

Stanisław Topolewski

OCHRONA INFORMACJI NIEJAWNYCH W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Stwierdzić należy z dużą dozą prawdopodobieństwa, że już od początku istnienia ludzkości informacja zawsze była cennym środkiem, choć nie zawsze zdawano sobie z tego sprawę. Współcześnie jej rola została właściwie doceniona, uczestnicząc we wszystkich sferach naszego życia. Pewne jest natomiast to, że w dzisiejszych czasach trudno byłoby bez niej funkcjonować, więc można stwierdzić, że jest jednym z podstawowych składników życia.

Szybko zdobyta i wykorzystana informacja pozwala na skuteczniejsze działanie podmiotów, które nią operują. Dlatego też, w kontekście państwa jej znaczenie tym bardziej wzrasta, jeżeli mamy na uwadze informacje, zwłaszcza te, które mają szczególne znaczenie dla jego trwania i przetrwania.

W dzisiejszych czasach ilość informacji w tym chronionych dynamicznie wzrasta. W związku z tym wyodrębniono z nich te informacje, które wiążą się bezpośrednio z bezpieczeństwem narodowym każdego państwa. Wszelkie informacje niejawne należy odnosić przede wszystkim do sfery bezpieczeństwa danego podmiotu, ponieważ nieuprawniony dostęp do tych informacji skutkować może zburzeniem całego porządku wewnątrz państwa lub zmniejszeniem wiarygodności na arenie międzynarodowej wśród sojuszników. Istotą ochrony informacji niejawnych (OIN) stanowią działania (prawne, organizacyjne i fizyczne) ukierunkowane na zablokowanie dostępu do pewnych ściśle strzeżonych informacji²²⁵. Należy zwrócić szczególną uwagę na to, iż czasy współczesne charakteryzują się ogromnym postępem technicznym i informatycznym, dlatego też OIN stanowi podstawowe zadanie dla służb bezpieczeństwa w celu zabezpieczenia podstawowych interesów państwa.

Zakres przedmiotowy ochrony informacji niejawnych skupia się na tych informacjach, które mają charakter niejawny, w związku z czym ich ochrona jest podstawowym zadaniem państwa. System ochrony powinien być skorelowany w taki sposób, aby informacja niejawna nie trafiła w niepowołane ręce. Z kolei zakres podmiotowy obejmuje wszelkie organy oraz instytucje, które są zobowiązane przepisami prawa do zapewnienia ochrony tym informacjom. W aspekcie bezpieczeństwa państwa podstawowe znaczenie ma ochrona tajemnicy państwowej (informacji ważnych ze względu na bezpieczeństwo kraju).

²²⁵ Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz. 1228)

Dlatego też, nie do wszystkich informacji każdy obywatel RP ma prawo wglądu i dostępu. Aby móc mieć dostęp do informacji niejawnych dana osoba musi posiadać odpowiednie poświadczenie bezpieczeństwa umożliwiające mu dostęp do określonych klauzul tajności. Z tym dostępem wiąże się także zasada zawarta w ustawie mówiąca o „wiedzy niezbędnej”²²⁶, czyli w zakresie niezbędnym do wykonywania obowiązków służbowych.

OIN jest ważnym elementem systemu funkcjonowania państwa, ściśle związanym z jego szeroko pojętym bezpieczeństwem. Jest ona dziedziną życia publicznego w państwie i może być rozpatrywana jako ujęcie systemowe, mówiące o funkcjonowaniu powiązanych ze sobą instytucji razem tworzących pewien model postępowania, z informacjami niejawnymi w taki sposób, by zapewnić im pełną ochronę przed ich nieuprawnionym ujawnieniem. W ujęciu instytucjonalnym jest to zatem grupa organów każdego państwa i instytucji publicznych oraz niepublicznych powiązanych ze sobą według kryterium występowania poszczególnych informacji niejawnych, a także obowiązków nałożonych na nich przepisami prawa.

Ochrona informacji niejawnych rozpatrywana jako czynnik bezpieczeństwa państwa jest sama w sobie instrumentem, którego stosowanie nie jest łatwe i rodzi wiele wyzwań, któremu system musi stawić czoła. W dynamicznie zmieniającym się świecie ważną rolę odgrywa monitorowanie i ciągłe doskonalenie systemu bezpieczeństwa informacji w taki sposób, aby zapobiegał on wszelkim możliwym zagrożeniom mogącym nieść negatywne skutki, zarówno dla jednostki, jak i państwa. „Istotą tego procesu powinno być utrwalenie właściwej – instrumentalnej roli procedur ochrony informacji niejawnych w relacji do bezpieczeństwa państwa”²²⁷.

Kontynuując należy stwierdzić, że ochrona wszelkich informacji niejawnych leży w katalogu podstawowych zadań na rzecz bezpieczeństwa każdego państwa. Organy odpowiedzialne za tę ochronę powinny ciągle doskonalić swoje systemy (środki ochrony informacji niejawnych) w taki sposób, aby odzwierciedlały one nowe realia w zglobalizowanym świecie informacji. Rola informacji niejawnych dla funkcjonowania państwa jest niepodważalnym i jednym z najważniejszych atrybutów jego działalności.

Organizacja systemu ochrony informacji niejawnych

Podstawą prawną systemu ochrony informacji niejawnych w Rzeczypospolitej Polskiej jest Konstytucja²²⁸ oraz wydawane na jej podstawie akty wykonawcze. W Art. 54 ust. 1. Konstytucji Rzeczypospolitej Polskiej w rozdziale „Wolności

²²⁶ Tamże Art. 4

²²⁷ S. Zalewski, *Informacje niejawne we współczesnym państwie (w:) Ochrona informacji niejawnych teoria i praktyka*, (red.) M. Kubiak, S. Topolewski, Siedlce 2013, s. 22.

²²⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.,

i prawa osobiste” zapisano „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji”. Wyrażono w ten sposób wolę społeczeństwa, aby stworzony porządek prawny szanujący wolność człowieka respektował także jego prawa do zdobywania, przekazywania, przetwarzania czy odtwarzania informacji.

Kolejne ważne zapisy znajdujące się w Konstytucji RP dotyczące informacji niejawnych znajdują się w rozdziale „Wolności i prawa polityczne”, tam też znajduje się artykuł 61 który stanowi ²²⁹:

1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.
2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegalnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu.
3. Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.
4. Tryb udzielania informacji, o których mowa w ust. 1 i 2, określają ustawy, a w odniesieniu do Sejmu i Senatu ich regulaminy.

Może zaistnieć sytuacja, która będzie zmuszać do wprowadzenia ograniczeń z przewidzianych przez Konstytucję powodów. Właśnie art. 61 ust 3 Konstytucji RP daje podstawy do wnioskowania, iż funkcjonują prawnie dozwolone sytuacje, w których nawet sam ustawodawca jest zobligowany do ograniczania praw obywateli ze względu na ich dobrze rozumiany interes. Powyższą tezę potwierdza wprowadzenie do porządku prawnego dwóch aktów prawnych, które są wypełnieniem delegacji ustawowej z art. 61 ust 3 Konstytucji RP:

- ustawa o ochronie danych osobowych z 1997 r.²³⁰,
- ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych.

Ustawy te, z jednej strony miały zapobiec pełnej swobodzie dysponowania informacjami, z drugiej wprowadzić w systemie prawnym międzynarodowych standardów bezpieczeństwa informacyjnego.

Ustawa o OIN wprowadziła poziom zabezpieczeń informacji porównywalny do stosowanego już w państwach członkowskich NATO, co było takim wymogiem.

²²⁹ Tamże, art. 61.

²³⁰ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926)

Zadania dotyczące ochrony informacji niejawnych znalazły się również w kolejnych dokumentach wytyczających działalność organów i instytucji bezpieczeństwa, tj. Strategii Bezpieczeństwa Narodowego RP z 2000, 2003 i 2007 r.

W Strategii Bezpieczeństwa Narodowego z 2007 roku w części 3.8. zatytułowanej „Bezpieczeństwo informacyjne i telekomunikacyjne”. Treść tego zapisu brzmi następująco: „Zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjną, w tym zapobieganie atakom na elementy tej infrastruktury. Szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej. Ważnym zadaniem jest opracowanie i wdrożenie przejrzystych zasad dostępu uprawnionych organów państwa do treści przesyłanych drogą elektroniczną. Wymaga to ciągłego dostosowywania przepisów prawa telekomunikacyjnego, by - mimo szybkiego postępu technologicznego – stale odpowiadały współczesnym realiom, uwzględniając bezpieczeństwo Polski.”²³¹

Głównym aktem prawnym, który określa zasady i organizację systemu ochrony informacji niejawnych w Polsce jest ustawa z dnia 5 sierpnia 2010 r.²³² o ochronie informacji niejawnych, która zastąpiła regulację o tej samej nazwie z 1999 r. oraz wydawane na jej podstawie akty wykonawcze rozporządzenia, zarządzenia, decyzje.

Powyższy podział oraz analiza obowiązującego w Polsce stanu prawnego pozwala na stwierdzenie, że system ochrony informacji niejawnych uwzględnia zakresy odpowiedzialności struktur organizacyjnych instytucji państwowych. System ten ujmuje trzy podstawowe obszary: aparat kierujący wydający stosowne przepisy, powiązania informacyjne niezbędne do realizacji procesu kierowania oraz zbiór metod i działań regulujących sposób oraz zasady funkcjonowania opisywanego systemu. System ochrony informacji niejawnych stanowią więc²³³:

- przepisy i reguły z zakresu ochrony informacji niejawnych (ustawa, rozporządzenia, zarządzenia, decyzje, dyrektywy, instrukcje, procedury, wytyczne),
- struktury organizacyjne (Agencja Bezpieczeństwa Wewnętrznego, Służba Wywiadu Wojskowego oraz pioniry ochrony) powiązane ze sobą relacjami (kierowania) w taki sposób, że stanowią one całość zdolną do zapewnienia ochrony informacji niejawnych,
- środki bezpieczeństwa fizycznego służące do ochrony informacji niejawnych (strefy ochronne, systemy alarmowe, sejfy, drzwi, niszcarki do dokumentów, oprogramowanie itp.).

²³¹ Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007., s. 20.

²³² Ustawa z dnia 5 sierpnia..., cyt. wyd.

²³³ *Ochrona informacji niejawnych teoria i praktyka*, (red). M. Kubiak, S. Topolewski, Siedlce 2013, s. 22.

Cechą charakterystyczną systemu ochrony informacji niejawnych RP jest stabilność, zarówno celu jego funkcjonowania, jak i struktury. W systemie tym zarysowane są precyzyjnie funkcje jego elementów, które się zazębiają, przynosząc oczekiwaną, wcześniej zaplanowaną skuteczność działań.

Kolejnymi cechami charakterystycznymi systemu ochrony informacji niejawnych RP jest przejrzystość zasad współdziałania między elementami systemu i wspólnota celów. Pierwsza z nich pozwala na jego sprawne funkcjonowanie w sytuacji zagrożenia, druga zaś pozwala uzyskać w pełni korzyści płynące ze specjalizacji elementów. Częścią stabilną systemu ochrony informacji niejawnych państwa jest struktura organizacyjna, zmienną natomiast – sytuacje zagrożeń dla informacji niejawnych. Naturalną konsekwencją cech opisywanego systemu są funkcje koordynacyjne w systemie ochrony informacji niejawnych RP zlokalizowane na wszystkich szczeblach hierarchii organizacji. Funkcje te sprawują ABW i SKW oraz pionory ochrony.

Przedstawiając strukturę systemu ochrony informacji niejawnych, należy uwzględnić także zasady wynikające z jego organizacji, do których można zaliczyć:

- zasadę jednolitości,
- zasadę sprawnego działania,
- zasadę fachowości.

Zasada jednolitości oznacza, że wszystkie jej organy powinny współdziałać ze sobą, opierając się na więzi organizacyjnej o charakterze nadrzędności i podporządkowania. Dlatego też system ochrony informacji powinien stanowić jednolity, zamknięty układ zróżnicowanych organów, między którymi występują więzi organizacyjne i zależności funkcjonalne.

Zasada sprawnego działania oznacza, że elementy systemu ochrony informacji niejawnych muszą działać zgodnie z zasadami prakseologii, tzn. szybko, skutecznie i ekonomicznie. Sprawne działanie nakazuje uwzględnienie współzależności struktury organizacyjnej i funkcji elementów systemu oraz doboru odpowiednich metod i form działania, a także reguł wypracowanych przez naukę o organizacji i zarządzaniu.

Zasada fachowości jest rezultatem realizacji zasad sprawnego działania za pomocą podziału zadań pomiędzy elementami systemu ochrony informacji niejawnych.²³⁴

System Ochrony Informacji Niejawnych opiera się o działający na wszystkich szczeblach organizacyjnych aparat wykonawczy, którego zadaniem jest do wykonywania prac i wspierania innych instytucji w obszarze zadań wyznaczonych przez ustawę. Aparaty te posiadają odpowiednie kompetencje, stwarzające warunki do koordynacji i kierowania działaniami w sytuacjach godzących w bezpieczeństwo informacji niejawnych.

²³⁴ Tamże, s. 23.

Współdziałanie ABW i SKW z innymi częściami systemu ochrony informacji niejawnych płynie z ustawy i rozporządzeń, jak i porozumień zawieranych pomiędzy różnymi służbami. Prawne przepisy oraz porozumienia ściśle określają formy i sposoby współpracy poszczególnych elementów systemu. Najczęstszymi sposobami koordynacji działań są: wymiana posiadanych zasobów informacyjnych, wspólne szkolenia, podejmowanie działań na wniosek współpracujących partnerów, wzajemnie udzielana pomoc, udostępnianie sił i środków jakie są do dyspozycji.

Mając na celu utrzymanie bezpieczeństwa informacji niejawnych na odpowiednim poziomie, konieczne jest, podejmowanie szeregu posunięć systemowych, takich jak:

- zapobieganie zagrożeniom i ich skutkom,
- minimalizowanie ryzyka zagrożeń i ich skutków,
- przygotowanie systemów reagowania odpowiednich do możliwości zagrożeń,
- skuteczne reagowanie w przypadku wystąpienia zagrożeń,
- przygotowanie i realizacje programów odbudowy,
- współczesne wymagania stawiane systemowi ochrony informacji niejawnych kładą szczególny nacisk na jego spójność i jednolitość w warstwie koordynowania działań i wspólnych procedur, w szczególności: planowania, organizowania, wymiany informacji, szkolenia.

Zgodnie z art. 1 ust. 1 przedmiotem ustawy są zasady ochrony informacji niejawnych, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, a w szczególności:

- klasyfikowania informacji niejawnych,
- organizowania ochrony informacji niejawnych,
- przetwarzania informacji niejawnych,
- postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym” lub „kontrolnym postępowaniem sprawdzającym”,
- postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego”,
- organizacji kontroli stanu zabezpieczenia informacji niejawnych,
- ochrony informacji niejawnych w systemach teleinformatycznych,
- stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Podmiotami które zostały przez ustawodawcę zobowiązane do przestrzegania przepisów ustawy o ochronie informacji niejawnych w myśl art. 1 ust. 2 są:

- organów władzy publicznej, w szczególności:
 - Sejmu i Senatu,
 - Prezydenta Rzeczypospolitej Polskiej,
 - organów administracji rządowej,
 - organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
 - sądów i trybunałów,
 - organów kontroli państwowej i ochrony prawa,
- jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,
- Narodowego Banku Polskiego,
- państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych,
- jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy,
- przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

Zgodnie z polskim prawodawstwem za problematykę ochrony informacji niejawnych w państwie, ujętą w ramy systemu odpowiadają stosownie do posiadanych kompetencji odpowiednie organy, którymi są:

- Rada Ministrów a w szczególności kolegium do spraw służb specjalnych,
- Agencja Bezpieczeństwa Wewnętrznego dla sfery cywilnej i Służba Kontrwywiadu Wojskowego dla resortu wojskowego,
- kierownicy jednostek organizacyjnych w poszczególnych podmiotach systemu,
- pełnomocnicy ochrony w jednostkach,
- kierownicy Kancelarii tajnych,
- administratorzy bezpieczeństwa Teleinformatycznego,
- inspektorzy bezpieczeństwa Teleinformatycznego,
- osoby upoważnione do dostępu do informacji niejawnych.

Przy Radzie Ministrów funkcjonuje kolegium do Spraw Służb Specjalnych, które jest organem opiniodawczo-doradczym w sprawach programowych, nadzorczych i koordynacyjnych ABW, AW, SKW, SWW oraz CBA ogólnie rzecz biorąc, wszystkich służb specjalnych w RP. Kolegium to za zadanie ma formułowanie ocen, bądź wyrażania opinii m.in. w sprawach ochrony informacji niejawnych, a dotyczących w szczególności²³⁵:

²³⁵ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Art. 12 ust. 1.

- zagrożeń w skali ogólnokrajowej w ramach ochrony informacji niejawnych które stanowią tajemnice państwową,
- sposobów działania w okolicznościach zagrożenia o skali ogólnokrajowej, zaistniałej poprzez ujawnienie informacji niejawnych stanowiących tajemnicę państwową, jak i ocenianie skutków ujawnienia takowych informacji,
- projektowania aktów normatywnych i innych dokumentów rządowych dotyczących ochrony informacji niejawnych,
- innych spraw polecanych przez RM lub PRM oraz przez ministrów poszczególnych resortów, w ramach wypełniania zadań powiązanych z ochroną informacji niejawnych,
- rozporządzenie RM z dnia 2 lipca 2002 r. szczegółowo reguluje sady oraz tryb funkcjonowania Kolegium do Spraw Służb Specjalnych.

Szczególną rolę w systemie ochrony informacji niejawnych pełnią ABW oraz SKW. Obie służby można nazwać „fundamentem” całego systemu. Zadaniem ich jest nadzorowanie funkcjonowania systemu ochrony informacji niejawnych w jednostkach organizacyjnych, które pozostają w ich właściwości.

Głównym zadaniem Agencji Bezpieczeństwa Wewnętrznego jest ochrona państwa przed planowymi i zorganizowanymi posunięciami, mogącymi rodzić zagrożenia dla niepodległości lub porządku konstytucyjnego Polski, zaburzać działanie struktur państwowych, bądź narażać na szwank zasadnicze interesy państwa. Najważniejszymi zasadami ABW są:

- zwalczanie terroryzmu,
- działalność kontrwywiadowcza,
- przeciwdziałanie proliferacji Broni Masowego Rażenia (BMR),
- zwalczanie przestępczości zorganizowanej,
- przeciwdziałanie korupcji,
- **ochrona informacji niejawnych,**
- analizy oraz informacje.

Swoje obowiązki ABW wypełnia m.in. poprzez uzyskiwanie, analizowanie i przetwarzanie informacji o niebezpieczeństwach. Gotowe opracowania przekazywane są właściwym organom konstytucyjnym, zaś przy realizacji zadań Agencja korzysta z uprawnień operacyjnych oraz procesowych.

W zakresie ochrony informacji niejawnych realizacja przez ABW zadań nałożonych przez przepisy ustawy ma głównie charakter prewencyjny, wynikający z nierepresyjnej filozofii systemu ochrony informacji niejawnych, zgodnego z wypracowanymi przez lata w krajach o ugruntowanej strukturze demokratycznej standardami. Koncentracja na działaniach systemowych, opartych na zapobieganiu i minimalizowaniu zagrożeń w tym obszarze, ma na celu skuteczne zapobieganie przypadkom ujawniania informacji niejawnych podmiotom do tego nieuprawnionym, a gdy do takiego przypadku dojdzie – na precyzyjne ustalenie osób za to odpowiedzialnych i uzupełnianie systemu o wnioski wynikające z wy-

krytych nieprawidłowości. Dostrzegalne w przestrzeni społecznej działania ABW w zakresie ochrony informacji niejawnych są realizowane w dwóch zasadniczych obszarach: nadzorze nad systemem ochrony informacji niejawnych, który realizowany jest przez funkcjonariuszy Departamentu Ochrony Informacji Niejawnych oraz Wydziałów Ochrony Informacji Niejawnych w Delegaturach ABW i w bezpieczeństwie teleinformatycznym, które to zadania realizuje Departament Bezpieczeństwa Teleinformatycznego.

W ramach współpracy międzynarodowej Polska musi zapewnić jednolity stopień bezpieczeństwa informacji klasyfikowanych, które są wymieniane z zagranicznymi partnerami. Taką gwarancję dają umowy dwustronne oraz regulacje organizacji międzynarodowych, których Polska jest członkiem. Od dnia 2 stycznia 2011 r. Ssef ABW pełni funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych, tzn. odpowiada za wdrażanie uzgodnionych zasad i środków ochrony informacji niejawnych. W sferze wojskowej funkcję tę szef ABW pełni za pośrednictwem szefa SKW.

Podstawowe zadania SKW określa artykuł 5 ustawy o SKW i SWW. Zaliczyć do nich należy²³⁶:

- przeciwdziałanie przestępstwom,
- realizowanie zadań z zakresu ochrony informacji niejawnych z zakresu swoich właściwości,
- ochrona jednostek MON poza granicami kraju,
- analizowanie i zwalczanie zagrożeń,
- ochrona badań naukowych zleczanych przez SZ RP.

Zgodnie z art. 10. 1. Ustawy o ochronie informacji niejawnych ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ust. 2 i 3:

- prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie,
- realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
- prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego,
- zapewniają ochronę informacji niejawnych wymienianych między Rzeczypospolitą Polską a innymi państwami lub organizacjami międzynarodowymi,
- prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

SKW realizuje zadania w odniesieniu do:

- Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,

²³⁶ Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, art. 5 ust. 1.

- ataszatów obrony w placówkach zagranicznych,
- żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1 i 2.

ABW realizuje zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie.

Podsumowaniem prawnych uwarunkowań systemu bezpieczeństwa informacji niejawnych może być stwierdzenie S. Zalewskiego: „ochrona informacji niejawnych jest to w ujęciu instytucjonalnym, grupa organów państwa oraz instytucji publicznych i niepublicznych wzajemnie powiązanych według kryterium występowania informacji niejawnych oraz obowiązków nałożonych nań z tego tytułu przez przepisy prawa. System ochrony informacji niejawnych można rozumieć, jako zespół środków prawnych regulacji wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych”²³⁷.

Odpowiedzialność prawna za naruszenie przepisów o ochronie informacji niejawnych

Naruszenie przepisów zapewniających ochronę informacji niejawnych niesie za sobą poważne konsekwencje. Akty prawne regulują zasady odpowiedzialności karnej, służbowej lub dyscyplinarnej względem osób zatrudnionych w poszczególnych jednostkach. Mówiąc o odpowiedzialności za ujawnienie informacji niejawnych, warto przypomnieć, iż ustawodawca zawarł w ustawie zasady, których bezprawne ujawnienie mogłoby spowodować szkody dla RP albo być niekorzystne dla jej interesów. Niemniej jednak obowiązująca ustawa nie uwzględnia regulacji karnych, które dotyczą nieprzestrzegania ochrony informacji niejawnych, ponieważ są one zawarte w przepisach kodeksu karnego. Rozdział XXXIII „Przestępstwa przeciwko ochronie informacji”, wskazuje na przewinienia dotyczące tych kwestii. Osoby pełniące funkcje z zakresu ochrony informacji niejawnych, upoważnione są do zwrócenia szczególnej uwagi na zapisy o odpowiedzialności karnej i dyscyplinarnej, gdyż z racji pełnionego stanowiska mogą uczestniczyć w tych procesach. Najistotniejsze przestępstwa związane z ochroną informacji niejawnych są opisane w art. 265 i 266 Kodeksu Karnego. Zgodnie z tym artykułem osoba, która ujawni informacje niejawne oznaczone klauzulą „tajne”, bądź „ściśle tajne” lub też wykorzysta je niezgodnie z prawem, ponosi karę pozbawienia wolności (więzienia) od 3 miesięcy do 5 lat. Ważne jest również to, że pomimo tego, czy osoba ta dysponowała informacjami podlegającymi ochronie z racji pełnionych obowiązków, czy też przypadkowo miała je w posiadaniu, obowiązuje ją bezwzględne zachowanie tajemnicy. Co więcej, kolejny artykuł mówi o tej samej

²³⁷ S. Zalewski, *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009, s. 38-39.

sprawie – ujawnieniu tajemnicy, lecz odnoszącej się do osób pełniących określone funkcje, bądź wykonujących zawód:

- § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narażać na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.
- § 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego. Warty podkreślenia wydaje się również art. 267 KK, który formułuje konsekwencje jakie niesie za sobą bezprawne pozyskanie wiadomości czy też treści pisma z systemu telekomunikacyjnego albo wykorzystanie urządzenia w celu zdobycia takich informacji. Przestępstwo powyższe można popełnić tylko umyślnie²³⁸.

Odminną rangę przestępstw stanowi art. 269 KK, mówiący o uszkodzeniu, usuwaniu, zmienianiu informacji, mających istotny wpływ na bezpieczeństwo kraju, czy np. funkcjonowanie administracji państwowej. Znaczenie tego jednoznacznie akcentują słowa „kara za ww. przestępstwa jest najwyższa, bo górna granica pozbawienia wolności wynosi w takich przypadkach 8 lat”²³⁹. W dzisiejszych czasach coraz większy wydźwięk nabierają oszustwa technologiczne, a w dużej mierze komputerowe. Na ich temat również zawarto wzmiankę w oddzielnym artykule KK (art. 287). Oprócz tego, jak dostrzega A. Jędruszczak „przepisy karne dotyczące naruszania przepisów o ochronie informacji niejawnych zawarte są również w ustawie o ochronie danych osobowych – dotyczą one ujawnienia informacji zawierających dane osobowe”²⁴⁰. Potwierdza te słowa artykuł z ww. ustawy, który brzmi²⁴¹:

- 1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym,

²³⁸ R. Stefański (red.) *Komentarz online do Kodeksu karnego*, C.H. Beck 2012.

²³⁹ B. Nowakowski, A. Jędruszczak, A. Gałach *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, C.H. Beck 2013 s. 236.

²⁴⁰ Tamże, s. 237.

²⁴¹ Ustawa z dnia 29 sierpnia 1997 ..., cyt. wyd., art. 49.

sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Warte uwagi są stwierdzenia wspomnianej powyżej autorki, która uważa, że „odpowiedzialność karna jest najbardziej dotkliwym skutkiem naruszenia przepisów dotyczących ochrony informacji, w tym niejawnych. Poza ww. odpowiedzialnością w polskim systemie prawnym przewidziane są również inne skutki naruszenia przepisów o ochronie informacji”²⁴².

Zwrócono już uwagę na odpowiedzialność karną, jaka obowiązuje w stosunku do osób ujawniających informacje chronione. Stąd też warty uwagi jest inny rodzaj odpowiedzialności tzn. odpowiedzialność służbowa. W tej kwestii najszerze uregulowania mieszczą się w ustawie z 26.6.1974 r. – Kodeks pracy²⁴³. Z jednego z przepisów KP wynika, iż „pracownik jest obowiązany w szczególności (...) 4) dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę, 5) przestrzegać tajemnicy określonej w odrębnych przepisach”²⁴⁴. Szczególnie punkt 5 ww. przepisu warto rozważyć ze względu na to, że obejmuje on swym zasięgiem wszystkie tajemnice chronione przez prawo, nie tylko służbową, bądź państwową. Nieprzestrzeganie zalecanych zobowiązań niesie za sobą poważne konsekwencje, a co za tym idzie, nawet rozwiązanie umowy o pracę z pracownikiem. Wypełnianie podanych obowiązków przez zatrudnionego, który ma świadomość ponoszenia odpowiedzialności za nie jest podstawą wykonywanych przez niego zajęć.

Istnieją także inne akty normatywne, w których są zapisy dotyczące regulacji przestrzegania tajemnicy państwowej i służbowej, odnoszące się do wykonywanego zawodu, czy np. stosunku do pracy. Są to takie akty, jak np.: Ustawa o służbie cywilnej z 21.11.2008²⁴⁵ i jej zapis mówiący o obowiązku dochowania tajemnicy chronionej ustawowo, spoczywającym na członku korpusu służby cywilnej. Za jej naruszenie może być on wydany ze służby, bądź w mniejszym stopniu odpowiadać dyscyplinarnie za swoje czyny. Regulacje prawne w stosunku do pracowników samorządowych również posiadają taki zapis w ustawie jak podano powyżej. Zobowiązania w kwestii przestrzegania tajemnicy państwowej i służbowej ujęte również zostały w niektórych przyrzeczeniach funkcjonariuszy służb mundurowych. Jak dostrzega A. Jędruszczak „osoby na stanowiskach kierowniczych, odpowiedzialne za funkcjonowanie systemu ochrony informacji niejawnych w jednostce organizacyjnej, w tym samorządu terytorialnego, w przypadku stwierdzenia naruszeń przepisów o ochronie informacji, posiadają różnorodne instrumenty prawne i dyscyplinarne dotyczące skutków działania lub zaniechania wbrew przepisom o ochronie informacji”²⁴⁶.

²⁴² B. Nowakowski, *Ochrona danych osobowych...* cyt. wyd., s. 237.

²⁴³ Ustawa z 26.czerwca.1974 r. – Kodeks pracy (Dz. z 1994 r. Nr 24, poz. 141).

²⁴⁴ Kodeks pracy, art. 100 §2.

²⁴⁵ Ustawa z dnia 21 listopada 2008 r. o służbie cywilnej (Dz.U. 2008 nr 227 poz. 1505).

²⁴⁶ A. Jędruszczak, *Odpowiedzialność za naruszenie przepisów o ochronie informacji niejawnych*, (w.) B. Nowakowski,

Reasumując ten problem rozstrzygającą tezą jest ta, która mówi, że „prawo karne penalizuje ujawnianie osobom nieuprawnionym informacji niejawnych stanowiących tajemnicę państwową, służbową i zawodową oraz inne czyny godzące w ich ochronę. Jednakże przedmiotem ochrony prawno-karnej nie jest sama tajemnica, lecz ważne interesy polityczne lub gospodarcze państwa, albo inne prawnie chronione interesy”²⁴⁷.

Informacje niejawne we współczesnym świecie

Kwestie dotyczące bezpieczeństwa państwa nie mogą być rozpatrywane bez odniesienia się do informacji i procesów informacyjnych obejmujących obszar decydowania o sprawach i interesie publicznym. „Informacją w szerokim ujęciu nazywa się treść zaczerpniętą ze świata zewnętrznego, w procesie naszego dostosowania się do niego i przystosowania naszych zamysłów. Informacją w tym znaczeniu jest nie tylko wiadomość o czymś, ale także każda decyzja, zakaz, sugestia czy polecenie. Takie ujęcie informacji zakłada, że może być ona przekazywana w układzie człowiek – człowiek”²⁴⁸, ale także w innych systemach, w których funkcjonuje. „Role nadawcy i odbiorcy mogą pełnić istoty żywe, maszyny lub inne obiekty”²⁴⁹. Polityka zaś jest sposobem rządzenia państwem, a bezpieczeństwo państwa jest sprawą polityczną. Oczywistym jest więc fakt, że informacje o dużym znaczeniu dla polityki państwa, które spowodowałyby zagrożenie dla bezpieczeństwa, nie mogą zostać ujawnione i muszą być chronione. W dobie rozwoju profesjonalizacji i technicznego obszaru pozyskiwania i ochrony informacji, czynniki te nie są uwzględniane podczas projektowania systemów mających na celu strzeżenie tajemnic państwowych. „Ustępują przed wymogami tworzonych przez wyspecjalizowane struktury procedur opartych na względnie stałych normach prawa. Nawet jednak najdoskonalsze normy i rozwiązania techniczne, nie uwzględniają politycznej natury informacji niejawnych, nie są jednak dostateczną barierą ochronną. Funkcją informacji jest jej wykorzystanie. Zatem opisywane zjawiska przyjmują postać „naturalnego” wykorzystania przez władzę informacji do realizacji celów politycznych oraz innych, partykularnych i doraźnych, ale w konsekwencji mających również polityczny wymiar”²⁵⁰. W wielu krajach zaobserwowano częste przypadki ujawniania informacji niejawnych przez osoby, które posiadają do nich oficjalny dostęp, między innymi funkcjonariuszy publicznych.

Ochrona danych osobowych... cyt. wyd., s. 239.

²⁴⁷ Tamże, s. 102.

²⁴⁸ Informacja w wąskim znaczeniu jest natomiast wiadomością uzyskiwaną przez człowieka poprzez obserwację lub czynność umysłową, podlegającą przekazowi w układzie nadawca (człowiek) – odbiorca (człowiek). Pojęcie informacji ulega zatem w tym wypadku ograniczeniu zarówno co do treści, jak i układu odniesienia. H. Groniewski, *Koordinacja systemu zasilania w informacji*, „Przegląd Organizacji” 1990, nr 11, za: J. Czekaj, *Zarządzanie informacją jako funkcja przedsiębiorstwa* [w:] T. Borkowski, A. Marciniowski, A. Oherow – Urbaniec, *W kręgu zarządzania. Spojrzenie multidyscyplinarne*, Kraków 2000, s. 178.

²⁴⁹ Tamże, s. 178.

²⁵⁰ S. Zalewski, *Informacje niejawne*, cyt. wyd., s. 9.

Osoby te działają często w swoim interesie, bądź też na zlecenie organizacji niepaństwowych.

Powyższe stwierdzenia pozwalają na zidentyfikowanie istniejących napięć, tkwiących w działającym systemie ochronnym, dotyczących formalnego wzrostu znaczenia ochrony informacji niejawnych w państwie, a ich bezpośredniego odbioru, często wywołującego znaczne trudności osobom bezpośrednio odpowiedzialnym za ich ochronę.²⁵¹ Problem wymaga wnikliwej analizy ochrony informacji niejawnych we współczesnym świecie. Ważnym jest zatem uchwycenie powiązań między informacją utajnioną ze względu na interes państwa a sferą interesu politycznego narodu, funkcjonującego w warunkach zależności pomiędzy ekonomią a polityką. Jest to dylemat dotyczący zapewnienia ochrony informacji niejawnych w dynamicznie zmieniających się kryteriach funkcjonowania państwa jako podmiotu bezpieczeństwa. Priorytetem jest więc odpowiedź na pytanie dotyczące znaczenia informacji niejawnych we współczesnym świecie.²⁵²

Informacje niejawne traktuje się jako istotny instrument władzy politycznej. Istotą tego ujęcia jest postrzeganie ich jako środków wywierania wpływu w relacjach społecznych. Tajemnica od dawien dawna jest instrumentem służącym do sprawowania władzy przez jednego człowieka nad resztą społeczeństwa. Służy ona jednostce, ale i różnego rodzaju organizacjom.

Zwyczajowo sfera informacji niejawnych obejmuje zakres wartości uwarunkowanych z trwaniem i przetrwaniem państwa. Są to „integralność terytorialna, suwerenność i niepodległość, na straży których to wartości stoi siła zbrojna”²⁵³ – ostateczny instrument, po który może sięgnąć państwo, aby bronić swoich wartości. W tym obszarze również dostrzega się podstawy do zmian. Poszerzenie zakresu podmiotowego ochrony informacji niejawnych nie jest tożsame z minimalizacją niebezpieczeństwa utraty nad nimi kontroli. W sposób naturalny zwiększa możliwości wykorzystania tych informacji, nie tylko w sposób założony pierwotnie. Tajemnica jest zatem narzędziem polityki państwa, ale również działaniem skierowanym przeciwko niemu. Stosunki międzynarodowe ukazują rolę tajemnicy jako dobra pożądanego z punktu widzenia interesów podmiotów, co ma bezpośredni wpływ na znaczenie dla procesu zapewnienia równowagi w procesach kooperacji, rywalizacji i międzynarodowych konfliktów. Oczywiście odbiega to od przyjętego w przeszłych wiekach wzoru starcia niepodległych państw”.

Granica pomiędzy bezpieczeństwem wewnętrznym a zewnętrznym jest coraz to mniej rozpoznawalna i widoczna, można nawet mówić o jej zanikaniu. W sensie podmiotowym odnoszonym do państwa, wyraźnie wpływa to, na funkcjonowania obszaru instytucjonalnego bezpieczeństwa. Znaczenia nabierają natomiast poza-państwowe i międzynarodowe podmioty. Aczkolwiek wzrost ich znaczenia nie

²⁵¹ Tamże.

²⁵² S. Zalewski, *Dylematy ochrony ...*, cyt. wyd., s. 95.

²⁵³ S. Zalewski, *Informacje niejawne ...*, cyt. wyd., s. 14.

zagroza jeszcze państwu jako podstawowym formom kształtowania organizacji społeczeństwa. Jest tak ponieważ mimo utraty swej pozycji, to nadal państwo ustala sposób życia społecznego na swym obszarze, co za tym idzie dba o zapewnienie bezpieczeństwa obywateli. Wnioskiem jest więc to, że nie uległ zmianie cel istnienia państwa, a warunki w jakich się go osiąga.²⁵⁴ Dlatego konieczna jest spójność polityki podmiotu, jakim jest państwo w sytuacji, gdy jest ono zależne od otaczającego go otoczenia. Pomimo, iż pewna zależność od otoczenia powoduje trudności w realizowaniu pewnych celów, to można pokładać wiarę w gwarancje z strony sojuszników i członkostwa w UE, które daje czas na przystosowanie systemu bezpieczeństwa narodowego RP do wyzwań współczesnego świata.

Te wymagania są określane współcześnie poprzez znaczenie informacji, jako elementu wpływającego na zmiany społeczne. Uzasadnione zatem jest uznawanie bezpieczeństwa informacyjnego za jeden z fundamentalnych elementów podsystemu bezpieczeństwa narodowego. „Język współczesnego bezpieczeństwa informacyjnego nie obejmuje i nie odnosi się do kategorii względnych – łatwo dających się interpretować w sposób zróżnicowany znaczeniowo: jak interes narodowy, racja stanu, wartości demokratycznego społeczeństwa otwartego itp. Istnieje zatem potrzeba świadomego stosowania instrumentu, jakim jest zespół procedur ochrony informacji w warunkach niestabilnego otoczenia, upadku tradycyjnych wartości stanowiących o istocie racji pomiędzy obywatelem a państwem-patriotyzmu, czy też kryzysu zaufania obywatela do organów państwa (to wszak obowiązująca w Polsce norma konstytucyjna).”²⁵⁵

Po odniesieniach do sfery czysto politycznej działania systemu informacyjnego bezpieczeństwa państwa, koniecznym jest zwrócenie uwagi na walor porządkujący norm prawa i procedur na nich opartych. Wedle powszechnie obowiązującego prawa metodyka ma charakter rozbudowanego zespołu procedur, dzięki czemu ma być zachowany odpowiedni poziom ochrony przedmiotowych informacji.²⁵⁶ W Polsce przepisy te reguluje, jak wcześniej opisywano, ustawa o ochronie informacji niejawnych i rozporządzenia wydane na jej podstawie. Metodyka ta uznawana jest powszechnie za bardzo skuteczne narzędzie zarządzania zasobami informacyjnymi, które wymagają ochrony. Należy podkreślić, że nie tylko w odniesieniu do państwowych tajemnic. Zauważalne jest więc, iż ma ona charakter kompleksowy i obejmuje wszystkie istotne kwestie „od wytwarzania informacji (oraz nadanie stosownej klauzuli tajności) poprzez jej przekazanie uprawnionym odbiorcom do archiwizacji, bądź zniszczenia.”²⁵⁷ We wszystkich etapach istnienia dokumentu niejawnego system ten funkcjonuje tak, aby odpowiednia uprawniona osoba – kontroler – był w stanie stwierdzić, na jakiego rodzaju nośniku i w którym

²⁵⁴ Tamże, s. 15.

²⁵⁵ Tamże

²⁵⁶ S. Zalewski, *Bezpieczeństwo polityczne państwa, Studium funkcjonalności instytucji*, Wydawnictwo Akademii Podlaskiej, Siedlce 2010, s. 303.

²⁵⁷ Tamże, s. 303-304.

miejsu podmiotowa informacja się znajduje, kto miał do niej dostęp (czy tylko osoby do tego uprawnione, które posiadają odpowiednie poświadczenie bezpieczeństwa bądź wykonujące w ramach obowiązków służbowych zadania, do których niezbędna jest wiedza zawarta w dokumencie niejawnym).

Odpowiednio podobny zbiór zasad jakimi są integralność, dostępność i poufność zawierają międzynarodowe normy zajmujące się regulowaniem pewnych kwestii zarządzania informacją, krajowe prawo i normy. Podmioty w celu wykazania swoich określonych walorów, jako że chcą uchodzić za nowoczesne organizacje oparte na wiedzy, podkreślają ściśle i rzetelne przestrzeganie tych norm. Aktualnie chronienie (ochrona) zasobów informacyjnych, mających znaczenie dla bezpieczeństwa państwa, czy też prywatnego przedsiębiorstwa jest sferą praktyki, jak też polem badań naukowych. To właśnie informacja jest podstawą absolutnie każdej podstawowej działalności człowieka, który mając w zamiarze osiągnąć swoje cele jest zmuszony do rozpoznania zagrożeń i skutecznie im przeciwdziałać.²⁵⁸

Wartość procedur ochrony informacji niejawnych jest zatem bezsporna. Zarówno z punktu widzenia dobra chronionego, jakim jest żywotny interes bezpieczeństwa państwa, jak też bardziej instrumentalnego (uporządkowujący obieg informacji w instytucji w sposób zgodny z zasadami wiedzy niezbędnej).

Zapobieganie wszelkim zagrożeniom bezpieczeństwa narodowego – z perspektywy podmiotowej roli organu, jakim jest państwo – jest aktualnie osiąganе w warunkach wzrostu czynnika korelacji, czyli współzależności, bardzo wyraźne zauważanego w relacjach wspólnotowych i sojuszniczych. Oczywiście tego konsekwencją jest zwiększone znaczenie powiązań instytucjonalnych, jak i zmiany w procesach decyzyjnych, w konsekwencji czego wywoływana jest potrzeba ujednolicenia w zakresie komunikowania i odczytywania znaczeń, ale również instrumentów ochrony informacji niejawnych. Administrowanie informacją nabiera znaczenia zasadniczego. To właśnie te procesy skłaniają do tworzenia procedur i standardów bezpieczeństwa informacji przy zwiększającej się liczbie osób zaangażowanych w wymianę posiadanej wiedzy.²⁵⁹

Zakładamy więc z jednej strony wzrost znaczenia tematyki bezpieczeństwa informacji, wzmocnienie możliwości zaangażowania w procesy ochrony, ale również zwiększenia podatności ze strony zagrożeń asymetrycznych. To właśnie zagrożenia asymetryczne w odniesieniu do zagrożeń bezpieczeństwa państwa, bieżą ze strony często nie w pełni rozpoznawanych struktur przestępczych, np. o międzynarodowym pochodzeniu. Badania nad tymi właśnie procesami wyznaczać będą nowe kierunki myślenia nad zagrożeniami dla ochrony informacji niejawnych.

²⁵⁸ S. Zalewski, *Dylematy ...*, cyt. wyd., s.95.

²⁵⁹ Tamże.

Rozpatrywanie znaczenia informacji jako czynnika bezpieczeństwa, nie jest zabiegiem nowym. Informacje można uznać za składową każdej działalności ludzkiej. Jeśli odnieść to do określenia bezpieczeństwa państwa, można rozpoznać rolę informacji dla formowania postępowania podmiotu, zabiegającego o kreowanie pewnych warunków rozwoju i egzystencji. W takim ujęciu informacja jest czynnikiem sprawczym ewolucji w dziedzinie bezpieczeństwa.

Podstawową czynnością jest postrzeganie bezpieczeństwa państwa nie tylko jako stanu wolności od zagrożeń. Należy zwrócić uwagę na ujęcie dynamiczne, to znaczy takie, które obejmuje całokształt starań podejmowanych dla zagwarantowania bezpieczeństwa danego podmiotu. To właśnie w tym rozumieniu procesy informacyjne gwarantują bezpieczeństwo państwa. Pozyskiwane informacje są przetwarzane, a następnie archiwizowane i udostępniane dla odpowiednich organów państwa. Podczas tych wszystkich wyżej wymienionych procesów widoczna jest konieczność zagwarantowania ochrony źródeł informacyjnych, ponieważ ich ujawnienie może zagrozić bezpieczeństwu państwa. Ocena kryteriów tajności informacji nie jest mimo wysiłków ustawodawców dość jasna i klarowna. Pozostawiają one w pełnomocnictwie decyzyjnym organów rządowych, przez to narażane są one na wpływ aktualnie kreowanej polityki. Pomijając wpływ polityki zawsze jednak znajduje się ważna część obywatelskiego systemu komunikowania i to właśnie w tym aspekcie zauważalne są wpływy rewolucji informacyjnej.²⁶⁰

Współcześnie warunki, w jakich państwo zarządza ochroną kluczowych z punktu widzenia bezpieczeństwa zasobów informacyjnych, posiadają obiektywny charakter i w dużej mierze pozostają poza zasięgiem narodowych rządów i podporządkowanych im służb.²⁶¹ Rewolucja informacyjna spowodowała, że społeczeństwa demokratyczne swoje szanse rozwoju upatrywać zaczynają bardziej w obszarze powszechnej wymiany informacji, a nie jej utajnienia. Problematyczność zjawisk, jakie zachodzą w sferach procesów decyzyjnych oraz ich poziomy w zależności, czy są one na poziomie państwa czy organizacji międzynarodowej – sprawiają, iż niemożliwym staje się pojedynczej jednostce skutecznie wpływać na rozwój sytuacji. Stwarza to konkretne konsekwencje społeczne, które ujmować można zarazem w kategoriach negatywnych, powiązanych z zwiększającym się syndromem biurokratyzacji obszaru zarządzania częścią problemów publicznych. Ale i pozytywnych, jako instrumentu wspomagającego kierowanie współczesnych organizacji min. administracją publiczną.

Odnosząc to do praktyk postępowania prowadzonych na podstawie ustawy o ochronie informacji niejawnych, w tym pierwszym ujęciu zauważalne jest niebezpieczeństwo przewagi czynników oficjalnych procedur nad przedmiotem decyzyjnym. „Owa formalizacja w omawianym aspekcie może rodzić zjawisko „wykorzystywania” tajemnicy przeciwko obywatelowi przez państwo. Tam, gdzie

²⁶⁰ S. Zalewski, *Informacje niejawne ...*, cyt. wyd., s. 19.

²⁶¹ S. Zalewski, *Dylematy ...*, cyt. wyd., s. 98-99.

z mocy przepisów prawa powszechnie obowiązującego, utajnia się przed obywatelami informacje dotyczące działań organów państwa, dochodzić może do naruszeń do naruszeń praw i wolności.”²⁶² Tworzy to pokusę obejmowania czynnościami ochrony informacji niejawnych coraz większego obszaru spraw, ale i zatracenia granicy pomiędzy tym, co istotne i wymagającego ochrony, a zagadnieniami nie wymagającymi ochrony, które powiększą koszt ochrony tajemnic. Pomimo dużego znaczenia, które formalnie przypisuje się ochronie informacji ważnych z perspektywy bezpieczeństwa państwa, w praktyce administracja problematykę tą często marginalizuje.²⁶³

Kolejne pozytywne ujęcie, widoczne jest w konsekwentnej proceduralizacji działań organów państwowych. Funkcjonującego w realiach społeczeństwa informacyjnego to znaczy opartego na wiedzy, propagowaniu metodyki ochrony informacji niejawnych prowadzi do skutecznej ochrony innych informacji prawnie chronionych. Podobne rozwiązania wprowadza się do ochrony danych osobowych w urzędach publicznych, co zwiększa poczucie bezpieczeństwa obywateli. Standaryzacja umożliwia dokonanie oceny działania systemu ochrony informacji, co jest niezbędne w celu usprawnienia jego funkcjonowania. Niewątpliwie wzrasta również zaufanie do instytucji, w których naruszenie zasad integralności, poufności i dostępności są incydentem niż normą.²⁶⁴

Podsumowując, rolę informacji niejawnych z perspektywy władzy politycznej, można scharakteryzować przez pryzmat interesów jednostkowych, jak i zbiorowych. Odnosząc to do jednostki uznaje się niejawną sferę jako atrakcję, co za tym idzie rzadkie i pożądane dobro, do którego dostęp posiadają tylko nieliczni. To powoduje pewnego rodzaju integrację ludzi posiadających ten dostęp i w dalszej mierze powoduje zespolenie całej organizacji. Rozwój ochrony informacji niejawnych jest zatem niezbędny w celu zapewnienia bezpieczeństwa państwa, a standaryzacja przepisów sprzyja ościąganiu tego celu. W realizacji tego celu niezbędne jest rzetelne i fachowe szkolenie kadr dla państwowego i pozapaństwowego sektora bezpieczeństwa oraz monitorowanie zagrożeń poprzez, m. in. sprawowanie konstruktywnego nadzoru w celu eliminowania nieprawidłowości i uszczelniania systemu.

Bibliografia

1. Iwaszko B. *Ochrona informacji niejawnych w praktyce*, Wrocław 2012.
2. Jabłoński M., Radziszewski T., *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012.
3. Nowakowski B., Jędruszczak A., Gałach A., *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, C.H. Beck 2013.

²⁶² S. Zalewski, *Informacje niejawne ...*, dz. cyt., s. 20.

²⁶³ Tamże

²⁶⁴ Tamże, s. 21.

4. *Ochrona informacji niejawnych teoria i praktyka*, (red) M. Kubiak, S. Topolewski, Siedlce 2013.
5. *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, (red) S. Topolewski, P. Żarkowski, Siedlce 2014.
6. Stankowska I., *Ustaw o ochronie informacji niejawnych. Komentarz*, Warszawa 2011.
7. Stefański R., (red.) *Komentarz online do Kodeksu karnego*, C.H. Beck 2012.
8. Zalewski S., *Bezpieczeństwo polityczne państwa, Studium funkcjonalności instytucji*, Wydawnictwo Akademii Podlaskiej, Siedlce 2010.
9. Zalewski S., *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009.
10. Zalewski S., *Informacje niejawne we współczesnym państwie*, Siedlce (w:) *Ochrona informacji niejawnych teoria i praktyka*, (red). M. Kubiak, S. Topolewski, Siedlce 2013.

Akty prawne

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
2. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007.
3. Ustawa o ochronie informacji niejawnych z dnia 5. sierpnia. 2010 r., (Dz.U. z 2010 r. Nr 182, poz. 1228).
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 nr 133 poz. 883).
5. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.
6. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.
7. Ustawa z 26.czerwca.1974 r. – Kodeks pracy (Dz. z 1994 r. Nr 24, poz. 141).
8. Ustawa z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. 2008 nr 227 poz. 1505).

Liczba znaków ze spacjami: 49785

Informacje o autorze

dr Stanisław Topolewski

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

e-mail: stanislaw_topolewski@wp.pl