ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3469
PRZEGLĄD PRAWA I ADMINISTRACJI XCI
WROCŁAW 2012

RAFAŁ MIKOWSKI
Uniwersytet Wrocławski

WYBRANE PODSTAWY PRAWNE OCHRONY INFORMACJI NIEJAWNYCH

1. WPROWADZENIE

Źródła prawa administracyjnego w zakresie ochrony informacji niejawnych obejmują znaczną liczbę aktów prawnych, co ze względu na zasadę dostępu do informacji publicznej[1] dowodzi złożoności problemu i potrzeby ciągłego dookreślania pojęć nieostrych, chociażby poprzez nieustanne weryfikowanie zasad na rzecz wyjątków. Wyodrębnienie problemu ochrony informacji niejawnych w zamkniętym systemie źródeł prawa[2] niezbędne jest w konstruowaniu pojęcia państwa prawnego czy też w konstatowaniu istnienia państwa prawnego. Podczas gdy dostęp do treści prawa ma niewątpliwie charakter powszechny, sam zamknięty system źródeł prawa musi w swoich aktach normatywnych wyrazić sprzeczną z ideą dostępu do informacji zasadę, że do pewnych uregulowań, których treść sam ten porządek prawny nie wskazuje, zabronione jest dojście dla powszechnych odbiorców w wyniku regulacji tego porządku prawnego. Mamy tu zatem do czynienia z sytuacją, w której w powszechnym porządku prawnym obowiązującymi aktami prawnymi są tylko: konstytucja, umowy międzynarodowe, ustawy,

[1] Artykuł 54 ust. 1, art. 61, 74 ust. 3, art. 213 ust. 1 Konstytucji RP z 2 kwietnia 1997 r. (Dz.U. z 1997 r., Nr 78, poz. 483), art. 2 ust. 1 Ustawy z 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198 z późn. zm.).

[2] W wyszukiwaniu i badaniu aktów prawnych z zakresu ochrony informacji niejawnych istotne wydaje się skonfrontowanie ich znaczenia z ogólnym pojęciem, jakim jest termin „źródła prawa". W literaturze odnaleźć można zgodny pogląd, że nie jest to pojęcie rozumiane jednoznacznie. Zob. F. Longchamps, *O źródłach prawa administracyjnego (problemy poznawcze)*, [w:] *Studia z zakresu prawa administracyjnego ku czci Prof. dr. Mariana Zimmermanna*, Warszawa-Poznań 1973, s. 95–104. Autor uznaje termin „źródła prawne" za nie najtrafniej dobrane pojęcie, wykazując, że zostało ono przejęte z uniwersyteckiej tradycji historii prawa (przez *sources du droit*, *Rechtsquellen* i podobne nazwy historycy rozumieli głównie dokumenty i przekazy, w których spisywano dawne prawa). Uważa on, że nazwa „drogi tworzenia się prawa" byłaby w tym względzie trafniejsza.

rozporządzenia i prawo miejscowe — a w obrębie regulacji ochrony informacji niejawnych granice i możliwości wyznaczane są niewątpliwie przez akty niższego rzędu. Rolę podstawową, spośród powszechnie obowiązujących źródeł prawa, poza przyzwoleniem zawartym w konstytucji dopuszczającym ograniczenie dostępu obywateli do pewnej kategorii informacji[3], spełnia tu Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[4]. Interpretacja przepisów konstytucji w oparciu o uznane akty prawa międzynarodowego z zakresu dostępu do informacji (Powszechna deklaracja praw człowieka ONZ, Konwencja o ochronie praw człowieka i podstawowych wolności, Międzynarodowy pakt praw obywatelskich i politycznych ONZ) potwierdza wyjątkowość unormowań dotyczących ochrony informacji, ale i konieczność stworzenia prawnego wyłomu w regule swobodnego dostępu do informacji[5].

2. KONSTYTUCYJNE PODSTAWY OCHRONY INFORMACJI NIEJAWNYCH

Regulacje zawarte w konstytucji zezwalają na ograniczenia w korzystaniu z wolności i praw pod warunkiem konieczności ich statuowania w demokratycznym państwie ze względu na ich merytoryczną zasadność. Ograniczenia powinny przy tym być wyważone tak, aby nie przekraczały koniecznego zakresu i nie prowadziły do dowolności oceny[6]. Konstytucja, wprowadzając w art. 54 ust. 1 ogólne prawo do pozyskiwania i rozpowszechniania informacji, nie ustanawia kategorycznej, absolutnej i nieograniczonej wolności w tym zakresie. Również art. 61 ust. 1 i 2 dający prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, działalności organów samorządu gospodarczego i zawodowego, a także innych jednostek organizacyjnych, w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa, podlega ograniczeniom określonym w art. 61 ust. 3. Ograniczenie powyższych praw może nastąpić tylko w drodze ustawy[7]. Zatem konstytucyjna zasada swobody pozyskiwania i rozpo-

[3] T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 115.

[4] Dz.U. z 2010 r., Nr 182, poz. 1228.

[5] K. Liedel, *Ochrona informacji niejawnych*, Warszawa 2003, s. 3.

[6] B. Fischer, *Ochrona informacji niejawnych*, „Prawo i Życie" 1999, nr 2.

[7] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228 z późn. zm.), dział VII ustawy z dnia 29 sierpnia 1997 r. — Ordynacja podatkowa (Dz.U. z 2012 r., poz. 749), art. 104, 105 i 105a ustawy z dnia 29 sierpnia 1997 r. — Prawo bankowe (Dz.U. z 2002 r., Nr 72, poz. 665), art. 8a Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2001 r., Nr 142, poz. 1592), art. 11b Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r., Nr 142, poz. 1591), art. 15a Ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz.U. z 2001 r., Nr 142, poz. 1590), art. 10, 14 i 36 — art. 39 Ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz.U. z 2012 r., poz. 591).

wszechniania informacji z jednej strony ustala zakres tych praw, z drugiej zaś wyznacza granice dopuszczalności ograniczeń wynikających z praw i wolności obywatelskich.

Określone w art. 61 ust. 3 przesłanki ograniczania prawa do informacji budzą wątpliwości jedynie w kwestii ewentualnej nadinterpretacji pojęcia ważnego interesu gospodarczego państwa[8]. Większość zatem przesłanek ograniczania dostępu do informacji wydaje się zasadna, zważywszy na nieustanne przemiany społeczno-polityczne i związany z tym rozwój i rozrost ingerencji państwa w dobie internetu, digitalizacji działań administracji, a także narastającego zagrożenia terrorystycznego, niekoniecznie związanego z używaniem siły i przemocy — sprowadzającego się coraz częściej do wykradania informacji nieprzeznaczonych do powszechnego wglądu. Konstytucja RP pozostawia możliwość, aby w sposób konkretny, a zarazem obiektywny ograniczyć dostęp do sfery informacyjnej, po to by chronić porządek i bezpieczeństwo państwa, a co za tym idzie — bezpieczeństwo obywatela.

Ogólna norma zezwalająca na ograniczenia w korzystaniu z konstytucyjnych praw i wolności ustanowiona została w art. 31 ust. 3 Konstytucji RP. Ograniczenia te są możliwe wyłącznie, jeżeli dotyczą zapewnienia bezpieczeństwa i porządku publicznego, ochrony środowiska, moralności publicznej, wolności i praw innych osób — wyrażone mogą być jedynie w ustawie.

Obowiązek zachowania i zabezpieczenia pewnych informacji przed dostępem do nich każdego, kto nie ma prawnych, jasno sformułowanych uprawnień, można wyprowadzić także z art. 82 konstytucji. Powstrzymywanie się od działań szkodzących państwu, a także czynne przeciwstawianie się działaniom innych podmiotów godzących w bezpieczeństwo i dobro państwa[9] potwierdza obowiązek ochrony informacji niejawnych pomimo braku określenia tajemnicy państwowej jako odrębnej wartości (taki obowiązek wprowadzony był w art. 93 ust. 1 Konstytucji PRL z dnia 22 lipca 1952 r.)[10]. Uregulowanie to potwierdza nienaruszalność przepisów ustaw o ochronie innych tajemnic prawnie chronionych, do których zaliczyć możemy między innymi tajemnicę korespondencji, tajemnicę lekarską, tajemnicę danych osobowych, a które mogą mieć duży wpływ na funkcjonowanie aparatu państwowego. Oznacza to, że do wszystkich innych rodzajów informacji prawnie chronionych stosuje się przepisy tych ustaw, które zawierają regulacje odnoszące się do danej tajemnicy. Sama ustawa o ochronie informacji niejawnych w art. 1 ust. 4 zalicza do podstawowych źródeł prawa z zakresu ochrony

[8] J. Boć, [w:] *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998, s. 115.

[9] B. Banaszak, M. Jabłoński, [w:] *Konstytucje*…, s. 147.

[10] S. Hoc, *Ochrona informacji niejawnych. Wybrane problemy*, „Wojskowy Przegląd Prawniczy" 1999, nr 3/4, s. 3.

informacji niejawnych także odpowiednie przepisy[11] kodeksu postępowania administracyjnego. Do postępowania sprawdzającego, odwoławczego oraz postępowania bezpieczeństwa przemysłowego stosuje się w zakresie nieuregulowanym w ustawie przepisy ustawy z dnia 14 czerwca 1960 r. — Kodeks postępowania administracyjnego[12].

3. PODSTAWY BEZPIECZEŃSTWA INFORMACJI NIEJAWNYCH ZWIĄZANE Z TRAKTATEM PÓŁNOCNOATLANTYCKIM

Uniwersalizacja ochrony informacji niejawnych zapoczątkowana podpisaniem przez Polskę umowy o bezpieczeństwie z NATO[13] wpłynęła na konkretyzację i wydatne dookreślenie nieskrępowanej zasady dostępu do informacji, przede wszystkim przez stworzenie systemu bezpieczeństwa informacji klasyfikowanych NATO[14]. W państwach członkowskich Paktu Północnoatlantyckiego obowiązują bezsprzeczne procedury i standardy wypracowane mimo braku konkretnego nakazu przez procesy normatywne dążące do stworzenia jednolitych wzorców zabezpieczenia informacji[15]. Podstawą skutecznego realizowania celów Traktatu jest niewątpliwie wypracowanie wspólnych zasad dotyczących wymiany informacji niejawnych poprzez stworzenie standardów i procedur związanych ze współdziałaniem narodowych systemów ochrony informacji niejawnych z odpowiednimi strukturami stron Traktatu Północnoatlantyckiego. Zgodnie z art. 2 umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji[16] podstawę bezpieczeństwa działalności NATO powinny stanowić krajowe instytucje bezpieczeństwa zajmujące się ochroną informacji wytworzonych przez NATO lub przekazywanych NATO przez państwa członkowskie. Trwała współpraca pomiędzy stronami umowy skutkować ma wypracowaniem wspólnych zasad umożliwiających jednakowe traktowanie informacji zastrzeżonych, czego przejawem jest niewykorzystywanie informacji niejawnych w inny sposób niż ten, który wspólnie ustaliły strony w Traktacie, przez co dostęp do tych informacji dla stron niebędą-

[11] Artykuł 1 ust. 4 Ustawy z 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198, z późn. zm.).

[12] Ustawa z dnia 14 czerwca 1960 r. — Kodeks postępowania administracyjnego (Dz.U. z 2000 r., Nr 98, poz. 1071, z późn. zm.).

[13] Traktat Północnoatlantycki z dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r., Nr 87, poz. 970).

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

[15] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczpospolitej*, Kraków 2000, s. 181 nn.

[16] Dz.U. z 2000 r., Nr 64, poz. 740.

cych członkami NATO jest niemożliwy bez zgody nakładającego odpowiednią klauzulę.

W literaturze stosunkowo łatwo można odnaleźć pogląd, że podstawowy, a zarazem minimalny zakres wyznaczający zasady bezpieczeństwa informacji niejawnych opracowany został przez sygnatariuszy NATO w dokumencie *Security within the North Atlantic Treaty Organisation* (Dokument C-M/55/15, wersja ostateczna wraz z uzupełnieniem dok. C-M/95/79). Określony został tutaj minimalny zakres podstaw bezpieczeństwa, stanowiący zobowiązanie każdego z państw członkowskich do wdrożenia w rozwiązaniach wewnętrznych, wspólnych, a przede wszystkim podstawowych, zasad ochrony informacji niejawnych[17]. Jak podkreśla L. Woźniak, polski system ochrony informacji niejawnych, przez uwzględnienie zasad określonych w dokumencie C-M, został w pełni dostosowany do rozwiązań Sojuszu, a nawet znacznie przekroczył wymagania postawione przez porozumienie w sprawie bezpieczeństwa, w którym to określono podstawowe, a zarazem bezwzględnie wymagane minimum standardów bezpieczeństwa.

Podstawa organizacji polskiego systemu ochrony informacji niejawnych opiera się także na uregulowaniach zawartych w umowie o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w których przypadku zostały złożone wnioski o udzielenie patentów[18]. Ratyfikując powyższą umowę, każdy kraj członkowski Organizacji Traktatu Północnoatlantyckiego zobowiązał się do ochrony informacji związanych z wynalazkami dotyczącymi obronności, w których przypadku zostały złożone wnioski patentowe. Oczywista współpraca gospodarcza oraz wzajemna pomoc w dziedzinie obronności, polegająca na rozwoju myśli technicznej wymaga wzajemnego informowania się o wynalazkach dotyczących obronności. Powyższe zobowiązania do ochrony tajemnicy wynalazków związane są bezwzględnie z zawartymi między rządami stron Traktatu Północnoatlantyckiego zobowiązaniami do wzajemnej ochrony i zabezpieczania informacji niejawnych podlegających wymianie, w tym także informacji związanych z wynalazkami, na które została nałożona tajemnica w interesie obrony narodowej. Zgodnie z art. III umowy nieodzownym elementem ochrony wynalazków podnoszących bezpieczeństwo NATO jest ochrona wynalazków skutkująca ograniczaniem dostępu poprzez nakładanie klauzuli tajemnicy, co niejednokrotnie może wiązać się ze zrzeczeniem się roszczeń do rekompensaty za utratę wynalazku lub z powodu szkody powstałej z nałożenia klauzuli tajemnicy na ten wynalazek od osoby ubiegającej się o patent. Wynalazek podlegający ochronie podlega takim samym procedurom dostępowym przy wymianie informacji związanych z obronnością NATO co informacje niejawne, natomiast tajemnica może zostać zniesiona, zgodnie z art. IV umowy, jedynie na wniosek rządu wydającego

[17] 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 nn.

[18] Dz.U. z 2000 r., Nr 64, poz. 744.

zakaz. Istotne wydaje się także uregulowanie wypowiedzenia niniejszej umowy, które jednakowoż nie wpływa na podjęte zobowiązania oraz prawa nabyte przez strony-sygnatariuszy na mocy tej umowy. Zapis taki charakterystyczny jest dla większości umów zawieranych przez rządy państw członkowskich, co świadczyć może o solidnych podstawach i nienaruszalności ochrony jakichkolwiek informacji, które zdecydowano się zabezpieczać[19].

Podobnie mocno zaakcentowane zostały uregulowania dotyczące ochrony wrażliwych informacji z dziedziny techniki w umowie Organizacji Traktatu Północnoatlantyckiego o przekazywaniu informacji technicznych dla celów obronnych[20]. Umowa ratyfikowana przez RP zawarta została w celu zwiększenia indywidualnej i zbiorowej zdolności do odparcia zbrojnej napaści. Rozwój zdolności obronnych szczególnie wyraźnie uwidacznia się w zapisach niniejszej umowy, które wskazują na wagę zastrzeżonych informacji technicznych przekazywanych między rządami-stronami i organizacjami NATO. Informacje techniczne służące badaniom w dziedzinie obronności, rozwoju oraz produkcji sprzętu i materiałów wojskowych powinny być w sposób szczególny zabezpieczone, przez co w art. I umowy zdefiniowane zostały pojęcia: „zastrzeżone informacje techniczne", „ujawnienie zgodne z wymogami poufności", „nieuprawnione ujawnienie" oraz „nieuprawnione korzystanie". Poprzez dookreślenie powyższych pojęć wykazany został w art. II obowiązek ochrony informacji zastrzeżonych, które zostały przekazane zgodnie z procedurami zachowania poufności. Obowiązek ten polega na ochronie informacji przed przekazaniem, opublikowaniem lub wykorzystaniem bez wymaganego upoważnienia. Aby można było skutecznie realizować zobowiązania wynikające z tej umowy, a także by można mówić o komplementarności systemu ochrony jakichkolwiek informacji, do których dostęp został ograniczony, rządy-strony niniejszej umowy zobowiązują się podejmować i rozwijać w ramach Rady Północnoatlantyckiej odpowiednie prawne działania. Dotyczyć one mają, zgodnie z art. IV umowy, przekazywania, otrzymywania oraz korzystania z zastrzeżonych informacji technicznych, udziału NATO w procedurach związanych z informacjami technicznymi oraz wypracowaniem procedur związanych ze zmianą warunków wykorzystywania zastrzeżonych informacji technicznych. Skutkować ma to zapewnieniem informacjom technicznym odpowiedniego bezpieczeństwa. W art. V umowy określone to zostało jako co najmniej ten sam stopień ochrony dla informacji zastrzeżonej, uzyskanej przez odbiorcę, jaki zapewnił tej informacji przekazujący.

[19] Por. art. VII umowy o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w przypadku których zostały złożone wnioski o udzielenie patentów na przykład z art. 9 umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji niejawnych i z art. X umowy między stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych.

[20] Dz.U. z 2000 r., Nr 64, poz. 742.

Sprostać wymogom stawianym przez Organizację Traktatu Północnoatlantyckiego, dotyczącym szeroko rozumianego bezpieczeństwa państwa, muszą także strony Traktatu w zakresie współpracy wojskowej. Zważywszy, że siły zbrojne jednego państwa mogą zostać wysłane na podstawie porozumienia na terytorium umawiającej się strony, regulacjom został poddany status sił zbrojnych na terytorium państwa przyjmującego. Mając na uwadze art. II umowy między państwami-stronami Traktatu Północnoatlantyckiego dotyczącej statusu sił zbrojnych, w związku z art. VII przedmiotowej umowy[21], siły zbrojne, ich członkowie, personel cywilny, członkowie rodzin mają obowiązek przestrzegać prawa państwa przyjmującego oraz powstrzymywać się od działalności niezgodnej z niniejszą umową. Za działalność niezgodną z prawem strony umowy uznają między innymi wszystko, co narusza lub zagraża bezpieczeństwu państwa zarówno przyjmującego, jak i wysyłającego. Zachowanie takie obejmuje czyny związane z naruszeniem ochrony różnego rodzaju informacji, do których dostęp jest zabroniony, co przejawia się w przestępstwach obejmujących zdradę państwa, sabotaż, szpiegostwo, a także działania naruszające jakiekolwiek przepisy dotyczące tajemnicy państwowej lub tajemnicy związanej z obronnością. Jak z tego wynika, bezpieczeństwo państwa można naruszyć także poprzez nielegalne działania informacyjne. W takich wypadkach strony umowy określiły dość szczegółowo postępowanie w sprawach sprawowania jurysdykcji zarówno w stosunku do osób podlegających prawu wojskowemu, jak i personelu cywilnego oraz członków rodzin. Umowa nie stanowi przeszkody do wprowadzenia obostrzonych przepisów, niezbędnych do zapewnienia należytego bezpieczeństwa i ochrony w stosunku do instalacji, sprzętu, mienia, archiwów i oficjalnych informacji innych umawiających się stron, o czym świadczy zapis w art. VII, pkt 11 umowy[22].

Stworzenie skutecznych form i metod ochrony wiadomości niejawnych odgrywa główną rolę z punktu widzenia bezpieczeństwa i obronności państw zaangażowanych nie tylko w działania NATO, lecz także Unii Europejskiej. W celu stworzenia takich podstaw, przede wszystkim funkcjonalnych, oraz pogłębiania wiedzy na potrzeby operacji połączonych NATO i działań bojowych na szczeblu taktycznym Polska podpisała 13 kwietnia 2005 r. umowę[23], która dotyczy mieszczącego się w Bydgoszczy Centrum Szkolenia Sił Połączonych — JFTC, służącego wspieraniu szkolenia sił NATO i państw uczestniczących w Partnerstwie dla Pokoju. Cel umowy został określony w art. I, który mówi także o poprawie interoperacyjności oraz wspieraniu Naczelnego Sojuszniczego Dowódcy Transformacji w realizacji jego zadań jako organu kierowniczego NATO w kwestii transforma-

[21] Dz.U. z 2000 r., Nr 21, poz. 257 (sprost. Dz.U. z 2008 r., Nr 170, poz. 1052).

[22] *Ibidem*.

[23] Umowa między Rządem Rzeczypospolitej Polskiej a Dowództwem Naczelnego Sojuszniczego Dowódcy Transformacji (HQ SACT) dotycząca ustanowienia i wsparcia Centrum Szkolenia Sił Połączonych (JFTC) NATO na terytorium Rzeczypospolitej Polskiej, (Dz.U. z 2005 r., Nr 227, poz. 1945).

cji. Także tutaj zauważyć można podstawowe zasady bezpieczeństwa i związane z nimi standardowe postępowania sprawdzające związane zarówno z wykonawcami kontraktowymi, jak i osobami cywilnymi. W art. V umowy sprecyzowany został obowiązek, niezależny od narodowości, poddania odpowiednim procedurom wymaganym przez przepisy NATO wszystkich osób personelu cywilnego w celu uzyskania stosownych poświadczeń bezpieczeństwa. Umowa nakłada na Polskę jako państwo przyjmujące obowiązek udostępnienia nieruchomości położonych w Bydgoszczy, zapewnienia zewnętrznej ochrony obiektów JFTC, dostarczania kopii wszelkich obowiązujących przepisów dotyczących zdrowia, bezpieczeństwa czy ochrony środowiska, a także przepisów związanych z obchodzeniem się z materiałami niebezpiecznymi. Adekwatnie określone zostały także w art. VI obowiązki dowództwa Naczelnego Sojuszniczego Dowódcy Transformacji, jego przedstawicieli oraz JFTC.

Wymiernym wkładem w rozwój mobilności militarnej, bezpieczeństwa Sojuszu oraz państw zaangażowanych, a szczególnie bezpieczeństwa związanego z JFTC służącego wspieraniu szkolenia sił NATO i państw uczestniczących w Partnerstwie dla Pokoju, jest zapewnienie odpowiednich warunków przechowywania, wykorzystywania, przekazywania i ochrony informacji niejawnych, co gwarantuje art. X umowy, w całości poświęcony wyłącznie ochronie informacji niejawnych[24]. Odpowiednio uregulowane zostało postępowanie ze sprzętem mającym niejawny charakter, co wskazuje, że zapewnienie bezpieczeństwa poprzez ochronę informacji niejawnych może dotyczyć nie tylko informacji pojmowanej jako wiadomość, wiedza, dane, lecz może to także być związane z pewnego rodzaju wytworami stanowiącymi część lub całość określonego urządzenia, do którego dostęp został ograniczony. Ograniczenie to może dotyczyć zarówno danych technicznych objętych odpowiednią klauzulą, jak i samego wyglądu zewnętrznego. Można zatem chronić samą zewnętrzność w rozumieniu cech fizycznych, wyglądu samej rzeczy. Obowiązek ochrony wynikający z niniejszego artykułu dotyczy także korespondencji oraz informacji wytwarzanej przez JFTC — zarówno dostarczanej, jak i wymienianej. Strony umowy zobowiązują się chronić informacje niejawne przed nieuprawnionym dostępem i ujawnieniem wszelkimi dostępnymi, ale wyłącznie zgodnymi z prawem środkami, do których zaliczyć można między innymi zachowanie oryginalnych klauzul tajności lub oznaczenie klauzulą zapewniającą stopień ochrony równorzędny z tym, jaki jest wymagany przez jedną ze stron umowy. Pomocne ma tu być także oznaczenie informacji

[24] Wyodrębnienie osobnego artykułu poświęconego informacjom niejawnym wskazuje na wagę i prawidłowe podejście do problemu ochrony informacji oraz na wskazanie sposobu realizacji podstawowych obowiązków związanych z przepisami dotyczącymi bezpieczeństwa i dyrektywami NATO, na co wskazują również A. Żebrowski i W. Kwiatkowski, *op. cit.*, s. 191, którzy przedstawiają zasady udostępniania informacji niejawnych w taki sposób, aby interesy bezpieczeństwa NATO i państw członkowskich były zawsze uwzględniane już na etapie planowania i wdrażania programów kooperacyjnych. Dotyczy to zarówno personelu wojskowego, jak i cywilnego.

niejawnych odpowiednim opisem, zawierającym pochodzenie, klauzulę tajności, warunki ujawnienia oraz adnotację, że informacja jest niejawna. Także w tym wypadku można mówić o wypracowanych, wspólnie uzgodnionych standardach ochrony informacji niejawnych, które są charakterystyczne dla współdziałania w ramach NATO, co można zauważyć w różnego rodzaju dokumentach, identyfikowanych w ściśle określony i przyjęty sposób.

W Organizacji Traktatu Północnoatlantyckiego obowiązują klauzule niejawności, którym odpowiadają określone klauzule w państwie będącym stroną odpowiedniej umowy. Dodatkowo w NATO wiele dokumentów oznaczanych jest w sposób kwalifikowany, to znaczy taki, który świadczy o tym, że dokument ten jest własnością Sojuszu, a informacja w nim zawarta zawsze stanowi własność autora. Rozumieć przez to należy, że w momencie zdjęcia klauzuli niejawności nie może być ona przekazana poza NATO z wyjątkiem tych przypadków, które określone zostały w odrębnych przepisach[25].

Zgodnie z art. 5 umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji w żaden sposób nie jest ograniczone prawo zawierania przez strony umów dotyczących pozyskiwania, opracowywania, przetwarzania czy przekazywania informacji niejawnych, które od nich pochodzą. Umowy takie nie mają wpływu na obowiązywanie umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji.

Jak widać, na podstawie przeanalizowanych umów wskazać można na wiele regulacji dotyczących ochrony informacji niejawnych charakterystycznych przede wszystkim dla wspólnego i zgodnego funkcjonowania Sojuszu oraz państw członkowskich, a także takich, które z chwilą przystąpienia Polski do NATO zostały uznane i przyjęte do wewnętrznego porządku prawnego, stając się niewątpliwie odnośnikiem, a zarazem źródłem i pewnego rodzaju systemem, w jakim postanowiono zorganizować ochronę informacji niejawnych. Omawianą w tym miejscu ochronę informacji niejawnych wzmacniają także inne umowy zawarte przez Polskę z NATO, a także z państwami-stronami Traktatu Północnoatlantyckiego, które jednak nie regulują wprost omawianego zagadnienia, przez co należy jedynie zasygnalizować i wymienić je z racji uznania ich przez doktrynę[26] za mające wpływ na organizację i pogłębianie zasad bezpieczeństwa w NATO. Wskazać tu można na takie akty, jak: Umowa dotycząca statusu Organizacji Traktatu Północnoatlantyckiego, przedstawicieli narodowych i personelu międzynarodowego[27], Umowa w sprawie przedstawicielstw i przedstawicieli państw trzecich przy Organizacji Traktatu Północnoatlantyckiego[28], Protokół dotyczący statusu międzynarodowych dowództw, ustanowionych na podstawie Traktatu Północnoatlantyckiego[29],

[25] A. Żebrowski, W. Kwiatkowski, *op. cit*., s. 187.
[26] Zob. I. Stankowska, *op. cit*., s. 381 nn.
[27] Dz.U. z 2000 r., Nr 64, poz. 736.
[28] Dz.U. z 2000 r., Nr 64, poz. 738.
[29] Dz.U. z 2000 r., Nr 64, poz. 746.

czy Umowa między państwami-stronami Traktatu Północnoatlantyckiego a innymi państwami uczestniczącymi w Partnerstwie dla Pokoju, dotycząca statusu ich sił zbrojnych, oraz jej Protokół dodatkowy[30].

4. UMOWY MIĘDZYNARODOWE Z ZAKRESU OCHRONY INFORMACJI NIEJAWNYCH

Potwierdzeniem ważkości i aktualności problemu regulacji prawnomiędzynarodowych z zakresu informacji niejawnych jest liczba umów międzynarodowych, zawartych przez Polskę od dnia sporządzenia 6 marca 1997 r. w Brukseli umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji niejawnych. Kolejno wyróżnić można w tym miejscu umowy w sprawie wzajemnej ochrony informacji niejawnych zawarte między Rządem RP a: Rządem RFN, sporządzoną w Gdańsku 30 kwietnia 1999 r.[31], Gabinetem Ministrów Ukrainy, podpisaną w Warszawie 4 września 2001 r.[32], Rządem Republiki Słowackiej, podpisaną w Starej Lutowni 29 lipca 2002 r.[33], Rządem Republiki Łotewskiej, podpisaną w Warszawie 26 lutego 2003 r.[34], Rządem Republiki Estońskiej, podpisaną w Warszawie 12 maja 2003 r.[35], Rządem Republiki Chorwacji, podpisaną w Zagrzebiu 17 września 2003 r.[36], Rządem Republiki Albanii, podpisanąw Tiranie 21 września 2004 r.[37], Rządem Republiki Czeskiej, podpisaną w Pradze 7 grudnia 2004 r.[38], Rządem Republiki Włoskiej, podpisaną w Rzymie 22 lutego 2007 r.[39], Rządem Republiki Bułgarii, podpisaną w Warszawie 7 kwietnia 2005 r.[40], Królestwem Hiszpanii, podpisaną w Madrycie 18 kwietnia 2006 r.[41], Rządem Rumunii, podpisaną w Bukareszcie 5 lipca 2006 r.[42], Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, podpisaną w Warszawie 18 sierpnia 2006 r.[43], Rządem Królestwa Norwegii, podpisaną w Warszawie 28 lutego 2007 r.[44] Następnie także Umowa między Rządem RP a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących

[30] Dz.U. z 1998 r., Nr 97, poz. 605.
[31] Dz.U. z 2002 r., Nr 206, poz. 1748.
[32] Dz.U. z 2004 r., Nr 193, poz. 1974.
[33] Dz.U. z 2004 r., Nr 117, poz. 1214.
[34] Dz.U. z 2004 r., Nr 221, poz. 2242.
[35] Dz.U. z 2005 r., Nr 189, poz. 1585.
[36] Dz.U. z 2007 r., Nr 141, poz. 992.
[37] Dz.U. z 2005 r., Nr 247, poz. 2093.
[38] Dz.U. z 2005 r., Nr 193, poz. 1612.
[39] Dz.U. z 2007 r., Nr 30, poz. 196.
[40] Dz.U. z 2006 r., Nr 197, poz. 1446.
[41] Dz.U. z 2007 r., Nr 141, poz. 994.
[42] Dz.U. z 2007 r., Nr 141, poz. 996.
[43] Dz.U. z 2007 r., Nr 140, poz. 985.
[44] Dz.U. z 2008 r., Nr 22, poz. 132.

ochronie informacji niejawnych w sferze wojskowej, podpisana w Warszawie 30 listopada 2007 r.[45], a w dalszej kolejności umowa między RP a: Rządem Republiki Finlandii o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie 25 maja 2007 r.[46], Rządem Królestwa Szwecji, podpisana w Warszawie 6 września 2007 r.[47], Rządem Federacji Rosyjskiej, podpisana w Moskwie 8 lutego 2008 r.[48], Rządem Republiki Francuskiej o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie 28 maja 2008 r.[49], Rządem Republiki Litewskiej w sprawie wzajemnej ochrony informacji niejawnych, podpisana w Warszawie 12 maja 2008 r.[50], Republiką Portugalską o wzajemnej ochronie informacji niejawnych, podpisana w Lizbonie 2 sierpnia 2007 r.[51] Wskazać należy również na Umowę zawartą między Rządem Rzeczypospolitej Polskiej a Organizacją do spraw Współpracy w Zakresie Uzbrojenia (OCCAR) o ochronie informacji niejawnych dotyczących realizacji Programu OCCAR ESSOR, podpisaną w Warszawie dnia 29 kwietnia 2009 r. oraz w Bonn dnia 4 maja 2009 r.[52] Należy wreszcie wymienić umowy między Rządem RP a: Rządem Republiki Słowenii o wymianie i wzajemnej ochronie informacji niejawnych, podpisaną w Warszawie 14 maja 2009 r.[53], Rządem Republiki Korei o ochronie wojskowych informacji niejawnych, podpisaną w Warszawie 30 września 2009 r.[54], Rządem Republiki Macedonii o wzajemnej ochronie informacji niejawnych, podpisaną w Skopje 24 listopada 2009 r.[55], Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych, podpisaną w Hanoi 9 września 2010 r.[56] oraz ostatnią z podpisanych umów z Rządem Państwa Izrael reprezentowanym przez Ministerstwo Obrony o wzajemnej ochronie informacji niejawnych związanych ze współpracą obronną i wojskową, podpisaną w Jerozolimie 24 lutego 2011 r.[57]

Jak wynika z powyższego, Polska zawarła umowy międzynarodowe w zakresie wzajemnej ochrony informacji niejawnych nie tylko ze wszystkimi sąsiadującymi bezpośrednio państwami, lecz także z wieloma innymi, z którymi uznano uregulowanie omawianej kategorii za celowe i niezbędne do prawidłowego funkcjonowania aparatu państwa w stosunkach międzynarodowych związanych z szeroko rozumianym bezpieczeństwem.

[45] Dz.U. z 2007 r., Nr 224, poz. 1658.
[46] Dz.U. z 2008 r., Nr 121, poz. 780.
[47] Dz.U. z 2008 r., Nr 217, poz. 1382.
[48] Dz.U. z 2008 r., Nr 217, poz. 1384.
[49] Dz.U. z 2009 r., Nr 49, poz. 394.
[50] Dz.U. z 2009 r., Nr 117, poz. 980.
[51] Dz.U. z 2009 r., Nr 154, poz. 1228.
[52] Dz.U. z 2010 r., Nr 70, poz. 455.
[53] Dz.U. z 2010 r., Nr 118, poz. 791.
[54] Dz.U. z 2010 r., Nr 141, poz. 947.
[55] Dz.U. z 2010 r., Nr 203, poz. 1349.
[56] Dz.U. z 2012 r., Nr 0, poz. 232.
[57] Dz.U. z 2012 r., Nr 0, poz. 253.

Analizując umowę między Polską a RFN, która stanowi *sui generis* wzorzec następnych regulacji, można wskazać na wiele analogicznie uregulowanych kwestii, powtórzonych w innych umowach międzynarodowych dotyczących wzajemnej ochrony informacji niejawnych. Regulacje te dotyczą kwestii związanych z definiowaniem najważniejszych pojęć oraz ich porównywalności, wskazaniem właściwych organów i działań wewnątrzpaństwowych, zleceniami oraz wykonywaniem zleceń dotyczących informacji niejawnych, nazywanych często kontraktami niejawnymi, czy jak w wypadku umowy między Rządem RP a Rządem USA — udostępnianiem kontrahentom, oznaczaniem informacji niejawnych i środkami ich ochrony, przekazywaniem informacji niejawnych z jednego państwa do drugiego, co dokonuje się przez kurierów dyplomatycznych lub wojskowych. Możliwe jest także przekazywanie informacji zabezpieczonych w odpowiedni sposób przez osoby upoważnione do dostępu do informacji niejawnych o porównywalnej klauzuli tajności, w sytuacji gdy właściwe organy umawiających się stron uzgodnią tak w odniesieniu do określonych przypadków.

Uregulowane zostały także wizyty osób przybywających z terytorium jednej z umawiających się stron na terytorium drugiej. Osobom takim zapewnia się dostęp zarówno do informacji podlegających ochronie, jak i do obiektów związanych z informacjami niejawnymi wyłącznie za zezwoleniem strony przyjmującej. Dotyczy to ograniczonej kategorii osób, które pozytywnie przeszły postępowanie sprawdzające oraz podejmować mają czynności służbowe uzasadniające dostęp do informacji niejawnych.

W omawianych umowach zawarte zostały także przepisy odnoszące się do konsultacji w zakresie ochrony informacji niejawnych mających na celu zapewnienie ścisłej współpracy, wymiany doświadczeń oraz wzajemnego i bieżącego informowania się o przepisach obowiązujących w prawie wewnętrznym oraz o ich zmianach. Można mówić również o odesłaniach do odpowiednich organów i procedur właściwych ze względu na naruszenie postanowień umowy traktujących o wzajemnej ochronie informacji niejawnych, co zapewnione jest dodatkowo przez poinformowanie zainteresowanej strony o wynikach czynności podjętych w celu wyjaśnienia przyczyn ujawnienia tajemnicy oraz wyciągnięciu odpowiednich konsekwencji.

Późniejsze umowy o wzajemnej ochronie informacji niejawnych podobnie do „umowy wzorcowej" regulują sprawy dotyczące kosztów stosowania środków bezpieczeństwa. Wydatki upoważnionych organów jednej strony, powstające w związku ze stosowaniem środków ochrony informacji niejawnych, nie podlegają zwrotowi przez upoważnione organy drugiej strony. We wszystkich zawartych przez Polskę umowach o wzajemnej ochronie informacji niejawnych znajduje się jednoznaczny zapis mówiący, że koszty związane z realizacją postanowień dotyczących stosowania środków bezpieczeństwa mających na celu ochronę informacji niejawnych każda ze stron pokrywa samodzielnie.

Na koniec warto wskazać na unormowania w zakresie stosunku poszczególnych umów, z przedmiotowego zagadnienia, do wcześniejszych porozumień.

W każdym wypadku uregulowane to zostało analogicznie do „pierwotnej umowy" poprzez objęcie informacji chronionych na podstawie wcześniejszych porozumień odpowiednią ochroną wynikającą bezpośrednio z umowy o wzajemnej ochronie informacji niejawnych, przez co rozumieć należy, że przepisy zawarte w porozumieniach obowiązujących między stronami zachowują moc, jeżeli nie są sprzeczne z postanowieniami nowej umowy. Rozstrzyganie kwestii spornych, wynikłych wskutek rozbieżności w interpretacji lub zastosowania umowy, strony zadeklarowały rozwiązywać wyłącznie w drodze rozmów, konsultacji i bezpośrednich negocjacji pomiędzy właściwymi organami bezpieczeństwa, a w razie gdy rozwiązanie tą drogą będzie niemożliwe, drogą dyplomatyczną. W żadnym wypadku rozstrzyganie sporu nie może zostać przekazane sądowi krajowemu, trybunałowi międzynarodowemu czy też osobie lub podmiotowi zewnętrznemu.

We wszystkich umowach o wzajemnej ochronie informacji niejawnych, jakie zawarła Polska, uregulowana została także problematyka okresu obowiązywania, zmian oraz wypowiedzenia postanowień umowy. Poza uregulowaniami typowymi i charakterystycznymi dla umów międzynarodowych, takich jak wejście w życie umowy po zakończeniu wszystkich procedur wewnętrznych, wymianie odpowiednich not oraz zapisów związanych z ewentualnymi zmianami w umowie po obustronnej akceptacji, wszystkie zawarte umowy zawierają ważną z punktu widzenia ochrony i bezpieczeństwa informacji niejawnych regulację dotyczącą trwałości i niezmienności ochrony informacji raz objętych daną klauzulą. Przejawia się to w nieprzerwanej ochronie informacji bez względu na wypowiedzenie umowy. Wszystkie informacje niejawne, przekazane na podstawie umowy o wzajemnej ochronie informacji niejawnych, mają pozostać nadal chronione zgodnie z postanowieniami umowy. Informacje przekazane na podstawie analizowanych tu umów lub powstałe u zleceniobiorcy informacje niejawne chronione pozostają tak długo, jak długo wymaga tego obowiązywanie klauzuli tajności.

Jak podkreśla S. Hoc[58], umowy bilateralne o wzajemnej ochronie informacji niejawnych mają ważne znaczenie między innymi dla przedsięwzięć realizowanych na polu bezpieczeństwa przemysłowego i należy postulować dalsze ich podpisywanie przede wszystkim ze względów wewnętrznych interesów narodowych, w szczególności gospodarczych.

5. PODSTAWY OCHRONY INFORMACJI NIEJAWNYCH WYNIKAJĄCE Z PRZYSTĄPIENIA POLSKI DO UNII EUROPEJSKIEJ

Problematyka związana z ograniczaniem dostępu do informacji związana jest także ściśle z regulacjami obowiązującymi w Unii Europejskiej. Przystąpienie

[58] S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia*, Opole 2006, s. 174.

Polski do UE implikuje wiele rozwiązań zarówno materialnych, jak i organizacyjnych związanych z funkcjonowaniem różnych sektorów administracji publicznej w zakresie ochrony i bezpieczeństwa państwa i jego obywateli. Znaczący nacisk kładzie się tu oczywiście na działania wewnątrzpaństwowe, dzieląc obowiązki wynikające z prawa wspólnotowego pomiędzy organy centralne, regionalne i lokalne[59]. Przywilejem a zarazem obowiązkiem państwa członkowskiego jest możliwość wykorzystywania wszelkich rozwiązań prawnych zaliczanych do dorobku prawnego UE. Do źródeł zaliczyć tu należy obok dorobku prawnego także orzecznictwo sądowe, zwyczaj oraz umowy międzynarodowe, nie zapominając również o ogólnych zasadach prawa[60].

Regulacje odnoszące się do organizacji i funkcjonowania rozwiązań w dziedzinie bezpieczeństwa zarówno w strukturach UE, jak i poszczególnych państwach czerpiących z dorobku wspólnoty znajdują swój początek w systemie źródeł pierwotnego prawa wspólnotowego. Zaliczyć tu należy przede wszystkim traktaty założycielskie[61] wraz z protokołami i aneksami, a także Jednolity Akt Europejski czy Traktat o Unii Europejskiej podpisany 7 lutego 1992 r. w Maastricht, ale tylko w tej części, która zmienia traktaty rzymskie i traktat paryski, czy jak w odniesieniu do JAE — tylko część modyfikującą lub uzupełniającą traktat o EWG[62]. Jak wynika z orzecznictwa Europejskiego Trybunału Sprawiedliwości, prawo pierwotne bezpośrednio wiąże państwa członkowskie[63], przy czym swoistość prawa europejskiego polega na zasadzie, że Wspólnota nie korzysta z przymiotu suwerenności, ma natomiast kompetencje atrybucyjne[64]. W efekcie, jak zaznacza się w piśmiennictwie, państwa członkowskie pozostają co do istoty suwerenne, a prawo tworzone jest przez ponadnarodowy związek, wyposażony w pierwotną władzę publiczną[65].

Mając na uwadze powyższe rozważania na temat pierwotnego prawa wspólnotowego oraz próbując wskazać na początki regulacji dotyczących zagadnień związanych z bezpieczeństwem struktur UE i państw członkowskich, wskazać

[59] A. Nowak-Far, *Stosowanie* acquis communautaire *przez administracje publiczne państw członkowskich Unii Europejskiej — zagadnienia prawne i organizacyjne*, „Służba Cywilna" 2002, nr 4, s. 31 nn.

[60] J. Barcz, *Prawo Unii Europejskiej. Zagadnienia systemowe*, Warszawa 2003, s. 182.

[61] Traktat paryski z 18 kwietnia 1951 r., ustanawiający Europejską Wspólnotę Węgla i Stali; Traktat rzymski z 25 marca 1957 r., ustanawiający Europejską Wspólnotę Energii Atomowej; Traktat rzymski z 25 marca 1957 r., ustanawiający Europejską Wspólnotę Gospodarczą.

[62] A. Wiktorowska, [w:] M. Wierzbowski *et al.*, *Prawo administracyjne*, Warszawa 2003, s. 73 nn.

[63] J. Boć, [w:] *Prawo administracyjne…*, red. J. Boć, Wrocław 2007, s. 75 nn.

[64] Tylko takie, jakie państwa członkowskie przyznają w traktacie założycielskim, por. C. Mik, *Polskie organy państwowe wobec perspektywy przystąpienia RP do Unii Europejskiej*, [w:] *Polska w Unii Europejskiej. Perspektywy, warunki, szanse i zagrożenia*, red. C. Mik, Toruń 1997, s. 243; J. Boć, [w:] *Prawo administracyjne*, s. 75 nn.

[65] J. Boć, [w:] *Prawo administracyjne…*, s. 75 nn.

należy na art. 10 Traktatu ustanawiającego Wspólnotę Europejską, podpisanego 25 marca 1957 r.[66] Cytując postanowienia art. 10,

> Państwa członkowskie podejmują wszelkie właściwe środki o charakterze ogólnym lub specjalnym w celu zapewnienia realizacji zobowiązań wynikających z niniejszego Traktatu lub z działań podejmowanych przez instytucje Wspólnoty. Państwa te ułatwiają wykonywanie jej zadań. Niepodejmują one żadnych środków, które mogłyby przeszkodzić w realizacji celów niniejszego traktatu […],

należy pamiętać, że traktat jako prawo pierwotne reguluje w zakresie bezpieczeństwa informacji sfery dotyczące całego obszaru działania UE. Regulacje te nie zostały jednak ujęte w obszarze obowiązującego wszystkie państwa członkowskie jednolitego prawa wspólnotowego (pierwszy filar)[67].

Chociaż kwestie bezpieczeństwa i ochrony tajemnicy nie są kompleksowo determinowane wprost przez sam Traktat, to unormowania zawarte w art. 296 ust. 1 wskazują, że Traktat nie stanowi przeszkody w stosowaniu następujących reguł: „a) żadne Państwo Członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa". W literze b niniejszego artykułu zaakcentowana jest druga zasada, kładąca nacisk na samodzielność każdego z państw członkowskich w podejmowaniu działań, jakie uzna za konieczne w celu ochrony podstawowych interesów swojego bezpieczeństwa, co jak już zostało wykazane, świadczy o tym, że każde państwo członkowskie ma kompetencje do samodzielnego normowania obszarów związanych z ochroną informacji niejawnych na swoim terenie.

Warto przytoczyć tu art. 287 Traktatu, zgodnie z którym:

> Członkowie instytucji Wspólnoty, członkowie komitetów, jak również urzędnicy i inni pracownicy Wspólnoty są zobowiązani, również po zaprzestaniu pełnienia swoich funkcji, nie ujawniać informacji, objętych ze względu na swój charakter tajemnicą służbową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych.

Natomiast art. 284 Traktatu przyznaje Komisji Europejskiej kompetencje do zbierania niezbędnych informacji potrzebnych do wykonywania zadań jej powierzonych. Komisja może także dokonywać wszelkich weryfikacji w granicach i na warunkach wyznaczonych przez Radę Europejską zgodnie z postanowieniami Traktatu.

Całkowicie odmiennie przedstawia się sytuacja na poziomie organów UE, czyli dokumentów pochodzących od organów Rady Europejskiej i Komisji Europejskiej. Możemy tutaj mówić o szczegółowej regulacji wszystkich problemów związanych z ochroną informacji niejawnych. Wśród dokumentów pochodzących od UE, regulujących kwestie bezpieczeństwa i ochrony informacji niejawnych

[66] Dz.U. z 2004 r., Nr 90, poz. 864/2.

[67] T. Kęsoń, *Przepisy bezpieczeństwa i ochrony informacji niejawnych Rady Unii Europejskiej*, www.osrodekbadania.waw.pl/files/keson_8.doc (dostęp: 10 maja 2008).

wymienić należy: rozporządzenie EURATOM nr 3 w sprawie wykonania art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej[68], decyzję Rady Europejskiej z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa, 2001/264/WE[69] i decyzję Komisji Europejskiej zmieniającą jej regulamin wewnętrzny, 2001/844/WE, EWWiS, Euratom[70].

Należy powiedzieć, jak zaznacza A. Wiktorowska[71], że zarówno rozporządzenia, jak i decyzje pochodzące od organów Wspólnoty, obok dyrektyw, zaleceń, opinii czy prawa powstałego w wyniku zawierania umów międzynarodowych, są pochodnym prawem wspólnotowym. Akty prawa wtórnego mają zarówno bezpośredni skutek dla państw członkowskich, jego obywateli i podmiotów gospodarczych, jak i skutek pośredni, przy czym przesądza o tym nie nazwa aktu, lecz jego cel i treść[72].

W tym miejscu wymienić należy Rozporządzenie EURATOM nr 3 z dnia 31 lipca 1958 r., w art. 1, regulujące zakres w odniesieniu do przedmiotu, ustalające stopnie tajności oraz środków bezpieczeństwa, które mają zastosowanie w odniesieniu do informacji uzyskanych przez Wspólnotę lub przekazywanych przez państwa członkowskie objęte art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej[73]. Zgodnie z art. 1 Rozporządzenia EURATOM nr 3 w sprawie wykonania art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej uregulowania te dotyczą także informacji zawartych w art. 25 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej. Informacje takie są traktowane jako informacje niejawne Euratom z zastrzeżeniem jednak, że rozporządzenie stosuje się jedynie do tych informacji, których użycie podlega zakresowi Traktatu. Zatem jako informacje niejawne Euratom należy traktować zarówno informacje uzyskane przez Wspólnotę lub przekazane przez państwa członkowskie, objęte art. 24 i art. 25 Traktatu ustanawiającego Wspólnotę Energii Atomowej, jak i różnego rodzaju sprawozdania, dane, dokumenty, przedmioty oraz środki reprodukcji.

Jak podkreśla M. Woźniak[74], prymat prawa wspólnotowego implikuje zasadę bezpośredniego stosowania prawa wspólnotowego, co z kolei stanowi fundamentalną wartość całego systemu prawnego Unii Europejskiej. Jak podnosi autorka, zasada pierwszeństwa odnosi się do pierwszeństwa w stosowaniu, a nie do pierwszeństwa obowiązywania. Skutkuje to oparciem rozstrzygnięcia organu krajowego na prawie wspólnotowym w momencie kolizji normy prawa krajowego z normą prawa wspólnotowego. Z powyższego autorka wyprowadza zasadę bezpośrednie-

[68] Dz. Urz. L 17 z 6.10.1958, s. 406.
[69] Dz. Urz. L 101 z 11.04.2001, s. 1.
[70] Dz. Urz. L 317 z 3.12.2001, s. 1.
[71] A. Wiktorowska, *op. cit*., s. 74.
[72] J. Boć, [w:] *Prawo administracyjne*..., s. 75 nn.
[73] Dz.U. z 2004 r., Nr 90, poz. 864/3.
[74] M. Woźniak, *Administracja publiczna wobec prawa wspólnotowego*, [w:] *Nowe problemy badawcze w teorii prawa administracyjnego*, red. J. Boć, A. Chajbowicz, Wrocław 2009, s. 510.

go skutku, oznaczającą (w momencie gdy organem stosującym prawo wspólnotowe jest organ administracji publicznej), że normy prawa wspólnotowego mogą stanowić samodzielne źródło praw i obowiązków osób fizycznych i prawnych.

Zawarte w decyzjach Rady i Komisji unormowania z zakresu bezpieczeństwa, szczególnie w decyzji Rady z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa[75], mają duże znaczenie również dla polskiego porządku prawnego, dotyczącego ochrony informacji niejawnych. Regulacje te dotyczą wymiany informacji niejawnych w UE, ich obiegu, klasyfikowania, bezpieczeństwa osobowego, przemysłowego, fizycznego, teleinformatycznego oraz postępowania w przypadkach utraty dokumentów niejawnych, czy wreszcie udostępniania informacji niejawnych pochodzących od UE, a przekazywanych poza jej ramy.

Do skutecznej realizacji, wprowadzania w życie i egzekwowania decyzji Rady i Komisji wykształcone zostały w organach Unii Europejskiej odpowiednie struktury odpowiedzialne za bezpieczeństwo informacji. W organie odgrywającym pierwszorzędną rolę w zadaniach z zakresu bezpieczeństwa informacji UE, jakim niewątpliwie jest Rada Unii Europejskiej, wskazać można na podstawowe zadania wykonywane przez Sekretarza Generalnego (Wysoki Przedstawiciel ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa), Komitet Rady ds. Bezpieczeństwa, Biuro ds. Bezpieczeństwa Sekretariatu Generalnego Rady i zdecentralizowane agencje UE. Natomiast w Komisji Europejskiej za bezpieczeństwo informacji odpowiadają: Komisarz odpowiedzialny za kwestie bezpieczeństwa, Dyrektoriat bezpieczeństwa, Grupa Doradcza ds. Polityki Bezpieczeństwa[76].

Należy w tym miejscu zaznaczyć, że głównym organem posiadającym inicjatywę legislacyjną UE jest Rada Europejska traktowana jako jedno z najważniejszych ogniw decyzyjnych, w której skład wchodzą przedstawiciele wszystkich państw członkowskich na szczeblu ministerialnym. Jest to organ międzyrządowy, wspierany przez Sekretariat Generalny, który jest organem pomocniczym o charakterze techniczno-administracyjnym, spełniającym zadania z zakresu organizacyjno-finansowego w działaniach Rady. Ze wskazanej powyżej decyzji Rady wynika, że Sekretarz Generalny dysponuje instrumentami niezbędnymi do zapewnienia bezpieczeństwa informacjom klasyfikowanym UE w ramach prac Sekretariatu Generalnego Rady. Dotyczy to urzędników, innych pracowników oraz kontrahentów zewnętrznych, natomiast państwa członkowskie zobowiązane są do podjęcia odpowiednich środków, zgodnych z regulacjami krajowymi, w celu zapewnienia przestrzegania przepisów bezpieczeństwa Rady w trakcie prac z informacjami klasyfikowanymi UE w ramach ich służb i obiektów[77].

[75] Dz. Urz. L 101, z 11.04.2001, s. 1.

[76] T. Kęsoń, *op. cit*.

[77] S. Hoc, *Ochrona informacji niejawnych i innych tajemnic*…, s. 162.

Z analizowanej decyzji Rady z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów dotyczących bezpieczeństwa wynika, że Rada, Sekretariat Generalny, państwa członkowskie UE oraz zdecentralizowane agencje UE składają się na powszechny system bezpieczeństwa. Decyzja określa minimalne normy bezpieczeństwa tworzące jeden wspólny system o podstawowych zasadach dających gwarancje ustanowienia wspólnych norm ochrony informacji niejawnych.

Oprócz powyższych postanowień wprowadzających zawartych w art. 1–5 decyzja zawiera przepisy bezpieczeństwa Rady, które zostały zamieszczone w załączniku stanowiącym integralną jej część. Zdefiniowane zostały takie pojęcia, jak: informacja niejawna UE, dokument, materiał; wskazane zostały podstawowe cele systemu bezpieczeństwa, przy czym państwa członkowskie zobowiązane są do podjęcia krajowych środków koniecznych do zapewnienia skuteczności tworzonego systemu w każdym przypadku, gdy ich organy lub pracownicy mają styczność z informacjami klasyfikowanymi UE. Określone zostały także podstawy bezpieczeństwa i podstawowe zasady obejmujące środki bezpieczeństwa, nakreślona została organizacja bezpieczeństwa zawierająca wspólne normy minimalne, które mają być przestrzegane we wszystkich służbach administracyjnych i/lub rządowych, instytucjach UE oraz przez wykonawców. Dalej określone zostało bezpieczeństwo pracowników, które gwarantują postępowania sprawdzające, ewidencje postępowań sprawdzających, instrukcje bezpieczeństwa dla pracowników, obowiązki kierownictwa w zakresie znajomości personelu mającego dostęp do różnych tajemnic, a także status bezpieczeństwa pracowników. Wskazać trzeba także na regulacje załącznika w zakresie bezpieczeństwa fizycznego. W tym miejscu określono potrzebę ochrony, przejawiającą się w zasadzie proporcjonalności, polegającą na sprawdzaniu chronionego obszaru przed opuszczeniem przez uruchomienie urządzeń zabezpieczających oraz kontrole przeprowadzane po godzinach pracy, bezpieczeństwo budynków oraz plany awaryjne ochrony informacji niejawnych, które przewiduje się z odpowiednim wyprzedzeniem, na wypadek zagrożenia o charakterze lokalnym lub o zasięgu krajowym. Ochrona bezpieczeństwa informacji wsparta przez system INFOSEC jest kolejnym elementem omówionym w części I załącznika wraz z przeciwdziałaniem sabotażowi oraz innym formom złośliwych i umyślnych szkód, czy wreszcie udostępnianiem informacji niejawnych państwom trzecim lub organizacjom międzynarodowym.

Oprócz najważniejszych organów ustawodawczych Wspólnoty, jakimi niewątpliwie są Parlament Europejski i Rada, wskazać można na ważne miejsce Komisji Europejskiej w działaniach z zakresu inicjatywy legislacyjnej, funkcji wykonawczej i reprezentacyjnej. Zadania Komisji ukierunkowane zostały przez ówczesny art. 155 traktatu rzymskiego na koordynację rozwoju wspólnego rynku, wykonywanie postanowień traktatu, podejmowanie decyzji, uczestniczenie w pracach Rady i Parlamentu Europejskiego oraz podejmowanie uchwał we wszystkich sprawach Wspólnoty i jej polityki[78].

[78] J. Boć, [w:] *Prawo administracyjne*..., s. 72, 73.

System bezpieczeństwa Komisji, ze względu na wypracowanie gwarancji bezpiecznego i sprawnego podejmowania decyzji w Unii, opiera się na ustalonych zasadach, które zostały zawarte w decyzji Rady 2001/264/WE z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów bezpieczeństwa Rady[79]. W decyzji Komisji Europejskiej z dnia 29 listopada 2001 r. zmieniającej jej regulamin wewnętrzny[80] zawarte zostały postulaty stworzenia całościowego systemu bezpieczeństwa obejmującego Komisję, inne instytucje, struktury, biura i agencje ustanowione na mocy Traktatu ustanawiającego Wspólnotę Europejską, lub Traktatu o Unii Europejskiej, państwa członkowskie. Dotyczyć to powinno także wszystkich pozostałych odbiorców informacji klasyfikowanych UE. W tym celu Komisja ma za zadanie udostępniać informacje niejawne wyłącznie takim odbiorcom zewnętrznym, którzy wykażą, że są w stanie stosować wszelkie konieczne środki zapewniające należytą ochronę informacjom klasyfikowanym UE. Warto podkreślić, że powyższe ustalenia nie naruszają przepisów rozporządzenia nr 3 z dnia 31 lipca 1958 roku w sprawie wykonania art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej[81], Rozporządzenia Rady (WE) nr 1588/90 z dnia 11 czerwca 1990 r. w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności[82] i decyzji C (95) 1510 z dnia 23 listopada 1995 roku w sprawie ochrony systemów informatycznych. Postanowień art. 255 i 286 Traktatu ustanawiającego Wspólnotę Europejską[83], Rozporządzenia nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[84] ani Rozporządzenia nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[85]. Komisja podkreśla, że przepisy, a szczególnie standardy bezpieczeństwa konieczne do ochrony interesów Unii i jej państw członkowskich znalazły aprobatę i zostały wdrożone przez inne instytucje, gdy będą mogły zostać zastosowane, wspólnie wypracowane i sprawdzone rozwiązania systemowe. Mając na uwadze swój szczególny charakter, Komisja dążyć będzie do umocnienia własnej koncepcji bezpieczeństwa przy uwzględnieniu wszystkich elementów znanych już obecnemu systemowi ochrony. Zasady bezpieczeństwa Komisji zostały określone w załączniku, przy czym Komisja zastrzega, że państwa trzecie, organizacje międzynarodowe i inne struktury mogą otrzymywać informacje klasyfikowane UE pod warunkiem przestrzegania w toku prac z tymi informacjami zasad ściśle odpowiadających przepisom ustalonym przez UE.

[79] Dz. Urz. L 101 z 11.04.2001, s. 1.
[80] Dz. Urz. L 317 z 3.12.2001, s. 1.
[81] Dz. Urz. L 17 z 6.10.1958, s. 406.
[82] Dz. Urz. L 151 z 15.06.1990, s. 1.
[83] Dz.U. z 2004 r., Nr 90, poz. 864/2.
[84] Dz. Urz. L 145 z 31.05.2001, s. 43.
[85] Dz. Urz. L 8 z 12.01.2001, s. 1.

6. PODSUMOWANIE

W dzisiejszych czasach ogólna zasada wyrażająca prawo dostępu do informacji jest nie do podważenia. Nie wydaje się jednak, by możliwe było stworzenie takiego systemu prawnych uregulowań, który pozwoli na całkowity dostęp do wszystkich informacji, jakie znajdują się w posiadaniu państwa. Dzięki zastosowaniu najnowocześniejszych technik dostęp do informacji staje się tak powszechny, łatwy i oczywisty, że jedyne ograniczenia pochodzą wyłącznie z uregulowań prawnych, obowiązujących w danym systemie prawnym. Analiza wybranych źródeł prawa kształtujących wewnątrzkrajowy system ochrony informacji niejawnych, przy szczególnym uwzględnieniu wpływu uregulowań umiejscowionych poza tym systemem, pozwala zaakcentować nie tylko zmiany, jakie zaszły po przystąpieniu Polski do Paktu Północnoatlantyckiego, ale przede wszystkim nieustanne doskonalenie ochrony informacji niejawnych poprzez wykorzystywanie ponadkrajowych procedur (wzorców) decyzyjnych. W państwach członkowskich Paktu Północnoatlantyckiego obowiązują procedury i standardy tworzące jednolite wzory zabezpieczenia informacji. Do zasad tych należą między innymi: jednakowe traktowanie informacji niejawnych, obowiązek posiadania przez osoby mogące mieć dostęp do informacji chronionych odpowiednich poświadczeń, dających gwarancje dochowania tajemnicy, dopuszczenie do informacji niejawnych NATO wymaga wcześniejszego przeprowadzenia procedury sprawdzającej, a także zakaz wydawania uprawnień do dostępu do informacji niejawnych wyłącznie ze względu na pełnioną funkcję lub zajmowane stanowisko — poświadczenia bezpieczeństwa wydawane powinny być wyłącznie osobom, którym dostęp taki jest niezbędny do wykonania danej pracy czy powierzonego zadania. Wyodrębniając problem ochrony informacji niejawnych w zamkniętym systemie źródeł prawa, niezbędny w konstruowaniu pojęcia państwa prawnego czy też w konstatowaniu istnienia państwa prawnego, zauważyć należy, że wzorowanie się przede wszystkim na zasadach międzynarodowych nie zapobiegło wielu sytuacjom, w których dochodziło do wykorzystania informacji chronionych w sposób nieuprawniony, a wręcz nielegalny. Opieranie zatem systemu ochrony informacji niejawnych wyłącznie na standardach zewnętrznego, międzynarodowego sytemu bezpieczeństwa nie daje gwarancji jego prawidłowego funkcjonowania, bez wykorzystania administracyjnoprawnych regulacji, mających wyraz szczególnie w formach działania organów administrujących. Nasuwa to przypuszczenie, że coś w tym mechanizmie funkcjonuje wadliwie, nie zawsze bowiem istniejące problemy dotyczące nieuprawnionego wykorzystania informacji chronionych leżą w sferze niedostatecznie szczelnej czy niepełnej legislacji. Niejednokrotnie związane jest to z niewłaściwym wykorzystaniem instrumentów prawa publicznego, a zamknięty, precyzyjny, oparty na ścisłej hierarchii system źródeł prawa, porządkujący prawo i czyniący je bardziej przejrzystym, bardziej bezpiecznym dla obywatela, staje się jednocześnie mało elastyczny, powolny i ociężały i nie zawsze stanowi w wystarczającym stopniu

skuteczną ochronę przed nieuprawnionym ujawnieniem informacji chronionych. Jak się niekiedy zauważa, dobre prawo wymaga dobrych wykonawców.

SELECTED LEGAL BASIS FOR THE PROTECTION OF CLASSIFIED INFORMATION

Summary

This paper presents a synthetical analysis of selected legal acts that determine the protection of classified information in national law. By discussing the most important sources of law underlying the organization of the Polish system of the protection of classified information, the author presents further regulations and the resulting rules allowing treatment of the issues concerning the protection of classified information as adequately organized and synchronized primarily with the regulations of NATO and EU member states.

Przegląd Prawa i Administracji XCI, 2012