Paweł Antosiak
Jakub Pałka

Wybrane aspekty ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Problemy, interpretacje oraz propozycje ewentualnych rozwiązań legislacyjnych

1. Wstęp

Wnioski wynikające z praktycznego stosowania przepisów obowiązującej już od ponad sześciu lat ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[1] (zwanej dalej „ustawą") umożliwiają wskazanie tych obszarów systemu ochrony informacji niejawnych w Rzeczpospolitej Polskiej, w których przypadku przyjęte rozwiązania prawne, organizacyjne i proceduralne nie są w pełni efektywne. Tym samym możliwe jest sformułowanie propozycji takich zmian legislacyjnych w powyższym zakresie, które mogłyby znacznie wzmocnić skuteczność działania systemu ochrony informacji niejawnych przez uwzględnienie wieloletniego doświadczenia nabytego przez organy sprawujące nadzór nad tym systemem oraz pozostałe podmioty ustawy, jak również dostosowałyby tę ustawę do wprowadzanych zmian w systemie bezpieczeństwa państwa, którego częścią jest system ochrony informacji niejawnych. Stwierdzone problemy związane ze stosowaniem przepisów ustawy wskazują przede wszystkim na potrzebę dalszego doprecyzowania i zracjonalizowania rozwiązań przyjętych w 1999 i 2010 r.

W związku z tym warto rozważyć dokonanie zmian o znaczeniu zasadniczym dla prawidłowego i efektywniejszego funkcjonowania systemu ochrony informacji niejawnych, a także wzmocnienie – tam, gdzie nie powoduje to żadnego zagrożenia interesu ochrony informacji niejawnych – pozycji obywatela względem państwa i jego organów, jako głównych podmiotów odpowiedzialnych za prawidłowe funkcjonowanie systemu ochrony tych informacji.

W niniejszym opracowaniu nie zawarto wszystkich problemów i związanych z nimi ewentualnych propozycji zmian, a tylko te zasadnicze, w tym rozwiązania, które – w subiektywnej opinii autorów opracowania – istotnie wzmocniłyby system ochrony informacji niejawnych w RP. Dlatego byłoby wskazane, aby stały się one elementem składowym przepisów regulujących jego funkcjonowanie.

2. Organizacja systemu ochrony informacji niejawnych

System ochrony informacji niejawnych w Rzeczpospolitej Polskiej powinien zapewniać stosowanie jednolitych standardów w zakresie tej ochrony w odniesieniu do wszystkich jednostek organizacyjnych uczestniczących w obiegu takich informacji. Zachowanie pełnej spójności wyżej wymienionego systemu i jednolitości stosowanych rozwiązań wymagałoby zasadniczej zmiany ustawowej mającej na celu ustanowienie jednego organu sprawującego ogólny nadzór nad tym systemem, zarówno w sferze cy-

[1] Dz.U. z 2016 r. poz. 1167, ze zm.

wilnej, jak i wojskowej. Biorąc pod uwagę pozytywne doświadczenia wynikające ze stosowania przepisów dotyczących nadzoru ABW nad informacjami niejawnymi międzynarodowymi (art. 11 ustawy), właściwe wydaje się wprowadzenie analogicznego modelu sprawowania nadzoru nad krajowymi informacjami niejawnymi, tj. przypisanie głównej roli jednemu organowi w sprawowaniu nadzoru nad systemem ochrony tych informacji, co pozwoliłoby uniknąć rozbieżnych interpretacji, a przez to – odmiennego stosowania przepisów ustawy przez ABW i SKW.

Widocznym mankamentem ustawy stało się niedostatecznie precyzyjne uregulowanie działalności osób najważniejszych dla systemu ochrony informacji niejawnych, tj. kierownika jednostki organizacyjnej, pełnomocnika ochrony (i jego zastępcy), kierownika kancelarii tajnej, inspektora bezpieczeństwa teleinformatycznego i administratora systemu. Przy czym nie chodzi tu jedynie o wymogi, jakie te osoby powinny spełniać, aby pełnić funkcje wynikające z ustawy, ale o istotny z punktu widzenia prawidłowości funkcjonowania systemu ochrony informacji niejawnych problem, jakim jest określenie, kogo należy uważać np. za kierownika jednostki w rozumieniu ustawy, co dotychczas jest w różny sposób interpretowane – zwłaszcza w jednostkach administracji publicznej.

W związku z powyższym wskazane byłoby przede wszystkim doprecyzowanie pojęcia kierownik jednostki organizacyjnej pojawiającego się w treści ustawy, przez określenie w sposób jednoznaczny, kto pełni tę funkcję (a tym samym ponosi odpowiedzialność za ochronę informacji niejawnych), tj. przez wprowadzenie jego definicji. W opinii autorów opracowania kierownikiem jednostki organizacyjnej powinna być osoba stojąca na jej czele, która nią zarządza i zapewnia – przy pomocy lub za pośrednictwem podległych pracowników – realizację jej zadań. Taka definicja uniemożliwia przyjęcie rozwiązania (dotychczas często spotykanego) polegającego na wyznaczeniu do pełnienia roli kierownika jednostki organizacyjnej innej osoby, niż kierująca daną jednostką. Oczywiście ta propozycja musiałaby uwzględniać odmienność traktowania osoby pełniącej funkcję kierownika przedsiębiorcy z uwagi na konieczność uwzględnienia mnogości form reprezentowania podmiotów gospodarczych wynikających z odrębnych przepisów. Tak skonstruowany przepis dodatkowo spowodowałby zaniechanie faktycznego kontestowania przez kierowników jednostek organizacyjnych zasady bezpośredniej podległości pełnomocnika ochrony kierownikowi jednostki organizacyjnej, przejawiającego się w usytuowaniu pionu ochrony i pełnomocnika ochrony w strukturze innych komórek organizacyjnych.

Kolejnym krokiem mającym na celu precyzyjne uregulowanie definicji kierownika jednostki organizacyjnej powinno być wskazanie, że kierownik jednostki organizacyjnej przetwarzającej informacje niejawne musi posiadać poświadczenie bezpieczeństwa upoważniające go do dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli informacji niejawnych przetwarzanych w kierowanej przez niego jednostce, bądź upoważnienie, w przypadku gdy w tej jednostce są przetwarzane informacje niejawne oznaczone wyłącznie klauzulą „zastrzeżone". Właściwe byłoby również, aby w sytuacji, w której osoba pełniąca tę funkcję nie uzyskała poświadczenia bezpieczeństwa (lub upoważnienia – odpowiednio), mogła tę funkcję pełnić osoba ją zastępująca, wskazana przez osobę niespełniającą wspomnianego wymogu lub przez organ uprawniony do obsady stanowiska.

Powyższe propozycje pozostają w korespondencji z odpowiedzialnością, jaką ponosi kierownik jednostki za ochronę informacji niejawnych, gdyż brak wymogu posiadania powyższych uprawnień uniemożliwia skuteczne i realne realizowanie tego obowiązku. Poza

tym taki wymóg ustawodawca określił wobec innych osób realizujących zadania w zakresie ochrony informacji, np. wobec pełnomocnika ochrony, kierownika kancelarii tajnej oraz ich zastępców. Należy podkreślić, że na poziomie jednostki organizacyjnej to funkcja kierownika jednostki jest zasadnicza w zakresie ochrony informacji niejawnych, a tym samym posiadanie przez niego – odpowiednio – poświadczenia bezpieczeństwa lub upoważnienia do dostępu do tych informacji jest naturalną tego konsekwencją. Wymóg posiadania odpowiedniego poświadczenia nie powinien obejmować jedynie kierowników jednostek organizacyjnych, którzy mają dostęp do informacji niejawnych *ipso iure*.

Powyższe jest o tyle istotne, że przepisy ustawy nie precyzują jednoznacznie konieczności poddania się kierownika jednostki organizacyjnej stosownemu postępowaniu sprawdzającemu, co w zestawieniu z odpowiedzialnością spoczywającą na nim w zakresie ochrony informacji niejawnych należy uznać za nielogiczne, czyniące tę odpowiedzialność fikcyjną.

Jeśli natomiast chodzi o wymagania dotyczące pozostałych osób zajmujących najważniejsze stanowiska w sferze ochrony informacji niejawnych, należy je również uznać za niewystarczające, jednakże tylko w odniesieniu do osób zajmujących te stanowiska w podmiotach najważniejszych z punktu widzenia zapewniania bezpieczeństwa państwa[2] i jego strategicznych interesów. W przypadku tych osób, z uwagi na ich szczególną rolę w systemie bezpieczeństwa RP, i w tych podmiotach, właściwym rozwiązaniem byłoby określenie dodatkowych warunków, jakie te osoby powinny spełniać. I tak wydaje się, że pełnomocnik ochrony i jego zastępca poza obywatelstwem polskim, wykształceniem wyższym oraz poświadczeniem bezpieczeństwa i aktualnym zaświadczeniem o przeszkoleniu wydanymi przez ABW lub SKW powinien uzyskać zgodę szefa jednej z wymienionych służb (w zależności od tego, w czyjej właściwości podmiot się znajduje) na pełnienie tej funkcji. Powinna się z tym wiązać procedura przesyłania przez kierowników jednostek organizacyjnych do ABW lub SKW stosowych wniosków zawierających wykaz obowiązków i opis sposobu ich realizacji przez kandydata, dane o przebiegu jego kariery zawodowej oraz szczegółowe uzasadnienie zamiaru obsadzenia tej osoby na stanowisku pełnomocnika ochrony lub jego zastępcy. Ten warunek powinien być wprowadzony również w przypadku osób kandydujących na takie stanowiska, jak: kierownik kancelarii tajnej i jego zastępca oraz administrator systemu teleinformatycznego oraz inspektor bezpieczeństwa teleinformatycznego – w podmiotach odgrywających główną rolę w zapewnianiu bezpieczeństwa państwa.

Kolejnym problemem związanym z osobami najważniejszymi dla systemu ochrony informacji niejawnych są występujące przypadki, w których osoby niespełniające ustawowych wymogów obejmowały funkcję pełnomocnika ochrony (lub zastępcy) i wydawały poświadczenia bezpieczeństwa, które następnie musiały być przez ABW lub SKW unieważniane (w trybie określonym w kodeksie postępowania administracyjnego) ze względu na ich wadę prawną, tj. wydanie przez nieuprawniony organ. Dlatego też, mając na uwadze potrzebę uszczelnienia systemu ochrony informacji niejawnych w tym zakresie, zasadne byłoby wprowadzenie obowiązku informacyjnego zobowiązującego kierownika jednostki organizacyjnej do uzyskania z ABW lub SKW potwierdzenia spełniania ustawowych wymogów formalnych przez osoby, które miałby zamiar zatrudnić na stanowisku pełnomocnika ochrony lub jego zastępcy. To rozwiązanie dotyczyłoby wszystkich pełnomocników (i ich zastępców), nie tylko tych zatrudnionych w podmiotach najważniejszych z punktu widzenia zapewniania bezpieczeństwa państwa.

[2] Wykaz głównych podmiotów powinien zostać dookreślony w odrębnym akcie prawnym.

Dobór osób zatrudnianych w pionie ochrony jednostki organizacyjnej jest ściśle powiązany z odpowiedzialnością nałożoną przez ustawodawcę na szefów ABW i SKW – organów odpowiedzialnych za nadzór nad systemem ochrony informacji niejawnych w Polsce. Wskazane powyżej propozycje nowych rozwiązań są motywowane koniecznością uzyskania przez szefa ABW i szefa SKW, jako głównych podmiotów odpowiedzialnych za kontrwywiadowcze i antyterrorystyczne (ABW) bezpieczeństwo państwa, realnego i skutecznego narzędzia do prawidłowego, również w aspekcie prewencyjnym, kształtowania polityki i standardów w tym zakresie. Z założenia mają więc wykluczyć możliwość obsadzania wspomnianych stanowisk osobami przypadkowymi, nieprzygotowanymi i nieświadomymi zagrożeń wynikających z niewłaściwego przetwarzania informacji niejawnych.

3. Właściwość ABW i SKW

W nawiązaniu do wskazanej, zasadniczej roli ABW i SKW w systemie ochrony informacji niejawnych, należy podkreślić, że ta rola może być odgrywana w pełni efektywnie wtedy, gdy przepisy prawa odpowiednio precyzyjnie określą właściwość obu organów w zakresie czynności realizowanych przez obie służby. Tak więc w celu zapewnienia większej przejrzystości i zapobieżenia sporom dotyczącym właściwości obu służb zasadne jest jej doprecyzowanie. Przy czym wskazane jest jednoznaczne przypisanie właściwości SKW wszystkich struktur wojskowych, w tym spółek podległych ministrowi obrony narodowej publikowanych w wykazie[3], a także sądów wojskowych oraz osób zatrudnionych w międzynarodowych dowództwach wojskowych, wielonarodowych jednostkach wojskowych z udziałem wojska polskiego lub innych podmiotach wielonarodowych z siedzibą na terytorium RP zajmujących się obronnością i wojskowością. Tak określona właściwość byłaby naturalną konsekwencją i dopełnieniem odpowiedzialności SKW (wynikającej z odrębnych przepisów), a nie ABW, w zakresie zapewniania także kontrwywiadowczej ochrony tych podmiotów. Sugerowane włączenie sądów wojskowych do jednostek organizacyjnych będących we właściwości SKW jest podyktowane także statusem tych sądów. Są one bowiem jednostkami wojskowymi w rozumieniu przepisów ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej oraz ustawy o służbie wojskowej żołnierzy, w związku z czym cała problematyka związana ze stosowaniem przez sądy wojskowe przepisów wykonawczych dotycząca ochrony informacji niejawnych opiera się na odpowiednich przepisach wydanych przez ministra obrony narodowej.

Przy uwzględnieniu występujących niekiedy w praktyce przypadków, gdy względy bezpieczeństwa państwa uzasadniają odstępstwo od ustalonej właściwości wymienionych powyżej organów, należy również rozważyć wprowadzenie w przepisach zasady, że niezależnie od właściwości do prowadzenia konkretnego postępowania wynikającego z ustawy, w szczególnie uzasadnionych okolicznościach Prezes Rady Ministrów mógłby zlecić innemu organowi (np. organowi nadzorującemu system ochrony informacji niejawnych – zob. pkt I pt. *Organizacja systemu ochrony informacji niejawnych*) wszczęcie i prowadzenie tego postępowania.

[3] Obecnie jako taki wykaz traktuje się *Obwieszczenie Ministra Obrony Narodowej z dnia 24 sierpnia 2016 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych*.

4. Bezpieczeństwo osobowe (postępowania sprawdzające)

W wyniku kilkunastoletniej praktyki prowadzenia postępowań sprawdzających stwierdzono, że liczba wydawanych poświadczeń bezpieczeństwa stale rośnie. Ta tendencja – w opinii autorów opracowania – nie jest niestety wynikiem rzeczywistej potrzeby udostępniania informacji niejawnych coraz większej liczbie osób, lecz traktowaniem postępowań sprawdzających przez jednostki organizacyjne jako procedury kadrowej, co faktycznie wypacza ich cel określony w ustawie. Mając więc na względzie konieczność zapobiegania zjawisku „nadprodukcji" tego typu poświadczeń, zasadne byłoby wprowadzenie mechanizmu korygującego i filtrującego zasadność kierowania do ABW lub SKW wniosków o wydanie takich poświadczeń – wymogu uzasadnienia wniosku, które musiałoby zawierać wskazanie zadań danej osoby powiązanych ze wskazaniem konkretnej klauzuli i rodzaju informacji niejawnych (informacje niejawne krajowe lub międzynarodowe), do których dostęp byłby niezbędny przy realizacji tych zadań. Przy tym rozwiązaniu ABW i SKW powinny mieć prawo – w razie wątpliwości co do treści takiego uzasadnienia (np. po stwierdzeniu braku związku pomiędzy zadaniami a koniecznością uzyskania dostępu do informacji niejawnych) – zwrócenia się do wnioskodawcy o przekazanie bardziej szczegółowego uzasadnienia. W takim przypadku realizacja postępowania następowałaby dopiero z chwilą uzyskania odpowiedzi od wnioskodawcy.

Współpraca w toku postępowań z innymi podmiotami

Z punktu widzenia jakości i sprawności prowadzenia postępowań, o których mowa w ustawie, rzeczą elementarną jest zapewnienie prawnej możliwości zebrania na temat osoby lub podmiotu, których dotyczy postępowanie, wszelkich informacji mogących mieć wpływ na jego wynik. Najważniejsza do osiągnięcia tego celu jest sprawna wymiana informacji zarówno z jednostkami organizacyjnymi niebędącymi podmiotami ustawy, jak i służbami uprawnionymi do prowadzenia wspomnianych postępowań[4]. Niestety, w czasie wieloletniej praktyki służby prowadzące postępowania sprawdzające niejednokrotnie napotykały poważne problemy z uzyskiwaniem informacji, obowiązujące przepisy pozwalają bowiem na różne interpretacje prowadzące w skrajnych przypadkach do odmowy przez niektóre jednostki (głównie niepaństwowe, w tym banki, biura maklerskie, placówki służby zdrowia i komorników) przekazania informacji niezbędnych do skutecznego przeprowadzenia procedury albo żądania opłat za realizację sprawdzeń. Z tego powodu zasadne jest rozważenie wprowadzenia takich zmian w ustawie, które umożliwią skuteczne przeprowadzenie czynności sprawdzających w każdej jednostce organizacyjnej, a nie tylko w jednostce organizacyjnej będącej podmiotem ustawy (czyli takiej, w której przetwarza się informacje niejawne).

Liczne doświadczenia negatywne wynikają również ze współpracy służb między sobą w zakresie wymiany informacji na temat osób, które przechodziły z właściwości jednej służby we właściwość innej. Tu problemem było uzyskanie danych na ich temat. Obecne przepisy pozwalają na odmowę przekazania informacji (a nawet tę odmowę wymuszają), nawet jawnych, mogących mieć wpływ na dawanie rękojmi zachowania tajemnicy, ponieważ przekazanie danych przez służby może nastąpić (…) *wyłącznie w przypadku, gdy w ich opinii osoba objęta postępowa-*

[4] Oprócz ABW i SKW, są to: SWW, CBA, Policja, Żandarmeria Wojskowa, Straż Graniczna, Służba Więzienna i Biuro Ochrony Rządu (Państwowa Służba Ochrony).

niem sprawdzającym lub kontrolnym postępowaniem sprawdzającym nie daje rękojmi zachowania tajemnicy[5] (a dodatkowo nakłada się na to problem ograniczeń dotyczących udostępniania akt postępowań sprawdzających przez większość służb specjalnych). Dlatego też należy rozważyć przyjęcie takiego rozwiązania ustawowego, że odmowa udzielenia informacji między służbami odpowiedzialnymi za bezpieczeństwo państwa i jego obywateli dotyczyłaby jedynie niektórych informacji o klauzuli „ściśle tajne" o szczególnym znaczeniu dla bezpieczeństwa państwa (lub interesu służby), stanowiących większe dobro niż dokonanie oceny dawania rękojmi zachowania tajemnicy przez organ prowadzący postępowanie. *Lex specialis* w stosunku do powyższego przepisu powinien nadal stanowić art. 72 odnoszący się do udostępniania akt postępowań sprawdzających.

Ogólne zasady dostępu osób do informacji niejawnych

Przepisy ustawy określają warunki, jakie powinny spełniać osoby uzyskujące dostęp do informacji niejawnych, przy czym podkreślenia wymaga to, że ujawnienie każdej informacji niejawnej – niezależnie od jej klauzuli tajności – osobom nieupoważnionym, może przynieść państwu określone szkody. Dotyczy to także informacji niejawnych o najniższej klauzuli, tj. „zastrzeżone", czyli tych, których ujawnienie może mieć negatywny wpływ na wykonywanie zadań związanych z bezpieczeństwem państwa[6]. Przepisy obecnie obowiązującej ustawy nie narzucają żadnej weryfikacji osób, którym informacje o tej klauzuli mają być udostępnione, pozostawiając decyzję w tej sprawie kierownikowi jednostki organizacyjnej. W tej sytuacji zasadne byłoby umożliwienie minimalnej weryfikacji osób, które mają zapoznawać się z tego typu informacjami, i wykluczenie występującej obecnie uznaniowości kierownika jednostki organizacyjnej w dopuszczaniu osób do dostępu do nich (w tym np. osób skazanych). Z uwagi na dotychczasową całkowitą dowolność i brak jakichkolwiek uregulowań dotyczących zasad wydawania upoważnień osobom, które mają mieć dostęp do tak oznaczonych informacji niejawnych, należy rozważyć uregulowanie w przepisach prawa zasad wydawania tych upoważnień**.** I tak np. kierownikom jednostek organizacyjnych upoważnienia byłyby wydawane przez ABW lub SKW, pełnomocnicy ochrony zaś – oraz ABW i SKW w odniesieniu do samych kierowników – byliby uprawnieni do sprawdzania osób ubiegających się o wydanie upoważnienia w Krajowym Rejestrze Karnym[7].

Warto nadmienić, że osoby uzyskujące dostęp do informacji niejawnych o klauzuli odpowiadającej klauzuli „zastrzeżone" podlegają sprawdzeniom m.in. w takich krajach, jak Kanada[8], Dania, Luksemburg oraz Turcja.

---

[5] Art. 13 ust. 3 ustawy.

[6] Art. 5 ust. 4 ustawy: „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 opraw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej*"*.

[7] ABW i SKW dodatkowo byłyby uprawnione do sprawdzania osób ubiegających się o wydanie upoważnienia w ewidencjach niejawnych.

[8] W przypadku dostępu do informacji niejawnych oznaczonych klauzulą „NATO RESTRICTED" lub odpowiednikami tej klauzuli stosowanymi przez inne państwa (brak odpowiednika kanadyjskiego wymienionej klauzuli).

Zakres przedmiotowy postępowań sprawdzających – ważność poświadczeń (upoważnień)

Zgodnie z przepisami ustawy w trakcie zwykłego postępowania sprawdzającego (prowadzonego przez pełnomocników ochrony konkretnych jednostek organizacyjnych do poziomu „poufne") nie są weryfikowane: stan zdrowia psychicznego (w tym uzależnienia) oraz sytuacja finansowa osoby sprawdzanej. W konsekwencji choroba psychiczna lub uzależnienie od narkotyków albo alkoholizm nie są przeszkodami w uzyskaniu (lub podstawą do pozbawienia) dostępu do informacji niejawnych o klauzuli „poufne" – co jest nie do utrzymania nie tylko z punktu widzenia elementarnej logiki, lecz także przede wszystkim z punktu widzenia interesu ochrony informacji niejawnych, a co za tym idzie – także interesu bezpieczeństwa państwa. Zasadne byłoby zatem stwierdzanie niedawania rękojmi zachowania tajemnicy w odniesieniu do osób objętych zwykłymi postępowaniami sprawdzającymi także w przypadku wątpliwości natury zdrowotnej i finansowej, jednakże z uwzględnieniem możliwości uzyskiwania i weryfikacji przez pełnomocnika ochrony tylko informacji o stanie zdrowia osoby sprawdzanej (oczywiście wraz z możliwością zobowiązywania tej osoby do poddania się specjalistycznemu badaniu). W przypadku wątpliwości dotyczących sytuacji finansowej, jakkolwiek ich stwierdzenie mogłoby stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa w zwykłym postępowaniu sprawdzającym (np. w sytuacji, gdyby te wątpliwości zostały ustalone we wcześniej przeprowadzonym poszerzonym postępowaniu sprawdzającym), to jednak pełnomocnik ochrony nie powinien mieć możliwości gromadzenia i weryfikacji szczegółowych informacji w tym zakresie, przede wszystkim z uwagi na to, że sytuacja finansowa osoby sprawdzanej jest z reguły rozpatrywana nie tylko wyłącznie w odniesieniu do niej samej, ale często również w kontekście innych osób (np. rodziców, współmałżonka, darczyńców), a także z uwagi na szczególną wrażliwość ochrony danych finansowych (przede wszystkim stanowiących tajemnicę bankową).

Przetwarzanie informacji w ramach postępowania

Zgodnie z przepisami ustawy organ prowadzący postępowanie sprawdzające ma możliwość przetwarzania w ramach tego postępowania informacji o osobie sprawdzanej, najbliższych członkach jej rodziny oraz ewentualnie innych osobach wskazanych w ankiecie bezpieczeństwa osobowego. Jednocześnie jednak przepisy ustawy zobowiązują organ prowadzący postępowanie sprawdzające m.in. do ustalenia, czy poziom życia osoby sprawdzanej jest adekwatny do uzyskiwanych przez nią dochodów (oczywiście w znaczeniu dochodu legalnie uzyskanego). Tymczasem jedynym punktem odniesienia do poziomu życia osoby sprawdzanej wcale nie muszą być – i w zdecydowanej większości przypadków nie są – tylko jej własne dochody, ale także dochody współmałżonka, a nierzadko także dochody innych osób – w przypadku, gdy te osoby przekazały osobie sprawdzanej np. darowiznę (lub darowiznę otrzymały)[9]. W obecnym stanie prawnym, jeżeli te osoby nie zostały wymienione w ankiecie, to organ nie może przetwarzać informacji na ich temat.

Analogiczny problem dotyczy osób podejrzewanych o kontakty z obcym wywiadem czy grupami przestępczymi. W celu określenia dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną organ powinien mieć możliwość sprawdzenia wszystkich

[9] W tym przypadku celem sprawdzenia jest ustalenie, czy tego typu operacja nie miała na celu np. ukrycia majątku przed opodatkowaniem.

osób, które się z nią kontaktowały albo kontaktują, lub z członkiem jej bliskiej rodziny. Powinno to nastąpić także wtedy, gdy te osoby nie są wymienione w ankiecie, a zwłaszcza – gdy nie są wymienione w ankiecie, a być powinny. Tak więc skuteczność postępowania (rzetelność dokonania oceny, czy osoba sprawdzana daje rękojmię zachowania tajemnicy) jest obecnie uzależniona od danych przekazanych przez osobę sprawdzaną.

Z tego względu jak najbardziej zasadne jest poszerzenie kręgu osób, których dane można przetwarzać w ramach postępowania, szczególnie biorąc pod uwagę dobro, jakim jest bezpieczeństwo państwa, w tym informacji niejawnych (oraz informacji niejawnych międzynarodowych, których zachowania w tajemnicy Rzeczpospolita Polska zobowiązała się strzec). Nie chodzi przy tym o możliwość przetwarzania dowolnych danych o dowolnych osobach, a jedynie tych danych (i tylko o tych osobach), które są niezbędne do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

Byłoby zatem wskazane dopuszczenie możliwości przetwarzania w ramach postępowań sprawdzających nie tylko informacji o osobie sprawdzanej, najbliższych członkach jej rodziny oraz ewentualnie innych osobach wymienionych w ankiecie (tak jak w obecnie obowiązującej ustawie), lecz także o wszystkich innych osobach, również niewymienionych w ankiecie, z którymi kontakty – choćby pośrednie – mogą mieć wpływ na ocenę dawania rękojmi zachowania tajemnicy. Dotyczy to przede wszystkim prowadzenia przez tego typu osoby (mające kontakt z samą osobą sprawdzaną, członkami jej rodziny, ale też np. z obywatelami innych państw, z którymi kontakt utrzymuje osoba sprawdzana) działalności w obcym wywiadzie, zorganizowanej grupie przestępczej albo w innej organizacji o podobnym charakterze.

Narzędzia weryfikacji danych

W aktualnie obowiązujących przepisach dotyczących czynności podejmowanych w ramach postępowań sprawdzających niewątpliwie brakuje regulacji umożliwiających wykorzystywanie badania poligraficznego jako skutecznego narzędzia weryfikacji zebranych informacji. Warto zaznaczyć, że wprowadzenie do ustawy możliwości wykonania takiego badania byłoby korzystne zarówno dla osoby poddanej postępowaniu (wprowadzenie możliwości przeprowadzenia badania wyłącznie na wniosek tej osoby w przypadku wątpliwości służby prowadzącej postępowanie dotyczących dawania przez nią rękojmi, przy zastrzeżeniu, że to badanie dotyczyłoby tylko weryfikacji występowania tych wątpliwości), jak i z punktu widzenia bezpieczeństwa państwa (wprowadzenie możliwości zobowiązania osoby sprawdzanej do poddania się takiemu badaniu w przypadku ściśle określonych wątpliwości[10]). Przy tym rozwiązaniu badanie powinny przeprowadzać wyłącznie służby uprawnione do realizacji poszerzonych postępowań sprawdzających. Nie powinno być ono przeprowadzane w przypadku wątpliwości natury zdrowotnej.

Analizując rozwiązania w powyższym zakresie obowiązujące w prawodawstwach innych państw, można stwierdzić, że badanie poligraficzne bywa elementem – obligatoryjnym lub fakultatywnym – postępowań sprawdzających (m.in. na Litwie, w Kanadzie i Rumunii) albo też niezbędnym uzupełnieniem tych postępowań (w USA – przy niektórych kategoriach dostępu do informacji niejawnych).

[10] Chodzi o wątpliwości dotyczące zagrożeń ze strony obcych służb specjalnych, grup terrorystycznych, wywrotowych lub przestępczych, a także niewłaściwego postępowania osoby sprawdzanej z informacjami prawnie chronionymi.

Poświadczenia bezpieczeństwa

Zasadne wydaje się wprowadzenie zmiany dotyczącej ważności (w znaczeniu: odpowiedniości) poświadczeń bezpieczeństwa wydanych przez inne służby niż ABW i SKW, zgodnie z którą poświadczenia w zakresie dostępu do informacji niejawnych o klauzuli „poufne" wydawane przez te organy byłyby ważne także poza służbą w tych organach[11]. To rozwiązanie jest w pełni uzasadnione pozycją wspomnianych służb w systemie organów państwowych odpowiedzialnych za bezpieczeństwo państwa, nawet w sytuacji, gdy postępowania poprzedzające wydanie takich poświadczeń nie będą podlegać kontroli zewnętrznej. Trudno bowiem uznać, że tego typu postępowania są i będą prowadzone według gorszych standardów niż zwykłe postępowania sprawdzające prowadzone przez pełnomocników ochrony w innych instytucjach państwowych, samorządowych oraz u przedsiębiorców, w których wyniku wydane poświadczenia umożliwiające dostęp do informacji o klauzuli „poufne" są przecież ważne po zmianie miejsca pracy osoby posiadającej takie poświadczenie.

Decyzja o odmowie wydania poświadczenia bezpieczeństwa

O prawnych podstawach decyzji negatywnej (odmowie wydania lub cofnięciu poświadczenia) powinien być informowany także kierujący wniosek o przeprowadzenie postępowania. Jest to całkowicie logiczne ze względu na dalsze konsekwencje tej decyzji w kontekście np. przepisów prawa pracy i korzystne dla obywateli. Warto przypomnieć, że obecnie kierownik jednostki otrzymuje jedynie informację o sposobie zakończenia postępowania.

Ponadto należy zauważyć, że przepisy ustawy w jej obecnym kształcie nie wykluczają sytuacji, gdy osoba, w stosunku do której stwierdzono, że nie daje rękojmi zachowania tajemnicy, nadal (przynajmniej na jakiś czas lub nawet w dłuższym okresie) będzie miała dostęp do informacji niejawnych na podstawie dotychczas posiadanych poświadczeń lub upoważnień. W związku z powyższym właściwe jest wprowadzenie zasady, zgodnie z którą w przypadku stwierdzenia przez służby uprawnione do prowadzenia poszerzonych postępowań sprawdzających, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy (a więc odmowy wydania poświadczenia bezpieczeństwa), z mocy prawa, bez konieczności wszczynania odrębnych, kontrolnych postępowań sprawdzających (szczególnie w sytuacji, gdy musiałby to zrobić inny organ niż ten, który odmówił wydania poświadczenia bezpieczeństwa), tracą ważność wszystkie posiadane przez taką osobę poświadczenia bezpieczeństwa, a także wydane przez ABW lub SKW upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone". Takie rozwiązanie w konsekwencji wymagałoby obowiązkowego poinformowania o takiej decyzji wszystkich organów, które wydały wcześniej wyżej wymienionej osobie poświadczenia i upoważnienia, ważne w chwili wydania decyzji o odmowie. Analogicznie, należałoby również rozważyć wprowadzenie wspomnianej zmiany do kontrolnych postępowań sprawdzających.

[11] Chodzi o przywrócenie stanu prawnego obowiązującego w latach 1999–2010, choć niezapisanego wprost w obowiązujących wówczas przepisach, a bazującego na opinii prawnej Agencji Bezpieczeństwa Wewnętrznego.

Decyzja o cofnięciu poświadczenia bezpieczeństwa

W celu uwzględnienia interesu obywateli, którzy z powodu braku zatrudnienia nie mają już dostępu do informacji niejawnych i o taki dostęp nie zamierzają się ubiegać, a jednocześnie nie życzą sobie być objętymi postępowaniami kontrolnymi, byłoby wskazane wprowadzenie prawnej możliwości skutecznego „zabezpieczenia" się przed taką aktywnością służb. Dana osoba powinna mieć możliwość złożenia oświadczenia o zrzeczeniu się uprawnień do dostępu do informacji niejawnych, jednocześnie jednak powinna odesłać oryginały posiadanych poświadczeń do organu, który je wydał (i zawiadomić o tym ABW lub SKW). Zasadne jest, aby w takim przypadku organ był zobowiązany do umorzenia już wszczętego postępowania kontrolnego oraz aby nie mógł wobec takiej osoby wszcząć tego typu postępowania.

Zasady realizacji postępowania kontrolnego

Z punktu widzenia systemu bezpieczeństwa informacji niejawnych istotna jest możliwość odpowiednio szybkiego i skutecznego reagowania przez ABW i SKW na nowe fakty dotyczące osoby posiadającej poświadczenie bezpieczeństwa, które mogą wpływać na jej wiarygodność (np. w sytuacji, gdy osoba zatrudniona w MSZ wstąpi w związek małżeński z obywatelem innego państwa). W powyższym zakresie przepisy ustawy nie zapewniają organom możliwości w pełni elastycznego reagowania i dlatego należy rozważyć ich uzupełnienie.

Przede wszystkim dla systemu ochrony informacji niejawnych byłoby istotne wprowadzenie możliwości weryfikacji przez służby tych danych, które mogą mieć kluczowe znaczenie dla oceny dawania rękojmi zachowania tajemnicy przez osobę posiadającą ważne poświadczenie bezpieczeństwa i zajmującą stanowisko związane z dostępem do informacji niejawnych. Ta weryfikacja powinna z jednej strony polegać na dokonaniu określonych sprawdzeń[12], a z drugiej – na zobowiązaniu osoby do uaktualnienia niezbędnych informacji zawartych w ankiecie (niewypełnienie tego zobowiązania będzie mogło stanowić podstawę do wszczęcia postępowania kontrolnego).

Warto dodać, że analogiczne lub zbliżone do proponowanych powyżej, a niekiedy nawet bardziej restrykcyjne, rozwiązania są stosowane przez takie państwa europejskie, jak m.in. Wielka Brytania[13], Niemcy czy Belgia[14].

[12] Nie tylko sprawdzenie w ewidencjach, rejestrach i kartotekach oraz innych zasobach informacyjnych, w tym niejawnych, w KRK, także uzyskanie informacji lub sprawdzenie innych danych zdobytych w toku postępowania, ale również rozmowa z osobą sprawdzaną oraz z innymi osobami, jeżeli mogą one dysponować informacjami, które mają wpływ na ocenę dawania rękojmi zachowania tajemnicy przez osobę sprawdzaną.

[13] Przykładowe rozwiązanie: informację wskazującą, że osoba może niewłaściwie postępować z informacjami niejawnymi, przekazuje drogą elektroniczną (formularz – *Aftercare Incident Report*) właściwemu organowi pełnomocnik ochrony albo każda inna osoba, w której ocenie istnieją uzasadnione wątpliwości w tym zakresie.

[14] W przypadku poinformowania właściwego organu o zawarciu małżeństwa lub nawiązaniu trwałej relacji z partnerem (partnerką) przez osobę mającą ważne uprawnienia w zakresie dostępu do informacji niejawnych, a jeżeli ta osoba ma dostęp do klauzuli odpowiadającej polskiej klauzuli „ściśle tajne" – w przypadku pojawienia się nowych pełnoletnich współmieszkańców osoby sprawdzonej – pełnomocnik ochrony składa wniosek o przeprowadzenie wobec tej osoby kolejnego postępowania sprawdzającego.

Zwolnienia z postępowań. Specjalny tryb realizacji postępowań sprawdzających

Względy bezpieczeństwa państwa skłaniają do rozważenia ewentualnych korekt w odniesieniu do ustawowego wykazu osób zwolnionych z obowiązku poddania się postępowaniu sprawdzającemu. Wyłączeniu z obowiązku poddania się postępowaniom sprawdzającym (wyłącznie w przypadku dostępu do „krajowych" informacji niejawnych o klauzuli nie wyższej, niż „tajne") – ze względu na umocowanie ustrojowo-konstytucyjne – powinni podlegać tylko sędziowie i prokuratorzy, a nie ławnicy i asesorzy, jak jest obecnie w ustawie. W stosunku zaś do samych sędziów i prokuratorów właściwe byłoby rozważenie wprowadzenia zasady, *per analogiam* do regulacji dotyczących posłów i senatorów, że wyłączenie z obowiązku poddania się sędziów i prokuratorów postępowaniom sprawdzającym nie będzie dotyczyło przypadków, gdy mają oni uzyskać dostęp do informacji niejawnych o klauzuli „ściśle tajne".

Odwołania i zasady realizacji postępowań odwoławczych

Zgodnie z przepisami ustawy w przypadku wydania przez pełnomocnika ochrony decyzji o odmowie wydania lub cofnięciu poświadczenia bezpieczeństwa albo decyzji o umorzeniu postępowania sprawdzającego postępowanie odwoławcze prowadzi ABW lub SKW. Ponieważ jednak większość decyzji pełnomocnika o odmowie wydania poświadczeń bezpieczeństwa oraz zdecydowana większość decyzji o ich cofnięciu była wydawana na podstawie informacji uzyskanych z ABW lub SKW, wskazane jest, aby organem odwoławczym od tych decyzji był organ inny (np. KPRM) niż wymienione powyżej. W opinii autorów opracowania nie jest właściwe, aby sama służba rozpatrywała odwołanie od decyzji wydanej na podstawie własnej opinii (osoby sprawdzane mogłyby wtedy podnosić, że wynik takiego postępowania łatwo przewidzieć). Powyższa zmiana z pewnością poprawiłaby pozycję obywatela w procesie odwoławczym. Zasadne jest zatem, aby wszystkie postępowania odwoławcze, w tym postępowania prowadzone po wydaniu decyzji przez pełnomocnika ochrony, prowadził wskazany w ustawie organ wyższej instancji, inny niż ABW i SKW[15].

5. Kontrole

W sferze kontroli stanu zabezpieczenia informacji niejawnych najczęściej spotykanym problemem jest brak możliwości zweryfikowania wszelkich informacji zebranych w ramach kontroli od osób oraz podmiotów, które nie są jej przedmiotem – chodzi o weryfikację informacji u byłych pracowników kontrolowanej jednostki, a także w podmiotach, których działalność pozostaje w związku z kontrolowaną jednostką. Obecne uprawnienie polegające na możliwości zasięgania – z uwagi na przeprowadzaną kontrolę – informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądanie wyjaśnień od kierowników i pracowników tych jednostek nie pozwala na wszechstronną weryfikację informacji uzyskanych w takim trybie. Tym samym nie można w sposób jednoznaczny ustalić stanu faktycznego badanych okoliczności.

[15] Dotyczy to również składania zażaleń na postanowienia wydawane w trakcie postępowań sprawdzających (o zawieszeniu postępowania lub postępowania kontrolnego oraz o podjęciu zawieszonego postępowania lub zawieszonego postępowania kontrolnego, a także na postanowienie o odmowie wszczęcia postępowania) – art. 40 ustawy.

Wskazane byłoby więc umożliwienie odbierania wyjaśnień właśnie od byłych pracowników kontrolowanej jednostki organizacyjnej, co zresztą pozostawałoby w korespondencji z uprawnieniami kontrolerów NIK w tym zakresie. Ponadto zasadne byłoby dodanie możliwości wykonywania określonych uprawnień kontrolnych (m.in. żądania udzielania wyjaśnień, dokonywania oględzin, badania obiegu informacji niejawnych) w stosunku do jednostek niekontrolowanych, ale wyłącznie w zakresie weryfikacji ustaleń, które pozostają w związku z prowadzoną kontrolą w jednostce kontrolowanej. Uprawnienie w nowej formule miałoby na celu umożliwienie dogłębnego ustalenia stanu faktycznego przez weryfikację uzyskanych informacji czy ustaleń mających lub mogących mieć wpływ na stan zabezpieczenia informacji niejawnych, bez konieczności wszczynania odrębnej kontroli w jednostce niebędącej jej przedmiotem.

6. Bezpieczeństwo fizyczne

W obszarze wskazanym w tytule uwagę zwraca brak jednolitych wymagań dotyczących stosowania wyposażenia i urządzeń służących ochronie informacji niejawnych we wszystkich jednostkach organizacyjnych, w których są przetwarzane informacje oznaczone klauzulą „poufne" i wyższą. Przepisy ustawy powinny nałożyć obowiązek stosowania przez te jednostki jednolitych wymogów określonych szczegółowo w odpowiednich aktach prawnych (rozporządzeniach) w odniesieniu do dedykowanych środków bezpieczeństwa fizycznego.

Wprowadzenie powyższej zmiany pozwoliłoby na określenie wykazu środków bezpieczeństwa fizycznego wraz z wymaganiami, jakie winny spełniać poszczególne urządzenia i wyposażenie, by mogły być wykorzystywane do ochrony informacji niejawnych (np. posiadanie certyfikatu, poświadczenia zgodności czy spełniania określonych parametrów technicznych lub norm). Metodologie oraz dobór tych środków w zależności od poziomu zagrożeń byłyby regulowane, podobnie jak to jest dotychczas, odpowiednimi przepisami wykonawczymi z uwzględnieniem statusu (charakteru) danej jednostki organizacyjnej (tj. rozporządzenie, zarządzenie).

Opisane propozycje rozwiązań nie powinny natomiast dotyczyć służb (ABW, SKW, SWW, CBA, BOR, Policji, ŻW, Służby Więziennej, Straży Granicznej[16]), ale jedynie w zakresie wymogów określonych w rozporządzeniu. Jest to uzasadnione przyjętymi rozwiązaniami w zakresie bezpieczeństwa fizycznego w tych służbach, które z uwagi na specyfikę ich zadań przewyższają ogólne standardy wynikające z obowiązujących przepisów w tej materii. W związku z tym brak powyższego wymogu nie spowodowałby zagrożenia bezpieczeństwa informacji niejawnych przetwarzanych przez te służby. Wyłączenie, o którym mowa, nie powinno dotyczyć wyposażenia i urządzeń służących ochronie informacji niejawnych międzynarodowych ze względu na odrębne przepisy w tym zakresie.

7. Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

Przepisy regulujące problem udostępniania akt postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego nie-

[16] Te służby nie będą np. zobligowane do stosowania certyfikowanego wyposażenia i urządzeń służących ochronie informacji niejawnych.

jednokrotnie uniemożliwiają wyjaśnienie wątpliwości dotyczących dawania rękojmi zachowania tajemnicy, także przez osoby ważne dla bezpieczeństwa państwa, tylko dlatego, że służba, która przeprowadziła poprzednie postępowanie, nie może udostępnić akt służbie prowadzącej kolejne lub kontrolne postępowanie sprawdzające. Bardzo rygorystyczne regulacje w tym zakresie uniemożliwiają ponadto najważniejszym organom odpowiedzialnym za bezpieczeństwo państwa zapoznanie się z ustaleniami służb specjalnych powołanych m.in. w celu realizacji procedur określonych w ustawie, zmierzających do zapewnienia tego bezpieczeństwa. W ustawie nie wskazano również, że przepisy dotyczące udostępniania akt postępowań sprawdzających dotyczą także akt kontrolnych postępowań sprawdzających.

W związku z powyższym rozważenie wprowadzenia w przepisach takich zmian, które wyeliminowałyby część ograniczeń w udostępnianiu akt postępowań, a także zawartych w nich informacji i dokumentów (wyciągów), należy uznać za priorytetowe. Przede wszystkim udostępnieniu powinny podlegać nie tylko same akta zgodnie z przepisami art. 72 ustawy, lecz także konkretne informacje zgromadzone w tych aktach, przy czym służba – dysponent akt (także informacji z akt) – powinna mieć możliwość odmówienia ich udostępnienia z uwagi na jej ważny interes. Powyższe mogłoby dotyczyć także udostępniania akt (także informacji z akt) właściwemu organowi do celów postępowania karnego, karno-skarbowego oraz podatkowego.

Ze względów praktycznych wskazane byłoby również zrezygnowanie z ograniczenia dotyczącego udostępniania akt postępowań tylko na potrzeby postępowań prowadzonych wobec tej samej osoby – także dlatego, że taki zapis czyni martwym przepis o udostępnianiu akt postępowań bezpieczeństwa przemysłowego. Niejednokrotnie też informacje i dokumenty zgromadzone przez służbę wobec jednej osoby mogłyby zostać wykorzystane do postępowania prowadzonego wobec małżonka tej osoby, co z jednej strony ułatwiłoby prowadzenie postępowania organowi, a z drugiej – byłoby mniej uciążliwe dla osoby sprawdzanej.

Istotną propozycją, której wprowadzenie należy rozważyć, jest możliwość udostępnienia informacji z akt postępowań najwyższym organom państwa: Prezydentowi RP, Prezesowi Rady Ministrów, Marszałkowi Sejmu, jak również ministrowi nadzorującemu służby specjalne. Dodatkowo proponuje się rozważenie wprowadzenia regulacji, aby za zgodą tego ostatniego informacje te mogły zostać udostępnione ministrowi obrony narodowej, ministrowi sprawiedliwości oraz ministrom właściwym do spraw wewnętrznych i do spraw zagranicznych. Ma to uzasadnienie z uwagi na odpowiedzialność wyżej wymienionych organów za bezpieczeństwo państwa.

Zasadne wydaje się również wprowadzenie dodatkowej regulacji prawnej, na której podstawie dane z ewidencji osób mających dostęp do informacji niejawnych, prowadzonej przez ABW i SKW, w celu potwierdzenia posiadania lub braku uprawnień do dostępu do informacji niejawnych przez konkretne osoby, będą mogły dodatkowo zostać udostępnione podmiotowi, który wykaże interes prawny w uzyskaniu takich informacji, jeżeli nie będzie to stało w sprzeczności z interesem ochrony informacji niejawnych.

8. Bezpieczeństwo przemysłowe

Zgoda na dostęp przedsiębiorcy do informacji niejawnych

Zgodnie z przepisami ustawy upoważnieni do wydawania przedsiębiorcy zgody na dostęp do informacji niejawnych są: szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów, minister właściwy dla okre-

ślonego działu administracji rządowej oraz prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku – szef ABW albo szef SKW[17]. Tak wiele podmiotów uprawnionych do wydawania powyższej zgody niewątpliwie nie sprzyja bezpieczeństwu informacji niejawnych udostępnianych przedsiębiorcy objętemu zgodą, ponieważ większość z wymienionych organów nie ma uprawnień do wykonywania jakichkolwiek sprawdzeń i gromadzenia informacji o takim przedsiębiorcy. W celu zapewnienia właściwego poziomu ochrony informacjom przekazywanym w tym trybie i uniknięcia wydawania przedmiotowych zgód bez jakichkolwiek sprawdzeń w służbach odpowiedzialnych za ten obszar bezpieczeństwa państwa, należy rozważyć zawężenie kręgu podmiotów uprawnionych do wydawania zgody w zakresie dostępu do krajowych informacji niejawnych o klauzuli „poufne" lub wyższej przedsiębiorcom, wobec których wszczęto postępowanie bezpieczeństwa przemysłowego lub postępowanie sprawdzające (w przypadku przedsiębiorców prowadzących działalność jednoosobowo i osobiście), a także podmiotom, wobec których nie wszczęto postępowania (tzw. zgoda jednorazowa). Zgodę w powyższym zakresie wydawałyby wyłącznie ABW albo SKW, czyli organy uprawnione do prowadzenia postępowań bezpieczeństwa przemysłowego i postępowań sprawdzających, które z racji posiadanych uprawnień mogą dysponować szerszą wiedzą dotyczącą wnioskodawcy.

Kaskada świadectw bezpieczeństwa przemysłowego (ŚBP) I stopnia

Jeden z poważniejszych problemów w sferze bezpieczeństwa przemysłowego dotyczy następstw upływu terminu ważności akredytacji bezpieczeństwa systemu teleinformatycznego w przypadku przedsiębiorcy posiadającego ważne świadectwo bezpieczeństwa przemysłowego I stopnia[18]. W tej sytuacji ustawa dopuszcza dwa warianty postępowania: pierwszy z nich przewiduje zrzeczenie się przez przedsiębiorcę uprawnień określonych w posiadanym świadectwie (w rzeczywistości brak możliwości przetwarzania informacji niejawnych), drugi zaś – możliwość cofnięcia przez ABW lub SKW przedsiębiorcy świadectwa po stwierdzeniu utraty przez niego zdolności do ochrony informacji niejawnych z powodu utarty funkcjonalności sytemu ochrony tych informacji. Oba warianty skutkują brakiem możliwości wykonywania przez przedsiębiorcę umów związanych z dostępem do informacji niejawnych.

Proponowanym, niewątpliwie korzystnym dla przedsiębiorców, rozwiązaniem byłoby wprowadzenie tzw. kaskady stopni świadectwa bezpieczeństwa przemysłowego. Kaskada dotyczyłaby świadectwa pierwszego stopnia i skutkowałaby utrzymaniem ważności świadectwa bezpieczeństwa przemysłowego na poziomie stopnia drugiego[19] w przypadku upływu terminu ważności akredytacji bezpieczeństwa teleinformatycznego. Zastosowanie powyższego rozwiązania byłoby korzystne z punktu widzenia tych przedsiębiorców wykorzystujących systemy teleinformatyczne, w których przypadku w okresie ważności ŚBP upływa termin ważności wspomnianej akredytacji; w tej sytuacji zachowaliby oni możliwość realizowania umów wymagających posiadania świadectwa drugiego lub trzeciego stopnia[20], co nie pozostaje bez znaczenia również dla pod-

[17] Art. 54 ust. 7 ustawy

[18] Świadectwo potwierdzające pełną zdolność przedsiębiorcy do ochrony informacji niejawnych.

[19] Świadectwo potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych.

[20] Świadectwo potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych, z wyłączeniem

miotów zlecających realizację umów związanych z dostępem do informacji niejawnych, miałyby one bowiem możliwość podpisania umowy w zakresie świadectwa drugiego i trzeciego stopnia z przedsiębiorcą legitymującym się świadectwem bezpieczeństwa przemysłowego pierwszego stopnia, bez ryzyka utraty przez wykonawcę umowy – w trakcie jej realizacji – zdolności do ochrony informacji niejawnych z powodu upływu terminu ważności akredytacji bezpieczeństwa systemu teleinformatycznego.

Przesłanki odmowy wydania świadectwa bezpieczeństwa przemysłowego i cofnięcia posiadanego świadectwa

Praktyka stosowania przepisów ustawy w obszarze bezpieczeństwa przemysłowego skłania do rozważenia zmiany w zakresie przesłanek odmowy wydania świadectwa bezpieczeństwa przemysłowego:

a) przesłanki obligatoryjne:
   - obecna ustawa zawiera nieprecyzyjny zapis, zgodnie z którym ABW lub SKW odmawia wydania świadectwa z powodu (…) *braku możliwości ustalenia* (…) *źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy*[21], co wpływa na to, że ten zapis może być interpretowany jako konieczność ustalenia jedynie źródła wspomnianych środków, z pominięciem legalności ich uzyskania. To z punktu widzenia przyznania jakichkolwiek uprawnień podmiotowi nie może być akceptowane. Dlatego też należy rozważyć rozszerzenie katalogu przesłanek obligatoryjnych wprost o brak możliwości ustalenia legalności pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy. Chodzi o możliwość wydania decyzji o odmowie przyznania świadectwa przedsiębiorcy w przypadku uzasadnionego podejrzenia pochodzenia tych środków ze źródła nielegalnego;
   - stwierdzono również przypadki, w których członkami organów zarządzających lub kontrolnych przedsiębiorcy oraz osobami powoływanymi do pełnienia funkcji kierownika jednostki organizacyjnej zostają osoby, które de facto nie mają realnego wpływu na działalność przedsiębiorcy. Faktycznie natomiast działalnością podmiotu kieruje osoba, wobec której występują wątpliwości mogące mieć szkodliwy wpływ na poziom ochrony informacji niejawnych przetwarzanych przez przedsiębiorcę. Chodzi zarówno o osoby dysponujące bezpośrednio lub pośrednio większością głosów na zgromadzeniu wspólników lub walnym zgromadzeniu sprawdzanego przedsiębiorcy, jak i posiadające możliwość samodzielnego decydowania o powołaniu większości członków rady nadzorczej i zarządu oraz wywierania decydującego wpływu na działalność podmiotu np. przez umowę na zarządzanie podmiotem. Wskazane jest więc rozważenie poszerzenia wykazu przesłanek obligatoryjnych o wystąpienie negatywnych okoliczności[22] związanych z osobą, która ma rzeczywisty

możliwości ich przetwarzania w użytkowanych przez niego obiektach.

[21] Art. 64 ust. 2 pkt 2 ustawy.

[22] Skazanie prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe albo nieprawomocne skazanie lub oskarżenie albo przedstawienie zarzutów popełnienia przestępstwa umyślnego, ściganego z oskarżenia publicznego lub umyślnego przestępstwa skarbowego, zagrożonego karą pozbawienia wolności powyżej lat 3.

wpływ na działalność przedsiębiorcy[23]. Obecnie fakultatywną podstawą do odmowy wydania świadectwa są niedające się usunąć wątpliwości (określone w ustawie[24]) dotyczące wyłącznie osób wchodzących w skład organów zarządzających, kontrolnych oraz osób działających z ich upoważnienia.
Proponowana zmiana miałaby na celu uzależnienie wyniku postępowania od niewystępowania wątpliwości wobec osób będących faktycznymi zarządcami lub właścicielami przedsiębiorstwa.

b) przesłanki fakultatywne:
   – w coraz większej liczbie podmiotów instytucjonalnych mających udziałowców zagranicznych może występować ryzyko związane z nielegalną działalnością ze sfery terroryzmu czy szpiegostwa lub występowaniem innych przestępstw. Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego, jako organy prowadzące postępowania bezpieczeństwa przemysłowego, muszą mieć możliwość adekwatnego reagowania w wymienionych przypadkach przez negatywną ocenę zdolności do ochrony informacji niejawnych tych przedsiębiorców. Dlatego też należy rozważyć uwzględnienie w przepisach, co najmniej jako przesłanki fakultatywnej, negatywnych wyników sprawdzeń podmiotu zagranicznego posiadającego wkład, udziały lub akcje w sprawdzanym podmiocie, wobec którego organ prowadzący postępowanie bezpieczeństwa przemysłowego uzyskał informacje o jakiejkolwiek działalności nielegalnej.

Konsekwencją ewentualnego wprowadzenia powyższych rozwiązań powinno być wprowadzenie analogicznych zmian w przepisach dotyczących podstawy (obligatoryjnej bądź fakultatywnej) cofnięcia posiadanego świadectwa bezpieczeństwa przemysłowego.

Warto wspomnieć, że problematyka dotycząca wpływu podmiotów zagranicznych na zdolność przedsiębiorcy do ochrony informacji niejawnych jest w ostatnich latach mocno eksponowana przez zagranicznych ekspertów w dziedzinie ochrony tego typu informacji w sferze bezpieczeństwa przemysłowego. Przepisy wykonawcze w tym zakresie wprowadziły do swojego systemu prawnego m.in. Stany Zjednoczone Ameryki[25], Kanada[26] i Wielka Brytania[27].

9. Wzór ankiety bezpieczeństwa osobowego

Uwzględniając dynamiczny rozwój informatyczny, należy dokonać zmian dotyczących wzoru ankiety bezpieczeństwa osobowego, będącego załącznikiem do ustawy, i sposobu jego przesyłania do organu prowadzącego postępowanie. Należy zmierzać do takiego rozwiązania, aby ankieta bezpieczeństwa osobowego mogła stać się dokumen-

[23] Obecnie są to jedynie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia.

[24] Artykuł 24 ust. 2 pkt 1–3 lub 5 lub art. 24 ust. 3 ustawy – uczestnictwo w działalności wymierzonej przeciwko RP (szpiegostwo, terroryzm, sabotaż); zagrożenia ze strony obcych służb specjalnych; nieprzestrzeganie porządku konstytucyjnego; okoliczności powodujące podatność na szantaż lub wywieranie presji; poziom życia wyraźnie przewyższający uzyskiwane dochody; choroby psychiczne i uzależnienia (alkohol, środki odurzające lub substancje psychotropowe).

[25] Department of Defense Manual 5220.22 „National Industrial Security Program: Procedures For Government Activities Relating To Foreign Ownership, Control Or Influence (FOCI)".

[26] „Industrial Security Manual", Public Works and Services Canada.

[27] „Security Requirements for List X Contractors", Cabinet Office, National Security and Intelligence, Government Security Profession.

tem wypełnianym za pośrednictwem odpowiedniego programu komputerowego, dostępnego do jednorazowego pobrania ze strony ABW lub SKW (podobnie jak w przypadku deklaracji podatkowych). W dalszej perspektywie należy przeanalizować możliwość przesyłania wypełnionej ankiety do ABW lub SKW także drogą elektroniczną. Użycie odpowiedniego programu umożliwiłoby „spłaszczenie" ankiety w postaci eliminacji wszystkich jej podpunktów powiązanych z nadrzędnym pytaniem, jeżeli odpowiedź na to pytanie czyni bezzasadnym ich wypełnienie. Przy każdym pytaniu powinna istnieć możliwość wyświetlenia szczegółowych wskazówek dotyczących sposobu udzielania odpowiedzi (wypełnienia tego konkretnego punktu).

Tak jak podkreślono na wstępie, opracowanie jest oparte na subiektywnej ocenie autorów i jest ich propozycją zmian wybranych zagadnień z zakresu ochrony informacji niejawnych. Należy je traktować jako głos w szerszej dyskusji dotyczącej konieczności dostosowywania wszelkich środków bezpieczeństwa państwa do zmieniającej się rzeczywistości, nowych zagrożeń i oczekiwań skierowanych do służb specjalnych w zakresie skutecznego reagowania na te zagrożenia. Ponieważ mowa jest o bezpieczeństwie państwa, dyskusja na temat ewentualnych zmian w obowiązujących przepisach związanych z ochroną informacji niejawnych, jako integralnego elementu tego bezpieczeństwa, wydaje się nieunikniona i niezbędna.