 5., podobnie jak dotyczące bezpieczeństwa osobowego przepisy przejściowe i końcowe (rozdział 12).

[4] Odpowiednią zmianę w ustawie Prawo bankowe wprowadza art. 120 nowej ustawy, a w ustawie o obrocie instrumentami finansowymi – art. 162.

Jak wspomniano na początku ustawodawca tak skonstruował przepisy rozdziału 5 (art. 21-34) nowej ustawy, że każda jednostka redakcyjna stanowi wyczerpujący opis odrębnego zagadnienia. W art. 21 określono ogólne warunki dostępu do informacji niejawnych, dotychczas opisane w art. 27 ust. 1, art. 28 ust. 1 oraz znajdującym się w rozdziale *Bezpieczeństwo przemysłowe* art. 68 ust. 4-5. W stosunku do poprzednio obowiązujących rozwiązań zniesiono obowiązek posiadania poświadczenia bezpieczeństwa (a tym samym prowadzenia postępowań sprawdzających) w przypadku ubiegania się o dostęp do informacji niejawnych o klauzuli „zastrzeżone" (a tym samym także adekwatnych im klauzulą, np. „*Restreint UE/ UE restricted"* czy „*NATO Restricted"*, informacji niejawnych organizacji międzynarodowych). Dostęp do tego typu informacji będzie możliwy na podstawie pisemnego upoważnienia kierownika jednostki organizacyjnej (jeżeli osoba nie będzie posiadać wydanego wcześniej poświadczenia bezpieczeństwa) oraz oczywiście – po przeszkoleniu w zakresie ochrony informacji niejawnych (art. 21 ust. 4 nowej ustawy). Powyższe nie dotyczy jednak osób zajmujących stanowiska pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony. Osoby te, co wynika z przepisów dotyczących wymagań niezbędnych do objęcia tych funkcji (art. 14 ust. 3), muszą posiadać wydane przez ABW lub SKW poświadczenie bezpieczeństwa, nawet wówczas, gdy w „ich" jednostce organizacyjnej niezbędne jest uzyskanie dostępu do informacji niejawnych jedynie o klauzuli „zastrzeżone" (wówczas uzyskają poświadczenie bezpieczeństwa, upoważniające do dostępu do informacji niejawnych o klauzuli „poufne", ponieważ ustawa nie przewiduje poświadczeń, upoważniających do dostępu do informacji niejawnych o klauzuli „zastrzeżone"). Ponadto wymóg posiadania stosownego upoważnienia kierownika jednostki organizacyjnej nie dotyczy samego kierownika jednostki organizacyjnej. Aby mógł on mieć dostęp do informacji niejawnych o klauzuli „zastrzeżone", nie musi sam sobie wystawiać stosownego upoważnienia (wystarczy sam fakt objęcia takiej funkcji).

Z katalogu okoliczności wyłączających dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne" (a także adekwatnych im klauzulą informacji niejawnych organizacji międzynarodowych) usunięto ukaranie prawomocnym wyrokiem za przestępstwa umyślne ścigane z oskarżenia publicznego, także popełnione za granicą. W nowej ustawie jest to przesłanka do odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa, ale tylko przy jednoczesnym wystąpieniu dwóch warunków − orzeczenia kary pozbawienia wolności oraz gdy czyn, za który nastąpiło skazanie, wywołuje ustawowe wątpliwości związane z oceną dawania rękojmi zachowania tajemnicy[5].

[5] Więcej miejsca temu zagadnieniu będzie poświęcone przy omówieniu zmian dotyczących decyzji o odmowach wydania poświadczenia bezpieczeństwa. Dotychczas, w przypadku ustalenia w toku postępowania prowadzonego wobec osoby ubiegającej się o dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne", że osoba ta jest skazana za przestępstwo umyślne, ścigane z oskarżenia publicznego, w tym przestępstwo karno-skarbowe, postępowanie sprawdzające musiało skończyć się decyzją o odmowie wydania poświadczenia bezpieczeństwa.

W art. 22 określono rodzaje postępowań sprawdzających, dotychczas opisane w art. 36 ust. 1 oraz art. 37 ust. 2-3. W stosunku do poprzednio obowiązujących rozwiązań zniesiono instytucję specjalnych postępowań sprawdzających. Według generalnej zasady w przypadku ubiegania się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli „poufne" będzie prowadzone zwykłe postępowanie sprawdzające, a w pozostałych przypadkach – tj. w przypadku ubiegania się o wydanie poświadczenia bezpieczeństwa, upoważniającego do dostępu do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" oraz adekwatnych im klauzulą, np. „*Secret UE/EU secret", „Très secret UE/EU top secret", „NATO Secret", „Cosmic Top Secret"*, informacji niejawnych organizacji międzynarodowych – postępowanie poszerzone. Ponadto postępowania poszerzone będą również prowadzone w przypadku kierowników jednostek organizacyjnych, pełnomocników ochrony, zastępców pełnomocników ochrony i kandydatów na te stanowiska (wobec pełnomocników ochrony i ich zastępców oraz kandydatów na te stanowiska – także w przypadku konieczności uzyskania dostępu do informacji niejawnych jedynie o klauzuli „zastrzeżone") oraz wobec osób ubiegających się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych organizacji międzynarodowych o klauzuli adekwatnej do klauzuli „poufne" (np. „*Confidentiel UE/EU confidential"* czy *„NATO Confidential"*). W przypadku gdy osoby te będą ubiegać się jedynie o dostęp do informacji niejawnych o klauzuli „poufne" i (lub) adekwatnych im klauzulą, informacji niejawnych organizacji międzynarodowych – po przeprowadzeniu postępowania poszerzonego, będzie wówczas wydawane poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych jedynie o klauzuli „poufne" (lub adekwatnych międzynarodowych). Podobnie dotyczy to kierowników jednostek organizacyjnych czy pełnomocników ochrony – w przypadku ubiegania się przez nich o dostęp do informacji niejawnych o klauzuli „poufne", będzie im wydane poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych jedynie o klauzuli „poufne". A ponieważ nie ma poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych o klauzuli „zastrzeżone", pełnomocnicy ochrony i ich zastępcy, ubiegający się o dostęp do informacji niejawnych jedynie o takiej klauzuli tajności, otrzymają poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych jedynie o klauzuli „poufne".

W art. 23 określono właściwość organów do prowadzenia postępowań sprawdzających[6], która była dotychczas opisana w art. 30, art. 37 ust. 1, art. 38 ust. 1 i art. 39. W stosunku do poprzednio obowiązujących rozwiązań doprecyzowano, że ABW i SKW oraz inne służby upoważnione do prowadzenia postępowań

[6] W zależności od rodzaju postępowania; ogólna właściwość ABW i SKW jest opisana w art. 10 nowej ustawy, a uprawnienie tylko tych służb do prowadzenia postępowań przed wydaniem poświadczeń bezpieczeństwa organizacji międzynarodowych – w art. 11.

wobec własnych pracowników, prowadzą również postępowania wobec osób, które wykonują na ich rzecz czynności zlecone lub ubiegają się o wykonywanie takich czynności. Najistotniejszą zmianą merytoryczną w kwestii właściwości organów do prowadzenia postępowań sprawdzających jest upoważnienie Biura Ochrony Rządu do prowadzenia „samodzielnych" postępowań sprawdzających (tj. wobec własnych pracowników, żołnierzy lub funkcjonariuszy oraz kandydatów do zatrudnienia lub podjęcia służby) oraz upoważnienie ABW do prowadzenia postępowań sprawdzających wobec Szefów SKW, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Biura Ochrony Rządu, Komendantów Głównych Policji i Straży Granicznej oraz Dyrektora Generalnego Służby Więziennej, a także kandydatów na te stanowiska. Szef SKW został natomiast uprawniony do prowadzenia postępowań wobec Szefa ABW, Służby Wywiadu Wojskowego oraz Komendanta Głównego Żandarmerii Wojskowej, a także kandydatów na te stanowiska. Taki zapis oznacza praktyczną realizację zasady wyłączenia pracownika od udziału w sprawie, w której jedną ze stron jest osoba pozostająca wobec niego w stosunku nadrzędności służbowej (art. 24 § 1 pkt 7 kpa), podobnie jak w przypadku uprawnienia ABW i SKW do realizacji postępowań sprawdzających wobec kierowników jednostek organizacyjnych, nawet gdy ubiegają się oni o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych jedynie o klauzuli „poufne".

Ponadto sprecyzowano, że w przypadku pełnomocników ochrony w SKW, AW, CBA, BOR, SG, SW i Policji, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska, postępowania sprawdzające będzie prowadziła ABW, a wobec pełnomocników w ABW, SWW i ŻW – postępowania będą prowadzone przez SKW. Takie zasady (ale z wyjątkiem pełnomocników w ABW i SKW) wynikały dotychczas pośrednio z art. 18 ust. 3 pkt 3 określającego formalne warunki dla pełnomocników, ale pozostającego w sprzeczności z dotychczasowym art. 30, wskazującym, że niektóre służby prowadzą „samodzielne" postępowania wobec własnych pracowników. Według niektórych interpretacji mogło z tego wynikać, że pełnomocnik ochrony w służbie wskazanej w art. 30, jako jej pracownik bądź funkcjonariusz, nie musiał posiadać poświadczenia wydanego przez ABW bądź SKW.

W art. 24 określono zasady prowadzenia postępowań sprawdzających, dotychczas opisane w art. 31 ust. 1, art. 32, art. 34 i art. 35 oraz art. 42 ust. 1. W stosunku do poprzednio obowiązujących rozwiązań poszczególne kategorie wątpliwości, ustalane w toku postępowania, pogrupowano hierarchicznie, poczynając od najpoważniejszego dla bezpieczeństwa państwa zagrożenia w postaci prowadzenia działalności szpiegowskiej bądź terrorystycznej, poprzez zagrożenie ze strony obcych służb specjalnych w postaci prób werbunku, po członkostwo w organizacjach ekstremistycznych. Występującą wcześniej w jednym przepisie wątpliwość zwią-

zaną z podawaniem nieprawdziwych informacji w postępowaniu sprawdzającym oraz związaną z pojawieniem się okoliczności powodujących ryzyko podatności na szantaż lub wywieranie presji, rozdzielono, ponieważ o ile podawanie nieprawdziwych informacji w postępowaniu jest istotnie najczęściej związane z jednoczesnym występowaniem okoliczności powodujących ryzyko podatności na wywieranie presji (obawa przed ujawnieniem kompromitujących faktów), o tyle w praktyce realizacji postępowań często zdarzało się, że podatność na szantaż lub presję była samoistną podstawą do decyzji o odmowie wydania poświadczenia bezpieczeństwa, bez związku z podawaniem w toku postępowania nieprawdziwych informacji. Taki przypadek ma miejsce wówczas, gdy osoba sprawdzana wpadnie w spiralę zadłużenia (nie jest w stanie na bieżąco regulować zobowiązań finansowych, ponieważ jej miesięczne dochody są niższe od miesięcznych rat tych zobowiązań) albo gdy osobie sprawdzanej przedstawiono zarzut popełnienia przestępstwa np. o charakterze korupcyjnym.

Istotną zmianą jest sprecyzowanie przez ustawodawcę, jakiego typu postępowanie osoby sprawdzanej z informacjami niejawnymi wywołuje niedające się usunąć wątpliwości – dotychczasowy przepis był na tyle ogólny, że za niewłaściwe postępowanie z informacjami niejawnymi można było uznać choćby jednorazowe naruszenie formalnych przepisów dotyczących ochrony informacji niejawnych. W przyjętym obecnie rozwiązaniu, aby można było stwierdzić występowanie wątpliwości dotyczących właściwego postępowania osoby sprawdzanej z informacjami niejawnymi, niezbędne jest spełnienie co najmniej jednego z czterech warunków: 1) jeżeli doprowadziło ono bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym; 2) jeżeli było wynikiem celowego działania; 3) jeżeli stwarzało realne zagrożenie ich nieuprawnionego ujawnienia i nie miało charakteru incydentalnego; 4) jeżeli dopuściła się go osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych, tj. pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej. Powyższe rozwiązanie w większym stopniu gwarantuje osobom sprawdzanym, że ocena ich niewłaściwego postępowania z informacjami niejawnymi będzie dokonywana przez organ prowadzący postępowanie na podstawie rzeczywistego wpływu uchybień na ochronę informacji niejawnych, a nie na podstawie formalnego naruszania tego typu przepisów. Nie oznacza to jednak, że formalne naruszanie przepisów nie będzie mogło w takim przypadku stanowić podstawy do odmowy wydania poświadczenia bezpieczeństwa – stanie się tak wówczas, gdy dopuści się go osoba szczególnie zobowiązana, na podstawie ustawy, do ochrony informacji niejawnych, ale oczywiście przy ocenie tego typu przypadków będzie brana pod uwagę skala tych naruszeń oraz potencjalne szkody, jakie te naruszenia mogły spowodować.

Ustawodawca zastąpił również nieprecyzyjny dotychczas zapis, dotyczący ustalania w toku postępowania wątpliwości związanych z uzależnieniem od narko-

tyków, na szerszy semantycznie zapis o ustalaniu wątpliwości związanych z uzależnieniem od środków odurzających lub substancji psychotropowych.

Kolejną zmianą jest wprowadzenie jednego dla każdego rodzaju postępowań sprawdzających, trzymiesięcznego terminu ich realizacji, który nadal pozostaje terminem instrukcyjnym, co oznacza, że jego przekroczenie nie wywołuje skutków prawnych. Sytuacja taka musi być jednak zawsze uzasadniona dobrem postępowania. W obecnie przyjętym rozwiązaniu dodatkową gwarancją dla osób sprawdzanych terminowej realizacji postępowań sprawdzających przez uprawnione organy jest wprowadzenie obowiązku – o ile zainteresowana osoba o to wystąpi – poinformowania jej przez ten organ o przyczynach niedotrzymania trzymiesięcznego terminu realizacji postępowania oraz wskazania jej nowego terminu zakończenia sprawy. Taki zapis jest wprowadzeniem do ustawy zmodyfikowanego nieco art. 36 kpa – zmodyfikowanego dlatego, że często przekazanie osobie sprawdzanej pełnej informacji o przyczynach przedłużenia się prowadzonego wobec niej postępowania nie byłoby możliwe z uwagi na przepisy samej ustawy (tj. jeżeli przyczyna tego przedłużenia będzie wyczerpywała definicję informacji niejawnej).

W art. 25 określono czynności podejmowane w toku zwykłych postępowań sprawdzających, opisane dotychczas w art. 37 ust. 4-6 oraz art. 40 ust. ust. 1-2. W stosunku do poprzednio obowiązujących rozwiązań nastąpiły trzy fundamentalne zmiany. Pierwszą z nich jest ograniczenie obligatoryjnych sprawdzeń w ewidencjach, rejestrach i kartotekach – oprócz sprawdzenia w ewidencjach niedostępnych powszechnie dokonywanego za pośrednictwem ABW lub SKW – tylko do sprawdzenia w Krajowym Rejestrze Karnym (dotychczas obowiązkowe było również sprawdzenie w aktach stanu cywilnego oraz Centralnym Zarządzie Służby Więziennej). Powyższe nie wyklucza przeprowadzania innych sprawdzeń, w tym w aktach stanu cywilnego oraz w CZSW, ale daje organowi prowadzącemu postępowanie większą swobodę w doborze czynności sprawdzających, które ten uzna za konieczne w ramach konkretnego postępowania.

Druga zmiana dotyczy możliwości weryfikacji w ramach postępowania sprawdzającego nie tylko – jak dotychczas – danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie bezpieczeństwa osobowego, ale także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego – oczywiście tylko tych, które organ prowadzący to postępowanie uzna za niezbędne do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

Trzecią fundamentalną zmianą jest wprowadzenie również do postępowania zwykłego obowiązku zapewnienia osobie sprawdzanej przez organ je prowadzący możliwości osobistego ustosunkowania się – w trybie wysłuchania – do in-

formacji wywołujących wątpliwości niepozwalajace na ustalenie, czy osoba ta daje rękojmię zachowania tajemnicy (dotychczas tylko w postępowaniach poszerzonych i specjalnych). Dodatkowo sprecyzowano, że z przebiegu wysłuchania należy sporządzić protokół, który podpisują osoba prowadząca wysłuchanie, osoba wysłuchiwana oraz jej pełnomocnik, jeżeli uczestniczył w wysłuchaniu. Od wysłuchania odstępuje się, jeżeli mogłoby ono doprowadzić do ujawnienia informacji niejawnych (wcześniej warunkiem odstąpienia było tylko zagrożenie ujawnieniem osobie nieuprawnionej informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"), a zmiana w tym zakresie jest wynikiem zmiany definicji informacji niejawnych. Wprowadzono także obowiązek odstąpienia od wysłuchania, w sytuacji gdy postępowanie doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy (taki zapis jest wynikiem uwzględnienia treści jednego z uzasadnień wyroku Naczelnego Sądu Administracyjnego, wydanego w sprawie dotyczącej uchylenia decyzji o odmowie wydania poświadczenia bezpieczeństwa).

Ponadto upoważniono ABW lub SKW do przekazywania pełnomocnikowi ochrony nie tylko informacji o wynikach sprawdzeń w ewidencjach niedostępnych powszechnie, ale także o wyniku rozmowy z osobą sprawdzaną, jeżeli w toku postępowania, prowadzonego przez pełnomocnika, ABW lub SKW uznała, że przeprowadzenie takiej rozmowy jest konieczne.

W art. 26 odniesiono się do czynności podejmowanych w toku poszerzonych postępowań sprawdzających opisanych dotychczas w art. 38 i 39. Odpowiednia redakcja art. 26 nowej ustawy (poprzez odwołania do art. 25 i likwidację odrębnych postępowań specjalnych) spowodowała, że nie ma już wątpliwości interpretacyjnych dotyczących tego, czy czynności, które były fakultatywne w postępowaniu wobec osoby ubiegającej się o dostęp do informacji niejawnych o klauzuli „tajne", mają być obligatoryjne w postępowaniu wobec osoby ubiegającej się o dostęp do informacji niejawnych o klauzuli „ściśle tajne". W stosunku do poprzednio obowiązujących rozwiązań wprowadzono możliwość bardziej elastycznego i racjonalnego doboru takiego zakresu podejmowanych czynności, jaki organ prowadzący postępowanie uzna za niezbędny w konkretnej sytuacji (uwzględniając z jednej strony zasadę rzetelnego dokumentowania, a z drugiej zasadę ekonomiczności podejmowanych działań). Podobnie jak w przypadku postępowania zwykłego, obowiązkowe będzie jedynie sprawdzenie w KRK oraz ewidencjach niedostępnych powszechnie. Jeżeli organ uzna to za konieczne (na podstawie uzyskanych wcześniej informacji), w toku postępowania poszerzonego będzie oczywiście możliwość sprawdzeń w innych ewidencjach, rejestrach i kartotekach oraz przeprowadzenia rozmowy z osobą sprawdzaną lub – jeżeli jest to konieczne na podstawie uzyskanych informacji – jej wysłuchania.

W ramach postępowania poszerzonego pozostaje możliwość przeprowadzania rozmów z przełożonymi osoby sprawdzanej lub z innymi osobami, wywiadu w miejscu zamieszkania, sprawdzenia stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, zwłaszcza wobec Skarbu Państwa, a także zobowiązania osoby sprawdzanej do poddania się specjalistycznym badaniom i udostępnienia wyników tych badań. Przy tej ostatniej czynności sprecyzowano, że lekarzowi przeprowadzającemu badanie pod kątem stwierdzenia bądź wykluczenia choroby lub dolegliwości psychicznej, lub też uzależnienia od alkoholu, środków odurzających lub psychotropowych, może być udostępniona dokumentacja medyczna osoby sprawdzanej – oczywiście wyłącznie w zakresie dotyczącym wątpliwości, o których mowa w art. 24 ust. 3 pkt. 2 i 3 nowej ustawy.

Rozmowy z osobami polecającymi nie będą – jak dotychczas – czynnością obligatoryjną. Będzie można je przeprowadzać tylko w przypadku ubiegania się o wydanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli „ściśle tajne" oraz adekwatnych im klauzulą: *„Très secret UE/EU top secret"* i „*Cosmic Top Secret"*. Celem takiej rozmowy nie będzie potwierdzenie tożsamości osoby sprawdzanej, ale uzyskanie wszelkich informacji mogących mieć wpływ na ocenę dawania rękojmi zachowania tajemnicy przez tę osobę.

W art. 27 określono zasady zawieszania postępowań sprawdzających, dotychczas opisane w art. 36 ust. 2c-2e. W stosunku do poprzednio obowiązujących rozwiązań do okoliczności umożliwiających zawieszenie postępowania dodano *brak możliwości przeprowadzenia skutecznego postępowania sprawdzającego z przyczyn niezależnych od organu je prowadzącego*[7]. Przepis ten można zastosować np. w sytuacji, gdy osoba objęta postępowaniem sprawdzającym odmawia kontaktu lub przekazania informacji organowi prowadzącemu postępowanie, ale formalnie nie cofa swojej zgody na prowadzenie postępowania. Z kolei dotychczasową podstawę do zawieszenia postępowania, w postaci wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe, uznano za szczególny przypadek sytuacji, gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ (jest to nieco zmieniona formuła art. 97 § 1 pkt 4 kpa mającego zastosowanie do postępowań sprawdzających). Ponadto sprecyzowano, że długotrwała choroba umożliwiająca zawieszenie postępowania, to choroba dłuższa niż 30 dni.

[7] W pierwotnym brzemieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 1999 r., Nr 11, poz. 95), w art. 37 ust. 9, okoliczność taka stanowiła podstawę do odmowy wydania poświadczenia bezpieczeństwa.

Do dotychczasowego obowiązku podjęcia przez organ prowadzący zawieszonego postępowania, w przypadku ustąpienia przyczyny uzasadniającej jego zawieszenie, wprowadzono dodatkowo możliwość odwieszenia zawieszonego postępowania, gdy ujawniono okoliczności mogące stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego. Tak więc w sytuacji, gdy wnioskodawca postępowania wystąpi w stosunku do osoby sprawdzanej, wobec której prowadzone postępowanie sprawdzające zostało zawieszone z uwagi na przedstawienie jej zarzutów popełnienia przestępstwa o charakterze korupcyjnym, o umorzenie tego postępowania z uwagi na rezygnację z zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych, postępowanie takie będzie można umorzyć (oczywiście po jego uprzednim podjęciu), bez konieczności – jak to było w poprzedniej ustawie – czekania na zakończenie postępowania karnego. Ponadto na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego zawieszeniu oraz o jego podjęciu nie tylko osoby sprawdzanej i wnioskodawcy, ale również pełnomocnika ochrony (o ile oczywiście to sam pełnomocnik ochrony nie jest organem, który prowadzi to postępowanie).

Z punktu widzenia osób objętych postępowaniami niezwykle istotne jest sprecyzowanie trybu składania zażaleń na postanowienia o zawieszeniu oraz o podjęciu zawieszonego postępowania sprawdzającego, które ma się odbywać według zasad właściwych dla odwołań od decyzji kończących postępowanie. Dotychczas obowiązujące rozwiązanie przewidywało co prawda – na podstawie ogólnego zapisu w art. 101 § 3 kpa – możliwość złożenia zażalenia na postanowienie o zawieszeniu postępowania, ale nie precyzowało, do kogo należy takie zażalenie składać.

W art. 28 określono formy zakończenia postępowania sprawdzającego, opisane dotychczas w art. 36 ust. 1-2 oraz 2b. W stosunku do poprzednio obowiązujących rozwiązań sprecyzowano, że decyzjami kończącymi postępowanie sprawdzające są nie tylko poświadczenie bezpieczeństwa oraz decyzja o odmowie wydania poświadczenia bezpieczeństwa, ale również decyzja o umorzeniu postępowania.

Art. 29 dotyczy poświadczeń bezpieczeństwa, okresów ważności oraz trybu i zasad ich wydawania i przekazywania, opisanych dotychczas w art. 33, art. 36 ust. 2-2a, ust. 3 pkt 1 oraz ust. 4, art. 37 ust. 7 oraz art. 40 ust. 3. W stosunku do poprzednio obowiązujących rozwiązań wskazano wprost, że poświadczenia bezpieczeństwa wydane w wyniku przeprowadzenia postępowań sprawdzających, o których mowa w art. 23 ust. 5 (czyli przez AW, SWW, CBA, Policję, ŻW, SG, SW oraz BOR), zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające. Do tej samej kwestii nawiązuje również art. 34 ust. 1 nowej ustawy, zgodnie z którym *nie przeprowadza się po-*

stępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku postępowań sprawdzających, o których mowa w art. 23 ust. 5.

Bardzo ważną zmianą, której wprowadzenie poprzedzono konsultacjami z instytucjami odpowiedzialnymi w UE i NATO za ochronę informacji niejawnych, jest wprowadzenie zasady „kaskadowej" ważności poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych. Dotychczas zasada ta była stosowana tylko w odniesieniu do poświadczeń upoważniających do dostępu do „krajowych" informacji niejawnych i to dopiero od nowelizacji z 2005 r.[8]. Tak więc obecnie wydane poświadczenie bezpieczeństwa, które będzie upoważniało do dostępu do informacji niejawnych o klauzuli *'Cosmic Top Secret'* na 5 lat, będzie jednocześnie upoważniało jego posiadacza do dostępu do informacji niejawnych o klauzuli *„NATO Secret"* przez kolejne 2 lata (7 lat od wydania poświadczenia), a o klauzuli *„NATO Confidential"* – jeszcze przez następne 3 lata (10 lat od wydania poświadczenia). Podobna zasada będzie obowiązywała w przypadku poświadczeń bezpieczeństwa Unii Europejskiej. Należy jednak mieć na uwadze to, że wprowadzenie zasady „kaskadowej" ważności poświadczeń upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych będzie dotyczyło tylko tych postępowań, które zostaną wszczęte po wejściu w życie nowej ustawy (o czym stanowi przepis przejściowy w art. 182).

W art. 30 określono decyzje o odmowie wydania poświadczeń bezpieczeństwa, w tym w szczególności prawnych i faktycznych podstaw decyzji oraz trybu i zasad jej wydawania i przekazywania, opisanych dotychczas w art. 36 ust. 2, ust. 3 pkt 2 oraz ust. 4-4a, art. 37 ust. 7-9, art. 40 ust. 3-4 oraz art. 41. W stosunku do poprzednio obowiązujących rozwiązań zmieniono zasady wyłączania dostępu do informacji niejawnych osobom sprawdzanym[9]. Oznacza to odejście od automatycznego uznawania, że osoba skazana, np. za jazdę rowerem będąc w stanie nietrzeźwości (art. 178a kk) albo ukarana za nieodprowadzanie składek ZUS za pracowników, nie daje rękojmi zachowania tajemnicy w zakresie dostępu do informacji niejawnych o klauzuli „tajne" i „ściśle tajne". Ustawodawca uznał bowiem, że skazanie prawomocnym wyrokiem za przestępstwo umyślne (sprecyzowano, że chodzi tu także o umyślne przestępstwo skarbowe), ścigane z oskarżenia publicznego, będzie stanowić podstawę do decyzji o odmowie wydania poświad-

[8] Wynikało to z art. 8 *Ustawy z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw* (Dz.U. z 2007 r., Nr 85, poz. 727).

[9] Jeżeli osoba ubiegała się o dostęp do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", fakt skazania prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego, stanowił bezwzględną przesłankę wyłączenia dostępu do informacji niejawnych; w przypadkach klauzul „poufne" i „zastrzeżone" była to jedynie przesłanka fakultatywna.

czenia bezpieczeństwa, ale tylko wówczas, gdy osoba sprawdzana została skazana na karę pozbawienia wolności (trudno uznać, aby sądy skazywały kogoś na taką karę za przestępstwa mniejszej wagi) – choćby wykonanie tej kary warunkowo zawieszono. Ponadto skazanie osoby sprawdzanej prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego będzie podstawą do odmowy tylko wówczas, gdy jednocześnie będzie ono wywoływać wątpliwości ustalane w toku postępowania (przy czym nie jest konieczne wykazanie, że wątpliwości te są niemożliwe do usunięcia).

Zmieniono również formułę dotyczącą zasad odstępowania od przekazywania przez organ prowadzący postępowanie faktycznego uzasadnienia decyzji o odmowie. W obecnym brzmieniu tego przepisu uzasadnienie faktyczne *podlega ochronie na zasadach określonych w ustawie*, co oznacza, że osoba nieposiadająca poświadczenia, nie będzie mogła się z nim zapoznać, czyli w praktyce będzie się odstępować od przekazywania takiego uzasadnienia (o ile będzie ono zawierać informacje niejawne).

Analogicznie jak w przypadku postanowień o zawieszeniu postępowania sprawdzającego, na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego zakończeniu decyzją o odmowie nie tylko wnioskodawcy, ale również pełnomocnika ochrony, o ile nie jest on organem, który wydał tę decyzję.

W art. 31 opisano zasady umarzania postępowań sprawdzających, zawarte dotychczas w art. 36 ust. 2b i 2d. W stosunku do poprzednio obowiązujących rozwiązań do nowej ustawy włączono treść art. 105 § 1 kpa mówiącego o tym, że postępowanie zostaje umorzone, gdy stało się bezprzedmiotowe (czyli np. w sytuacji, gdy wygasła właściwość organu do prowadzenia postępowania sprawdzającego). I analogicznie jak w przypadku postanowień o zawieszeniu postępowania sprawdzającego oraz zakończeniu postępowania decyzją o odmowie, na organ prowadzący postępowanie nałożono obowiązek poinformowania o jego umorzeniu nie tylko wnioskodawcy, ale również pełnomocnika ochrony (o ile oczywiście to sam pełnomocnik ochrony nie jest on organem, który umorzył to postępowanie). Ponadto sprecyzowano tryb składania odwołań od decyzji o umorzeniu postępowania sprawdzającego (analogicznie, jak w przypadku odwołań od decyzji o odmowie wydania poświadczenia bezpieczeństwa).

W art. 32 opisano kolejne postępowania sprawdzające, dotychczas określone w art. 44. W stosunku do poprzednio obowiązujących rozwiązań wprowadzono możliwość przeprowadzenia „uproszczonego" postępowania sprawdzającego wobec osoby ubiegającej się o wydanie poświadczenia bezpieczeństwa organizacji międzynarodowych, która posiada ważne poświadczenie „krajowe", wydane przez

ABW, SKW, AW lub SWW – nie ma wtedy konieczności wypełnienia ankiety, a poświadczenie upoważniające do dostępu do informacji niejawnych organizacji międzynarodowych wydaje się tylko na okres ważności poświadczenia „krajowego". Mimo że nie zapisano tego wprost, to dla przeprowadzenia tego typu kolejnego postępowania niezbędna jest pisemna zgoda osoby mającej być nim objętej (art. 24 ust. 9), co wynika ze zbiegu innych przepisów ustawy (art. 32 ust. 2, art. 24 ust. 8).

W art. 33 opisano kontrolne postępowania sprawdzające, dotychczas określone w art. 45-47. W stosunku do poprzednio obowiązujących rozwiązań usankcjonowano możliwość dokonania *wstępnych czynności weryfikacyjnych* jeszcze przed wszczęciem postępowania kontrolnego. Pełnomocnik ochrony może dokonać sprawdzeń w ewidencjach i kartotekach, a ABW, SKW, AW, SWW, CBA, Policja, ŻW, SW, SG oraz BOR – dodatkowo sprawdzeń w ewidencjach niedostępnych powszechnie. Czynności te należy rzetelnie dokumentować, a dokumentację włączyć do akt postępowania kontrolnego – jeśli zostanie wszczęte lub poprzedniego – jeżeli postępowanie kontrolne nie zostało wszczęte. Sprecyzowano ponadto, który organ jest właściwy do prowadzenia kontrolnego postępowania sprawdzającego – jest nim ten organ, który byłby właściwy – w momencie wszczęcia postępowania kontrolnego – do przeprowadzenia kolejnego postępowania sprawdzającego. Odstępstwem od tej reguły jest zapis, że w przypadkach uzasadnionych względami bezpieczeństwa państwa kontrolne postępowanie sprawdzające może zostać przeprowadzone przez ABW albo SKW, ale tylko wówczas, gdy osoba, wobec której ma być wszczęte postępowanie kontrolne, posiada poświadczenie wydane przez ABW lub SKW. Należy mieć również na względzie to, że jeżeli organ, który wszczął postępowanie kontrolne, utracił – w toku tego postępowania – właściwość do jego prowadzenia (np. SKW w przypadku żołnierza zwolnionego ze służby wojskowej posiadającego poświadczenie bezpieczeństwa wydane przez SKW lub WSI), to wówczas organ ten i tak musi zakończyć to postępowanie decyzją merytoryczną, tj. potwierdzeniem ważności poświadczenia bądź decyzją o jego cofnięciu, a nie umorzeniem z uwagi na bezprzedmiotowość. Powyższa interpretacja wynika wprost z orzeczeń organu odwoławczego.

Najważniejszą zmianą z punktu widzenia osoby sprawdzanej jest wprowadzenie zawitego terminu realizacji postępowania kontrolnego. Postępowanie kontrolne powinno się zakończyć po upływie 6 miesięcy, jednakże w szczególnie uzasadnionych przypadkach organ prowadzący to postępowanie jednorazowo może je przedłużyć o kolejne 6 miesięcy. Po upływie tego drugiego terminu, a więc po upływie roku od wszczęcia postępowania kontrolnego, jeżeli nie zostanie ono zakończone decyzją o cofnięciu poświadczenia bezpieczeństwa albo poinformowaniem o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem, kontrolne postępowanie sprawdzające musi zostać umorzone. Następna zmiana dotyczy trybu informowania o wszczęciu, przedłużeniu o kolejne

6 miesięcy oraz o zakończeniu postępowania kontrolnego – o tych faktach organ prowadzący postępowanie kontrolne będzie zobowiązany poinformować nie tylko kierownika jednostki organizacyjnej, w której jest zatrudniona osoba objęta takim postępowaniem, ale także samą osobę sprawdzaną oraz pełnomocnika ochrony. W przypadku gdy osoba mająca być objęta postępowaniem kontrolnym, nie jest nigdzie zatrudniona (lub jest zatrudniona bez dostępu do informacji niejawnych), nie ma obowiązku powiadamiania ani kierownika takiej jednostki organizacyjnej, ani tamtejszego pełnomocnika ochrony. Ponadto wyraźnie wskazano, że na potrzeby postępowania kontrolnego nie wypełnia się ankiety bezpieczeństwa osobowego. Wprowadzono również – m.in. ze względu na zmianę definicji informacji niejawnych – bezwzględną konieczność wyłączenia osoby, wobec której wszczęto kontrolne postępowanie sprawdzające, dostępu do informacji niejawnych (dotychczas była też możliwość jedynie ograniczenia tego dostępu).

W art. 34 opisano przypadki wyłączenia osób z konieczności poddania się postępowaniu sprawdzającemu, dotychczas opisane w art. 27 ust. 2-10, art. 28 ust. 2, art. 29a, art. 31 ust. 3 oraz w zawartym w rozdziale 6. (*Udostępnianie informacji niejawnych*) art. 49, a także w *Ustawie prawo o ustroju sądów powszechnych*[10]. W stosunku do poprzednio obowiązujących rozwiązań do katalogu osób, które wyłączone są z konieczności poddawania się jakimkolwiek postępowaniom sprawdzającym (prezydent, premier, marszałek sejmu i marszałek senatu), w tym prowadzonych w związku z koniecznością posiadania poświadczenia bezpieczeństwa organizacji międzynarodowych, dodano osobę wybraną na urząd prezydenta (prezydenta-elekta, tj. osobę ogłoszoną przez Państwową Komisję Wyborczą zwycięzcą wyborów prezydenckich, do momentu zaprzysiężenia przed Zgromadzeniem Narodowym, co trwa zwykle miesiąc). Natomiast do katalogu osób, które nie muszą poddawać się postępowaniom sprawdzającym przed uzyskaniem dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej, dodano ławników sądów powszechnych i wojskowych oraz asesorów prokuratury pełniących czynności prokuratorskie.[11] Sprecyzowano też, że postępowaniom sprawdzającym nie muszą się w takich przypadkach poddawać sędziowie sądów powszechnych i wojskowych, Sądu Najwyższego, sądów administracyjnych i Naczelnego Sądu Administracyjnego, a także Trybunału Stanu i Trybunału Konstytucyjnego (ale nadal wszyscy nie są oni zwolnieni z konieczności poddania się procedurom sprawdzającym, jeżeli zachodzi konieczność wydania im poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych).

---

[10] Na podstawie *Ustawy z dnia 27 lipca 2001 roku Prawo o ustroju sądów powszechnych* (Dz.U. z 2001 r., Nr 98, poz. 1070, z późn. zm.) z konieczności poddawania się procedurom sprawdzającym przed uzyskaniem dostępu do informacji niejawnych wyłączono sędziów (art. 85 § 4) i prokuratorów (art. 185 pkt 15).

[11] Na decyzję ustawodawcy w tej sprawie miała zapewne wpływ uchwała Sądu Najwyższego nr 1 KZP34/09 z dnia 24.02.2010 r., w której stwierdzono, iż przepisy dotyczące prowadzenia postępowań sprawdzających nie mają zastosowania do ławników sądów powszechnych.

Utrzymano, funkcjonującą wcześniej, 14-dniową procedurę sprawdzania przez ABW kandydatów na niektóre najważniejsze stanowiska w państwie, opartą wcześniej na standardach poszerzonego lub specjalnego postępowania sprawdzającego, ale w przypadku wniosków o przeprowadzenie takiej procedury (teraz nazwanej już wprost postępowaniem sprawdzającym, art. 34 ust. 13 nowej ustawy), ABW nie będzie – jak dotychczas – wydawała opinii (art. 27 ust. 7 starej ustawy), tylko poświadczenie bezpieczeństwa. Ponadto – oprócz istniejącego obowiązku informowania w ciągu 7 dni organu, który wydał poświadczenie bezpieczeństwa, o zatrudnieniu osoby posiadającej to poświadczenie na stanowisku związanym z dostępem do informacji niejawnych – wprowadzono obowiązek dodatkowego poinformowania także służby właściwej dla danej „sfery", po to, aby nie dochodziło do sytuacji, kiedy w sferze „cywilnej" zatrudniano osoby posiadające poświadczenie wydane przez SKW, a nadzorująca tę sferę ABW nie posiadałaby na ten temat żadnej wiedzy. Podobny mechanizm działa także w drugą stronę, tzn. jeżeli w MON zostanie zatrudniona osoba posiadająca poświadczenie wydane przez ABW, to informację o tym fakcie uzyska nie tylko ABW, ale również SKW (jako służba realizująca zadania z zakresu ochrony informacji niejawnych w MON). Z obowiązku informowania są zwolnieni szefowie AW, SWW, CBA, Policji, ŻW, SW, SG oraz BOR, którzy, w zakresie udostępniania informacji niejawnych swoim funkcjonariuszom, żołnierzom czy pracownikom, cieszą się daleko posuniętą autonomią (realizowanie „samodzielnych" postępowań sprawdzających).

W nowej ustawie sprecyzowano także tryb udostępniania informacji niejawnych osobom nieposiadającym poświadczenia bezpieczeństwa w stanach nadzwyczajnych. W takiej sytuacji to prezydent lub premier – tak jak dotychczas – wydają zgodę na udostępnienie informacji niejawnych, ale kopia takiej zgody musi być przekazana do ABW lub SKW. Obowiązek ten nie dotyczy sytuacji, gdy osoba ta ma uzyskać dostęp do informacji niejawnych w związku z zatrudnieniem lub wykonywaniem prac na rzecz ABW, SKW, AW, SWW, CBA, Policji, ŻW, SW, SG oraz BOR.

Bezpośrednio do zagadnień związanych z postępowaniami sprawdzającymi odnosi się również rozdział 6 ustawy, noszący nazwę *Postępowanie odwoławcze i skargowe, wznowienie postępowania*, funkcjonujący wcześniej (od nowelizacji z 2001 r.) jako rozdział 5a „*Postępowanie odwoławcze i skargowe*" (art. 48a-m).

W art. 35 odniesiono się do trybu i zasad składania odwołań do Prezesa Rady Ministrów, dotychczas opisanych w art. 48a-b. W stosunku do poprzednio obowiązujących rozwiązań sprecyzowano, że od wszystkich decyzji o odmowie wydania i cofnięcia poświadczenia bezpieczeństwa, będących rezultatem postępowań sprawdzających prowadzonych przez ABW, SKW, AW, SWW, CBA, Policję, ŻW, SW, SG oraz BOR (nawet, gdy będą to zwykłe postępowania sprawdza-

jące prowadzone przez pełnomocników ochrony w tych służbach lub ich jednostkach organizacyjnych), osobom sprawdzanym przysługuje odwołanie do premiera. Dodano również, że ten sam tryb odnosi się zarówno do odwołań od decyzji o umorzeniu postępowania, jak również zażaleń na postanowienie o zawieszeniu lub podjęciu zawieszonego postępowania sprawdzającego. Dodatkowo sprecyzowano, że wniesienie odwołania nie wstrzymuje wykonania decyzji.

W art. 36 opisano rozstrzygnięcia postępowań odwoławczych, dotychczas opisane w art. 48c-h. Poszerzono „katalog" możliwych rozstrzygnięć postępowania odwoławczego, dodając uchylenie decyzji o cofnięciu poświadczenia bezpieczeństwa, uchylenie decyzji i przekazanie sprawy do ponownego rozpatrzenia oraz stwierdzenie nieważności decyzji[12]. Ponadto wskazano, że zlecenie dodatkowych czynności w postępowaniu odwoławczym może dotyczyć ponownego przeprowadzenia specjalistycznych badań medycznych (pod kątem stwierdzenia występowania wątpliwości, związanych z chorobą lub dolegliwością psychiczną oraz uzależnieniem od alkoholu lub środków odurzających albo psychotropowych), które powinny być wykonane przez innego specjalistę niż w postępowaniu sprawdzającym.

W art. 37 odniesiono się do trybu i zasad składania odwołań do ABW lub SKW, dotychczas opisanych w art. 48i oraz art. 48m, a art. 38 nowej ustawy – do trybu i zasad składania skarg na decyzje organów odwoławczych i pierwszoinstancyjnych, dotychczas zawartych w art. 48j-ł. W opisie obu procedur wprowadzono jedynie zmiany o charakterze redakcyjnym.

Nowością w postępowaniach sprawdzających jest natomiast wprowadzenie instytucji wznowienia postępowania, co jest wynikiem zgłoszonego, na etapie prac legislacyjnych i konsultacji, postulatu włączenia do stosowania w ustawie rozdziału 12 kpa (art. 145-152). Ponieważ nie było możliwe zastosowanie przedmiotowych przepisów wprost, ustawodawca zdecydował się na rozwiązanie kompromisowe, opierając się na przepisach dotyczących wznowień postępowań administracyjnych. Taką możliwość wprowadzono do postępowań sprawdzających (i odwoławczych), ale zastosowano procedury właściwe dla specyfiki tych postępowań.

W art. 39 określono tryb i zasady wznawiania postępowań. Postępowanie wznawia się, jeżeli zostało ono zakończone odmową wydania (lub cofnięciem) poświadczenia bezpieczeństwa, której podstawą było skazanie osoby nim objętej bądź toczące się postępowanie karne wobec tej osoby, w sytuacji, gdy postępowanie karne zostało zakończone uniewinnieniem bądź umorzeniem. Postępowanie wznawia organ odwoławczy albo pierwszoinstancyjny (czyli ten, który prowadził

[12] Jest to w praktyce wpisanie wprost do ustawy niektórych przepisów kpa, m.in. z art. 138 i art. 156 – ten ostatni jest wpisany do art. 3 ustawy jako mający zastosowanie w postępowaniach sprawdzających.

postępowanie sprawdzające) z urzędu lub na wniosek zainteresowanej osoby. Taka konstrukcja przepisu (wznowienie postępowań zakończonych odmową/cofnięciem z uwagi na fakt toczącego się postępowania karnego) jest niezwykle istotna dla pragmatyki postępowań sprawdzających, ponieważ sankcjonuje, od dawna praktykowaną i wielokrotnie potwierdzoną rozstrzygnięciami organów odwoławczych oraz sądu administracyjnego, zasadę, że w szczególnych okolicznościach fakt toczącego się wobec osoby sprawdzanej postępowania karnego (a więc od momentu przedstawienia zarzutów do uprawomocnienia się wyroku sądu lub postanowienia prokuratury) może stanowić podstawę do zawieszenia nie tylko toczącego się postępowania, ale nawet decyzji o odmowie wydania bądź o cofnięciu poświadczenia bezpieczeństwa. Wynika to m.in. z art. 24 ust. 4, zgodnie z którym w przypadku występowania okoliczności wywołujących ustawowe wątpliwości w zakresie dawania rękojmi zachowania tajemnicy, interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami. Dostęp do informacji niejawnych nie jest bowiem traktowany w kategoriach prawa obywatelskiego, a postępowanie sprawdzające nie jest postępowaniem karnym, gdzie obowiązuje zasada *in dubio pro reo* (wątpliwości niedających się rozstrzygnąć, nie można tłumaczyć na niekorzyść oskarżonego – przyp. red.).

W praktyce więc ustalone w toku postępowania sprawdzającego wątpliwości dotyczące osoby sprawdzanej muszą być – przez wzgląd na pierwszeństwo interesu ochrony informacji niejawnych – rozstrzygnięte na korzyść tego interesu, a nie na korzyść osoby objętej postępowaniem sprawdzającym. Oczywiście organ prowadzący postępowanie musi wykazać, że wątpliwości te nie są jedynie nieuprawnioną, niepotwierdzononą lub niemającą perspektyw urzeczywistnienia hipotezą, a mają oparcie w konkretnym materiale zgromadzonym w toku postępowania sprawdzającego. Z dotychczasowej praktyki wynika, że przedstawienie osobie sprawdzanej zarzutu popełnienia przestępstwa może być wystarczającą podstawą do stwierdzenia, że taka osoba nie daje rękojmi zachowania tajemnicy (oczywiście dotyczy to tylko niektórej kategorii przestępstw, np. tych o charakterze hańbiącym czy zagrożonych wysoką karą). Wprowadzona nową ustawą instytucja wznowienia postępowania sprawdzającego − w przypadku uniewinnienia osoby w procesie karnym bądź umorzenia postępowania karnego − zapewni jej prawo ponownej, rzetelnej oceny dawania rękojmi zachowania tajemnicy w sytuacji istotnej zmiany okoliczności faktycznych (w praktyce − zniknięcia przesłanek negatywnie wpływających na tę ocenę).

Wniosek o wznowienie postępowania wnosi się do organu pierwszoinstancyjnego w terminie 30 dni od dowiedzenia się o okoliczności stanowiącej podstawę wznowienia (w przypadku uchybienia tego terminu organ w drodze postanowienia stwierdza to uchybienie, które jest ostateczne, ale można je zaskarżyć do sądu administracyjnego), a jego rozpatrzenie powinno nastąpić w terminie 3 miesięcy

od otrzymania wniosku. Wznowienie postępowania następuje w drodze postanowienia, a jego odmowa – w drodze decyzji, od której można się odwołać na zasadach przewidzianych dla odwołania od decyzji o odmowie wydania poświadczenia bezpieczeństwa.

W art. 40 określono rozstrzygnięcia zapadłe w wyniku wznowienia postępowania. Wznowione postępowanie może zostać zakończone: 1) odmową uchylenia pierwotnej decyzji; 2) uchyleniem pierwotnej decyzji i wydaniem nowej decyzji; 3) uchyleniem pierwotnej decyzji i przekazaniem sprawy do ponownego rozpatrzenia; 4) uchyleniem pierwotnej decyzji o cofnięciu poświadczenia i (lub) o utrzymaniu w mocy cofnięcia.

W art. 41 ustawodawca odniósł się do odwołań od rozstrzygnięć zapadłych w wyniku wznowienia postępowania. Zasady odwołań są identyczne jak w przypadku odmowy, o ile wznowione postępowanie było prowadzone przez organ pierwszoinstancyjny – o właściwości organu do rozpatrzenia odwołania decyduje to, który organ pierwszoinstancyjny wydał decyzję: jeżeli były to ABW, SKW, AW, SWW, CBA, Policja, ŻW, SW, SG oraz BOR, w tym pełnomocnicy ochrony w tych instytucjach – to odwołanie wnosi się do premiera, a jeżeli był to pełnomocnik ochrony spoza tych instytucji – odwołanie wnosi się do Szefa, odpowiednio, ABW lub SKW. Jeżeli natomiast postępowanie zostało wznowione na etapie postępowania odwoławczego (czyli prowadził je organ drugoinstancyjny, tj. Prezes Rady Ministrów − w przypadku piewrszoinstancyjnych decyzji wydanych przez ABW, SKW, AW, SWW, CBA, Policję, ŻW, SW, SG oraz BOR − albo Szef ABW lub Szef SKW w przypadku pierwszoinstancyjnych decyzji wydanych przez pełnomocników ochrony, z wyjątkiem pełnomocników we wskazanych wyżej instytucjach) – to od takiej decyzji nie można się odwołać, ale *osoba niezadowolona z decyzji* może zwrócić się do organu, który wydał decyzję we wznowionym postępowaniu odwoławczym, o ponowne rozpatrzenie sprawy.

Zagadnienia dotyczące archiwizowania i udostępnia akt oraz danych z ewidencji postępowań sprawdzających, opisane dotychczas w rozdziale *Bezpieczeństwo osobowe* − art. 42 ust. 2-8, wyodrębniono w osobny rozdział 10 (*Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego*) m.in. z uwagi na to, że przepisy te odnoszą się nie tylko do akt postępowań sprawdzających prowadzonych wobec osób, ale również do archiwizowania i udostępniania akt postępowań bezpieczeństwa przemysłowego.

Najbardziej obszernym rozdziałem ustawy jest rozdział 11 zatytułowany *Zmiany w przepisach obowiązujących*. Generalną ideą zmian, dotyczących prowadzenia postępowań sprawdzających, było jednoznaczne nadanie dotychczaso-

wych uprawnień służb ochrony państwa (ABW i SKW) wszystkim służbom i organom uprawnionym do prowadzenia samodzielnych postępowań sprawdzających, tj. AW, SWW, CBA, Policji, ŻW, SG, SW oraz BOR, przede wszystkim związanych z prawem do występowania o przekazanie niezbędnych informacji i udostępnienie dokumentów[13].

Niezwykle ważne dla zagadnień związanych z bezpieczeństwem osobowym regulacje znajdują się w ostatnim rozdziale nowej ustawy (*Przepisy przejściowe i końcowe*). W art. 182 wskazano, że poświadczenia bezpieczeństwa wydane na podstawie dotychczasowych przepisów (tj. *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*) zachowują ważność przez okres wskazany w tych przepisach. Oznacza to, że dla poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych organizacji międzynarodowych, wydanych przed wejściem w życie nowej ustawy, nie będzie obowiązywała „kaskada" ważności. Jest to odmienne uregulowanie kwestii związanych z okresem przejściowym w stosunku do nowelizacji starej ustawy, dokonanej w 2005 r., gdzie uznano, że poświadczenia bezpieczeństwa wydane przed dniem wejścia w życie ustawy, ważne w tym dniu, zachowują ważność w zakresie i okresie określonym ustawą z 22 stycznia 1999 r., w brzmieniu nadanym znowelizowaną ustawą.[14]

Również odmiennie niż w 2005 r. w art. 188 uregulowano kwestię stosowania nowych przepisów do postępowań rozpoczętych przed wejściem w życie obecnie obowiązującej ustawy[15]. Obecnie przyjęto rozwiązanie, że do tych postępowań będą stosowane przepisy dotychczasowe, co oznacza, że przez pewien okres przejściowy (do momentu zakończenia postępowań sprawdzających wszczętych przed wejściem w życie nowej ustawy) w postępowaniach sprawdzających stosowane będą podwójne standardy, przede wszystkim co do zakresu i czynności sprawdzających oraz podstaw decyzji o odmowie wydania poświadczenia bezpie-

[13] Dotyczy to następujących ustaw: 1) *Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa* (Dz.U. z 2005 r., Nr 8, poz. 60 z późn. zm.) – art. 119 pkt. 8 i 9 nowej ustawy, zmieniające odpowiednio art. 297 w § 1 pkt 7 oraz art. 298 pkt 5a ustawy Ordynacja Podatkowa; 2) *Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe* (Dz.U. z 2002 r., Nr 72, poz. 665 z późn. zm.) – art. 120 pkt 1 i 2 nowej ustawy, zmieniające odpowiednio w art. 105 w ust. 1 w pkt 2 lit. k oraz art. 110 pkt 6 ustawy Prawo bankowe; 3) *Ustawa z dnia 26 października 2000 r. o giełdach towarowych* (Dz.U. z 2010 r., Nr 48, poz. 284 z późn. zm.) – art. 128 nowej ustawy, zmieniający w art. 54 w ust. 1 pkt 6 ustawy o giełdach towarowych; 4) *Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych* (Dz.U. z 2004 r., Nr 146, poz. 1546 z późn. zm.) – art. 153 nowej ustawy, zmieniający w art. 281 w ust. 1 pkt 8 ustawy o funduszach inwestycyjnych; oraz 5) *Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi* (Dz.U. z 2005 r., Nr 183, poz. 1538 z późn. zm.) – art. 162 nowej ustawy, zmieniający w art. 149 pkt 7 ustawy o obrocie instrumentami finansowymi.

[14] Tej kwesti dotyczył art. 8 *Ustawy z 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw* (Dz.U. z 2005 r., Nr 85, poz. 727).

[15] Tej kwesti dotyczył art. 7 *Ustawy z 15 kwietnia 2005 r. o zmianie ustawy...* : *Do postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy tej ustawy.*

czeństwa. Dotychczasowe przepisy wykonawcze będą obowiązywać do momentu wydania nowych rozporządzeń, jednak nie dłużej niż 12 miesięcy (art. 189). Z uwagi na wejście w życie z dniem 2 stycznia 2011 r. nowych rozporządzeń (określających wzory decyzji o odmowie wydania poświadczenia bezpieczeństwa[16] oraz o cofnięciu poświadczenia bezpieczeństwa[17]), w przypadku decyzji wydawanych wobec postępowań wszczętych przed 2 stycznia 2011 r. wydawane są decyzje oparte na wzorach określonych już w nowych rozporządzeniach, ale z powołaniem się na art. 188 ustawy oraz przepisy poprzedniej ustawy. Podobne standardy należy stosować w przypadku decyzji o umorzeniu postępowania sprawdzającego czy postanowieniu o zawieszeniu postępowania sprawdzającego (ustawa nie narzuca obowiązującego wzoru takich decyzji czy postanowień).

Integralną częścią ustawy (jako załącznik do niej) pozostaje wzór ankiety bezpieczeństwa osobowego. Dokładny opis wprowadzonych zmian w ankiecie bezpieczeństwa znajduje sie w artykule pt. *Najważniejsze zmiany w systemie ochrony informacji niejawnych wprowadzone przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,* zamieszczonym w niniejszym poradniku.

[16] *Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa* (Dz.U. z 2010 r., Nr 258, poz. 1753).

[17] *Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa* (Dz.U. z 2010 r. Nr 258, poz. 1754).

Barbara Dobroń

Bezpieczeństwo przemysłowe w kontekście przepisów nowej ustawy o ochronie informacji niejawnych

W dniu 2 stycznia 2011 r. weszła w życie *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, która zastąpiła obowiązujące dotychczas przepisy, tj. ustawę z dnia 22 stycznia 1999 r. (Dz.U. z 2005 r., Nr 196, poz. 1631 z późn. zm.).

Jedną z kwestii, która w sposób zasadniczy wpłynęła na funkcjonowanie na rynku przedsiębiorców jest zmiana odnosząca się do bezpieczeństwa przemysłowego.

Nowa ustawa ogranicza właściwość Służby Kontrwywiadu Wojskowego co do postępowań bezpieczeństwa przemysłowego. Oznacza to, że obecnie SKW realizuje zadania wynikające z przepisów ustawy wyłącznie wobec Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, ataszatów obrony w placówkach zagranicznych oraz żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione powyżej. Zapis ten nie obejmuje jednak wykonawców lub podwykonawców umów zlecanych przez te jednostki.

W pozostałych przypadkach odpowiedzialność za realizację zadań związanych z przeprowadzaniem postępowań bezpieczeństwa przemysłowego spoczywa na Agencji Bezpieczeństwa Wewnętrznego.

Nowa ustawa znosi również dotychczasowy podział na dwie krajowe władze bezpieczeństwa, tj. ABW i SKW, realizujące swoje zadania odpowiednio w sferze cywilnej i wojskowej. Obecnie funkcję krajowej władzy bezpieczeństwa pełni Szef ABW. Jednak w odniesieniu do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych MON lub przez nie nadzorowanych, Szef ABW pełni tę funkcję za pośrednictwem Szefa SKW. Powyższe zapisy oznaczają zarówno poszerzenie uprawnień ABW w odniesieniu do postępowań bezpieczeństwa przemysłowego prowadzonych w celu wydania świadectw bezpieczeństwa przemysłowego Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej oraz innych organizacji międzynarodowych, jak również realizowanie innych zadań krajowej władzy bezpieczeństwa, np. udzielanie zgody na złożenie wizyty międzynarodowej, przedsiębiorcom, którzy nie są nadzorowani przez MON, ale realizują na jego rzecz zadania.

Analiza zapisów zawartych w nowej ustawie wskazuje na ich większe doprecyzowanie w stosunku do poprzedniej ustawy, co wydaje się swego rodzaju wyjściem naprzeciw oczekiwań przedsiębiorców. Jednakże zakres podmiotowy pozostał bez zmian, wystarczy bowiem sam zamiar ubiegania się, ubieganie się lub faktyczna realizacja umów, bądź wynikających z przepisów prawa zadań związanych z dostępem do informacji niejawnych, aby przepisy niniejszej ustawy miały zastosowanie wobec tej kategorii podmiotów.

Warto podkreślić, że doprecyzowanie pojęcia przedsiębiorcy – czego poprzednio brakowało – pozwala jednoznacznie określić kategorie podmiotów, które podlegają przepisom ustawy w części dotyczącej bezpieczeństwa przemysłowego. Zgodnie z tą definicją przedsiębiorcą jest nie tylko podmiot określony w ustawie o swobodzie działalności gospodarczej, ale także inne jednostki organizacyjne prowadzące działalność gospodarczą, np. spółdzielnie mieszkaniowe, instytuty badawcze, które realizują umowy związane z dostępem do informacji niejawnych.

Dotychczasowy brak definicji kierownika jednostki organizacyjnej (w przepisach nowej ustawy jest to kierownik przedsiębiorcy) w przypadku postępowania bezpieczeństwa przemysłowego powodował istotne problemy interpretacyjne co do odpowiedzialności za ochronę informacji niejawnych, zwłaszcza dotyczące kolegialnych organów zarządzających lub kierujących sprawami podmiotu (zarząd, wspólnicy, pełnomocnicy). Doprecyzowanie tego terminu, z uwzględnieniem różnych form prawnych prowadzenia działalności gospodarczej występujących na obszarze RP, ułatwia stosowanie w praktyce przepisów ustawy w tym zakresie. Reguluje również tak istotną kwestię, jak odpowiedzialność za ochronę informacji niejawnych w przypadku ogłoszenia upadłości lub likwidacji przedsiębiorcy.

Ponadto na uwagę zasługuje fakt, że definicja nie obejmuje wszelkiego rodzaju pełnomocników ustanowionych przez osoby lub organy zarządzające (a zatem również i prokurentów, którzy poprzednio niejednokrotnie pełnili funkcję kierownika jednostki organizacyjnej), w przypadku których występowały wątpliwości co do ich faktycznego wpływu na ochronę informacji niejawnych z uwagi na tryb ich powoływania i odwoływania oraz ograniczoną odpowiedzialność, w tym karną, za naruszenie przepisów.

Nowe przepisy odstępują także od podziału informacji niejawnych na tajemnicę służbową i państwową, nadając jednocześnie nieco wyższą rangę klauzuli „poufne" (jest to m.in. konsekwencja ograniczenia ilościowego informacji niejawnych, które mogą być oznaczane klauzulami „tajne" lub „ściśle tajne"). Dlatego też obowiązek uzyskania świadectwa bezpieczeństwa przemysłowego dotyczy

obecnie także podmiotów zamierzających realizować umowy związane z dostępem do informacji niejawnych oznaczonych klauzulą „poufne". Jest to rozwiązanie analogiczne do uregulowań stosowanych przez NATO oraz Unię Europejską. A zatem wydawanie świadectw tych organizacji do poziomu *Confidential* nie jest już traktowane jako swego rodzaju wyjątek od stosowanych zasad.

Kolejną zmianą, jaka pojawiła się w nowych przepisach, jest odstąpienie od wymogu posiadania świadectwa bezpieczeństwa przemysłowego przez osoby fizyczne, prowadzące działalność gospodarczą jednoosobowo i osobiście – przedsiębiorca jest zobowiązany poddać się postępowaniu sprawdzającemu prowadzonemu przez ABW, zmierzającemu do wydania poświadczenia bezpieczeństwa, oraz do udziału w zorganizowanym przez te służby przeszkoleniu w zakresie ochrony informacji niejawnych. Wyjątek stanowią sytuacje, kiedy obowiązek wydania świadectwa bezpieczeństwa przemysłowego wynika z przepisów międzynarodowych – zapis taki umożliwia elastyczne dostosowywanie się do kryteriów zawartych w umowach bilateralnych lub przepisach organizacji międzynarodowych, jeżeli bowiem bezwzględnie wymagane jest posiadanie świadectwa bezpieczeństwa przemysłowego przez każdego przedsiębiorcę, ABW lub SKW przeprowadzają takie postępowanie, jeżeli zaś takiego wymagania nie ma – wystarczające jest przeprowadzenie postępowania zmierzającego do wydania poświadczenia bezpieczeństwa przez ABW.

Pewną wątpliwość może budzić zastosowanie określenia przedsiębiorca wykonujący działalność jednoosobowo i osobiście. *Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej* (Dz.U. z 2010 r., Nr 220, poz. 1447 ze zm.) w art. 4 definiuje przedsiębiorcę m.in. jako *osobę fizyczną* (…) *wykonującą we własnym imieniu działalność gospodarczą*, ale definicja ta obejmuje także osoby prowadzące działalność gospodarczą w formie dużych przedsiębiorstw o rozbudowanej strukturze organizacyjnej i kadrowej, wobec których zasadne jest przeprowadzenie postępowania bezpieczeństwa przemysłowego. Dlatego ustawodawca celowo doprecyzował, że powyższy przepis dotyczy wyłącznie tych osób fizycznych prowadzących działalność gospodarczą, które nie zatrudniają żadnych pracowników (jednoosobowo) i nie prowadzą działalności poprzez ustanowionych pełnomocników lub osoby trzecie (osobiście).

Według obecnych przepisów obowiązek posiadania świadectwa bezpieczeństwa przemysłowego dotyczy przedsiębiorców mających uzyskać dostęp do informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą, natomiast nie wydaje się świadectw do poziomu „zastrzeżone". Przedsiębiorca uzyskujący dostęp do informacji oznaczonych klauzulą „zastrzeżone" jest zobowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych oznaczonych tą klauzulą, ale nie jest zobowiązany do powoływania pełnomocnika ochrony, jeże-

li będzie uzyskiwał dostęp do informacji niejawnych na terenie obiektów jednostki zlecającej. Poprzednio każdy przedsiębiorca uzyskujący dostęp do informacji niejawnych zobowiązany był do powołania pełnomocnika.

Przepisy nowej ustawy pozostawiają bez zmian trzy stopnie świadectw bezpieczeństwa przemysłowego. Przeredagowano (skrócono) definicje każdego ze stopni, ponieważ definicje przedsiębiorcy, przetwarzania informacji niejawnych oraz systemów teleinformatycznych zostały zawarte w art. 2. Nowością jest natomiast przyjęcie funkcjonującego w postępowaniach osobowych modelu „kaskadowej" ważności uprawnień w zakresie ochrony informacji niejawnych. Ważność świadectwa bezpieczeństwa przemysłowego potwierdzającego zdolność do ochrony informacji niejawnych oznaczonych wyższą klauzulą jest odpowiednio dłuższa dla klauzul niższych. Poprzednie przepisy obligowały przedsiębiorcę do ponownego ubiegania się o świadectwo bezpieczeństwa przemysłowego po upływie daty ważności określonej w tymże świadectwie, nawet jeżeli zostało ono wydane do klauzuli „ściśle tajne", a podmiot nie zamierzał realizować umów o klauzuli wyższej niż „tajne". Obecnie przedsiębiorca nie musi występować z kolejnym wnioskiem o wydanie świadectwa przez następne 2 lata dla klauzuli „tajne" lub 5 lat dla klauzuli „poufne".

Obowiązująca ustawa określa wprost, że w przypadku przedsiębiorców zamierzających uzyskać dostęp do informacji niejawnych organizacji międzynarodowych (np. NATO, Unia Europejska), oznaczonych odpowiednikiem klauzuli „poufne" lub „tajne", wydawane są odrębne świadectwa, jednak na takich samych wzorach jak w przypadku świadectw „krajowych". Poprzednie przepisy przewidywały odrębne wzory świadectw potwierdzających zdolność do ochrony informacji niejawnych Unii Europejskiej oraz NATO.

Tryb wnioskowania o wydanie świadectwa bezpieczeństwa przemysłowego nie uległ zasadniczej zmianie. Wniosek składa we własnym imieniu przedsiębiorca. W obecnych przepisach określono wprost, że wniosek nie musi zawierać uzasadnienia.

Ważną zmianą jest wprowadzenie 30-dniowego terminu usunięcia braków formalnych we wniosku. Powyższy termin jest dłuższy niż określony w kodeksie postępowania administracyjnego (7 dni), dzięki czemu przedsiębiorca wnioskujący o wszczęcie postępowania bezpieczeństwa przemysłowego ma więcej czasu na przekazanie brakujących danych.

Zapis art. 56 ust. 3 wskazuje na wymóg przekazywania wraz z wnioskiem ankiet bezpieczeństwa osobowego lub kopii poświadczeń osób wymienionych w art. 57 ust. 3. Podkreślenia jednak wymaga fakt, iż przepis ten nie odnosi się

do wszystkich pracowników przedsiębiorcy mających uzyskać dostęp do informacji niejawnych oznaczonych klauzulą „poufne", ponieważ z kolei artykuł 23 ust. 1 stanowi, że zwykłe postępowanie sprawdzające wobec pracowników przedsiębiorcy przeprowadza pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej. Wyjątek stanowią postępowania wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska, a także kierownika przedsiębiorcy, u którego są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, jak również wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską. Osoby te są zobowiązane do wypełnienia ankiety bezpieczeństwa osobowego w sposób przewidziany dla postępowań poszerzonych.

Uzasadnione zatem jest uznanie art. 22 ust. 1 oraz art. 23 jako nadrzędnych regulacji dotyczących zwykłych postępowań sprawdzających w bezpieczeństwie przemysłowym i wyłączenie pracowników przedsiębiorcy zamierzających uzyskać dostęp do informacji niejawnych oznaczonych klauzulą „poufne" z katalogu osób zobowiązanych do przekazywania ankiet bezpieczeństwa osobowego.

Powyższe zapisy dowodzą, że nowa ustawa wskazuje jednoznacznie na fakt, iż postępowanie bezpieczeństwa przemysłowego to nie tylko sprawdzenia przedsiębiorcy, ale również postępowania sprawdzające wobec osób objętych wnioskiem.

Katalog osób, wobec których przeprowadza się postępowania sprawdzające, również uległ zmianom, dodano bowiem pełnomocnika ochrony oraz jego zastępcę (poprzednio traktowanych jako osoby zatrudnione w pionie ochrony). Zrezygnowano natomiast z dość nieczytelnego rozróżnienia na osoby uczestniczące w czynnościach zmierzających do zawarcia umowy oraz osoby mające kierować wykonaniem umowy lub zadania albo uczestniczyć w ich bezpośredniej realizacji. Zamiast tych dwóch kategorii osób pojawił się ogólny zapis wskazujący inne osoby wymienione w kwestionariuszu bezpieczeństwa przemysłowego, które powinny mieć dostęp do informacji niejawnych. Natomiast w trakcie postępowania bezpieczeństwa przemysłowego oraz po wydaniu świadectwa wpływające wnioski o wszczęcie postępowania sprawdzającego należy traktować jako informację uzupełniającą kwestionariusz bezpieczeństwa przemysłowego, zważywszy na to, że postępowania sprawdzające przeprowadza się nie tylko w trakcie postępowania bezpieczeństwa przemysłowego, lecz także w okresie ważności świadectwa (poprzednie przepisy stanowiły, że postępowania sprawdzające prowadzone są tylko w ramach postępowania bezpieczeństwa przemysłowego).

Ponadto sprecyzowano przepis, kiedy przeprowadzane jest postępowanie, jeżeli osoba nie posiada poświadczenia bezpieczeństwa albo upływa okres ważności tego poświadczenia.

Podkreślenia wymaga również zmiana polegająca na określeniu klauzuli tajności umieszczonej w poświadczeniu bezpieczeństwa, które posiadają lub o które ubiegają się osoby pełniące funkcje związane z ochroną informacji niejawnych (kierownik przedsiębiorcy, pełnomocnik ochrony i jego zastępca, kierownik kancelarii tajnej, administrator systemu, inspektor bezpieczeństwa teleinformatycznego) – nie może być ona niższa od klauzuli tajności określonej w świadectwie bezpieczeństwa przemysłowego.

Z rozdziału dotyczącego bezpieczeństwa przemysłowego usunięto przepis dotyczący obywatelstwa osób, wobec których prowadzane są postępowania sprawdzające. Regulacje w tym zakresie pojawiają się w art. 21 ust. 2-3, zgodnie z którym nie mogą być dopuszczone do pracy lub pełnienia służby na stanowiskach albo wykonywania czynności zleconych, z którymi łączy się dostęp do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" osoby nieposiadające obywatelstwa polskiego, z wyjątkiem:

- zajmujących stanowiska związane z kierowaniem wykonywania przez przedsiębiorcę umowy, związanej z dostępem do informacji niejawnych, lub związane z bezpośrednim wykonywaniem takiej umowy albo wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa, związane z dostępem do informacji niejawnych u przedsiębiorcy,
- które w imieniu przedsiębiorcy, o którym mowa w pkt 1, uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli czynności te są związane z dostępem do informacji niejawnych,
- zatrudnionych w pionie ochrony przedsiębiorcy, z wyjątkiem osoby zajmującej stanowisko pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony.

Wymóg posiadania obywatelstwa polskiego nie dotyczy informacji niejawnych oznaczonych klauzulą do poziomu „poufne", a w przypadku klauzul „tajne" lub „ściśle tajne" nie dotyczy pracowników przedsiębiorcy, osób wchodzących w skład organów zarządzających (w tym kierowników przedsiębiorcy) pionu ochrony, z wyjątkiem pełnomocnika ochrony oraz zastępcy pełnomocnika ochrony. Innymi słowy, w ramach postępowania bezpieczeństwa przemysłowego ABW lub SKW uprawniona jest do prowadzenia postępowań sprawdzających wobec cudzoziemców.

Odmiennie niż w przypadku poprzednich przepisów obecna ustawa wprowadza regulacje dotyczące wydawania zgody na udostępnienie informacji niejawnych bezpośrednio w rozdziale dotyczącym bezpieczeństwa przemysłowego.

W przypadku sprawdzeń, jakim podlega przedsiębiorca w toku postępowania bezpieczeństwa przemysłowego, w nowych przepisach (art. 57 ust. 2) dokonano zmian polegających na połączeniu w jeden punkt sprawdzeń struktury kapitału, powiązań kapitałowych przedsiębiorcy oraz źródeł pochodzenia środków finansowych i sytuacji finansowej. Zmianie uległ także punkt dotyczący sprawdzeń osób wchodzących w skład organów zarządzających albo kontrolnych oraz osób działających z ich upoważnienia, uściślając, że chodzi o każdą z tych osób.

Ponadto dodatkowy punkt, zezwalający na sprawdzenia osób posiadających poświadczenia bezpieczeństwa, umożliwia realizację sprawdzeń np. wobec osób zasiadających w zarządzie bądź wchodzących w skład pionu ochrony, które posiadają ważne, ale wydane jakiś czas temu poświadczenia bezpieczeństwa. Rozwiązanie takie wydaje się ze wszech miar racjonalne, ponieważ daje możliwość uzyskania informacji mogących mieć wpływ na zdolność podmiotu do ochrony informacji niejawnych.

Istotną zmianą jest również uwzględnienie możliwości prowadzenia sprawdzeń na podstawie informacji innych niż dane zawarte w kwestionariuszu bezpieczeństwa przemysłowego. Tym samym prawnie usankcjonowane są sprawdzenia oparte np. na informacjach uzyskanych ze źródeł otwartych, które mogą mieć znaczenie z punktu widzenia oceny zdolności podmiotu do ochrony informacji niejawnych (np. informacje mogące wskazywać na pogorszenie się sytuacji finansowej podmiotu, powstanie zobowiązań finansowych, wszczęcie postępowań karnych). Także punkt dotyczący sytuacji finansowej został uzupełniony o źródła pochodzenia środków finansowych.

Rozszerzeniu uległ także wykaz pracowników posiadających poświadczenia bezpieczeństwa, co oznacza, że w kwestionariuszu należy wskazać wszystkie osoby posiadające poświadczenia bezpieczeństwa, bez względu na określoną w nich klauzulę tajności.

Ponadto katalog instytucji, do których ABW i SKW mogą zwracać się z prośbą o udzielenie niezbędnej pomocy w związku z prowadzonymi postępowaniami bezpieczeństwa przemysłowego ma formę otwartą, a zatem w uzasadnionych przypadkach służba prowadząca postępowanie może kierować pytania do dowolnej instytucji lub organu.

Termin na przeprowadzenie czynności w ramach postępowania bezpieczeństwa przemysłowego nie uległ zmianie. Zmiana polegająca na usunięciu fragmentu wskazującego, że postępowanie powinno być przeprowadzone bez zbędnej zwłoki, nie oznacza, że służba przeprowadzająca postępowanie ma w tym zakresie swobodę – w tym przypadku, zgodnie z art. 3 ustawy, stosowany jest art. 12 kpa, zgodnie z którym organy administracji publicznej powinny działać w sprawie wnikliwie i szybko, posługując się możliwie najprostszymi środkami prowadzącymi do jej załatwienia, a sprawy, które nie wymagają zbierania dowodów, informacji lub wyjaśnień, powinny być załatwione niezwłocznie.

Realizacja powyższych czynności może zostać poddana kontroli w celu oceny prawidłowości ich prowadzenia. Kontrolę taką może zarządzić Prezes Rady Ministrów.

W poprzednich przepisach brakowało odrębnych regulacji dotyczących przedsiębiorców ubiegających się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia w zakresie obowiązku powoływania pełnomocnika ochrony oraz przeprowadzania postępowań sprawdzających i szkolenia pracowników przedsiębiorcy. Obecne przepisy, dotyczące wskazanego zagadnienia, stanowią istotną zmianę w stosunku do zapisów ustawy w jej poprzednim brzmieniu. Przedsiębiorca ubiegający się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia – który nie będzie przetwarzał informacji niejawnych we własnych obiektach – nie musi powoływać pełnomocnika ochrony ani tworzyć pionu ochrony. Wyjątkiem jest ubieganie się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych organizacji międzynarodowych (NATO, Unia Europejska).

Powyższe rozwiązanie jest korzystne dla przedsiębiorcy, który poniesie mniejsze koszty związane z ubieganiem się o wydanie świadectwa.

Obowiązujące przepisy umożliwiają przeprowadzanie, przez pełnomocników ochrony jednostek zlecających wykonanie umów, postępowań sprawdzających do poziomu „poufne", wobec pracowników przedsiębiorcy posiadającego świadectwo trzeciego stopnia oraz szkolenie tych osób w zakresie ochrony informacji niejawnych.

Poprzednio możliwość przeprowadzenia postępowań sprawdzających przez pełnomocnika ochrony jednostki zlecającej umowę dotyczyła tylko okresu poprzedzającego rozpoczęcie faktycznej realizacji umowy przez przedsiębiorcę (zamiar ubiegania się lub ubieganie się o realizację umowy). Zgodnie z przepisami obecnej ustawy możliwość ta istnieje na każdym etapie działań związanych z umową, począwszy od momentu jej podpisania lub podpisania wstępnego porozumienia o jej zawarciu, do zakończenia jej realizacji.

Nowe przepisy utrzymują zasadę odpłatności za podejmowane przez ABW lub SKW czynności, tj. prowadzenie postępowania bezpieczeństwa przemysłowego oraz poszerzonych postępowań sprawdzających wobec osób – pracowników podmiotu sprawdzanego lub posiadającego ważne świadectwo bezpieczeństwa przemysłowego. Obecne przepisy szczególnie akcentują związek tej odpłatności z kosztami ponoszonymi przez ABW lub SKW za przeprowadzenie czynności w ramach postępowań sprawdzających – termin *opłata* zastąpiono terminem *zwrot zryczałtowanych kosztów.*

Ważną zmianą jest wskazanie, iż odpłatności nie podlegają postępowania wobec osób posiadających ważne poświadczenia bezpieczeństwa, wydane przez ABW lub SKW, wobec których skierowano wniosek o przeprowadzenie postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej. W tego rodzaju sytuacji wydawane jest poświadczenie bezpieczeństwa na okres ważności posiadanego przez tę osobę „krajowego" poświadczenia bezpieczeństwa.

Opłacie nie podlega również postępowanie kontrolne wszczynane po stwierdzeniu faktów mogących wskazywać na to, że osoba posiadająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy.

Zgodnie z obowiązującymi przepisami ABW przeprowadza szkolenie w zakresie ochrony informacji niejawnych nie tylko wobec pełnomocników ochrony i ich zastępców, ale także wobec osób fizycznych prowadzących jednoosobowo działalność gospodarczą, kierowników przedsiębiorcy, który nie powołał pełnomocnika ochrony oraz – wspólnie z pełnomocnikiem ochrony – wobec kierownika jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „ściśle tajne" lub „tajne".

Wprowadzenie nowych regulacji skutkuje obecnie zmianami w takich kwestiach, jak umorzenie i zawieszenie postępowania bezpieczeństwa przemysłowego oraz odmowa wydania i cofnięcie świadectwa bezpieczeństwa przemysłowego.

Poprzednie przepisy umożliwiały umorzenie postępowania sprawdzającego w przypadku skierowania wniosku o jego umorzenie przez podmiot, który wystąpił z wnioskiem o wszczęcie tego postępowania (art. 105 § 2 kpa) oraz w przypadku, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe (art. 105 § 1 kpa).

Nowa ustawa w dalszym ciągu zezwala na umorzenie postępowania na podstawie art. 105 § 2 kpa, wprowadzając jednocześnie specyficzne dla bezpieczeństwa przemysłowego przesłanki umorzenia postępowania z urzędu. Chodzi tu o wyco-

fanie wniosku przez przedsiębiorcę (rezygnacja z ubiegania się o świadectwo bezpieczeństwa przemysłowego), wydanie orzeczenia o zakazie prowadzenia przez podmiot działalności gospodarczej (zakaz taki może być m.in. wydany przez sąd za popełnienie przestępstwa skarbowego lub w przypadku działalności regulowanej – przez właściwy podmiot prowadzący rejestr tej działalności, np. Urząd Komunikacji Elektronicznej w stosunku do operatorów telekomunikacyjnych, a w przypadku oddziałów lub przedstawicielstw przedsiębiorcy zagranicznego – minister właściwy do spraw gospodarki) oraz przejęcie lub likwidacja przedsiębiorcy (podmiot przejmujący nie może zatem żądać kontynuowania postępowania bezpieczeństwa przemysłowego prowadzonego do chwili przejęcia).

Przepisy poprzedniej ustawy zezwalały również na zawieszenie postępowania bezpieczeństwa przemysłowego w przypadkach określonych w art. 97 § 1 pkt 4 i art. 98 kpa, tj. gdy rozpatrzenie sprawy i wydanie decyzji zależało od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd, lub gdy wystąpi o to strona, na żądanie której postępowanie zostało wszczęte, a nie sprzeciwiają się temu inne strony oraz nie zagraża to interesowi społecznemu.

Nowa ustawa wprowadziła obowiązek zawieszenia, a następnie podjęcia postępowania na wniosek strony (odmiennie niż w art. 98 kpa jest to przesłanka obligatoryjna). Jednocześnie, z uwagi na brak odpowiedniej regulacji w ustawie, nadal obowiązuje przepis art. 98 § 2 kpa, zgodnie z którym żądanie wszczęcia postępowania uznaje się za wycofane, jeżeli w okresie 3 lat od daty jego zawieszenia strona wnioskująca nie wystąpi o jego podjęcie.

W dalszym ciągu istnieje również możliwość zawieszenia postępowania z urzędu, gdy jego zakończenie zależy od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd.

Ustawodawca wprowadził też katalog zdarzeń, w przypadku których ABW lub SKW może zawiesić prowadzone postępowanie. Jest to korzystne dla przedsiębiorcy ubiegającego się o świadectwo bezpieczeństwa przemysłowego, ponieważ umożliwia zawieszenie postępowania w sytuacjach, gdy jednoznaczna ocena zdolności do ochrony informacji niejawnych nie jest w danym momencie możliwa, np. z uwagi na toczące się postępowanie upadłościowe, wstrzymanie prowadzenia działalności gospodarczej lub zadłużenie z tytułu podatków, składek lub opłat lokalnych.

Według poprzedniej ustawy świadectwo bezpieczeństwa przemysłowego wydawane było w przypadku pozytywnego wyniku postępowania. Korzystając z tego samego przepisu, na zasadzie wnioskowania *a contrario*, wprowadzono za-

pis oznaczający, że negatywny wynik postępowania pociąga za sobą wydanie decyzji o odmowie wydania świadectwa. Jednocześnie, jako przesłankę fakultatywną do wydania decyzji o odmowie wydania świadectwa, przyjęto świadome podanie nieprawdziwych danych lub ich zatajenie w kwestionariuszu albo niewywiązanie się z tzw. obowiązków informacyjnych wobec ABW lub SKW.

Obecna ustawa enumeratywnie wskazuje sytuacje, w których postępowanie bezpieczeństwa przemysłowego kończy się wydaniem decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, w tym m.in. brak poświadczenia bezpieczeństwa wynikające z odmowy jego wydania lub cofnięcia kierownikowi przedsiębiorcy, brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych (np. w przypadku spółek finansowanych przez podmioty zagraniczne). Podstawą do odmowy wydania świadectwa jest również podanie nieprawdziwych danych albo ich zatajenie w kwestionariuszu oraz – co stanowi racjonalne uzupełnienie – podanie nieprawdziwych danych o zmianach zawartych w kwestionariuszu.

Zarówno ABW, jak i SKW mogą odmówić przedsiębiorcy wydania świadectwa pierwszego lub drugiego stopnia, jeżeli nie zorganizuje on w terminie 6 miesięcy od daty wszczęcia postępowania kompleksowego systemu ochrony informacji niejawnych – niejednokrotnie przedsiębiorcy ubiegali się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych przetwarzanych w ich obiektach, nie posiadając w ogóle systemu fizycznej ochrony informacji niejawnych, skutkiem czego zakończenie postępowania w istotnym stopniu opóźniało się z winy wnioskodawcy.

Istotną zmianą odnoszącą się do przesłanek fakultatywnych wydania decyzji o odmowie wydania świadectwa bezpieczeństwa jest wprowadzenie możliwości wydania takiej decyzji w przypadku niedających się usunąć wątpliwości dotyczących osób wchodzących w skład organów zarządzających, kontrolnych lub osób działających z ich upoważnienia w zakresie:

- uczestnictwa, współpracy lub popierania przez te osoby działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej, wymierzonej przeciwko Rzeczypospolitej Polskiej,

- zagrożenia tych osób ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania kontaktu,

- przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoby te uczestniczyły lub uczestniczą w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji

Rzeczypospolitej Polskiej, albo współpracowały lub współpracują z takimi partiami lub organizacjami,

- wystąpienia okoliczności mających związek z tymi osobami, powodujących ryzyko ich podatności na szantaż lub wywieranie presji,

Wydanie decyzji o odmowie wydania świadectwa może być również skutkiem niepowiadomienia w terminie 30 dni o zmianach danych zawartych w kwestionariuszu bezpieczeństwa przemysłowego (ściśle określono termin na wniesienie powiadomienia, zastępując nim nie do końca precyzyjne określenie *niezwłoczne informowanie*).

Utrzymana została możliwość przeprowadzenia z urzędu wybranych sprawdzeń lub sprawdzenia w pełnym zakresie przedsiębiorcy posiadającego ważne świadectwo bezpieczeństwa przemysłowego. Zmiana dotyczy możliwości zainicjowania sprawdzeń lub przeprowadzenia kontroli podmiotu posiadającego świadectwo na wniosek służby, która nie wydała świadectwa oraz uczestniczenia jej funkcjonariuszy lub żołnierzy w tych czynnościach. SKW może wnioskować o przeprowadzenie kontroli lub sprawdzeń w przypadku podmiotu posiadającego ważne świadectwo wydane przez ABW, jeżeli w związku z realizacją przez ten podmiot umowy (umów) na rzecz jednostki (jednostek) organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej ujawni fakty wskazujące na możliwość utraty zdolności do ochrony informacji niejawnych.

Tak samo ABW może wystąpić z wnioskiem o przeprowadzenie przez SKW sprawdzeń lub kontroli w przypadku podmiotu posiadającego świadectwo wydane przez SKW, a realizującego umowę (umowy) na rzecz jednostek organizacyjnych, które nie podlegają MON ani nie są przez niego nadzorowane. Funkcjonariusze lub żołnierze ABW lub SKW mogą zapoznać się w zakresie dotyczącym sprawdzeń lub kontroli z aktami postępowania bezpieczeństwa przemysłowego prowadzonego wobec tego podmiotu przez drugą służbę.

Określając przesłanki wydania decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, obecne przepisy wskazują w pierwszej kolejności na wyniki sprawdzeń podejmowanych z urzędu lub przeprowadzonej kontroli. Warto przy tym zwrócić uwagę, że przepisy te wskazują na możliwość, a nie konieczność wydania takiej decyzji, jak to stanowiła ustawa w jej poprzednim brzmieniu. Jednocześnie jako podstawę ewentualnego wydania takiej decyzji, przyjęto wyniki sprawdzeń lub ustalenia będące wynikiem kontroli, bez określenia, czy są to wyniki wskazujące na utratę zdolności do ochrony informacji niejawnych. Tego rodzaju zapis umożliwia bardziej elastyczne reagowanie w konkretnych przypadkach, akcentując rolę ABW lub SKW jako organów, które, analizując wyniki sprawdzeń lub

ustalenia kontroli, oceniają, czy w danym przypadku uzasadniają one wydanie decyzji o cofnięciu świadectwa.

Do przesłanek obligatoryjnych należy odmowa wydania lub cofnięcie poświadczenia bezpieczeństwa kierownikowi przedsiębiorcy, co pozwala ograniczyć sytuacje, w których podmiot posiadający świadectwo nie będzie czasowo posiadał kierownika przedsiębiorcy w rozumieniu ustawy.

Kolejną przesłanką wydania decyzji o cofnięciu świadectwa jest brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy, czyli negatywny wynik sprawdzeń z urzędu podejmowanych na podstawie art. 65 ust. 1 w zw. z art. 57 ust. 2 pkt 1.

Sprawdzenia z urzędu lub kontrola systemu ochrony informacji niejawnych, w przypadku ich negatywnego wyniku, tj. stwierdzenia utraty funkcjonalności tego systemu, również skutkują wydaniem decyzji o cofnięciu świadectwa. Jako utratę funkcjonalności należy uznać niewypełnienie wymagań ustawy i aktów wykonawczych w zakresie organizacji systemu.

Ostatnią z przesłanek obligatoryjnych jest podanie nieprawdziwych danych lub zatajenie danych w ramach uzupełnień kwestionariusza, analogicznie jak w art. 64 ust. 2 pkt. 4-5.

Po wydaniu decyzji o cofnięciu świadectwa ABW lub SKW powinna niezwłocznie poinformować o zaistniałym fakcie jednostki organizacyjne, które zawarły z przedsiębiorcą umowy lub realizują zadania związane z dostępem do informacji niejawnych.

Zasadniczą zmianą dotyczącą danych, które powinny zostać zawarte w świadectwie, decyzji o odmowie wydania świadectwa lub o jego cofnięciu, jest wymóg podania numeru Krajowego Rejestru Sądowego i numeru REGON sprawdzanego podmiotu, przy czym konieczność podania numeru KRS dotyczy oczywiście tych podmiotów, które podlegają z mocy prawa obowiązkowi wpisu do właściwego rejestru prowadzonego w ramach KRS. Tego rodzaju dodatkowe informacje pozwalają jednoznacznie zidentyfikować podmiot wymieniony w świadectwie (niepowtarzalność obu wymienionych numerów), nawet w przypadku zmiany nazwy firmy, pod jaką przedsiębiorca prowadzi działalność, która nastąpiła po wydaniu dokumentu.

Kolejną zmianą jest zastąpienie dotychczasowego pojęcia *służby ochrony państwa* wskazaniem ABW lub SKW jako organów odpowiedzialnych za przepro-

wadzanie postępowań bezpieczeństwa przemysłowego i wydawania dokumentów potwierdzających uprawnienia w tym zakresie.

W przypadku decyzji o odmowie wydania świadectwa lub decyzji o jego cofnięciu zmianie uległa regulacja odnosząca się do faktycznego uzasadnienia decyzji. Poprzednio można było odstąpić od faktycznego uzasadnienia decyzji lub je ograniczyć w zakresie, w jakim udostępnienie mogłoby spowodować istotne zagrożenie dla podstawowych interesów RP dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa.

Powyższe przesłanki, uzasadniające odstąpienie lub ograniczenie uzasadnienia, nawiązywały wprost do definicji tajemnicy państwowej.

Nowa ustawa odstępuje od poprzedniego podziału na dwie kategorie informacji niejawnych: tajemnicę państwową lub służbową, dlatego też wskazano, że uzasadnienie decyzji podlega ochronie na zasadach określonych w ustawie, tj. powinno być chronione odpowiednio do klauzuli tajności zawartych w nim informacji. Tym samym należy uznać, że w przypadku decyzji, których uzasadnienie w całości lub w części zawiera informacje niejawne, uzasadnienie to lub jego część nie będzie zamieszczana w decyzji.

Tryb odwoławczy i skargowy przysługuje przedsiębiorcy, w przypadku gdy ABW lub SKW wydała decyzje o odmowie wydania i cofnięciu świadectwa – analogicznie jak w poprzednich przepisach – oraz w przypadku decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego.

Obowiązujące obecnie przepisy, zawarte w rozdziale dotyczącym bezpieczeństwa przemysłowego, odwołują się w powyższym zakresie do wybranych artykułów odnoszących się do postępowań sprawdzających wobec osób. Zgodnie z nimi postępowanie odwoławcze przedstawia się następująco:

- przedsiębiorca wnosi odwołanie w terminie 14 dni od dnia doręczenia decyzji za pośrednictwem organu, który przeprowadził postępowanie. Odwołanie nie wymaga uzasadnienia,

- organ, który przeprowadził postępowanie, jest obowiązany przesłać odwołanie wraz z aktami postępowania Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym otrzymał odwołanie,

- rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia jego otrzymania,

- wniesienie odwołania nie wstrzymuje wykonania decyzji,
- Prezes Rady Ministrów stwierdza, w drodze postanowienia, niedopuszczalność odwołania lub uchybienie terminowi do wniesienia odwołania,
- Prezes Rady Ministrów może, na żądanie sprawdzanego podmiotu lub z urzędu, zlecić właściwemu organowi (ABW lub SKW) przeprowadzenie dodatkowych czynności w celu uzupełnienia dowodów i materiałów w postępowaniu,
- Prezes Rady Ministrów wydaje decyzję, w której:
  - utrzymuje w mocy decyzję organu, który przeprowadził postępowanie,
  - uchyla decyzję organu, który przeprowadził sprawdzenia lub kontrolę zakończone cofnięciem świadectwa bezpieczeństwa przemysłowego,
  - uchyla decyzję organu, który przeprowadził postępowanie, i nakazuje mu wydanie świadectwa bezpieczeństwa przemysłowego,
  - uchyla decyzję organu, który przeprowadził postępowanie, i przekazuje sprawę do ponownego rozpatrzenia,
  - stwierdza nieważność decyzji organu, który przeprowadził postępowanie;
- po wydaniu decyzji lub postanowienia Prezes Rady Ministrów niezwłocznie zwraca właściwemu organowi akta postępowania,
- decyzje i postanowienia doręcza się na piśmie sprawdzanemu przedsiębiorcy i właściwemu organowi.

Dodatkowe regulacje odnoszące się do postępowania odwoławczego:

- uzasadnienie faktyczne decyzji w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w ustawie,
- postępowanie odwoławcze może zostać zawieszone w przypadku:
  - gdy ocena zdolności podmiotu do ochrony informacji niejawnych zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ,
  - gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego;

- zawieszone postępowanie odwoławcze zostaje podjęte, jeżeli:
  - ustąpiły przyczyny uzasadniające zawieszenie postępowania,
  - ujawniono okoliczności mogące stanowić podstawę do odmowy wydania świadectwa bezpieczeństwa przemysłowego lub umorzenia postępowania bezpieczeństwa przemysłowego;
- o zawieszeniu postępowania odwoławczego oraz o jego podjęciu organ prowadzący postępowanie zawiadamia przedsiębiorcę.

Postępowanie skargowe przedstawia się następująco:

- przedsiębiorcy przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie organu odwoławczego w terminie 30 dni od dnia doręczenia,
- sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym,
- odpis sentencji wyroku z uzasadnieniem doręcza się tylko właściwemu organowi odwoławczemu. Skarżącemu doręcza się odpis wyroku,
- po wydaniu wyroku, sąd administracyjny niezwłocznie zwraca akta postępowania bezpieczeństwa przemysłowego.

Postępowanie odwoławcze prowadzone przez Prezesa Rady Ministrów jest umarzane w przypadku likwidacji przedsiębiorcy, przejęcia lub wydania orzeczenia o zakazie prowadzenia działalności gospodarczej – zmiana w stosunku do poprzednich przepisów polega na uwzględnieniu zakazu prowadzenia działalności, natomiast nie dochodzi do umorzenia postępowania w przypadku ogłoszenia upadłości podmiotu.

W nowej ustawie wskazano jednoznacznie sytuacje, w przypadku których świadectwo wygasa. Zgodnie z tym przepisem w przypadku połączenia dwóch spółek prawa handlowego poprzez przejęcie spółki przejmowanej przez spółkę przejmującą, świadectwo nie przechodzi na podmiot przejmujący, odmiennie niż w przypadku zezwoleń i koncesji posiadanych przez spółkę przejmowaną, które przechodzą zgodnie z przepisami kodeksu spółek handlowych na spółkę przejmującą.

Do wygaśnięcia świadectwa dochodzi również wtedy, gdy przedsiębiorca zrzeka się uprawnień określonych w tym świadectwie, zostaje zlikwidowany lub upływa okres ważności świadectwa, z uwzględnieniem „kaskadowej" ważności.

W porównaniu do poprzedniej ustawy nie uległ istotnej zmianie przepis dotyczący obowiązków informacyjnych nałożonych na przedsiębiorcę w trakcie trwania postępowania bezpieczeństwa przemysłowego lub w okresie ważności świadectwa. W ustawie dodano regulacje, które porządkują kompetencje ABW i SKW w zakresie przekazywania informacji uzyskiwanych od przedsiębiorców odnośnie zawieranych umów związanych z dostępem do informacji niejawnych.

Również art. 71 nowej ustawy, dotyczący instrukcji bezpieczeństwa przemysłowego, nie zawiera istotnych różnic w stosunku do swojego odpowiednika w poprzedniej ustawie. Dodane zostały zapisy regulujące obowiązek jednostki organizacyjnej, która zawarła umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, niezwłocznego przekazania ABW lub SKW m.in. danych przedsiębiorcy, z którym zawarto umowę, a także obowiązek przekazywania kopii instrukcji bezpieczeństwa przemysłowego lub kopii świadectwa przedsiębiorcy, z którym zawarto umowę.

W nowej ustawie wprowadzono przepisy przejściowe, które zakładają kontynuację przez określony czas skutków prawnych poprzedniej ustawy. Zgodnie z art. 186 nowej ustawy świadectwa bezpieczeństwa przemysłowego wydane na podstawie przepisów poprzednich, ważne w dniu wejścia w życie ustawy, potwierdzające zdolność do ochrony informacji niejawnych o klauzuli „ściśle tajne" – potwierdzają także zdolność do ochrony informacji o klauzuli „tajne" i „poufne" w okresie wskazanym w nowej ustawie, natomiast o klauzuli „tajne" – potwierdzają także zdolność do ochrony informacji niejawnych o klauzuli „poufne" w okresie wskazanym w niniejszej ustawie. Okresy ważności wskazanych wyżej świadectw liczone są od daty wydania świadectwa.

Zgodnie z art. 187 ustawy przedsiębiorcy wykonujący umowy związane z dostępem do informacji niejawnych o klauzuli „poufne", nieposiadający w dniu wejścia w życie nowej ustawy ważnego świadectwa bezpieczeństwa przemysłowego powinni uzyskać takie świadectwo w terminie 12 miesięcy od dnia wejścia w życie nowej ustawy.

Na mocy art. 188 nowej ustawy do postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

Paweł Antosiak

Krajowa władza bezpieczeństwa

Celem niniejszego artykułu jest przedstawienie zmian w funkcjonowaniu systemu ochrony informacji niejawnych Sojuszu Północnoatlantyckiego (NATO) oraz Unii Europejskiej (UE) w Polsce związanych z wejściem w życie nowej ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r.[1], zwanej w dalszej części artykułu „nową ustawą", i powołaniem jednej krajowej władzy bezpieczeństwa, zwanej dalej „KWB".

Na wstępie warto przypomnieć, że *Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji*[2] oraz przepisy bezpieczeństwa Unii Europejskiej[3] nakładają na państwa członkowskie obowiązek powołania KWB – instytucji odpowiedzialnej za nadzorowanie systemu ochrony informacji niejawnych NATO i UE w danym państwie członkowskim.

Zadaniem KWB jest więc wdrażanie standardów bezpieczeństwa NATO i UE. Jest ona odpowiedzialna za zapewnienie – przez instytucje krajowe i podległe im jednostki organizacyjne, zarówno w sferze cywilnej, jak i wojskowej, działające w kraju i za granicą – właściwego poziomu ochrony informacji niejawnych międzynarodowych. Do zadań ABW należy również współpraca ze strukturami bezpieczeństwa NATO i UE oraz krajowymi władzami bezpieczeństwa państw członkowskich.

Do dnia wejścia w życie nowej ustawy funkcję KWB w Polsce pełnili Szef ABW i Szef SKW i były to jedyne organy upoważnione m.in. do wydawania decyzji o przyznaniu dostępu do informacji niejawnych NATO i UE (poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego) tych organizacji. Dotychczas istniały dwa równoległe i niezależne od siebie systemy ochrony informacji niejawnych Sojuszu Północnoatlantyckiego i Unii Europejskiej, jeden dla sfery cywilnej, drugi dla sfery wojskowej, i choć obydwa spełniały wymogi bezpieczeństwa NATO i UE, to stosowały odmienne standardy w tym zakresie.

---

[1] Dz. U. z 2010 r., Nr 182, poz. 1228.

[2] Art. 2 *Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji* (Dz.U. z 2000 r., Nr 64, poz. 740).

[3] Art. 15 pkt 3a Decyzji Rady Unii Europejskiej z dnia 31.03.2011 r., Nr 2011/292/EU (OJ L 141, 27.05.2011, str. 17). Obowiązek powołania jednej KWB był również określony w poprzedniej decyzji Rady UE z dnia 19 marca 2001 nr 2001/264/EC w część II Sekcja I pkt 9.

Nowa ustawa wprowadziła fundamentalną zmianę, zgodnie bowiem z jej art. 11 funkcję KWB pełni jeden organ (Szef ABW), co jest stosowaną praktyką w zdecydowanej większości państw członkowskich NATO i UE. W rezultacie jeden ośrodek w kraju koordynuje czynności właściwe dla tej funkcji.

Powyższa zmiana miała na celu przede wszystkim ujednolicenie obu systemów ochrony informacji niejawnych międzynarodowych (tj. NATO, UE i wymienianych na podstawie innych umów międzynarodowych), przez m.in. jasne określenie kompetencji, wprowadzenie jednolitych rozwiązań oraz interpretację przepisów. Nie bez znaczenia był również fakt, że w kontaktach bilateralnych z KWB innych państw czy na forum międzynarodowym Polska za granicą była reprezentowana przez dwie delegacje. Nowa ustawa ten stan zmieniła, co podkreślali w uzasadnieniu jej projektodawcy.

Na podstawie art. 11 nowej ustawy[4], a także uzasadnienia sporządzonego przez ustawodawcę można wskazać główne założenia funkcjonowania jednej KWB. W myśl przepisów jest ona właściwa do „nadzorowania" systemu ochrony informacji niejawnych w stosunkach Polski z innymi państwami lub organizacjami międzynarodowymi. Tak więc Szef ABW nie posiada wyłączności na prowadzenie

[4] Art. 11: „1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.
2. Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „NATO", Unii Europejskiej lub innych organizacji międzynarodowych, zwanych dalej „informacjami niejawnymi międzynarodowymi".
3. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2, za pośrednictwem Szefa SKW.
4. W zakresie niezbędnym do wykonywania funkcji krajowej władzy bezpieczeństwa odpowiednio Szef ABW lub upoważnieni przez niego funkcjonariusze ABW oraz Szef SKW lub upoważnieni przez niego żołnierze lub funkcjonariusze SKW mają prawo do:
1) wglądu do dokumentów i pomieszczeń związanych z ochroną informacji niejawnych międzynarodowych;
2) wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
3) dostępu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
4) uzyskiwania wyjaśnień i informacji dotyczących ochrony informacji niejawnych międzynarodowych.
5. Szef ABW organizuje współdziałanie z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa.
6. Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, tryb i sposób współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW.
7. W rozporządzeniu, o którym mowa w ust. 6, Prezes Rady Ministrów uwzględni rolę Szefa ABW w nadzorze nad systemem ochrony informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi oraz konieczność zapewnienia jednolitości stosowanych przez krajową władzę bezpieczeństwa procedur w sferze cywilnej i wojskowej".

postępowań sprawdzających kończących się decyzją administracyjną, a poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego są i będą nadal wydawane – zgodnie z właściwością rzeczową – przez ABW i SKW.

W świetle powyższego ważne jest, jak interpretować art. 11 ust. 2, według którego *KWB jest właściwa do* (…) *wydawania dokumentów upoważniających do dostępu do informacji niejawnych* (…) *Organizacji Traktatu Północnoatlantyckiego* (...)*, Unii Europejskiej lub innych organizacji międzynarodowych*. ABW stoi na stanowisku, że wspomnianymi dokumentami powinny być zaświadczenia, wydawane przez KWB na podstawie przeprowadzonych przez ABW lub SKW procedur, potwierdzających, że dana osoba fizyczna, podmiot (przedsiębiorca) lub system teleinformatyczny został poddany określonej procedurze sprawdzającej lub certyfikacji, w wyniku której określono, czy spełnia on wymogi bezpieczeństwa NATO lub UE czy też ich nie spełnia.

Co ważne, w odróżnieniu od wydanych poświadczeń, świadectw lub certyfikatów akredytacji, zaświadczenia – i tylko one – są obowiązujące za granicą.

Najbardziej złożonym problemem wydaje się kwestia realizacji zadań KWB w sferze wojskowej *za pośrednictwem Szefa SKW* (art. 11 ust. 3). Ustawodawca w delegacji ustawowej (art. 11 ust. 6 i 7) zobowiązał Prezesa Rady Ministrów do określenia w rozporządzeniu zasad współpracy szefów obu służb w tym zakresie i choć projekt rozporządzenia Prezesa Rady Ministrów w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa jest dostępny[5], to w dalszym ciągu w Kancelarii PRM trwają nad nim prace (projekt został rozesłany 8 kwietnia 2011 r. do uzgodnień międzyresortowych). Za wcześnie jest więc przytaczać lub analizować przygotowywane projekty aktów prawnych, ponieważ trudno przewidzieć, jaki ostatecznie kształt one przybiorą oraz jak współpraca szefów obu służb będzie przebiegała w tym zakresie.

Mając na uwadze fakt, że do końca 2010 r. nie uregulowano kompleksowo zasad bezpieczeństwa informacji niejawnych międzynarodowych (wspomniane rozporządzenie będzie regulowało jedynie kwestię współpracy Szefów ABW i SKW w tym obszarze), że systemy bezpieczeństwa NATO i UE w sferze cywilnej i wojskowej są odmienne, wchodzi w życie nowa ustawa, a także to, że ta ustawa wyznacza nowe zadania i nakłada odpowiedzialność na Szefa ABW, Szef ABW wydał 31 grudnia 2010 r. *Wytyczne w sprawie postępowania z informacjami nie-*

[5] Projekt jest opublikowany na stronie Biuletynu Informacji Publicznej Kancelarii Prezesa Rady Ministrów: http://bip.kprm.gov.pl/kprm/dokumenty/61_3932.html.

jawnymi międzynarodowymi[6] i jak dotychczas jest to jedyny dokument w kraju porządkujący przedmiotowe zagadnienie w całości.

Podsumowując założenia funkcjonowania jednej KWB i realizowane przez nią obecnie zadania należy stwierdzić, że pełni ona funkcję opiniotwórczą, nadzorczą i jest organem wydającym zaświadczenia potwierdzające spełnianie bądź niespełnianie określonych wymogów bezpieczeństwa przez osobę, przedsiębiorcę lub system teleinformatyczny. Do głównych zadań KBW należy ponadto kształtowanie polityki ochrony informacji niejawnych NATO i UE w kraju, opracowanie jej założeń oraz kierunków rozwoju, wypracowanie oficjalnych stanowisk, interpretacja przepisów bezpieczeństwa obu organizacji, a także potwierdzanie i przekazywanie partnerom zagranicznym informacji dotyczących spełniania przez osoby, przedsiębiorców, transport, sprzęt lub system warunków bezpieczeństwa. Zadaniem KWB jest również negocjowanie treści umów bilateralnych o ochronie informacji niejawnych.

Czynności te, w imieniu Szefa ABW jako KWB, wykonują Departament Ochrony Informacji Niejawnych oraz Departament Bezpieczeństwa Teleinformatycznego ABW, zgodnie z właściwością. Podejmowane przez wymienione jednostki przedsięwzięcia powinny zmierzać do ujednolicenia systemu ochrony informacji niejawnych NATO i UE w kraju.

Blisko półroczne funkcjonowanie jednej KWB wydaje się okresem zbyt krótkim, aby pokusić się o pełną i rzetelną ocenę tego rozwiązania. Nie ulega wątpliwości, iż wejście w życie nowej ustawy o ochronie informacji niejawnych i powołanie jednej KWB to duże wyzwanie dla podmiotów odpowiedzialnych za wdrożenie przewidzianych ustawą zasad. Niemniej jednak powołanie jednej KWB jest korzystne zarówno dla sprawnego obiegu informacji niejawnych NATO i UE w kraju, jak również przyczyni się do efektywniejszej współpracy ze strukturami bezpieczeństwa tych organizacji.

[6] *Wytyczne w sprawie postępowania*… są dostępne na stronie internetowej ABW: www.abw.gov.pl (zakładka „Ochrona informacji niejawnych").

Jerzy Poskoczym

Korzystanie z dokumentów i materiałów zawierających informacje niejawne oraz zasady dostępu do nich

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228)[1], zwana dalej „nową ustawą OIN", określa zasady postępowania z informacjami niejawnymi, które wymagają ochrony przed nieuprawnionym ujawnieniem.

W stosunku do *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. z 2005 r., Nr 196, poz. 1631 z późn zm.) nowa ustawa OIN wprowadza wiele zmian, między innymi nową terminologię czy zmiany w definiowaniu klauzul tajności. Zmienione również zostają zasady dostępu do dokumentów i materiałów zawierających informacje niejawne.

Dostęp do informacji niejawnych można uzyskać po otrzymaniu poświadczenia bezpieczeństwa oraz po odbyciu szkolenia z zakresu ochrony informacji niejawnych[2]. Wyjątkiem od tej zasady jest dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone", które może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa, i po odbyciu szkolenia w zakresie ochrony informacji niejawnych – art. 21 ust. 4 nowej ustawy OIN. Przepis ten jest nową regulacją. W poprzedniej ustawie w przypadku dostępu do informacji niejawnych o klauzuli „zastrzeżone" wymagane było posiadanie poświadczenia bezpieczeństwa, otrzymanego po pozytywnym zakończeniu zwykłego postępowania sprawdzającego[3].

Przepisy nowej ustawy OIN dają również możliwość udostępnienia informacji niejawnych osobom, które nie posiadają stosownego poświadczenia bezpieczeństwa. W art. 34 ust. 5 nowej ustawy OIN przewidziano bowiem, iż szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu, Kancelarii Senatu lub Kancelarii Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego, Prezes

---

[1] Stan prawny wszystkich cytowanych przepisów na dzień 15 kwietnia 2011 r.

[2] Art. 21 ust. 1 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228).

[3] Art. 37 ust. 7 *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. z 2005 r., Nr 196, poz. 1631 z późn zm.).

Najwyższej Izby Kontroli lub kierownik urzędu centralnego, a w przypadku ich braku − ABW albo SKW, mogą w szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4 ust. 2 nowej ustawy[4], wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa. Mogą również wyrazić pisemną zgodę na udostępnienie informacji o klauzuli „tajne" lub „ściśle tajne" osobie, wobec której wszczęto poszerzone postępowanie sprawdzające.

Ponadto, zgodnie z art. 34 ust. 9 nowej ustawy OIN, kierownik jednostki organizacyjnej może wyrazić zgodę w formie pisemnej na udostępnienie informacji niejawnych o klauzuli „poufne" osobie, wobec której wszczęto postępowanie sprawdzające.

Należy również pamiętać, iż w stanach nadzwyczajnych Prezydent Rzeczypospolitej Polskiej lub Prezes Rady Ministrów, każdy w swoim zakresie, może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego. W art. 34 ust. 7 nowej ustawy OIN sprecyzowano, że w przypadkach opisanych powyżej kopię zgody na udostępnienie informacji niejawnych lub odstąpienie od przeprowadzenia postępowania sprawdzającego przekazuje się odpowiednio do ABW lub SKW. Obowiązek ten nie dotyczy służb i instytucji uprawnionych do przeprowadzania poszerzonych postępowań sprawdzających, o których mowa w art. 23 ust. 5[5] nowej ustawy OIN.

W art. 4 ust. 2 nowej ustawy OIN podkreślono natomiast, iż zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

Przepis ten odsyła zatem w sprawach dotyczących postępowania z materiałami niejawnymi do innych rozwiązań prawnych, których należy poszukiwać w normach określających daną procedurę.

Jeśli chodzi o dostęp do informacji niejawnych w postępowaniu karnym, będą tu miały zastosowanie odpowiednie przepisy procedury karnej zawarte w *Ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego* (Dz.U. z 1997 r. Nr 89, poz. 555, z późn zm.), zwanej dalej kpk, i aktach wykonawczych do przed-

[4] Art. 4 ust. 2 nowej ustawy OIN – zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

[5] Tj. Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Biuro Ochrony Rządu, Policja, Służba Więzienna, Służba Wywiadu Wojskowego, Straż Graniczna oraz Żandarmeria Wojskowa.

miotowego aktu prawnego, a nie bezpośrednio przepisy ustawy o ochronie informacji niejawnych.

Przedstawiając rozwiązania regulujące wykorzystanie dokumentów zawierających informacje niejawne jako dowodów w postępowaniu karnym, należy przywołać przepis art. 226 kpk[6] stanowiący normę o charakterze dość ogólnym. Szczegółowe zasady postępowania z tego rodzaju dokumentami określa *Rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2003 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania tajemnicy państwowej, służbowej albo związanej z wykonywaniem zawodu lub funkcji* (Dz.U. z 2003 r. Nr 108, poz. 1023), zwane dalej „rozporządzeniem", wydane na podstawie art. 181 § 2 kpk (tym miejscu należy dodać, iż rozporządzenie nie zostało jeszcze znowelizowane).

W obecnie obowiązującym rozporządzeniu stosowana jest jeszcze terminologia obowiązująca w *Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, między innymi tajemnica państwowa i tajemnica służbowa, natomiast nowa ustawa OIN zastępuje ją zwrotami: informacje niejawne o klauzuli „zastrzeżone", „poufne", „tajne" i „ściśle tajne".

Zgodnie z przepisami wyżej wymienionego rozporządzenia z przesłuchań oskarżonych, świadków, biegłych i kuratorów, obejmujących okoliczności, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo związanej z wykonywaniem zawodu lub funkcji, sporządza się odrębny protokół, który wyłącza się z akt sprawy (§ 2 rozporządzenia). Odrębny protokół sporządzany jest również w przypadku zatrzymania lub przyjęcia w postępowaniu karnym dokumentów lub przedmiotów, na które rozciąga się obowiązek zachowania tajemnicy informacji niejawnych albo związanej z wykonywaniem zawodu lub funkcji (§ 3 rozporządzenia)[7].

Wszystkie dokumenty, które w toku postępowania karnego uznano za zawierające informacje niejawne, należy oznaczyć klauzulą tajności „zastrzeżone", „poufne", „tajne" lub „ściśle tajne" odpowiednio do ich treści (§ 5 i § 6 rozporządzenia). Odpowiednią klauzulę tajności nadaje prezes sądu, a w postępowaniu przygotowawczym kierownik właściwej jednostki organizacyjnej prokuratury w sposób określony przepisami o ochronie informacji niejawnych.

---

[6] Artykuł 226 kpk – w kwestii wykorzystania dokumentów zawierających informacje niejawne lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się odpowiednio zakazy i ograniczenia określone w art. 178-181. Jednakże w postępowaniu przygotowawczym o wykorzystaniu, jako dowodów, dokumentów zawierających tajemnicę lekarską decyduje prokurator.

[7] W. Grzeszczyk, *Komentarz do Dz.U. 1997.89.555,* „Lex Polonica".

Inną istotną kwestią, którą reguluje wspomniane rozporządzenie, jest udostępnianie stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym dokumentów, akt i przedmiotów oznaczonych klauzulą tajności. Wyjątek stanowią tu materiały dotyczące świadka, o którym mowa w art. 184 § 1 kpk[8].

Zgodnie z § 10 pkt 1 rozporządzenia materiały oznaczone klauzulą tajności udostępniane są jedynie na zarządzenie prezesa sądu, a przed uprawomocnieniem się wyroku – na zarządzenie sądu, natomiast w postępowaniu przygotowawczym na zarządzenie kierownika właściwej jednostki organizacyjnej prokuratury. W zarządzeniu tym należy wskazać osobę uprawnioną do przejrzenia dokumentów, akt lub przedmiotów oznaczonych klauzulą tajności oraz określić czas zapoznania się z nimi w sekretariacie lub kancelarii tajnej sądu lub prokuratury w obecności pracownika sekretariatu lub kancelarii tajnej. Niedopuszczalne jest sporządzanie kopii odpisów, wyciągów i notatek z dokumentów oraz akt oznaczonych klauzulą tajności.

Te same zasady udostępniania materiałów oznaczonych klauzulą tajności obowiązują osoby pozbawione wolności (§ 11 rozporządzenia). Przepis § 14 umożliwia udostępnienie biegłemu dokumentów, akt lub przedmiotów oznaczonych klauzulą tajności w drodze zarządzenia i w sposób określony przez prezesa sądu, sąd lub kierownika właściwej jednostki organizacyjnej prokuratury w zakresie niezbędnym do wydania opinii. Przepisy dotyczące zasad udostępniania tego rodzaju materiałów, zawarte w § 10 ust. 2 i 3, § 12 i § 13 rozporządzenia, stosowane są wówczas odpowiednio. Należy również pamiętać, że chociaż zakres podmiotowy tego przepisu odnosi się do biegłego, to w myśl art. 204 § 3 kpk wspomniany przepis stosuje się wprost do tłumaczy. Skoro bowiem norma kodeksowa nakazuje odpowiednie stosowanie przepisów kodeksu dotyczących biegłych do omawianej grupy uczestników procesu, to odnosi się to nie tylko do przepisów zawartych w kodeksie, ale również do rozwiązań zamieszczonych w aktach wykonawczych.

W celu udokumentowania zapoznania się z materiałami niejawnymi, każdy przypadek udostępnienia odnotowuje się w karcie zapoznania z dokumentem, z zaznaczeniem daty, miejsca, nazwiska i imienia osoby przeglądającej, a osoba ta potwierdza fakt zapoznania się z dokumentem, aktami lub przedmiotem własnoręcznym podpisem (§ 13 rozporządzenia).

---

[8] Artykuł 184 § 1 kpk – jeżeli zachodzi uzasadniona obawa niebezpieczeństwa dla życia, zdrowia, wolności albo mienia w znacznych rozmiarach świadka lub osoby dla niego najbliższej, sąd, a w postępowaniu przygotowawczym prokurator, może wydać postanowienie o zachowaniu w tajemnicy okoliczności umożliwiających ujawnienie tożsamości świadka, w tym danych osobowych, jeżeli nie mają one znaczenia dla rozstrzygnięcia w sprawie. Postępowanie w tym zakresie toczy się bez udziału stron i objęte jest tajemnicą jako informacja niejawna o klauzuli tajności „tajne" lub „ściśle tajne". W postanowieniu pomija się okoliczności, o których mowa w zdaniu pierwszym.

Jak już wspomniano udostępnienie dokumentów, akt lub przedmiotów oznaczonych klauzulą tajności, następuje w sekretariacie lub kancelarii tajnej sądu lub prokuratury w obecności pracownika sekretariatu lub kancelarii tajnej. W wyjątkowych wypadkach prezes sądu lub kierownik właściwej jednostki organizacyjnej prokuratury może przesłać dokumenty, akta lub przedmioty oznaczone klauzulą tajności komendantowi jednostki organizacyjnej Policji, komendantowi jednostki organizacyjnej Żandarmerii Wojskowej, kierownikowi jednostki organizacyjnej Agencji Bezpieczeństwa Wewnętrznego, komendantowi jednostki organizacyjnej Straży Granicznej lub innemu organowi, uprawnionemu zgodnie z przepisami o ochronie informacji niejawnych, na ich wniosek zawierający uzasadnienie potrzeby zapoznania się z nimi.

Reasumując, omówione rozporządzenie spełnia swoją rolę i skutecznie reguluje sposób postępowania z aktami spraw zawierających informacje niejawne w postępowaniu przed sądami i innymi organami przy zachowaniu zasady rzetelnego i sprawiedliwego postępowania karnego. Należy jednak pamiętać, iż niezbędna będzie jego nowelizacja polegająca przede wszystkim na wprowadzeniu zmian porządkowych związanych z dostosowaniem do terminologii, którą posługuje się nowa *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*.

Stanisław Smykla

Zmiany w przepisach dotyczących ewidencji i udostępniania danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

Jeżeli jednym z podstawowych celów podjęcia prac nad nową ustawą o ochronie informacji niejawnych było *uproszczenie istniejącego systemu i jego aktualizacja*[1], to wydaje się, iż udało się ten cel osiągnąć w ustawie z dnia 5 sierpnia 2010 r. (Dz.U. z 2010 r., Nr 182, poz. 1228), zwanej „ustawą", szczególnie w przypadku przepisów odnoszących się do postępowania z materiałami i danymi zgromadzonymi w związku z postępowaniami sprawdzającymi i kontrolnymi postępowaniami sprawdzającymi oraz postępowaniami bezpieczeństwa przemysłowego. Co ważne, cel ten osiągnięto bez uszczerbku dla bezpieczeństwa informacji gromadzonych w toku wymienionych procedur. Wręcz przeciwnie, na skutek wprowadzonych zmian kwestiom tym nadano wyższy poziom ochrony.

Podstawowa zmiana polega na tym, że zagadnienia dotyczące prowadzenia ewidencji i udostępniania danych oraz procedur[2] zrealizowanych na podstawie przepisów ustawy zgromadzono w jednym, wyodrębnionym rozdziale (*Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego*). W przypadku *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (tekst jednolity Dz.U. z 2005 r., Nr 196, poz. 1631 z późn. zm.), zwanej dalej „ustawą z 1999 r.", przedmiotowe kwestie umieszczono w różnych rozdziałach, w odległych od siebie jednostkach redakcyjnych[3].

W nowej ustawie omawiane zagadnienia ujęto w dwóch artykułach, przy czym w art. 72 określono kompleksowo sposób postępowania z aktami procedur przeprowadzonych wobec osób i przedsiębiorców, natomiast w art. 73 – kwestie związane z prowadzeniem przez ABW i SKW ewidencji z zakresu bezpieczeństwa osobowego.

---

[1] Uzasadnienie do projektu ustawy przesłanego do Sejmu (http://orka.sejm.gov.pl/Druki6ka.nsf/wgdrukuj/2791).

[2] Mowa o postępowaniach sprawdzających, kontrolnych postępowaniach sprawdzających i postępowaniach bezpieczeństwa przemysłowego.

[3] Art. 42 ust. 2-8, art. 75 *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.*

Zgodnie z przyjętymi rozwiązaniami zarówno akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez organy i służby uprawnione do prowadzenia poszerzonych postępowań sprawdzających, jak też akta postępowań bezpieczeństwa przemysłowego przeprowadzonych przez ABW i SKW są udostępniane do wglądu lub przekazywane wyłączenie na pisemne żądanie wskazanych podmiotów w pięciu określonych przypadkach (zamknięty katalog):

1) sądowi lub prokuratorowi dla celów postępowania karnego,
2) służbom i organom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających dla celów postępowania sprawdzającego wobec tej samej osoby,
3) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań, o których mowa w art. 23 ust. 5,
4) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia,
5) sądowi administracyjnemu w związku z rozpatrywaniem skargi.

W stosunku do dotychczasowego stanu prawnego wprowadzono wiele innych zmian. Ustawodawca zastrzegł, że akta mogą być *udostępnione do wglądu* lub *przekazane*, do tej pory zaś stosowano pojęcie u d o s t ę p n i e n i a – w przypadku akt procedur zrealizowanych przez służby, określone w art. 30 ustawy z 1999 r. lub u d o s t ę p n i e n i a d o w g l ą d u – w przypadku akt postępowań przeprowadzonych przez pełnomocników ochrony. W praktyce występowały wątpliwości, czy pojęcie udostępnienia zawiera także przesłanie akt do innej jednostki organizacyjnej w celu dokonania tamże ich przeglądu.

Ponadto, określając przypadki uzasadniające *udostępnienie do wglądu* lub *przekazanie* akt, zrezygnowano z zastrzeżenia, że dotyczy to procedur „zakończonych". Niejasne było bowiem, czy sądowi lub prokuraturze można udostępnić akta trwającego postępowania, i podobnie, czy Prezes Rady Ministrów może mieć wgląd – w ramach rozpatrywania zażalenia – do akt niezakończonego postępowania, w którym wydano postanowienie o zawieszeniu procedury.

W ustawie przyjęto także, że akta postępowań bezpieczeństwa przemysłowego (do realizacji których uprawnione są nadal wyłącznie ABW i SKW) udostępniane są w przypadku zaistnienia tych samych okoliczności i w tym samym trybie co akta postępowań sprawdzających i kontrolnych postępowań sprawdzających. Oznacza to między innymi, że nie przeniesiono z ustawy z 1999 r. uprawnień Prezydenta RP i Prezesa Rady Ministrów do zapoznania się z aktami postępowań bezpieczeństwa, *gdy wymaga tego istotny interes Rzeczypospolitej Polskiej*.

Rozszerzenie katalogu przypadków, w których nastąpić może udostępnienie do wglądu lub przekazanie akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i akt postępowań bezpieczeństwa przemysłowego, o sytuacje związane z przeprowadzeniem kontroli prawidłowości postępowania oraz w związku z rozpatrywaniem zażalenia wynika z wprowadzenia do ustawy tych instytucji[4].

Co istotne, w art. 72 ust. 1 pkt 3 ustawy wskazano (normę tę wprowadzono w art. 12 ust. 3 ustawy), że spod kontroli prawidłowości przeprowadzonego postępowania, a co za tym idzie – z prawa do wglądu na tej podstawie, wyłączone są akta postępowań przeprowadzonych przez organy i służby wymienione w art. 23 ust. 5 ustawy (AW, CBA, BOR, Policja, Służba Więzienna, SWW, Straż Graniczna oraz Żandarmeria Wojskowa).

Szczególnie ważne zastrzeżenie zawarto w art. 72 ust. 2, w którym stwierdzono wprost, że akta postępowań sprawdzających i kontrolnych postępowań sprawdzających, przeprowadzonych przez AW, ABW, SKW lub SWW, mogą być udostępnione wyłącznie *dla celów postępowania sprawdzającego prowadzonego przez tę samą służbę wobec tej samej osoby*. Oznacza to, że dostęp do akt postępowania przeprowadzonego przez wymienione służby będzie miała tylko ta służba, która przeprowadziła tę procedurę.

Dwie ważne zmiany znalazły się ponadto w przepisach odnoszących się do udostępniania do wglądu lub przekazywania akt zwykłych postępowań sprawdzających i kontrolnych postępowań sprawdzających zrealizowanych przez pełnomocników ochrony. Przede wszystkim uznano, że z przedmiotowymi aktami, poza przypadkami określonymi w art. 72 ust. 1, można zapoznać się także dla celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, ale dotyczy to tylko postępowania prowadzonego wobec tej samej osoby. Chociaż utrzymano możliwość zapoznania się przez osobę sprawdzaną z aktami przeprowadzonego wobec niej zwykłego postępowania sprawdzającego, to wprowadzono ograniczenie, że prawo to nie dotyczy *danych dotyczących osób trzecich*. Zważywszy jednak na nadal bardzo ograniczony zakres czynności, jakie podejmuje się w toku zwykłego postępowania, przepis ten nie powinien mieć częstego zastosowania i należy go raczej traktować jako wyrażenie ogólnej intencji projektodawców, aby zabezpieczyć prawa osób trzecich, których dane gromadzone są w ramach procedur określonych w ustawie (vide także art. 24 ust. 9 ustawy).

[4] Zażalenie na postanowienie o zawieszeniu postępowania – art. 27 ust. 4, kontrola w zakresie prawidłowości postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego – art. 12 ust. 3 ustawy.

Zmiany wprowadzone w przepisach odnoszących się do udostępniania akt postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego mają zatem charakter porządkowy i stanowią dostosowanie do generalnych zmian w systemie. Należy jednak zwrócić uwagę na nowe przepisy wprowadzające dodatkowe zabezpieczenia, takie jak zdecydowane ograniczenie możliwości dokonania przeglądu akt postępowań przeprowadzonych przez służby wywiadowcze i kontrwywiadowcze, ograniczenie możliwości dokonania przeglądu akt zwykłego postępowania sprawdzającego tylko do przypadków kolejnego postępowania prowadzonego wobec tej samej osoby czy też brak dostępu osoby sprawdzanej do danych osób trzecich zgromadzonych w aktach przeprowadzonego wobec tej osoby postępowania. Nie wszystkie z tych zmian znalazły uznanie w doktrynie[5].

Jako niezwykle istotne należy ocenić określenie w art. 72 ust. 6 minimalnego okresu przechowywania akt zakończonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego (20 lat) i wskazanie na zastosowanie w tym zakresie przepisów ustawy o narodowym zasobie archiwalnym. Powinno to jednoznacznie wykluczyć odnotowane w ostatnich latach sytuacje sprzecznego z prawem brakowania przez niektórych pełnomocników ochrony akt postępowań sprawdzających po zakończeniu pracy danej osoby w jednostce organizacyjnej lub upływie ważności poświadczenia bezpieczeństwa wydanego na podstawie przeprowadzonego zwykłego postępowania sprawdzającego.

Dodano także, że akta zakończonych zwykłych postępowań sprawdzających mogą być przechowywane nie tylko przez pełnomocnika ochrony (jak to było do tej pory), ale także w pionie ochrony, co umożliwia racjonalne postępowanie z aktami, zwłaszcza w dużych jednostkach, w których do informacji niejawnych o klauzuli „poufne" dopuszczonych zostało kilkaset osób. Zdarzało się bowiem, że na stanie ewidencyjnym pełnomocnika ochrony pozostawało kilkanaście tysięcy dokumentów tylko dlatego, że jedynie pełnomocnik mógł – zgodnie z art. 42 ust. 3 ustawy z 1999 r. – przechowywać akta zwykłych postępowań sprawdzających przeprowadzonych wobec osób z danej jednostki organizacyjnej. Z tych względów rozliczanie takiego pełnomocnika w przypadku jego odejścia ze stanowiska było niejednokrotnie bardzo czaso- i pracochłonnym obowiązkiem.

W art. 72 ust. 7 ustawy utrzymano sprawdzony przepis nakładający na ABW i SKW obowiązek przejmowania – w przypadku braku następcy prawnego – akt postępowań sprawdzających z jednostek organizacyjnych, które uległy rozwiąza-

[5] S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz.* Warszawa 2010, Wydawnictwo LexisNexis, s. 279.

niu, zniesieniu, likwidacji, przekształceniu i reorganizacji. Tym samym pełnomocnik ochrony nie ma prawa przekazywać akt postępowań sprawdzających do archiwum zakładowego lub innego podmiotu zajmującego się składowaniem akt[6].

Odmiennie niż w ustawie z 1999 r. uregulowano zasady prowadzenia przez ABW i SKW ewidencji osób uprawnionych – na podstawie przepisów ustawy – – do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej oraz osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa.

Przede wszystkim przesądzono, że ABW i SKW prowadzą – każda we własnym zakresie – jedną ewidencję dotyczącą bezpieczeństwa osobowego, niezależnie od podstawy dostępu lub braku dostępu do informacji niejawnych. Wcześniej obowiązek gromadzenia niezbędnych danych wynikał z dwóch przepisów: art. 42 ust. 5 (dot. wydanych poświadczeń bezpieczeństwa i odmów wydania poświadczeń bezpieczeństwa) oraz art. 49 ust. 1 (dot. wydanej zgody na udostępnienie informacji) ustawy z 22 stycznia 1999 r.

Z analizy treści przepisów ustawy, m.in. art. 73 ust. 1, w związku z art. 15 ust. 1 pkt. 8 i 9, wynika, że pełnomocnicy ochrony powinni przekazywać do ewidencji prowadzonych przez ABW i SKW dane dotyczące osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych na podstawie przepisów ustawy, tzn. osób:

- wobec których przeprowadzono postępowanie sprawdzające i wydano poświadczenie bezpieczeństwa,
- które przedstawiły w nowym miejscu pracy, pełnienia służby lub wykonywania czynności zleconych ważne, aktualne i odpowiednie poświadczenie bezpieczeństwa (zgodnie z art. 34 ust. 1 ustawy),
- które uzyskały dostęp do informacji niejawnych o klauzuli „poufne" i wyższej na podstawie pozwolenia właściwego organu zgodnie z art. 34 ust. 5, 6 i 9 ustawy.

W art. 73 ust. 1 ustawy jednoznacznie wskazano, że ewidencja ta nie dotyczy osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w podmiotach, o których mowa w art. 23 ust. 5 ustawy. W ten sposób usankcjonowano występującą od 1999 r. praktykę. Organy i służby wymienione w art. 30 ustawy z 1999 r. nie przekazywały służbom ochrony państwa informacji niezbędnych do prowadzenia ewidencji, o której mowa w art. 42 ust. 5 tej ustawy, opierając

[6] Tamże, s. 279.

się na wykładni, że ich nie dotyczy obowiązek, określony w art. 48 ust. 2 ustawy z 1999 r., gdyż został on nałożony na pełnomocników ochrony, a nie na przedmiotowe organy i służby. Wyłączenie zawarte w art. 73 ust. 1 ustawy wyklucza zatem wszelkie wątpliwości w tej kwestii. Należy przy tym pamiętać, że rozwiązanie to stanowi jeden z elementów nowego, jednoznacznego określenia odpowiedniości poświadczeń wydanych w trybie art. 23 ust. 5 ustawy.

Ustawodawca zdecydował ponadto o ograniczeniu danych, które ABW i SKW mogą gromadzić w ramach ewidencji, o której mowa w art. 73 ust. 1 ustawy. Zrezygnowano m.in. z podawania *sygnatury postępowania*, co było konieczne z uwagi na fakt, iż żaden przepis ustawy (podobnie jak ustawy z 1999 r.) nie nakazuje stosowania sygnatury i w ogóle brak jest definicji tego pojęcia. Informacje na temat *daty wydania i numeru poświadczenia bezpieczeństwa* zastąpiono danymi dotyczącymi *określenia dokumentu kończącego procedurę, daty wydania i numeru*, co było niezbędne, gdyż ewidencja dotyczy nie tylko wydanych poświadczeń bezpieczeństwa, ale także decyzji o odmowie wydania i cofnięciu poświadczenia bezpieczeństwa.

Rezygnacja z innych danych, takich jak *data objęcia stanowiska*, *określenie, z dostępem do jakich informacji niejawnych łączy się to stanowisko* stanowi wprost konsekwencję ostatecznego odejścia od powiązania zasady *need to know* ze stanowiskiem służbowym, które musiało być wpisane do wykazu określonego przez kierownika jednostki organizacyjnej, aby dana osoba miała dostęp do informacji niejawnych[7].

Na takim samym poziomie utrzymano ochronę danych gromadzonych w omawianych ewidencjach. Udostępnianie danych z ewidencji, prowadzonych przez ABW i SKW, oraz wykazów prowadzonych przez pełnomocników ochrony, na podstawie art. 15 ust. 1 pkt 8 ustawy, ograniczono do przypadków analogicznych jak przesłanki udostępnienia do wglądu lub przekazania akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego.

Wydaje się, że zmiany wprowadzone w ustawie w zakresie przepisów odnoszących się do postępowania z materiałami i danymi zgromadzonymi w związku z postępowaniami sprawdzającymi i kontrolnymi postępowaniami sprawdzającymi

[7] Związek taki w *Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* wziął się z obowiązku wynikającego z art. 26:
Art. 26. 1. Kierownik jednostki organizacyjnej określi, z zastrzeżeniem ust. 2, stanowiska lub rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności.
2. Rada Ministrów określi, w drodze rozporządzenia, stanowiska i rodzaje prac zleconych w organach administracji rządowej, których wykonywanie w tych organach może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową (art. 26 ust. 2 został uchylony w 2005 r. – Dz.U. z 2005 r., Nr 85, poz. 727*).*

oraz postępowaniami bezpieczeństwa przemysłowego rzeczywiście doprowadziły do uproszczenia istniejącego systemu i jego aktualizacji.

Ustawodawca utrzymał rozwiązania sprawdzone w praktyce na przestrzeni ostatnich lat, których stosowanie nie wywoływało kontrowersji, takich jak zamknięty katalog warunków dostępu do akt postępowań sprawdzających i danych zgromadzonych w ewidencjach czy też przejmowanie przez ABW i SKW akt postępowań z jednostek likwidowanych i niemających następcy prawnego.

Wprowadzono unormowania, które są konsekwencją zmian systemu ochrony informacji niejawnych, w innych jego elementach składowych. Należy w tym miejscu zwrócić uwagę nie tylko na nowe podejście do udostępniania akt procedur przeprowadzonych przez ABW i SKW, ale także AW i SWW oraz na zmianę zakresu gromadzonych danych ze względu na rezygnację z tworzenia wykazów stanowisk, związanych z dostępem do informacji niejawnych.

Za szczególnie cenne należy uznać zmiany, na których potrzebę od wielu lat wskazywali przedstawiciele jednostek będących podmiotami ustawy, z uwagi na nieprecyzyjność dotychczasowych przepisów i możliwości ich niezgodnej z intencjami ustawodawcy interpretacji. Chodzi przede wszystkim o określenie sposobu postępowania z aktami po zakończeniu postępowania, zwłaszcza powiązanie tego zagadnienia z przepisami ustawy o narodowym zasobie archiwalnym, określenie minimalnego okresu przechowywania i umożliwienie ich przechowywania w pionie ochrony danej jednostki.

Podkreślić także należy znaczenie drobnych zmian, które jednak przyczyniają się do racjonalności systemu ochrony informacji niejawnych w obszarze postępowania z aktami procedur i danymi z ewidencji. Nie przypadkiem bowiem akta postępowań przeprowadzonych przez pełnomocnika ochrony udostępniane są do wglądu osobie sprawdzanej po zakończeniu postępowania, podczas gdy w przypadku akt postępowań przeprowadzonych przez organy i służby uprawnione do realizacji poszerzonych postępowań sprawdzających, do których osoby sprawdzane nie mają wglądu, warunek zakończenia postępowania nie występuje. Brak zastrzeżenia, że prawo wglądu przez osobę sprawdzaną w akta prowadzonego wobec niej, ale tylko zakończonego zwykłego postępowania sprawdzającego, powodowałoby de facto czynny udział strony na każdym etapie procedury i mogłoby uniemożliwić pełnomocnikowi ochrony przeprowadzenie skutecznego postępowania.

Należy jeszcze raz podkreślić istotę zmian wynikających z ogólnych zasad tworzenia prawa, które mają zabezpieczać system przed ewentualnymi nadużyciami. W tym przypadku chodzi o wyłączenie możliwości udostępnienia danych doty-

czących osób trzecich, zgromadzonych w aktach zwykłych postępowań sprawdzających, oraz nakaz *niezwłocznego* zwrotu akt po ich wykorzystaniu.

Biorąc powyższe pod uwagę należy pozytywnie ocenić nowe przepisy odnoszące się do postępowania z materiałami i danymi zgromadzonymi w związku z postępowaniami sprawdzającymi i kontrolnymi postępowaniami sprawdzającymi oraz postępowaniami bezpieczeństwa przemysłowego, zarówno w kontekście ich spójności z innymi przepisami ustawy, jak też funkcjonalności zastosowanych zabezpieczeń odnoszących się do przetwarzania informacji uzyskanych w toku tych procedur.

Sylwia Stefaniak

Postępowanie sprawdzające a instytucja odstąpienia od wymierzenia kary w postępowaniu karnym

Niniejszy artykuł dotyczy problematycznego zagadnienia odstąpienia od wymierzenia kary w postępowaniu sprawdzającym, uregulowanym ustawą o ochronie informacji niejawnych. Odstąpienie od wymierzenia kary daje możliwość wydania orzeczenia skazującego za przestępstwo popełnione w specyficznych, nietypowych okolicznościach. Instytucja ta uregulowana jest przepisami kodeksu karnego oraz kodeksu karnego skarbowego. Sąd, negatywnie oceniając popełniony czyn, może postanowić, iż niecelowe staje się ukaranie sprawcy i odstąpić od wymierzenia kary lub środka karnego. Odstąpienie od wymierzenia kary często stwarza w postępowaniu sprawdzającym praktyczne problemy interpretacyjne. Celem artykułu jest wyjaśnienie pojęcia kary, środków karnych i instytucji odstąpienia od wymierzenia kary, następnie wskazanie, jakie są przypadki jej występowania i kiedy następuje zatarcie skazania, a w dalszej kolejności przedstawienie konsekwencji jej wystąpienia w postępowaniu sprawdzającym oraz w kontrolnym postępowaniu sprawdzającym. Przeprowadzona wykładnia przepisów prawa, normujących odstąpienie od wymierzenia kary, odnosi się do najistotniejszych wątpliwości występujących podczas przeprowadzania postępowania sprawdzającego zarówno w kontekście przepisów poprzedniej ustawy o ochronie informacji niejawnych, jak i nowej regulacji z 5 sierpnia 2010 r.

Uwagi wstępne dotyczące kary i środków karnych

Słowo „kara" posiada bardzo rozległy zakres semantyczny i może być różnie definiowane.

Nie ulega wątpliwości, iż kara jest integralną częścią określonej kultury i można w niej odnaleźć wiele założeń aksjologicznych dotyczących wizji człowieka i społeczeństwa. Określa ona również podstawy normatywne ładu społecznego w kontekście dywagacji na temat zła i cierpienia[1]. Działania społeczne określane mianem kary polegają na świadomym wyrządzeniu przykrości osobie karanej, to zaś nieuchronnie domaga się wyjaśnienia, usprawiedliwienia i legitymizacji[2].

[1] J. Utrat-Milecki, *Podstawy penologii. Teoria kary*, Warszawa 2006, Wydawnictwo Uniwersytetu Warszawskiego, s. 48.

[2] Tamże, s. 153.

W celu uzyskania odpowiedniego wyobrażenia o pojęciu kary należy skoncentrować się na dwóch założeniach. Pierwsze z nich wiąże się z usprawiedliwianiem zastosowania kary, drugie zaś z jego istotą. Usprawiedliwianie wiąże się z koniecznością karania za naruszenie dóbr prawnych, tym samym naruszenie porządku prawnego[3], w celu zapewnienia harmonijnego funkcjonowania społeczeństwa. Karanie za czyny naruszające normy prawne obowiązujące w tej wspólnocie to konieczny warunek przestrzegania tych norm. Rezygnacja z kary oznaczałaby bowiem rezygnację z prawa i ograniczanie się jedynie do regulacji współżycia społecznego za pomocą norm etycznych. Kara jest też niezbędna, by czynić zadość społecznemu zapotrzebowaniu na sprawiedliwość w stosunkach międzyludzkich oraz w relacji obywatele – państwo. Jej istota wiąże się z przypisywaniem sprawcy czynu publicznej oceny z powodu zawinionego przez niego naruszenia prawa. Należy zgodzić się ze stwierdzeniem, iż kryminalizacja jest uzasadniona, jeśli z punktu widzenia ochrony dobra prawnego jest konieczna (zasada subsydiarności) i efektywna (jest zdatnym środkiem do ochrony danego dobra prawnego), a jej rozmiar jest adekwatny do wartości tego dobra[4].

Wyróżnia się dwa podstawowe cele kary: odpłatę za uczynione zło, które ma doprowadzić do swoistego wyrównania naruszenia prawa – *malum passionis propter malum actionis* (kara albo celowo, albo niezamierzenie, wyrządza człowiekowi pewną dolegliwość za uczynione zło i sama w sobie jest złem – przyp. red.) oraz zapobieganie popełnienia przez sprawcę lub innych obywateli przestępstw w przyszłości – *nemo prudens punit, quia peccatum est, sed ne peccetur*[5] (nikt rozumny nie karze dlatego, że popełniono przewinienie, lecz dlatego, by nie popełniono – przyp. red.). Współcześnie dominującą rolę w zakresie prewencyjnego oddziaływania kary na społeczeństwo zyskała pozytywna prewencja generalna (integrująca). Karanie ma zarówno stabilizować i internalizować normy prawa karnego, jak również ułatwiać przyswajanie ich przez społeczeństwo oraz budować zaufanie społeczeństwa do działania wymiaru sprawiedliwości. Ponadto ważne staje się kształtowanie świadomości i zapewnienie zadośćuczynienia poczuciu społecznej sprawiedliwości, spełniającej funkcję integrującą, z którą wiąże się najczęściej uzasadnienie systemu sankcji karnych[6].

Na potrzeby niniejszego artykułu przyjęto wykładnię kary stosowaną w prawie karnym i interpretowanie jej jako kary kryminalnej. Według Lecha Gardockiego *karą kryminalną jest osobista dolegliwość ponoszona przez sprawcę, jako od-*

[3] K. Buchała, A. Zoll, *Kodeks karny: część ogólna: komentarz do art. 1-116 kodeksu karnego*, tom I, Kraków 2000, Zakamycze, s. 299.

[4] M. Dąbrowska-Kardas, *Kara jako konflikt dóbr i kolizja norm*, „Przegląd Sejmowy" 1996, z. 4, s. 32.

[5] K. Buchała., A. Zoll, *Kodeks karny* ..., s. 301.

[6] Tamże, s. 305.

płata za popełnione przestępstwo, wyrażająca potępienie popełnionego przez niego czynu i wymierzana w imieniu państwa przez sąd[7]. Karą kryminalną nazywane są także działania społeczne ze sfery kontroli społecznej zaspokajające potrzeby osób i zbiorowości w zakresie poczucia ładu społecznego, sprawiedliwości i bezpieczeństwa, posiadające zasadę naczelną, czyli zamiary i cele, które stanowią podstawę ich racjonalizacji, normy oraz personel i urządzenia materialne, a także funkcje społeczne, rozumiane jako ich uświadomione i nieuświadomione konsekwencje, podjęte w formach organizacyjnych i podlegających instytucjonalizacji w przepisach prawa i decyzjach sądów oraz innych uprawnionych organów państwa[8].

W polskim prawie katalog kar zawarty jest w art. 32 *Ustawy z dnia 6 czerwca 1997 roku Kodeks karny*[9], do którego zaliczono następujące kary:

1) grzywnę,
2) ograniczenie wolności,
3) pozbawienie wolności,
4) 25 lat pozbawienia wolności,
5) dożywotnie pozbawienie wolności.

Kolejność kar ma na celu wyrażanie preferencji ustawodawcy co do ich stosowania. Pierwszeństwo mają mianowicie kary niezwiązane z pozbawieniem wolności[10]. Zgodnie bowiem z założeniami nowej polityki kryminalnej, a przede wszystkim z zasadą *ultima ratio* (ostatni argument – przyp. red.) kary pozbawienia wolności, dominującą rolę w zwalczaniu przestępczości powinny pełnić kary inne niż kara pozbawienia wolności, a więc kara grzywny, ograniczenia wolności bądź kara pozbawienia wolności z warunkowym zawieszeniem[11].

Oprócz katalogu kar ustawodawca wprowadził także w art. 39 kk wykaz środków karnych. Dominującymi funkcjami środków karnych jest prewencja i kompensacja[12]. Środki karne można podzielić na wymierne w czasie (pozbawie-

---

[7] L. Gardocki, *Prawo karne*, Warszawa 2002, C.H. Beck, s. 150.

[8] J. Utrat-Milecki, *Podstawy penologii* ..., s. 78.

[9] *Ustawa z dnia 6 czerwca 1997 roku Kodeks karny* (Dz.U. z 1997 r., Nr 88, poz. 553 z późn. zm.) – stan prawny wszystkich podanych aktów na dzień 10 września 2010 r.

[10] L. Gardocki, *Prawo karne* ..., s. 153.

[11] Z. Sienkiewicz, *Kodeks karny. Komentarz,* Warszawa 2008, Wydawnictwo Prawnicze LexisNexis, s. 1291.

[12] M. Szewczyk, *System środków karnych w projekcie nowego kodeksu karnego* (w:) *Problemy kodyfikacji prawa karnego. Księga ku czci Profesora M. Cieślaka*, red. S. Waltoś, Kraków 1993, Uniwersytet Jagielloński, s. 153.

nie praw i zakazy wymienione w art. 39 pkt. 1-3 kk[13]) i środki karne jednorazowe (art. 39 pkt 4-8 kk[14]). Środki karne wymierne w czasie określone w art. 39 pkt. 2, 2d, 2e i 3 orzeka się na okres od roku do lat 10, określone w art. 39 pkt. 2a i 2b orzeka się na okres od roku do lat 15, a zakaz wymieniony w art. 39 pkt. 2c orzeka się w latach od 2 do 6 (art. 43 § 1 kk[15]). Okres ten biegnie od uprawomocnienia się orzeczenia, z tym że nie biegnie on w czasie odbywania kary pozbawienia wolności, chociażby orzeczonej za inne przestępstwo (art. 43 § 2 kk). Wskazano między innymi następujące środki karne:

1) pozbawienie praw publicznych,

2) zakaz zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej,

3) zakaz prowadzenia działalności związanej z wychowaniem, leczeniem, edukacją małoletnich lub z opieką nad nimi,

4) obowiązek powstrzymania się od przebywania w określonych środowiskach lub miejscach, zakaz kontaktowania się z określonymi osobami, zakaz zbliżania się do określonych osób lub zakaz opuszczania określonego miejsca pobytu bez zgody sądu,

5) zakaz prowadzenia pojazdów,

6) przepadek,

7) obowiązek naprawienia szkody lub zadośćuczynienie za doznaną krzywdę,

8) świadczenie pieniężne,

9) podanie wyroku do publicznej wiadomości.

---

[13] Art. 39 pkt 2b kk zmieniony przez art. 5 pkt 1 lit. a) *Ustawy z dnia 10 czerwca 2010 r. o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych innych ustaw* (Dz.U. z 2010 r., Nr 125, poz. 842) z dniem 1 sierpnia 2010 r.

[14] Art. 39 pkt 5 kk zmieniony przez art. 1 pkt 8 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw* (Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r.

[15] Art. 43 § 1 kk zmieniony przez art. 1 pkt 9 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy...* (Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r. i art. 5 pkt 3 *Ustawy z dnia 10 czerwca 2010 r. o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych innych ustaw* (Dz.U. z 2010 r., Nr 125, poz. 842) z dniem 1 sierpnia 2010 r.

Oprócz odpowiedzialności karnej ustawodawca wyróżnił także odpowiedzialność karną za przestępstwo skarbowe. Przewidziane kary za przestępstwa skarbowe wymienione są w art. 22 § 1 *Ustawy z dnia 10 września 1999 r. Kodeks karny skarbowy* (kks)[16] i obejmują:

1) karę grzywny w stawkach dziennych,
2) karę ograniczenia wolności,
3) karę pozbawienia wolności.

Katalog kar jest ułożony według abstrakcyjnie ujętego stopnia dolegliwości: od kary grzywny, do najsurowszej – pozbawienia wolności, co jest tożsame z katalogiem kar wskazanych w kodeksie karnym. Ten układ ma dodatkowe uzasadnienie ze względu na wyraźny priorytet środków mających charakter dolegliwości ekonomicznej za przestępstwa skarbowe[17].

Wymienionych w art. 22 § 2 kks środków karnych nie należy traktować jako formy kary, lecz jako środki represyjne orzekane oprócz kary[18]. Środki karne wyróżnione w kodeksie karnym skarbowym, tak jak i w kodeksie karnym, można podzielić na wymierne w czasie (art. 22 § 2 pkt 5, 7 i 8 kks) i środki karne jednorazowe (art. 22 § 2 pkt 1- 4a i 6 kks). Środki karne wymierne w czasie wymienione w art. 22 § 2 pkt. 5 i 7 kks orzeka się w latach, od roku do lat 5 – art. 34 § 4 kks. Środkami karnymi są między innymi:

1) dobrowolne poddanie się odpowiedzialności,
2) przepadek przedmiotów,
3) przepadek korzyści majątkowej,
4) zakaz prowadzenia określonej działalności gospodarczej, wykonywania określonego zawodu lub zajmowania określonego stanowiska,
5) podanie wyroku do publicznej wiadomości,
6) pozbawienie praw publicznych,
7) środki związane z poddaniem sprawcy próbie.

---

[16] *Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy* (Dz.U. z 2007 r., Nr 111, poz. 765 z późn. zm.).

[17] J. Michalski, *Komentarz do kodeksu karnego skarbowego. Tytuł I „Przestępstwa skarbowe i wykroczenia skarbowe"*, Warszawa 2000, Wydawnictwo Prawnicze, s. 226.

[18] B. Kurzępa, W. Kotowski, *Najnowsze wydanie: Kodeks karny skarbowy. Komentarz,* Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, s. 640.

Istotne staje się podkreślenie, iż w przypadku, gdy sąd zezwoli na dobrowolne poddanie się odpowiedzialności, to prawomocne orzeczenie nie podlega wpisowi do Krajowego Rejestru Karnego, choć skutki prawne takiego orzeczenia są identyczne jak prawomocnego orzeczenia kończącego proces karny[19].

Środki karne, podobnie jak kary, zawierają w sobie element dolegliwości. Treść ich odpowiada zatem treści kary[20].

Przykładem negatywnych konsekwencji prawnych skazania są bezsprzecznie przepisy nowej *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[21], zwanej dalej nową UOIN, ale także były nimi przepisy poprzedniej *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*[22], zwanej dalej poprzednią UOIN.

W poprzedniej ustawie użyte sformułowania często stawały się niejasne i wymagały wnikliwej wykładni. Z tego powodu zrodziła się potrzeba uaktualnienia, uporządkowania i uproszczenia przepisów. Rozpoczęto proces kodyfikacyjny[23], którego rezultatem jest wprowadzenie nowelizacji sensu largo dotychczasowego aktu prawnego.

Wśród problematycznych zagadnień, wymagających zmiany lub sprecyzowania, znalazły się także kwestie związane z prawomocnym skazaniem. Zasadne jest zatem przedstawienie poniżej interpretacji przepisów prawa, które faktycznie przyczyniły się do przekształcenia treści ustawy o ochronie informacji niejawnych w omawianym zakresie.

Zgodnie z treścią art. 28 ust. 1 pkt 2 poprzedniej UOIN nie mogły być dopuszczone do pracy lub pełnienia służby na stanowisku albo do wykonywania prac zleconych, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę państwową (tj. informacji oznaczonych klauzulą „tajne" lub „ściśle tajne" w myśl nowej UOIN), osoby skazane prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego, także popełnione za grani-

[19] Tamże.

[20] M. Szewczyk, *System środków karnych...*

[21] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228).

[22] *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. z 2005 r., Nr 196, poz. 1631 z późn. zm.).

[23] Treść projektu ustawy w formie druku sejmowego nr 2791 dostępny na stronie www.sejm.gov.pl/Prace Sejmu/Proces legislacyjny – wyszukiwanie http://orka.sejm.gov.pl/proc6.nsf [dostęp dnia 10 września 2010 r.] Tekst ustawy uchwalony ostatecznie po rozpatrzeniu poprawek Senatu http://orka.sejm.gov.pl/proc6.nsf/ustawy/2791-u.htm [dostęp dnia 10 września 2010 r.]. Przedmiotowa ustawa została podpisana przez Prezydenta w dniu 30 sierpnia 2010 r.

cą. Ustawodawca określił, iż prawomocne skazanie stawało się obligatoryjną przesłanką odmowy wydania poświadczenia bezpieczeństwa lub jego cofnięcia. Natomiast na podstawie art. 37 ust. 9 poprzedniej UOIN pełnomocnik ochrony lub służba ochrony państwa, w przypadkach postępowań określonych w ust. 2 i 3, mogły odmówić wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnionym za granicą. W tym przypadku istniała fakultatywność decyzji.

Co ważne, w poprzedniej UOIN istniała pewna niekonsekwencja redakcyjna, gdyż w art. 28 ust. 1 pkt 2 była mowa generalnie o przestępstwie umyślnym, ściganym z oskarżenia publicznego, także popełnionym za granicą, natomiast już w art. 36 ust. 2c pkt 3 ustawodawca wprowadził rozróżnienie na przestępstwo lub przestępstwo skarbowe, umyślne, ścigane z oskarżenia publicznego.

Skazanie prawomocnym wyrokiem dotyczy zarówno przestępstw karnych, jak i przestępstw skarbowych. W prawie karnym wyróżniono bowiem podział na przestępstwa karne i przestępstwa skarbowe. Podział ten jest wyraźnie stosowany w ustawach karnych, a sam ustawodawca konkretnie wskazuje, czy regulacja odnosi się tylko do przestępstw karnych, czy również odpowiednio do przestępstw skarbowych.

Wydaje się, iż w normie art. 28 ust. 1 pkt 2 poprzedniej UOIN, ale również w art. 37 ust. 9 poprzedniej UOIN, była mowa ogólnie o *przestępstwie*, które powinno odpowiadać definicji przedstawionej w art. 1 kk. Jednakże wątpliwości interpretacyjne budził właśnie art. 36 ust. 2c pkt 3 poprzedniej UOIN wprowadzający przywołane rozróżnienie przestępstw. Interpretując przedmiotowy przepis, przyjmowano, iż nie powinien mieć on zastosowania tylko w przypadku zawieszenia, ale także w stosunku do podejmowanej ewentualnej decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz decyzji o jego cofnięciu. Miała mieć tutaj zastosowanie zasada *a minore ad maius*, decyzja kończąca postępowanie w sprawie ma bowiem większe znaczenie niż postanowienie o jego zawieszeniu.

W doktrynie pojawił się pogląd, iż jeżeli zachodzi potrzeba dopuszczenia do informacji niejawnych stanowiących tajemnicę państwową – według nowej UOIN oznaczonych klauzulą „tajne" lub „ściśle tajne" – osoby niespełniającej wymagań wskazanych w art. 28 poprzedniej UOIN, można skorzystać z trybu przewidzianego w art. 49 poprzedniej UOIN – obecnie art. 34 ust. 5 i 9 nowej UOIN[24].

[24] T. Szewc, *Ochrona informacji niejawnych Komentarz*, Warszawa 2007, C.H.Beck, s. 140.

Z takim poglądem nie można się zgodzić, w przypadku bowiem spełnienia przesłanki z art. 28 ust. 1 pkt 2 poprzedniej UOIN, obligatoryjnie odmawiano wydania poświadczenia bezpieczeństwa, które miałoby upoważniać do dostępu do informacji niejawnych oznaczonych klauzulą „tajne" lub „ściśle tajne", a zatem stwierdzano, iż konkretna osoba sprawdzana nie może mieć w ogóle dostępu do informacji niejawnych i nie powinno być od tego wyjątków. Nie wydaje się również słuszne, iż w przypadku tajemnicy służbowej (oznaczonej klauzulą „poufne" i „zastrzeżone" w myśl nowej UOIN), jeżeli osoba sprawdzana została ukarana za przestępstwo umyślne ścigane z oskarżenia publicznego, to organy prowadzące postępowanie mają pełną swobodę decydowania, czy odmówić wydania poświadczenia bezpieczeństwa[25]. Fakultatywności odmowy wydania poświadczenia bezpieczeństwa nie można utożsamiać z dowolnością. Decyzja o wydaniu poświadczenia bezpieczeństwa uprawniającego do dostępu do tajemnicy służbowej – oznaczonej klauzulą „zastrzeżone" lub „poufne" – bądź też o odmowie wydania przedmiotowego poświadczenia, bądź też o cofnięciu takiego poświadczenia powinna być wydana po wnikliwej analizie stanu faktycznego oraz po przeprowadzeniu rozmowy wyjaśniającej z osobą sprawdzaną.

Tworząc przepisy nowej UOIN, bazowano na dorobku już dokonanych, także tych powyżej przedstawionych interpretacji. Dążąc do wyjaśnienia wątpliwości i sprecyzowania regulacji, zrezygnowano z obligatoryjności odmowy lub cofnięcia dostępu do informacji niejawnych i teraz, zgodnie z art. 30 ust. 2 i art. 33 ust. 1 nowej UOIN, skazanie prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe będzie stawało się przyczyną odmowy udzielenia dostępu do informacji niejawnych tylko wtedy, jeżeli czyn, za który nastąpiło skazanie, wywołuje uzasadnione wątpliwości, o których mowa w art. 24 ust. 2 i 3 nowej UOIN[26].

Ustawodawca, rezygnując z podziału na tajemnicę państwową oraz służbową i pozostając jedynie przy oznaczaniu informacji niejawnych poszczególny-

[25] Tamże, s. 175.

[26] Są to uzasadnione wątpliwości dotyczące uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej, zagrożenia ze strony obcych służb specjalnych w postaci werbunku lub nawiązania kontaktu, przestrzegania porządku konstytucyjnego, ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego lub postępowaniu sprawdzającym informacji mających znaczenie dla ochrony informacji niejawnych, wystąpienia okoliczności powodujących podatność na szantaż lub wywieranie presji, niewłaściwego postępowania z informacjami niejawnymi, poziomu życia wyraźnie przewyższającego uzyskiwane dochody, informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpływać na zdolność do wykonywania prac, uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

mi klauzulami tajności, odstąpił od podawania w różnych jednostkach redakcyjnych prawomocnego skazania jako przesłanki odmowy lub cofnięcia. Co więcej, ujednolicił zasady poprzez rezygnację z obligatoryjności wyłączenia dopuszczenia do klauzuli „ściśle tajne" lub „tajne", gdy wobec osoby sprawdzanej został wydany prawomocny wyrok za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą lub umyślne przestępstwo skarbowe. Niewątpliwie takie ujęcie przedmiotowej kwestii wprowadza uproszczenie i staje się bardziej klarowane oraz praktyczne.

Ciekawe jest, iż w nowej ustawie nie określono wyraźnie ewentualnych obostrzeń dotyczących dostępu do klauzuli „zastrzeżone". Trudna do wyobrażenia wydaje się jednak sytuacja, w której kierownik jednostki organizacyjnej, posiadając wiedzę lub uzasadnione podejrzenie o prawomocnym skazaniu za czyn wywołujący wątpliwości określone w art. 24 ust. 2 i 3 nowej UOIN, wyda upoważnienie do dostępu do przedmiotowych informacji.

Nie ulega wątpliwości, iż jeśli w toku dokonywanych w postępowaniu sprawdzeń organ prowadzący ustali, iż osoba została skazana prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego i figuruje w Krajowym Rejestrze Karnym[27], to istnieją podstawy do odmowy wydania poświadczenia bezpieczeństwa lub jego cofnięcia.

Często jednak problematyczne w praktyce staje się interpretowanie, w jaki sposób postępować w przypadku, gdy sąd orzekł o odstąpieniu od wymierzenia kary. Prawomocne orzeczenie sądu o odstąpieniu od wymierzenia kary lub środka karnego jest wpisywane do Krajowego Rejestru Karnego, co skutkuje uznaniem, iż osoba sprawdzana została prawomocnie skazana. W takich sytuacjach organ prowadzący stosowne postępowanie sprawdzające powinien skoncentrować się na ustaleniu, czy popełnione przestępstwo było przestępstwem umyślnym, ściganym z oskarżenia publicznego, a następnie ustalić okoliczności faktyczne sprawy i ewentualne występowanie wątpliwości co do dawania rękojmi zachowania tajemnicy.

Jeśli osoba sprawdzana nie figuruje w Krajowym Rejestrze Karnym, bo podlegała wyłączeniu z wpisu, jak jest w przypadku zezwolenia na dobrowolne poddanie się odpowiedzialności karnej skarbowej, to wydaje się, iż taką osobę należy uznać za niekaraną w powszechnym znaczeniu, staje się bowiem trudne do wykazania, iż wydano wobec niej taki wyrok.

---

[27] *Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym* (Dz.U. z 2008 r., Nr.50, poz. 292 z późn. zm.).

Instytucja odstąpienia od wymierzenia kary – zastosowanie w kodeksie karnym

Instytucja odstąpienia od wymierzenia kary stwarza możliwość wydania orzeczenia skazującego za przestępstwo popełnione w specyficznych, nietypowych okolicznościach, którego treść odpowiadać będzie zasadzie sprawiedliwości oraz spełni wyznaczone przez ustawodawcę cele kryminalno-polityczne[28]. Podstawą odstąpienia od kary może być niski stopień winy (np. przekroczenie granic obrony koniecznej – art. 25 § 2 lub stan wyższej konieczności – art. 26 § 3 kk), niski stopień społecznej szkodliwości czynu (np. usiłowanie nieudolne – art. 14 § 2 kk), wreszcie względy kryminalnopolityczne (np. przekroczenie granic obrony koniecznej – art. 25 § 3 kk[29]).

Odstąpienie od wymierzenia kary występuje w wypadkach wskazanych w ustawie. Ogólna podstawa odstąpienia od wymierzenia kary zamieszczona jest w art. 61 kk.

Odstąpienie od wymierzenia kary jest fakultatywne (art. 61 § 1 i § 2 oraz art. 59 kk[30]), choć do czasu nowelizacji kk z 5 listopada 2009 r. był jeden wyjątek, kiedy było ono obligatoryjne (art. 25 § 3 kk), tj. w razie przekroczenia granic obrony koniecznej w wyniku strachu lub wzburzenia. W przeciwieństwie do niepodlegania karze, sprawca nie jest automatycznie ex lege zwolniony z poniesienia kary (art. 17 § 1 pkt 4 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, zwanej dalej kpk[31]), lecz może to tylko nastąpić na mocy decyzji sądu wydającego wyrok skazujący sprawcę i stwierdzający jego winę w znaczeniu procesowym. Decyzja ta oznacza, że sąd, nie zmieniając negatywnej oceny popełnionego czynu, uważa za niecelowe ukaranie sprawcy[32].

Odstąpienie od wymierzenia kary jest możliwe również w wyniku określonym w art. 60 § 3 kk, czyli w stosunku do sprawcy współdziałającego z inny-

---

[28] K. Buchała, A. Zoll, *Kodeks karny* ..., s. 450

[29] Art. 25 § 3 kk zmieniony przez art. 1 pkt 2 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy...*(Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r.

[30] Art. 59 kk zmieniony przez art. 1 pkt 14 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy...* (Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r.
Art. 59. § 1. Jeżeli przestępstwo jest zagrożone karą pozbawienia wolności nieprzekraczającą 3 lat albo karą łagodniejszego rodzaju i społeczna szkodliwość czynu nie jest znaczna, sąd może odstąpić od wymierzenia kary, jeżeli orzeka równocześnie środek karny, a cele kary zostaną przez ten środek spełnione.
§ 2.Przepisu § 1 nie stosuje się do sprawcy występku o charakterze chuligańskim.

[31] *Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego* (Dz.U. z 1997 r.,, Nr 89, poz. 555 z późn. zm.).

[32] L. Gardocki, *Prawo karne ...,* s.172.

mi osobami w popełnieniu przestępstwa, jeżeli ujawni on wobec organu powołanego do ścigania przestępstw informacje dotyczące osób uczestniczących w popełnieniu przestępstwa oraz istotne okoliczności jego popełnienia. Co ważne, zgodnie z art. 61 § 1 kk, w takiej sytuacji bierze się pod uwagę, czy rola sprawcy w popełnieniu przestępstwa była podrzędna, a przekazane informacje przyczyniły się do zapobieżenia popełnieniu innego przestępstwa. Przesłanka dotycząca podrzędnej roli sprawcy w popełnieniu przestępstwa oznacza, że możliwość odstąpienia od wymierzenia kary nie obejmuje osób kierujących grupą przestępczą, organizujących przestępne współdziałanie lub niepełniących takiej funkcji formalnie, lecz odgrywających zasadniczą rolę w realizacji przestępstwa.

Odrębną podstawę odstąpienia od wymierzenia kary zawiera art. 59 kk[33]. Wskazuje on, iż jeżeli przestępstwo jest zagrożone karą pozbawienia wolności nieprzekraczającą 3 lat albo karą łagodniejszego rodzaju i społeczna szkodliwość czynu nie jest znaczna, sąd może odstąpić od wymierzenia kary, jeżeli orzeka równocześnie środek karny, a cele kary zostaną przez ten środek spełnione. Chodzi tu o cele wymienione w art. 53 kk, tj. cele zapobiegawcze i wychowawcze związane z prewencją indywidualną oraz potrzeby w zakresie kształtowania świadomości prawnej społeczeństwa, tj. pozytywną prewencję ogólną, ale również właściwości i warunki osobiste sprawcy oraz okoliczności popełnienia przestępstwa[34]. Sąd, odstępując od wymierzenia kary, uwzględnia także stopień społecznej szkodliwości czynu, mając na względzie art. 1 § 2 kk. Nie można jednak zapominać, iż przepisu 59 § 1 kk nie stosuje się do sprawcy występku o charakterze chuligańskim.

Odstąpienie od wymierzenia kary z jednoczesnym koniecznym wymierzeniem środka karnego (innego niż pozbawienie praw publicznych) może być też, zgodnie z art. 60 § 7 kk, jednym ze sposobów nadzwyczajnego złagodzenia kary.

Obligatoryjne odstąpienie od wymierzenia kary występowało wówczas, gdy sprawca przekroczył granice obrony koniecznej w wyniku strachu lub wzburzenia usprawiedliwionych okolicznościami zamachu – art. 25 § 3 kk[35]. W zmienionym stanie prawnym w takim przypadku nie będzie się w ogóle podlegać karze.

---

[33] Art. 59 kk zmieniony przez art. 1 pkt 14 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy...*(Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r.

[34] K. Buchała, A. Zoll, *Kodeks karny ...*,s. 432.

[35] Art. 25 § 3 kk zmieniony przez art. 1 pkt 2 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy* (Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kk z dniem 8 czerwca 2010 r.
§ 3. Nie podlega karze, kto przekracza granice obrony koniecznej pod wpływem strachu lub wzburzenia usprawiedliwionych okolicznościami zamachu. We wprowadzonej nowelizacji zrezygnowano ze zwrotu „Sąd odstępuje od kary", co może sugerować, iż jedyny dotychczas przypadek obligatoryjnego odstąpienia od kary został usunięty na rzecz depenalizacji przedmiotowego czynu, a to będzie skutkowało całkowitą fakultatywnością instytucji odstąpienia od kary.

Przyjmuje się, iż sąd, odstępując od wymierzenia kary, rezygnuje głównie z orzeczenia kar wymienionych w art. 32 kk, ale możliwe i stosowane jest również odstąpienie od wymierzenia środka karnego, chociażby jego orzeczenie było obowiązkowe.

Nie można jednak zapominać, iż zgodnie ze stanowiskiem Sądu Najwyższego[36] *odstąpienie przez sąd od obowiązku orzeczenia konkretnej kary (zasadniczej lub dodatkowej* – obecnie środka karnego – *np. na podstawie art. 56, art. 57 § 4 dawny kk) jest rozstrzygnięciem, które – w myśl art. 360 § 1 pkt 5 dawny kpk – powinno być zawarte w wyroku w postaci wyraźnego zapisu. Samo powołanie przepisu upoważniającego do podjęcia określonego rozstrzygnięcia nie jest wystarczające. Nie wystarcza również powołanie się na taki przepis w uzasadnieniu wyroku. Wskazać w nim bowiem należy, czym kierował się sąd podejmując konkretne rozstrzygnięcie (art. 372 § 2 dawny kpk)*.

Instytucja odstąpienia od wymierzenia od kary – zastosowanie w kodeksie karnym skarbowym

Instytucja odstąpienia od wymierzenia kary i środka karnego występuje również w kodeksie karnym skarbowym. Treść art. 19 kks stanowi samodzielną podstawę sądowego wymiaru kary o charakterze fakultatywnym, zawsze zależną od uznania sądu, mającą zastosowanie zarówno do sprawców przestępstw skarbowych, jak i wykroczeń skarbowych. Odstąpienie jest możliwe w przypadkach wskazanych w art. 19 § 1 pkt 1 i 2 kks, ale także w przepisach szczególnych kks, do których stosuje się odpowiednio przepisy kodeksu karnego.

W art. 19 § 1 kks przewidziano możliwość bezwarunkowego odstąpienia od wymierzenia kary lub środka karnego. Sąd jednak może to uczynić tylko wtedy, gdy w związku z tymi czynami nie nastąpiło uszczuplenie należności publicznoprawnej. Z omawianej instytucji można skorzystać także w sytuacji uregulowania uszczuplonej należności przed wydaniem orzeczenia[37]. Odstępując od kary, sąd może jednak orzec środek karny wymieniony w art. 22 § 2 pkt. 2-6 kks, jeżeli zachodzą warunki jego orzeczenia i cele kary zostaną przez ten środek spełnione.

Ponadto sąd może odstąpić od wymierzenia kary za przestępstwo skarbowe zagrożone karą pozbawienia wolności nieprzekraczającą 3 lata lub karą łagodniejszą, gdy stopień społecznej szkodliwości popełnionego czynu nie jest znaczny. Kryteria oceny szkodliwości określa art. 53 § 7 kks. Co istotne, szkodliwość musi

[36] Wyrok SN – Izba Wojskowa z dnia 17 marca 1988 r., WRN 4/88, LexPolonica nr 306818, Krakowskie Zeszyty Sądowe – dodatek 1993/6-8 poz. 7, OSNKW 1988/9-10 poz. 65.

[37] B. Kurzępa, W. Kotowski, *Najnowsze wydanie: Kodeks...* .

być większa niż znikoma, gdyż w przeciwnym wypadku – zgodnie z art. 1 § 2 kks – czyn taki nie stanowiłby przestępstwa skarbowego. Nie może to być także sytuacja, w której czyn zabroniony stanowi wypadek mniejszej wagi, gdyż wówczas sprawca ponosi odpowiedzialność za wykroczenie skarbowe.

Inna sytuacja została uregulowana w art. 19 § 4 kks, w którym przewidziano, iż w stosunku do nieobecnych sprawców orzeczenie co do kary, środka karnego lub innego środka można ograniczyć do przepadku przedmiotów. Dotyczy to jednak tylko postępowania w stosunku do sprawców, którzy przebywają stale poza granicami albo gdy nie można ustalić ich miejsca zamieszkania lub pobytu w kraju (art. 173 § 1 kks). Orzeczenie przepadku będzie możliwe tylko wtedy, kiedy środek ten grozi za popełnienie danego czynu.

W art. 19 § 4 kks wskazano, iż decyzja sądu ma charakter fakultatywny, ale podejmowana jest głównie ze względów pragmatycznych, wobec bowiem nieobecnego sprawcy niemożliwe staje się wykonanie kary lub innych środków karnych.

Przewidziana w art. 19 § 3 kks możliwość odstąpienia od orzeczenia środka karnego nie dotyczy przepadku przedmiotów, których wytwarzanie, posiadanie, obrót, przechowywanie, przewóz, przenoszenie lub przesyłanie jest zabronione, w takim bowiem przypadku jest ono obligatoryjne – art. 29 pkt 4 kks.

Konsekwencje odstąpienia od wymierzenia kary w postępowaniu sprawdzającym

Kara, a w konsekwencji wyrok skazujący określający jej rodzaj i wysokość, zawierają element potępienia sprawcy z powodu popełnienia przez niego czynu przestępnego. Osobą skazaną jest osoba, wobec której wydano prawomocny wyrok za popełnienie przestępstwa karnego lub przestępstwa karnego skarbowego, a także osoba, wobec której odstąpiono od wymierzenia kary bądź środka karnego. Osoba taka zostaje bowiem uznana za winną popełnienia przestępstwa, ale ze względu na przesłanki wskazane w kodeksie karnym lub w kodeksie karnym skarbowym (między innymi, gdy społeczna szkodliwość czynu nie jest znaczna bądź jeśli cele kary zostaną spełnione przez środek karny) stwierdzono, iż nie jest niezbędne wymierzenie jej kary czy – nawet we wskazanych ustawą przypadkach – środka karnego. Wyróżnia się następujące formy odstąpienia od wymierzenia kary:

1) odstąpienie od wymierzenia kary i obligatoryjne orzeczenie środka karnego – art. 59 § 1 kk, 60 § 7 kk, art. 36 § 1 pkt 2 kks,

2) odstąpienie od wymierzenia kary i fakultatywne odstąpienie od środka karnego, chociażby jego orzeczenie było obowiązkowe – art. 61 § 2 kk, art. 19 § 3 kks, 36 § 1 pkt 3 kks,

3) odstąpienie od wymierzenia kary i fakultatywne wymierzenie środka karnego – 61 § 1 kk,

4) odstąpienie od wymierzenia kary lub środka karnego, po spełnieniu dodatkowej przesłanki – art. 19 § 2 kks.

Warto podkreślić, iż odstąpienie od kary, tak jak inne orzeczenia kończące proces karny, będzie podlegało wpisowi do Krajowego Rejestru Karnego i może tu znaleźć zastosowanie instytucja zatarcia skazania.

Dla realizacji funkcji sprawiedliwościowej kary, a zwłaszcza dla prewencji generalnej, upowszechnia się informacje o skazaniu poprzez rejestrację w Krajowym Rejestrze Karnym[38]. Figurowanie w Krajowym Rejestrze Karnym, potwierdzające fakt skazania, i możliwość uzyskania wiedzy na ten temat przez członków społeczeństwa[39] są środkami niezbędnymi dla realizacji celów karania, a także jednym z elementów składających się na dolegliwość odpowiedzialności karnej. Po upływie określonego ustawowo czasu od wykonania, darowania lub przedawnienia kary lub środka karnego, znajomość faktu skazania przez inne osoby i zachowanie oficjalnej informacji o skazaniu w państwowym rejestrze przestają być potrzebne, ale mogą być również szkodliwe dla samego sprawcy czynu przestępczego. Mogą powodować bowiem wypominanie faktu popełnienia przestępstwa w nieskończoność, co – poza dolegliwością psychiczną – może również skutkować powstawaniem negatywnych konsekwencji w innych sferach życia, również w ubieganiu się o pracę związaną z dostępem do informacji niejawnych o określonej klauzuli tajności. Aby uniknąć takich niekorzystnych sytuacji, ustawodawca utworzył instytucję zatarcia skazania, która polega na przyjęciu pewnej fikcji prawnej. Fikcja ta polega na tym, że po spełnieniu określonych przesłanek uważa się osobę skazaną za niekaraną, natomiast wpis o skazaniu usuwa się z rejestru[40] – – art. 106 kk. Przypadki usunięcia danych z rejestru określa art. 14 ustawy o Krajowym Rejestrze Karnym. Zatarcie skazania oznacza, że w świetle prawa skazany uważany jest za niekaranego i może sam składać potwierdzające ten fakt oświadczenia woli. Nie można też wobec takiej osoby stosować ograniczeń, które prawo łączy z faktem skazania.

Zatarcie skazania następuje w niektórych sytuacjach *ex lege*. Jest tak w przypadku, gdy czyn objęty wyrokiem nie jest już zabroniony pod groźbą kary

[38] L. Gardocki, *Prawo karne ...,* s. 201.

[39] Określenie warunków uzyskania informacji z Krajowego Rejestru Karnego znajduje się w *Rozporządzeniu Ministra Sprawiedliwości z dnia 7 listopada 2003 r. w sprawie udzielania informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym* (Dz.U. z 2003 r., Nr 198, poz. 1930 z późn. zm.).

[40] L. Gardocki, *Prawo karne ...*,s.201.

(art. 4 § 4 kk oraz art. 2 § 6 kks), a także, gdy upłynęło 6 miesięcy od pomyślnego zakończenia okresu próby przy warunkowym zawieszeniu wykonywania kary (art. 76 § 1 kk).

W razie odstąpienia od wymierzenia kary, zatarcie skazania następuje z mocy prawa po upływie roku od dnia wydania prawomocnego orzeczenia – art. 107 § 5 kk i art. 20 § 2 kks[41].

Jeśli jednak orzeczono środek karny, zatarcie skazania nie może nastąpić przed jego wykonaniem, darowaniem albo przedawnieniem jego wykonania, z zastrzeżeniem art. 76 § 2 kk – art. 107 § 6 kk i art. 20 § 2 kks. Bieg terminów niezbędnych dla zatarcia skazania rozpoczyna się od wykonania lub darowania kary albo od przedawnienia jej wykonania (art. 103 kk i art. 45 § 1 kks), a także od daty uznania jej za wykonaną (art. 83, 84 i 84a kk). W art. 107 § 6 pominięto kwestię zatarcia skazania co do prawa prowadzenia pojazdów mechanicznych orzeczonego na zawsze. Oznacza to, że jest ono możliwe w wypadku darowania tej kary (środka) lub przedawnienia jej wykonania[42].

W razie skazania sprawcy z warunkowym zawieszeniem wykonania kary, skazanie ulega zatarciu z mocy prawa po upływie 6 miesięcy od zakończenia okresu próby – art. 76 § 1 kk. Jeżeli jednak wobec skazanego orzeczono grzywnę lub środek karny, zatarcie skazania nie może nastąpić przed ich wykonaniem, darowaniem albo przedawnieniem ich wykonania – art. 76 § 2 kk.

Bieg okresów wymaganych do zatarcia skazania rozpoczyna się od faktycznego odbycia kary, uznania jej za odbytą (art. 82 kk) lub wykonaną (art. 83 kk), zakończenia okresu, na jaki orzeczono środek karny, wykonania środka karnego lub uznania go za wykonany (art. 84 § 1 kk), od uiszczenia grzywny w całości lub jej umorzenia (art. 51 kodeksu karnego wykonawczego[43]), od daty wydania indywidualnego aktu łaski lub od daty określonej w ustawie o amnestii, wreszcie od przedawnienia wykonania kar lub środków karnych[44].

Ponieważ w przypadku odstąpienia od wymierzenia kary, czas oczekiwania na zatarcie skazania jest najkrótszy, wydaje się, iż ustawodawca nie uwzględnił tu wnioskowania o wcześniejsze zatarcie skazania. Nie można zapominać jednak

---

[41] Art. 20 § 2 kks zmieniony przez art. 4 pkt 1 *Ustawy z dnia 5 listopada 2009 r. o zmianie ustawy...* (Dz.U. z 2009 r., Nr 206, poz. 1589) zmieniającej kks z dniem 8 czerwca 2010 r.

[42] T. Bojarski, *Najnowsze wydanie: Kodeks karny. Komentarz*, Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, s. 784.

[43] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy* (Dz.U. z 1997 r., Nr 90, poz. 557 z późn. zm.)

[44] L. Wilk, *Kodeks karny. Komentarz,* Warszawa 2008, Wydawnictwo Prawnicze LexisNexis, s. 1291.

o art. 107 § 6 kk, który może istotnie przedłużyć zatarcie skazania. Mając bowiem na względzie terminy przedawnienia wykonania kary określone w art. 103 § 2 kk, w razie skazania na środek karny wymieniony w art. 39 pkt. 1-4 oraz 6 i 7 kk przedawnienie nastąpi po 10 latach od uprawomocnienia się wyroku skazującego, a w przypadku środka karnego wymienionego w art. 39 pkt 5, aż po 15 latach.

Zatarcie skazania następujące z mocy prawa nie wymaga oczywiście żadnej konstytutywnej decyzji, a jedynie stwierdzenia zaistnienia przesłanki formalnej i usunięcia karty karnej z rejestru skazanych. Sam wpis ma charakter deklaratoryjny. Nieusunięcie karty karnej z rejestru, mimo że skazanie uległo zatarciu, nie stanowi (podobnie jak np. niezarejestrowanie skazania) wyłącznego i niepodważalnego dowodu karalności (lub niekaralności) danej osoby. Ustalenia w tym względzie mogą być dokonywane na podstawie akt spraw i oceniane w drodze wykładni stosownych przepisów[45]. Co więcej, Naczelny Sąd Administracyjny uznał, iż *usunięcie danych z Krajowego Rejestru Karnego nie następuje w drodze decyzji administracyjnej. Czynność taka mieści się w zakresie art. 16 ust. 1 pkt 4 ustawy z dnia 11 maja 1995 r. o Naczelnym Sądzie Administracyjnym (Dz. U. z 1995, Nr 74, poz. 368 ze zm.) i podlega kontroli sądowej*[46].

***

Brak wskazania w ankiecie bezpieczeństwa osobowego faktu, iż wobec osoby sprawdzanej odstąpiono od wymierzenia kary stanowi okoliczność negatywnie wpływającą na ocenę dawania rękojmi zachowania tajemnicy. Podobnie jest w przypadku pojawienia się tej informacji, jako nowej okoliczności, powstałej już po wydaniu poświadczenia bezpieczeństwa, co może być podstawą wszczęcia postępowania kontrolnego – art. 33 ust 1 nowej UOIN (art. 45 ust. 1 poprzedniej UOIN). Można wnioskować, iż obecnie obowiązujące przepisy regulujące ochronę informacji niejawnych, analogicznie jak w kodeksie karnym i kodeksie karnym skarbowym, przyjmują, iż zarówno kara, jak i środki karne powinny wiązać się z dolegliwością dla sprawcy odczuwaną w różnych sferach życia, ale również wyrażają potępienie sprawcy, co znajduje wyraz w zerwaniu z nim dotychczasowych więzi społecznych i wpływa niekorzystnie na możliwość i sposób realizacji jego uprawnień polegających w danym przypadku na dostępie do informacji niejawnych. Warto podkreślić, iż dotychczas osobie, która została skazana prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, chcącej wykonywać pracę lub pełnić służbę łączącą się z dostępem do klauzuli „ściśle tajne" lub „tajne", należało obligatoryjnie odmówić wydania poświadczenia, a gdy osoba posiadała już poświadczenie, należało je cofnąć – art. 28 ust. 1 pkt 2 poprzed-

[45] S. Zimoch, *Istota i znaczenie instytucji zatarcia skazania,* Warszawa 1997, „Biblioteka Palestry", s. 7.

[46] Wyrok Naczelnego Sądu Administracyjnego z dnia 20 marca 2003 r., II S.A. 2558/2002.

niej UOIN. Mimo, że w przypadku dostępu do dotychczasowej tajemnicy służbowej decyzja o odmowie lub cofnięciu poświadczenia była fakultatywna, to nie ulega wątpliwości, iż prawomocne skazanie było i jest nadal poważnym utrudnieniem dla osób sprawdzanych i istotnie wpływa na ocenę dawania rękojmi zachowania tajemnicy.

Czasami jednak wskazane w poprzedniej ustawie formy zakończenia postępowania sprawdzającego mogły wydawać się zbyt radykalne. Często rodziły się poważne problemy przy ocenianiu, czy popełniony przez osobę sprawdzaną czyn zabroniony, za który ona została prawomocnie skazana, rzeczywiście negatywnie wpływa na dawanie przez nią rękojmi zachowania tajemnicy. Z tych przyczyn ustawodawca, dążąc do zmniejszenia zakresu wątpliwości, wskazał w art. 30 ust. 2 oraz w art. 33 ust. 1 i 8 nowej UOIN, iż organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa lub cofa wydane poświadczenie, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, ale wtedy gdy fakt skazania wywołuje wątpliwości, o których mowa w art. 24 ust. 2 i 3. Dotyczą one między innymi uczestnictwa, współpracy lub popierania działalności szpiegowskiej, terrorystycznej sabotażowej, występowania związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji czy niewłaściwego postępowania z informacjami niejawnymi. Wprowadzona fakultatywność odmowy wydania lub cofnięcia poświadczenia z uwagi na prawomocne skazanie, w zależności od występowania dodatkowych przesłanek, wskazuje na wolę swoistego uproszczenia istniejących wcześniej rozwiązań proceduralnych poprzez każdorazową ocenę indywidualnych przypadków w konkretnych sytuacjach. Co więcej, takie sformułowanie przepisu ograniczy przypadki, gdy w tożsamych stanach faktycznych podejmowano odmienne, często nieadekwatne decyzje, gdyż organowi trudno było jednoznacznie ustalić, czy popełniony czyn niekorzystnie oddziałuje, czy też nie oddziałuje na dawanie rękojmi zachowania tajemnicy.

W postępowaniu sprawdzającym problematyczne staje się także określenie, czy cofnięcie poświadczenia bezpieczeństwa wydanego w postępowaniu poszerzonym[47] skutkuje również cofnięciem poświadczenia w postępowaniu zwykłym, bo zgodnie z praktyką wynikającą ze stosowania art. 46 w związku z art. 37 ust. 9 poprzedniej UOIN, skazanie prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego jest przesłanką fakultatywną, a nie obligatoryjną cofnięcia poświadczenia bezpieczeństwa. Zgodnie z art. 33 ust. 11 nowej UOIN (art. 47 ust. 1 pkt 1 i 2 poprzedniej UOIN) kontrolne postępowanie sprawdzające kończy się wydaniem decyzji o cofnięciu poświadczenia bezpieczeństwa, poinfor-

[47] Według przepisów poprzedniej UOIN poszerzonego i specjalnego postępowania sprawdzającego.

mowaniem kierownika jednostki organizacyjnej lub osoby odpowiedzialnej za obsadę stanowiska o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem jej dalszej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa albo też, co jest wprowadzonym novum, decyzją o umorzeniu postępowania, w przypadku gdy postępowanie nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia, co będzie wiązać się z dalszym dostępem do informacji niejawnych.

Powyższe formy zakończenia kontrolnego postępowania sprawdzającego oznaczają, iż ustawa nie daje możliwości zakończenia go wydaniem decyzji utrzymującej w części ważność posiadanego przez osobę sprawdzaną poświadczenia bezpieczeństwa. Występowanie przesłanki określonej w art. 28 ust. l pkt 2 poprzedniej UOIN, odnoszącej się tylko do dostępu do tajemnicy państwowej, nie przesądzało o dostępie osoby sprawdzanej do informacji niejawnych stanowiących tajemnicę służbową.

Zgodnie z art. 33 ust. 1 i 2 poprzedniej UOIN poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne" uprawniało do dostępu, w oznaczonych okresach, do informacji niejawnych oznaczonych klauzulą „tajne", „poufne" i „zastrzeżone". Jednak konstrukcja art. 47 ust l poprzedniej UOIN wskazywała, iż osoba ta nie może posiadać takiego dostępu na podstawie cofniętego jej poświadczenia bezpieczeństwa.

Tak więc cofnięcie ważności dokumentu uprawniającego do dostępu do klauzuli „ściśle tajne" lub „tajne" oznaczało w praktyce brak dostępu jego posiadacza również do informacji niejawnych o klauzuli „poufne" lub „zastrzeżone". Nie było przy tym podstaw do wydania nowego poświadczenia bezpieczeństwa *de facto* o zmienionych uprawnieniach bez przeprowadzenia odpowiedniego postępowania sprawdzającego. Zachowanie dostępu do takich informacji byłoby natomiast możliwe tylko w przypadku posiadania przez osobę sprawdzaną odrębnego poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych stanowiących dotychczasową tajemnicę służbową.

Nowa regulacja o ochronie informacji niejawnych wprowadza w tym temacie dość istotną zmianę. Generalnie powtórzono w art. 29 ust. 4 nowej UOIN[48], iż ten sam dokument, czyli poświadczenie bezpieczeństwa uprawniające do dostępu do informacji oznaczonych wyższą klauzulą tajności, uprawnia do dostępu do informacji niejawnych oznaczonych niższą klauzulą tajności wyłącznie w zakresie określonym w art. 4 ust. 1 nowej UOIN. Jednak odstąpienie od przeprowa-

[48] Kaskadowość ważności poświadczenia bezpieczeństwa regulował art. 33 ust. 1 i 2 poprzedniej UOIN.

dzania postępowań sprawdzających do klauzuli „zastrzeżone" na rzecz wprowadzenia pisemnego upoważnienia uprawniającego do dostępu do tych informacji – art. 21 ust. 4 nowej UOIN, spowodowało wprowadzenie zastrzeżenia, wskazującego, iż osoba uprawniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania poświadczenia bezpieczeństwa lub jego cofnięciu, uniemożliwić dostęp do informacji niejawnych, ale gdy osoba sprawdzana miała wydane wcześniej przedmiotowe upoważnienie, to nadal może mieć dostęp do klauzuli „zastrzeżone" – art. 30 ust. 6 i art. 33 ust. 8 nowej UOIN.

Na koniec można dodać, iż w przypadku odstąpienia od wymierzenia kary zatarcie skazania następuje z mocy prawa z upływem roku od wydania prawomocnego orzeczenia i termin ten można uznać za tożsamy z terminem wskazanym w art. 30 ust. 7 nowej UOIN[49], zgodnie z którym postępowanie sprawdzające wobec osoby, która nie uzyskała poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po roku od daty doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa lub cofnięcia poświadczenia bezpieczeństwa. Sytuacja będzie odmienna w przypadku wymierzenia środka karnego, jego zatarcie bowiem liczone jest od dnia wykonania, darowania albo przedawnienia jego wykonania i dopiero od momentu uznania osoby za niekaraną będzie można wszcząć kolejne postępowanie sprawdzające.

[49] Termin przejęty z art. 41 ust. 3 poprzedniej UOIN.

Michał Jastrzębski
Henryk Lech
Anna Matwiejczuk
Jerzy Popowicz
Sławomir Witosławski

Kasowanie i niszczenie nośników zawierających informacje jawne i niejawne

W mediach często pojawiają się informacje o znalezieniu na śmietnikach stert dokumentów z danymi klientów banków czy firm ubezpieczeniowych, słyszy się także o gubieniu pendrive'ów z rzekomo wykasowanymi danymi. Kilka lat temu wybuchła afera z dyskami twardymi pewnej instytucji państwowej, które trafiły do redakcji popularnego, żeby nie powiedzieć brukowego, tygodnika. System ochrony danych osobowych, również niejawnych, nakłada na nas obowiązek właściwego, tzn. bezpiecznego, zapisu tych danych na wszelkiego typu nośnikach oraz niszczenia zapisów, gdy przestaną być przydatne, niezależnie od tego, czy umieszczone są na papierze, czy na dysku twardym komputera lub serwera.

Ochrona informacji

W systemach służących do przetwarzania, przesyłania i przechowywania informacji używa się wielu rodzajów urządzeń i nośników. Informacje umieszczane na tych nośnikach znajdują się w różnego typu urządzeniach, które wymagają specjalnych procedur zarządzania w celu ograniczenia ryzyka nieautoryzowanego dostępu do nich i uniemożliwienia naruszenia poufności informacji w nich przechowywanych.

W celu skutecznego zapewnienia bezpieczeństwa informacji należy uwzględniać cały cykl życia systemu teleinformatycznego, tj. od momentu wytworzenia informacji, przetwarzania w systemie, aż do chwili, kiedy zachodzi konieczność jej zniszczenia. Zapewnienie przestrzegania odpowiednich procedur i zarządzeń jest obowiązkiem zarówno wytwórcy informacji, jak i organizatorów (administratorów i inspektorów) systemu teleinformatycznego, którzy nim zarządzają oraz innych osób, które mają lub będą miały do niej uprawniony dostęp.

Zabezpieczanie informacji w trakcie jej przesyłania i przechowywania za pomocą narzędzi kryptograficznych jest w praktyce powszechnie stosowane i ma chronić przed zagrożeniami zewnętrznymi i wewnętrznymi. Pozostaje jednak problem związany z bezpieczeństwem danych w sytuacji, kiedy należy je wykaso-

wać z nośników lub pozbyć się samych nośników, które zawierały wrażliwe informacje. Rozwiązaniem jest właściwie wdrożona i przeprowadzona procedura utylizacji informacji zbędnych i ich nośników, minimalizująca ryzyko rekonstrukcji wykasowanych danych.

Rodzaje nośników informacji

Nośniki informacji wykorzystywane w systemach teleinformatycznych dzielimy w zależności od formy utrwalenia na:

- trwałe – na przykład papierowy wydruk, mikrofilm czy zdjęcia tradycyjne,
- elektroniczne – na przykład dyski twarde, pamięci przenośne USB, dyskietki, płyty CD, DVD, pamięci DRAM, PROM (EAPROM, EEPROM), EPROM, ROM, RAM, karty magnetyczne, urządzenia takie, jak telefony komórkowe, urządzenia PDA (palmtopy, Pocket PC itp.), routery, faksy, kserokopiarki, popularne karty pamięci typu flash, karty SD czy MS (informacje są tu zawarte w formie zapisu cyfrowego).

Wymienione rodzaje nośników są obecnie najbardziej popularne i dostępne na rynku. Należy jednak pamiętać, że postęp technologiczny (pamięci holograficzne, molekularne) dotyczący nośników i różnego rodzaju pamięci jest tak duży, że wymusza konieczność nieustannego monitorowania wszelkich zmian w tej dziedzinie. To dyktuje ciągłe opracowywanie nowych technik kasowania danych i niszczenia nośników. Należy zwrócić uwagę, że obecnie coraz więcej urządzeń zawiera, jako podzespół, części elektroniczne pełniące rolę pamięci. Czasami są to urządzenia, których nawet nie podejrzewamy o to, że mogą przechowywać informacje. I tu właśnie pojawia się największe zagrożenie. W swojej nieświadomości nie chronimy tych urządzeń. Przeciętny użytkownik nie zdaje sobie często sprawy z tego, że np. obecnie produkowane drukarki laserowe posiadają nie tylko różnego rodzaju pamięci typu RAM, ale również normalne dyski twarde. Czasami nie trzeba trudzić się programowym odzyskiwaniem danych, a wystarczy obejrzeć bęben drukarki, na którym może pozostawać informacja z ostatniego wydruku.

Metody utylizacji i kasowania nośników danych zawierających informacje wrażliwe

Jednym z podstawowych kryteriów, ale nie jedynym, doboru odpowiedniej metody i urządzeń do niszczenia nośników i kasowania informacji jest forma jej utrwalenia. Równie ważne jest kryterium klasyfikowania informacji wrażliwych przetwarzanych w systemie wykorzystywanym w firmie bądź instytucji. Ja-

sno określone zasady klasyfikowania są podstawą postępowania z informacjami na różnych etapach ich przetwarzania. Połączenie tych dwóch czynników jest warunkiem wyboru odpowiedniej metody utylizowania informacji. Inaczej bowiem będziemy niszczyć wydruki z wrażliwymi informacjami dotyczącymi danych osobowych, a inaczej zbędne materiały na papierze z informacjami o klauzuli „tajne". Takie same różnice będą występowały w przypadku niszczenia lub kasowania danych jawnych i niejawnych na dyskach twardych oraz innych nośnikach elektronicznych.

Metoda programowa kasowania informacji

Metoda programowa kasowania informacji polega na zastosowaniu odpowiedniego oprogramowania, które usuwa informacje z nośnika w sposób uniemożliwiający ponowne ich odczytanie za pomocą aplikacji lub narzędzi programistycznych służących do odzyskiwania wykasowanych danych. Należy pamiętać, że zastosowanie w programie Microsoft Windows poleceń pod nazwą „usuń", „delete" albo „format", nie usuwa zawartości pliku z elektronicznego nośnika danych i pamięci komputera. Komendy te zmieniają jedynie logiczne położenie danych na nośniku. Urządzenie, na przykład komputer, ich nie rozpoznaje z uwagi na fakt pozbawienia systemu operacyjnego możliwości odnalezienia wcześniej zapisanej informacji, podobnie do sytuacji usunięcia spisu treści w tradycyjnej książce. Do czasu ponownego zapisania określonego obszaru pamięci nośnika wcześniej istniejące dane ciągle są dostępne i można je odtworzyć, stosując nawet niezbyt wyspecjalizowane narzędzia informatyczne.

Usunięcie informacji z nośnika polega na jego jednokrotnym lub wielokrotnym nadpisaniu, w zależności od klasyfikacji zawartych na nim informacji. Nadpisanie musi dotyczyć całej powierzchni nośnika z uwzględnieniem tablicy alokacji plików (charakterystycznych dla zainstalowanego systemu plików np. FAT, MFT) i całej adresowalnej przestrzeni. Podczas wielokrotnego nadpisywania nośnika, zapisane informacje powinny być zastępowane przez losowo wygenerowane dane, a w ostatnim etapie – zastąpione zadaną wartością, co ułatwia weryfikację poprawności kasowania. Wybierając tę metodę, należy uwzględnić pojemność nośnika, jego typ oraz ilość nośników ze względu chociażby na czas, jaki potrzebny jest na zrealizowanie całej procedury.

Agencja Bezpieczeństwa Wewnętrznego w korespondencji z różnymi podmiotami wskazuje na konieczność uwzględniania klauzuli tajności podczas nadpisywania dysków. Dla dysków jawnych i o klauzuli „zastrzeżone" zalecane jest stosowanie odpowiednich aplikacji umożliwiających co najmniej jednokrotne nadpisywanie odpowiednim algorytmem, przy dyskach o klauzuli „poufne" – co naj-

mniej trzykrotne, a przy klauzuli „tajne" – co najmniej siedmiokrotne nadpisywanie całej powierzchni nośnika. Istotne są również zalecenia ABW dotyczące deklasyfikacji (obniżania klauzul). Według nowych wytycznych (będących w trakcie opracowywania) nie zaleca się przeprowadzania deklasyfikacji nośników. Czynność tę proponuje się wykonywać tylko w szczególnych przypadkach, np. w odniesieniu do starych systemów, gdy nie można już kupić odpowiednich nowych nośników na rynku. Powyższe podyktowane jest tym, że cena nośników informacji bardzo zmalała, a zagrożenie znacznie wzrosło (coraz więcej jest dostępnych programów do odzyskiwania itd.). Ponadto projekt rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego zawiera zapis, że klauzula tajności informatycznych nośników danych umożliwiających wielokrotny zapis, na których przechowywane są informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne", nie podlega zniesieniu lub obniżeniu.

Zaleca się, aby dyski, które w wyjątkowych przypadkach podlegały deklasyfikacji, pozostawały w jednostce organizacyjnej, w której były zarejestrowane, i nie były pod żadnym pozorem zbywane poza tę jednostkę.

Taka metoda utylizacji nie może być jednak stosowana w odniesieniu do nośników uszkodzonych i nienadających się do ponownego zapisu, na przykład w przypadku stwierdzenia anomalii w procesie tzw. wipowania (nadpisywania), gdy zostaną wykryte uszkodzone sektory.

Ze względu na niedoskonałość stosowanych metod programowego usuwania danych oraz na fakt, iż ciągły postęp technologiczny może w przyszłości umożliwić dostęp do informacji, które pierwotnie uznano za bezpowrotnie usunięte, przy podejmowaniu decyzji o wyborze tej właśnie metody, jako jedynie pewnej do usuwania zapisów na nośnikach danych, należy zachować szczególną ostrożność.

Metoda fizycznego niszczenia nośników informacji

Metoda fizycznego zniszczenia nośnika informacji jest działaniem ostatecznym, eliminującym możliwość jego ponownego wykorzystania. Jest to metoda polegająca na utylizacji przez rozdrobnienie, spalenie, sproszkowanie, stopienie lub pocięcie. Ze względu na wysoki stopień bezpieczeństwa zalecana jest do niszczenia nośników klasyfikowanych najwyżej.

Niszczenie nośników poprzez ich rozdrobnienie, spalenie, sproszkowanie i stopienie polega na ich całkowitym zniszczeniu za pomocą specjalistycznych urządzeń, w sposób skuteczny i bezpieczny.

Metoda polegająca na pocięciu nośnika na drobne elementy ma zastosowanie do nośników trwałych i elastycznych takich, jak papier, dyskietki, płyty CD, DVD oraz elementów wyjętych z obudowy nośników, tj. taśm, talerzy dysków itp. Należy jedynie pamiętać, żeby rozmiary pociętych elementów, zgodnie z wymogami dotyczącymi klasyfikowania informacji, były dostatecznie małe i uniemożliwiały fizyczną rekonstrukcję nośnika.

Prawidłowy dobór urządzenia niszczącego, ze względu na wrażliwość informacji i jej klasyfikację, gwarantuje niemiecka norma DIN 32757, która jednoznacznie wskazuje, jakie urządzenie powinno być użyte do niszczenia nośnika zawierającego informacje o określonej klauzuli tajności. Niżej przedstawione dane dotyczą niszczenia nadruków na papierze, foliach, plastikach oraz niszczenia metalowych matryc do drukowania. Można jednak z nich korzystać również przy niszczeniu nośników elektronicznych. Zalecane jest stosowanie niszczarek II i III klasy. Dokładne informacje na temat zastosowanych w tym wypadku procedur zawarte są w *Szczegółowych zaleceniach dotyczących ochrony fizycznej systemów i sieci teleinformatycznych*. Odsyłamy również do szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez Departament Bezpieczeństwa Teleinformatycznego ABW dla administratorów i inspektorów bezpieczeństwa teleinformatycznego.

Przedstawioną poniżej normę należy rozpatrywać w ten sposób, że materiały można wyrzucić do śmieci dopiero w przypadku uzyskania skrawków o wymaganych wielkościach. Pojawia się jednak pytanie, co zrobić z papierem, którego ze względów technicznych bądź z powodu braku odpowiednich urządzeń nie dało się pociąć na kawałki o zalecanej wielkości? Należy wskazać, że w większych miastach działają spalarnie bądź papiernie, do których można dostarczyć rozdrobniony papier. Ważne jest, aby proces utylizacji odbywał się pod stałym nadzorem pracowników firmy lub jednostki organizacyjnej – właściciela niszczonych dokumentów.

Norma DIN 32757		
KLASA TAJNOŚCI	**DOKUMENTY**	**WYMAGANIA**
I	Materiały ogólne, korespondencja	Długość nielimitowana, szerokość paska =< 12 mm, powierzchnia ogółem =< 2000 mm^2
II	Korespondencja wewnętrzna, materiały wewnętrzne	Długość nielimitowana, szerokość paska =< 6 mm, powierzchnia ogółem =< 800 mm^2

III	Materiały poufne	szerokość paska =< 2 mm, powierzchnia ogółem =< 594 mm^2 szerokość paska =< 4 mm, długość =< 80 mm, powierzchnia ogółem =< 320 mm^2
IV	Materiały tajne	szerokość paska =< 2 mm, długość =< 15 mm, powierzchnia ogółem =< 30 mm^2
V	Materiały ściśle tajne	szerokość paska =< 0.8 mm, długość =< 13 mm, powierzchnia ogółem =< 10 mm^2

Metoda demagnetyzacji

Demagnetyzacja jako metoda utylizacji nośników, polega na bezpowrotnym wykasowaniu informacji poprzez poddanie nośnika działaniu silnego pola elektromagnetycznego. Pole to powoduje usunięcie wszystkich informacji w warstwie magnetycznej. Metoda ta jest szczególnie zalecana w sytuacji, kiedy nośnik jest uszkodzony i brak jest możliwości jego odczytu, a więc zastosowania wykasowywania programowego. Charakteryzuje się dużą skutecznością i szybkością realizacji. Należy jednak pamiętać o tym, że nośniki optyczne, na przykład płyty CD i DVD, nie mogą być niszczone tą metodą ze względu na inną technologię zapisu. Nośniki magnetyczne, takie jak dyski HDD, dyskietki, kasety, taśmy magnetyczne czy taśmy do streamerów, utylizowane są degausserami[1].

Decydując się na wykorzystanie urządzeń demagnetyzujących, należy zwrócić uwagę na wartość pola magnetycznego, jaką generuje dane urządzenie, i ściśle przestrzegać zasad eksploatacji oraz serwisowania, aby zapewnić właściwe parametry pracy urządzeń przez cały czas eksploatacji. Na własne potrzeby ABW stosuje obecnie degausser o mocy ponad 10 000 gaussów zapewniający całkowite zniszczenie zapisu magnetycznego. Należy pamiętać, że po takim zniszczeniu nie jest możliwe ponowne wykorzystanie dysku twardego, gdyż w procesie demagnetyzacji niszczone są również jego zapisy fabryczne. W przypadku nośników zawierających informacje klasyfikowane zaleca się również, aby były one niszczone w sposób fizyczny poprzez ścięcie, spalenie, stopienie lub zmiażdżenie (o czym wspomniano wyżej).

Metoda demagnetyzacji może być stosowana tylko w odniesieniu do zapisu magnetycznego. Nie można jej zastosować na przykład w przypadku pamięci pół-

[1] Degausser – specjalne urządzenie służące do trwałego i skutecznego niszczenia danych z nośników magnetycznych.

przewodnikowych typu flash, dysków hybrydowych i SSD. Pozostaje tu jedynie nadpisywanie i niszczenie fizyczne lub metoda niszczenia chemicznego.

Metoda chemicznego niszczenia nośników informacji

Niszczenie nośników informacji metodą chemiczną, oferowane obecnie w Polsce, polega na całkowitym chemicznym zniszczeniu płyt dysków twardych oraz innych nośników elektronicznych w silnych reagentach chemicznych. W przypadku standardowego dysku twardego o zapisie magnetycznym metoda ta polega na wstępnym rozdrobnieniu dysku, rozpuszczeniu jego podkładu w silnym roztworze alkalicznym oraz na rozpuszczeniu pozostałych wiórków ferrytowych w silnym roztworze kwaśnym. Podstawową zaletą tej metody jest całkowite zniszczenie dysku. Poza roztworami nic po nim nie zostaje. Brakuje nawet wiórków, jak ma to miejsce po zastosowaniu metody fizycznej, czyli nie ma tzw. materiału dowodowego, który można by poddać dalszej analizie. Metoda ta ma jednak również wady w postaci uciążliwości i czasochłonności całego procesu.

Roztwory pozostałe po reakcji nie mogą być wylewane do kanalizacji. Przekazuje się je do oczyszczalni ścieków. Poza tym cały proces wymaga zastosowania profesjonalnej aparatury chemicznej. Ważne jest również, aby niszczenie nośnika odbywało się w obecności jego właściciela.

Jak widać, metod niszczenia elektronicznych nośników informacji jest wiele, dlatego ważne jest dobranie odpowiedniej metody do konkretnego nośnika. Istotne jest również zachowanie nawet przesadnych środków ostrożności podczas procesu niszczenia i stosowanie przynajmniej dwóch metod utylizacyjnych jednocześnie. W przypadku stosowania poszczególnych rozwiązań technicznych należy zwracać uwagę, aby posiadały one certyfikaty krajowe, NATO-wskie bądź unijne, bądź też pozytywną opinię Agencji Bezpieczeństwa Wewnętrznego.

Podsumowując, należy wspomnieć, że istnieje również problem pozostałości elektronicznych po nośnikach, czyli tzw. złomu elektronicznego. Zgodnie z ustawą o zużytym sprzęcie elektrycznym i elektronicznym z 2005 r., która zakazuje wyrzucania tego typu sprzętu na śmietnik, na firmy i jednostki organizacyjne nakłada się określone obowiązki w tym zakresie. Przed przekazaniem złomu elektronicznego do profesjonalnej utylizacji należy oczywiście się upewnić, czy w przekazywanym sprzęcie nie znajdują się jakieś dodatkowe nośniki pamięci.