Centrum Ekspertyzy Lokalnej

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

OPINIE I KOMENTARZE FRDL

OPINIA nr 7/2022

OCHRONA INFORMACJI NIEJAWNYCH W JST

dr Mariusz Paradowski

1.Wiadomości wstępne

Wkraczając w podjętą analizę należy odnieść się do genezy ochrony informacji niejawnych na ziemiach polskich. Wymieniona problematyka znalazła swoje odzwierciedlenie w literaturze. *Po odzyskaniu niepodległości przez Polskę na terytorium państwa obowiązywały systemy prawne państw zaborczych. Mieliśmy do czynienia z prawem rosyjskim, pruskim i austriackim oraz węgierskim (na Spiszu i Orawie). Przy czym systemy te charakteryzowały się archaicznością rozwiązań oraz odmiennymi i trudnymi do pogodzenia cechami. W pierwszym okresie niepodległości narzędziem ochrony informacji niejawnych były przepisy karne. Aż do roku 1932 system prawa polskiego nie regulował tych zagadnień w sposób spójny (...) w okresie istnienia Polskiej Rzeczypospolitej Ludowej mieliśmy do czynienia z nowym podejściem do ochrony informacji niejawnych. Wynikało ono z autorytarnego charakteru państwa Ponadto w latach 1945-1956 prawo karne było otwarcie używane do walki z przeciwnikami politycznymi11. W dekrecie Rady Ministrów z 16 listopada 1945 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa (Dz. U. nr 53, poz. 300) (...) w dniu 22 stycznia 1999 r. Prezydent RP podpisał ustawę o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95). Zmiana ustawy pociągnęła za sobą konieczność przyjęcia szeregu nowych aktów wykonawczych i procedur działania* **/A. Szymczak, O systemie ochrony informacji niejawnych w Polsce w latach 1918-2011 [w:] Czasopismo Historyczno-Prawne t. LXV z. 1, Poznań 2013, s. 470-480/.**

Problematyka dotycząca ochrony informacji niejawnych w jednostkach samorządu terytorialnego na gruncie działania prawa administracyjnego stanowi ważny obszar normatywny. Zdaniem przedstawicieli nauki: *„ochrona informacji niejawnych jest dziedziną niezwykle trudną i wrażliwą”***/B. Radziszewska, E. Kuśnierz, Uprawnienia i obowiązki kierownika jednostki oraz pełnomocnika ochrony w świetle ustawy o ochronie informacji niejawnych {w:] Wojskowy Przegląd Prawniczy nr 4, Warszawa 2011, s. 91/**. Za takim argumentem niewątpliwie przemawiają względy rozpiętości normatywnej regulacji prawnych dotyczących ochrony informacji niejawnych oraz wielowątkowość zagadnień merytorycznych wpisujących się w wymieniony obszar. Podstawę prawną stanowi ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych **/t. j. Dz. U. z 2019 r. poz. 742/**. Stosownie do treści przepisu art. 1 ust. 1 wskazanego aktu prawnego ustawa określa zasady ochrony informacji, 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, zwanych dalej *„informacjami niejawnymi”*. W literaturze prawniczej dostrzega się zależność pomiędzy regulacją ustawową oraz naukowym rozumieniem informacji niejawnych. Wedle poglądów doktryny przez informacje niejawne należy rozumieć: *„takie informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, zarówno w trakcie ich opracowywania, jaki i niezależnie od formy i sposobu ich wyrażania”* **/M. Gorbaczuk, Zarys problematyki ochrony informacji niejawnych w postępowaniach kontrolnych i audytowych [w:] Kontroler Info nr 10, Warszawa 2018, s. 53/**. Trudno nie zauważyć, iż tematyka związana z ochroną informacji niejawnych odczytywana jest również w perspektywie standardów konstytucyjnych, w szczególności zasady demokratycznego państwa prawnego. *Fundamentalną zasadą demokratycznego państwa prawnego pozostaje prawo obywateli do uzyskiwania informacji o działalności jego organów. Towarzyszy jej zwrotny problem aktywności tych ostatnich zobowiązanych do ochrony żywotnych interesów całej wspólnoty kosztem uprawnień jednostki. Wypełnieniu powyższego zadania służy wyodrębnienie wartościowych dla bezpieczeństwa państwa zasobów informacji wymagających szczególnej ochrony przed szkodliwym dla niego ujawnieniem, które precyzuje ustawa o ochronie informacji niejawnych* **/R. Zapart, Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji [w:] Polityka i społeczeństwo nr 3, Rzeszów 2020, s. 121/.**

2. Aspekt przedmiotowy oraz sfera podmiotowa ochrony informacji niejawnych

Przedmiotem regulacji prawnej objętej treścią analizowanej ustawy pozostają zagadnienia normatywne dotyczące klasyfikowania informacji niejawnych, organizowania ochrony informacji niejawnych, przetwarzania informacji niejawnych, postępowania sprawdzającego oraz kontrolnego postępowania sprawdzającego prowadzonych w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, postępowania bezpieczeństwa przemysłowego prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, organizacji kontroli stanu zabezpieczenia informacji niejawnych, ochrony informacji niejawnych w systemach teleinformatycznych oraz stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych. Przepisy wymienionego źródła prawa mają zastosowanie m. in. wobec organów władzy publicznej - organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych. W świetle powyższych aspektów nasuwają się istotne wnioski. Ochrona informacji niejawnych w polskim systemie prawnym należy do kręgu rozwiązań normatywnych o szerokim spektrum regulacji ustawowej, której częścią pozostają nie tylko przepisy prawa materialnego, prawa ustrojowego, ale także postępowania szczególne w obrębie których ma miejsce dopuszczenie do pracy zawodowej osób wyselekcjonowanych w procedurze, spełniających kryterium zachowania tajemnicy informacji niejawnych.

3. Klasyfikacja informacji niejawnych na gruncie jednostek samorządu terytorialnego

Rozwiązania prawne przyjęte na gruncie de lege lata ustawy o ochronie informacji niejawnych w krajowym porządku prawnym wprowadzają typologię informacji niejawnych, przy czym dla administracji samorządowej znamienną rolę spełniają informacje niejawne objęte klauzulą „*poufne*" oraz „*zastrzeżone*". W swej zasadniczej części informacje niejawne, którym przypisano klauzulę „*tajne*" lub „*ściśle tajne*" wykazują fundamentalne znaczenie w obliczu centralnych organów administracji rządowej oraz innych struktur państwowych.

W myśl treści przepisu art. 5 ust. 3 analizowanego aktu prawnego informacjom niejawnym nadaje się klauzulę „*poufne*", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej,
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej,
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli,
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej,
- 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 systemu finansowego Rzeczypospolitej Polskiej,
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Wedle treściprzepisu art. 5 ust. 4 niniejszego źródła prawa informacjom niejawnym nadaje się klauzulę „*zastrzeżone*", jeżeli nie nadano im wyższej klauzuli tajności, 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 praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej. Interesujące wnioski na temat klasyfikowania informacji niejawnych do określonej kategorii wynikają z orzecznictwa sądowego-administracyjnego. Zgodnie z poglądami judykatury *dla zakwalifikowania informacji niejawnej do informacji niejawnej wystarczy element materialny, tzn. istnienie takiej cechy przez którą stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania* **/wyr. WSA w Warszawie z dnia 23 listopada 2020 r. II SA/Wa 1187/20, Legalis nr 2569949/.** Nie może umknąć uwadze fakt, że na szczeblu jednostek samorządu terytorialnego ochrona informacji niejawnych odbywa się nie tylko w oparciu o obowiązujące treści ustawowe, ale wdrażana jest przede wszystkim na mocy aktów wykonawczych, w szczególności zarządzeń wójtów, burmistrzów lub prezydentów miast. Tutaj ma miejsce ustalenie planu ochrony informacji niejawnych zawierającego szczegółowe rozwiązania prawne zapobiegające niekorzystnym sytuacjom mogącym naruszyć przepisy ustawodawstwa zwykłego. Podstawę prawną stanowi przepis art. 15 ust. 1 pkt 5 analizowanej ustawy.

Przywołane źródło prawa precyzuje procedurę przypisywania klauzul tajności poszczególnym dokumentom oraz materiałom .Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Trzeba odnotować, że dokumentom lub materiałom dotychczas objętym niższą klauzulą tajności w toku prowadzonego postępowania może zostać przydzielona wyższa klauzula tajności. Co więcej, kierownicy jednostek organizacyjnych przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

.Informacje niejawne, którym nadano określoną klauzulę tajności:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności,
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności,
- muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

4. Organizacja ochrony informacji niejawnych na szczeblu samorządowym

Dokonując wykładni przepisów obowiązującej ustawy o ochronie informacji niejawnych nie sposób przemilczeć faktu, iż tematyka ustrojowa organów administracji publicznej we wskazanym źródle prawa jest wyjątkowo zawiła, a przez to niejasna i chaotyczna. Niemniej jednak z uwagi na zawężoną tutaj analizę względem organizacji ochrony informacji niejawnych na szczeblu samorządowym charakterystyka normatywna będzie uproszczona. Stosownie do treści przepisu art. 10 omawianej ustawy Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości 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 Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi oraz prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych. Co znamienne, ABW realizuje zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, a zatem również wobec jednostek samorządu terytorialnego.

W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych, upoważnieni pisemnie funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mają prawo do:

- wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane;
- wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
- żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji;
- przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
- żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień;
- zasięgania w związku z przeprowadzaną kontrolą informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;
- powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
- uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Należy podkreślić, że w odniesieniu do postępowań zrealizowanych przez pełnomocników ochrony zatrudnionych w jednostkach samorządu terytorialnego wyposażonych w kompetencje do stosowania prawa administracyjnego w dziedzinie ochrony informacji niejawnych czynności kontrolne uregulowane analizowaną ustawą prowadzą ABW oraz SKW. Trzeba nadmienić, iż kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego *pełnomocnik do spraw ochrony informacji niejawnych*, czyli *pełnomocnikiem ochrony*, *ex lege* odpowiadający za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

Pełnomocnikiem ochrony może być osoba, która posiada:

- obywatelstwo polskie,
- wykształcenie wyższe,
- odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne,
- zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Do zadań pełnomocnika ochrony należy:

- zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
- zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne,
- zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów,
- opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji,
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych,
- prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających,
- prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto
- przekazywanie odpowiednio ABW lub SKW do ewidencji danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.

W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli *„poufne”* lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie również odpowiednio ABW lub SKW.

5.Postępowanie sprawdzające

Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli *„poufne”* lub wyższej może nastąpić po uzyskaniu poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych. Z kolei dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli *„zastrzeżone”* może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych.

W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej „osobą sprawdzaną”, przeprowadza się:

- zwykłe postępowanie sprawdzające – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli *„poufne”*,
- poszerzone postępowanie sprawdzające: przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli *„tajne”* lub *„ściśle tajne”*, wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska, wobec kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli *„poufne”* lub wyższej oraz wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską. Wymienionym podmiotom wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana we wniosku lub poleceniu.

Na ten temat wypowiada się także literatura prawnicza. *Artykuł 22 ust. 1 pkt 1 i 2 u.o.i.n. wyróżnia dwa rodzaje postępowań sprawdzających – zwykłe i poszerzone. Pierwsze, mające charakter ograniczony, jest przeprowadzane przez pełnomocnika ochrony w odniesieniu do stanowisk i prac związanych z dostępem do informacji niejawnych o klauzuli „poufne”. Drugie, mające szerszy zakres podmiotowy i przedmiotowy, przeprowadzane jest w odniesieniu do stanowisk i prac związanych z dostępem do informacji niejawnych o klauzuli „tajne” lub „ściśle tajne”. Ten typ postępowania sprawdzającego ma także zastosowanie wobec pełnomocników ochrony, ich zastępców i kandydatów na te stanowiska oraz wobec kierowników jednostek organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej* **/M. Dela, Bezpieczeństwo osobowe jako element ochrony informacji niejawnych [w:] Wojskowy Przegląd Prawniczy, Warszawa 2015, s. 7/.** Innymi słowy, pełnomocnik ochrony przeprowadza zwykłe postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej. Agencja Bezpieczeństwa Wewnętrznego albo Służba Kontrwywiadu Wojskowego przeprowadzają poszerzone postępowania m. in. wobec kierowników jednostek organizacyjnych, kandydatów na te funkcje oraz względem administracji rządowej jako szerokiego katalogu podmiotów wymieniony w analizowanej ustawie.

Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. W ramach tej procedury ustala się, czy istnieją uzasadnione wątpliwości dotyczące:

- uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej,
- zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu,
- przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, albo współpracowała lub współpracuje z takimi partiami lub organizacjami,

- ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego, zwanej dalej „ankietą", lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych,
- wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji,
- niewłaściwego postępowania z informacjami niejawnymi, jeżeli: doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym, było to wynikiem celowego działania, stwarzało to realne zagrożenie ich nieuprawnionym ujawnieniem i nie miało charakteru incydentalnego lub dopuściła się tego osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej.

W toku poszerzonego postępowania sprawdzającego z kolei ustala się ponadto, czy istnieją wątpliwości dotyczące:

- poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody,
- informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac, związanych z dostępem do informacji niejawnych,
- uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

Organ prowadzący postępowanie sprawdzające, kierując się zasadami bezstronności i obiektywizmu, jest obowiązany do wykazania najwyższej staranności w toku prowadzonego postępowania sprawdzającego co do jego zgodności z przepisami ustawy.
Zwykłe postępowanie sprawdzające obejmuje:

- sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy
- sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

Poszerzone postępowanie sprawdzające obejmuje ponadto czynności takiej jak: rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami, przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej, sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa.

Przepisy ustawowe przewidują także możliwość zawieszenia postępowania sprawdzającego. Ma to miejsce w przypadku: trwającej powyżej 30 dni choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego, wyjazdu za granicę osoby sprawdzanej na okres przekraczający 30 dni, gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ, w szczególności w przypadku wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe lub gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego. Zawieszone postępowanie sprawdzające zostaje podjęte, jeżeli: ustąpiły przyczyny uzasadniające zawieszenie postępowania lub ujawniono okoliczności mogące stanowić podstawę do odmowy wydania poświadczenia bezpieczeństwa lub umorzenia postępowania sprawdzającego.

Postępowanie sprawdzające kończy się:

- wydaniem poświadczenia bezpieczeństwa,
- odmową wydania poświadczenia bezpieczeństwa,
- umorzeniem postępowania

Poświadczenie bezpieczeństwa jako akt administracyjny powinno zawierać: numer poświadczenia, podstawę prawną, wskazanie wnioskodawcy postępowania sprawdzającego, określenie organu, który przeprowadził postępowanie sprawdzające, datę i miejsce wystawienia, imię, nazwisko i datę urodzenia osoby sprawdzanej, określenie rodzaju przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp, stwierdzenie, że osoba sprawdzana daje rękojmię zachowania tajemnicy, termin ważności oraz imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające. W przypadku dostępu do informacji niejawnych objętych klauzulą *„poufne”* poświadczenie bezpieczeństwa wydaje się na okres 7 lat.

Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli nie zostaną usunięte wątpliwości względem braku dawania rękojmi zachowania tajemnicy (art. 24 ust. 2 ustawy) lub w trakcie poszerzonego postępowania sprawdzającego nie zostaną usunięte wątpliwości dotyczące sposobu życia (art. 24 ust. 3 ustawy). Co więcej, organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie, wywołuje wątpliwości, o których mowa w art. 24 ust. 2 i 3.

Decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać: podstawę prawną oraz uzasadnienie faktyczne i prawne, wskazanie wnioskodawcy postępowania sprawdzającego, określenie organu, który przeprowadził postępowanie sprawdzające, datę i miejsce wydania, imię, nazwisko i datę urodzenia osoby sprawdzanej, określenie rodzaju przeprowadzonego postępowania sprawdzającego, ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp, stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy, imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające, pouczenie o dopuszczalności i terminie wniesienia odwołania odpowiednio do Prezesa Rady Ministrów albo Szefa ABW lub Szefa SKW.

Normy ustawowe przewidują także instytucję umorzenia postępowania sprawdzającego mające zastosowanie w przypadku: śmierci osoby sprawdzanej, rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac, związanych z dostępem do informacji niejawnych, odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac, związanych z dostępem do informacji niejawnych lub gdy postępowanie z innej przyczyny stało się bezprzedmiotowe.

- uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia,
- stwierdza nieważność decyzji podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające.

Decyzja powinna zawierać w szczególności: oznaczenie organu, datę wydania, oznaczenie osoby sprawdzanej, powołanie podstawy prawnej, rozstrzygnięcie oraz uzasadnienie faktyczne i prawne, pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego oraz podpis, z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do jej wydania.

Co istotne, od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, w wyniku zwykłego postępowania sprawdzającego, osobie sprawdzanej co do zasady służy odwołanie odpowiednio do Szefa ABW lub Szefa SKW. Do postępowania odwoławczego prowadzonego przed Szefem ABW lub Szefem SKW stosuje się odpowiednio przepisy ustawy dotyczące postępowania odwoławczego prowadzonego przed Prezesem Rady Ministrów. Odwołanie do Szefa ABW lub Szefa SKW składa się za pośrednictwem pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające. Warto dodać, że osobie sprawdzanej przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie organu odwoławczego w terminie 30 dni od dnia doręczenia. Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym.

Podsumowanie

Podsumowując dotychczasowe spostrzeżenia warto przywołać poglądy doktryny. Zachowanie tajemnicy zarówno przez kierownictwo, jak i szeregowy personel wymaga jasnego i klarownego systemu klasyfikującego informacje jako tajne lub jawne, a także szeregującego dostęp do tych pierwszych. Pomimo coraz doskonalszych technologii zabezpieczeń, uwzględniających także ludzkie niedbalstwo czy wręcz bezmyślność, niemożliwe jest wyeliminowanie tzw. czynnika ludzkiego /P. Kocoń, Budowa świadomości informacji niejawnych wśród pracowników sądów [w:] Prace naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 487, Wrocław 2017 s. 161/. Taki stan rzeczy niewątpliwie wymusił potrzebę stworzenia regulacji prawnej dotyczącej ochrony informacji niejawnych. Nie tylko obszar administracji rządowej, ale także sfera administracji samorządowej została objęta niniejszym aktem prawnym. Powszechnie wydaje się, iż ze szczególnego rodzaju tajemnicami państwowymi mamy do czynienia w płaszczyźnie centralnego aparatu państwowego. Nie jest to jednak prawdą, bowiem już na szczeblu samorządu terytorialnego organy władzy publicznej dysponują dokumentami oraz materiałami mającymi znamienne znaczenie w perspektywie ochrony informacji niejawnych. Wśród przykładów informacji niejawnych objętych ochroną wymienia się: ankiety bezpieczeństwa osobowego związane z postępowaniem sprawdzającym, wnioski do Agencji Bezpieczeństwa Wewnętrznego w sprawie postępowań sprawdzających, roczne sprawozdania z akcji kurierskiej lub zadania z zakresu praw obronnych szczególnie w przypadku wprowadzenia stanu nadzwyczajnego. Powyższe sytuacje wymuszają konieczność inicjowania procedur objętych ustawą, głównie postępowań sprawdzających oraz kontrolnych postępowań sprawdzających. Badania społeczne pokazuję, *że małe samorządy najgorzej radzą sobie z ochroną informacji niejawnych – wynika z raportu Agencji Bezpieczeństwa Wewnętrznego. Zdaniem kontrolerów, głównym powodem jest brak odpowiednich środków na tworzenie kancelarii tajnej i zastosowanie właściwych środków bezpieczeństwa.*

Zdaniem kontrolerów, najsłabiej przepisy ustawy o ochronie informacji niejawnych wypełniają małe urzędy samorządowe. Jak przyznaje ABW, jest to związane głównie z problemem wygospodarowania odpowiednich środków na stworzenie pionu ochrony, organizację kancelarii tajnej i zastosowanie środków ochrony fizycznej zgodnych z obowiązującymi przepisami. Najistotniejsze uchybienia administracji lokalnej w zakresie organizacji ochrony informacji niejawnych dotyczyły powoływania na stanowisko pełnomocnika ochrony osób, które nie spełniały wszystkich wymagań (poświadczenie bezpieczeństwa i przeszkolenia z ochrony informacji niejawnych) oraz łączenia funkcji kierownika jednostki organizacyjnej z funkcją pełnomocnika ochrony. Urzędy nie dysponowały planami ochrony informacji niejawnych, stwierdzano także udostępnianie informacji niejawnych osobom, które nie posiadały poświadczeń bezpieczeństwa lub odpowiedniego upoważnienia. Nieprawidłowości dotyczyły również zastosowanych środków ochrony fizycznej. Zastrzeżenia najczęściej dotyczyły nie wydzielenia lub niewłaściwej organizacji strefy bezpieczeństwa, przechowywania dokumentów niejawnych w pomieszczeniach zlokalizowanych poza strefą bezpieczeństwa, braku stosownych certyfikatów lub świadectw kwalifikacyjnych urządzeń służących do zabezpieczenia informacji niejawnych oraz braku systemu sygnalizacji pożarowej oraz systemu sygnalizacji włamania i napadu w kancelarii tajnej. Informacje niejawne sporządzane były przy użyciu nieakredytowanych systemów teleinformatycznych. Samorządy rzadko też decydowały się na powoływanie osób odpowiedzialnych za bezpieczeństwo takiego oprogramowania (administratorów systemów lub inspektorów bezpieczeństwa teleinformatycznego). Niemal we wszystkich kontrolowanych urzędach stwierdzono naruszenia przepisów w zakresie prawidłowości prowadzenia zwykłych postępowań sprawdzających. Najczęściej brakowało pisemnego polecenia kierownika jednostki oraz weryfikacji w Centralnym Zarządzie Służby Więziennej lub w Krajowym Rejestrze Karnym. Jak podkreśla Agencja Bezpieczeństwa Wewnętrznego, o ile brak odpowiednich środków ochrony fizycznej można usprawiedliwiać trudnościami finansowymi, o tyle jej zdaniem nierzetelność w prowadzeniu ewidencji i udostępnianie dokumentów niejawnych osobom nieuprawnionym świadczy o nieznajomości przepisów lub ich świadomym nieprzestrzeganiu. Autorzy raportu przytaczają jednak także opinie samorządów, które wskazują na nieadekwatność przewidzianych przepisami rozwiązań w stosunku do ilości i klauzuli tajności przechowywanych dokumentów. Zwłaszcza, że obowiązujące przepisy obligują kierowników jednostek dysponujących chociażby jednym dokumentem oznaczonym klauzulą „poufne" do kosztochłonnego zorganizowania kancelarii tajnej, strefy administracyjnej i bezpieczeństwa. Efektem kontroli ABW było w sumie 91 wystąpień pokontrolnych oraz, w przypadku rażącego naruszenia przepisów lub podejrzenia przestępstwa, 15 zawiadomień do prokuratury. Raport nie precyzuje ile z nich dotyczyło samorządu terytorialnego **/https://samorzad.pap.pl/kategoria/prawo/jawne-niejawne-0/.**

W świetle wskazanych argumentów odnotować trzeba, że tematyka dotycząca ochrony informacji niejawnych w sferze samorządu terytorialnego nieustannie wymaga podejmowania dyskusji mającej na celu usuwanie wszelkich wątpliwości z zakresu wykładni przepisów prawa materialnego oraz niejasności w ramach procedowania prawnego. Niejednokrotnie dostrzega się bowiem, że kierownicy samorządowych jednostek organizacyjnych oraz pełnomocnicy ochrony traktują obszar ochrony informacji niejawnych bez należytej staranności oraz w sposób powierzchowny. Warto zatem podejmować działania programowe mogące niwelować negatywne skutki tych działań. Trzeba również zauważyć, że w przypadku naruszenia standardów ochrony informacji niejawnych racjonalny prawodawca wprowadził sankcje karne. Podstawę prawną stanowi ustawa z dnia 6 czerwca 1997 r. - Kodeks karny **/t. j. Dz. U. 2021 poz. 2345/**. Rozdział XXXIII zawiera przepisy dotyczące przestępstw przeciwko ochrony informacji. W myśl treści przepisu art. 265 § 1 k.k. kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „*tajne*" lub „*ściśle tajne*", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Wedle z kolei treści przepisu art. 266 § 2 k.k. funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3. Z tego względu przestrzeganie przepisów prawnych *de lege lata* ustawy o ochronie informacji niejawnych dotyka znamion prawa karnego oraz stanowi niezwykle ważny obszar regulacji normatywnej.

O AUTORZE

dr Mariusz Paradowski - Adoktor nauk prawnych, kwalifikacje III stopnia uzyskał na Wydziale Prawa, Administracji i Stosunków Międzynarodowych Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego w Krakowie. Dysertację doktorską pt. Pozwolenie budowlane napisał pod kierunkiem prof. zw. dra hab. Józefa Filipka. Był słuchaczem studiów podyplomowych z zakresu prawa, ekonomii i pedagogiki: w Warszawskiej Szkole Zarządzania – Szkole Wyższej w Warszawie, Wyższej Szkole Ekonomii i Innowacji w Lublinie, Politechnice Krakowskiej im. Tadeusza Kościuszki w Krakowie, Politechnice Częstochowskiej oraz Wyższej Szkole Zarządzania w Częstochowie. Studia magisterskie ukończył na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach.

Warszawa, marzec 2022
www.frdl.org.pl
Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
ul. Żurawia 43, 00-680 Warszawa