

CO WARTO WIEDZIEĆ O TAJEMNICACH PRAWNIE CHRONIONYCH W POLSCE

Przedmiotem niniejszego artykułu są wybrane problemy z dziedziny ochrony informacji niejawnych. Chodzi o takie informacje, które zawierają tajemnicę państwową i służbową oraz tajemnice zawodowe i inne informacje chronione przez polskie prawo. Częstość stykamy się z nimi, wykonując obowiązki służbowe, lecz rzadko rozpatrujemy je w kategoriach towaru. Wiedza na ten temat, poza znaczeniem czysto praktycznym, może okazać się przydatna do baczniejszej obserwacji wydarzeń w życiu publicznym, w trosce o prawidłowe funkcjonowanie prawa w społeczeństwie obywatelskim.

Czwarta władza żywo reaguje na przypadki niezgodnego z prawem upubliczniania informacji niejawnych głównie przez polityków i wysokich urzędników państwowych. Nie oznacza to jednak, że jeżeli jakiegoś tematu nie ma w mediach to problem nie istnieje. Jak na ponad dziesięcioletni okres funkcjonowania życia publicznego pod rządami obecnej ustawy o ochronie informacji niejawnych, zbyt często pojawiają się informacje, które niepokoją opinię społeczną z powodu nieprzestrzegania zasad bezpieczeństwa w tym zakresie. Żyjemy przecież w czasach, kiedy informacja (jawna i niejawna) jest towarem strategicznym i dlatego należy ją odpowiednio chronić przed nieuprawnionym ujawnieniem. Każde państwo tworzy więc odpowiednio zorganizowane systemy ochrony informacji ważnych ze względu na jego interes i bezpieczeństwo.

Mając powyższe na uwadze, w artykule zamieszczono definicje i pojęcia z zakresu polityki bezpieczeństwa informacji, urządzeń, systemu, danych niejawnych, które wynikają z przepisów ustawy o ochronie informacji niejawnych¹ oraz ustawy o ochronie danych osobowych². Przy pomocy tej terminologii dokonano analizy pojęć i klasyfikacji informacji niejawnych w Polsce.

¹ Mowa o ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tekst jednolity Dz.U. z 2005 r., Nr 196, poz. 1631).

² Mowa o ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2004 r., Nr 33, poz. 285).

Podana została wykładnia tajemnicy państwowej i służbowej oraz pokazano zachodzące między nimi relacje. Jednocześnie dokonano opisu używanych klauzul tajności.

Kolejny obszar spraw dotyczy warunków dostępu do informacji niejawnych oraz związanej z tym ustawowej procedury postępowania sprawdzającego. Zagadnienie to zostało przedstawione także w kontekście informacji klasyfikowanych NATO i możliwości dostępu do nich w naszym kraju.

W związku z tym, że w prawodawstwie polskim istnieje wiele rodzajów tajemnic a tajemnica państwowa i służbowa nie są jedynymi, które podlegają ochronie, w artykule przedstawiono również tajemnice zawodowe oraz informacje wrażliwe, czyli prawnie chronionych.

Podstawowe definicje i pojęcia z zakresu polityki bezpieczeństwa informacji

- 1) Administratorzy danych – *organy państwowe, organy samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne, podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej).*
- 2) Akredytacja bezpieczeństwa teleinformatycznego – *dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie o ochronie informacji niejawnych.*
- 3) Ankieta bezpieczeństwa osobowego – *ankieta zawierająca informacje o osobie ubiegającej się o dostęp do informacji niejawnych.*
- 4) Ankieta bezpieczeństwa przemysłowego – *ankieta zawierająca informacje o podmiocie gospodarczym ubiegającym się o dostęp do informacji niejawnych.*
- 5) Bezpieczeństwo – *stan, który daje poczucie pewności i gwarancje jego zachowania oraz szansę na doskonalenie. jedna z podstawowych potrzeb człowieka (...)* Wyróżnia się m.in. *bezpieczeństwo globalne regionalne, narodowe; bezpieczeństwo militarne, polityczne, społeczne; bezpieczeń-*

stwo fizyczne, psychiczne, socjalne; bezpieczeństwo strukturalne i personalne (na podstawie Słownika terminów z zakresu psychologii dowodzenia i zarządzania, Warszawa 2000, s. 17).

- 6) Dokument – *każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych.*
- 7) Dokumentacja bezpieczeństwa systemu lub sieci informatycznej – *Szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie o ochronie informacji niejawnych.*
- 8) Informacje niejawne – *informacje stanowiące tajemnicę państwową lub służbową, niezależnie od formy i sposobu ich wyrażania, także w trakcie ich opracowania; takie, które wymagają ochrony przed nieuprawnionym ujawnieniem.*
- 9) Jednostka organizacyjna to:
 - 1) organ władzy publicznej, w szczególności:
 - a) Sejm i Senat Rzeczypospolitej Polskiej,
 - b) Prezydent Rzeczypospolitej Polskiej,
 - c) organa administracji rządowej,
 - d) organa jednostek samorządu terytorialnego,
 - e) sądy i trybunały,
 - f) organa kontroli państwowej i ochrony prawa,
 - 2) Siły Zbrojne Rzeczypospolitej Polskiej i ich jednostki organizacyjne, a także inne jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane,
 - 3) Narodowy Bank Polski i banki państwowe,
 - 4) państwowe osoby prawne i inne niż wymienione wyżej państwowe jednostki organizacyjne,
 - 5) przedsiębiorcy, jednostki naukowe lub badawczo-rozwojowe, zamierzające ubiegać się, ubiegające się o zawarcie lub wykonujących umowy związanej z dostępem do informacji niejawnych albo wykonujące na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

- 10) Jednostka naukowa – *jednostka naukowa w rozumieniu przepisów o zasadach finansowania nauki.*
- 11) Kierownik jednostki organizacyjnej – *osoba odpowiadająca za ochronę informacji niejawnych w jednostce, w której takie informacje są wytwarzane, przetwarzane, przekazywane lub przechowywane.*
- 12) Klasyfikowanie informacji niejawnej – *przyznanie informacji przewidzianej w ustawie jednej z klauzul tajności („Zastrzeżone”, „Poufne”, „Tajne”, „Ścisłe tajne”).*
- 13) Odbiorca danych (w myśl ustawy o ochronie danych osobowych) – *każdy, komu udostępnia się dane osobowe, z wyłączeniem:*
 - *osoby, której dane dotyczą,*
 - *osoby upoważnionej do przetwarzania danych,*
 - *przedstawiciela (w przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim),*
 - *podmiotu, o którym mowa w art. 31,*
 - *organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.*
- 14) Pełnomocnik do spraw ochrony informacji niejawnych – *osoba, która odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych i podlega bezpośrednio kierownikowi jednostki organizacyjnej.*
- 15) Materiał – *dokument, jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia.*
- 16) Postępowanie sprawdzające – *postępowanie mające na celu ustalenie, czy osoba nim objęta daje rękojmię zachowania tajemnicy.*
- 17) Przetwarzanie danych – *jakikolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.*
- 18) Służby ochrony państwa – *Agencja Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego.*
- 19) Rękojmia zachowania tajemnicy – *spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem.*
- 20) Sieć teleinformatyczna – *organizacyjne i techniczne połączenie systemów teleinformatycznych.*

- 21) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- 22) System teleinformatyczny – system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji.
- 23) Tajemnica państwowa – informacja niejawna określona w wykazie rodzajów informacji niejawnych i oznaczona klauzulą „Tajne” lub „Ścisłe tajne”, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa.
- 24) Tajemnica służbowa – informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Informacje niejawne stanowiące tajemnicę służbową odpowiednio oznacza się klauzulą „poufne” lub „zastrzeżone”.
- 25) Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
- 26) Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, które mają zapewnić ochronę danych przed ich nieuprawnionym przetwarzaniem.
- 27) Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- 28) Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Tajemnica państwowa i służbowa oraz klauzule tajności

Jak już wspomniałem, każde państwo ma swoje tajemnice, których pilnie strzeże. Informacje zawierające tajemnicę państwową i służbową są niezwykle cennym towarem strategicznym i dlatego należy je odpowiednio chronić

przed nieuprawnionym ujawnieniem. Ochrona tajemnicy państwowej i służbowej stanowi jedno z ważniejszych zadań państwa i jego wyspecjalizowanych organów.

Jeżeli chodzi o tajemnicę państwową, to w tym miejscu trzeba również wspomnieć o klauzulach tajności, jakie jej towarzyszą. Dokładnie rzecz ujmując, tajemnicą państwową jest informacja określona w „Wykazie rodzajów informacji, które mogą stanowić tajemnicę państwową”, będącym załącznikiem nr 1 do ustawy o ochronie informacji niejawnych. W pierwszej części tegoż załącznika zawarte są informacje niejawne, które mogą być oznaczone klauzulą „ściśle tajne”. W jego drugiej części podano natomiast informacje, które mogą być oznaczone klauzulą „tajne”. Ustawodawca założył, iż ujawnienie jakiegokolwiek informacji określonej w obu częściach wspomnianego załącznika może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa. W Polsce informacje niejawne stanowiące tajemnicę państwową podlegają ustawowej ochronie przez okres 50 lat od daty ich wytworzenia.

Z kolei pojęcie tajemnicy służbowej zostało zdefiniowane w art. 2 ust. 2 ustawy o ochronie informacji niejawnych. W myśl tego artykułu tajemnicą służbową jest *informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej.*

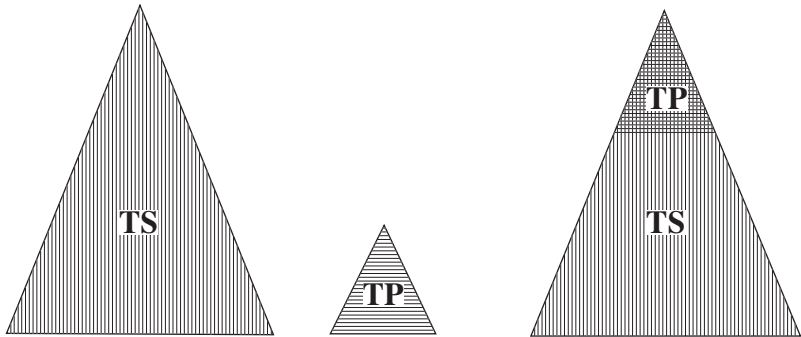
Należy podkreślić, iż taka formuła definicji tajemnicy służbowej powoduje, że tajemnica służbowa nie będzie używana do ochrony informacji chronionych na podstawie innych ustaw, o których szerzej będzie jeszcze mowa.

Z definicji natomiast wynika, że informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą „poufne” lub „zastrzeżone”. Wyższą klauzulę ustawodawca przewidział w przypadku gdy nieuprawnione ujawnienie informacji powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli. Natomiast klauzulę „zastrzeżone” stosuje się w przypadku gdy nieuprawnione ujawnienie informacji mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

Zgodnie z ustawą, informacje niejawne stanowiące tajemnicę służbową podlegają ochronie – informacje oznaczone klauzulą „poufne” przez 5 lat od daty wytworzenia, a oznaczone klauzulą „zastrzeżone” przez 2 lata.

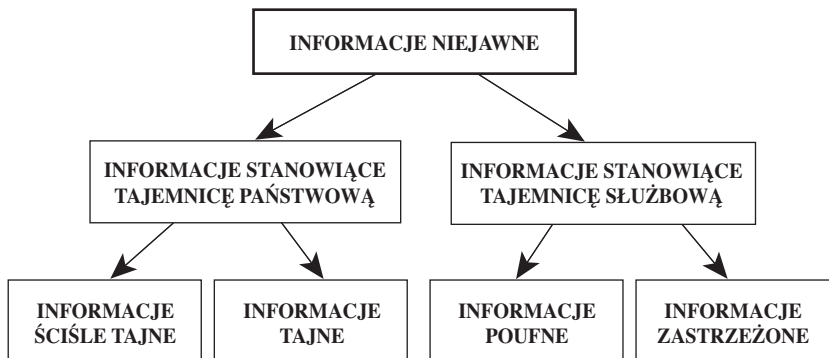
Analizując zależności pomiędzy informacjami niejawnymi trzeba pamiętać o tym, że tajemnica państwowa spełnia kryteria tajemnicy służbowej. W związku z tym pomiędzy informacjami niejawnymi stanowiącymi tajemnicę państwową i służbową zachodzi pewna relacja, którą przedstawiono graficznie (rys. 1).

Rysunek 1. Zależność pomiędzy informacjami zawierającymi tajemnicę służbową i państwową



Z powyższej relacji wynika, że informacja sklasyfikowana jako tajemnica państwowa stanowi podzbiór informacji sklasyfikowanej jako tajemnica służbowa. Ustawowy podział informacji niejawnych został przedstawiony graficznie (schemat 1).

Schemat 1. Podział informacji niejawnych w Polsce



Oprac. na podst. ustawy o ochronie informacji niejawnych

Do informacji niejawnych, które stanowią tajemnicę służbową lub państwową, poza ustawą o ochronie informacji niejawnych, odnosi się wiele innych ustaw. Część z nich odnosi się do tajemnicy państwowej lub tajemnicy państwowej i służbowej, a niektóre tylko do tajemnicy służbowej. Można je więc sklasyfikować ze względu na skutek, jaki może spowodować odsłonięcie zawartej w nich tajemnicy. W związku z tym do aktów prawnych odnoszących się do tajemnicy państwowej, bądź państwowej i służbowej należałoby zaliczyć ustawy, które zawarto w wykazie (tab. 1). Trzeba jednak zaznaczyć, że wykaz ten nie jest trwały z uwagi na jego otwarty charakter na nowe regulacje prawne.

Tabela 1. Wykaz aktów prawnych odnoszących się do tajemnicy państwowej lub tajemnicy państwowej i służbowej

| Lp. | Nazwa aktu prawnego | Publikator | Nr art. |
|-----|--|----------------------|-----------------|
| 1. | Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych | Dz.U. 2003. 179.1750 | art. 51 |
| 2. | Ustawa z dnia 19 października 1972 r. o wynalazczości | Dz.U. 1993.26.117 | art. 59 |
| 3. | Ustawa z dnia 13 kwietnia 2007r. o Państwowej Inspekcji Pracy | Dz.U. 2007.89.589 | art. 30, 44, 45 |
| 4. | Ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy | Dz.U. 1983.35.163 | art. 8 |
| 5. | Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych | Dz.U. 2001.98.1070 | art. 67 |
| 6. | Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich | Dz.U. 2001.14.147 | art. 4 |
| 7. | Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych | Dz.U. 2008.223.1458 | art. 24, ust. 4 |
| 8. | Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu | Dz.U. 2002.74.676 | art. 47 |
| 9. | Ustawa z dnia 6 kwietnia 1990 r. o Policji | Dz.U. 2007. 43.277 | art. 27 |
| 10. | Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej | Dz.U. 1991.88. 400 | art. 30 |
| 11. | Ustawa z dnia 26 kwietnia 1996 r. o Służbie Więziennej | Dz.U. 2002. 207.1761 | art. 27, 61 |
| 12. | Ustawa z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji przedsiębiorstw państwowych | Dz.U. 2002.171.1397 | art. 62 |

cd. tabeli 1

| Lp. | Nazwa aktu prawnego | Publikator | Nr art. |
|-----|---|----------------------|---|
| 13. | Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym | Dz.U. 2006.149.1078 | art. 23 |
| 14. | Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji | Dz.U. 2006.167.1191 | art. 14, 20 |
| 15. | Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu | Dz.U. 2004.163.1712 | art. 22 |
| 16. | Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych | Dz.U. 1997.123.779 | art. 27 |
| 17. | Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim | Dz.U. 2005.1.2 | art. 55 |
| 18. | Ustawa z dnia 20 czerwca 1985 o prokuraturze | Dz.U. 2008.7.39 | 45, 48 |
| 19. | Ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka | Dz.U. 2000.6.69 | art. 5 |
| 20. | Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu | Dz.U. 2003.153. 1505 | art. 6, 33 ust. 6-7, art. 29-30 |
| 21. | Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli | Dz.U. 1995. 13. 59 | art. 29 ust. 1, art. 40 ust. 1, art. 44, 73 |
| 22. | Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej | Dz.U. 2001.49.508 | Dział II Rozdz. 4, art. 270 |
| 23. | Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie | Dz.U. 189.1158 | art. 15, 18 |
| 24. | Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne | Dz.U. 2006.89.625 | art. 28 |

Biorąc pod uwagę znacznie mniejszy skutek wywołany ujawnieniem informacji prawnie chronionych, w odrębnym zestawieniu pokazano dla przykładu akty prawne odnoszące się do tajemnicy służbowej (tab. 2).

Tabela 2. Wykaz aktów prawnych odnoszących się do tajemnicy służbowej

| Lp. | Nazwa aktu prawnego | Publikator | Nr art. |
|-----|--|---------------------|-------------------------------|
| 1. | Ustawa z dnia z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne | Dz.U. 2006.216.1584 | art. 8 ust. 5, art. 10 ust. 3 |
| 2. | Ustawa z dnia z dnia 27 czerwca 1997 r. o służbie medycyny pracy | Dz.U. 2004.125.1317 | art. 11, ust. 3 |
| 3. | Ustawa z dnia 12 grudnia 2003 r. o ogólnym bezpieczeństwie produktów | Dz.U. 2003.229.2275 | art. 27 |
| 4. | Ustawa z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej | Dz.U. 2004.123.1291 | art. 41 ust. 1, 3 |
| 5. | Ustawa z dnia 15 grudnia 2000 r. o Inspekcji Handlowej | Dz.U. 2001.4.25 | art. 16 ust. 5 |
| 6. | Ustawa z dnia 21 sierpnia 1997 r. Prawo o ustroju sądów wojskowych | Dz.U. 1997.117.753 | art. 28, § 5 |

Dostęp do informacji niejawnych

Warunki dostępu do informacji niejawnych zostały określone w rozdziale 5 ustawy o ochronie informacji niejawnych, w którym unormowano dostęp do informacji niejawnych oraz procedurę postępowania sprawdzającego. Zgodnie z art. 26 teje ustawy kierownik jednostki organizacyjnej w formie pisemnej określa stanowiska lub rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności.

Na tej podstawie pełnomocnik kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych prowadzi wykaz stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych. Ma to istotne znaczenie przy doborze kadr pracowniczych zgodnie z przepisami ustawy, która szczegółowo reguluje procedurę udzielania dostępu do informacji niejawnych.

Od pozytywnego przebiegu tej procedury, nazwanej w ustawie postępowaniem sprawdzającym, zależy dopuszczenie osoby zainteresowanej do pracy na stanowisku albo zlecenie jej pracy. Bowiern informacje niejawne mogą być udostępnione tylko takiej osobie, która daje rękojmię zachowania tajemnicy. Należy również zaznaczyć, że udostępnienie tej osobie informacji klasyfikowanych musi być zgodne z zajmowanym przez nią stanowiskiem i rodzajem wykonywanej pracy.

Postępowanie sprawdzające mogą przeprowadzać tylko podmioty ustawowo do tego powołane, tj. Agencja Bezpieczeństwa Wewnętrznego (ABW), Służba Kontrwywiadu Wojskowego (SKW) oraz pełnomocnik do spraw ochrony informacji niejawnych. Wymienione podmioty przeprowadzają postępowanie sprawdzające:

- **zwykłe** – pełnomocnik do spraw ochrony informacji niejawnych przy stanowiskach i pracach związanych z dostępem do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulami „zastrzeżone” i „poufne”;
- **poszerzone** – ABW i SKW przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne”;
- **specjalne** – ABW i SKW przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne”.

Podstawą do wszczęcia przez pełnomocnika ochrony postępowania sprawdzającego zwykłego jest pisemne polecenie kierownika jednostki organizacyjnej. W wypadku postępowania sprawdzającego poszerzonego lub specjalnego, które prowadzi służby ochrony państwa, podstawą do jego wszczęcia jest wniosek kierownika jednostki organizacyjnej o wszczęcie postępowania sprawdzającego. Do wniosku musi być dołączona wypełniona odpowiednia ankieta bezpieczeństwa osobowego³. Podpisując ją, osoba sprawdzana wyraża zgodę na prowadzenie wobec niej czynności przewidzianych w ustawie. Wycofanie zgody lub odmowa poddania się ustawowym czynnościom proceduralnym jest jednoznaczna z rezygnacją z kandydowania na stanowisko lub ubiegania się o pracę związaną z dostępem do informacji niejawnych.

Po zakończeniu zwykłego postępowania sprawdzającego z wynikiem pozytywnym, pełnomocnik ochrony wydaje **poświadczenie bezpieczeństwa** osobie sprawdzanej, zawiadamiając o tym osobę upoważnioną do obsady stanowiska. Podobnie rzecz się ma w przypadku zakończenia z wynikiem pozytywnym postępowania poszerzonego lub specjalnego. Służby ochrony państwa wydają wówczas odpowiednie poświadczenie bezpieczeństwa i przekazują

³ Osoby ubiegające się o dostęp do informacji niejawnych wypełniają ankiety bezpieczeństwa osobowego według wzorów stanowiących załączniki do ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. W przypadku ubiegania się o dostęp do informacji niejawnych stanowiących tajemnicę służbową wypełnia się ankiety: a) dla klauzuli „zastrzeżone” według załącznika 2a; b) dla klauzuli „poufne” według załącznika 2b. W przypadku ubiegania się o dostęp do informacji niejawnych stanowiących tajemnicę państwową o klauzuli „tajne” lub „ściśle tajne”, wypełnia się ankietę według załącznika 2c.

je osobie sprawdzanej, zawiadamiając o tym osobę upoważnioną do obsady stanowiska.

Należy zaznaczyć, iż świadome podanie nieprawdziwych lub niepełnych danych w ankiecie przez osobę sprawdzaną stanowi podstawę do **odmowy wydania poświadczenia bezpieczeństwa** przez pełnomocnika ochrony. Odmówić wydania poświadczenia bezpieczeństwa mogą również służby ochrony państwa, jeżeli przeprowadzenie skutecznego postępowania sprawdzającego nie było możliwe z przyczyn od nich niezależnych. Wzory wszystkich poświadczeń bezpieczeństwa jak też decyzja o odmowie wydania poświadczenia oraz decyzja o cofnięciu poświadczenia bezpieczeństwa znajdują się w rozporządzeniu Prezesa Rady Ministrów⁴.

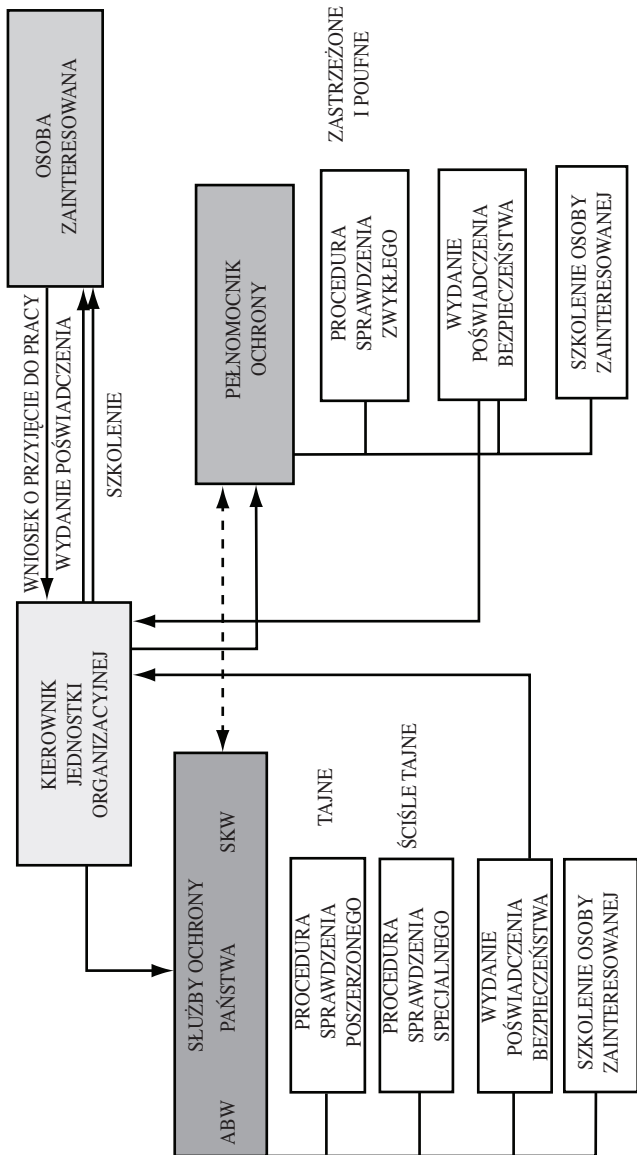
Przeprowadzenie postępowania sprawdzającego i wydanie osobie zainteresowanej poświadczenia bezpieczeństwa nie zamyka katalogu wymaganych czynności, które warunkują dopuszczenie osoby zainteresowanej do pracy lub pełnienia służby na stanowisku związanym z dostępem do tajemnicy państwowej lub służbowej. Dopiero przeszkolenie tej osoby w zakresie ochrony informacji niejawnych spełnia ten warunek. Zgodną z przepisami ustawy procedurę udzielania dostępu do informacji niejawnych przedstawiono graficznie (schemat 2).

Postępowanie specjalne powtarza się co 5 lat, postępowanie poszerzone co 7 lat, a postępowanie zwykłe co 10 lat. Pamiętać jednak należy, aby wniosek o wszczęcie kolejnego postępowania sprawdzającego został złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa.

Dotychczas omówione warunki dostępu do informacji niejawnych nie dotyczą osób zajmujących wysokie stanowiska państwowe. Postępowania sprawdzającego nie przeprowadza się wobec osób sprawujących urzędy: Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu Rzeczypospolitej Polskiej, Marszałka Senatu Rzeczypospolitej Polskiej i Prezesa Rady Ministrów, a także wobec kandydatów na członków Rady Ministrów powoływanych w trybie art. 154, 155 lub 161 Konstytucji Rzeczypospolitej Polskiej.

⁴ Mowa o rozporządzeniu Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie wzorów poświadczenia bezpieczeństwa, decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. z 2005 r. Nr 171, poz. 1431).

Schemat 2. Ustawowy tryb udzielania dostępu do informacji niejawnych



Oprac. na podst. ustawy o ochronie informacji niejawnych

Inną procedurę sprawdzania przepisy ustawy przewidują dla osób, które zajmują ważne stanowiska w państwie. Chodzi w tym przypadku o stanowiska: Pierwszego Prezesa Sądu Najwyższego, Prezesa Naczelnego Sądu Administracyjnego, Prezesa Trybunału Konstytucyjnego, Prezesa Narodowego Banku Polskiego, Prezesa Najwyższej Izby Kontroli, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, członków Rady Polityki Pieniężnej, członków Krajowej Rady Radiofonii i Telewizji, Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz Szefów Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów. Wobec tych osób postępowanie sprawdzające przeprowadza właściwa służba ochrony państwa na wniosek organu uprawnionego do powołania na to stanowisko. Jeżeli do powołania jest uprawniony Sejm albo Senat, z wnioskiem tym występuje odpowiednio Marszałek Sejmu albo Marszałek Senatu⁵. Organom tym właściwa służba ochrony państwa zobowiązana jest w ciągu czternastu dni przekazać stosowną opinię, co jest równoznaczne z zakończeniem postępowania sprawdzającego.

Dostęp do informacji klasyfikowanych NATO

Polska po przystąpieniu do Organizacji Sojuszu Północnoatlantyckiego i po wejściu do Unii Europejskiej zobowiązała się do wzajemnej ochrony informacji niejawnych. W celu wykonania umów międzynarodowych w korespondencji z państwami NATO i UE stosuje się w naszym kraju odpowiednie do treści dokumentu klauzule tajności określone w ustawie o ochronie informacji niejawnych oraz jej zagraniczne odpowiedniki (tab. 3).

Dostęp do informacji klasyfikowanych NATO poprzedzony został przystąpieniem naszego kraju do Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, którą sporządzono 6 marca 1997 r. w Brukseli⁶. Zapis o przystąpieniu Rzeczypospolitej Polskiej do porozumienia znajduje się w Załączniku III, który jest integralną częścią tejże umowy.

⁵ Zob. art. 27, ust. 6 i 7 ustawy o ochronie informacji niejawnych.

⁶ Patrz: Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r. (Dz.U. 2000 nr 64, poz. 740) oraz Oświadczenie Rządowe z dnia 29 grudnia 1999 r. w sprawie ratyfikacji przez Rzeczpospolitą Polską Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzonej w Brukseli dnia 6 marca 1997 r. (Dz.U. 2000 nr 64, poz. 741).

Tabela 3. Zestawienie klauzul tajności w wybranych państwach NATO i UE oraz sąsiadujących z Polską

| PAŃSTWO | KLAUZULA | | | |
|--|------------------------|-------------------|-------------------------------------|--|
| | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Odpowiedniki w języku angielskim | | | | |
| POLSKA | ŚCIŚLE TAJNE | TAJNE | POUFNE | ZASTRZEŻONE |
| NIEMCY | STRENG GEHEIM | GEHEIM | VS – VERYRAULICH | ----- |
| FRANCJA | TRES SEKRET | SEKRET DEFENSE | CONFIDENTIEL DEFENSE | DIFFUSION RESTREINTE |
| ZJEDNOCZONE KRÓLESTWO WLK. BRYTANII IRLANDII PŁN. | UK TOP SECRET | UK SECRET | UK CONFIDENTIAL | UK RESTRICTED |
| DANIA | YDERST HEMMELIGT | HEMMELIGT | FORTOLIGT | TILTJENESTEBRUG |
| HISZPANIA | MAKSIMO SEKRETO | SEKRETO | CONFIDENCIAL | DIFFUSION LIMITADA |
| POTRUGALIA | MUITO SEKRETO | SEKRETO | CONFIDENCIAL | RESERYADO |
| NORWEGIA | STRENGT HEMMELIG | HEMMELIG | KOFIDENSIELL | BERGRENSET |
| HOLANDIA | ZEER GEHEIM | GEHEIM | CONFIDENTIELL lub YERTOUWELUK | DIENSTGEHEIM |
| USA | TOP SECRET | SECRET | CONFIDENTIAL | Brak odpowiednika i traktowane jest jak POUFNE |
| KANADA | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| FEDERACJA ROSYJSKA | COBEPИEHHO CEKPETHO | CEKPETHO | CEKPETHO | ----- |
| UKRAINA | ÖIEKOM TAEMHO | TAEMHO | ----- | ----- |
| REPUBLIKA ŁOTEWSKA | SEVIŠKI SLEPENI | SLEPENI | KONFIDENCIALI | IEROBEŽOTA LIETOŠANA |
| REPUBLIKA CZESKA | PRÍSŇNĚ TAJNĚ | TAJNĚ | DUVĚRNĚ | WHRAZENĚ |
| REPUBLIKA SŁOWACKA | PRISNE TAJNĚ | TAJNĚ | DÔVERNĚ | VYHRADENĚ |

Źródło: http://www.iniejawna.pl/pomoce/przyc_pom/klauzule_nato.html

Istotnym warunkiem, który towarzyszył temu procesowi było określenie standardów i procedur wzajemnej ochrony i zabezpieczenia informacji niejawnych, jakie mogą między sobą wymieniać Rządy Stron. Umożliwiło to skuteczne konsultacje polityczne, współpracę i planowanie obronne przy realizacji celów Traktatu. W związku z tym w umowie określono „informację niejawną NATO” w następujący sposób:

- (a) *informacja oznacza wiedzę, która może być przekazana w jakiegokolwiek formie;*
- (b) *informacja niejawna oznacza informację lub materiał, który został tak oznaczony, wymagający ochrony przed nieupoważnionym ujawnieniem;*
- (c) *wyraz „materiał” obejmuje dokumenty, jak też dowolną część urzędzenia, wyposażenia lub broni wyprodukowanych lub będących w trakcie produkcji;*
- (d) *wyraz „dokument” oznacza dowolną zarejestrowaną informację, niezależnie od jej fizycznej postaci lub cech charakterystycznych, w tym, bez ograniczeń, tekst pisany lub drukowany, dane w postaci kart i taśm, mapy, wykresy, fotografie, obrazy, rysunki, ryciny, szkice, notatki i materiały robocze, kalki węglowe i taśmy atramentowe lub kopie wykonane dowolnymi środkami i metodami oraz nagrania dźwiękowe, magnetyczne, elektroniczne, optyczne lub wideo w dowolnej postaci, jak również przenośny sprzęt elektroniczny z wbudowaną na stałe lub wymienną pamięcią⁷.*

Generalnie rzecz biorąc, najważniejsze zobowiązania dla polskiego rządu z tytułu przystąpienia do Umowy sprowadzało się do utworzenia i wprowadzenia w życie standardów bezpieczeństwa, które zapewnią Stronom jednolity stopień ochrony informacji niejawnych. W tym celu utworzono krajowe władze bezpieczeństwa do spraw działalności NATO, na których spoczęła odpowiedzialność za wprowadzenie w życie środków ochrony bezpieczeństwa.

Zgodnie z obowiązującą ustawą o ochronie informacji niejawnych, krajową władzą bezpieczeństwa jest Agencja Bezpieczeństwa Wewnętrznego. Odpowiada ona za to aby wszystkie osoby, które w ramach swoich obowiązków służbowych mają dostęp do informacji o klauzuli NATO CONFIDENTIAL lub wyższej, zostały odpowiednio sprawdzone. Dlatego też postępowania sprawdzające na poziomie „poufne” dla sfery cywilnej prowadzi ABW.

Natomiast dostęp do informacji o klauzuli „zastrzeżone” (RESTRICTED) jest przyznawany przez kierownika jednostki organizacyjnej na podstawie sprawdzenia przeprowadzonego przez pełnomocnika ochrony. Procedura

⁷ Zob. Załącznik I Umowy między Stronami...

sprawdzeniowa jest analogiczna jak w przypadku postępowania zwykłego, o którym już była mowa.

Wniosek o przeprowadzenie postępowania musi jednak zawierać uzasadnienie potrzeby wydania certyfikatu uprawniającego do dostępu do informacji klasyfikowanych NATO oraz wskazanie klauzuli tajności, do której dana osoba ma być dopuszczona. Ponadto osoba sprawdzana wypełnia ankietę bezpieczeństwa osobowego zgodnie z ogólnymi zasadami, dopisując odpowiednią klauzulę NATO wraz z odpowiednim oznaczeniem. W takim przypadku przy klauzuli SECRET w ankiecie należy zaznaczyć pole „tajne” i z boku dopisać NATO SECRET.

Certyfikaty bezpieczeństwa osobowego NATO mogą być wydane zainteresowanym osobom również na podstawie posiadanych już krajowych poświadczeń bezpieczeństwa wydanych przez służby ochrony państwa.

Tajemnice zawodowe i inne tajemnice prawnie chronione

W prawodawstwie polskim istnieje wiele rodzajów tajemnic, a tajemnica państwowa i służbowa nie są jedynymi, które podlegają ochronie. Definicja tajemnicy zamieszczona w słowniku języka polskiego określa to pojęcie jako: „coś tajnego, rzecz, której nie należy rozgłaszać, która nie powinna wyjść na jaw; sekret”⁸.

W potocznym użyciu nie rozróżniamy wielu używanych na co dzień pojęć takich, jak: dane, informacje, kontekst, znaczenie, wiedza. W sensie semantycznym nie zajmujemy się ustawicznym badaniem znaczenia słów, czyli interpretacją znaków oraz interpretacją zdań i wyrażeń języka. Ma to jednak znaczenie gdy wchodzimy w obszar związany z potrzebą zagwarantowania „dostępności” i „poufności” informacji chociażby z racji wykonywanego zawodu. Wówczas dotykamy sfery pojęciowej związanej z tajemnicą rozumianą najogólniej jako dane lub informacje, których ujawnienie osobom nieuprawnionym jest zakazane, głównie ze względu na normy społeczne i prawne. I choć istnieje w naszym kraju prawodawstwo regulujące wiele tajemnic związanych z wykonywaniem różnych zawodów, to często nie definiuje tych tajemnic w sposób precyzyjny.

Można jednak przytoczyć wiele przykładów tajemnic zawodowych, kierując się klasyfikacją informacji niejawnych chronionych według właściciela informacji. Taki podział tajemnic z uwagi na właściciela informacji, rozu-

⁸ *Mały słownik języka polskiego*, PWN, Warszawa 1997, s. 929.

mianego jako organizacja z określonego sektora gospodarczego, proponują naukowcy z Uniwersytetu im. Adama Mickiewicza w Poznaniu⁹. Ramy takiej systematyzacji obejmują:

- **tajemnicę publicznego obrotu papierami wartościowymi**, którą objęte są informacje związane z publicznym obrotem, jakich ujawnienie mogłoby naruszyć interes uczestników tego obrotu na podstawie ustawy Prawo o publicznym obrocie papierami wartościowymi art. 159 i następane;
- **tajemnicę ubezpieczeniową** na podstawie ustawy o działalności ubezpieczeniowej art. 9, 37 i n.;
- **tajemnicę przekazu informacji** na podstawie ustawy o łączności art. 29;
- **tajemnicę bankową**, którą objęte są wszystkie wiadomości dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez których ujawnienia nie jest możliwe należyte wykonanie zawartej przez bank umowy oraz dotyczące osób, które, nie będąc stroną umowy, dokonały czynności pozostających w związku z zawarciem takiej umowy na podstawie ustawy prawo bankowe, zgodnie z art. 104 i następane oraz ustawy o Narodowym Banku Polskim art. 55;
- **tajemnicę telekomunikacyjną** na podstawie ustawy Prawo telekomunikacyjne, rozdz. 5;
- **tajemnicę lekarską**, którą objęte są osoby wykonujące czynności lekarskie w zakresie zachowania w tajemnicy wszystkiego, o czym powezmą wiadomość w związku z wykonywaniem tych czynności, ponadto dane osobowe dotyczące dawcy i biorcy przeszczepu, na podstawie ustawy o zawodzie lekarza art. 40, ustawy o zwalczaniu chorób zakaźnych art. 6 ust. 1, ustawy o zawodach pielęgniarstwa i położnej art. 21, ustawy o ochronie zdrowia psychicznego Rozdz. VI i XVI, ustawy o służbie medycyny pracy art. 3 ust. 3 i art. 11 ust. 3, ustawy o pobieraniu i przeszczepianiu komórek, tkanek i narządów art. 12, ustawy o publicznej służbie krwi art. 13, ustawy o zakładach opieki zdrowotnej art. 18 oraz Kodeksu karnego art. 266 § 1;
- **tajemnicę dziennikarską lub prasową**, którą objęte są dane umożliwiające identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających infor-

⁹ Zob. Andrzej Adamczyk, Rafał Renk, Jakub Radziulis i prof. Witold Hołubowicz, *Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania*. XI Konferencja PLOUG Kościelisko, październik 2005, strona: http://www.ploug.org.pl/konf_05/materialy/pdf/11.pdf; dnia 18.01.2009.

macji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnienie powyższych danych oraz wszelkie informacje, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich, na podstawie ustawy Prawo prasowe art. 10 i art. 16 ust. 1 oraz Kodeksu karnego art. 240;

- **tajemnicę notarialną i adwokacką**, którą objęte są wszelkie fakty, o których adwokat dowiedział się w związku z udzielaniem pomocy prawnej, na podstawie ustawy Prawo o adwokaturze art. 3 i 6.

Ci sami autorzy¹⁰ do tajemnic zawodowych, które obejmują szeroko rozumiany krąg odbiorców informacji zaliczają:

- **tajemnicę pracodawcy** na podstawie Kodeksu pracy art. 100;
- **tajemnicę skarbową**, którą objęte są indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez podatników, płatników lub inkasentów na podstawie ustawy o kontroli skarbowej art. 34 oraz ordynacji podatkowej Dział VII;
- **tajemnicę przedsiębiorstwa lub przedsiębiorcy**, którą objęte są nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności na podstawie ustawy o zwalczaniu nieuczciwej konkurencji art. 11 ust. 4 oraz ustawy o ochronie konkurencji i konsumentów art. 63;
- **tajemnicę źródeł informacji** na podstawie ustawy o prawie autorskim i prawach pokrewnych art. 84;
- **tajemnicę statystyczną** na podstawie ustawy o statystyce publicznej art. 12 oraz ustawy o narodowym spisie powszechnym ludności i mieszkań w 2002 r. art. 10;
- **tajemnicę handlową** na podstawie np. ustawy Prawo energetyczne art. 28;
- **pozostałe tajemnice zawodowe** na podstawie: ustawy Prawo prasowe art. 15 ust. 2, ustawy o działalności ubezpieczeniowej art. 9 i 37n, ustawy Prawo o notariacie art. 15 i 18, ustawy o izbach aptekarskich art. 21, ustawy z o biegłych rewidentach i ich samorządzie art. 4a, ustawy o doradztwie podatkowym art. 37, ustawy o funduszach inwestycyjnych art. 45, ustawy o organizacji i funkcjonowaniu funduszy emerytalnych art. 49,

¹⁰ A. Adamczyk, R. Renk, J. Radziulis, W. Hołubowicz, *Klasyfikacja informacji...*

ustawy o komornikach sądowych i egzekucji art. 14 i 20, ustawy o giełdach towarowych Rozdz. 8, ustawy o rzecznikach patentowych art. 14, ustawy o służbie cywilnej art. 67, ustawy o sejmowej komisji śledczej art. 16, ustawy o wykonywaniu mandatu posłała i senatora art. 19 oraz ustawy o gospodarce nieruchomościami art. 175.

Przytoczony powyżej rodzaj klasyfikacji ochrony informacji określonych w oparciu o ich właściciela nie wyczerpuje tematu. Lista tajemnic pozostaje bowiem otwarta na wciąż rosnące potrzeby. Przykładem niech będzie ochrona dostępności danych przetwarzanych w instytucjach administracji publicznej na podstawie ustawy o dostępie do informacji publicznej.