**Piotr Budzyń**

# Ochrona informacji w świetle krajowych aktów prawnych

Bezpieczeństwo : teoria i praktyka : czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 9/3, 13-26

2015

BEZPIECZEŃSTWO • 2015 nr 3 TEORIA I PRAKTYKA

**Piotr Budzyń***

# Ochrona informacji niejawnych w świetle krajowych aktów prawnych[1]

## Wprowadzenie

Bezpieczeństwo informacji niejawnych w ujęciu przedmiotowym stanowi wyspecjalizowaną sferę bezpieczeństwa informacyjnego, które jest jednym z elementów bezpieczeństwa narodowego. Z uwagi na złożony charakter analizowane zagadnienie ujmowane jest wieloaspektowo[2]. Znajduje to wyraz m.in. w *Strategii Bezpieczeństwa Narodowego RP* z 5 listopada 2014 roku (zastępującej z 2007 roku)[3]. Wśród zagrożeń, mających wpływ na funkcjonowanie państwa wprowadza ona problematykę ujawnienia bądź kradzieży informacji o charakterze niejawnym[4]. Obecnie informacja staje się usługą, a nawet pożądanym towarem. Specyfika działania poszczególnych wyspecjalizowanych instytucji rządowych, pozarządowych oraz podmiotów prywatnych jest nastawiona na szereg operacji przeprowadzanych na danych, szerzej na ich zdobywanie, ochronę oraz przetwarzanie. Rosnące znaczenie tej problematyki znalazło

* Student II roku SUM na kierunku Bezpieczeństwo Wewnętrzne, Wydziału Humanistycznego Uniwersytetu Pedagogicznego w Krakowie.

1 Artykuł powstał w oparciu o pracę podyplomową *Ochrona informacji niejawnych w rozumieniu poszczególnych aktów prawnych w kontekście krajowym* napisaną pod kierunkiem prof. nadzw. dra hab. Piotra Semkowa i obronioną na Wydziale Nauk Humanistycznych i Społecznych, specjalności: Ochrona danych osobowych i informacji niejawnych w stosunkach międzynarodowych, Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni.

2 Por. W. Kitler, *Bezpieczeństwo Narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 280–281.

3 *Strategia Bezpieczeństwa Narodowego Rzeczypospolite Polskiej*, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf [dostęp: 10.10.2015].

4 *Ibidem*, s. 25.

swój wyraz w przepisach prawa krajowego, wspólnotowego oraz międzynarodowego. W Polsce, w myśl przyjętej zasady hierarchicznego podporządkowania aktów prawnych, wzmianki o rozpatrywanym zjawisku można odnaleźć kolejno w konstytucji, ustawach i rozporządzeniach oraz w aktach prawa miejscowego. Ważność ochrony informacji wynika z jej bezpośredniego funkcjonowania we wszystkich sektorach życia społecznego (publicznego, prywatnego i NGO). Prowadzi to do uściślenia przepisów w postaci instrukcji i wytycznych wewnętrznych ukierunkowanych na działalność specjalistyczną.

## Przesłanki wolności informacji zawarte w ustawie zasadniczej

Konstytucja gwarantuje powszechny dostęp do informacji, jako fundamentu pozyskiwanej wiedzy w ramach tzw. edukacji obywatelskiej, do której zapewnienia zobligowane jest państwo. Determinantem tej treści jest rozdział II konstytucji zatytułowany *Wolności, prawa i obowiązki człowieka i obywatela.* Podjęcie jakiejkolwiek aktywności, działalności, czy sprzeciw społeczeństwa w ramach uprawnień zagwarantowanych przez procesy ustawodawcze poprzedzone jest informacją o działalności i procesie funkcjonowania poszczególnych gałęzi władzy publicznej. Według ustawy zasadniczej (artykułu 61.1.)

> 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[5].

Z zapisu wynika, że ustawodawca ma obowiązek udzielić osobom zainteresowanym odpowiedzi na wybrane zagadnienia. Jest on obowiązany poinformować o kierunkach rozwojowych i dotychczasowych dokonaniach. Ponadto jawnie publikuje treści w formie raportów czy sprawozdań w myśl koncepcji kontroli obywatelskiej

> procesu ingerencji w stanowione prawa (krajowego i lokalnego) oraz skutków wdrażania i działania regulacji prawnych oraz kontrolowanie różnych aspektów funkcjonowania administracji rządowej i samorządowej, podległych im funduszy i agencji, wymiaru sprawiedliwości, instytucji korzystających ze środków publicznych (np. uczelni wyższych, organizacji pozarządowych oraz innych instytucji, o ile ich działanie jest istotne z punktu widzenia dobra publicznego); podejmowanie działań zmierzających do eliminowania złych praktyk[6].

Przytoczone wyżej regulacje nie odnoszą się bezpośrednio do interesów państwa oraz powszechnego dostępu do informacji publicznej. Podejmują one jednak

[5] *Ibidem*.

[6] http://www.ngofund.org.pl/projekty/projekty-tematyczne/kontrola-obywatelska [dostęp: 4.05.2015].

kwestie związane z obywatelem i gwarantami przepisów oraz praktyk państwa prawnego w procesach związanych z działaniami przeprowadzanymi na poszczególnych danych. Artykuł 51 stanowi, że:

> 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym, 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa, 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa[7].

Poruszone zagadnienia dotyczą bezpośredniego interesu obywateli. Z socjologicznego punktu widzenia wprowadzony został podział na sferę publiczną i prywatną. Wyróżniono bezpośrednie interesy obywateli (jako treści rodzinne i intymne) oraz w pkt. 3 stworzono podwaliny aktu regulującego informację niejawną („ograniczenie tego prawa może określić ustawa”[8]).

## Klasyfikacja informacji niejawnych i sposoby nanoszenia klauzuli tajności

W myśl Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych – informacje niejawne to „informacje, 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”[9]. Obejmują one wszelkie operacje przeprowadzane na danych sklasyfikowanych jako niejawne w poszczególnych stadiach rozwojowych. Jednocześnie należy zwrócić uwagę na różnicę w stosunku do konstytucyjnej swobody dostępu do informacji. Forma utajnienia poszczególnych treści jest determinowana jedynie ochroną interesów Rzeczypospolitej i tworzona zgodnie z zasadami poszanowania praw ogółu oraz jednostki[10], w myśl reguł funkcjonowania państwa prawa oraz składowego i wielosektorowego systemu bezpieczeństwa.

Klasyfikowanie informacji niejawnych ujęto w rozdziale drugim ustawy. Począwszy od artykułu piątego uwzględnia on rozmiary szkód i zagrożenia wynikłe z nieuprawnionego ujawnienia treści informacyjnej. Kolejno w dokumentach ściśle tajnych zachodzą najpoważniejsze skutki (szkody) godzące w „niepodległość, suwerenność lub integralność; porządek konstytucyjny; sojusze lub pozycje międzynarodowe;

---

7 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 Nr 78 poz. 483, http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970780483 [dostęp: 10.10.2015].

8 *Ibidem*.

9 Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010 Nr 182 poz. 1228, http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228 [dostęp: 10.10.2015].

10 M. Jabłoński, T. Radziszewski, *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012, s. 19.

gotowość obronną"; poszczególne aspekty związane z funkcjonariuszami, specyfiką i czynnościami służbowymi[11]. Pierwsze z nich to interesy żywotne ujęte w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2014 r. Są one postrzegane w perspektywie długofalowej, jako nadrzędne w drabinie potrzeb państwa. Niepodległość i suwerenność rozumiane są jako zachowanie niezależności decyzyjnej i integralności, także w odniesieniu do roli odgrywanej na arenie międzynarodowej. Zachowanie porządku konstytucyjnego oraz sojuszy stanowi podstawę bezpieczeństwa wewnętrznego i narodowego (zewnętrznego) państwa. W związku z powyższym rola funkcjonariusza wynika ze specyfiki wykonywanych przez niego czynności o charakterze operacyjno-rozpoznawczym (o charakterze niejawnym), administracyjno-porządkowym oraz operacyjno-rozpoznawczym.

Charakter klauzuli *tajne* ustawodawca określił jako *poważna szkoda z* punktu widzenia państwa[12]. Specyfika ujawnienia

> uniemożliwi realizację zadań związanych z ochroną suwerenności i porządku konstytucyjnego; pogorszy stosunki międzynarodowe; zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych; utrudni wykonywanie czynności operacyjno-rozpoznawczych, zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości; przyniesie stratę znacznych rozmiarów w interesie ekonomicznym[13].

W tym przypadku następuje nastawienie na potencjalne skutki, czy efekty ujawnienia poszczególnych treści informacyjnych, odmiennie niż w klauzuli opisanej wyżej ze wskazaniem na zaistnienie straty. Odzwierciedlenie wartościuje realną, rzeczywistą i poważną szkodę[14]. W ostatnim podpunkcie skonkretyzowano oraz określono ważność strat ekonomicznych, które w przekonaniu autora winny znaleźć odniesienie w dokumentach *ściśle tajnych* z uwagi na współczesną rangę gospodarczą państw.

Informacje niejawne o klauzuli *poufne* w myśl zapisów ustawy powodują jedynie szkodę dla interesów Rzeczypospolitej Polskiej[15], w szczególności te, których ujawnienie:

> utrudni prowadzenie bieżącej polityki zagranicznej; utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych; zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli; utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów; utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości; zagrozi stabilności finansowego; wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej[16].

---

11 Ustawa z dnia 5 sierpnia 2010 r., art. 5.

12 *Ibidem*, rozd. 2.

13 *Ibidem*.

14 M. Jabłoński, T. Radziszewski, *op. cit*., s. 37.

15 Ustawa z dnia 5 sierpnia 2010 r., rozd. 2.

16 *Ibidem*.

Klasyfikacja informacji niejawnej o klauzuli *poufne* ujmuje ogólnikowo zagrożenia (prawdopodobieństwa) ujawnienia danych treści. Otwarte domniemania należy połączyć z konkretnymi przykładami i istotą notyfikacji oraz scharakteryzować specyfikę działania[17]. Istotę „zakłócenia porządku publicznego" odzwierciedla zaburzenie efektywności pracy Rady Ministrów bądź podmiotu wyspecjalizowanego jakim jest Policja.

Klasyfikacja *zastrzeżona* nadawana jest informacjom,

> jeżeli nie nadano im klauzuli wyższej, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania prawa i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej[18].

Poruszone kwestie w dużej mierze dotyczą charakteru wspomnianego aparatu bezpieczeństwa państwa (wewnętrznego i zewnętrznego). Uogólnienia spowodowane są możliwością dopasowania hipotetycznych sytuacji do tzw. stanu faktycznego i tak jak w powyższych przypadkach – należy rozpatrywać je indywidualnie.

Procedury związane z nanoszeniem klauzuli tajności informacji, sklasyfikowanych jako niejawne, reguluje opisywana Ustawa o ochronie informacji niejawnych, a uszczegółowia Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności. Terminem oznaczanie określa się

> czynność techniczną nanoszenia na materiał informacji określonych w rozporządzeniu, w tym umieszczania na nim klauzuli tajności, oraz nanoszenia informacji o zmianie lub zniesieniu nadanej klauzuli, a także umieszczania informacji w metryce dokumentu elektronicznego[19].

Za nadanie lub ewentualną zmianę klauzuli tajności odpowiedzialna jest osoba do tego uprawniona i upoważniona[20]. W przypadku braku ujednolicenia danych niejawnych, dla zasady nadaje się klauzulę najwyższą spośród wyodrębnionych oraz jasno określa granice poszczególnych materiałów z uwzględnieniem jawnych[21]. W myśl przepisów przyjęto następującą kategoryzację (symbolikę) informacyjną: *00* – dla klauzuli *ściśle tajne*; *0* – dla klauzuli *tajne*; *Pf* – dla klauzuli *poufne*; *Z* – dla klauzuli *zastrzeżone*[22]. Zgodnie z procedurą przetwarzania, dokumenty podzielono na elektroniczne i nieelektroniczne. Pierwsze z nich to dane zawarte w systemach teleinformatycznych, zapisane na poszczególnych nośnikach elektronicznych. Przekaz informacji niejawnych jest możliwy jedynie po uzyskaniu certyfikacji danego systemu. Dokumenty o specyfikacji nieelektronicznej to pozostałe treści utworzone najczęściej

---

17 M. Jabłoński, T. Radziszewski, *op. cit*., s. 40.

18 Ustawa z dnia 5 sierpnia 2010 r., rozd. 2.

19 Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności, Dz.U. 2011 Nr 288 poz. 1692, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112881692 [dostęp: 10.10.2015].

20 Ustawa z dnia 5 sierpnia 2010 r., rozd. 2.

21 M. Jabłoński, T. Radziszewski, *op. cit*., s. 137.

22 Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku.

w formie papierowej, podlegającej rejestracji w utworzonych certyfikowanych rejestrach (np. w dziennikach ewidencji wykonywanych). Dokładne wytyczne i instrukcje oznaczania dokumentacji niejawnych ujęte są we wspomnianym rozporządzeniu.

## Tryb tworzenia, praca i funkcje kancelarii tajnych

Wymienione akty prawne zobowiązują poszczególne jednostki organizacyjne do ochrony treści utajnionych. W tym celu ustawodawca normuje i wdraża kolejne zalecenia. Rozdział 7 Ustawy o ochronie informacji niejawnych z 2010 roku w art. 42 nakłada na kierownika jednostki organizacyjnej obowiązek utworzenia kancelarii tajnej w wypadku przetwarzania materiału niejawnego o klauzuli *tajne* lub *ściśle tajne*. Obowiązany jest on również do zatrudnienia, powołania odpowiednio jej kierownika[23]. Definiowana osoba prowadzi

> bezpośredni nadzór nad obiegiem materiałów; udostępnia materiały osobom do tego uprawnionym; wydaje materiały osobom uprawnionym, które zapewniają odpowiednie warunki ich przechowywania; egzekwuje zwroty materiałów; kontroluje przestrzeganie właściwego oznaczenia i rejestrowania materiałów w kancelarii oraz jednostce organizacyjnej; prowadzi nadzór nad pracą oddziałów kancelarii[24].

Każdorazowo po zakończeniu pracy kierownik lub osoba przez niego upoważniona jest zobowiązana sprawdzić prawidłowość poszczególnych zabezpieczeń fizycznych, w tym szaf ochronnych oraz pomieszczeń kancelaryjnych, wszelkie naruszenia i nieprawidłowości należy zgłaszać pełnomocnikowi ochrony[25]. Podczas zmiany na opisywanym stanowisku sporządza się protokół zdawczo – zbiorczy. Czynność przeprowadza się w obecności osoby przekazującej dotychczasowe obowiązki, osoby która ma owe zadania powziąć, pełnomocnika ochrony lub osoby przez niego pisemnie upoważnionej. Protokół sporządza się w dwóch egzemplarzach; pierwszy zostaje w kancelarii, a drugi przechowuje pełnomocnik[26]. Właściwa koordynacja pracy kancelarii tajnych opiera się na stosownym współdziałaniu osób tworzących całkowity pion ochrony. Opisywana komórka organizacyjna musi zostać wyodrębniona (ulokowana w odpowiedniej strefie ochronnej) oraz podległa powołanemu pełnomocnikowi ochrony. Specyfiką w przetwarzaniu informacji niejawnych jest możliwość ustanowienia nowych kancelarii (chociażby międzynarodowych), współudziału pojedynczych kancelarii w obsłudze kilku podmiotów organizacyjnych[27] oraz tworzenie jej oddziałów kierowanych przez osobę z pionu ochrony, którą wyznacza pełnomocnik ochrony[28]. O utworzeniu bądź likwidacji kancelarii kierownik jednostki informuje odpowiednio

[23] Ustawa z dnia 5 sierpnia 2010 r., rozd. 7.

[24] Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych, § 4, Dz.U. 2011 Nr 276 poz. 1631, http://isap.sejm.gov.pl/KeyWordServlet?viewName=thasK&passName=kancelaria%20tajna [dostęp: 10.10.2015].

[25] *Ibidem*, § 6.

[26] *Ibidem*, § 5.

[27] *Ibidem*, § 2.

[28] *Ibidem*.

Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego, wraz z przypisaniem klauzuli tajności (odpowiednio najwyższą spośród wyodrębnionych)[29].

Działanie kancelarii jest docelowo ukierunkowane na właściwe sposoby operacji dokonywane na informacjach niejawnych. Klasyfikując jest to bezpieczne rejestrowanie, wydawanie oraz przechowywanie materiałów. Zatem w kategoriach działań kancelarii tajnych wyodrębniono:

> rejestr dzienników ewidencji i teczek, dziennik ewidencyjny, książkę doręczeń przesyłek miejscowych, wykaz przesyłek nadanych, rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów[30].

Istnieje również możliwość utworzenia pomieszczenia określanego *czytelnią*, dla zapoznania się z przechowywanymi materiałami. Miejsce musi pozostać pod stałym nadzorem pracowników kancelarii, jednak bez użycia monitoringu wizyjnego[31]. Ewidencjonowanie materiałów może przebiegać drogą elektroniczną, co może przysporzyć wielu trudności związanych z normami niezaprzeczalności (w odniesieniu do uczestnictwa w procederze wymiany danych przez jeden z podmiotów uczestnictwa) oraz rozliczalności (działań wykonywanych przez podmiot i bezpośrednio jemu przypisanych) podczas odbioru treści niejawnych[32]. Wykorzystanie w tym celu środków technicznych, a zarazem organizacyjno-prawnych w postaci elektronicznego podpisu, w pełni uwiarygodni proces wysłania bądź odbioru treści niejawnych. Uwierzytelnienie podpisu musi spełniać ustawową *rangę bezpieczeństwa*, czyli winno być przypisane określonej osobie; sporządzenie podpisu należy wykonywać urządzeniami certyfikowanymi przeznaczonymi do tego celu, nad którą kontrolę zwierzchnią ma konkretna osoba; podpis jest przypisywany wraz z danymi „do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna”[33].

## Stosowanie środków bezpieczeństwa fizycznego w ochronie informacji niejawnych

W ustawie z 2010 roku o ochronie informacji niejawnej zawarto skumulowany rozdział o kancelarii tajnej oraz wdrażaniu środków bezpieczeństwa fizycznego[34]. Inicjowaniem wprowadzenia fizycznych zabezpieczeń jest, zdaniem autora, sam cykl tworzenia kancelarii jako wyspecjalizowanych, autonomicznych pomieszczeń przeznaczonych do kooperacji na danych niejawnych. Była to również podstawowa przesłanka podziału opisanych wyżej zagadnień dotyczących komórek kancelaryjnych

---

[29] Ustawa z dnia 5 sierpnia 2010 r., rozd. 7.

[30] Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku, § 2.

[31] *Ibidem*.

[32] M. Jabłoński, T. Radziszewski, *op. cit*., s. 131.

[33] Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym, art. 1, Dz.U. 2001 Nr 130 poz. 1450, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20011301450 [dostęp: 10.10.2015].

[34] Ustawa z dnia 5 sierpnia 2010 roku, rozd. 7.

(procesów tworzenia czy obsługi) oraz (w tej części) doboru odpowiednich środków bezpieczeństwa fizycznego.

Dobór zastosowania środków danego rodzaju uzależnia się od poziomu hipotetycznego wystąpienia potencjalnych zagrożeń związanych z niepożądanym i nieuprawnionym dostępem do chronionych dóbr.

Punktem wyjścia jest zdefiniowanie pojęć: ryzyka − jako rachunku prawdopodobieństwa zaistnienia poszczególnych zagrożeń oraz ich skutków; szacowania ryzyka − całościowej analizy zagrożeń wraz z ich obiektywną oceną; zarządzania ryzykiem − jako działań koordynacyjnych z wykorzystaniem dostępnych sił i środków[35]. Skonkretyzowanie potencjalnych zagrożeń przypisane zostało indywidualnie dla pomieszczenia bądź obszaru z uwzględnieniem poziomu: wysokiego, średniego lub niskiego. Ponadto ustawodawca przyjmuje podział zagrożeń na naturalne (związane z siłami natury) oraz związane z nieodpowiednią działalnością człowieka[36]. Wskazane byłoby rozgraniczenie podziału technicznego zawartego w pierwszej klasie, zważywszy na możliwość awarii chociażby infrastrukturalnej związanej z działaniem innych czynników.

Na bezpieczeństwo fizyczne w kontekście ochrony informacji niejawnych składa się szereg zorganizowanych, specjalistycznych podmiotów ściśle ze sobą powiązanych tworzących integralną całość. Mowa tu o skoordynowanych procedurach: osobowych, tworzących stały czynny nadzór nad informacjami; organizacyjno-prawnych, działających w ramach utworzonych rozwiązań o poszczególnych rangach, w granicach i ustanowionych normach prawnych oraz fizycznych, polegających na doborze certyfikowanych zabezpieczeń udaremniających bezpośredni dostęp do chronionych treści niejawnych.[37] System dozoru wizyjnego, wraz z systemem kontroli osób i przedmiotów, stanowi swoiste uzupełnienie całości ochrony fizycznej[38].

Istotnym zabezpieczeniem informacji niejawnych jest tworzenie stref ochronnych. Ustawodawca wyodrębnia:

– strefę ochronną I, w której informacje o klauzuli *poufne* lub wyższej, są przetwarzane w sposób bezpośredni, każdorazowy wstęp osoby skutkuje w dostępie do treści chronionej. Nakazuje określenie granicy strefy; wprowadza „system kontroli wejść i wyjść"; obliguje do nadzoru nad osobą nieuprawnioną poruszającą się w strefie; określa dostępność miejsca wyłącznie z innego obszaru chronionego;
– strefę ochronną II, w której występują podobne zasady przetwarzania danych z uwzględnieniem ich dostępności, lecz nie bezpośrednim po każdorazowym wejściu do obwodu chronionego;
– strefę ochronną III, która charakteryzuje się organizacją kontroli osób i pojazdów w jej granicach. Istnieje możliwość utworzenia tzw. ,,specjalnej strefy ochronnej chronionej przed podsłuchem", spełniającej wymogi: sygnalizacji włamania i napadu; obligatoryjnego zamknięcia podczas nieobecności pracowników; ochrony podczas posiedzenia o charakterze niejawnym; kontroli przeprowadzanej

[35] *Ibidem*, rozd. 1.

[36] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych, § 3, Dz.U. 2012 poz. 683, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000683 [dostęp: 10.10.2015].

[37] S. Topolewski, P. Żarkowski, *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, Siedlce 2014, s. 101.

[38] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 roku, § 4.

odpowiednio przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego; „bezwarunkowym brakiem ulokowania linii komunikacyjnych, telefonów, innych urządzeń komunikacyjnych ani sprzęt elektryczny lub elektroniczny, których umieszczenie nie zostało zaakceptowane w sposób określony w procedurach bezpieczeństwa". Pomieszczenia, w których praca nie odbywa się w systemie całodobowym winny być sprawdzane każdorazowo po zakończeniu pracy. Dodatkowo można tworzyć pomieszczenia wzmocnione (w praktyce pozwalające przechowywać informacje niejawne poza szafami ochronnymi)[39].

Zabezpieczenia fizyczno-elektroniczne (kody, klucze) dające dostęp do obszarów, w których przetwarzane są informacje niejawne, mogą być udostępniane osobom wyłącznie w celu wykonywania obowiązków służbowych. Należy je zmieniać każdorazowo w sytuacjach: zmiany kadry osób znających kod dostępu; realnego podejrzenia, że osoba nieuprawniona mogła powziąć kod; „zamek poddano konserwacji bądź naprawie"[40].

Opisywana procedura zmierza do utworzenia planu ochrony zatwierdzanego bezpośrednio przez kierownika jednostki organizacyjnej z uwzględnieniem wyodrębnionych zabezpieczeń fizycznych. Jej bieżąca ocena uzależniona będzie od zobligowania pełnomocnika do analizy przyszłych i ewoluujących zagrożeń.

Określone działanie ma na celu uniemożliwienie dostępu w szczególności wymierzone przeciwko: obcym służbom; „zamachom terrorystycznym lub sabotażom", chroniące przez „kradzieżą lub zniszczeniem materiału", nieuprawnionym wejściem w strefy ochronne przetwarzające treści niejawne; „dostępem do informacji o wyższej klauzuli" niż posiadane uprawnienia[41].

## Tryb i sposoby przemieszczania materiałów o charakterze niejawnym

Pojęcie ochrony informacji niejawnych charakteryzuje się wielowątkowością nieograniczoną jedynie do protekcji związanej z bezpośrednim znaczeniem tego słowa. W rozumieniu ustawowym to również szereg zabezpieczanych operacji wykonywanych na treściach utajnionych w świetle potencjalnych zagrożeń, do których należy m.in. przemieszczanie materiałów.

W rozdziale 7 Ustawy o ochronie informacji niejawnej z 2010 roku ustawodawca uwzględnia wydanie rozporządzenia Prezesa Rady Ministrów dotyczące: „trybu i sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów", postępowania nadawców, związanego z prawidłowym adresowaniem przesyłek (czynności techniczne) oraz wymogi obowiązujące przesyłki; postępowania przewoźników podejmujących przewóz informacji niejawnych; sposoby dokumentowania (czynności kancelaryjne), „przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom wraz z załącznikami wzorów formularzy; warunki ochrony, sposoby

39 *Ibidem,* § 5.

40 *Ibidem*.

41 Ustawa z dnia 5 sierpnia 2010 roku, rozd. 7.

zabezpieczenia przesyłek przez przewoźnika oraz warunki" należne do spełnienia w związku ze środkami transportu i uczestnikami konwoju; postępowania w zaistniałych okolicznościach mogących mieć bezpośredni wpływ na przesyłkę[42]. Zapisy te mają na celu zabezpieczenia treści niejawnych podczas czynności związanych z wymianą informacji.

Przepływ materiałów niejawnych dokonywany jest z pomocą określonych przewoźników, do których należą: *poczta specjalna* (lub wydział poczty specjalnej komórka organizacyjna Policji podległa ministrowi spraw wewnętrznych); „komórka organizacyjna urzędu obsługującego ministra właściwego do spraw zagranicznych, zapewniająca przewóz materiałów za granicę i poza granicami Rzeczypospolitej Polskiej pomiędzy urzędem obsługującym ministra właściwego do spraw zagranicznych i jednostkami organizacyjnymi podległymi lub nadzorowanymi przez tego ministra, zwanymi dalej «placówkami zagranicznymi»"; jednostki Ministerstwa Obrony Narodowej lub Służby Kontrwywiadu Wojskowego; „operatorzy pocztowi" (certyfikowani przedsiębiorcy w postaci podmiotów prywatnych); przedsiębiorcy, podmioty prywatne koncesjonowane w zakresie ochrony osób i mienia oraz w zakresie transportowym[43].

Z uwagi na kategoryzację tajności przewóz materiałów *ściśle tajnych* oraz *tajnych* następuje wyłącznie przez trzy pierwsze wymienione podmioty. Istnieje również wyjątek: kierownik jednostki organizacyjnej w formie decyzji może wydać zgodę na przewóz informacji niejawnych innym subiektem (np. ze względu na specjalny charakter przesyłki: rozmiar, wagę, wielkość)[44]. Przesyłka może być transportowana bez udziału przewoźnika, jeżeli przewozu podejmuje się nadawca lub adresat, a zabezpieczenie eliminuje ingerencję osób nieuprawnionych[45]. Nadawany materiał jest przygotowywany z uwzględnieniem wytycznych i instrukcji, zostaje ewidencjonowany w dzienniku przesyłek nadanych (z uwzględnieniem adnotacji załączników), po czym przekazany zostaje przewoźnikowi. Uwzględniając specyfikę warunków przewozowych osoba sprawdza go pod względem zabezpieczenia, wymiaru oraz zawartości. Następnie ustala sposób opakowania uniemożliwiający rozpoznanie przesyłki, swoistość ewentualnych substancji niebezpiecznych oraz sposób łączności[46]. Potwierdzenie przyjęcia lub odmowy przyjęcia przesyłki składa się w formie pisemnej, liczbowej, ustnej oraz nakłada stosowną pieczęć. Przesyłkę konwojuje się „środkami transportu publicznego lądowego" – z uwzględnieniem wydzielenia miejsca niedostępności osób nieuprawnionych, stałego dozoru konwojentów (w praktyce rzadko spotykana forma); „samochodem przewoźnika; statkami powietrznymi lub statkami transportu wodnego"[47].

O przewozie przesyłek o klauzuli *ściśle tajne*, *tajne* powiadamia się kolejno Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego[48], np. w celu

42 *Ibidem*.

43 Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne, § 2, Dz.U.2011.271.1603, http://www.abc.com.pl/du-akt/-/akt/dz-u-2011-271-1603 [dostęp: 10.10.2015].

44 M. Jabłoński, T. Radziszewski, *op. cit.*, s. 147.

45 Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 roku, § 5.

46 *Ibidem*.

47 *Ibidem*.

48 *Ibidem*.

podglądu procesu transportu przy użyciu systemów teleinformatycznych. Ponadto przepisy o przewozie uwzględniają klauzulę dokumentów niejawnych. *Ściśle tajne* są ochranianie przez

> co najmniej dwóch uzbrojonych w broń palną konwojentów, posiadających odpowiednie poświadczenie bezpieczeństwa, przesyłkę o klauzuli „tajne" ochrania co najmniej jeden konwojent [ze specyfiką opisaną wyżej] oraz klauzulę zawierającą informacje niejawne o klauzuli „poufne" lub „zastrzeżone" przewozi i ochrania co najmniej jeden konwojent posiadający odpowiednie poświadczenie bezpieczeństwa lub upoważnienie[49].

Odbiorca jest obowiązany okazać dokument uprawniający do odbioru przesyłki oraz wspólnie z przewoźnikiem sprawdzić stan przesyłki. „W przypadku uszkodzenia przesyłki lub stwierdzenia śladów jej otwierania przewoźnik" wręcza odbiorcy protokół [50]. Następnie powinien ją przekazać i zarejestrować w kancelarii tajnej, ewidencjonując przyjęcie pokwitowaniem i odciskiem pieczęci właściwej jednostki organizacyjnej[51].

Ostatecznie przesyłka trafia do adresata, którym w kontekście ustawowym mogą być:

> Sejm i Senat; Prezydent Rzeczypospolitej Polskiej; organ administracji rządowej; organy jednostki samorządu terytorialnego a także inne podległe mu jednostki organizacyjne lub przez nie nadzorowane; sady i trybunały; organy kontroli państwowej i ochrony państwa[52].

## Funkcjonowanie Krajowej Władzy Bezpieczeństwa

*Strategia Bezpieczeństwa Narodowego* z 2014 roku podkreśla istotę znaczenia ochrony informacji niejawnych z uwzględnieniem roli Krajowej Władzy Bezpieczeństwa, która ustawowo podlega szefowi Agencji Bezpieczeństwa Wewnętrznego. Jednak w odniesieniu do strefy wojskowej współdziała on z szefem Służby Kontrwywiadu Wojskowego[53]. O ile priorytetem procedur wykonywanych przez zdefiniowany podmiot jest szeroko rozumiany kontekst międzynarodowy, o tyle współdziałanie w sferze wojskowej i cywilnej opiera się na konsensusie i dwustronnym porozumieniu.

W rozumieniu ustawy do zadań pokrywających kompetencje naczelnych organów kontrolnych treści niejawnej w kontekście krajowym należy: prowadzanie kontroli właściwej ochrony informacji niejawnej w świetle obowiązujących przepisów; pełnienie zadań związanych z systemami teleinformatycznymi (uwzględniającymi głównie sposób funkcjonowania ochrony czy akredytacje); prowadzanie postępowań sprawdzających, kontrolnych postępowań sprawdzających, weryfikujących proces

[49] *Ibidem*, § 12.

[50] *Ibidem*.

[51] *Ibidem*.

[52] Ustawa z dnia 5 sierpnia 2010 roku, rozd. I.

[53] *Ibidem*, art. 10.

rękojmi zachowania tajemnicy oraz postępowań bezpieczeństwa przemysłowego w odniesieniu do przedsiębiorców; prowadzenie wielopłaszczyznowego doradztwa oraz szkoleń w rozumieniu ochrony informacji niejawnych. W świetle kontroli stanu zabezpieczeń ustawodawca uwzględnia uprawnienia funkcjonariuszy do: „wstępu do obiektów i pomieszczeń kontrolowanych", wezwania do udostępnienia dokumentów sprawdzanych; dostępu do systemów teleinformatycznych; oględzin obiektów, elementów majątkowych oraz czynności związanych z treściami niejawnymi; „żądanie od kierowników i pracowników ustnych i pisemnych wyjaśnień; zasięgania w związku z przeprowadzoną kontrolą informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych oraz żądania wyjaśnień od kierowników i pracowników jednostek"; korzystania z ekspertyz, doradztwa biegłych w okolicznościach stwierdzenia ujawnienia treści; funkcji opiniodawczo-doradczej oraz „uczestnictwa w posiedzeniach kierownictwa organów zarządzających lub doradczych"[54].

## Sankcje związane z bezprawnymi operacjami na informacjach niejawnych

Ochrona informacji niejawnych interpretowana jest w związku z konstytucyjnymi zapisami o „obowiązku wierności Rzeczypospolitej Polskiej oraz trosce o dobro wspólne" (art. 82) oraz „obowiązku przestrzegania prawa" (art. 83). Wiernością wobec państwa będą zatem przesłanki zawarte w *Strategii Bezpieczeństwa Narodowego* z 2014 roku dotyczące osłony kontrwywiadowczej czyli „profilaktyki związanej z ochroną informacji niejawnych"[55], a przestrzeganiem prawa chociażby ochrona danych.

Ustawodawca podzielił odpowiedzialność za naruszenia na odpowiedzialność wynikającą z ustawy o ochronie informacji niejawnych, dyscyplinarną oraz usankcjonowaną karnie[56]. W pierwszym przypadku nie ma stosownych unormowań co do rozmiaru kary. Ujęte zostały przepisy instruktażowe dotyczące tzw. postępowania sprawdzającego oraz kontrolnego postępowania sprawdzającego. Postępowanie sprawdzające jest procesem weryfikacji osoby pod kątem rękojmi zachowania tajemnicy[57]. Ustawodawca już w tej fazie (art. 24 ust. 2) używa określenia „istnienia uzasadnionych wątpliwości" oraz kolejno wymienia przykłady zmierzające do odmowy udzielenia dostępu, a nawet innej odpowiedzialności. Kontrolne postępowanie sprawdzające wszczyna się „w przypadku gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy". Jeżeli podczas prowadzonej weryfikacji w rzetelny sposób udowodni się osobie niewłaściwą pracę z informacjami o charakterze niejawnym, rzutować to będzie na brak możliwości awansu, a nawet wydalenie, zwolnienie ze służby lub odsunięcie od pełnionych obowiązków. Ponadto osoba,

[54] *Ibidem.*

[55] *Strategia Bezpieczeństwa Narodowego Rzeczypospolite Polskiej*, *op. cit*., punkt 82.

[56] B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, Wrocław 2012, s. 205.

[57] Ustawa z dnia 5 sierpnia 2010 r., art. 24.

wobec której toczy się opisywana procedura, nie może pełnić stanowiska związanego z dostępem do treści niejawnych, czy przebywać w określonych strefach ochronnych.

Odpowiedzialność o charakterze dyscyplinarnym (bądź zależnie od charakteru pracy służbowym) ponoszą pracownicy w związku z uwarunkowaniami określonymi w poszczególnych przepisach prawnych. Specyfika dyscyplinarna dotyczy unormowań swoistości pracy zawartych w kodeksie pracy oraz innych związanych z wykonywaniem konkretnego zawodu. Czynnikiem warunkującym opisywaną procedurę jest pozyskanie pracownika stosownym nawiązaniem pracy czyli aktem nominacyjnym. Chodzi tu o grupę, do której zalicza się: żołnierzy zawodowych, urzędników państwowych, innych funkcjonariuszy mundurowych, sędziów, prokuratorów, pracowników organów kontroli państwowej, urzędników rządowych i samorządowych oraz członków korpusu służby cywilnej. Właściwymi organami orzekającymi o rodzaju odpowiedzialności, zgodnie z obowiązującymi przepisami, będą kolejno: rzecznicy lub komisje dyscyplinarne działające w systemie dwuinstancyjności (z możliwością odwołania niesatysfakcjonujących decyzji). W procesie decyzyjnym postanowieniami są: upomnienie, nagana (z wpisem lub bez adnotacji do akt), degradacja (najczęściej niższe stanowisko), obniżenie rangi urzędniczej (odebranie częściowych uprawnień), wydalenie bądź zwolnienie. Odpowiedzialność o charakterze służbowym ponoszą pracownicy w związku z kodeksem pracy oraz wytycznymi, instrukcjami przyjętymi w danym podmiocie zatrudnienia[58]. W odróżnieniu od postępowania dyscyplinarnego pracownik ponosi odpowiedzialność bezpośrednio przed przełożonym. Typy odpowiedzialności można łączyć z unormowaniami karnymi.

Ustawa z dnia 6 czerwca 1997 roku Kodeks karny[59] reguluje omawiane zagadnienie w rozdziale XXXIII, zatytułowanym *Przestępstwa przeciwko ochronie informacji*[60], wyróżniając te popełnione przeciwko treściom niejawnym. Ustawa, jako przepis sankcyjno-prawny, samoistnie normuje jedynie zachowania karalne i nie może stanowić podstawy samej w sobie, musi współdziałać z ustawą o ochronie informacji niejawnej celowością rozszerzenia[61]. Artykuł 265 w paragrafie pierwszym mówi ogólnikowo o ujawnieniu informacji niejawnych o klauzuli *tajne* lub *ściśle tajne*. Wyjawnienie, to zachowanie polegające na upublicznieniu[62], okazaniu treści nieznanych osobie – „nie dającej rękojmi zaufania".

Klasyfikacja czynu, uwzględniona w paragrafie drugim, zaostrza wymiar kary oraz zmierza do zabiegu kumulatywnego czynów z przestępstwem szpiegostwa (art. 130 Kodeksu karnego). Paragraf trzeci przedstawia nieumyślność ujawnienia danych, powstałych w skutek np. przestępstwa zaniechania, w typologii uprzywilejowanej (łagodzącej wymiar kary). Artykuł 266 wskazuje na indywidualizm przestępstwa. Oznacza to, że jedynie konkretna osoba może popełnić dane przestępstwo, w tym przypadku ta, która powzięła informację o treści niejawnej w związku z „pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną gospodarczą, naukową"[63]. Kwa-

---

58 B. Iwaszko, *op. cit*., s. 207.

59 Ustawa z dnia 6 czerwca 1997 roku Kodeks karny, http://kodeksy.net/index.php/kodeks-karny.html [dostęp: 4.05.2015].

60 *Ibidem*, s. 115.

61 S. Topolewski, P. Żarkowski, *op. cit.*, s. 206.

62 *Ibidem*, s. 207.

63 Ustawa z dnia 6 czerwca 1997 roku Kodeks karny, art. 265.

lifikacja, uwzględniona w paragrafie drugim, zaostrza wymiar kary z uwzględnieniem popełnienia przestępstwa przez „funkcjonariusza, który uzyskał informację w związku z wykonywaniem czynności służbowych”[64].

## Podsumowanie

Wykreowanie tzw. towaru informacyjnego stało się poważnym zagrożeniem dla treści chronionych. Świadczy o tym chociażby wprowadzanie przez ustawodawcę ciągle udoskonalanych form zapobiegania nieuprawnionemu dostępowi do informacji. Kontekst niejawny jest szczególnie atrakcyjnym podłożem dla kształtującej się protekcji. Jego ujawnienie godzi bowiem bezpośrednio w interesy Rzeczypospolitej Polskiej w ujęciu ogólnym, gdyż zabezpiecza wszelkie istotne dla funkcjonowania państwa sfery jego aktywności (energetyczną, militarną, polityczną czy ekonomiczną). Do wyzwań związanych z zagrożeniem szpiegostwem czy cyberprzestępczością odnosi się również najnowsza *Strategii Bezpieczeństwa Narodowego RP*, która eksponując znacznie bezpieczeństwa informacyjnego, nie wskazuje jednak efektywnych sposobów jego ochrony. O ile doskonaleniu ochrony niejawnej służą m.in. wdrażane przez Polskę rozwiązania techniczno-organizacyjne, będące konsekwencją zobowiązań międzynarodowych (UE, NATO), o tyle eksponuje się aspekt nadmiernego wchodzenia w sojusze, doboru wspólnych interesów jako konsekwencji współzależności, znacznie ograniczających suwerenność. Bezpieczeństwo informacji niejawnych jest przede wszystkim uzależnione od podatności człowieka na błędy, co sprawia, że staje się on kluczowym elementem systemów bezpieczeństwa informacji, determinującym tym samym ich prawidłowe funkcjonowanie.

[64] *Ibidem*.