

OCHRONA INFORMACJI NIEJAWNYCH

Komentarz

redakcja naukowa Agnieszka Ziółkowska

Michał Cyndel, Dorota Fleszer, Paweł Gacek, Anna Gronkiewicz
Mariusz Jagielski, Grzegorz Krawiec, Grzegorz Łaszczyca
Andrzej Matan, Barbara Palenik, Ewa Pierzchała, Leszek Pietraszek
Olga Sitarz, Magdalena Strożek-Kucharska, Robert Suwaj
Dorota Sylwestrzak, Joanna Wyporska-Frankiewicz, Agnieszka Ziółkowska

KOMENTARZE PRAKTYCZNE

OCHRONA INFORMACJI NIEJAWNYCH

Komentarz

redakcja naukowa Agnieszka Ziółkowska

Michał Cyndel, Dorota Fleszer, Paweł Gacek, Anna Gronkiewicz
Mariusz Jagielski, Grzegorz Krawiec, Grzegorz Łaszczyca
Andrzej Matan, Barbara Palenik, Ewa Pierzchała, Leszek Pietraszek
Olga Sitarz, Magdalena Strożek-Kucharska, Robert Suwaj
Dorota Sylwestrzak, Joanna Wyporska-Frankiewicz, Agnieszka Ziółkowska

KOMENTARZE PRAKTYCZNE

Zamów książkę w księgarni internetowej

profinfo.pl
księgarnia internetowa

Stan prawny na 15 listopada 2023 r.

Recenzent

Dr hab. Agnieszka Piskorz-Ryń, prof. UKSW

Wydawczyni

Monika Pawłowska

Redaktor prowadzący

Paulina Staniszevska-Chudzik

Opracowanie redakcyjne

Agata Czuj

Projekt okładek serii

Wojtek Janikowski, Przemek Dębowski

Poszczególne artykuły skomentowali:

Dorota Fleszer – art. 1 ust. 1–2, art. 5 (poza ust. 1 pkt 7, ust. 2 pkt 4–6), art. 6, 8, 9

Paweł Gacek – art. 19–20, 72

Anna Gronkiewicz – art. 31–33

Mariusz Jagielski – art. 7, 73

Grzegorz Krawiec – art. 65–71

Grzegorz Łaszczycza – art. 3

Andrzej Matan – art. 38

Ewa Pierzchała – art. 22–28

Barbara Palenik, Michał Cyndel – art. 42–47

Leszek Pietraszek, Michał Cyndel – art. 10–18

Magdalena Strożek-Kucharska – art. 74–180 (pominięte), 181–191

Olga Sitarz – art. 5 ust. 1 pkt 7, art. 5 ust. 2 pkt 4

Robert Suwaj – art. 35–37, 39–41

Dorota Sylwestrzak – art. 2 pkt 1–2, 6–19, art. 4, 21, 34

Joanna Wyporska-Frankiewicz – art. 54–64

Agnieszka Ziółkowska – art. 1 ust. 3–5, art. 2 pkt 3–5, art. 5 ust. 2 pkt 5–6, art. 29–30, 48–53

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2024

ISBN 978-83-8358-279-5

Wolters Kluwer Polska Sp. z o.o.

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. +48 728 313 462

e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

Wstęp

Dostęp do informacji publicznej ma rangę konstytucyjną i wynika z art. 61 ust. 1 i 2 Konstytucji RP. Prawo to nie ma jednak charakteru absolutnego, na co wskazuje ust. 3 tego samego przepisu, zgodnie z którym ograniczenie prawa może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa, co pozostaje nadto w zgodzie z treścią art. 31 ust. 3 Konstytucji RP. Jednym z aktów prawnych ograniczających to prawo jest ustawa z 5.08.2010 r. o ochronie informacji niejawnych¹, co wynika z art. 5 ust. 1 u.d.i.p.

Rozwiązania prawne w zakresie ochrony informacji niejawnych mają swoją długowieczną tradycję², a pierwsze regulacje miały głównie charakter karny. Obecnie obowiązująca już 12 lat ustawa o ochronie informacji niejawnych zastąpiła tę pochodzącą z 22.01.1999 r. o takim samym tytule, która wzorowana na pochodzącym z 2.03.1955 r. dokumencie C-M(55)15 (Final) określającym politykę bezpieczeństwa Sojuszu Północnoatlantyckiego³ była dotknięta rozwiązaniami uznawanymi nie tylko za kontrowersyjne, lecz także sprzeczne z regulacją konstytucyjną⁴, zwłaszcza ze względu na nad-

¹ Dz.U. z 2023 r. poz. 756 ze zm.

² M. Ryszkowski, T. Zybala, *Rys historyczny działań z zakresu ochrony informacji niejawnych w Polsce do roku 1939* [w:] *X lat ustawy o ochronie informacji niejawnych 1999–2009. Materiały konferencyjne*, red. M. Gajos, Katowice 2009, s. 157–188; M. Leciak, *Karnoprawna ochrona informacji niejawnych. Uwagi w świetle ustawy z dnia 5.8.2010 r. o ochronie informacji niejawnych*, Toruń 2012, s. 17–66; A. Szymczak, *O systemie ochrony informacji niejawnych w Polsce w latach 1918–2011*, „Czasopismo Prawno-Historyczne” 2013/LXV/1, s. 467–502; R. Szałowski, *Informacje niejawne. Zagadnienia prawnoadministracyjne*, Częstochowa 2015, s. 11–21.

³ W dniu 17.06.2002 r. wydano nowy dokument regulujący politykę bezpieczeństwa – C-M(2002)49 „Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego”, wielokrotnie zmieniany. Niebawem istotne są przy tym dyrektywy wykonawcze, w tym: AC/35-D/2000 – dyrektywa bezpieczeństwa osobowego; AC/35-D/2001 – dyrektywa bezpieczeństwa fizycznego; AC/35-D/2002 – dyrektywa bezpieczeństwa obiegu informacji; AC/35-D/2003 – dyrektywa projektów niejawnych i bezpieczeństwa przemysłowego; AC/35-D/2004 – dyrektywa podstawowa INFOSEC; AC/35-D/2005 – dyrektywa zarządzania INFOSEC w systemach teleinformatycznych.

⁴ S. Hoc, *Geneza ustawy o ochronie informacji niejawnych* [w:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VI Kongresu*, red. M. Gajos, Katowice 2010, s. 35; R. Szałowski, *Uwagi w zakresie przedmiotowym tajemnicy służbowej*, „Ius Novum” 2009/1, s. 35 i n.; M. Leciak, *Definicja*

mierne ograniczenie konstytucyjnego prawa dostępu do informacji publicznej oraz niemożność zaskarżenia rozstrzygnięcia kończącego postępowanie sprawdzające do sądu administracyjnego⁵. Ponadto wskazywano na wymóg nadawania klauzul ogromnej ilości informacjom, częste przypadki ich zawyżania przy jednoczesnym lekceważeniu wykazów zawartych w załącznikach do ustawy, brak skutecznej procedury w przypadku zawyżenia lub zaniżenia klauzul tajności. Podkreślano niemający praktycznego znaczenia podział na informacje państwowe i służbowe.

Mimo tego oraz kilku nowelizacji ustawy⁶ zmieniających ją niemal w połowie dopiero po 10 latach, w 2009 r., Prezes RM zobowiązał ówczesnego Sekretarza Kolegium do spraw Służb Specjalnych do podjęcia działań zmierzających do przygotowania projektu nie tyle nowelizacji, ile nowej ustawy ze względu na rozmiar i charakter zmian. W rezultacie uzgodnień i konsultacji 16.02.2010 r.⁷ do Sejmu wpłynął projekt, który z założenia miał ważyć z jednej strony potrzebę stworzenia maksymalnie efektywnego, prostego i elastycznego systemu ochrony informacji niejawnych, a z drugiej konieczność gwarantowania odpowiedniego stopnia ich bezpieczeństwa. *Ratio legis* miała być także potrzeba zbliżenia rozwiązań krajowych do unormowań wypracowanych zarówno w NATO, Unii Europejskiej, jak i w krajach europejskich. Przejawem tego zbliżenia stało się między innymi wprowadzenie jednej krajowej władzy bezpieczeństwa, zniesienie postępowań sprawdzających wobec osób, które mają mieć dostęp do informacji z klauzulą „zastrzeżone”. Istotą nowej ustawy stało się nadto rozszerzenie odpowiedniego stosowania przepisów Kodeksu postępowania administracyjnego w postępowaniach sprawdzających. Do katalogu uproszczeń wprowadzonych nową ustawą w szczególności należy zaliczyć: zniesienie obowiązku prowadzenia kancelarii tajnej w jednostkach organizacyjnych przetwarzających informacje z klauzulą „poufne”, dopuszczenie możliwości organizacji jednej kancelarii tajnej dla wielu jednostek organizacyjnych, zniesienie obowiązku użytkowania świadectw bezpieczeństwa przemysłowego przez przedsiębiorców wykonujących działalność gospodarczą osobiście, dopuszczalność jednorazowego i tymczasowego dostępu przedsiębiorcy do informacji niejawnych. Za istotne ustawodawca uznał także uwzględnienie zmieniającej się rzeczywistości technologicznej wykorzystywanej w procesie ochrony i przepływu informacji niejawnych, zwłaszcza w zakresie środków łączności, a w konsekwencji systemów teleinformatycznych.

legalna tajemnicy państwowej i tajemnicy służbowej w świetle przepisów Konstytucji RP, „Studia Iuridica Toruniensia” 2009/IV, s. 79 i n.; zob. też uchwała TK z 13.06.1994 r., W 3/94, OTK 1994/1, poz. 26.

⁵ Zob. wyrok TK z 10.05.2000 r., K 21/99, OTK ZU 2000/4, poz. 109.

⁶ Ustawę nowelizowano 23 razy, w tym m.in. ustawą z 21.01.2000 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz.U. Nr 12, poz. 136), ustawą z 3.02.2001 r. o zmianie ustawy o ochronie informacji niejawnych (Dz.U. Nr 22, poz. 247); ustawą z 24.08.2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. Nr 123, poz. 1353); ustawą z 15.04.2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw (Dz.U. Nr 85, poz. 727).

⁷ Rządowy projekt ustawy o ochronie informacji niejawnych oraz o zmianie niektórych ustaw, druk nr 2791, Sejm VI kadencji, <http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/2791> (dostęp: 29.01.2023 r.).

Ustawa o ochronie informacji niejawnych została uchwalona 5.08.2010 r. i weszła w życie trzy miesiące po jej ogłoszeniu, 2.01.2011 r.; obowiązuje z wieloma przepisami wykonawczymi, do których należą:

- rozporządzenie Prezesa Rady Ministrów z 22.12.2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności⁸;
- rozporządzenie Prezesa Rady Ministrów z 4.10.2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa⁹;
- rozporządzenie Prezesa Rady Ministrów z 27.04.2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych¹⁰;
- rozporządzenie Prezesa Rady Ministrów z 7.12.2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego¹¹;
- rozporządzenie Ministra Obrony Narodowej z 19.12.2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych¹²;
- rozporządzenie Prezesa Rady Ministrów z 9.07.2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego¹³;
- rozporządzenie Prezesa Rady Ministrów z 28.12.2010 r. w sprawie wzorów poświadczeń bezpieczeństwa¹⁴;
- rozporządzenie Prezesa Rady Ministrów z 28.12.2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa¹⁵;
- rozporządzenie Prezesa Rady Ministrów z 28.12.2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa¹⁶;
- rozporządzenie Prezesa Rady Ministrów z 7.12.2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne¹⁷;

⁸ Dz.U. Nr 288, poz. 1692.

⁹ Dz.U. Nr 220, poz. 1302.

¹⁰ Dz.U. Nr 93, poz. 541.

¹¹ Dz.U. poz. 2334.

¹² Dz.U. z 2022 r. poz. 322 ze zm.

¹³ Dz.U. poz. 1256.

¹⁴ Dz.U. z 2015 r. poz. 220 ze zm.

¹⁵ Dz.U. Nr 258, poz. 1753.

¹⁶ Dz.U. Nr 258, poz. 1754.

¹⁷ Dz.U. Nr 271, poz. 1603.

- rozporządzenie Prezesa Rady Ministrów z 20.07.2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego¹⁸;
- rozporządzenie Prezesa Rady Ministrów z 20.07.2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego¹⁹;
- rozporządzenie Ministra Obrony Narodowej z 29.09.2022 r. w sprawie trybu oceny i sposobu dopuszczania rozwiązań informatycznych, w których mają być przetwarzane informacje niejawne²⁰;
- rozporządzenie Prezesa Rady Ministrów z 9.07.2020 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego²¹;
- rozporządzenie Prezesa Rady Ministrów z 13.01.2021 r. w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających²²;
- rozporządzenie Rady Ministrów z 16.05.2019 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego²³.

Zagwarantowanie ochrony informacjom niejawnym stanowi istotny element zachowania ciągłości działania państwa i jego istotnych interesów, zarówno zewnętrznych, jak i międzynarodowych. Komentowana ustawa wraz z aktami wykonawczymi stanowi zbiór regulacji stanowiących system metod i sposobów prawnych, administracyjno-organizacyjnych, fizycznych i technicznych pozwalających chronić informacje przed nieuprawnionym wyjawieniem. *Ratio legis* ustawy jest zatem zabezpieczenie dobra państwa *sensu largo*, polegające na zachowaniu w tajemnicy informacji chronionych.

Niniejszy komentarz stanowi próbę przedstawienia problematyki ochrony informacji niejawnych uregulowanej w ustawie o ochronie informacji niejawnych z uwzględnieniem poglądów doktryny reprezentowanej przez przedstawicieli prawa administracyjnego, postępowania administracyjnego, postępowania sądownoadministracyjnego, konstytucyjnego oraz prawa karnego z licznych ośrodków naukowych w kraju, a także reprezentantów praktyki – funkcjonariuszy Policji oraz byłych funkcjonariuszy ABW. Stanowiska i tezy prezentowane w komentarzu wyrażają poglądy poszczególnych autorów.

Komentarz odnosi się do stanu prawnego na dzień 15.11.2023 r.

¹⁸ Dz.U. Nr 156, poz. 926.

¹⁹ Dz.U. Nr 159, poz. 948.

²⁰ Dz.U. poz. 2098.

²¹ Dz.U. poz. 1236.

²² Dz.U. poz. 84.

²³ Dz.U. poz. 1103.

Ustawa

z dnia 5 sierpnia 2010 r.

o ochronie informacji niejawnych

(Dz.U. z 2023 r. poz. 756; zm. Dz.U. z 2023 r. poz. 2030 i 1532)

ROZDZIAŁ 1

Przepisy ogólne

Art. 1. [Zakres stosowania ustawy]

1. 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”, to jest zasady:

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

2. Przepisy ustawy mają zastosowanie do:

- 1) organów władzy publicznej, w szczególności:
 - a) Sejmu i Senatu,
 - b) Prezydenta Rzeczypospolitej Polskiej,
 - c) organów administracji rządowej,
 - d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
 - e) sądów i trybunałów,
 - f) organów kontroli państwowej i ochrony prawa;

- 2) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
- 3) Narodowego Banku Polskiego;
- 4) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych;
- 5) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;
- 6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych, z zastrzeżeniem art. 5.

4. Do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych.

5. Do danych osobowych stanowiących informacje niejawne stosuje się przepisy niniejszej ustawy.

1. Celem przepisów ustawy o ochronie informacji niejawnych było zabezpieczenie dobra państwa, polegające na zachowaniu w tajemnicy informacji chronionych¹ przez stworzenie warunków do adekwatnego i efektywnego stosowania instytucji związanych z ochroną informacji niejawnych². Ich funkcjonowanie jest powiązane z fundamentalnymi interesami bezpieczeństwa państwa, co bezpośrednio wpływa na zasady organizacji całego systemu ochrony (legalizm, obiektywizm, bezstronność, ograniczoność dostępu, hierarchiczność organów ochrony, kontrola, instancyjność, pierwszeństwo informacji niejawnych)³. Na ich gruncie miał być zorganizowany system ochrony informacji niejawnych, który, po pierwsze, byłby systemem wszechstronnym, kompletnym w tym znaczeniu, że uwzględniałby kluczowe elementy ochrony informacji niejawnych. Po drugie, byłby systemem efektywnym, skutecznym. Jednocześnie, po trzecie, miał to być system w swej organizacji cechujący się „prostotą i elastycznością funkcjonowania, lecz bez uszczerbku dla bezpieczeństwa informacji niejawnych”⁴. Mowa tu o klasyfikowaniu informacji niejawnych, organizowaniu ochrony informacji niejawnych, przetwarzaniu informacji niejawnych, postępowaniu sprawdzającym, prowadzonym w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki ochrony informacji niejawnych, organizacji kontroli stanu zabezpieczenia informacji

¹ Wyrok WSA w Warszawie z 27.04.2019 r., II SA/Wa 2543/19, LEX nr 3058988.

² P. Ostojski, *Ochrona praw jednostki w administracyjnym postępowaniu sprawdzającym*, PPP 2018/12, s. 81 i podana tam literatura.

³ R. Zapart, *Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji*, „Polityka i Społeczeństwo” 2020/3(18), s. 114 i podana tam literatura.

⁴ P. Ostojski, *Ochrona praw jednostki...*, s. 81 i podana tam literatura.

niejawnych, ochrony informacji niejawnych w systemach teleinformatycznych oraz stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

2. Legalna definicja informacji niejawnych została zawarta w ust. 1 komentowanego przepisu. Ze sposobu jej sformułowania należy wywieść wnioski, że opiera się ona na następujących elementach konstrukcyjnych. Po pierwsze, informacja jest uznana za informację niejawną ze względu na jej treść i skutek związany z ich nieuprawnionym ujawnieniem⁵. Idąc dalej, nie jest możliwa sytuacja, w której informacja, nie będąc informacją niejawną, podlegałaby ochronie takiej, jak informacje niejawne⁶. Po drugie, dla zakwalifikowania danej informacji jako informacji niejawnej wystarczy stwierdzenie elementu materialnego, tzn. istnienie takiej jej cechy, przez którą stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłyby z punktu widzenia jej interesów niekorzystne, także w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania⁷. Nie ma tutaj znaczenia charakter tej szkody – może to być zarówno szkoda majątkowa (uszczerbek materialny lub osiągnięty zysk), jak i niemajątkowa (np. osłabienie prestiżu czy zaufania do państwa), o jakiej mowa na gruncie regulacji Kodeksu cywilnego i Kodeksu karnego. Szkoda ta może być także utożsamiana z powstaniem zagrożenia dla wypełniania przez podmioty zobowiązane obowiązków w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej⁸. W związku z powyższym postulowane jest w doktrynie stosowanie wykładni celowościowej przepisów ustawy o ochronie informacji niejawnych. W oparciu o nią powinno dochodzić do ustalenia, czy ujawnienie żądanych informacji może zagrozić interesom państwa, porządkowi prawnemu, bezpieczeństwu funkcjonariuszy albo bezpieczeństwu prowadzonych przez nich operacji⁹. Po trzecie, do uznania, że dana informacja publiczna stanowi prawnie chronioną informację niejawną, nie jest konieczne opatrzenie jej jedną z klauzul przewidzianych przez art. 5 u.o.i.n.¹⁰ Zaznaczyć przy tym należy, że brak wymogu nadania informacji klauzuli tajności nie oznacza jednak zakazu posługiwania się wyznaczonymi w tej regulacji wytycznymi kwalifikowania okreś-

⁵ D. Fleszer, *Informacja niejawna i jej klasyfikacja*, PPH 2014/8, s. 23.

⁶ R. Szałowski, *Uwagi o ustawowej regulacji zakresu przedmiotowego informacji niejawnych*, „Administracja. Teoria. Dydaktyka. Praktyka” 2017/1, s. 12–35.

⁷ T. Szewc, *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007, s. 115–117; por. wyrok NSA z 21.09.2012 r., I OSK 1393/12, LEX nr 1363604; wyrok NSA z 8.03.2017 r., I OSK 1777/15, LEX nr 2338895; wyrok NSA z 6.07.2017 r., I OSK 932/16, LEX nr 2375583; wyrok NSA z 24.04.2018 r., I OSK 1422/16, LEX nr 2592324.

⁸ J. Wyporska-Frankiewicz, E. Jarzęcka-Siwik, *Informacje niejawne [w:] Dostęp do informacji publicznej w praktyce jednostek samorządu terytorialnego*, red. J. Wyporska-Frankiewicz, Warszawa 2019, s. 145.

⁹ Wyrok NSA z 1.10.2010 r., I OSK 1149/10, LEX nr 1611994.

¹⁰ T. Szewc, *Ochrona informacji...*, s. 115–117; por. wyrok NSA z 21.09.2012 r., I OSK 1393/12, LEX nr 1363604; wyrok NSA z 8.03.2017 r., I OSK 1777/15, LEX nr 2338895; wyrok NSA z 6.07.2017 r., I OSK 932/16, LEX nr 2375583; wyrok NSA z 24.04.2018 r., I OSK 1422/16, LEX nr 2592324.

lonej informacji jako informacji niejawnej¹¹, bo są one bardzo przydatne¹². Przyjmuje się bowiem, że zakres informacji uznawanych za informacje niejawne wyznacza art. 1 w zw. z art. 5 u.o.i.n.¹³ Inaczej zależność wymienionych regulacji można ująć w ten sposób – element materialny określa art. 1 ust. 1 u.o.i.n., wskazujący na możliwość powstania określonej szkody czy zagrożenia dóbr, natomiast element formalny wyraża się w nadanej klauzuli tajności zgodnie z art. 5 u.o.i.n. Klauzulę tajności można nadać tylko informacjom niejawnym w znaczeniu materialnym¹⁴. Po czwarte, dla zakwalifikowania informacji jako informacji niejawnych istotna jest nie tylko treść informacji, lecz także skutek ich nieuprawnionego ujawnienia¹⁵. Jest ono bezprawne, jeżeli informacja posiadająca atrybut tajności zostanie przekazana poza krąg osób prawnie do niej dopuszczonych lub wówczas, gdy zostanie pozbawiona tego atrybutu wbrew obowiązкови dyskrekcji¹⁶. Podkreślić trzeba, że czynność „ujawnienia” musi być tutaj interpretowana szeroko, z położeniem nacisku na powstanie skutku, jakim będzie zapoznanie się z informacją osoby nieupoważnionej. „Ujawnienie to uczynienie jawnym tego, co dotychczas jawne nie było. Działanie takie ma charakter jednorazowy – osoba ujawniająca informację niejawną czyni ją jawną dla kolejnych odbiorców. Forma czy sposób ujawnienia mogą być różne – wypowiedź ustna, udostępnienie pisma zawierającego informacje niejawne, okazanie dokumentu lub przedmiotu, opublikowanie w masowych środkach przekazu, przekazanie informacji klasyfikowanych za pośrednictwem technicznych środków przekazu, np. telefonu, faksu”¹⁷. Forma ujawnienia informacji niejawnych nie ma tutaj znaczenia – „może być także znak lub gest”¹⁸.

3. Posługiwanie się definicją informacji niejawnej w oparciu o elementy materialne wskazane w ust. 1 komentowanego przepisu nie oznacza braku możliwości wykorzystania w ramach wykładni systemowej innych norm regulujących ochronę informacji niejawnych, wręcz przeciwnie. Nie może być to jednak utożsamiane z przyzwoleniem na dowolne, swobodne uznawanie informacji jako niejawnych. Na przykład według art. 39 ust. 1 ustawy o SKW oraz SWW w związku z wykonywaniem swoich zadań SKW i SWW zapewniają ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy tych służb. Według Naczelnego Sądu Administracyjnego przepis ten nie wprowadza odrębnej, w stosunku do ust. 1 komentowanego przepisu, kategorii informacji niejawnych, ale wskazuje informacje związane z działalnością obu służb, które spełniają kryteria z komentowanego przepisu. Są to informacje o środkach, formach i metodach realizacji zadań,

¹¹ Wyrok NSA z 6.09.2016 r., I OSK 210/15, LEX nr 2143005.

¹² Wyrok NSA z 6.09.2016 r., I OSK 210/15, LEX nr 2143005.

¹³ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej a ochrona informacji niejawnych. Zagadnienia wybrane*, ZNSA 2016/4(67), s. 38–39.

¹⁴ Wyrok NSA z 6.07.2017 r., I OSK 932/16, LEX nr 2375583.

¹⁵ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 38–39.

¹⁶ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 37–38 i podana tam literatura.

¹⁷ D. Fleszer, *Informacja niejawna...*, s. 21.

¹⁸ Wyrok SN z 17.03.1971 r., III KR 260/70, LEX nr 18292.

zgrupowanych informacjach oraz własnych obiektach i danych identyfikujących funkcjonariuszy tych służb. Ochrona tych informacji, jak stanowi we wstępie art. 39 ust. 1 ustawy o SKW oraz SWW, występuje „w związku z wykonywaniem swoich zadań”. Zadania SKW zostały zdefiniowane w art. 1 i 5 ustawy o SKW oraz SWW. Służba Kontrwywiadu Wojskowego jest służbą specjalną, właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej (art. 1 ustawy o SKW oraz SWW). Zadania z zakresu obronności i bezpieczeństwa państwa zostały skonkretyzowane w jej art. 5 (np. art. 5 pkt 4, 5, 7). Informacje wymienione w art. 39 ust. 1 ustawy o SKW oraz SWW stanowią informacje niejawne nie tylko zatem z uwagi na objęcie ich dodatkową ochroną przewidzianą w przepisach tej ustawy, lecz także z tego względu, że wyczerpują pojęcie informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej. Ponadto zakwalifikowanie informacji z zakresu ochrony obronności i bezpieczeństwa państwa, jako tych, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej, wynika wprost z brzmienia art. 1 ust. 1 wyłożonego z zastosowaniem katalogu z art. 5 u.o.i.n. W tym sensie przepis art. 39 ust. 1 ustawy o SKW oraz SWW powinien być powiązany z regulacjami ustawy o ochronie informacji niejawnych¹⁹. W innym orzeczeniu Naczelny Sąd Administracyjny uznał za nieuprawnione ujawnienie informacji w zakresie technicznych możliwości śledzenia połączeń telefonicznych oraz komunikacji w sieci Internet za pomocą słów kluczowych, ponieważ spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne. Regulacja zawarta w komentowanym przepisie pozwala uznać takie informacje za podlegające reżimowi przewidzianemu dla ochrony informacji niejawnych, bez względu na to, czy takiej informacji nadano klauzulę tajności. Udostępnienie tych informacji byłoby zagrożeniem realnym, stanowiącym możliwość wyrządzenia określonej w ustawie o ochronie informacji niejawnych szkody. Powyższe dane pozwalają bowiem na sformułowanie wniosków dotyczących nie tylko kierunków zainteresowań CBA, lecz przede wszystkim realnych możliwości tej służby. Skoro CBA jest służbą specjalną do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa, to poznanie używanych przez nie metod i środków technicznych z dużym prawdopodobieństwem zagroziłoby realizacji ustawowych zadań. Informacja niejawna chroniona jest bez względu na to, czy osoba uprawniona do jej nadania uznała za stosowne oznaczyć ją odpowiednią klauzulą. Jest ona niejawna z uwagi na zagrożenia wynikające z jej treści, a nie wyniku klasyfikacji. Na tę postać ochrony informacji niejawnych wskazuje art. 7 ust. 1 u.o.i.n.²⁰ (zob. komentarz). Za informacje niejawne należy traktować notatki urzędowe dotyczą-

¹⁹ Wyrok NSA z 28.04.2016 r., I OSK 2620/14, LEX nr 2081157; wyrok NSA z 6.09.2016 r., I OSK 210/15, LEX nr 2143005.

²⁰ Wyrok NSA z 18.08.2015 r., I OSK 1679/14, LEX nr 1984363; wyrok NSA z 6.07.2017 r., I OSK 932/16, LEX nr 2375583.

ROZDZIAŁ 2

Klasyfikowanie informacji niejawnych

Art. 5. [Rodzaje klauzul tajności, zasady nadawania]

1. Informacjom niejawnym nadaje się klauzulę „ściśle tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) zagrazi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- 2) zagrazi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- 3) zagrazi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- 4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
- 5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrazi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- 6) zagrazi lub może zagrazić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- 7) zagrazi lub może zagrazić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz.U. z 2015 r. poz. 21), albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych.

2. Informacjom niejawnym nadaje się klauzulę „tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;

- 2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- 3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- 4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- 5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- 6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

3. Informacjom niejawnym nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- 2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- 3) zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- 4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- 5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- 6) zagrazi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- 7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

4. 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.

5. Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem posiadanej klauzuli tajności.

1. Cechą charakteryzującą informacje niejawne jest ich formalizm. Związany jest on z opatrzeniem oznaczonej informacji niejawnej klauzulą tajności. Klasyfikowanie informacji niejawnej oznacza przyznanie tej informacji jednej z klauzul tajności¹. Jeśli dokument (materiał) nie zostanie opatrzony stosowną klauzulą, to trudno mówić o niejawności

¹ Wyrok WSA w Warszawie z 9.02.2012 r., II SA/Wa 2451/11, LEX nr 1121569.

informacji. Nie można domniemywać niejawności, skoro w ustawie są zdefiniowane zasady, procedury i skutki utajniania konkretnej informacji².

Warto w tym miejscu podkreślić, że w orzecznictwie ugruntowane zostało stanowisko, zgodnie z którym niejawny charakter informacji wynika z jej cech materialnych, a nie z tego, czy została poddana procedurze określonej w art. 5 u.o.i.n.³ Informacja jest bowiem niejawna z uwagi na zagrożenia wynikające z jej treści, a nie w wyniku klasyfikacji⁴. Informacja jest niejawna – o czym była mowa w komentarzu do art. 1 u.o.i.n. – ze względu na jej treść. Oznaczenie jej odpowiednią klauzulą tajności jest tylko wskazówką dla odbiorcy do właściwej jej ochrony przed nieuprawnionym ujawnieniem czy zniszczeniem⁵, a samo nadanie klauzuli nie decyduje o konieczności ochrony. Informacja ze względu na swą treść i skutki, jakie wiąże się z jej ujawnieniem, nawet bez klauzuli, może być uznana za niejawną i stanowić informację publiczną⁶.

Konsekwencją dokonanej klasyfikacji informacji niejawnej przez wykładnię przesłańek określonych w art. 5 u.o.i.n. jest nadanie tej informacji określonej klauzuli tajności. Klauzulę tę w sposób właściwy należy nanieść na dokument lub materiał. Zanim jednak ta czynność zostanie wykonana, informacja musi zostać oceniona i na jej podstawie musi zostać dokonany dobór odpowiedniej klauzuli tajności, czyli inaczej – musi być przeprowadzona czynność klasyfikowania informacji niejawnych⁷. Podsumowując, klasyfikowanie informacji niejawnych ma charakter dwustopniowy. Najpierw następuje zaliczenie materiału do kategorii informacji niejawnych, później dopiero do określonego stopnia ochrony. Ten drugi etap tego procesu jest następstwem uznania określonej informacji za informację niejawną⁸.

2. Norma art. 5 u.o.i.n., pomimo rezygnacji z wykazów informacji stanowiących tajemnicę państwową, które istniały pod rządami ustawy o ochronie informacji niejawnych

² P. Fajgielski, *Informacja w administracji publicznej – prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007, s. 144–145.

³ Wyrok NSA z 21.09.2012 r., I OSK 1393/12, LEX nr 1363604; wyrok NSA z 18.08.2015 r., I OSK 1679/14, LEX nr 1984363; wyrok NSA z 28.04.2016 r., I OSK 2620/14, LEX nr 2081157; A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 37 i podana tam literatura; P. Burzyński, *Tajemnica państwowa jako przedmiot ochrony regulacji prawnokarnej*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2002/1, s. 24; wyrok NSA z 6.09.2016 r., I OSK 210/15, LEX nr 2143005. Odmienne T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 117–118, oraz wyrok WSA w Warszawie z 9.02.2012 r., II SA/Wa 2451/11, LEX nr 1121569.

⁴ Wyrok NSA z 21.09.2012 r., I OSK 1393/12, LEX nr 1363604; wyrok NSA z 18.08.2015 r., I OSK 1679/14, LEX nr 1984363; wyrok NSA z 6.09.2016 r., I OSK 210/15, LEX nr 2143005; wyrok WSA w Warszawie z 6.10.2016 r., II SA/Wa 885/16, LEX nr 2158781.

⁵ Wyrok NSA z 21.09.2012 r., I OSK 1393/12, LEX nr 1363604; wyrok WSA w Warszawie z 16.11.2015 r., II SA/Wa 1171/15, LEX nr 1957661; wyrok NSA z 9.10.2017 r., I OSK 1822/16, LEX nr 2461535; wyrok WSA w Warszawie z 11.09.2014 r., II SA/Wa 723/14, LEX nr 1553168; wyrok WSA w Warszawie z 8.01.2020 r., II SA/Wa 1385/19, LEX nr 3078853.

⁶ J. Wyporska-Frankiewicz, E. Jarzęcka-Siwik, *Informacje niejawne...*, s. 145.

⁷ T. Szewc, *Publicznoprawna ochrona...*, s. 117–118.

⁸ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 43 i podana tam literatura.

W komentarzu autorzy omówili zagadnienia dotyczące m.in.:

- klasyfikowania i przetwarzania informacji niejawnych,
- organizacji ochrony informacji niejawnych,
- bezpieczeństwa osobowego,
- kancelarii tajnych i środków bezpieczeństwa fizycznego,
- bezpieczeństwa teleinformatycznego,
- bezpieczeństwa przemysłowego.

Autorzy wyjaśniają wątpliwości, które mogą pojawić się w związku ze stosowaniem przepisów komentowanej ustawy, i formułują szereg postulatów *de lege ferenda*, które wymagają dostrzeżenia przez ustawodawcę.

Publikacja przeznaczona jest dla praktyków – adwokatów i radców prawnych, jak również pracowników administracji rządowej i samorządowej, a także specjalistów zajmujących się kwestią bezpieczeństwa i obronności państwa.

„Od strony merytorycznej komentarz analizuje problematykę ochrony informacji niejawnej w sposób praktyczny przy pełnym poszanowaniu warsztatu naukowego. Na uwagę zasługuje dobór autorów publikacji. (...) Jest to pierwszy komentarz na rynku napisany w większości przez prawników administratywistów, co wyraźnie wpływa na jego wysoką ocenę.”

Dr hab. Agnieszka Piskorz-Ryń, prof. UKSW

Agnieszka Ziółkowska – doktor habilitowana nauk prawnych; profesor Uniwersytetu Śląskiego w Katowicach w Zespole Badawczym Postępowania Administracyjnego i Sądowo-administracyjnego na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach, radca prawny, autorka i współautorka licznych opracowań naukowych z zakresu prawa administracyjnego, postępowania administracyjnego i sądownictwa administracyjnego.



9788383582795 W01P01

Kup e-book i czytaj
w aplikacji Smarteca

ISBN 978-83-8358-279-5



9 788383 582795

ZAMÓWIENIA:

INFOLINIA: +48 801 044 545

ZAMOWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL

