Stanisław Hoc

Bezpieczeństwo informacyjne. Wybrane problemy

1. UWAGI WSTĘPNE

Pojęcie bezpieczeństwa informacyjnego obejmuje ochronę informacji niejawnych i innych tajemnic ustawowo chronionych, danych osobowych, zasady dostępu do informacji publicznej. Zakres przedmiotowy tego bezpieczeństwa odnosi się do ochrony interesów państwa oraz interesów obywateli. Niekiedy trudno będzie rozgraniczyć te interesy.

P. Sienkiewicz podkreśla, że bezpieczeństwo informacyjne, często utożsamiane jest z bezpieczeństwem informatycznym odnoszonym do narzędzi i procedur ochrony danych, informacji i systemów teleinformatycznych. Zapewnienie bezpieczeństwa systemów sieci informacyjnych, ich stabilności, nienaruszalności itp. stanowi „jądro" bezpieczeństwa informacyjnego. Zasoby informacyjne posiadają charakter zasobów strategicznych, sprzyjają powstawaniu nowych branż i profesji, a także miejsc pracy itp. Infrastrukturę informacyjną państwa tworzą: normy informacyjne, zasoby informacji, systemy informacyjne, instytucje informacyjne, systemy organizacyjno-techniczne gromadzenia, przechowywania, przetwarzania i przekazywania informacji. Ryzyko utraty wartościowych zasobów informacyjnych jest immanentną cechą systemów bezpieczeństwa. Bezpieczeństwo informacyjne ze względu na liczność interakcji powinno

być analizowane na kilku płaszczyznach bezpieczeństwa: bezpieczeństwa organizacji i instytucji oraz obywatela[1].

2
OCHRONA INFORMACJI NIEJAWNYCH I INNYCH TAJEMNIC USTAWOWO CHRONIONYCH

W dniu 22 stycznia 1999 roku Sejm uchwalił ustawę o ochronie informacji niejawnych, (dalej – u.o.i.n.), która weszła w życie z dniem 11 marca 1999 roku, czyli w przeddzień przyjęcia RP do NATO. Należy zauważyć, iż w dniu 18 marca 1999 roku Sejm uchwalił ustawę wyrażającą zgodę na ratyfikację umowy między stronami Traktatu Północnoatlantyckiego z dnia 6 marca 1997 roku o ochronie informacji wraz z 6 innymi umowami międzysojuszniczymi, które w dniu 27 maja 1999 roku zostały ratyfikowane przez Prezydenta RP (Dz.U. z 2000 r. Nr 64, poz. 740).

Według art. 1 umowy Strony:

> (i) będą ochraniać i zabezpieczać:
> a) informacje (określone w załączniku II) lub przekazywane NATO przez państwo członkowskie,
> b) informacje oznaczone jako niejawne, pochodzące od państwa członkowskiego i przekazywane innemu państwu członkowskiemu w ramach programu, projektu lub kontraktu NATO,
> (ii) będą utrzymywać klauzulę tajności informacji, określonych w ustępie (i), oraz dołożą wszelkich starań w celu ich odpowiedniego zabezpieczenia,
> (iii) nie będą wykorzystywać informacji niejawnych określonych w ustępie (i), w celu innym niż ustanowione w Traktacie Północnoatlantyckim oraz w decyzjach i uchwałach odnoszących się do tego traktatu,
> (iv) nie będą ujawniać informacji określonych w ustępie (i) Stronom nie będącym członkami NATO bez zgody organu zastrzegającego.

Ustawa o ochronie informacji niejawnych jest aktem kazuistycznym, uwzględnia podstawowe standardy NATO i UE w zakresie ochrony informacji niejawnych, w wielu kwestiach znacznie wykracza poza standardy i rozwiązania przyjęte w państwach natowskich, np. RFN, wprowadza

[1] P. Sienkiewicz, *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli*, w: *Ochrona informacji niejawnych i biznesowych, Materiały IV Kongresu*, red. M. Ciecierski, Katowice 2008, s. 22–23.

nowe instytucje, które mogą spowodować szereg problemów i kontrowersji, zawiera niejasności terminologiczne oraz posługuje się niejednokrotnie wyrażeniami nieostrymi. To wyraz wymuszonego pośpiechu legislacyjnego w związku ze zbliżającym się przystąpieniem RP do NATO.

Należy zaakceptować celowość i użyteczność ustawy oraz podjętej próby zbudowania nowoczesnego systemu ochrony informacji niejawnych.

Już po krótkim okresie obowiązywania ustawa stała się przedmiotem przedsięwzięć nowelizacyjnych, a dalsze prace w tym zakresie są kontynuowane. Potrzeba taka wynika przede wszystkim ze zbliżającej się prezydencji RP w UE.

Przepisy u.o.i.n. chronią informacje stanowiące tajemnicę państwową lub służbową, które nazywają informacjami niejawnymi. Jednocześnie według art. 1 ust. 3 przepisy ustawy nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych prawnie chronionych. Ustawodawca tym samym dopuścił możliwość szerszej ochrony tajemnicy, o ile taka zostanie przewidziana w innych ustawach[2]. U.o.i.n. postawiła interes bezpieczeństwa narodowego na pierwszym miejscu, stwarzając mechanizmy ochrony przed zagrożeniami, uszczuplając prawo jednostki do tego, co należy do informacji. W Konstytucji RP nie określono jako odrębnej wartości tajemnicy państwowej (taki obowiązek wynikał z art. 93 ust. 1 Konstytucji PRL z 1952 roku).

K. Rodziewicz[3] podkreśla, że kwestia prawidłowej ochrony informacji niejawnych jest trudna, a problemy, jak zawsze, mnożą się w praktyce stosowania ustawy, dlatego też krytycznie odnosi się do u.o.i.n., która w wielu rozwiązaniach łamie zasady konstytucyjne. Stąd uważa, że to przede wszystkim obywatele, domagając się swych praw i posiłkując poglądami doktryny, będą krok po kroku weryfikować wadliwe przepisy i z pomocą struktur państwowych dostosować do formy, która wypośrodkuje interesy państwa i obywatela (jak to się stało na przykład przy nowelizacji dotyczącej postępowania skargowego i odwoławczego).

Zdaniem tej autorki, u.o.i.n. posługuje się bardzo niejasną i często nieostrą terminologią (np. czym tak naprawdę są: tajemnica służbowa, rękojmia zachowania tajemnicy, okoliczność powodująca ryzyko podatności na szantaż lub wywieranie presji, zasada bezstronności i obiektywizmu lub najwyższa staranność w postępowaniu sprawdzającym).

---

[2] K. Rodziewicz, *Ochrona informacji niejawnych – analiza przepisów*, „Przegląd Prawa i Administracji" 2003, nr 53, s. 182.

[3] Ibidem, s. 206–207.

Ustawa zawiera wiele rozwiązań kontrowersyjnych, a nawet sprzecznych z Konstytucją RP[4]. Problematyce rozwiązań prawnych tej ustawy poświęcono wiele interesujących opracowań[5].

Konstytucja RP zapewnia obywatelom prawo do informacji publicznej, które jednak podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych (art. 61 ust. 3 Konstytucji RP i art. 5 ust. 1 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej). Należy zauważyć, iż prawo do informacji w Unii Europejskiej znajduje wyraz w treści art. 1 i 255 TUE oraz w rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego, Rady i Komisji z dnia 30 maja 2001 roku w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji („Official Journal" L 145/31/05/2001 s. 43–48). Rozporządzenie określa zasady, warunki i ograniczenia w dostępie do dokumentów Parlamentu Europejskiego, Rady i Komisji i ma na celu ustalenie zasad zapewniających możliwie najłatwiejsze wykonanie tego prawa, oraz promowanie dobrych praktyk administracyjnych w dostępie do dokumentów (art. 1). Artykuł rozporządzenia dotyczy dokumentów sensytywnych, czyli zawierających informacje podlegające szczególnej ochronie. Dokumenty sensytywne zgodnie z ust. 1 to dokumenty pochodzące od instytucji lub utworzonych przez nie agencji, z Państw Członkowskich, państw trzecich lub Organizacji Międzynarodowych, zakwalifikowane jako „TRES SECRET/TOP SECRET", „SECRET" lub „CONFIDENTIEL" zgodnie z przepisami obowiązującymi w danej instytucji, które chronią podstawowe interesy Państw Członkowskich w obszarach objętych art. 4 ust. 1 lit. a) rozporządzenia, czyli w obszarze bezpieczeństwa publicznego, obrony i spraw wojskowych.

Katalog przepisów o ochronie innych tajemnic ustawowo chronionych jest bardzo obszerny, co dowodzi, iż reguła stanowiąca o jawności informacji publicznej (każda informacja o sprawach publicznych stanowi informację publiczną) i jej utajnieniu jako wyjątku od reguły ma jedynie charakter formalny, gdyż w większości przypadków informację można

[4] A. Domańska, K. Skotnicki, *Spór o postępowanie sprawdzające według ustawy o ochronie informacji niejawnych*, „Gdańskie Studia Prawnicze" 2004, t. 12, s. 19–20.

[5] Por. np.: R. Białoskórski, *Kompendium ochrony informacji niejawnych w pytaniach i odpowiedziach*, Warszawa 2008; S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia*, Opole 2006; M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Warszawa 2006; A. Szewc, *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007; *Publicznoprawna ochrona informacji*, Warszawa 2007; M. Witkowski, D. Jęda, *Ochrona informacji niejawnych – nowe rozwiązania*, Warszawa 2007.

uznać za niejawną i tym samym w znacznym stopniu ograniczyć do niej dostęp[6].

W prawie polskim można wyróżnić w szczególności następujące tajemnice: państwową i służbową, przedsiębiorstwa, handlową, bankową, publicznego obrotu papierami wartościowymi, zamówień publicznych, statystyczną, NIK, geologiczną, wynalazczą, skarbową, czynności operacyjno-rozpoznawczych, postępowania karnego, postępowania administracyjnego, postępowania celnego, świadka koronnego, sędziowską, prokuratorską, adwokacką, radcowską, notarialną, zeznań świadków i opinii biegłych, komornika sądowego, rzeczoznawców majątkowych, doradcy podatkowego, biegłego rewidenta, lekarską, dziennikarską, korespondencji, autorską, spowiedzi, wolności sumienia i wyznania, życia prywatnego i rodzinnego, głosowania w wyborach, pomocy społecznej, akt stanu cywilnego, danych osobowych, geodezyjnych, ubezpieczeń społecznych, ubezpieczeniową, funduszy inwestycyjnych, detektywistyczną, miru domowego, świadka anonimowego, osób skazanych, obrad organów publicznych, ale tylko jako wyjątek od zasady ich jawności, działalności pracowników samorządowych i urzędników służby cywilnej, ale jako wyjątek od zasady ich jawności.

Warto odnieść się np. do tajemnicy spowiedzi, która występuje w art. 261 § 2 k.p.c., art. 178 pkt 2 k.p.k. i art. 82 pkt 2 k.p.a., ale żaden z tych przepisów nie zawiera definicji tego pojęcia. W przepisach tych ustaw chodzi o poszanowanie tajemnicy spowiedzi ze względu na szacunek do kościołów i związków wyznaniowych, a także ze względu na godność osoby przystępującej do spowiedzi[7]. Zgodnie z treścią kanonu 983 kodeksu prawa kanonicznego Kościoła katolickiego „tajemnica spowiedzi jest nienaruszalna, dlatego nie wolno spowiednikowi słowami lub w jakikolwiek inny sposób i dla jakiejkolwiek przyczyny w czymkolwiek zdradzić penitenta". Obowiązek zachowania tajemnicy ma także tłumacz, jeśli występuje, jak również wszyscy inni, którzy w jakikolwiek sposób zdobyli ze spowiedzi wiadomości o grzechach. Prawo kanoniczne przewiduje surową odpowiedzialność za naruszenie tajemnicy sakramentalnej, spowiednik, który narusza bezpośrednio tę tajemnicę, podlega ekskomunice, wiążącej mocą samego prawa, zastrzeżonej Stolicy Apostolskiej (kanon 1388 § 1). W doktrynie prawa kanonicznego tajemnicę spowiedzi traktuje się jako tajemnicę zawodową.

---

[6] T.R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2004, s. 140.

[7] B. Rakoczy, *Tajemnica spowiedzi w polskim postępowaniu cywilnym, karnym i administracyjnym*, „Przegląd Sądowy" 2003, nr 11–12, s. 129.

Rozpowszechnianie niektórych informacji (wiadomości) odnoszących się do sfery prywatności może być równoznaczne z naruszeniem przepisów k.k. (np. art. 212, 216).

Według ustawy o dostępie do informacji publicznej prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych i innych tajemnic ustawowo chronionych. Prawo do informacji to jedno z podstawowych praw człowieka (art. 19 Międzynarodowego Paktu Praw Obywatelskich i Politycznych i art. 10 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności zapewniają prawo każdego człowieka do swobodnego uzyskiwania informacji). Według art. 5 ust. 1 ustawy o dostępie do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Powyższa regulacja stanowi, że przepisy ustawy o ochronie informacji niejawnych stanowią wobec przepisów ustawy o dostępie do informacji publicznej *legi speciali* i stosowane są na zasadzie pierwszeństwa. Informacja niejawna stanowi informację publiczną w rozumieniu ustawy, a jedynie zasady i tryb uzyskiwania do niej dostępu określają inne przepisy.

P. Szustakiewicz[8] uważa, że po zamachach z dnia 11 września 2001 roku i w związku z zagrożeniem międzynarodowym terroryzmem należy się zastanowić, czy tak szeroko sformułowane uprawnienie nie powinno ulec ograniczeniu.

Należy zwrócić uwagę na fakt, że firmy i instytucje coraz częściej monitorują swoich pracowników, co może być oceniane jako naruszenie np. tajemnicy korespondencji (rejestracja rozmów telefonicznych, elektroniczny system rejestracji czasu pracy, moduły GPS umożliwiające lokalizację samochodów, systemy RFID umożliwiające śledzenie ruchu pracowników w obrębie monitorowanego terenu itp.). Prawo pracy nie określa wprost zakresu ochrony pracowników przed ich kontrolowaniem w miejscu pracy. Artykuł 11^1 k.p. stanowi, że pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika (wizerunek, tajemnicę korespondencji, cześć itp.). Jeżeli pracodawca zamierza podjąć działania monitorujące pracowników, to powinien je uregulować w regulaminie pracy i w umowie o pracę oraz poinformować pracowników.

[8] P. Szustakiewicz, *Dostęp do informacji na podstawie ustawy o dostępie do informacji publicznej, w: Obywatelskie prawo do informacji publicznej*, red. T. Gardocka, Warszawa 2008, s. 17.

Kontrola korespondencji służbowej (np. elektronicznej) jest dopuszczalna, pracodawca może wprowadzić zakaz stosowania korespondencji elektronicznej służbowej do celów prywatnych, natomiast nie powinien zapoznawać się z prywatną korespondencją pracowników. Europejski Trybunał Praw Człowieka w Strasburgu w wyroku z dnia 3 kwietnia 2007 roku w sprawie Copland przeciwko Wielkiej Brytanii (Izba (Sekcja IV), skarga nr 62617/00) orzekł, że pracodawca może monitorować podwładnych. Kontrola nie powinna jednak naruszać art. 8 Europejskiej Konwencji Praw Człowieka, który stanowi, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, mieszkania oraz korespondencji. Zdaniem Trybunału monitorowanie korzystania przez pracownika z telefonu, e-maila lub Internetu w miejscu pracy może być konieczne w pewnych okolicznościach w realizacji uprawnionego celu. W Wielkiej Brytanii w 2000 roku weszła w życie ustawa (Regulation of Investigatory Powers Act), która daje pracodawcom prawo do kontrolowania poczty elektronicznej, rozmów telefonicznych pracowników oraz sposobu korzystania przez nich z Internetu.

Polskie regulacje prawne dotyczące ochrony informacji niejawnych i innych tajemnic ustawowo chronionych odpowiadają w zasadzie standardom europejskim, wymagają jednak uporządkowania w sensie legislacyjnym, przy uwzględnieniu dotychczasowego dorobku doktryny i praktyki. Stąd postulat podjęcia kompleksowych prac legislacyjnych w tym zakresie, które powinny być prowadzone przy udziale zarówno przedstawicieli doktryny i praktyki, z uwzględnieniem stanowiska Rady Legislacyjnej, ale prace te nie mogą być poddawane naciskom utylitarnych gremiów administracji rządowej i wymuszane terminami, już minionymi.

3. OCHRONA INFORMACJI NIEJAWNYCH W UE

Problematyka związana z ochroną tajemnicy jest regulowana w Traktacie ustanawiającym Wspólnotę Europejską z dnia 25 marca 1957 roku (OJC 1992, Nr 224, poz. 1 wersja skonsolidowana uwzględniająca zmiany wprowadzone Traktatem z Nicei) w art. 296 ust. 1, według którego postanowienia Traktatu „nie stanowią przeszkody w stosowaniu następujących reguł: a) żadne Państwo Członkowskie nie ma obowiązku udzielania informacji,

których ujawnienie uznaje za sprzeczne z podstawowym interesem jego bezpieczeństwa (...)".

Zgodnie z art. 287 Traktatu członkowie instytucji Wspólnoty, członkowie komitetów, jak również urzędnicy i inni pracownicy Wspólnoty są zobowiązani, również po zaprzestaniu pełnienia swoich funkcji, nie ujawnić informacji objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych. Natomiast zgodnie z art. 284 Traktatu w celu wypełnienia zadań, które są jej powierzone, Komisja Europejska może zbierać wszelkie informacje i dokonywać wszelkich niezbędnych weryfikacji w granicach i na warunkach określonych przez Radę Europejską zgodnie z postanowieniami Traktatu. Problematyka ochrony tajemnicy stanowi, co do zasady domenę prawa wewnętrznego państw członkowskich. Państwo jest władne, aby prawnie przesądzić kwestie związane z ochroną informacji niejawnych.

Problematyka ochrony informacji niejawnych nie została więc zharmonizowana w prawie UE. Z tego też powodu, w zakresie informacji niejawnych chronionych tylko na poziomie krajowym brakuje przepisów UE, które wyznaczałyby tryby i zasady postępowania. Inna jest jednak sytuacja w odniesieniu do informacji niejawnych pochodzących od organów UE: Rady Europejskiej i Komisji Europejskiej. W tym zakresie obowiązują odpowiednio: Decyzja Rady Europejskiej z dnia 19 marca 2001 roku w sprawie przyjęcia przepisów bezpieczeństwa Rady, 2001/264/WE („Official Journal of the European Communities" L 101/1) oraz Decyzja Komisji Europejskiej z dnia 29 listopada 2001 roku w sprawie zmiany jej regulaminu wewnętrznego, 2001/844/WE („Official Journal of the European Communities" L 317/1), z późniejszymi zmianami określonymi w decyzji z dnia 2 sierpnia 2006 roku (2006/548/WE). Art. 1 decyzji z 29 listopada 2001 stanowi, iż: „W celu rozwijania działalności Komisji w dziedzinach wymagających zachowania stopnia poufności, odpowiednim jest ustanowienie wszechstronnego systemu bezpieczeństwa mającego zastosowanie do Komisji, innych instytucji, organów, biur i agencji, ustanowionych na mocy lub na podstawie Traktatu ustanawiającego Wspólnotę Europejską lub Traktatu o Unii Europejskiej, do Państw Członkowskich, a także innych odbiorców tajnych informacji Unii Europejskiej".

Decyzja Rady 2001/246/WE, która w stosunku do państw członkowskich UE przewiduje określone wymagania związane z dostępem, przechowywaniem, magazynowaniem i archiwizowaniem informacji niejawnych ma

ważne znaczenie również dla naszych wewnętrznych regulacji ochrony informacji niejawnych.

Z decyzji wynika, że Sekretarz Generalny jest zobowiązany do podjęcia odpowiednich środków w celu zapewnienia tego, aby przepisy bezpieczeństwa Rady były przestrzegane w toku pracy z informacjami klasyfikowanymi UE w ramach Sekretariatu Generalnego Rady przez urzędników i jego innych pracowników, przez jego zewnętrznych kontrahentów, przez osoby delegowane do pracy w Sekretariacie Generalnym Rady, a także w obiektach i zdecentralizowanych agencjach UE. Państwa członkowskie są zobowiązane do podjęcia odpowiednich środków, zgodnie z rozwiązaniami krajowymi, w celu zapewnienia tego, aby przepisy bezpieczeństwa Rady były przestrzegane w toku pracy z informacjami klasyfikowanymi UE w ramach ich służb i obiektów. Przepisy bezpieczeństwa Rady zostały ujęte w aneksie do decyzji.

Warto w tym miejscu nadmienić, iż Rada Europejska jest jednym z głównych ogniw decyzyjnych we Wspólnocie Europejskiej, w jej skład wchodzą przedstawiciele, na szczeblu ministerialnym wszystkich państw członkowskich (27). Jest ona organem międzyrządowym, którego członkowie są reprezentantami interesów państw swego własnego pochodzenia. Rada jest podstawowym organem prawodawczym. Radę wspiera Sekretariat Generalny z Sekretarzem Generalnym mianowanym na podstawie jednomyślnej decyzji Rady; Sekretariat jest organem pomocniczym o techniczno-administracyjnym charakterze spełniającym zadania w zakresie obsługi organizacyjnej i finansowej Rady. Sekretariat składa się z dyrekcji generalnych.

Należy podkreślić, iż na mocy Traktatu o przystąpieniu RP do UE z dniem 1 maja 2004 roku zaczęło obowiązywać w Polsce prawo UE. Traktat ten został ogłoszony w Dz.U. z dnia 30 kwietnia 2004 roku Nr 90, poz. 864. Według ogłoszenia Prezesa RM z dnia 11 maja 2004 roku w sprawie stosowania prawa UE (M.P. Nr 20, poz. 359) ogłoszenie aktów prawa UE w języku polskim będzie miało miejsce w specjalnym wydaniu „Dziennika Urzędowego Wspólnot Europejskich", który zawiera m.in. w serii L (legislacja); rozporządzenia, dyrektywy, decyzje, zalecenia, opinie). Na porządek prawny UE składa się prawo pierwotne i prawo wtórne, uzupełniane orzecznictwem Europejskiego Trybunału Sprawiedliwości (ETS).

Do aktów prawa pierwotnego zalicza się przede wszystkim traktaty wraz z towarzyszącymi im załącznikami i protokołami. Natomiast do aktów wspólnotowego prawa wtórnego należy zaliczyć rozporządzenia, dyrektywy, decyzje, zalecenia i opinie.

Aneks do decyzji Rady składa się z części I („Podstawowe zasady i minimalne standardy bezpieczeństwa") i części II („Organizacja bezpieczeństwa w Radzie UE") podzielonej na 12 sekcji oraz 6 załączników.

Przez pojęcie „informacje klasyfikowane UE" rozumie się wszelkie informacje i materiały, których nieupoważnione ujawnienie mogłoby w różnym stopniu narazić na szkodę interesy UE bądź jednego lub kilku państw członkowskich, niezależnie od tego, czy informacja ta została wytworzona w UE, czy też przekazana przez państwa członkowskie, państwa trzecie lub organizacje międzynarodowe. W części I zamieszczono wprowadzenie do podstawowych zasad i minimalnych standardów bezpieczeństwa (wyjaśniono pojęcia: dokument, materiał), przedstawiono podstawowe cele systemu bezpieczeństwa, podstawy bezpieczeństwa, podstawowe zasady, organizację bezpieczeństwa, bezpieczeństwa osobowe, bezpieczeństwo fizyczne, bezpieczeństwo teleinformatyczne, przeciwdziałanie sabotażom oraz innym formom złośliwego i celowego szkodzenia oraz udostępnianie informacji klasyfikowanych państwom trzecim i organizacjom międzynarodowym.

Przedstawione w części I zasady są wdrażane w życie zgodnie z przepisami szczegółowymi zawartymi w części II.

W sekcji I ujęto organizację bezpieczeństwa w Radzie UE, szczegółowo określającą obowiązki Sekretarza Generalnego, który przewodniczy Komitetowi Bezpieczeństwa Rady, w skład którego wchodzą przedstawiciele krajowych władz bezpieczeństwa państw członkowskich. W strukturze Rady działa również Biuro Bezpieczeństwa Sekretariatu Generalnego Rady, którego zadaniem jest koordynacja, nadzór i wdrażanie środków bezpieczeństwa. Dyrektor Biura Bezpieczeństwa jest głównym doradcą Sekretarza Generalnego do spraw bezpieczeństwa i sprawuje funkcję sekretarza Komitetu Bezpieczeństwa.

Każde państwo członkowskie jest zobowiązane do powołania krajowej władzy bezpieczeństwa odpowiedzialnej za ochronę informacji klasyfikowanych UE. Biuro Bezpieczeństwa, działając wspólnie i w porozumieniu z właściwą krajową władzą bezpieczeństwa, jest zobowiązane do przeprowadzenia okresowych kontroli rozwiązań w zakresie obrony informacji klasyfikowanych UE w Sekretariacie Generalnym oraz stałych przedstawicielstwach państw członkowskich przez UE, a także należących do państw członkowskich pomieszczeń w budynkach Rady.

Sekcja II reguluje klauzule i oznaczenia. Informacjom mogą być nadane następujące klauzule tajności:

- TRÉS SECRET UE / EU TOP SECRET, klauzulę tę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie spowodowałoby wyjątkowo duże szkody dla podstawowych interesów UE albo jednego lub więcej państwa członkowskich,
- SECRET UE, klauzulę tę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom UE albo jednego lub więcej państw członkowskich,
- CONFIDENTIEL UE, klauzulę tę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom UE albo jednego lub więcej państw członkowskich,
- RESTREINT UE, klauzulę tę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie byłoby niekorzystne z punktu widzenia interesów UE albo jednego lub więcej państw członkowskich.

Decyzje Komisji i Rady UE nakładają obowiązek stosowania dodatkowych oznaczeń:

- ESDP / PESD – oznaczenie stosowane na dokumentach i ich kopiach, które dotyczą zagadnień bezpieczeństwa i obrony UE albo jednego lub więcej jej państw członkowskich, bądź odnoszą się do wojskowego i cywilnego zarządzania kryzysowego,
- CRYPTO – oznaczenie to powinno być stosowane tylko wtedy, gdy istnieje potrzeba ograniczonej dystrybucji oraz specjalnej obsługi dokumentu przy zastosowaniu środków ochrony kryptograficznej, stosuje się tylko z właściwą, nadaną dokumentowi klauzulą tajności.

Ponadto w UE funkcjonuje także oznaczenie nie mające cech klauzul tajności, a wskazujące, że informacje nie są przeznaczone do publicznej wiadomości, np. LIMITE / LIMITED – w stosunku do informacji UE. Mogą być stosowane również inne oznaczenia ograniczające wykorzystanie i obieg dokumentów.

Klauzule i oznaczenia nanosi się w następujący sposób:

- na dokumentach RESTREINT UE za pomocą środków mechanicznych lub elektronicznych,

- na dokumentach CONFIDENTIEL UE za pomocą środków mechanicznych i ręcznie, możliwe jest także drukowanie ich na wcześniej oznakowanych i zarejestrowanych arkuszach,
- na dokumentach SECRET UE I TRÉS SECRET UE / EU TOP SECRET za pomocą środków mechanicznych i ręcznie.

W sekcji III określono zasady nadawania klauzul (stosowanie klauzuli, obniżanie i znoszenie klauzuli).

W sekcji IV określono bezpieczeństwo fizyczne, którego celem jest zapobieganie przypadkom uzyskania przez osoby nieupoważnione dostępu do informacji klasyfikowanych UE, odnosząc się do: wymagań w zakresie bezpieczeństwa, środków ochrony fizycznej (strefy bezpieczeństwa, strefa administracyjna, kontrola wejść i wyjść, patrolowanie przez strażników, sejfy, szafy metalowe i pomieszczenia wzmocnione, zamki, kontrola kluczy i kodów dostępu, urządzenia wykrywania wtargnięcia, zatwierdzony sprzęt, fizyczna ochrona kopiarek i telefaksów), ochrona przed poglądem i podsłuchem stref zabezpieczonych technicznie.

W sekcji V przedstawiono stosowanie zasady ograniczonego dostępu i postępowanie sprawdzające (szczególne zasady dostępu do informacji o klauzuli TRÉS SECRET UE / EU TOP SECRET, SECRET UE, CONFIDENTIEL UE i RESTREINT UE, przekazywanie, szkolenia). W sekcji VI określono procedurę sprawdzenia urzędników i innych pracowników Sekretariatu Generalnego Rady UE.

W sekcji VII uregulowano zasady sporządzania, dystrybucji, przesyłania, przechowywania i niszczenia materiałów klasyfikowanych UE (sporządzanie i dystrybucja dokumentów klasyfikowanych UE, przesyłanie dokumentów klasyfikowanych UE, przesyłanie za pośrednictwem elektronicznych i innych technicznych środków, kopie, tłumaczenia i wyciągi z dokumentów klasyfikowanych UE, kontrole kompleksowe i wyrywkowe, przechowywanie i niszczenie dokumentów klasyfikowanych UE, szczególnie zasady odnoszące się do dokumentów przeznaczonych dla Rady UE).

W sekcji VIII określono zadania kancelarii tajnych TRÉS SECRET UE / EU TOP SECRET (głównie kancelarie tajne, podkancelarie tajne, przeglądy).

W sekcji IX przedstawiono środki bezpieczeństwa stosowane w trakcie spotkań odbywanych poza siedzibą Rady UE i dotyczących kwestii szczególnie wrażliwych (zakresy odpowiedzialności – państwo przyjmujące, państwa członkowskie, pełnomocnik ochrony, spotkania Biuro

Bezpieczeństwa Sekretariatu Generalnego Rady, środki ochrony – przepustki, kontrola sprzętu fotograficznego i nagrywającego, kontrola teczek, przenośnych komputerów i pakietów, bezpieczeństwo techniczne, dokumenty należące do delegacji, bezpieczne przechowywanie dokumentów, kontrola pomieszczeń, niszczenie zbędnych wydruków zawierających informacje klasyfikowane UE).

W sekcji X określono różnego rodzaju sytuacje związane z nieprzestrzeganiem przepisów bezpieczeństwa i narażeniem na szwank bezpieczeństwa informacji klasyfikowanych UE. Sekcja XI została poświęcona problematyce ochrony informacji przekazywanych w systemach teleinformatycznych (definicje, zakresy odpowiedzialności, nietechniczne środki ochrony, techniczne środki ochrony, bezpieczeństwo przetwarzania informacji, zakupu sprzętu i oprogramowania, okresowe lub doraźne korzystanie ze sprzętu komputerowego).

W sekcji XII określono zasady udostępniania informacji klasyfikowanych UE państwom trzecim i organizacjom międzynarodowym (poziom współpracy, umowy).

Załączniki dotyczą następujących zagadnień: wykaz krajowych władz bezpieczeństwa, zestawienie porównawcze klauzul tajności, praktyczny przewodnik nadawania klauzul, zlecenia odnoszące się do udostępniania informacji klasyfikowanych UE państwom trzecim i organizacjom międzynarodowym – współpraca na poziomie 1, 2, i 3.

Warto zwrócić uwagę, iż problematyka bezpieczeństwa fizycznego pozostaje w szczególnym zainteresowaniu Rady UE, o czym może świadczyć dyrektywa dotycząca bezpieczeństwa fizycznego w zakresie związanym z ochroną informacji klasyfikowanych UE, która stanowi dokument wykonawczy w stosunku do części II, sekcja IV „Przepisów bezpieczeństwa UE" 2001/264/EC. Dyrektywa zawiera przepisy obligatoryjne, a także informacje wyjaśniające ich znaczenie dla pracowników Sekretariatu Generalnego Rady, odnosi się ona do następujących zagadnień: wymagania w zakresie bezpieczeństwa, środki ochrony fizycznej, standardy minimalne przechowywania informacji klasyfikowane UE, ochrona przed stosowaniem środków technicznych, bezpieczeństwo fizyczne systemów i sieci teleinformatycznych.

Komisja Europejska określana jest jako „Rząd Wspólnoty Europejskiej", za swoją działalność ponosi odpowiedzialność przed Parlamentem Europejskim. Komisja wykonuje funkcje w zakresie inicjatywy legislacyjnej, funkcje wykonawcze i funkcje reprezentacyjne.

Decyzja Komisji Europejskiej z dnia 29 listopada 2001 roku w sprawie zmiany jej regulaminu wewnętrznego postanowiła, że przepisy bezpieczeństwa Komisji, które są dołączone do tej decyzji, zostaną dodane do regulaminu wewnętrznego Komisji jako aneks. System bezpieczeństwa Komisji został oparty na zasadach zawartych w decyzji Rady 2001/264/EC, z uwagi na konieczność zapewnienia sprawnego przebiegu procesu podejmowania decyzji w ramach UE. Komisja podkreśla, że istotne jest, by także inne instytucje – gdy ma to zastosowanie – przyjmowały przepisy i standardy bezpieczeństwa, niezbędne w celu ochrony interesów UE i jej państw członkowskich. Komisja uznaje także potrzebę stworzenia własnej koncepcji ochrony, biorąc pod uwagę wszystkie elementy bezpieczeństwa i szczególny charakter Komisji jako instytucji. Komisarz odpowiedzialny za kwestie bezpieczeństwa jest zobowiązany do podjęcia odpowiednich środków w celu zapewnienia, że przepisy bezpieczeństwa Komisji będą przestrzegane w toku pracy z informacjami klasyfikowanymi w UE w ramach Komisji przez jej urzędników i innych pracowników, przez osoby delegowane do pracy w Komisji, a także we wszystkich obiektach Komisji, włącznie z jej przedstawicielstwami i biurami w UE oraz przedstawicielstwami w państwach trzecich, także przez zewnętrznych kontrahentów. W celu zapewnienia, że przestrzegane są podstawowe zasady i minimalne standardy bezpieczeństwa określone w części I aneksu, komisarz odpowiedzialny za kwestie bezpieczeństwa może stosować środki przewidziane w części II aneksu.

Aneks składa się z 2 części oraz 6 załączników.

W części I określono podstawowe zasady i minimalne standardy bezpieczeństwa, których celem jest zapewnienie bezpieczeństwa oraz zagwarantowanie każdemu z wymienionych podmiotów, że został ustanowiony jednolity stopień ochrony. W części I określono następujące zagadnienia: zasady ogólne, podstawy bezpieczeństwa, zasady ochrony informacji – cele, definicje, klauzule tajności, cele stosowania środków bezpieczeństwa, organizacja systemu bezpieczeństwa – wspólne standardy minimalne, organizacja (w ramach Komisji system bezpieczeństwa ma charakter dwupoziomowy: na poziomie Komisji istnieje Biuro Bezpieczeństwa Komisji razem z władzą akredytacji bezpieczeństwa Security Accreditation Authority (SAA), pełniące także funkcję władzy kryptograficznej Crypto Authority (CrA) i władzy TEMPEST, oraz władzą bezpieczeństwa teleinformatycznego (INFOSEC Authority, IA), a także jedną lub kilkoma głównymi kancelariami tajnymi UE (Central EUCI Registry), z których każda zatrudnia

jednego lub kilku urzędników kontroli kancelarii (Registry Control Oficer, RCO), na poziomie poszczególnych departamentów Komisji, za bezpieczeństwo są odpowiedzialni jeden lub kilku lokalnych pełnomocników ochrony (Local Security Oficer, LSO), jeden lub kilku głównych inspektorów bezpieczeństwa teleinformatycznego (Central Informatics Security Oficer, CSIO), lokalni inspektorzy bezpieczeństwa teleinformatycznego (Local Informatics Security Oficer, LISO) oraz lokalne kancelarie tajne UE (Local EU Classified Information Registry), zatrudniające jednego lub kilku urzędników kontroli kancelarii (RCO), bezpieczeństwo osobowe – postępowania sprawdzające, wykaz osób, które zostały poddane postępowaniom sprawdzającym, szkolenie w zakresie bezpieczeństwa, obowiązki przełożonych, weryfikacja pracowników mających dostęp do informacji klasyfikowanych, bezpieczeństwo fizyczne – potrzeba ochrony, kontrola zabezpieczeń, ochrona budynków, plany ochrony na wypadek sytuacji nadzwyczajnych, bezpieczeństwo teleinformatyczne, przeciwdziałanie sabotażowi oraz innym formom złośliwego i celowego szkodzenia, udostępnianie informacji klasyfikowanych państwom trzecim i organizacjom międzynarodowym.

W części II określono organizację bezpieczeństwa w Komisji (komisarz odpowiedzialny za kwestie bezpieczeństwa, Rada Bezpieczeństwa Komisji, Biuro Bezpieczeństwa Komisji, kontrole w zakresie bezpieczeństwa, klauzule, zastrzeżenia i oznaczenia, zasady nadawania klauzul, bezpieczeństwa fizyczne, stosowanie zasady ograniczonego dostępu i postępowania sprawdzające, sprawdzanie urzędników i innych pracowników Komisji, sporządzanie, dystrybucja, przesyłanie, bezpieczeństwo osobowe kurierów oraz dodatkowe egzemplarze lub tłumaczenia i wyciągi z dokumentów klasyfikowanych UE, kancelarie tajne UE, kontrole kompleksowe i wyrywkowe, archiwizowanie i niszczenie dokumentów klasyfikowanych UE, środki bezpieczeństwa stosowane w trakcie spotkań odbywanych poza siedzibą Komisji, w toku których wykorzystywane są informacje klasyfikowane UE, nieprzestrzeganie przepisów bezpieczeństwa i narażanie na szwank bezpieczeństwa informacji klasyfikowanych UE, ochrona informacji przetwarzanych w systemach teleinformatycznych, udostępnianie informacji klasyfikowanych UE państwom trzecim i organizacjom międzynarodowym). Załączniki dotyczą następujących spraw: zestawienia porównawcze klauzul tajności, praktyczny przewodnik nadawania klauzul, zalecenia odnoszące się do udostępniania informacji klasyfikowanych UE państwom trzecim lub organizacjom międzynarodowym – współpraca na poziomie 1, 2 i 3, wykaz skrótów.

Warto zwrócić uwagę na decyzję Rady 2007/274/WSiSW z dnia 23 kwietnia 2007 roku dotyczącą zawarcia Umowy między Unią Europejską a rządem Stanów Zjednoczonych Ameryki w sprawie bezpieczeństwa informacji niejawnych, która została zawarta 30 kwietnia 2007 roku w Waszyngtonie[9]. Umowa składa się z 20 artykułów, w których uregulowano następujące kwestie: zakres stosowania, definicje, klauzule tajności, ochrona informacji niejawnych, postępowania sprawdzające wobec pracowników, przeniesienie obowiązku ochrony, bezpieczeństwo należących do stron obiektów i placówek, w których przechowywane są informacje niejawne, udostępnianie informacji niejawnych wykonawcom, przesyłanie informacji, wizyty w obiektach i placówkach stron, wzajemne wizyty w celu sprawdzenia bezpieczeństwa, nadzór, uzgodnienia techniczne dotyczące bezpieczeństwa, zmiana klauzul tajności na niższe i znoszenie klauzul tajności, utrata lub narażenie na szwank bezpieczeństwa informacji niejawnych, rozstrzyganie sporów, koszty, możliwości w zakresie ochrony, inne umowy, wejście w życie, zmiany i wypowiedzenie. Ze strony rządu Stanów Zjednoczonych Ameryki nadzór nad wykonaniem umowy sprawują sekretarze: stanu i obrony oraz dyrektor państwowych służb wywiadowczych, a ze strony UE nadzór sprawują Sekretarz Generalny Rady oraz członek Komisji odpowiedzialny za kwestie bezpieczeństwa.

4 OCHRONA INFORMACJI NIEJAWNYCH W NATO

Podpisanie przez RP umowy o bezpieczeństwie z NATO, umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji nałożyło na RP szereg zobowiązań, m.in. w zakresie stworzenia systemu bezpieczeństwa informacji klasyfikowanych NATO[10]. RP zobowiązała się do:

- ☒ ochrony i zabezpieczenia przed ujawnieniem informacji niejawnych NATO, dokumentów przekazywanych przez NATO przez państwa członkowskie oraz informacji tajnych wymienionych

[9] Dz. Urz. UE, L 115/29-34 z 03.05.2007.

[10] I. Stankowska, *Procedury sprawdzeniowe umożliwiające dostęp do informacji klasyfikowanych w świetle przepisów ustawy z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych*, w: *Prawne i administracyjne aspekty bezpieczeństwa osób i porządku publicznego*, red. W. Bednarek, S. Pikulski. Olsztyn 2000, s. 381.

między partnerami Sojuszu w ramach realizacji programu, projektu lub kontraktu NATO,

- przestrzegania zasad, że informacje i materiały oznaczone klauzulą tajności będą w taki sam sposób traktowane przez wszystkich członków Sojuszu i chronione według wspólnie ustalonych norm,
- wykorzystywania informacji klasyfikowanych tylko w celach określonych w Traktacie Północnoatlantyckim bądź przy podejmowaniu decyzji zmierzających do realizacji programu lub rezolucji wspólnoty,
- nieprzekazywania informacji i materiałów niejawnych stronom nie będącym członkami NATO bez zgody strony, która dostarczyła.

Należy podkreślić, iż w Sekretariacie NATO funkcjonuje jako samodzielna jednostka organizacyjna NATO Office of Security, której dyrektor jest głównym doradcą Sekretarza Generalnego NATO w sprawach bezpieczeństwa oraz pełni funkcję przewodniczącego Komitetu Bezpieczeństwa NATO. W Sekretariacie NATO usytuowany jest także Komitet Specjalny skupiający szefów służb specjalnych państw członkowskich.

W Biurze Bezpieczeństwa NATO prowadzone były prace związane z przygotowaniem porozumienia z UE w sprawie bezpieczeństwa m.in. ochrony informacji niejawnych, mają one na celu jednolicenie zasad bezpieczeństwa w tych organizacjach, nie wszystkie kraje NATO są członkami UE, stąd występują pewne problemy. W NATO prezentowany był pogląd, iż UE powinna przyjąć zasady bezpieczeństwa, które już sprawdziły się w NATO i na to była zgoda organów UE. Umowa między Unią Europejską a Organizacją Traktatu Północnoatlantyckiego w systemie bezpieczeństwa informacji zawarta została 14 marca 2003 roku w Atenach.

Biuro Bezpieczeństwa NATO odpowiada za bezpieczeństwo personelu NATO (wewnętrzne monitorowanie, wyjaśnianie „przecieków" informacji, przekazywanie informacji właściwym służbom specjalnym, wyjaśnianie zainteresowań pracownikami NATO przez obce służby specjalne, współpraca ze służbami specjalnymi belgijskimi, briefingi dla personelu NATO, sprawdzenia gości NATO).

Unormowania NATO ściśle określają prawa dostępu do informacji i materiałów chronionych klauzulą tajności. Warunkiem dopuszczenia do tajemnicy Sojuszu jest stwierdzenie, że osoba, której przyznano takie

prawo, nie zagrozi – wskutek świadomego działania bądź jakichkolwiek zaniedbań – bezpieczeństwu wspólnoty i nie narazi na uszczerbek jej interesów.

Nakłada to – jak podkreśla I. Stankowska[11] – na organy odpowiedzialne za ochronę informacji klasyfikowanych w agencjach NATO i krajach członkowskich obowiązek uprzedniego sprawdzenia, czy osoby dopuszczone do informacji klasyfikowanych dają rękojmię zachowania tajemnicy, czy są godne zaufania i można im powierzyć cechowane określoną klauzulą tajności bez obawy ich utraty bądź nieuprawnionego ujawnienia. Służby temu mają procedury sprawdzające, prowadzone według wspólnie ustalonych reguł. Procedury te są podejmowane wobec każdej osoby ubiegającej się o dostęp do informacji klasyfikowanych i za jej zgodą. Pozytywny wynik postępowania sprawdzającego dokumentowany jest poświadczeniem, tzw. certyfikatem bezpieczeństwa NATO (*security clearance certificate*), upoważniającym do dostępu do informacji chronionych tajemnicą.

Dyrektywy NATO wprowadzają zasadę *need to know*, ograniczającą dostęp do informacji chronionych tajemnicą zarówno pod względem podmiotowym, jak i przedmiotowym. Standardy NATO nie przewidują możliwości zapewnienia dostępu do informacji niejawnych Sojuszu wyłącznie z tytułu zajmowanego stanowiska, posiadanego stopnia, czy też ze względu na konieczność wykonania powierzonej pracy i związanych z tym obowiązków, nie uprawnia również do tego fakt posiadania certyfikatu bezpieczeństwa NATO. Powyższe oznacza, że do informacji objętych tajemnicą mogą być dopuszczone wyłącznie osoby, które:

- nie mogłyby wykonywać swojej pracy i wypełniać powierzonych obowiązków bez korzystania z informacji niejawnych,
- zostały poddane procedurze sprawdzającej, przeprowadzonej zgodnie z obowiązującymi zasadami,
- posiadają certyfikat bezpieczeństwa NATO potwierdzający, że dają rękojmię zachowania tajemnicy.

Dyrektywy NATO dotyczące bezpieczeństwa osobowego nakazują, aby procedury sprawdzające były prowadzone ze szczególną starannością.

Prowadzenie postępowań sprawdzających i powiadamianie organów NATO o ich rezultatach należy do obowiązków krajowych władz bezpieczeństwa (ABW i SKW).

[11] Ibidem, s. 381 nast.

Należy podkreślić, iż RP, jak i pozostałe państwa członkowskie Sojuszu, zobowiązały się chronić informacje niejawne zgodnie ze wspólnymi zasadami i standardami bezpieczeństwa obowiązującymi w Sojuszu. Podstawowym układem odniesienia wyznaczającym zasady bezpieczeństwa informacji oraz procedury działania w tym zakresie jest dokument „Security within the North Atlantic Treaty Organisation" (Dokument C-M (2002) 49 z dnia 17 czerwca 2002). Dokument ten ma charakter wspólnego porozumienia, tzn. że każde państwo członkowskie przed przystąpieniem do Sojuszu podpisuje „Porozumienie w sprawie bezpieczeństwa", które w dokumencie C-M (2002) 49 jest oznaczone jako Aneks A, natomiast Aneks B – tego dokumentu tj. „Podstawowe zasady bezpieczeństwa", określa podstawowe zasady bezpieczeństwa w sojuszu. Oznacza to, że Aneks A i B wyznaczają zobowiązania sojusznicze każdego z państw członkowskich, jak i zasady, które muszą być implementowane do wewnętrznych rozwiązań ochrony informacji niejawnych[12].

Dokument C-M zawiera 7 aneksów oznaczonych literami od A-G oraz 6 dyrektyw wspierających, oznaczonych symbolami od AC/35 – D/2000 do AC/35 – D/ 2005. Dyrektywy wspierające określają struktury i zakres odpowiedzialności i wymagań oraz procedury działania w zakresie różnych obszarów bezpieczeństwa (bezpieczeństwo osobowe, fizyczne, informacji, INFOSEC, zarządzanie INFOSEC dla CIS, bezpieczeństwo przemysłowe).

Można zauważyć, że pomiędzy Dokumentem C-M a polskim systemem prawnym ochrony informacji niejawnych występuje pełna zgodność, aczkolwiek w wielu kwestiach szczegółowych nasze rozwiązania są bardziej rygorystyczne, niż zawarte w dokumencie C-M. W aneksie B pkt 2 stwierdza się, że „Państwa NATO oraz cywilne i wojskowe władze NATO zapewnią przestrzeganie minimum standardów bezpieczeństwa, które zostały przedstawione w dokumencie C-M. Dotyczy to zwłaszcza klasyfikowania informacji oraz ich ochrony przed utratą, nieuprawnionym udostępnianiem oraz zniekształceniem ich treści". W aneksie tym podkreślono, że wytworzone informacje/materiały niejawne podlegają kontroli wykonawcy/właściciela informacji i strona, której są one udostępniane, musi przestrzegać wymagań strony udostępniającej, jeżeli nawet wymagania te są bardziej rygorystyczne niż te, które określono w Dokumencie C-M.

[12] L. Woźniak, *Rządowe wymagania przetargów związanych z dostępem do informacji niejawnych*, w: *Ochrona informacji niejawnych i biznesowych. Materiały I Kongresu*, red. M. Gajos, S. Zalewski, Katowice 2005, s. 92 nast.

W NATO ustanowiono również zasady udostępniania informacji jawnych, gdyż uznano, iż nawet dokumenty jawne, ale wytworzone przez organy Sojuszu nie mogą być ogólnodostępne ani przekazywane mediom.

5
PRAWNOMIĘDZYNARODOWA REGULACJA OCHRONY INFORMACJI NIEJAWNYCH

Ochrona informacji niejawnych, które mogą być wymieniane między poszczególnymi państwami jest przedmiotem uregulowań wielostronnych bądź dwustronnych.

Należy nadmienić, iż Umowa między stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 roku weszła w życie w stosunku do RP dnia 21 października 1999 roku.

Podpisywane są także umowy dwustronne, i to zarówno między państwami członkami NATO, jak i z innymi, które mają przede wszystkim na celu wzajemną ochronę informacji niejawnych.

W dniu 30 kwietnia 1999 roku została podpisana umowa między rządem RP a rządem RFN w sprawie wzajemnej ochrony informacji niejawnych (Dz.U. z 2002 r. Nr 206, poz. 1748).

Dotychczas podpisano umowy także z rządami Norwegii, Federacji Rosyjskiej, Czech, Estonii, Łotwy, Ukrainy, Słowacji, Rumunii, Bułgarii, Włoch, Chorwacji, Hiszpanii, Wielkiej Brytanii, Węgier, Uzbekistanu, Albanii, Finlandii, Portugalii, Szwecji, Francji i Litwy oraz USA (umowa w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej).

Inne umowy dwustronne są przygotowywane, a już podpisane znajdują się w procedurze ratyfikacyjnej, ich dalsze podpisywanie uwarunkowane jest wzajemnymi interesami poszczególnych państw, które nie zawsze są tożsame z naszymi oczekiwaniami w tym zakresie.

Warto zwrócić uwagę na umowę między rządem RP a rządem RFN, która stanowiła *sui generis* wzorzec dla innych, składa się ona z 13 artykułów, w których uregulowano następujące kwestie: definicje i porównywalność, działania wewnątrzpaństwowe, zlecenia dotyczące informacji niejawnych, wykonywanie zleceń dotyczących informacji niejawnych, oznaczanie informacji niejawnych, przekazywanie informacji niejawnych, wizyty, naruszenie regulacji dotyczących wzajemnej ochrony informacji niejawnych,

koszty zastosowania środków bezpieczeństwa, właściwe organy, konsultacje, stosunek do wcześniejszych porozumień, wejście w życie, okres obowiązywania, zmiana, wypowiedzenie).

Podkreślić należy, iż umowy dwustronne o wzajemnej ochronie informacji niejawnych mają ważne znaczenie m.in. dla przedsięwzięć w zakresie bezpieczeństwa przemysłowego i warto postulować dalsze ich podpisywanie, kierując się przede wszystkim ochroną naszych interesów narodowych, głównie gospodarczych.

Problematyka ochrony informacji niejawnych została uregulowana także w: umowie Organizacji Traktatu Północnoatlantyckiego o przekazywaniu informacji technicznych dla celów obronnych, ratyfikowana przez RP (Dz.U. z 2000 r. Nr 64, poz. 742 i 743), umowie o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w przypadku których zostały złożone wnioski o udzielenie patentów, ratyfikowana przez RP (Dz.U. z 2000 r. Nr 64, poz. 744 i 745).

Wspomnieć należy również o umowie między RP a Europejskim Biurem Policji o współpracy w zwalczaniu przestępczości sporządzonej w Warszawie dnia 3 października 2001 roku (Dz.U. z 2002 r. Nr 144, poz. 1210), której art. 12 dotyczy poufności informacji Europolu, a art. 13 informacji przekazywanych Europolowi.

Zgodnie z art. 12 ust. 5 RP zobowiązuje się do zapewnienia, by wszystkie informacje dostarczone jej przez Europol i oznaczone jako „poziomy Europolu od 1 do 3" korzystały na jej terytorium z ochrony odpowiadającej poziomom zabezpieczeń określonych w Akcie Rady z dnia 3 listopada 1998 roku przyjmującym Zasady poufności informacji Europolu (OJ 1999/C26/02) („Przepisy o poufności") oraz w przepisach wykonawczych. Europol będzie informować RP, w niezbędnym zakresie, o środkach ochrony związanych z poziomami zabezpieczeń Europolu i pakietami bezpieczeństwa.

Natomiast według ust, 6 RP zapewnia, że przepisy jej prawa wewnętrznego o ochronie informacji oznaczonych jako wymagające ochrony stanowią wystarczającą podstawę do zapewnienia przekazywanym zgodnie z tą umową informacjom poziomu zabezpieczenia równorzędnego z określonym w „Przepisach o poufności" oraz w jego przepisach wykonawczych.

Przepis art. 13 ust. 2 stanowi, że wybierając poziom zabezpieczenia, jednostka organizacyjna do spraw współpracy z Europolem będzie uwzględniać klasyfikację informacji zgodną z przepisami prawa wewnętrznego, jak

również potrzebę operacyjnej elastyczności, wymaganej do prawidłowego funkcjonowania Europolu.

Należy podkreślić, iż na stan bezpieczeństwa informacyjnego wpływa wiele zagrożeń, mogą to być:

- przestępstwa komputerowe, cyberterroryzm,
- przestępstwa kryminalne, np. kradzież laptopa, dokumentów, włamanie do sieci, nielegalny podsłuch,
- zagrożenia ze strony służb specjalnych,
- zagrożenia nadzwyczajne,
- naruszanie przez organy władzy i administracji publicznej prywatności obywateli,
- „przecieki".

Wymieniony katalog jest otwarty. Istnieje stale niebezpieczeństwo ujawniania informacji prawnie chronionych nieuprawnionym podmiotom. Przyczyny tego zjawiska mogą być bardzo różne, wśród nich można wymienić słabą znajomość obowiązujących przepisów, lekceważący stosunek do tych przepisów, niespójność prawa. Nieuprawnione ujawnienia mogą mieć charakter: polityczny, komercyjny, błędu. Informacje prawnie chronione bywają przedmiotem bezprawnego obrotu ze strony nosicieli, którzy kierują się w tym zakresie różnego rodzaju motywacją (chęć osiągnięcia korzyści majątkowej lub osobistej, chęć zemsty, rozgoryczenie, złość itp.).

Nową sytuację dla ochrony informacji, w tym niejawnych stwarza zjawisko globalizacji. Niewątpliwie rosnąć będzie zagrożenie cyberterroryzmem, które wymaga podejmowania różnorodnych działań: legislacyjnych, logistycznych, operacyjnych, profilaktycznych. Rozwój techniki sprzyja szpiegowaniu (w tym uzyskiwaniu informacji prawnie chronionych), coraz nowocześniejsze urządzenia do inwigilacji są dostępne na rynku, rośnie również popyt na sprzęt wykrywający, wzrasta też zainteresowanie usługami detektywów szukających podsłuchów w pomieszczeniach. Rozszerzane są pola do przeprowadzania badań personelu przy użyciu poligrafu.