

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

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 Łaszczyca – 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

Spis treści

Wykaz skrótów	9
Wstęp	13
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.....	17
Rozdział 1. Przepisy ogólne	19
Art. 1. [Zakres stosowania ustawy]	19
Art. 2. [Definicje pojęć]	28
Art. 3. [Odpowiednie stosowanie K.P.A.]	43
Art. 4. [Udostępnienie informacji]	49
Rozdział 2. Klasyfikowanie informacji niejawnych.....	58
Art. 5. [Rodzaje klauzul tajności, zasady nadawania]	58
Art. 6. [Upoważnienie do nadania klauzuli, czas ochrony]	74
Art. 7. [Dane podlegające ochronie, wyjątki]	85
Art. 8. [Udostępnienie informacji tajnych]	90
Art. 9. [Zmiana klauzuli tajności]	93
Rozdział 3. Organizacja ochrony informacji niejawnych	97
Art. 10. [Zadania ABW i SKW]	97
Art. 11. [Wykonywanie funkcji krajowej władzy bezpieczeństwa przez Szefa ABW]	99
Art. 12. [Uprawnienia funkcjonariuszy ABW i SKW]	101
Art. 13. [Zasady współdziałania kierowników jednostek organizacyjnych ze służbami i instytucjami uprawnionymi]	105
Art. 14. [Podmioty odpowiadające za ochronę informacji: kierownik jednostki organizacyjnej i pełnomocnik ochrony]	107
Art. 15. [Zadania pełnomocnika ochrony. Pion ochrony]	110
Art. 16. [Wymagania stawiane pracownikom pionu ochrony]	113
Art. 17. [Postępowanie w razie stwierdzenia naruszenia przepisów o ochronie informacji]	114

Art. 18.	[Delegacja do określenia szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych]	115
Rozdział 4. Szkolenie w zakresie ochrony informacji niejawnych		117
Art. 19.	[Szkolenie, cel i przeprowadzenie]	117
Art. 20	[Zaświadczenie stwierdzające odbycie szkolenia]	124
Rozdział 5. Bezpieczeństwo osobowe		127
Art. 21.	[Dopuszczenie do pracy, warunki]	127
Art. 22.	[Postępowanie sprawdzające]	131
Art. 23.	[Postępowanie sprawdzające]	132
Art. 24.	[Cel postępowania sprawdzającego]	135
Art. 25.	[Zakres postępowania zwykłego]	139
Art. 26.	[Zakres postępowania poszerzonego]	141
Art. 27.	[Zawieszenie postępowania]	143
Art. 28.	[Zakończenie postępowania]	145
Art. 29.	[Poświadczenie bezpieczeństwa]	146
Art. 30.	[Odmowa wydania poświadczenia bezpieczeństwa]	151
Art. 31.	[Umorzenie postępowania]	159
Art. 32.	[Kolejne postępowanie sprawdzające]	161
Art. 33.	[Kontrolne postępowanie sprawdzające]	164
Art. 34.	[Wyłączenie przeprowadzenia postępowania sprawdzającego]	170
Rozdział 6. Postępowanie odwoławcze i skargowe, wznowienie postępowania		179
Art. 35.	[Odwołanie]	179
Art. 36.	[Postanowienie i decyzja Prezesa RM]	184
Art. 37.	[Odwołanie od decyzji pełnomocnika, Szefa ABW lub SKW]	190
Art. 38.	[Postępowanie sądowoadministracyjne w sprawie skargi na rozstrzygnięcie organu odwoławczego]	191
Art. 39.	[Wznowienie postępowania]	196
Art. 40.	[Decyzje organu]	199
Art. 41.	[Odwołanie od decyzji o odmowie wznowienia postępowania]	200
Rozdział 7. Kancelarie tajne. Środki bezpieczeństwa fizycznego		203
Art. 42.	[Obowiązek utworzenia kancelarii tajnej]	203
Art. 43.	[Organizacja pracy kancelarii]	207
Art. 44.	[Inne komórki organizacyjne]	210
Art. 45.	[Zakres zastosowania środków bezpieczeństwa]	211
Art. 46.	[Zabezpieczenie informacji „poufnych”]	213
Art. 47.	[Delegacja dla RM]	215

Rozdział 8. Bezpieczeństwo teleinformatyczne	220
Art. 48. [Akredytacja systemu teleinformatycznego]	220
Art. 49. [Dokument szczególnych wymagań bezpieczeństwa]	227
Art. 50. [Certyfikacja]	231
Art. 51. [Obowiązek akredytacji bezpieczeństwa teleinformatycznego, wyłączenia]	236
Art. 52. [Inspektor bezpieczeństwa teleinformatycznego, wyznaczenie i szkolenie]	240
Art. 53. [Opłaty]	244
Rozdział 9. Bezpieczeństwo przemysłowe	248
Art. 54. [Dostęp przedsiębiorcy do informacji niejawnych]	248
Art. 55. [Świadectwa potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych]	253
Art. 56. [Wniosek o wydanie świadectwa]	256
Art. 57. [Sprawdzenie przedsiębiorcy i postępowania sprawdzające wobec innych osób]	259
Art. 58. [Kwestionariusz bezpieczeństwa przemysłowego]	262
Art. 59. [Termin zakończenia postępowania bezpieczeństwa przemysłowego]	264
Art. 60. [Wyłączenie wymogu zatrudnienia pełnomocnika ochrony oraz utworzenia pionu ochrony w przypadku ubiegania się o świadectwo bezpieczeństwa przemysłowego trzeciego stopnia]	266
Art. 61. [Zwrot zryczałtowanych kosztów ponoszonych przez ABW i SKW za przeprowadzenie postępowania bezpieczeństwa przemysłowego]	267
Art. 62. [Umorzenie postępowania bezpieczeństwa przemysłowego]	269
Art. 63. [Zawieszenie lub podjęcie postępowania bezpieczeństwa przemysłowego]	270
Art. 64. [Zakończenie postępowania. Przesłanki odmowy wydania świadectwa]	272
Art. 65. [Postępowanie sprawdzające]	274
Art. 66. [Cofnięcie świadectwa]	277
Art. 67. [Dokumenty; wymogi formalne]	280
Art. 68. [Delegacja dla RM]	288
Art. 69. [Skarga do sądu administracyjnego]	290
Art. 70. [Obowiązek informacyjny]	295
Art. 71. [Instrukcja bezpieczeństwa przemysłowego]	298
Rozdział 10. Ewidencje i udostępnianie danych oraz akt postępowania sprawdzających, kontrolnych postępowania sprawdzających i postępowania bezpieczeństwa przemysłowego	302
Art. 72. [Udostępnianie akt postępowania sprawdzającego]	302
Art. 73. [Ewidencja osób]	309
Rozdział 11. Zmiany w przepisach obowiązujących	313
Art. 74–180. (pominięte)	313

Rozdział 12. Przepisy przejściowe i końcowe	314
Art. 181. [Obowiązek przeprowadzenia przeglądu materiałów]	314
Art. 182. [Zachowanie ważności poświadczenia bezpieczeństwa]	316
Art. 183. [Stosowanie art. 14 ust. 3 pkt 2]	317
Art. 184. [Kancelarie tajne, obowiązek informacyjny]	318
Art. 185. [Ważność akredytacji systemów teleinformatycznych]	319
Art. 186. [Ważność świadectw bezpieczeństwa przemysłowego]	320
Art. 187. [Obowiązek uzyskania świadectwa]	321
Art. 188. [Stosowanie przepisów dotychczasowych]	322
Art. 189. [Obowiązywanie przepisów wykonawczych]	323
Art. 190. [Derogacja]	328
Art. 191. [Wejście w życie]	329
Bibliografia	331
O autorach	343

Wykaz skrótów

Akty prawne

k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2022 r. poz. 1138 ze zm.)
k.k.w.	– ustawa z 6.06.1997 r. – Kodeks karny wykonawczy (Dz.U. z 2023 r. poz. 127 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2023 r. poz. 1465)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775 ze zm.)
k.p.c.	– ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2023 r. poz. 1550 ze zm.)
k.p.k.	– ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2022 r. poz. 1375 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm. i sprost.)
ord. pod.	– ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2022 r. poz. 2651 ze zm.)
p.p.s.a.	– ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2023 r. poz. 1634 ze zm.)
p.u.s.a.	– ustawa z 25.07.2005 r. o ustroju sądów administracyjnych (Dz.U. z 2022 r. poz. 2492 ze zm.)
p.u.s.p.	– ustawa z 27.07.2001 r. o ustroju sądów powszechnych (Dz.U. z 2023 r. poz. 217 ze zm.)
p.u.s.w.	– ustawa z 21.08.1997 r. – Prawo o ustroju sądów wojskowych (Dz.U. z 2022 r. poz. 2250)
pr. przeds.	– ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. z 2023 r. poz. 221 ze zm.)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 ze zm.)

RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 4.05.2016 r., s. 1)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 83 z 30.03.2010 r., s. 13)
u.d.i.p.	– ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.i.n.	– ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756 ze zm.)
u.o.i.n. z 1999 r.	– ustawa z 22.01.1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631 ze zm.), uchylona
u.o.O.	– ustawa z 11.03.2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 2305 ze zm.)
u.o.p.p.ś.	– ustawa z 28.11.2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz.U. z 2015 r. poz. 21 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.u.i.g.	– ustawa z 9.04.2010 r. o udostępnianiu informacji gospodarczej i wymianie danych gospodarczych (Dz.U. z 2023 r. poz. 2160 ze zm.)
ustawa o ABW oraz AW	– ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2023 r. poz. 1136 ze zm.)
ustawa o CBA	– ustawa z 9.06.2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2022 r. poz. 1900 ze zm.)
ustawa o NIK	– ustawa z 23.12.1994 r. o Najwyższej Izbie Kontroli (Dz.U. z 2022 r. poz. 623)
ustawa o Policji	– ustawa z 6.04.1990 r. o Policji (Dz.U. z 2023 r. poz. 171 ze zm.)
ustawa o SKW oraz SWW	– ustawa z 7.06.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2023 r. poz. 81 ze zm.)
ustawa o SN	– ustawa z 8.12.2017 r. o Sądzie Najwyższym (Dz.U. z 2023 r. poz. 1093 ze zm.)
ustawa o SW	– ustawa z 9.04.2010 r. o Służbie Więziennej (Dz.U. z 2023 r. poz. 1683 ze zm.)

Periodyki

FK	– Finanse Komunalne
GSP	– Gdańskie Studia Prawnicze

IAP	– Informacja w Administracji Publicznej
Mon. Praw.	– Monitor Prawniczy
OMT	– Organizacja – Metodyka – Technika
ONSAiWSA	– Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkiego Sądu Administracyjnego
OSNKW	– Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNwSK	– Orzecznictwo Sądu Najwyższego w Sprawach Karnych
OTK	– Orzecznictwo Trybunału Konstytucyjnego
PiP	– Państwo i Prawo
PiZS	– Praca i Zabezpieczenie Społeczne
PPC	– Polski Proces Cywilny
PPH	– Przegląd Prawa Handlowego
PPP	– Przegląd Prawa Publicznego
PS	– Przegląd Sądowy
RPEiS	– Ruch Prawniczy, Ekonomiczny i Socjologiczny
WPP	– Wojskowy Przegląd Prawniczy
ZNSA	– Zeszyty Naukowe Sądownictwa Administracyjnego

Trybunał i sądy

NSA	– Naczelny Sąd Administracyjny
SN	– Sąd Najwyższy
TK	– Trybunał Konstytucyjny
WSA	– wojewódzki sąd administracyjny

Organy

ABW	– Agencja Bezpieczeństwa Wewnętrznego
AW	– Agencja Wywiadu
CBA	– Centralne Biuro Antykorupcyjne
KIO	– Krajowa Izba Odwoławcza
SG	– Straż Graniczna
SKW	– Służba Kontrwywiadu Wojskowego
SOP	– Służba Ochrony Państwa
SW	– Służba Więzienna
SWW	– Służba Wywiadu Wojskowego
UODO	– Urząd Ochrony Danych Osobowych
ŻW	– Żandarmeria Wojskowa

Inne

SWB	– dokument szczególnych wymagań bezpieczeństwa
-----	--

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. Zybała, *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 nie-
możność 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 znacze-
nia 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 rezul-
tacie 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 gwaran-
towania 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 „zastrze-
żone”. Istotą nowej ustawy stało się nadto rozszerzenie odpowiedniego stosowania prze-
pisów 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 uzy-
skiwania świadectw bezpieczeństwa przemysłowego przez przedsiębiorców wykonują-
cych działalność gospodarczą osobiście, dopuszczalność jednorazowego i tymczasowe-
go 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/V, 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 sądowoadministracyjnego, 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 wnioszek, 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 byłoby 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.

zgromadzonych 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.

ce telefonicznych rozmów przeprowadzonych przez przywódców dwóch państw: Polski i Rosji. Polityka zagraniczna prowadzona na forum międzynarodowym wymaga wielu różnorodnych instrumentów o różnym stopniu oficjalności. Stosunki międzynarodowe są też kształtowane przez kontakty szefów rządów poszczególnych państw, co jest związane ze ścisłym przestrzeganiem protokołu dyplomatycznego. Kontakty takie z natury rzeczy wymagają zaufania i dyskrecji, trudno bowiem przyjąć, że partnerzy takich rozmów i spotkań w sposób domniemany godzą się na ujawnienie ich treści. Ponadto są ważnym narzędziem polityki zagranicznej i wymagają dla swojej skuteczności wzajemnego zaufania i wiarygodności. Przy ujawnianiu treści takich rozmów mogłaby powstać wątpliwość, czy Polska, jako kraj, akceptuje te wartości, co z pewnością mogłoby utrudnić prowadzenie bieżącej polityki zagranicznej²¹.

Objęcie ochroną informacji niejawnych następuje już na etapie ich wytworzenia i ma miejsce niezależnie od formy i sposobu ich wyrażania²². Nośnikami informacji niejawnych mogą być dokument lub materiał. Według definicji legalnej zawartej w art. 2 pkt 3 u.o.i.n. dokumentem jest każda utrwalona informacja niejawna. Natomiast materiałem jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia (por. komentarz do art. 2 ust. 4).

Obok informacji niejawnych wyróżnić można kategorię quasi-informacji niejawnych. Są to informacje, które nie są informacjami niejawnymi i nie mieszczą się w definicji wynikającej z komentowanego przepisu. Ustawodawca zagwarantował im jednak analogiczny poziom ochrony jak informacjom niejawnym, wskazując w normie prawnej klauzulę tajności, jaka jest nadawana określonej grupie informacji z mocy prawa. Wyodrębnienie tej kategorii informacji ma istotne znaczenie dla procesu odmowy dostępu do informacji publicznej. Wobec tej grupy informacji zakres ochrony wynika z przepisów prawa, a nie jest następstwem oceny skutków ich udostępnienia. Nie bada się więc *in concreto*, czy nieuprawnione ujawnienie wywoła lub może wywołać szkodę dla interesów Rzeczypospolitej Polskiej albo może być z punktu widzenia jej interesów niekorzystne. Analizy ryzyka dokonał bowiem w tym przypadku *in abstracto* sam ustawodawca²³.

Większość informacji niejawnych to informacje publiczne. Związane są one z realizacją zadań publicznych oraz ze sposobem korzystania ze środków publicznych. Zaznaczyć tutaj trzeba, że są jednak informacje publiczne o szczególnym charakterze ze względu na konsekwencje ich nieuprawnionego ujawnienia, które są szczególnie ekspozowane w treści ust. 1 komentowanego przepisu. Nie jest to jednak czynnik, który miałby wpływ

²¹ Wyrok NSA z 26.03.2013 r., I OSK 2863/12, LEX nr 1332343.

²² J. Wyporska-Frankiewicz, E. Jarzęcka-Siwik, *Informacje niejawne*, s. 144; A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 37.

²³ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 38–39 i podana tam literatura.

na pozbawienie tych informacji przymiotu informacji publicznych. Wręcz przeciwnie, konstruowane są na gruncie ustawy o ochronie informacji niejawnych w sposób specyficzny i wszechstronnie zmierzają do ich ochrony, a tym samym dostęp do nich nie jest powszechny. W doktrynie problematyka relacji między informacjami niejawnymi a informacjami publicznymi doczekała się jednak bardziej pogłębionej analizy. W jej rezultacie wyznaczono dwie kategorie informacji niejawnych. Do pierwszej grupy zaliczono informacje niejawne, które ze względu na skutek ich nieuprawnionego ujawnienia wywołają lub mogą wywołać szkodę dla Rzeczypospolitej, a jednocześnie nie mają bezpośredniego (lub w ogóle żadnego) związku z wykonywaniem zadań publicznych przez organy władzy publicznej. Mowa tu na przykład o informacjach, których nieuprawnione ujawnienie doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności. W tej grupie informacji ujęto także informacje dotyczące życia prywatnego, w tym rodzinnego, które jednak mogą prowadzić do identyfikacji takich osób, a co za tym idzie – zagrozić bezpieczeństwu wykonywanych przez nie czynności. Natomiast do drugiej grupy zaliczono informacje niejawne, do których nie ma zastosowania ustawa o dostępie do informacji publicznej ze względu na ich formę. Zapewnia ona dostęp do informacji niezależnie od form jej utrwalenia, natomiast nie zakłada dostępu do przedmiotu albo dowolnej jego części, która jest objęta ochroną w trybie właściwym dla informacji niejawnych. Szczególnie jest to widoczne wobec traktowania jako informacji niejawnej urządzenia, wyposażenia lub broni wyprodukowanej albo będącej w trakcie produkcji, a także składników użytych do ich wytworzenia. Trzecia grupa to informacje niejawne, do których ustawa o dostępie do informacji publicznej nie ma zastosowania ze względu na zakres podmiotowy tego aktu prawnego. Zakres podmiotów zobowiązanych do stosowania ustawy o ochronie informacji niejawnych i ustawy o dostępie do informacji publicznej jest porównywalny, ale nie identyczny. Są podmioty, które nie zostały objęte obowiązkiem stosowania przepisów o dostępie do informacji publicznej. Mowa tutaj o przedsiębiorcach, którzy nie wykonują zadań publicznych lub nie gospodarują majątkiem publicznym²⁴.

Zakres podmiotowy ustawy o ochronie informacji niejawnych wyznaczony został w ust. 2 komentowanego przepisu. Z jego konstrukcji wynika, że katalog podmiotów zobowiązanych do stosowania ustawy o ochronie informacji niejawnych, choć taksonomicznie wymieniony, to jednak faktycznie uzależniony jest od wykonywania zadań publicznych lub realizacji posiadanych kompetencji, w ramach których niezbędne jest posiadanie dostępu do informacji niejawnych. Tak ustalona metodologia wyznaczania kręgu podmiotów objętych obowiązkiem przestrzegania rygorów ustawy o ochronie informacji niejawnych jest widoczna zwłaszcza w jej art. 1 ust. 2 pkt 1. Obejmuje

²⁴ A. Piskorz-Ryń, J. Wyporska-Frankiewicz, *Dostęp do informacji publicznej...*, s. 40, za: D. Chromicka, *Struktura regulacji ochrony informacji niejawnych [w:] Jawność i jej ograniczenia*, red. G. Szpor, t. IV, *Znaczenie orzecznictwa*, red. M. Jaśkowska, Warszawa 2014, s. 156 i n.

ona co do istoty wszystkie organy władzy publicznej, a użyte w tej regulacji wyrażenie „w szczególności” wskazujące na rodzaje organów, które ponad wszelką wątpliwość do stosowania ustawy o ochronie informacji niejawnych są zobligowane, tylko tę zasadę potwierdza. Wynika to także chociażby ze stanowiska NSA wyrażonego w wyroku z 6.11.2020 r., w którym ustalał, czy Centrum Eksperckie Kontrwywiadu NATO jest podmiotem zobowiązanym do stosowania ustawy o ochronie informacji niejawnych. W jego ocenie brak jest podstaw do przyjęcia, że Centrum to stanowi jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną, o której mowa w art. 1 ust. 2 pkt 2 u.o.i.n. Centrum Eksperckie Kontrwywiadu NATO nie zostało również wymienione w żadnym z załączników do kolejnych decyzji Ministra Obrony Narodowej w sprawie wykazu jednostek organizacyjnych mu podległych lub przez niego nadzorowanych, obowiązujących w czasie podpisania oraz po podpisaniu Memorandum o porozumieniu dotyczącym utworzenia, administracji i działania Centrum Eksperckiego Kontrwywiadu NATO²⁵.

Uwaga ta dotyczy także podmiotów uwzględnionych w ust. 2 pkt 2 oraz pkt 4–5 komentowanego przepisu. Zauważyć przy tym należy, że niewątpliwie objęte zakresem podmiotowym ust. 2 pkt 2 komentowanego przepisu są jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, wymienione w obwieszczeniu Ministra Obrony Narodowej z 26.05.2023 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych²⁶.

Zwrócić należy uwagę na ust. 2 pkt 6 komentowanego przepisu, który zobowiązuje do stosowania ustawy o ochronie informacji niejawnych wobec 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. Przepis ten umożliwia podjęcie odpowiednich przygotowań przez przedsiębiorców planujących w przyszłości realizować zadania lub umowy związane z dostępem do informacji niejawnych²⁷.

4. Ustawodawca zastrzegł, że przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych (ust. 3 komentowanego przepisu). W ten sposób została wprowadzona norma kolizyjna. W konsekwencji należy przyjąć, że wszędzie tam, gdzie konkretne sprawy będące tajemnicą uregulowane są inaczej w ustawie szczególnej dotyczącej tajemnicy zawodowej lub innej prawnie chronionej i stosowania obu tych ustaw nie da się pogodzić, pierwszeństwo mają przepisy ustawy szczególnej.

²⁵ Decyzja Ministra Obrony Narodowej nr 394/MON z 7.10.2015 r., Dz.Urz. MON poz. 282; decyzja Ministra Obrony Narodowej nr 408/MON z 4.12.2015 r., Dz.Urz. MON poz. 329; decyzja Ministra Obrony Narodowej nr 63/MON z 14.03.2016 r., Dz.Urz. MON poz. 38.

²⁶ M.P. z 2023 r. poz. 590.

²⁷ S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, art. 1.

Ponadto wprowadzona konstrukcja prawna pozwala wyodrębnić trzy grupy tajemnic: podlegające reżimowi ustawy o ochronie informacji niejawnych, podlegające ochronie jako stanowiące tajemnicę zawodową oraz inne tajemnice podlegające ochronie prawnej.

Zauważyć należy, że tajemnica zawodowa to informacja uzyskana w związku z wykonywanym zawodem (np. radca prawny, adwokat²⁸, lekarz, pielęgniarka, dziennikarz, rzeczoznawca, doradca podatkowy), a obowiązek jej zachowania wynika zarówno z przepisów powszechnych regulujących te zawody, jak i z kodeksów deontologicznych. Ponadto należy podkreślić, że wyrażenie „tajemnica prawnie chroniona” nie zostało zdefiniowane przez ustawodawcę. W orzecznictwie sądowym podkreśla się, że powinien on być wykładany ściśle, z każdorazowym poszukiwaniem wyraźnej deklaracji ustawodawcy co do zakwalifikowania określonego rodzaju informacji jako informacji objętej tajemnicą ustawowo chronioną²⁹.

5. W zakresie danych osobowych, które pojawiają się na przykład w związku z prowadzeniem postępowań sprawdzających, wolą ustawodawcy, jeżeli stanowią jednocześnie informacje niejawne, pierwszeństwo ma ustawa o ochronie informacji niejawnych, zaś przepisów o ochronie danych osobowych nie stosuje się (ust. 4 i 5 komentowanego przepisu). Regulacja zawarta w ust. 4 i 5 komentowanego przepisu jest konsekwencją wprowadzenia ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości³⁰, a zwłaszcza art. 3 pkt 2, zgodnie z którym przepisów ustawy nie stosuje się do ochrony danych osobowych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych ABW, AW, SKW, SWW oraz CBA.

Wyłączenie, o którym mowa w ust. 4 komentowanego przepisu, występowało w poprzedniej regulacji ustawy o ochronie informacji niejawnych. Podkreślenia wymaga, że ma ono charakter generalny (*generalis exclusio*). Bez znaczenia przy tym pozostaje zatem to, czy problem ochrony danych osobowych został uregulowany przez prawodawcę w ustawie z 10.05.2018 r. o ochronie danych osobowych (dostosowującej prawny porządek krajowy do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO)) czy ustawie z 14.12.2018 r. o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości³¹ wydanej na podstawie dyrektywy unijnej 2016/680 z 27.04.2016 r.

²⁸ Zob. np. Ł. Błaszczak, *Problem tajemnicy zawodowej adwokata i radcy prawnego a dowód z zeznań świadka w procesie cywilnym*, „Palestra” 2019/7–8, s. 155–177; T. Niedziński, *Tajemnica zawodowa radców prawnych oraz ich niezależność*, „Radca Prawny” 2022/2(31), s. 83–93.

²⁹ Zob. uzasadnienie wyroku WSA w Warszawie z 3.06.2015 r., II SA/Wa 140/15, LEX nr 1730949; wyrok NSA z 10.01.2014 r., I OSK 2075/13, LEX nr 1456978.

³⁰ Dz.U. 2023 r. poz. 1206 ze zm.

³¹ Dz.U. z 2023 r. poz. 1206.

traktującej o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości³² (tzw. dyrektywa policyjna). Rozważania dotyczące relacji tych uregulowań oraz trudności związane ze stosowaniem dyrektywy policyjnej wynikające ze sposobu jej implementacji przekraczają ramy komentarza.

Wspomnieć jedynie należy, że przez dane osobowe należy rozumieć informacje, które spełniają dwie kumulatywne przesłanki: po pierwsze, informacja jest o osobie fizycznej, a po drugie, osoba ta jest zidentyfikowana lub możliwa do zidentyfikowania. Ochrona danych osobowych wiąże się z ochroną życia prywatnego, a zatem stanowi o wolności obywatela (zob. też komentarz do art. 7).

Art. 2. [Definicje pojęć]

W rozumieniu ustawy:

- 1) jednostką organizacyjną – jest podmiot wymieniony w art. 1 ust. 2;
- 2) rękojmią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- 3) dokumentem – jest każda utrwalona informacja niejawna;
- 4) materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
- 5) przetwarzaniem informacji niejawnych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
- 6) systemem teleinformatycznym – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344);
- 7) dokumentem szczególnych wymagań bezpieczeństwa – jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;
- 8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;
- 9) dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej

³² Dz.Urz. UE L 119 z 4.05.2016 r., s. 89.

eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;

- 10) akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
- 11) certyfikacją – jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;
- 12) audytem bezpieczeństwa systemu teleinformatycznego – jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;
- 13) przedsiębiorcą – jest przedsiębiorca w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. z 2023 r. poz. 221) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa;
- 14) kierownikiem przedsiębiorcy – jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy – cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę; w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;
- 15) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
- 16) szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka;
- 17) zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;
- 18) zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie;
- 19) rozwiązaniem informatycznym – jest urządzenie lub zespół urządzeń, oprogramowanie, narzędzie lub usługa informatyczna umożliwiająca przetwarzanie informacji niejawnych w postaci elektronicznej, eksploatowana lub planowana do wdrożenia wyłącznie w jednostkach organizacyjnych wskazanych w art. 10 ust. 2.

1. W komentowanym przepisie uregulowano „słowniczek”, który zawiera legalne definicje pojęć, którymi posługuje się ustawodawca na potrzeby stosowania komentowanej

ustawy. Przepis ten pełni rolę porządkującą, ale także odgrywa istotną rolę z punktu widzenia wykładni przepisów komentowanej ustawy. Ustawodawca w celu nadania jednolitego znaczenia danego określenia i ustalenia jego zakresu stosowania zdecydował na uregulowanie legalnych definicji pojęć. Definicje te odnoszą się do ustawy oraz aktów wykonawczych wydanych na podstawie tej ustawy. Przepis zawiera 19 definicji pojęć używanych w komentowanej ustawie. Nie mają one charakteru uniwersalnego, obowiązującego dla innych aktów prawnych. Mają one natomiast charakter wiążący i muszą być rozumiane tak, jak ustawodawca je określił na potrzeby stosowania komentowanej ustawy.

Najważniejsze nowelizacje komentowanego przepisu dotyczyły między innymi definicji przedsiębiorcy³³. W art. 2 zmianie uległ pkt 13 definiujący pojęcie przedsiębiorcy. Zmiana ta związana była z dostosowaniem definicji przedsiębiorcy przyjętej w ustawie – Prawo przedsiębiorców³⁴. Zmiana ta weszła w życie z dniem 30.04.2018 r. Kolejna zmiana polegała na dodaniu w art. 2 pkt 19 odnoszącego się do pojęcia „rozwiązania informatycznego”³⁵ w brzmieniu przyjętym na gruncie ustawy o obronie ojczyzny. Przyjęte rozwiązanie odnośnie do definiowania pojęć, polegające na zastosowaniu odesłania do ustaw, w których zdefiniowano pojęcia „system teleinformatyczny” i „przedsiębiorca”, ma na celu „zapewnienie spójności systemowej w polskim porządku prawnym”³⁶.

2. Pojęcie jednostki organizacyjnej nie ma definicji legalnej w prawie polskim. W świetle Kodeksu cywilnego ustawodawca, definiując pojęcie osób prawnych, zalicza do nich jednostki organizacyjne, którym przepisy szczególne przyznają osobowość prawną (art. 33 k.c.)³⁷. W doktrynie prawa cywilnego i orzecznictwie³⁸ jednostka organizacyjna ujmowana jest jako „twór społeczny, przejawiający się w postaci zorganizowanej formy działalności ludzkiej”³⁹. Pojęcie jednostki organizacyjnej jest także przedmiotem zainteresowania w nauce prawa administracyjnego i rozważane było w odniesieniu do

³³ Zmiana art. 2 pkt 13 na mocy art. 137 pkt 1 ustawy z 6.03.2018 r. – Przepisy wprowadzające ustawę – Prawo przedsiębiorców oraz inne ustawy dotyczące działalności gospodarczej (Dz.U. poz. 650), która weszła w życie 30.04.2018 r. Ostatnia nowelizacja – Dz.U. z 2023 r. poz. 221.

³⁴ Art. 4 ust. 1 i 2 pr. przedś., zgodnie z którym przedsiębiorcą jest osoba fizyczna, osoba prawna lub jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną, wykonująca działalność gospodarczą, a ponadto wspólnicy spółki cywilnej w zakresie wykonywanej przez nich działalności gospodarczej.

³⁵ Art. 2 pkt 19 dodany na mocy art. 749 u.o.O., która weszła w życie 23.04.2022 r.

³⁶ I. Stankowska, *Komentarz do art. 2 [w:] I. Stankowska, Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2014, LEX/el.

³⁷ Szerzej M. Dziurda, *Komentarz do art. 33 [w:] Kodeks cywilny. Komentarz*, t. I, Część ogólna, cz. 1 (art. 1–55⁴), red. J. Gudowski, Warszawa 2021, LEX/el.

³⁸ Uchwała SN z 26.01.1996 r., III CZP 111/95, LEX nr 23809.

³⁹ G. Gorczyński, *Komentarz do art. 33 [w:] Kodeks cywilny. Komentarz*, t. I, Część ogólna (art. 1–125), red. M. Fras, M. Habdas, Warszawa 2018, LEX/el.; J. Frąckowiak, *Jednostka organizacyjna jako substrat osoby prawnej i ustawowej [w:] Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, red. L. Ogiełło, W. Popiołek, M. Szpunar, Kraków 2005, s. 901 i n.

jednostek organizacyjnych samorządu terytorialnego⁴⁰, państwowych jednostek organizacyjnych⁴¹ czy wdrażania rozporządzenia ogólnego o ochronie danych osobowych⁴².

W komentowanej ustawie również nie zawarto definicji legalnej określającej, jakie cechy posiada jednostka organizacyjna. Ustawodawca posłużył się zabiegiem legislacyjnym polegającym na wskazaniu tych podmiotów, które posiadają status jednostki organizacyjnej, odsyłając do przepisu art. 1 ust. 2 u.o.i.n. (zob. komentarz do tego przepisu). W rozumieniu komentowanej ustawy jednostką organizacyjną są: organy władzy publicznej, w szczególności: Sejm, Senat, Prezydent RP, organy administracji rządowej, organy jednostek samorządu terytorialnego, a także inne podległe im jednostki organizacyjne lub przez nie nadzorowane, sądy i trybunały, organy kontroli państwowej i ochrony prawa, jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, NBP, państwowe osoby prawne i inne niż wymienione w pkt 1–3 art. 1 ust. 2 u.o.i.n. państwowe jednostki organizacyjne, jednostki organizacyjne podległe organom władzy publicznej lub nadzorowane przez te organy, przedsiębiorcy zamierzający ubiegać się albo ubiegający się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujący takie umowy albo wykonujący na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych. Zdaniem niektórych przedstawicieli doktryny katalog podmiotów zobowiązanych do ochrony informacji niejawnych ma charakter zamknięty⁴³. Analiza treści przepisu pozwala na przyjęcie, że na gruncie komentowanej ustawy definicja jednostki organizacyjnej obejmuje szeroki krąg podmiotów, bez względu na formę własnościową oraz organizacyjną⁴⁴. Zaliczyć należy do nich zarówno podmioty publiczne (organy władzy ustawodawczej, wykonawczej i sądowniczej), jak i podmioty prawa prywatnego (przedsiębiorcy). Jednostką organizacyjną w świetle komentowanej ustawy będą zatem zarówno osoby fizyczne, osoby prawne, jak i jednostki organizacyjne nieposiadające osobowości prawnej, którym przepisy szczególne przyznają osobowość prawną, oraz inne jednostki organizacyjne.

3. Przez pojęcie rękojmi zachowania tajemnicy ustawodawca rozumie zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych

⁴⁰ A. Szewc, *O pojęciu „jednostka organizacyjna” w polskim prawie samorządu terytorialnego*, RPEiS 2005/3, s. 105–111; B. Dolnicki, *Gminne jednostki organizacyjne a jednostki organizacyjne gminy*, GSP 2015/XXXIV, s. 67–87.

⁴¹ M. Dziurda, *Szczególna zdolność sądowa organów państwowych oraz państwowych jednostek organizacyjnych nieposiadających osobowości prawnej*, PPC 2010/1, s. 37 i n.

⁴² M. Czerniawski, *Zakres terytorialny a pojęcie „jednostki organizacyjnej” w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu*, Mon. Praw. 2016/20, Legalis/el.; M. Sakowska-Baryła, *Wdrażanie RODO w jednostce organizacyjnej – niezbędne obszary analizy*, FK 2018/5, s. 46–58.

⁴³ M. Chomycz-Śmigielka, *Bezpieczeństwo państwa a ochrona informacji niejawnych* [w:] *Współczesne problemy prawa publicznego i prywatnego*, red. A. Zoll, Z. Cwiakalski, K. Eckhardt, J. Posłuszny, A. Witkowski, Rzeszów 2020, s. 45.

⁴⁴ B. Opaliński, *Komentarz do art. 2* [w:] Ł. Nosarzewski, B. Opaliński, P. Szustakiewicz, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2023, Legalis/el.

przed ich nieuprawnionym ujawnieniem, stwierdzoną w wyniku przeprowadzenia postępowania sprawdzającego.

W ujęciu potocznym pojęcie rękojmi zdefiniowane jest jako „poręczenie, zagwarantowanie czegoś, zapewnienie o czymś, przyrzeczenie czegoś”⁴⁵. Ustawodawca w odniesieniu między innymi do zawodów zaufania publicznego (np. radców prawnych⁴⁶, adwokatów⁴⁷, notariuszy⁴⁸) czy podjęcia prowadzenia działalności gospodarczej reglamentowanej (np. prowadzenie apteki ogólnodostępnej)⁴⁹ bądź wykonywania obowiązków (np. wykonywanie obowiązków egzaminatora)⁵⁰ jako jedną z przesłanek warunkujących nabycie stosownych uprawnień do wykonywania zawodu lub świadczenia usług, prowadzenia działalności, wprowadza wobec kandydatów obowiązek wykazania „dawania rękojmi”, nie definiując jednakże tego pojęcia. W orzecznictwie sądów administracyjnych przez pojęcie rękojmi rozumie się oprócz wiedzy zweryfikowanej „taki zespół cech charakteru i zachowań w sferze zawodowej i prywatnej, które składają się na wizerunek osoby, na której nie ciążyą żadne zarzuty podważające jej wiarygodność”⁵¹. Przyjmuje się także, że pojęcie rękojmi obejmuje dwa elementy: „cechy charakteru i dotychczasowe zachowanie osoby”⁵². Dawanie rękojmi definiuje się jako „całość cech, zdarzeń i okoliczności dotyczących wykonywania danego zawodu, składających się na jego wizerunek jako zawodu zaufania publicznego. Na pojęcie rękojmi składają się takie cechy, jak: szlachetność, prawość, uczciwość osoby wykonującej ten zawód”⁵³. Z kolei przez pojęcie rękojmi należytego wykonywania obowiązków egzaminatora rozumie się „całokształt jego cech charakteru i właściwości osobistych egzaminatora, których suma daje gwarancję, że będzie on wykonywał swoje obowiązki rzetelnie i bezstronnie. Rękojmię może zatem zapewniać jedynie osoba bez istotnych wad, która gwarantuje należyte wykonywanie swoich obowiązków poprzez gwarancję posiadania zarówno odpowiednich kwalifikacji zawodowych, jak i odpowiednich predyspozycji etycznych-moralnych. Przy ocenie zatem »rękojmi należytego wykonywania obowiązków« liczy się dotychczasowa postawa kandydata, która wespół z osiągniętymi kwalifikacjami zawodowymi winna dawać przekonanie o należyтым wykonywaniu przezeń swoich obowiązków. W szczególności cechy osobiste kandydata, potwierdzone jego dotychczasowym postępowaniem, winny wykluczać obawy o jego uczciwość, wiarygodność, rzetelność i obiektywizm”⁵⁴.

⁴⁵ <https://sjp.pwn.pl/szukaj/r%C4%99kojmia.html> (dostęp: 23.04.2023 r.).

⁴⁶ Art. 24 ust. 1 pkt 5 ustawy z 6.07.1982 r. o radcach prawnych (Dz.U. z 2022 r. poz. 1166 ze zm.).

⁴⁷ Art. 65 pkt 1 ustawy z 26.05.1982 r. – Prawo o advokaturze (Dz.U. z 2022 r. poz. 1184 ze zm.).

⁴⁸ Art. 11 pkt 2 ustawy z 14.02.1991 r. – Prawo o notariacie (Dz.U. z 2022 r. poz. 1799 ze zm.).

⁴⁹ Art. 101 pkt 4 ustawy z 6.09.2001 r. – Prawo farmaceutyczne (Dz.U. z 2022 r. poz. 2301 ze zm.).

⁵⁰ Art. 58 ust. 1 pkt 8 ustawy z 5.01.2011 r. o kierujących pojazdami (Dz.U. z 2023 r. poz. 622 ze zm.).

⁵¹ Zob. wyroki NSA z: 2.06.2022 r., II GSK 261/19, LEX nr 3395998; 1.12.2016 r., II GSK 1117/15, LEX nr 2295021. Zob. też P. Kaczmarek, *O rękojmi prawidłowego wykonywania zawodu adwokata oraz radcy prawnego*, PPP 2015/1, s. 19–28.

⁵² Zob. wyrok NSA (do 31.12.2003 r.) w Warszawie z 5.04.2001 r., II SA 725/00, LEX nr 53476.

⁵³ Zob. wyrok WSA w Warszawie z 27.07.2016 r., VI SA/Wa 132/16, LEX nr 2137912.

⁵⁴ Zob. wyrok WSA w Łodzi z 30.06.2020 r., III SA/Łd 201/20, LEX nr 3031364.

W komentowanej ustawie pojęcie rękojmi ujmowane jest jako „spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem”⁵⁵. W doktrynie zwraca się uwagę na to, że rękojmia zachowania tajemnicy jest równoznaczna z wykazaniem spełnienia „ustawowych wymogów dotyczących zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem”⁵⁶. Przyjmuje się, że „jeśli wobec obywatela nie udokumentuje się w postępowaniu sprawdzającym przynajmniej jednej okoliczności faktycznej, np. wyraźnej różnicy pomiędzy dochodami a poziomem życia, czy też występowania okoliczności, które naraziłyby go na szantaż lub wywieranie presji albo może niewłaściwego postępowania z informacjami niejawnymi, przyjmuje się, że daje on rękojmię zachowania tajemnicy”⁵⁷. W orzecznictwie podkreśla się, że „na gruncie ustawy o ochronie informacji niejawnych niemożność wykluczenia istniejących wątpliwości, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, nie może być interpretowana na jej korzyść [...], a rękojmia zachowania tajemnicy oznacza spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, co powoduje, że w stosunku do osoby sprawdzanej nie mogą występować żadne uzasadnione wątpliwości określone w art. 24 ust. 2 i 3 u.o.i.n.”⁵⁸. Podsumowując, należy przyjąć, że na pojęcie rękojmi w komentowanej ustawie składa się zespół cech wartościujących konkretną osobę zarówno w sferze intelektualnej oraz profesjonalnej, jak i etyczno-moralnej, które dają podstawy do uznania, że wobec osoby poddanej weryfikacji nie zachodzą żadne okoliczności podające w wątpliwość dawanie rękojmi zachowania tajemnicy.

Badanie zdolności następuje w toku administracyjnego postępowania sprawdzającego (zwykłego lub poszerzonego) (zob. komentarz do art. 24 i n.). Zasady i tryb przeprowadzania postępowania sprawdzającego regulują przepisy rozdziału V ustawy o ochronie informacji niejawnych „Bezpieczeństwo osobowe”. Wykazanie spełnienia przesłanki wymogu rękojmi zachowania tajemnicy wymaga legitymowania się uzyskaniem poświadczenia bezpieczeństwa, uzyskanym w następstwie pozytywnego zakończenia postępowania sprawdzającego⁵⁹ (zob. komentarz do art. 21 ust. 1 pkt 1) bądź odbyciem szkolenia z zakresu ochrony informacji niejawnych⁶⁰ (zob. komentarz do art. 21 ust. 1 pkt 2). W świetle art. 4 ust. 1 u.o.i.n. wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na

⁵⁵ A. Zygmontowicz, E. Filipiuk, *Ochrona informacji niejawnych*, Szczytno 2007, s. 6.

⁵⁶ S. Hoc, *Komentarz do art. 2 [w:] S. Hoc, Ustawa o ochronie informacji...*, LEX/el.

⁵⁷ S. Zalewski, *Dylematy ochrony informacji niejawnych*, Katowice 2009, s. 70.

⁵⁸ Wyrok WSA w Warszawie z 11.12.2019 r., II SA/Wa 963/19, LEX nr 3041429.

⁵⁹ Wyrok WSA w Warszawie z 5.08.2015 r., II SA/Wa 1972/14, LEX nr 1819129. Zob. też P. Ostojski, *Ochrona praw jednostki...*, s. 77.

⁶⁰ A. Suchorzewska, *Ochrona informacji niejawnych* [w:] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Oficyna 2010, LEX/el.

zajmowanym stanowisku⁶¹ albo wykonywania czynności zleconych mogą być udostępnione informacje niejawne⁶².

W doktrynie zwraca się uwagę na to, że „informacja niejawna może zostać wykorzystana w celu realizacji ustawowych zadań przez określonych funkcjonariuszy lub przedsiębiorców. Każdy inny sposób jej wykorzystania będzie sprzeczny z ustawą o ochronie informacji niejawnych, np. gdy funkcjonariusz publiczny wykorzysta daną informację niejawną do swoich prywatnych celów, np. zakupu akcji jakiegoś przedsiębiorstwa”⁶³.

Dowodem potwierdzającym wykazanie spełnienia rękojmi zachowania tajemnicy jest uzyskanie poświadczenia bezpieczeństwa wydawanego w wyniku postępowania sprawdzającego⁶⁴, a w postępowaniu o udzielenie zamówienia w dziedzinie obronności i bezpieczeństwa – świadectwo bezpieczeństwa przemysłowego wydane w wyniku postępowania bezpieczeństwa przemysłowego⁶⁵.

4. Legalna definicja dokumentu jest bardzo ogólna i pojemna. Za dokument należy zatem uznać każdą informację opatrzoną jedną z klauzul wskazanych w ustawie o ochronie informacji niejawnych, która została utrwalona, przy czym nie ma znaczenia forma utrwalenia informacji niejawnej, ale sam fakt jej utrwalenia. Oznacza to, że dokument, w rozumieniu ustawy o ochronie informacji niejawnych, któremu nadano klauzulę tajności, stanowi fizyczne odwzorowanie informacji niejawnej i stanowi fizyczną całość. W konsekwencji „dokument stanowi zarówno jednostkowa informacja niejawna, jeżeli została w sposób jednostkowy utrwalona, jak i zbiór takich jednostkowych informacji, jeżeli został utrwalony w sposób zbiorczy. Chroniony jest więc cały dokument, jako zbiór informacji niejawnych, a nie jednostkowe informacje zawarte w tym dokumencie”⁶⁶. Dokument w rozumieniu ustawy może mieć zarówno postać elektroniczną, jak i nieelektroniczną; może to być na przykład raport opatrzony klauzulą tajności, dokument przygotowany na podstawie innych dokumentów niejawnych opatrzony klauzulą tajno-

⁶¹ Zob. R. Marek, *Skazanie a możliwość uzyskania poświadczenia bezpieczeństwa i dostęp do informacji niejawnych w jednostce organizacyjnej*, IAP 2016/1, s. 68 i n.; B. Kurzępa, *Ochrona informacji niejawnych. Ochrona danych osobowych*, Bielsko-Biała 2000, s. 10; B. Kurzępa, *Prokurator w ustawie o ochronie informacji niejawnych*, „Prokurator” 2000/2, s. 47; M. Ulasiewicz, *Ograniczenia dostępu do informacji publicznej – zagadnienia wybrane*, PPP 2010/9, s. 11; M. Mucha, *Obowiązki administracji publicznej w sferze dostępu do informacji*, Wrocław 2002, s. 202.

⁶² Zob. wyrok WSA w Warszawie z 27.11.2019 r., II SA/Wa 1111/19, LEX nr 3038453.

⁶³ E. Czarny-Drożdżewski, *Odpowiedzialność karna za ujawnienie i wykorzystanie informacji niejawnych (po nowelizacji)*, PiP 2013/1, s. 70.

⁶⁴ S. Hoc, *Komentarz do art. 2 [w:] S. Hoc, Ustawa o ochronie informacji...*, LEX/el.; M. Dela, *Bezpieczeństwo osobowe jako element ochrony informacji niejawnych*, file:///C:/Users/Dorota%20Sylwestrzak/Downloads/M_Dela_%E2%80%933_BEZPIECZE%C5%83STWO_OSOBOWE_JAKO_ELEMENT_OCHRONY_INFORMACJI_NIEJAWNYCH-1.pdf, s. 4 (dostęp: 22.04.2023 r.).

⁶⁵ R. Trzeciakowski, *Rękojmia zachowania tajemnicy informacji niejawnych w postępowaniu o udzielenie zamówienia w dziedzinie obronności i bezpieczeństwa*, IAP 2015/2, s. 76.

⁶⁶ Z uzasadnienia wyroku WSA w Warszawie z 6.10.2016 r., II SA/Wa 885/16, LEX nr 2158781.

ści, ale także informacja w zakresie terminu i klauzuli, jako że stanowi integralną część dokumentu i również pozostaje niejawna⁶⁷.

5. Ustawodawca zakresem materiału objął również dokument, co oznacza, że pojęcie materiału w świetle ustawy o ochronie informacji niejawnych jest szersze od pojęcia dokumentu i obejmuje również przedmiot albo dowolną jego część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia. Użyte przez ustawodawcę określenie „a zwłaszcza” czyni wyliczenie następujące po nim przykładowym. O uznaniu dokumentu lub przekazu za materiał niejawny decyduje treść przekazu. Za materiał można przykładowo uznać „czynność użyczenia statku powietrznego i specjalistycznej kamery cyfrowej przeznaczonej do wykonania zdjęć lotniczych terenów zamkniętych, a także nalot nad teren zamknięty, dokonany przez pilota”⁶⁸.
6. Przez przetwarzanie informacji niejawnych ustawodawca przyjmuje różne działania w odniesieniu do informacji niejawnych i realizowane na tych informacjach. Jednocześnie ustawodawca wskazał na przykładowy katalog operacji na informacjach niejawnych, które mogą polegać na wytwarzaniu (tworzeniu), modyfikowaniu (zmiana, przekształcenie), kopiowaniu (polegającym np. na odwzorowaniu cyfrowym), klasyfikowaniu (przyznanie jednej z klauzul tajności), gromadzeniu (w kancelariach tajnych), przechowywaniu (stosownie do nałożonej klauzuli, zgodnie z rozporządzeniem Rady Ministrów z 29.05.2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych⁶⁹), przekazywaniu lub udostępnianiu (wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych). Informacje niejawne mogą być przetwarzane tylko przez osoby dające rękojmię zachowania tajemnicy i przeszkolone z zasad ochrony informacji niejawnych. Działania polegające na przetwarzaniu informacji niejawnych powinny być podejmowane w wyznaczonych i specjalnie zabezpieczonych pomieszczeniach chronionych z wykorzystaniem środków bezpieczeństwa fizycznego. Informacje niejawne mogą być przetwarzane w strefach ochronnych, do których wstęp powinny mieć tylko uprawnione osoby. Z kolei informacje niejawne mające postać elektroniczną powinny być przetwarzane w akredytowanych systemach teleinformatycznych. Regulację w zakresie wydawania informacji niejawnych zawiera rozporządzenie z 7.12.2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne⁷⁰. Przekazywanie informacji niejawnych poza granice Rzeczypospolitej Polskiej umożliwiają umowy międzynarodowe, których Polska jest stroną.

⁶⁷ Wyrok WSA w Warszawie z 17.03.2016 r., II SA/Wa 1593/15, LEX nr 2072855.

⁶⁸ Wyrok KIO z 8.07.2020 r., KIO 871/20, LEX nr 3042056.

⁶⁹ Dz.U. poz. 683.

⁷⁰ Dz.U. Nr 271, poz. 1603.