Ochrona prawna informacji niejawnych

...by zachować posiadaną tajemnicę
nie wystarczy samo milczenie...
PAUL CLAUDEL

MONIKA BOGUCKA – ABW

Poniższy artykuł otwiera cykl poświęcony tematyce ochrony informacji niejawnych. W jego ramach zostaną przedstawione aktualne wymogi prawne, które muszą być spełnione przez każdą jednostkę organizacyjną, w której będą wytwarzane, przetwarzane, przechowywane lub przekazywane tego typu informacje.
W pierwszej części omówiono podstawy i zakres ochrony informacji niejawnych.

Legislacja dotycząca ochrony wiadomości, które ze względu na dobro państwa należy zachować w tajemnicy, nie jest nowym obszarem zainteresowania prawa. Pierwsze regulacje odnoszące się do tej problematyki pochodzą z lat 20. i 30. ubiegłego wieku (zob. rozporządzenie Prezydenta RP z 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciwko państwu, zastąpione rozporządzeniem Prezydenta RP z 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa). Początkowo ochroną prawną objęto wyłącznie tajemnicę państwową. Dopiero dekret z 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej wprowadził pojęcie „tajemnicy służbowej". Przepisy te ograniczały się do ogólnego nakazu zachowania pewnej wiedzy w tajemnicy i wprowadzały sankcje za jego naruszenie. Nie zawierały natomiast postanowień regulujących sposób ochrony tych wiadomości. Pierwszym, w miarę kompleksowym unormowaniem poruszającym ten problem była ustawa z 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej, która obowiązywała do 1999 r.

Obecnie regulacje prawne dotyczące ochrony informacji niejawnych zawarte są w ustawie z 22 stycznia 1999 r. o ochronie informacji niejawnych, oznaczanej dalej skrótem „UOIN" oraz wydanych na jej podstawie aktach wykonawczych. Ustawa określa organizację ochrony informacji niejawnych, ich klasyfikowanie, dostęp do nich, przebieg postępowania sprawdzającego, udostępnianie informacji, zasady prowadzenia kancelarii tajnych i obiegu dokumentów, a ponadto środki ich fizycznej ochrony oraz wymogi bezpieczeństwa systemów i sieci teleinformatycznych, w których będą przetwarzane, jak również podstawy bezpieczeństwa przemysłowego.

Zakres przedmiotowy UOIN

Przedmiotem ochrony, na gruncie uoin, są dwa rodzaje tajemnicy: państwowa i służbowa, określane zbiorczo **informacjami niejawnymi.**

Zgodnie z definicją ustawową, **tajemnicą państwową** jest informacja niejawna określona w wykazie rodzajów tych informacji (zob. załącznik nr 1 do UOIN), której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów RP albo narazić te interesy na co najmniej znaczną szkodę.

Wspomniany załącznik zawiera listę 98 rodzajów informacji, podzieloną na trzy części. Grupa pierwsza, obejmująca informacje oznaczone klauzulą „ściśle tajne", zawiera 30 rodzajów wiadomości, np. *hasła i kody dostępu do urządzeń przechowujących, przetwarzających i przesyłających informacje oznaczone klauzulą „ściśle tajne".* W drugiej części znalazły się informacje niejawne oznaczone klauzulą „tajne" ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny (40 rodzajów), np. *lokalizacja, rodzaj i przeznaczenie oraz właściwości techniczno-ochronne budownictwa specjalnego.*

Wreszcie w grupie trzeciej umieszczono informacje niejawne oznaczone klauzulą „tajne" ze względu na ważny interes państwa (28 rodzajów), np. *informacje dotyczące rozwiązań technicznych, technologicznych i organizacyjnych, których ujawnienie naraziłoby na szkodę ważny interes gospodarczy państwa.* Wykaz rodzajów informacji ujęty w załączniku należy rozumieć jako enumeratywne wyliczenie tych rodzajów informacji, które potencjalnie mogą stanowić tajemnicę państwową, jeżeli spełnione są pozostałe kryteria wynikające z jej definicji.

Tajemnicę służbową stanowią informacje niejawne nie będące tajemnicą państwową, uzyskane w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, których nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej.

Porównując obie kategorie informacji niejawnych należy zauważyć, iż wykaz informacji niejawnych stanowiących tajemnicę państwową jest ściśle określony w załączniku nr 1 do uoin, nie ma natomiast spisu rodzajów informacji niejawnych mogących stanowić tajemnicę służbową. W związku z tym należy przyjąć, iż tylko katalog tajemnic państwowych jest zamknięty. Ponadto, tajemnicą państwową informacja niejawna staje się już przez sam fakt umieszczenia

jej w wymienionym załączniku, natomiast warunkiem powstania tajemnicy służbowej jest jej „uzyskanie w związku z czynnościami służbowymi albo wykonywaniem prac zleconych". Jednakże podstawowa różnica między tajemnicą państwową a tajemnicą służbową sprowadza się do rozmiaru szkody, jaką mogłoby wyrządzić ich nieuprawnione ujawnienie. W przypadku tajemnicy państwowej godziłoby to w **podstawowe interesy państwa,** podczas gdy ujawnienie tajemnicy służbowej naraziłoby **interes państwa, interes publiczny lub prawnie chronione interesy obywateli albo jednostki organizacyjnej.**

Wśród podstawowych interesów RP ustawodawca wymienia: niepodległość lub nienaruszalność terytorium, interesy obronności, bezpieczeństwa państwa i obywateli. Wyliczenie to ma charakter przykładowy. W pozostałym zakresie należy sięgnąć do treści art. 61 ust. 3 Konstytucji RP, który odwołuje się do takich dóbr, jak: ochrona porządku publicznego oraz ważny interes gospodarczy państwa. Nie wszystkie interesy państwa związane z ochroną porządku publicznego czy też sferą gospodarczą mają charakter podstawowy. Taką cechę można przypisać wyłącznie najistotniejszym spośród nich, odnoszącym się do podstawowych funkcji, jakie spełniać musi organizacja państwowa[1]. Pozostałe interesy państwa, oprócz interesu publicznego, prawnie chronionych interesów obywateli (liczba mnoga, czyli nie chodzi o interesy pojedynczego obywatela) oraz interesy jednostki organizacyjnej są chronione za pomocą instytucji tajemnicy służbowej. Możliwość naruszenia tych interesów jest wysoce ocenna, jednakże, co podkreśla się w literaturze[2], groźba narażenia ich na szkodę powinna być konkretna, a nie jedynie abstrakcyjna.

Zakres podmiotowy UOIN

Obowiązek ochrony informacji niejawnych zgodnie z postanowieniami UOIN dotyczy licznych jednostek organizacyjnych, przede wszystkim podmiotów publicznych, czyli organów władzy publicznej (Sejmu, Senatu, Prezydenta RP, organów administracji rządowej, jednostek samorządu terytorialnego, sądów i trybunałów, organów kontroli państwowej) oraz Sił Zbrojnych, Narodowego Banku Polskiego i banków państwowych, innych państwowych osób prawnych oraz państwowych jednostek organizacyjnych. Pozostałą grupę tworzą przedsiębiorcy, jednostki naukowe lub badawczo – rozwojowe, ubiegające się o zawarcie lub wykonujące umowy związane z dostępem do informacji niejawnych albo wykonujące na podstawie przepisów prawa zadania na rzecz obronności i bezpieczeństwa państwa, związane z dostępem do tego typu informacji.

Organizacja ochrony informacji niejawnych w jednostce organizacyjnej

Za ochronę informacji niejawnych odpowiada **kierownik jednostki organizacyjnej,** w której takie informacje są wytwarzane, przetwarzane, przechowywane lub przekazywane. Przepisy uoin nie definiują pojęcia „kierownik jednostki organizacyjnej". Przyjmuje się, iż jest to osoba lub organ jednostki uprawniony – zgodnie z przepisami prawa, statutem, umową – do zarządzania nią. Zastosowanie będą miały zatem przepisy określające byt prawny poszczególnych jednostek (urzędów państwowych i samorządowych, spółek prawa handlowego, przedsiębiorstw).

Kierownik jednostki organizacyjnej jest zobowiązany do powołania **pełnomocnika ds. ochrony informacji niejawnych,** który będzie kierował wyodrębnioną, wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych **(pion ochrony).** W związku z tym, że uoin nie zawiera szczególnej regulacji dotyczącej sposobu powierzania tych zadań, mogą znaleźć tu zastosowanie przepisy kodeksu pracy oraz innych ustaw (np. o pracownikach urzędów państwowych i samorządowych, o służbie cywilnej), a także przepisy poszczególnych pragmatyk.

Kandydat na stanowisko pełnomocnika musi spełnić wymogi ustawowe, tj. posiadać obywatelstwo polskie i co najmniej średnie wykształcenie oraz uzyskać tzw. poświadczenia bezpieczeństwa, wydawane przez służby ochrony państwa*) i odbyć stosowne przeszkolenie przez w/w służby.

Rola pełnomocnika i pionu ochrony w procesie ochrony informacji niejawnych jest kluczowa i wymaga głębszego omówienia, co nastąpi w następnym artykule z tego cyklu.

Literatura:

[1] Rozporządzenie Prezydenta RP z 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciwko państwu (Dz.U. nr 18, poz. 160)

[2] Rozporządzenie Prezydenta RP z 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa (Dz.U. nr 94, poz. 851)

[3] Dekret z 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej (Dz.U. nr 55, poz. 437)

[4] Ustawa z 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. nr 40, poz. 271 ze zm.)

[5] Ustawa z 22 stycznia 1997 r. o ochronie osób i mienia (Dz.U. nr 114, poz. 740)

[6] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483)

[7] Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95 ze zm.)

[8] Kunicka-Michalska B., Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz, Wydawnictwo C. H. Beck, Warszawa 2000

[9] Szałowski R., Prawna ochrona informacji niejawnych i danych osobowych, Difin, Warszawa 2000

[10] Taradejna R. i M., Tajemnice państwowe i inne chroniące interesy państwa i obywateli. Zbiór przepisów z komentarzem, Mini Press 1998

[11] Wróbel W., Prawnokarna ochrona tajemnicy państwowej, PKiNP nr 1 z 2000 r.

*) W rozumieniu UOIN służbami ochrony państwa są Agencja Bezpieczeństwa Wewnętrznego i Wojskowe Służby Informacyjne