KORNELA OBLIŃSKA
Warszawa

Wpływ integracji europejskiej na zmianę przepisów prawa w Polsce w zakresie ochrony informacji niejawnych

Zobowiązania międzynarodowe a ochrona informacji niejawnych

Przystąpienie Polski do Unii Europejskiej oraz wynikające z tego faktu nieodzowne zobowiązania w ramach funkcjonowania w UE, a także akcesja Polski do Sojuszu Północnoatlantyckiego NATO, spowodowały szereg zmian, zmierzających do dostosowania standardów krajowych do ogólnie obowiązujących w prawodawstwie naszych zagranicznych partnerów. Proces kształtowania systemu koordynacji polityki europejskiej RP rozpoczął się na długo przed akcesją i opierał się na doświadczeniach z wcześniejszych etapów współpracy ze Wspólnotami Europejskimi czy Unią Europejską, chociażby z okresu stowarzyszenia czy rokowań akcesyjnych, jednak wraz z uzyskaniem członkostwa nastąpiła istotna zmiana jakościowa. Polska zaczęła współtworzyć politykę oraz współstanowić prawo Unii Europejskiej[1]. Dynamicznie rozwijająca się współpraca, poszerzanie naszej zagranicznej aktywności, zarówno w aspekcie bezpieczeństwa wewnętrznego, jak i zewnętrznego spowodowały konieczność dostosowania prawa do obowiązujących norm prawa międzynarodowego. Jednym ze strategicznych obszarów prawa, nieodzownym do prawidłowego funkcjonowania na arenie międzynarodowej, stała się ochrona informacji niejawnych tzn. informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem, jako stanowiące tajemnicę, niezależnie od formy i sposobu ich wyrażenia, także w trakcie ich opracowania. Unormowania w przedmiotowym zakresie, wynikają m.in. z Konstytucji RP (art. 61 ust. 3), ratyfikowanych, bilateralnych umów międzynarodowych o wzajemnej ochronie informacji niejawnych (m.in. z takimi państwami, jak: Albania, Bułgaria, Chorwacja, Czechy, Estonia, Finlandia, Francja, Hiszpania, Łotwa, Norwegia, Niemcy, Rosja itp.,), umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji (Bruksela, 6.03.1997 r., Dz. U. 2000, Nr 64, poz. 740), umowy między stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych (Paryż, 18.06.1964 r., Dz. U. 2001, Nr 143, poz. 1594) oraz ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (dotychczas 23-krotnie nowelizowanej).

Bez wątpienia, przystąpienie Polski do Unii Europejskiej spowodowało istotne konsekwencje w zakresie działalności prawodawczej. Obok krajowego porządku prawnego obowiązywać zaczął system prawny UE oparty na traktatach założycielskich oraz na tworzonym przez instytucje UE prawie pochodnym. Równolegle inicjatywy pro-

[1] *5 lat Polski w Unii Europejskiej*, red. M. Kałużyńska, K. Smyk, J. Wiśniewski, UKIE, Warszawa 2009, s. 447.

mowane na poziomie UE stanowiły dla Polski szansę na poprawę jakości polskiego prawa, zarówno obowiązującego, jak i nowo tworzonego[2].

Zobowiązania wynikające z dynamicznie rozwijającej się współpracy międzynarodowej, a także konieczność uelastycznienia uregulowań na niwie krajowej, wpłynęły na konieczność zmian prawnych, w tym w zakresie ochrony informacji niejawnych. Mając powyższe na uwadze, na wyraźne postulaty MSZ, rozpoczęto intensywne prace nad nową ustawą o ochronie informacji niejawnych. Dlaczego nową, a nie kolejną nowelizacją? Powód jest prosty, zakres wymaganych zmian wymusiłby konieczność całkowitego przemodelowania dotychczasowego aktu prawnego tj. ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Jak wspomniano powyżej, dotychczas przedmiotowa ustawa była nowelizowana 23-krotnie, zaś nowelizacja z 2005 roku spowodowała praktyczną zmianę ponad 1/3 obowiązujących zapisów. Kolejne zmiany mogłyby spowodować rażącą nieczytelność i niespójność ustawy.

Ze względu na zaistniałe okoliczności, a także z uwagi na konieczność zapewnienia maksymalnej efektywności, zarówno w sferze krajowej, jak i zagranicznej, uproszczenie strategicznych procedur m.in. ograniczenie liczby nadawania, zawyżania klauzul oraz możliwość zmiany klauzul, a także potrzebę racjonalizacji nakładów, w postaci m.in. ograniczenia liczby kancelarii tajnych, a tym samym kosztów związanych z ich utrzymaniem, postanowiono o radykalnych zmianach. Oprócz wyżej wymienionych czynników, nadrzędną rolę odgrywała konieczność należytego zapewnienia bezpieczeństwa informacji niejawnych, ze szczególnym uwzględnieniem bezpieczeństwa teleinformatycznego (proces akredytacji, certyfikacji), a w rezultacie potrzeba właściwego i skutecznego zabezpieczenia materiałów o charakterze niejawnym, przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

W wyniku intensywnych prac, przygotowano nową ustawę o ochronie informacji niejawnych z dnia 5 sierpnia 2010 roku, która 30 sierpnia została podpisana przez Prezydenta RP. Następnie, 1 października br., ustawa została ogłoszona, tym samym oznacza to, iż nowa ustawa zacznie obowiązywać od 1 stycznia 2011 roku. Z uwagi na obszerność i specyfikę zagadnienia, nowa ustawa przewiduje 12-miesięczny okres przejściowy, na przygotowanie niezbędnych aktów wykonawczych – rozporządzeń. W przedmiotowym okresie, użytkownicy ustawy będą działali na podstawie nowej ustawy, jednak posiłkując się starymi, nieaktualnymi rozporządzeniami, co może prowadzić do pewnych konfuzji i nieporozumień z uwagi na zmiany w zakresie ochrony informacji niejawnych o charakterze strategicznym. Będzie to swoisty dualizm, trudny szczególnie dla osób od lat zajmujących się ochroną informacji niejawnych, gdyż jak wiemy: „przyzwyczajenie jest drugą naturą", wymagający rozwagi, rzetelności i konsekwencji w działaniu. Kluczowym zagadnieniem w ochronie informacji niejawnych jest proces przetwarzania informacji niejawnych, polegający na: wytwarzaniu, modyfikowaniu, kopiowaniu, klasyfikowaniu, gromadzeniu, przechowywaniu, przekazywaniu oraz udostępnianiu informacji, wymagających prawnej ochrony.

W celu zapewnienia najwyższych standardów ochrony przyjęto założenia SZBI: Systemowego Zarządzania Bezpieczeństwem Informacji ISO/IEC 27002 (PN ISO/IEC

[2] Ibidem, s. 476.

17799:2007), mających na celu zapewnienie najbardziej pożądanych wymogów w zakresie bezpieczeństwa fizycznego, teleinformatycznego itp. w oparciu o zidentyfikowanie ryzyka (kombinacji prawdopodobieństwa wystąpienia zdarzeń niepożądanych i ich konsekwencji), przeprowadzenie całościowego procesu analizy i oceny ryzyka tzw. szacowanie ryzyka oraz finalnie, odpowiednio skoordynowanie działań w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka tj. umiejętne zarządzanie ryzykiem. Należy pamiętać, że zagrożenie jest potencjalną przyczyną niepożądanego zdarzenia, którego wystąpienie może prowadzić do szkody jest okolicznością sprzyjającą popełnieniu przestępstwa[3].

Ochrona informacji niejawnych

Klasyfikowanie informacji niejawnych – zmiana klauzuli

Właściwe zarządzanie informacją wymaga odpowiedniego sklasyfikowania informacji, w przedmiotowym przypadku informacji niejawnych. W celu określenia swoistych stopni ważności poszczególnych informacji niejawnych, nieodzowne jest nadanie stosownej klauzuli. W polskim ustawodawstwie, w oparciu o nową gradację – wysokości szkody, wyróżniamy następujące klauzule tajności:

– „ściśle tajne", oznaczające m.in., że nieuprawnione ujawnienie może spowodować wyjątkowo poważną szkodę dla RP (m.in. zagrożenie dla niepodległości, suwerenności, integralności);
– „tajne", gdy nieuprawnione ujawnienie może spowodować poważną szkodę dla RP (m.in. uniemożliwienie wykonania zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP);
– „poufne", oznaczające sytuację, gdy nieuprawnione ujawnienie może spowodować szkodę dla RP (m.in. utrudnienie prowadzenia bieżącej polityki zagranicznej RP);
– „zastrzeżone", gdzie ewentualne, nieuprawnione ujawnienie może mieć szkodliwy wpływ m.in. na wykonywanie przez organy władzy publicznej zadań albo interes ekonomiczny RP.

Z uwagi na intensywny proces integracji europejskiej, a tym samym międzynarodowe zobowiązania RP, należy zauważyć, że informacje niejawne przekazywane w ramach współpracy przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskimi odpowiednikami klauzul tajności tj.: „ściśle tajne" jako top secret, „tajne" jako secret, „poufne" confidential oraz „zastrzeżone" jako restricted. Na uwagę zasługuje fakt, iż pośród ogólnie ww. przyjętej przez środowisko międzynarodowe terminologii, zdarzają się wyjątki, jak np. w przypadku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej przed poszczególną klauzulą dodawane są litery UK np. UK SECRET itp. W przypadku Stanów Zjednoczonych, zauważalny jest brak klauzuli restricted (polskiego odpowiednika zastrze-

[3] J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, wyd. Konsalnet, Warszawa 2004, s. 15.

żone), gdzie informacje o klauzuli zastrzeżone traktowane są na równi z informacjami niejawnymi o klauzuli poufne. Ponadto, na uwagę zasługuje Francja, której klauzule niejawności wyglądają następująco: Tres secret (ściśle tajne), defense secret (tajne), defense confidentiel (poufne) i defense diffusion restreinte (zastrzeżone). Tak więc, mimo międzynarodowej polityki spójności, mamy do czynienia z indywidualnymi przypadkami odmiennych rozwiązań, wynikających głównie ze specyficznej mentalności.

W celu uelastycznienia wspomnianych procedur, nieodzowna stała się możliwość zmiany klauzuli tajności (dotychczas niedopuszczalna!), charakteryzująca się zniesieniem lub zmianą w wyniku ustania ustawowych przesłanek ochrony danej informacji. Ponadto, bardzo korzystną zmianą jest odejście od zdefiniowanych okresów obowiązywania klauzuli tajności, możliwość określenia z góry (bez względu na klauzulę) daty lub wydarzenia powodującego zmianę klauzuli oraz odrębnego nadawania klauzuli poszczególnym częściom dokumentu. Kolejnym, bardzo istotnym i potrzebnym zapisem jest obowiązek przeglądu raz na pięć lat, wszystkich wytworzonych dokumentów niejawnych, w celu sprawdzenia aktualności ustawowych przesłanek do posiadania danej klauzuli tajności. Obok możliwości zmiany klauzuli, kolejnym novum w przedmiotowym zakresie jest tzw. spór. W przypadku gdy mamy do czynienia z zawyżeniem lub zaniżeniem klauzuli, osobie stwierdzającej jedną z przedstawionych sytuacji tzw. odbiorcy materiału o charakterze niejawnym, przysługuje złożenie wniosku do osoby, która nadała daną klauzulę tajności, z którą nie zgadzamy się albo do jej przełożonego, w którym przestawiamy swoje uwagi. Adresat naszego wniosku ma 30 dni (od momentu otrzymania wniosku) na udzielenie odpowiedzi. W przypadku odmowy zmiany klauzuli tajności lub nieudzielenia odpowiedzi w terminie, mamy do czynienia ze „sporem", do którego rozwiązania jest właściwe ABW (Agencja Bezpieczeństwa Wewnętrznego tzw. sfera cywilna) lub SKW (Służba Kontrwywiadu Wojskowego tzw. sfera wojskowa), także w terminie 30 dni od otrzymania informacji. W przypadku potwierdzenia, iż dany dokument lub materiał o charakterze niejawnym wymaga zmiany lub zniesienia klauzuli, nieodzowna jest pisemna zgoda osoby nadającej klauzulę (albo jej przełożonego), następnie wymagane jest naniesienie odpowiednich zmian w oznaczeniu materiału oraz powiadomienie o zmianie wszystkich odbiorców danego materiału. Na uwagę zasługuje fakt, iż celem należytego zabezpieczenia materiałów o charakterze niejawnym, w przypadku rozwiązania lub likwidacji danej jednostki organizacyjnej, uprawniony następca prawny zobowiązany jest do przejęcia i odpowiedniego zabezpieczenia materiałów o charakterze niejawnym, zaś w przypadku jego braku, odpowiednio ABW lub SKW.

Bezpieczeństwo osobowe – dostęp do informacji niejawnych

W myśl uregulowań UE i NATO, niezbędne warunki, które muszą być zachowane, do uzyskania dostępu do informacji niejawnych, to konieczność posiadania odpowiednich i wymaganych uprawnień oraz gwarancja rękojmi zachowania tajemnicy tj. osobę dająca rękojmię musi charakteryzować zdolność do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem. Stwierdzenie zachowania rękojmi, a tym samym zachowania tajemnicy musi

nastąpić w wyniku przeprowadzenia odpowiedniego postępowania sprawdzającego. Istotnym jest, iż osoba ubiegająca się o dostęp do informacji niejawnych, otrzymuje dostęp do informacji w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku lub wykonywania czynności zleconych, z zachowaniem wszelkich zasad ochrony, zgodnie z nadaną klauzulą tajności tj. przetwarzanie informacji musi odbywać się w odpowiednich warunkach. Na uwagę zasługuje fakt, iż dopuszczenie do pracy, bądź pełnienia służby lub wykonywania zleconych prac, o klauzuli „poufne" lub wyższej wymaga uzyskania poświadczenia bezpieczeństwa oraz odbycia szkolenia w zakresie ochrony informacji niejawnych. Jeśli chodzi o dostęp do informacji niejawnych o klauzuli „zastrzeżone", zgodnie z systemem obowiązującym w większości krajów Europy (NATO i UE), niezbędne jest uzyskanie pisemnego upoważnienia kierownika jednostki organizacyjnej oraz odbycie szkolenia w zakresie ochrony informacji niejawnych.

W przypadku zmian, w zakresie prowadzenia postępowań sprawdzających, na szczególną uwagę zasługuje zniesienie obowiązku prowadzenia postępowań sprawdzających wobec osób mających uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone", tym samym eliminacja wymagania uzyskania poświadczenia bezpieczeństwa!

Godnym podkreślenia jest, iż kilka służb i instytucji samodzielnie przeprowadza postępowania sprawdzające tj.: Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Biuro Ochrony Rządu, Policja, Służba Więzienna, Służba Wywiadu Wojskowego, Straż Graniczna oraz Żandarmeria Wojskowa, z czego BOR w myśl nowej ustawy dopiero otrzymało przedmiotowe uprawnienia.

Postępowanie sprawdzające przeprowadzane jest za pisemną zgodą osoby sprawdzanej, zaś organ prowadzący postępowanie sprawdzające musi cechować: bezstronność, obiektywizm, najwyższa staranność, działanie zgodnie z przepisami ustawy, rzetelnie udokumentowane oraz terminowość tj. zakończenie postępowania przed upływem 3 miesięcy od wpływu ankiety lub złożenia wniosku wraz z wypełnioną ankietą. Istotnym jest, iż ankieta po wypełnieniu stanowi tajemnicę prawnie chronioną, otrzymując w przypadku poszerzonego postępowania sprawdzającego klauzulę „poufne", zaś w przypadku zwykłego postępowania sprawdzającego klauzulę „zastrzeżone". W celu sprawnego przeprowadzenia postępowania sprawdzającego, ustawa wprowadza jeden wzór ankiety bezpieczeństwa osobowego, która składa się z VII części, podczas gdy do tej pory funkcjonowały dwa wzory ankiety: do informacji oznaczonych klauzulą: zastrzeżone/poufne oraz tajne/ściśle tajne. Poszczególne części ankiety dotyczą: m.in. danych osobowych osoby sprawdzanej, współmałżonka (partnera życiowego), rodziców, rodzeństwa, dzieci oraz współmieszkańców, historii życia zawodowego i osobistego, ewentualnej współpracy, karalności, stanu zdrowia osoby sprawdzanej (kategorii zdrowia, ewentualnych zaburzeń psychicznych, zażywania leków psychotropowych, nałogów), sytuacji majątkowo-finansowej osoby sprawdzanej oraz osób pozostających z nią we wspólnym gospodarstwie domowym itp. Osoba ankietowana, ubiegająca się o dostęp do informacji niejawnych o klauzuli ściśle tajne, wskazuje w ostatniej – VII części, trzy osoby polecające.

Na uwagę zasługuje fakt, że osoby objęte zwykłym postępowaniem sprawdzającym, uprawniającym do dostępu do informacji opatrzonych klauzulą „poufne"

wypełniają części od I do IV ankiety, osoby objęte postępowaniem poszerzonym, ubiegające się o dostęp do informacji opatrzonych klauzulą „tajne" wypełniają części od I do VI, zaś osoby objęte postępowaniem poszerzonym, ubiegające się o dostęp do informacji opatrzonych klauzulą „ściśle tajne" lub stanowiących jej odpowiednik klauzul tajności organizacji międzynarodowej wypełniają całość ankiety.

Celem postępowania sprawdzającego jest ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, a także wyeliminowanie wątpliwości dotyczących ewentualnego uczestnictwa, współpracy lub popierania działań o charakterze:
– szpiegowskim;
– terrorystycznym;
– sabotażowym;
– innym przeciwko RP.

Ponadto, wyeliminowanie wątpliwości dotyczących ewentualnego zagrożenia przez obce służby specjalne próbami werbunku lub nawiązania kontaktu. Kluczową rolę odgrywa także konieczność przestrzegania porządku konstytucyjnego RP, z uwzględnieniem udziału w partiach, organizacjach itp. Postępowanie sprawdzające ma także na celu szczegółową analizę i sprawdzenie czy dane zawarte w ankiecie bezpieczeństwa są zgodne z prawdą, tym samym, czy osoba sprawdzana nie ukrywa lub świadomie nie podała w ankiecie bezpieczeństwa informacji niezgodnych z prawdą, ze szczególnym uwzględnieniem ewentualnego szantażu, wywierania presji, niewłaściwego postępowania z informacjami niejawnymi oraz informacji w zakresie poziomu życia, stanu zdrowia, nałogów itp.

Na uwagę zasługuje fakt, iż nie przeprowadza się postępowania sprawdzającego wobec: członków Rady Ministrów, Prezesa Narodowego Banku Polskiego, Prezesa Najwyższej Izby Kontroli, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, członków Rady Polityki Pieniężnej oraz Krajowej Rady Radiofonii i Telewizji, Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Szefów Kancelarii: Prezydenta RP, Sejmu, Senatu i Prezesa Rady Ministrów, posłów i senatorów, sędziów sądu powszechnego, wojskowego, Sądu Najwyższego, sądów administracyjnych, Naczelnego Sądu Administracyjnego, Trybunału Stanu i Trybunału Konstytucyjnego, ławników sądu powszechnego, sądu wojskowego, prokuratora, asesora prokuratury pełniącego czynności prokuratorskie. W przypadku, gdyby ww. osoby ubiegały się o dostęp do informacji niejawnych organizacji międzynarodowych lub o dostęp wynikający z umowy międzynarodowej zawartej przez RP, wówczas wymagane jest przeprowadzenie poszerzonego postępowania sprawdzającego przez ABW albo SKW. Przedmiotowe postępowanie przeprowadzane jest na wniosek osoby uprawnionej do powołania na dane stanowisko lub Marszałka Sejmu w stosunku do posłów albo Marszałka Senatu w stosunku do senatorów.

W ramach prowadzonego postępowania możliwe jest zawieszenie postępowania sprawdzającego, w przypadku gdy osoba sprawdzana choruje powyżej 30 dni, wyjeżdża za granicę na okres przekraczający 30 dni lub konieczne jest uzyskanie rozstrzygnięcia innego organu np. w sytuacji wszczęcia postępowania karnego itp. O zawieszeniu postępowania sprawdzającego, organ prowadzący postępowanie sprawdzające zobowiązany jest powiadomić: wnioskodawcę, pełnomocnika ochro-

ny oraz osobę sprawdzaną. Należy podkreślić, iż na postanowienie w sprawie zawieszenia przysługuje zażalenie.

Zawieszone postępowanie może zostać podjęte w sytuacji, gdy ustąpią przyczyny uzasadniające zawieszenie postępowania lub zostaną ujawnione okoliczności uzasadniające odmowę wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego. Analogicznie o podjęciu zawieszonego postępowania sprawdzającego organ prowadzący postępowanie sprawdzające zawiadamia: wnioskodawcę, pełnomocnika ochrony oraz osobę sprawdzaną. Postępowanie sprawdzające może zakończyć się wydaniem poświadczenia bezpieczeństwa, odmową wydania poświadczenia bezpieczeństwa lub umorzeniem. Zakończenie postępowania sprawdzającego z wynikiem pozytywnym jest jednoznaczne z wydaniem poświadczenia bezpieczeństwa, które powinno zawierać m.in.: numer poświadczenia, podstawę prawną, wskazanie wnioskodawcy postępowania sprawdzającego, określenie organu, który przeprowadził postępowanie sprawdzające, datę i miejsce wystawienia itp.

Istotnym jest procedura poszerzonej kontroli w zakresie prowadzonych postępowań, zarówno sprawdzającego, kontrolnego postępowania sprawdzającego oraz postępowania bezpieczeństwa przemysłowego, która w myśl nowych przepisów będzie prowadzona przez:

– Prezesa Rady Ministrów w stosunku do ABW albo SKW;
– ABW lub SKW (wg właściwości: sfera cywilna i wojskowa) w stosunku do poszczególnych pełnomocników ochrony.

Środki bezpieczeństwa fizycznego – kancelaria tajna

W celu uniemożliwienia dostępu do informacji niejawnych osobom nieuprawnionym lub ewentualnej utraty tych informacji, wymagane jest stosowanie środków bezpieczeństwa fizycznego. Zastosowanie przedmiotowych środków musi być poprzedzone oszacowaniem ryzyka i odpowiednio dostosowane do poziomu zagrożeń, z uwzględnieniem rodzajów zagrożeń, klauzul tajności, liczby informacji niejawnych, w tym ewentualnych wskazań ABW lub SKW. Środki bezpieczeństwa fizycznego mają za zadanie chronić w szczególności przed działaniem obcych służb, ewentualnymi zamachami terrorystycznymi, sabotażem, kradzieżą lub zniszczeniem materiału, próbą wejścia osób nieuprawnionych do pomieszczeń, w których przetwarza się informacje niejawne oraz przed nieuprawnionym dostępem, wynikającym z braku uprawnień do informacji o wyższej klauzuli tajności.

W przypadku informacji niejawnych o klauzuli „poufne" lub wyższej, nieodzowne jest zastosowanie środków, które uniemożliwią do nich dostęp m.in. poprzez zorganizowanie stref ochronnych (wraz z określeniem uprawnień do przebywania w nich oraz wprowadzeniem systemu kontroli wejść i wyjść), a także poprzez zastosowanie certyfikowanych urządzeń i wyposażenia, które posłużą do zapewnienia wymaganej ochrony.

Kluczową rolę w zakresie zapewnienia bezpieczeństwa informacji niejawnych pełni kancelaria tajna. W celu zachowania wysokich standardów ochrony informacji niejawnych o najwyższej klauzuli, zgodnie z zasadami funkcjonującymi w UE, obowiązek utworzenia kancelarii tajnej dotyczy posiadania, przetwarzania informacji nie-

jawnych o klauzuli „tajne" lub „ściśle tajne". Jednym z głównych celów utworzenia kancelarii tajnej jest odmowa udostępnienia lub wydania materiału osobie nieuprawnionej. Nowością jest, iż obecnie zasady dotyczące informacji niejawnych o klauzuli „poufne" określa kierownik jednostki organizacyjnej, na którym spoczywa obowiązek ustalania poziomu zagrożenia ujawnienia informacji niejawnych i szacowania wyżej wspomnianego ryzyka.

Jeśli chodzi o ilość kancelarii tajnych, głównym kryterium ich organizacji, powinna być racjonalizacja m.in. kilka jednostek organizacyjnych może być obsługiwane przez jedną kancelarię tajną, na zasadzie porozumienia kierowników w zakresie podległości i finansowania oraz za zgodą ABW lub SKW. Wymagane jest, aby zarówno o utworzeniu, jak i ewentualnej likwidacji kancelarii tajnej poinformować ABW lub SKW, wraz z podaniem klauzuli tajności. Przedmiotowe informacje są nieodzowne do prowadzenia aktualnego, na bieżąco weryfikowanego i uzupełnianego wykazu jednostek posiadających kancelarię tajną, co umożliwi sprawny przepływ informacji niejawnych o klauzuli tajne/ściśle tajne.

Kancelaria tajna, na której czele stoi kierownik, musi spełniać określone kryteria m.in.: stanowić wyodrębnioną komórkę organizacyjną, podlegająca pełnomocnikowi ochrony (w zakresie ochrony informacji niejawnych), która obsługiwana jest przez pracowników pionu ochrony.

Do głównych zadań kancelarii tajnej należy:
- rejestrowanie;
- przechowywanie;
- obieg materiałów
- wydawanie materiałów;
- oraz sprawne ustalenie, gdzie znajduje się dany materiał (w tym wykaz osób zapoznanych).

Bezpieczeństwo teleinformatyczne

Bezpieczeństwo teleinformatyczne jest zbiorem zagadnień z dziedziny telekomunikacji i informatyki, związanym z szacowaniem i kontrolą ryzyka, które wynika z korzystania z komputerów, sieci komputerowych oraz przesyłania danych do zdalnych lokalizacji. Powinno być analizowane i oceniane z perspektywy: poufności, integralności oraz dostępności.

W celu zapewnienia niezbędnych standardów bezpieczeństwa, wymaganych zarówno przez przepisy krajowe, jak i międzynarodowe nieodzowna jest akredytacja bezpieczeństwa teleinformatycznego, oznaczająca dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych. Akredytacji udziela ABW albo SKW. Wymagana jest w przypadku przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej. W celu przeprowadzenia procesu akredytacji, nieodzowny jest w określonych przypadkach audyt bezpieczeństwa systemu teleinformatycznego, polegający na weryfikacji poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego, składającego się z dokumentu szczególnych wymagań bezpieczeństwa oraz dokumentu procedur bezpiecznej eksploatacji

systemu teleinformatycznego. Jeśli chodzi o przetwarzanie informacji niejawnych o klauzuli „zastrzeżone", wymaganej akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego udziela kierownik jednostki organizacyjnej, poprzez zatwierdzenie dokumentacji, a następnie przekazanie w ciągu 30 dni odpowiednio do ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego.

Kolejnym istotnym elementem bezpieczeństwa teleinformatycznego jest certyfikacja, mająca na celu potwierdzenie zdolności danego:
- urządzenia kryptograficznego;
- narzędzia kryptograficznego;
- lub innego środka do ochrony informacji niejawnych, służącego do ochrony informacji niejawnych od klauzuli „zastrzeżone". Istotnym jest, iż jeszcze obowiązujące przepisy (ustawa z 1999 roku) obejmują informacje od klauzuli „poufne". Celem nowych regulacji, które zaczną obowiązywać od stycznia 2011 roku jest umożliwienie polskim wytwórcom narzędzi i urządzeń kryptograficznych uzyskiwanie certyfikatów, umożliwiających stosowanie ww. urządzeń zarówno w strukturach NATO, jak i UE.

Pozytywne wyniki ocen bezpieczeństwa (na podstawie wyników badań prowadzonych w ramach certyfikacji) skutkują wydaniem przez ABW albo SKW stosownego certyfikatu.

Na uwagę zasługuje fakt, iż nie podlegają obowiązkowej akredytacji oraz badaniom i ocenie bezpieczeństwa w ramach procesów certyfikacji prowadzonych przez ABW albo SKW: systemy teleinformatyczne oraz urządzenia lub narzędzia kryptograficzne, które wykorzystywane są przez Agencję Wywiadu lub Służbę Wywiadu Wojskowego do uzyskiwania lub przetwarzania informacji niejawnych podczas wykonywania czynności operacyjno-rozpoznawczych poza granicami RP, a także wydzielone stanowiska służące wyłącznie do odbierania i przetwarzania ww. informacji na terytorium RP.

Bezpieczeństwo przemysłowe

W celu dostosowania polskich przepisów w zakresie ochrony informacji niejawnych w aspekcie bezpieczeństwa przemysłowego, wzorowano się na rozwiązaniach powszechnie stosowanych w NATO i UE. Obowiązujące normy prawne, określają, iż zdolność przedsiębiorcy do ochrony informacji niejawnych jest jednoznaczna z możliwością uzyskania dostępu do informacji niejawnych, w związku z wykonywaniem umów albo zadań. W tym celu, wydawane jest świadectwo bezpieczeństwa przemysłowego, które jest dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, wydawanym przez ABW albo SKW. Pokrótce należy podkreślić, iż postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy, który nie wymaga uzasadnienia, ale musi określać stopień świadectwa oraz klauzulę tajności informacji niejawnych. Ponadto, do wniosku musi być dołączony kwestionariusz bezpieczeństwa przemysłowego, ankiety lub kopie poświadczeń bezpieczeństwa. Postępowanie bezpieczeństwa przemysłowego obejmuje:
- sprawdzenie przedsiębiorcy, polegające na sprawdzeniu danych zawartych w rejestrach, ewidencjach, kartotekach (także niedostępnych powszechnie), obejmujące

m.in.: strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych, sytuację finansową, strukturę organizacyjną itp.;
– przeprowadzenie postępowania sprawdzającego wobec kierownika przedsiębiorcy, pełnomocnika ochrony i jego zastępcy/ów, osób zatrudnionych w pionie ochrony, administratora systemu teleinformatycznego oraz pozostałych osób wskazanych w kwestionariuszu (z dostępem do informacji niejawnych). Na uwagę zasługuje fakt, iż wprowadzono nową definicję kierownika przedsiębiorcy.

Z punktu widzenia integracji europejskiej, istotnym jest, iż przedsiębiorca wykonujący działalność jednoosobowo i osobiście, zdolność do ochrony informacji niejawnych potwierdza poprzez posiadanie poświadczenia bezpieczeństwa, które jest jednoznaczne z dawaniem rękojmi zachowania tajemnicy, a tym samym posiadaniem dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, także wydawanym przez ABW albo SKW. W przedmiotowym przypadku nie jest wymagane uzyskanie świadectwa bezpieczeństwa, a jedynie odbycie przeszkolenia w zakresie ochrony informacji niejawnych, zakończone wydaniem przez ABW albo SKW zaświadczenia.

Przedstawionych powyżej zasad nie stosuje się, w określonych przypadkach, a mianowicie, gdy obowiązek uzyskania świadectwa wynika z ratyfikowanej przez RP umowy międzynarodowej lub prawa wewnętrznego strony zawierającej umowę.

Świadectwo nie jest wymagane także w przypadku umów związanych z dostępem do informacji niejawnych o klauzuli „zastrzeżone", gdyż przedsiębiorca w ww. przypadku, musi spełniać wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone", za wyjątkiem wymogu zatrudnienia pełnomocnika ochrony (jeżeli wykonuje umowę, z wyłączeniem możliwości przetwarzania informacji w użytkowanych przez niego obiektach).

Stopnie zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej określane są w świadectwach:
– pierwszego stopnia (oznacza potwierdzenie pełnej zdolności przedsiębiorcy do ochrony ww. informacji);
– drugiego stopnia (tj. potwierdzenie zdolności przedsiębiorcy do ochrony ww. informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych);
– trzeciego stopnia (oznacza potwierdzenie zdolności przedsiębiorcy do ochrony ww. informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach).

Istotnym z punktu widzenia założeń integracji europejskiej jest, iż postępowanie bezpieczeństwa przemysłowego, prowadzone w celu wydania świadectwa trzeciego stopnia nie wymaga zatrudnienia pełnomocnika ochrony oraz utworzenia pionu ochrony, za wyjątkiem przypadków, kiedy mamy do czynienia z ubieganiem się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne" lub „poufne", stosowanym przez organizacje międzynarodowe.

Okres obowiązywania świadectw potwierdzających zdolność do ochrony informacji niejawnych wynosi odpowiednio: dla informacji o klauzuli „ściśle tajne": „ściśle tajne" przez okres 5 lat od daty wystawienia, „tajne" przez okres 7 lat od daty wystawienia, „poufne" przez okres 10 lat od daty wystawienia. Jeśli chodzi o informacje nie-

jawne o klauzuli „tajne": „tajne" przez okres 7 lat od daty wystawienia, „poufne" przez okres 10 lat od daty wystawienia, natomiast informacje o klauzuli: „poufne" przez okres 10 lat od daty wystawienia.

Na uwagę zasługuje fakt, iż ABW albo SKW wydaje odrębne świadectwa (z zachowaniem ww. terminów) o klauzuli stanowiącej zagraniczny odpowiednik klauzuli „tajne" lub „poufne", stosowany przez organizacje międzynarodowe.

Oczywiście, decyzja o odmowie wydania świadectwa oznacza obligatoryjnie stwierdzenie braku zdolności do ochrony informacji niejawnych. Przyczyną może być m.in.:
- odmowa wydania lub cofnięcia poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy;
- brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy;
- niedające się usunąć wątpliwości dot.: ewentualnej działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko RP;
- zagrożenia ze strony obcych służb specjalnych itp.

Ponadto, ABW lub SKW może podjąć decyzję o cofnięciu świadectwa w oparciu o wyniki sprawdzenia przedsiębiorcy z urzędu lub ustaleń kontroli ochrony informacji niejawnych.

Kolejnym, nieodzownym elementem bezpieczeństwa przemysłowego jest instrukcja bezpieczeństwa przemysłowego, która powinna zawierać szczegółowe wymagania dotyczące ochrony informacji niejawnych o klauzuli „poufne" lub wyższej. Instrukcja bezpieczeństwa przemysłowego przekazywana jest przedsiębiorcy w związku z wykonywaniem umowy, musi być odpowiednia do liczby przedmiotowych informacji, rodzaju klauzuli tajności oraz liczby osób mających do nich dostęp.

Szkolenie w zakresie ochrony informacji niejawnych

Głównym celem procesu szkolenia jest zapoznanie potencjalnych użytkowników, osób sprawdzanych z przepisami z zakresu ochrony informacji niejawnych, możliwą odpowiedzialnością (karną, służbową/dyscyplinarną), zasadami ochrony informacji niejawnych, zasadami zarządzania ryzykiem bezpieczeństwa (SZBI, szacowanie ryzyka), sposobami ochrony informacji niejawnych, postępowaniem w sytuacjach zagrożenia dla informacji niejawnych oraz postępowaniem w przypadku ujawnienia informacji niejawnych.

W celu bieżącego aktualizowania informacji w zakresie ochrony informacji niejawnych, w tym w zakresie międzynarodowych uregulowań prawnych, wprowadzono obowiązek przeprowadzania szkoleń nie rzadziej niż raz na 5 lat.

Szkolenia przeprowadzane będą odpowiednio przez ABW lub SKW dla pełnomocników ochrony i ich zastępców (lub osób przewidzianych na te stanowiska), przedsiębiorców wykonujących działalność jednoosobowo, kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony. ABW lub SKW, wspólnie z danym pełnomocnikiem ochrony będą przeprowadzać szkolenia dla kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli „ściśle tajne" lub „tajne", zaś pełnomocnicy ochrony zobowiązani będą do przeprowadzenia

szkoleń dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej.

Ponadto, ABW odpowiada za przeprowadzenie w przedmiotowym zakresie wymaganych przepisami prawa szkoleń dla posłów i senatorów.

Podsumowanie

W związku z dynamicznie zmieniającą się sytuacją na arenie międzynarodowej, nieodzowne jest dostosowanie przepisów krajowych do norm i uregulowań obowiązujących w Unii Europejskiej oraz NATO. Niewątpliwie, nowa ustawa o ochronie informacji niejawnych, która zacznie obowiązywać od stycznia 2011 roku, wprowadza szereg rozwiązań, które wpłyną na szybsze wdrażanie norm prawa międzynarodowego, a w rezultacie na bezpieczną wymianę informacji, ze szczególnym uwzględnieniem informacji niejawnych.

Bez wątpienia, do najistotniejszych zmian i rozwiązań w nowej ustawie o ochronie informacji niejawnych, ze szczególnym uwzględnieniem sprawnej wymiany informacji niejawnych z partnerami zagranicznymi w aspekcie integracji europejskiej należy m.in.: likwidacja 2-stopniowego systemu definiowania informacji niejawnych, która oznacza rezygnację z rozbudowanych i niepraktycznych wykazów, utrudniających sprawną wymianę informacji, zarówno na niwie krajowej, jak i międzynarodowej. Kolejnym elementem jest rezygnacja ze ścisłej kontroli obiegu dokumentów o niższych klauzulach, ze szczególnym uwzględnieniem informacji niejawnych o klauzuli „zastrzeżone". Nowe definicje w ustawie, jak: przetwarzanie informacji, kierownik przedsiębiorcy oraz wprowadzenie założeń Systemowego Zarządzania Bezpieczeństwem Informacji z pewnością wpłyną, a przynajmniej pomogą w podjęciu wysiłków, zmierzających do zwiększenia jakości informacji niejawnych oraz sposobu zarządzania nimi. Wprowadzenie na grunt krajowy – nowej ustawy o ochronie informacji niejawnych, nowoczesnych metod zarządzania, takich jak audyt, zarządzanie ryzykiem lub zarządzanie procesowe, wynika także z wymogów stawianych przez Wspólnotę w ramach Strategii lizbońskiej, są szansą na wymuszenie zwiększenia przez polskich decydentów nakładów finansowych na rozwój, a tym samym jakość[4].

Bardzo istotną kwestią z punktu widzenia zintegrowanej Europy jest eliminacja równoległego pełnienia funkcji krajowej władzy bezpieczeństwa przez Szefów: ABW i SKW. Nowe regulacje spowodują, iż wyznaczony będzie jeden przedstawiciel RP do kontaktów z podmiotami zagranicznymi, do którego głównych zadań będzie należało m.in.: reprezentowanie RP na forum międzynarodowym, nadzorowanie całości zagadnień związanych z ochroną informacji niejawnych w RP, zapewnienie jednolitości i zgodności systemu ochrony informacji niejawnych z przepisami bezpieczeństwa organizacji międzynarodowych, a także wydawanie dokumentów upoważniających do dostępu do informacji niejawnych międzynarodowych „NATO", „EU" itp. Zachowanie pośrednictwa Szefa SKW w zakresie realizacji zadań wobec podmiotów w sferze

[4] *Rola nauki i edukacji w społeczeństwie wiedzy*, red. I. K. Hejduk, wyd. Instytut Organizacji i Zarządzania w Przemyśle ORGMASZ, Warszawa 2009, s. 64.

wojskowej, wydaje się sensowne z uwagi na specyficzne, odmienne standardy ochrony informacji: sfera cywilna i wojskowa.

Nowa klasyfikacja informacji niejawnych, z uwzględnieniem pojęcia szkody oraz możliwość zmiany klauzuli tajności (wg daty, konkretnego wydarzenia, części materiału) z pewnością w znacznym stopniu uelastyczni zarówno sposób klasyfikacji, jak i ewentualnej zmiany klauzuli. Ciekawym rozwiązaniem w aspekcie braku porozumienia co do rodzaju klauzuli oraz jej ewentualnej zmiany (zaniżenia lub zawyżenia), jest instytucja sporu, który może wystąpić pomiędzy odbiorcą a adresatem materiału o charakterze niejawnym. Ponadto, zwiększenie zakresu kontroli tj. Prezesa Rady Ministrów w stosunku do ABW i SKW oraz ABW i SKW w stosunku do pełnomocników ochrony, przy możliwości korzystania z uprawnień Najwyższej Izby Kontroli, a także postępowanie odwoławcze (odwołanie, skarga), wprowadzenie jednego wzoru ankiety bezpieczeństwa, wymogu posiadania przez pełnomocnika ochrony oraz jego zastępcę/ów wyższego wykształcenia i wiele innych, nowych elementów, powinno wpłynąć na zwiększenie jakości prowadzonych postępowań sprawdzających. Umiejętnie przeprowadzone postępowania sprawdzające, kontrolne postępowania sprawdzające, bądź postępowanie bezpieczeństwa przemysłowego, stanowią kluczowy element ochrony informacji niejawnych. W konsekwencji, wpływają bezpośrednio na jakość zarządzania informacją niejawną, ze szczególnym uwzględnieniem procesu ochrony, zarówno na niwie krajowej, jak i międzynarodowej.