

Redakcja naukowa Piotr Burczaniuk

Tomasz Batory
Roman Brzozowski
Piotr Burczaniuk
Magdalena Gołaszewska
Michał Kamiński
Renata Klejc
Marcin Nowiński
Michał Ordyniak
Gracjan Poterała
Bianka Skowronek
Mateusz Wiczerza

**Prawne aspekty
funkcjonowania
służb specjalnych
na przykładzie
Agencji Bezpieczeństwa
Wewnętrznego**

Prawne aspekty funkcjonowania
służb specjalnych na przykładzie
Agencji Bezpieczeństwa Wewnętrznego



WPIA
UKSW

Wydział Prawa i Administracji
UNIwersytet Kardynała
Stefana Wyszyńskiego
w Warszawie



Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego

Redakcja naukowa
Piotr Burczaniuk

Recenzenci:

dr hab. Artur Kotowski, prof. UKSW

dr hab. Marcin Wielec

Zespół redakcyjny:

Violetta Urbaniak (Wydawnictwo DiG, redakcja językowa, korekta)

Kornelia Piasecka (Agencja Bezpieczeństwa Wewnętrznego)

Projekt okładki:

Aleksandra Bednarczyk

Skład:

Andrzej Kaczmarek

© Copyright by Agencja Bezpieczeństwa Wewnętrznego, 2021

© Copyright by Wydawnictwo DiG, 2021

ISBN ABW: 978-83-956907-5-4

ISBN DiG: 978-83-286-0178-9

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego

Centralny Ośrodek Szkolenia i Edukacji w Emowie

im. gen. dyw. Stefana Roweckiego „Grota”

05-462 Wiązowna, ul. Nadwiślańczyków 2

tel. (+48 22) 58 58 613

e-mail: wydawnictwo@abw.gov.pl, <http://www.abw.gov.pl/wyd/>



Wydawnictwo DiG Sp.j.

PL 01-987 Warszawa, ul. Dankowicka 16c lok. 2

tel./fax: (+48 22) 839 08 38

e-mail: biuro@dig.pl, <http://www.dig.pl>

Druk cyfrowy

Spis treści

Przedmowa	7
Wstęp	9
Wykaz skrótów	13
Rozdział 1. Zadania Szefa ABW w zakresie obowiązków informacyjnych (<i>Piotr Burczaniuk</i>)	17
Rozdział 2. Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny (<i>Magdalena Gołaszewska</i>)	31
Rozdział 3. Zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw (<i>Tomasz Batory</i>)	65
Rozdział 4. Zadania ABW w zakresie bezpieczeństwa teleinformatycznego państwa (<i>Gracjan Poterała</i>)	89
Rozdział 5. Zadania służb specjalnych w obszarze ochrony informacji niejawnych ze szczególnym uwzględnieniem aspektów międzynarodowych (<i>Marcin Nowiński, Mateusz Wieczerza</i>)	117
Rozdział 6. Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW (<i>Roman Brzozowski</i>)	145
Rozdział 7. Prawne aspekty współpracy międzynarodowej służb specjalnych (<i>Michał Kamiński</i>)	177
Rozdział 8. Problematyka ochrony środków, form i metod realizacji zadań w praktyce funkcjonowania służb specjalnych (<i>Magdalena Gołaszewska</i>) ...	209
Rozdział 9. Problematyka tworzenia prawa wewnętrznego służb specjalnych na przykładzie ABW (<i>Piotr Burczaniuk</i>)	225
Rozdział 10. Charakterystyka stosunku służbowego funkcjonariuszy ABW ze szczególnym uwzględnieniem analizy fakultatywnych i obligatoryjnych przesłanek zwolnienia ze służby na podstawie wybranych orzeczeń sądów administracyjnych (<i>Bianka Skowronek</i>)	249

Rozdział 11. Szef ABW jako podmiot zobowiązany do udostępniania informacji publicznej w trybie <i>ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej</i> na tle dotychczasowej praktyki orzeczniczej sądów administracyjnych (<i>Renata Klejc</i>)	271
Rozdział 12. Wyzwania regulacyjne ustaw kompetencyjnych służb specjalnych z perspektywy zachodzących zmian w systemie prawa oraz kształtowania nowej siatki zagrożeń dla bezpieczeństwa państwa (<i>Piotr Bureczaniuk, Michał Ordyniak</i>)	295
Bibliografia	314
Wykaz autorów	325

Przedmowa

24 maja 2022 r. minie 20 lat od dnia, gdy Sejm Rzeczypospolitej IV kadencji uchwalił ustawę o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Ustawa ta swoimi przepisami ukształtowała obraz największej polskiej służby specjalnej, jaką jest Agencja Bezpieczeństwa Wewnętrznego.

Celem niniejszej publikacji jest z jednej strony analiza przepisów prawnych kształtujących ustrojowe i pragmatyczne ramy funkcjonowania tych służb, ze szczególnym uwzględnieniem doświadczeń płynących z mijającego okresu obowiązywania ustawy o ABW oraz AW. Z drugiej strony, monografia ta stanowi głos w dyskursie naukowym prowadzonym w obszarze nauk prawnych, w zakresie wykładni i praktycznych aspektów stosowania przepisów regulujących działalność tych służb, w tym w szczególności Agencji Bezpieczeństwa Wewnętrznego. Ponadto szerokie omówienie w poszczególnych rozdziałach tego opracowania 12 zagadnień problemowych, które bez wątpienia uznać należy za fundamentalne z perspektywy zadań wykonywanych przez te formacje, stanowi cenne źródło wiedzy, która może być przydatna zarówno z perspektywy dydaktyki akademickiej na takich kierunkach, jak prawo, stosunki międzynarodowe czy bezpieczeństwo wewnętrzne, ale również, a może przede wszystkim, być wykorzystywana w ramach procesu szkolenia prowadzonego przez organy ochrony prawnej.

Niniejsza publikacja stanowi kontynuację dyskusji naukowej zapoczątkowanej przez mojego poprzednika na stanowisku Szefa ABW, prof. dr. hab. Piotra Pogonowskiego, prowadzonej w wydanych w ramach „Biblioteki Przeglądu Bezpieczeństwa Wewnętrznego” opracowaniach pt. *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach* (maj 2017) oraz monografii pt. *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* (październik 2017).

Dodać należy, iż monografia ta nigdy by nie powstała bez zaangażowania grona ekspertów prawniczych — redaktora dr. Piotra Burczaniuka oraz autorów poszczególnych rozdziałów, jak i wsparcia pracowników naukowych Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, udzielanego w ramach realizacji porozumienia zawartego 1 czerwca 2021 r. między Uniwersytetem Kardynała Stefana Wyszyńskiego a Agencją Bezpieczeństwa Wewnętrznego. Wszystkim tym osobom należą się słowa uznania i podziękowania.

*Szef Agencji Bezpieczeństwa Wewnętrznego
plk Krzysztof Waclawek*

Wstęp

Oddana do rąk czytelnika — niniejsza wieloautorska monografia prawnicza, którą miałem zaszczyt zredagować — omawia najważniejsze aspekty prawnego funkcjonowania służb specjalnych we współczesnej Polsce, koncentrując się w szczególności na największej z nich Agencji Bezpieczeństwa Wewnętrznego.

Podjęwając się redakcji tej publikacji, miałem przekonanie o konieczności uporządkowania i usystematyzowania doktrynalnych rozważań teoretycznych, poświęconych służbom specjalnym oraz potrzebie dokonanie swoistej ich konfrontacji z doświadczeniami kształtowanymi m.in. praktyką sądowno-administracyjną z ostatnich 20 lat, jakie mijają od uchwalenia 24 maja 2002 r. ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, która to ustawa trwale ukształtowała rdzeń przepisów ustrojowych i pragmatycznych wszystkich funkcjonujących obecnie służb specjalnych w Polsce.

Wychodząc z tych założeń, ułożyłem przedmiotowy zakres monografii w 12 tematycznie powiązanych rozdziałów, odpowiadających treściowo tytułowi monografii. W rozdziale pierwszym, mojego autorstwa, pt. *Zadania Szefa ABW w zakresie obowiązków informacyjnych*, dokonałem prawnej analizy podstawowego zadania Szefa ABW, tj. obowiązku informacyjnego wyrażonego w art. 18 ustawy o ABW oraz AW, i jego zestawienia z zadaniami informacyjnymi samej ABW (art. 5 ustawy o ABW oraz AW), które to przepisy — choć absolutnie podstawowe z perspektywy zadań realizowanych przez tę służbę — nie były do tej pory przedmiotem szerszych rozważań doktrynalnych.

W rozdziale drugim, autorstwa Magdaleny Gołaszewskiej, pt. *Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny*, dokonano analizy podstawowych pojęć prawnych i instytucji dotyczących problematyki wskazanej w tytule rozdziału.

W rozdziale trzecim, autorstwa Tomasza Batorego, pt. *Zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw*, dokonano zarówno analizy historycznej niniejszych zagadnień, wywodzących się z UOP, jak również omówiono zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania powierzonych ABW przestępstw.

Rozdział czwarty, autorstwa Gracjana Poterały, porusza problem aspektów prawnych realizacji przez ABW zadań w zakresie bezpieczeństwa teleinformatycznego państwa oraz środków służących ich realizacji. W rozdziale autor

dokonał przede wszystkim rekonstrukcji pojęcia „bezpieczeństwo teleinformatyczne” w związku z „szeroko rozumianym bezpieczeństwem narodowym”.

Rozdział piąty, współautorski Marcina Nowińskiego i Mateusza Wieczery, pt. *Zadania służb specjalnych w obszarze ochrony informacji niejawnych ze szczególnym uwzględnieniem aspektów międzynarodowych*, omawia współczesne potrzeby ochrony tego rodzaju informacji, przeciwdziałanie działaniom kontrywywiadowczym oraz specyfikę czynności podejmowanych w tym zakresie przez ABW.

Rozdział szósty, autorstwa Romana Brzozowskiego, poświęcony został analizie prawno-porównawczej czynności wykonywanych przez funkcjonariuszy ABW na tle zadań Agencji. Rozdział został przygotowany ze stosownym uwzględnieniem stanowisk prezentowanych dotychczas w doktrynie prawniczej w zakresie przyjętego w Polsce modelu służb specjalnych oraz ogólnych założeń co do kompetencji i celów funkcjonowania ABW.

Rozdział siódmy, autorstwa Michała Kamińskiego, uczynił przedmiotem analizy prawne aspekty współpracy międzynarodowej służb specjalnych. W rozdziale omówiono pojęcie „służby specjalne” oraz przedstawiono podstawy ustawowe współpracy międzynarodowej służb, rolę Ministra-Koordynatora Służb Specjalnych w tym procesie oraz porównanie z regulacjami prawnymi innych służb. Dodatkowo w rozdziale scharakteryzowano instytucję umów międzynarodowych jako prawnej podstawy współpracy międzynarodowej służb specjalnych oraz kwestię współpracy służb z międzynarodowymi organizacjami.

Rozdział ósmy, autorstwa Magdaleny Gołaszewskiej, pt. *Problematyka ochrony środków, form i metod realizacji zadań w praktyce funkcjonowania służb specjalnych* omawia wybrane aspekty prawne i techniczne pozyskiwania informacji przez służby specjalne i ich ochronę.

Rozdział dziewiąty, mojego autorstwa, przedstawia problematykę tworzenia prawa wewnętrznego służb specjalnych na przykładzie ABW. W tekście tym poddaję analizie zarówno proceduralne kwestie powstawania takich aktów, jak również szersze rozważania doktrynalne na temat miejsca aktu prawa wewnętrznego w systemie źródeł prawa.

Rozdział dziesiąty, przygotowany przez Biankę Skowronek, poświęcony został charakterystyce stosunku służbowego funkcjonariuszy ABW, ze szczególnym uwzględnieniem analizy fakultatywnych i obligatoryjnych przesłanek zwolnienia ze służby, na tle doświadczeń płynących z wybranych orzeczeń sądów administracyjnych.

W rozdziale jedenastym, autorstwa Renaty Klejca, omówiono rolę Szefa ABW jako podmiotu zobowiązanego do udostępniania informacji publicznej w trybie ustawy z 2001 r. o dostępie do informacji publicznej. W rozdziale przybliżono m.in. tryby udostępniania informacji publicznej, kwestię publikacji informacji w Biuletynie Informacji Publicznej, postępowanie wnioskowe i kwestię ograniczenia dostępu do informacji publicznej, co ma istotne znaczenie w praktyce funkcjonowania służb specjalnych. W rozdziale poruszono także kwestię

informacji przetworzonej oraz ochrony informacji niejawnych i innych tajemnic prawnie chronionych jako przesłankę odmowy dostępu do informacji publicznej.

W finalnym rozdziale dwunastym, współautorstwa mojego oraz Michała Ordyniaka, pt. *Wyzwania regulacyjne ustaw kompetencyjnych służb specjalnych z perspektywy zachodzących zmian w systemie prawa oraz kształtowania nowej siatki zagrożeń dla bezpieczeństwa państwa*, przedstawiamy zarówno rys historyczny ustawy o ABW oraz AW, jak również porównujemy cechy wyróżniające obecne Agencje od ich poprzednika — Urzędu Ochrony Państwa, analizujemy dotychczasowe prace nad reformą cywilnych służb specjalnych oraz wskazujemy obszary, które pozostają do rozważania w przedmiocie podjęcia ewentualnej decyzji o inicjatywie prawodawczej.

Oprócz wskazanego zakresu przedmiotowego szczególną wartość monografii — zdecydowanie największą — stanowią jej Autorzy, którzy zetknęli się z analizowaną problematyką nie tylko w kontekście teoretyczno-prawnych rozważań doktrynalnych, lecz przede wszystkim mieli okazję zajmować się nią w trakcie swojej prawniczej drogi zawodowej jako legislatorzy lub radcy prawni. Im więc, szczególnie za chęć wzięcia udziału w przygotowaniu niniejszej monografii oraz za wnikliwość i zaangażowanie, jakim wykazali się podczas jej opracowania, dziękuję.

Dziękuję również za wsparcie merytoryczne, które otrzymaliśmy od pracowników naukowych Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, a w szczególności ze strony prof. UKSW dr. hab. Artura Kotowskiego oraz dr. hab. Marcina Wielca, recenzentów wydawniczych tej monografii.

Mam nadzieję, iż zarówno zakres przedmiotowy monografii, łączący rozważania teoretyczne z doświadczeniami praktyki, jak i wysoki poziom autorski oraz sprawowany przez wyższą uczelnię nadzór merytoryczny, czynią z niej cenną pozycję na liście krajowej literatury prawniczej poświęconej służbom specjalnym, która okaże się przydatna zarówno teoretykom prawa, jak i przede wszystkim praktykom jego stosowania.

Piotr Burczaniuk
Warszawa, październik 2021 r.

Wykaz skrótów

Źródła prawa

- BrońU — *Ustawa z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym* (Dz.U. 2017, poz. 290 ze zm.)
- k.p.a. — *Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego* (Dz.U. 2021, poz. 735)
- KK — *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. 2019, poz. 1950 i 2128)
- Konstytucja RP — *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. 1997, nr 78, poz. 483 z późn. zm.)
- KPK — *Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego* (Dz.U. 2021, poz. 534)
- NarkU — *Ustawa z 29 lipca 2005 r. o przeciwdziałaniu narkomanii* (Dz.U. 2017, poz. 783 ze zm.)
- Reg.RM — *Uchwała nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów* (M.P. 2016, poz. 1006 z późn. zm.)
- Reg.Sej. — *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. Regulamin Sejmu Rzeczypospolitej Polskiej* (M.P. 2019, poz. 1028 z późn. zm.)
- TFUE — *Traktat o funkcjonowaniu Unii Europejskiej* (Dz.U.2004.90.864/2)
- u. inf. niejaw. — *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. 2019, poz. 742)
- u. inf. publ. — *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej* (Dz.U. 2020, poz. 2176)
- u.r.m. — *Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów* (Dz.U. 2019, poz. 1171 z późn. zm.)
- ustawa o ABW oraz AW — *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U., nr 74, poz. 676)

ustawa o CBA	— <i>Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym</i> (Dz.U. 2019, poz. 1921 z późn. zm.)
ustawa o SKW oraz SWW	— <i>Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego</i> (Dz.U. 2019, poz. 687 z późn. zm.)
ustawa o służbie w SKW oraz SWW	— <i>Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego</i> (Dz.U. 2020, poz. 1221 z późn. zm.)
ustawa o Straży Granicznej	— <i>Ustawa z dnia 12 października 1990 r. o Straży Granicznej</i> (Dz.U. 2020, poz. 305 z późn. zm.)
ustawa o UOP	— <i>Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa</i> (Dz.U. 1999, poz. 526, 548 i 1255; 2000, poz. 852; 2001, poz. 877 i 1149)
ustawa o urzędzie Ministra SW	— <i>Ustawa z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów</i> (Dz.U. 1983, nr 38, poz. 172)
Kodeks karny wykonawczy	— <i>Ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy</i> (Dz.U. 2021, poz. 53 z późn. zm.)
ustawa o WSI	— <i>Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych</i> (Dz.U. 2003, nr 139, poz. 1326)
u. ogłasz. aktów	— <i>Ustawa o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych</i> (Dz.U. 2019.0.1461)
u. św. elektr.	— <i>Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną</i> (Dz.U. 2020.0.344)
ustawa o działaniach antyterrorystycznych	— <i>Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych</i> (Dz.U. 2019.796)
ustawa o zarządzaniu kryzysowym	— <i>Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym</i> (Dz.U. 2020.0.1856)

Organy

ABW	— Agencja Bezpieczeństwa Wewnętrznego
AW	— Agencja Wywiadu
CBA	— Centralne Biuro Antykorupcyjne
NBP	— Narodowy Bank Polski
NSA	— Naczelny Sąd Administracyjny
RCL	— Rządowe Centrum Legislacji
SB	— Służba Bezpieczeństwa
Sejm RP	— Sejm Rzeczypospolitej Polskiej
SKW	— Służba Kontrwywiadu Wojskowego
SN	— Sąd Najwyższy
SWW	— Służba Wywiadu Wojskowego
TK	— Trybunał Konstytucyjny

TSUE	— Trybunał Sprawiedliwości Unii Europejskiej
UOP	— Urząd Ochrony Państwa
WSA	— Wojewódzki Sąd Administracyjny
WSI	— Wojskowe Służby Informacyjne

Publikatory i czasopisma

Dz.U.	— Dziennik Ustaw
Dz.U.UE.C	— Dziennik Urzędowy Unii Europejskiej Seria C
Dz.U.UE.L	— Dziennik Urzędowy Unii Europejskiej Seria L
Dz.U.UE.S	— Dziennik Urzędowy Unii Europejskiej Seria S
Dz.Urz.	— Dziennik Urzędowy
Dz.Urz.KNF	— Dziennik Urzędowy Komisji Nadzoru Finansowego
ECR	— <i>European Court Reports</i>
LEX nr	— Program <i>Lex Omega</i> — numer publikacji LEX
LEX/el. nr.	— Program <i>Lex Omega</i> — numer w bazie LEX
M.P.	— Monitor Polski
OSN	— Orzecznictwo Sądu Najwyższego
OTK	— Orzecznictwo Trybunału Konstytucyjnego
OTK-A	— Orzecznictwo Trybunału Konstytucyjnego Seria A
RPL	— Rządowy Proces Legislacyjny
ZOTSiS	— Zbiór Orzeczeń Trybunału Sprawiedliwości i Sądu

Inne skróty

art.	— artykuł
BIP	— Biuletyn Informacji Publicznej
cyt.	— cytowanie
i nast.	— i następny
informacje niejawne międzynarodowe	— informacje niejawne NATO, Unii Europejskiej lub innych organizacji międzynarodowych
itp.	— i temu podobne
kom.	— komentarz
lit.	— litera
m.in.	— między innymi
NATO	— Organizacja Traktatu Północnoatlantyckiego
np.	— na przykład
nr	— numer
ust.	— ustęp

Piotr Burczaniuk

Rozdział 1.

Zadania Szefa ABW w zakresie obowiązków informacyjnych

Wstęp

Przedmiotem rozważań niniejszego rozdziału jest analiza prawnych aspektów realizacji przez Szefa ABW zadań w zakresie obowiązków informacyjnych.

Zgodnie z art. 5 ust. 1 pkt 4 ustawy o ABW oraz AW do zadań ABW należy uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Tak ukształtowana właściwość analityczno-informacyjna, jak wskazuje się w doktrynie, *jest uznawana za podstawową i najważniejszą funkcję realizowaną przez ABW. Warunkiem optymalnie funkcjonującego systemu bezpieczeństwa wewnętrznego państwa jest (bowiem — wł) zapewnienie stałego dopływu informacji z różnych źródeł, ich analiza oraz przetworzenie w procesach decyzyjnych polityki bezpieczeństwa*¹. Szczególne — podstawowe — miejsce w realizacji zakreślonych w ten sposób zadań ABW przypada jej Szefowi, który poprzez art. 18 ustawy o ABW oraz AW dostaje (wraz z Szefem AW) zadanie — zresztą jedyne na kanwie całej ustawy — eksportu właściwie wyselekcjonowanych, zinterpretowanych i wartościowych informacji na rzecz najważniejszych organów państwa, dla których pełnią one rolę *przesłanek w politycznych procesach decyzyjnych*². Realizacja tego zadania stanowi swoistą kwintesencję działań obu Agencji, przesądzających o ich „specjalności”.

Niniejsze rozważania zostały przeprowadzone z wykorzystaniem analizy prawno-porównawczej, opartej na badaniu historycznym tekstów aktów

¹ B. Opaliński, M. Rogalski P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, wyd. C.H. Beck, Warszawa 2017, s. 28.

² M. Kolaszyński, *Status ustrojowy polskich służb specjalnych po 1989 roku*, wyd. UJ, Kraków 2016, s. 146.

normatywnych i przebiegu prac legislacyjnych ich dotyczących, oraz analizy dogmatycznej teksów ustaw obowiązujących, zwłaszcza ustawy o ABW oraz AW, ze szczególnym uwzględnieniem regulacji zawartych w artykułach 5, 18 i 39 tej ustawy, w szczególności ich wzajemnej relacji.

W związku z powyższymi założeniami i przyjętymi metodami w analizie niniejszej przeprowadzono interpretację prawną w oparciu o powszechnie przyjęty w orzecznictwie Sądu Najwyższego³ i polskiej nauce prawa⁴ kanon wykładni przepisów prawa, oparty o regułę pierwszeństwa wykładni językowej, wspartą pomocniczo regułami wykładni systemowej i funkcjonalnej. Z uwagi na brak ustalonej linii orzeczniczej oraz stanowiska wypracowanego przez naukę prawa w odniesieniu do poddawanych analizie regulacji ustawy o ABW oraz AW niemożliwym było zastosowanie w ramach wykładni językowej dyrektyw wykładni języka prawniczego, obligując tym samym do skorzystania z dyrektyw języka prawnego nakazujących, gdzie było to możliwe, odwołanie się do ustalonego w drodze definicji legalnej ustawowego rozumienia interpretowanych pojęć, a w przypadku ich braku do skorzystania z dyrektyw języka potocznego, zakładających zastosowanie reguł semantycznych, syntaktycznych i kontekstowych dla wyprowadzenia rozumienia interpretowanych słów, wyrażeń i zwrotów, w szczególności tych, które są nieostre lub wieloznaczne.

Kształtowanie obowiązku informacyjnego szefa służby w ustawie o UOP

Jak wskazuje M. Kolaszyński, *już w momencie powstania UOP ustawodawca miał świadomość wagi informacji dla bezpieczeństwa państwa*⁵. Zgodnie bowiem z art. 11 ust. 2 ustawy o UOP (w brzmieniu obowiązującym od 10 maja 1990 do 1 października 1996 r.), jeśli uzyskane przez UOP informacje, w tym także informacje uzyskane w zakresie właściwości UOP w sposób tajny i poufny, które zostaną uznane za mogące mieć istotne znaczenie dla bezpieczeństwa państwa, Szef UOP ma obowiązek ich niezwłocznego przekazania do wiadomości Prezesa Rady Ministrów i Ministra Spraw Wewnętrznych. Podkreślenie w tym zakresie roli Ministra Spraw Wewnętrznych wynikało z faktu podległości w tym okresie Szefa UOP właśnie temu organowi.

Z dniem 1 października 1996 r., na mocy reformy przeprowadzonej *ustawą z dnia 8 sierpnia 1996 r. o zmianie niektórych ustaw normujących funkcjonowanie gospodarki i administracji publicznej*⁶, którą m.in. poddano Szefa UOP pod nadzór Prezesa Rady Ministrów, uległo zmianie brzmienie art. 11 ust. 2, który zakładał od tego momentu, iż uzyskane przez UOP informacje, w tym także informacje uzyskane w zakresie właściwości UOP w sposób tajny i poufny,

³ Por. orzeczenie Sądu Najwyższego z dnia 14 października 2004 r. w sprawie o sygn. akt III CZP 37/04.

⁴ Por. L. Morawski, *Zasady wykładni prawa*, wyd. TNOiK, 2010 r., s. 72–81.

⁵ M. Kolaszyński, dz. cyt., s. 149.

⁶ Dz.U. 1996, poz. 106, 496.

mogące mieć istotne znaczenie dla bezpieczeństwa państwa, Szef Urzędu Ochrony Państwa ma obowiązek niezwłocznego przekazania do wiadomości Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów. W tym zakresie więc obowiązek informacyjny Szefa UOP został przeniesiony z Ministra Spraw Wewnętrznych na Prezydenta RP. Jednocześnie, przez dodanie zdania drugiego, wprowadzono zupełnie nowy sposób dystrybucji tych informacji, zakładający, iż jeśli uzyskane informacje dotyczą ściśle spraw objętych zakresem działania właściwego ministra, Szef Urzędu Ochrony Państwa może je również przekazać temu ministrowi. W ten sposób uformowany został kształt regulacji obowiązku informacyjnego Szefa UOP, który — wraz z likwidacją tego urzędu i utworzeniem w jego miejsce ABW oraz AW — został praktycznie bezpośrednio transponowany do nowej ustawy jako obowiązek Szefa ABW oraz Szefa AW.

Obowiązek informacyjny Szefa ABW z art. 18 ustawy o ABW oraz AW jako zadanie Agencji Bezpieczeństwa Wewnętrznego

Zgodnie z art. 18 ust. 1 ustawy o ABW oraz AW Szefowie Agencji, każdy w zakresie swojej właściwości, przekazują niezwłocznie Prezydentowi Rzeczypospolitej Polskiej i Prezesowi Rady Ministrów informacje mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej. Obowiązek ten został zmodyfikowany w przepisie ust. 2, według którego powyższe informacje są przekazywane Prezydentowi RP w każdym przypadku, kiedy tak zdecyduje, zaś w ust. 3 przewidziano, iż te informacje są przekazywane właściwemu ministrowi, w zakresie jego działania, chyba że Prezes Rady Ministrów zdecyduje inaczej. Jak wskazuje się w doktrynie, *w omawianym przepisie ustanowiony został spoczywający na Szefach Agencji, w zakresie ich właściwości, doniosły obowiązek informacyjny. Obowiązek ten aktualizuje się poprzez informowanie o kwestiach mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej*⁷.

Jak wynika więc z brzmienia art. 18 ustawy o ABW oraz AW, obowiązek przekazywania informacji przez Szefów Agencji został zróżnicowany co do trybu i podmiotów uprawnionych do ich otrzymywania. W ust. 1 ustawodawca opisał podstawowy tryb *ex officio* (z urzędu) stosowany wobec szerszego kręgu podmiotów uprawnionych (Prezydent RP, Prezes Rady Ministrów, ministrowie), natomiast w ust. 2 przewidziano dodatkowy tryb *petitio* (na żądanie), mający zastosowanie wyłącznie wobec Prezydenta RP. W obu sytuacjach nałożono na Szefów Agencji obowiązek przekazywania stosownych informacji podmiotom uprawnionym, przy czym w drugiej z nich dzieje się tak w każdym przypadku, kiedy Prezydent RP tak zdecyduje. Przyjęte rozwiązanie podkreśla niewątpliwie rolę Prezydenta RP w systemie organów państwa. Z kolei wskazanie przez ustawodawcę, iż przekazywanie przez Szefów Agencji uzyskanych informacji

⁷ B. Opaliński, M. Rogalski P. Szustakiewicz, dz. cyt., s. 55.

podmiotom uprawnionym winno następować niezwłocznie, świadczy o randze tych informacji dla bytu i funkcjonowania państwa, która to ranga ulega jeszcze wzmocnieniu na skutek wąskiego zakreszenia katalogu odbiorców tych informacji.

Granice wskazanego obowiązku informacyjnego Szefów Agencji zostały zdefiniowane przez pryzmat ich właściwości. W wypadku Szefa ABW owe granice wytycza art. 1 ustawy o ABW oraz AW, statuując ABW jako organ właściwy w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Skoro zatem ABW jest właściwa w powyższym zakresie, to tym bardziej właściwy jest Szef ABW jako centralny organ administracji rządowej, działający przy pomocy ABW, będącej urzędem administracji rządowej (art. 3 ust. 1 ustawy o ABW oraz AW).

Wskazać należy, iż sformułowany w powyższy sposób obowiązek informacyjny został wprost zdefiniowany jako zadanie Szefów Agencji, obok innych zadań uregulowanych odpowiednio w art. 5 i 6 ustawy o ABW oraz AW, już na etapie prac legislacyjnych nad projektem ustawy o ABW oraz AW w latach 2001–2002. W uzasadnieniu do tego projektu ustawy, objętego drukiem nr IV.276, można przeczytać, iż: *Odrębnym zadaniem Szefów ABW i AW jest przygotowywanie dla najwyższych organów władzy wykonawczej, tj. Prezydenta RP i Prezesa Rady Ministrów, informacji dotyczących zagrożeń bezpieczeństwa Państwa oraz zagrożeń porządku konstytucyjnego*⁸.

Fundamentalne znaczenie obowiązku informacyjnego, wynikającego z przepisów art. 18 ustawy o ABW oraz AW, wynika jednak nie tylko z okoliczności potraktowania go przez ustawodawcę jako zadania Szefów Agencji, pośród innych zadań ustawowych ABW oraz AW wymienionych w art. 5 ustawy o ABW oraz AW, ale także z ulokowania tej regulacji w rozdziale 3 ustawy o ABW oraz AW, odnoszącym się do organizacji Agencji Bezpieczeństwa Wewnętrznego. Wspomniany obowiązek informacyjny został bowiem zamieszczony wśród przepisów dotyczących powoływania i odwoływania Szefa ABW, czy też wydawania przez niego aktów kierowania wewnętrznego. Przepisy rozdziału trzeciego ustawy o ABW oraz AW zawierają zatem fundamenty prawne dla funkcjonowania Szefa ABW oraz podległej mu Agencji Bezpieczeństwa Wewnętrznego, do których zalicza się także obowiązek informacyjny uregulowany w art. 18 ustawy o ABW oraz AW.

W tym kontekście za uzasadnione należy uznać stwierdzenie, iż wypełnianie tego zadania informacyjnego przez Szefa ABW stanowi kwintesencję działalności ABW, tj. informowania konstytucyjnych organów władzy wykonawczej o zagrożeniach bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

⁸ Uzasadnienie do druku nr drukiem nr IV.276, zob. [https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/\\$file/276.pdf](https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/$file/276.pdf), [dostęp: 16 VI 2021].

Podmioty uprawnione do otrzymywania informacji

Prezydent RP

W art. 126 Konstytucji RP określono w sposób ogólny rolę Prezydenta RP w ustroju politycznym Polski oraz jego najważniejsze zadania (cele działalności), jak również założenia co do sposobów ich realizacji. Wskazany przepis Konstytucji RP uzupełnia regulację zawartą w art. 10 Konstytucji RP, zgodnie z którym Prezydent RP jest — obok Rady Ministrów — organem władzy wykonawczej.

Ustrojowa pozycja Prezydenta RP jako „najwyższego przedstawiciela Rzeczypospolitej Polskiej” i „gwaranta ciągłości władzy państwowej” (ust. 1) została konstytucyjnie ukierunkowana przez wskazanie w ust. 2 najważniejszych zadań Prezydenta RP.

Podstawowy zakres urzeczywistnienia zadania ochrony bezpieczeństwa zewnętrznego i wewnętrznego państwa wiąże się z wykonywaniem przez Prezydenta RP kompetencji najwyższego zwierzchnika Sił Zbrojnych Rzeczypospolitej (art. 134 ust. 1 Konstytucji RP). Prezydent RP posiada ponadto decydujące kompetencje w warunkach szczególnego zagrożenia państwa, wiążące się z wprowadzaniem stanu wojennego i wyjątkowego oraz zarządzenia (powszechnej lub częściowej) mobilizacji.

W świetle przytoczonych regulacji Konstytucji RP nie budzi wątpliwości, iż z uwagi na wyjątkową rolę Prezydenta RP winien on otrzymywać od Szefów Agencji, jak również jest on uprawniony do żądania od nich, na zasadach i w trybie określonych w art. 18 ust. 1 i 2 ustawy o ABW oraz AW, informacji mogących mieć znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, które to uprawnienie służy realizacji przez Prezydenta RP jego konstytucyjnych zadań. Określony w ust. 2 zwrot „żądać” przypomina swoisty tryb wnioskowy, w którym Prezydent występuje do Szefów Agencji o przekazanie informacji *samodzielnie, nawet jeśli nie ma wiedzy o tym, czy Szefowie Agencji posiadają dane informacje*⁹.

Prezes Rady Ministrów

Zgodnie z art. 146 ust. 4 pkt 7 i 8 Konstytucji RP Rada Ministrów — w zakresie i na zasadach określonych w Konstytucji RP i ustawach — zapewnia bezpieczeństwo wewnętrzne państwa oraz porządek publiczny, a także bezpieczeństwo zewnętrzne państwa. Jak podkreśla się w doktrynie, *trzon odpowiedzialności za wewnętrzne i zewnętrzne bezpieczeństwo Rzeczypospolitej Polskiej został ulokowany w rządowym segmencie władzy wykonawczej*¹⁰.

Podstawową rolą Rady Ministrów jest *prowadzenie polityki wewnętrznej i zagranicznej Rzeczypospolitej Polskiej* (art. 146 ust. 1 Konstytucji RP).

⁹ B. Opaliński, M. Rogalski P. Szustakiewicz, dz. cyt., s. 57.

¹⁰ Tamże, s. 56.

W określeniu tym mieści się właściwie całość działania władzy publicznej, powierzona egzekutywie, od której swoistym wyjątkiem jest sytuacja, gdy prowadzenie tej polityki należałoby do legislatywy, judykatury czy ewentualnie jeszcze innych „władz”¹¹. Koresponduje to ze znaną tzw. negatywną definicją administracji państwowej, ujmowaną jako całość działalności publicznej danego państwa, z wyjątkiem ustawodawstwa i wymiaru sprawiedliwości.

Natomiast art. 147 Konstytucji RP określa skład Rady Ministrów jako konstytucyjnego organu państwa. Jest to swego rodzaju definicja legalna Rady Ministrów w aspekcie personalnym. Oprócz osób wymienionych w art. 147 Konstytucji RP nikt nie może zostać członkiem Rady Ministrów. Gdy w innych przepisach Konstytucji RP (np. art. 154 ust. 1 i 3, art. 155 ust. 1, czy art. 157) jest mowa ogólnie o członkach Rady Ministrów, rozumieć przez to należy osoby wskazane w art. 147 ust. 1, 2 i 4 Konstytucji RP. W skład Rady Ministrów nie wchodzi natomiast w szczególności sekretarze stanu w administracji rządowej (art. 103 Konstytucji RP) oraz osoby, którym Prezes Rady Ministrów (bez powołania ich w skład Rady Ministrów) powierzył kierowanie ministerstwem (art. 198 ust. 1 Konstytucji RP). Prezes Rady Ministrów jest koniecznym „elementem” Rady Ministrów. Wynika z tego, że nie może dojść do powołania rządu i jego trwałego funkcjonowania bez personalnej obsady tego stanowiska. Bardziej szczegółowe konsekwencje założenia, iż Prezes Rady Ministrów stoi na czele Rady Ministrów, zostały sprecyzowane w innych przepisach, np. w art. 148 Konstytucji RP.

Konstytucja RP dokonuje wyraźnej instytucjonalizacji urzędu wiceprezesa Rady Ministrów, co odpowiada wcześniejszej praktyce ustrojowej. Użycie w art. 147 ust. 2 Konstytucji RP liczby mnogiej nie oznacza jednak, że nie można powołać tylko jednego wicepremiera. W sensie językowym przedrostek „wice-” oznacza zastępcę kogoś (w tym przypadku premiera) lub osobę mającą tytuł albo stopień bezpośrednio niższy od kogoś. Oznacza to, że w strukturze administracji rządowej wicepremierzy zajmują miejsce (również w aspekcie tzw. precedencji) po Prezesie Rady Ministrów, ale przed innymi członkami Rady Ministrów. Znajduje to potwierdzenie na gruncie przepisów *ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów*¹². Mianowicie art. 6 tej ustawy stanowi, iż w razie nieobecności Prezesa Rady Ministrów lub w innym wypadku czasowej niemożności wykonywania przez niego obowiązków w Radzie Ministrów, pracami Rady Ministrów kieruje wiceprezes Rady Ministrów wyznaczony przez Prezesa Rady Ministrów lub jeden z ministrów, jeżeli wiceprezes Rady Ministrów nie został powołany. Wiceprezes Rady Ministrów wykonuje, w imieniu Prezesa Rady Ministrów, zadania i kompetencje w zakresie powierzonym przez Prezesa Rady Ministrów.

¹¹ Por. P. Sarnecki zob. *Komentarz do niektórych przepisów Konstytucji Rzeczypospolitej Polskiej*, w: *Prezydent Rzeczypospolitej Polskiej. Komentarz*, Kraków 2000, art. 146, <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587270804/68244/sarnecki-pawel-komentarz-do-niektorych-przepisow-konstytucji-rzeczypospolitej-polskiej-w...?cm=URRELATIONS>, [dostęp: 16 VI 2021].

¹² Dz.U. 2021, poz. 178.

Mając zatem na uwadze przywołane regulacje konstytucyjne oraz ustawowe, podmiotami uprawnionymi do otrzymywania od Szefów Agencji informacji, na zasadach i w trybie art. 18 ust. 1 ustawy o ABW oraz AW, są zarówno Prezes Rady Ministrów, jak również — z uwagi na usytuowanie w strukturze Rady Ministrów — wiceprezesa Rady Ministrów. Nadmienić należy, iż umocowanie wiceprezesa Rady Ministrów do uzyskiwania przedmiotowych informacji wynika jednak nie tylko z aktu powierzenia mu przez Prezesa Rady Ministrów określonych zadań i kompetencji (np. zakres jego działania określony rozporządzeniem, pełnienie funkcji przewodniczącego w Komitetach Rady Ministrów), ale także może być skutkiem faktycznego realizowania przez niego konkretnych zadań w danych okolicznościach faktycznych (np. przewodniczenie obradom Rady Ministrów podczas nieobecności Prezesa Rady Ministrów).

Ministrowie

Status ministra wynika z indywidualnego aktu powołania, zaś początkiem formalnego członkostwa w Radzie Ministrów jest moment złożenia przysięgi w sposób opisany w art. 151 Konstytucji RP. Trwa ono do momentu odwołania, względnie w sytuacji opisanej w art. 162 Konstytucji RP, do momentu powołania nowej Rady Ministrów. Z kolei z art. 147 w związku z art. 149 ust. 1 Konstytucji RP wynika, iż wykluczona jest natomiast sytuacja, w której minister nie ma żadnych innych zadań poza członkostwem w Radzie Ministrów i udziałem w jej posiedzeniach. Pozycja prawna ministra opisana została w art. 149 Konstytucji RP. Minister jest więc jednocześnie osobnym organem administracji rządowej i członkiem organu kolegialnego, Rady Ministrów.

Odwołując się do przepisów *ustawy z dnia 4 września 1997 r. o działach administracji rządowej* (Dz.U. 2020, poz. 1220), zwrócić należy uwagę na art. 3 ust. 1, ustalający szczegółowy zakres działania ministra kierującego określonym działem. Stanowi on, iż ustalenie szczegółowego zakresu działania ministra kierującego określonym działem następuje na zasadach określonych w przepisach wydanych na podstawie art. 33 ust. 1 pkt 1 *ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów*, z uwzględnieniem przepisów niniejszej ustawy. Przywołany przepis ustawy o Radzie Ministrów stanowi natomiast, iż Prezes Rady Ministrów ustala, w drodze rozporządzenia, szczegółowy zakres działania ministra niezwłocznie po powołaniu Rady Ministrów, a jeżeli minister został powołany w innym czasie — niezwłocznie po jego powołaniu.

Ustalenie zakresu działania właściwego ministra jest istotne z punktu widzenia zakresu informacji mogących mieć znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, możliwych do przekazania przez Szefów Agencji właściwemu ministrowi. Przepis art. 18 ust. 3 ustawy o ABW oraz AW wyposażył jednak w tym przypadku Prezesa Rady Ministrów w arbitralne uprawnienie kontrolne, polegające na wskazaniu przez niego innego (w tym siebie samego) adresata informacji pierwotnie przeznaczonych dla ministra.

Minister — Członek Rady Ministrów, Koordynator Służb Specjalnych

Na wstępie należy wskazać, iż stanowisko Koordynatora Służb Specjalnych, zwanego dalej „Koordynatorem”, znajduje umocowanie w przepisie ustawowym — art. 12 ust. 2 pkt 4 ustawy o ABW oraz AW, w którym wskazano, iż w skład Kolegium do spraw Służb Specjalnych wchodzi minister — członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, jeżeli został wyznaczony przez Prezesa Rady Ministrów. Już nawet sam ten przepis wskazuje na znaczącą rolę Koordynatora w systemie organów administracji publicznej związanych z bezpieczeństwem państwa.

Ponadto należy dodać, iż przypisana do tego stanowiska koordynacyjna rola w systemie nadzoru nad służbami specjalnymi, jako zastępującego w tym zakresie Prezesa Rady Ministrów, została potwierdzona w przepisie art. 13 ust. 7 ustawy o ABW oraz AW, który stanowi, iż Prezes Rady Ministrów może upoważnić ministra powołanego w celu koordynowania działalności służb specjalnych do wykonywania czynności, o których mowa w ust. 6, to jest żądania od szefów służb specjalnych informacji związanych z planowaniem i wykonywaniem powierzonych zadań.

Ponadto, na podstawie art. 33 ust. 1 przywołanej już wcześniej ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów zostało wydane rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra — Członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych (Dz.U. 2019, poz. 2273). Na podstawie przepisów tego rozporządzenia Prezes Rady Ministrów m.in. upoważnił Koordynatora do zapoznawania się z informacjami mogącymi mieć znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, o których mowa w art. 18 ust. 1 ustawy o ABW oraz AW.

W związku z tym można wnioskować, iż Prezes Rady Ministrów na podstawie wspomnianego upoważnienia, zawartego w akcie prawa powszechnie obowiązującego, upoważnił Koordynatora do wykonywania należytej mu kompetencji, nie ograniczając w żaden sposób zakresu tego uprawnienia. Dlatego też w świetle aktualnych przepisów prawa Koordynator, jako podmiot wywodzący swoje umocowanie z przepisów ustawowych, na podstawie przepisu rozporządzenia posiada analogiczny do Prezesa Rady Ministrów zakres dostępu do informacji przekazywanych w trybie art. 18 ustawy o ABW oraz AW.

Zakres przedmiotowy przekazywanych informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej

Informacje przekazywane przez Szefów Agencji podmiotom uprawnionym to informacje mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej. Ustawodawca nie zdecydował się jednak zdefiniować na potrzeby ustawy o ABW oraz AW rozumienia pojęć

zamieszczonych w przytoczonym sformułowaniu. W związku z tym w celu ustalenia ich znaczenia należy sięgnąć do systemu wykładni prawa z zachowaniem przyjętej wcześniej precedencji. Ustawodawca posłużył się w analizowanym przypadku słowem „może”, co oznacza, iż Szefowie Agencji mogą przekazywać podmiotom wskazanym w art. 18 ustawy o ABW oraz AW informacje uzyskane z różnych źródeł, na skutek wykonywania przez funkcjonariuszy Agencji pełnego spektrum czynności określonych ustawą o ABW oraz AW, w celu wypełniania zadań ustawowych Agencji, określonych odpowiednio w art. 5 i 6 ustawy o ABW oraz AW.

Na potrzeby interpretacji art. 18 ustawy o ABW oraz AW można uznać, iż międzynarodowa pozycja Rzeczypospolitej Polskiej związana jest ze środowiskiem międzynarodowym i dotyczy możliwości przeciwstawienia się negatywnym oddziaływaniom innych podmiotów międzynarodowych, tworząc warunki stabilnego i harmonijnego funkcjonowania i rozwoju państwa oraz zabezpieczając jego wartości i interesy. Natomiast bezpieczeństwo wewnętrzne państwa związane jest z jego stabilnością, harmonijnością funkcjonowania i rozwoju, zabezpieczeniem istotnych wartości interesów państwa przed zagrożeniami wewnętrznymi. *Najczęściej wśród składowych bezpieczeństwa wewnętrznego państwa wymienia się przede wszystkim trzy z nich: bezpieczeństwo publiczne, bezpieczeństwo powszechne oraz bezpieczeństwo ustrojowe*¹³.

W art. 18 ustawy o ABW oraz AW ustawodawca nałożył na Szefów Agencji, poddawany analizie w niniejszej opinii obowiązek informacyjny, dodając jednakże swoisty „filtr” w postaci kwantyfikatora „istotności” informacji mogących mieć znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej. Oznacza to zatem, że Szefowie Agencji są zobowiązani do przekazywania uprawnionym organom władzy wykonawczej informacji mogących mieć znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, lecz nie wszystkich posiadanych informacji, ale tylko takich, które mogą mieć istotne znaczenie z punktu widzenia realizacji konstytucyjnych i ustawowych zadań Prezydenta RP, Rady Ministrów czy konkretnego ministra, w zakresie powierzonych mu do realizacji zadań. Dodatkowa kwalifikacja treści tej normy prawnej poprzez użycie przymiotnika „istotne” wskazuje na wyraźną intencję ustawodawcy, aby informacje objęte zakresem tego przepisu były dodatkowo kwalifikowane przez pryzmat wywoływania istotnego, a więc *charakterystycznego, głównego, podstawowego, ważnego, zasadniczego*¹⁴, znaczenia dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej.

W świetle powyższego należy uznać, iż selekcja powyższych informacji powinna odbywać się przede wszystkim z uwzględnieniem przesłanki „istotnego znaczenia”, a także w oparciu o elastyczne kryteria uwzględniające okoliczności miejsca i czasu ich uzyskania oraz możliwości ich weryfikacji. W tym zakresie

¹³ B. Zdrowski, *Istota bezpieczeństwa państwa*, „Annales Universitatis Pedagogicae Cracoviensis, Studia de Securitate” 2019, nr 9 (3), s. 57.

¹⁴ *Słownik języka polskiego*, t. A-K, Wydawnictwo Naukowe PWN, Warszawa 1999, s. 759.

ustawodawca przewidział więc pewną autonomię w działaniu Szefów Agencji, pozostawiając w ich gestii ocenę spełnienia przez posiadane informacje kryterium „istotności” ich znaczenia, które pociąga za sobą, w przypadku ustalenia ich istotności na gruncie konkretnej sprawy, powinność Szefów Agencji przekazania tych informacji wskazanym organom władzy wykonawczej.

Dodać należy, iż art. 18 ustawy o ABW oraz AW nie różnicuje przekazywanych informacji z punktu widzenia przepisów *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. 2019, poz. 742), co oznacza, iż obowiązek informacyjny Szefów Agencji obejmuje zarówno informacje jawne, jak i niejawne *sensu largo*.

Konsekwencją przyznania Szefom Agencji autonomii decyzyjnej w kwestii uznania informacji za istotną i przekazania jej podmiotom wskazanym w art. 18 ustawy o ABW oraz AW jest to, że w przypadku nieuznania przez Szefów Agencji informacji za istotną bądź też ustalenia, że dotyczy ona podmiotów nieuprawnionych do jej uzyskania, analizowany obowiązek informacyjny Szefów Agencji zostaje ograniczony jedynie do ewentualnego przekazywania informacji, które pozostają jednak poza zakresem regulacji innego, istotnego z punktu widzenia niniejszej analizy, przepisu prawa zamieszczonego w art. 39 ust. 3 ustawy o ABW oraz AW. Zatem jeśli mamy do czynienia z innymi informacjami niejawnymi niż te mające istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, to przy przekazywaniu ich w innym trybie należy każdorazowo rozważyć ich zakres i ustalić, czy przekazanie tych informacji nie podlega zakazom ze wspomnianego art. 39 ust. 3 ustawy o ABW oraz AW. Oznacza to także, iż autonomia decyzyjna Szefów Agencji w zakresie uznania informacji za mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej nie doznaje na gruncie obowiązujących przepisów prawa ograniczeń, o których mowa w art. 39 ust. 3 ustawy o ABW oraz AW.

W tym kontekście, przechodząc na grunt regulacji art. 39 ustawy o ABW oraz AW, zauważyć należy, iż wprawdzie w ustępach 1 i 2 ustawodawca posłużył się zwrotem, iż Szefowie Agencji w zakresie swojego działania mogą zezwalać funkcjonariuszom i pracownikom Agencji oraz byłym funkcjonariuszom i pracownikom, po ustaniu stosunku służbowego lub stosunku pracy w Agencji, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych, oraz byłym funkcjonariuszom i pracownikom Urzędu Ochrony Państwa na udzielenie informacji niejawnej określonej osobie lub instytucji, to już w ust. 3 wskazano, iż wspomniane zezwolenie nie może dotyczyć udzielenia informacji o:

- 1) osobie, jeżeli zostały uzyskane w wyniku prowadzonych przez Agencje albo inne organy, służby lub instytucje państwowe czynności operacyjno-rozpoznawczych;
- 2) szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz o stosowanych w związku z ich prowadzeniem środkach i metodach;

- 3) osobie udzielającej pomocy Agencji, o której mowa w art. 36 ust. 1;
- 4) osobie udzielającej pomocy Urzędowi Ochrony Państwa w wykonaniu czynności operacyjno-rozpoznawczych.

Dodać należy, iż powyższy zakaz nie ma zastosowania w przypadku żądania prokuratora albo sądu zgłoszonego w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych. Zakazu tego nie stosuje się również w przypadku żądania prokuratora lub sądu uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych (art. 39 ust. 4–6 ustawy o ABW oraz AW).

Przytoczona regulacja stanowi rozwinięcie ustanowionej w art. 35 ust. 1 ustawy o ABW oraz AW podstawowej zasady funkcjonowania służby specjalnej przewidującej, że w związku z wykonywaniem swoich zadań Agencje zapewniają ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy Agencji. Owa ochrona jest immanentnie związana ze skutecznym realizowaniem przez ABW zadań przewidzianych w art. 5 ustawy o ABW oraz AW, a zatem także zadania polegającego na wypełnianiu przez Szefów Agencji — w ramach przyznanej im autonomii decyzyjnej — obowiązku informacyjnego, określonego w art. 18 ustawy o ABW oraz AW. O ile jednak przepisy art. 35 ust. 1 w związku z art. 39 ust. 3 ustawy o ABW oraz AW służą zapewnieniu Agencjom „szczelności informacyjnej”, to przepis art. 18 ustawy o ABW oraz AW pełni odmienną rolę, służy bowiem realizacji zadań przez organy władzy wykonawczej uprawnione do otrzymywania od Szefów Agencji informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej.

Jak już wskazano, art. 18 ustawy o ABW oraz AW statuuje obowiązek przekazywania przez Szefów Agencji informacji mogących mieć „istotne znaczenie” dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, co wyraźnie odróżnia zakres tych informacji od tych, na których udzielenie Szefowie Agencji mogą wyrazić zgodę na podstawie art. 39 ustawy o ABW oraz AW. O ile bowiem w art. 39 ustawy o ABW oraz AW mamy do czynienia z możliwością wyrażenia zezwolenia na udzielenie informacji niejawnej podmiotowi zewnętrznemu — z uwzględnieniem ograniczenia zakresu tych informacji z uwagi na zakazy, o których mowa w ust. 3 tego przepisu — to w art. 18 ustawy o ABW oraz AW uregulowano tę kwestię zupełnie inaczej, a mianowicie zastosowano jedynie ograniczenia zakresu przekazywanych informacji na podstawie kryterium ich „istotnego znaczenia” dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej.

Należy również wskazać, iż analizowane wyżej przepisy różnią się także od siebie konstrukcją zawartych w nich norm prawnych. W art. 18 ust. 1 i 3 ustawy o ABW oraz AW statuowany jest bowiem obowiązek działania Szefów Agencji niejako z urzędu, podczas gdy w art. 39 ustawy o ABW oraz AW mamy do

czynienia z uprawnieniem innego podmiotu do uzyskania informacji i autonomiczną decyzją Szefa ABW¹⁵ co do ewentualnego zezwolenia na ich udostępnienie podmiotowi zewnętrznemu (analogia do działania organu w trybie „na wnioski” w ramach uznania administracyjnego). Na podkreślenie zasługuje również odmiennosc tych przepisów wyrażona przez użycie w ich treści innych znamion czasownikowych, określających działanie Szefów Agencji, albowiem w art. 18 ustawy o ABW oraz AW mamy do czynienia z czasownikiem „przekazuje”, tj. nałożonym na Szefów Agencji obowiązkiem, zaś w art. 39 ustawy o ABW oraz AW zawarto czynność czasownikową w formie sformułowania „może zezwalać”, które wskazuje z kolei na uprawnienie Szefów Agencji w tym zakresie. Ponadto uwagę zwraca także zupełnie inny krąg adresatów tych norm — w art. 18 ustawy o ABW oraz AW mamy do czynienia z zamkniętym kręgiem podmiotów uprawnionych: Prezydent RP, Prezes Rady Ministrów i minister właściwy z uwagi na zakres jego działania, zaś w art. 39 ustawy o ABW oraz AW krąg ewentualnych wnioskujących o udzielenie informacji nie jest wprost wskazany i wynika z innych przepisów prawa, statuujących uprawnienia podmiotów zewnętrznych do uzyskiwania informacji od Szefów Agencji.

Oznacza to, że art. 18 ustawy o ABW oraz AW i art. 39 ustawy o ABW oraz AW regulują zupełnie odrębne od siebie tryby, które pomimo tego, że dotyczą czynności związanych z przekazywaniem informacji przez Szefów Agencji na zewnątrz, nie są ze sobą powiązane i stosowanie art. 18 ustawy o ABW oraz AW nie jest uzależnione od treści art. 39 ustawy o ABW oraz AW.

Potwierdzenie słuszności tego stwierdzenia można odnaleźć także w pracach legislacyjnych, które toczyły się w 2014 r. nad projektem ustawy o Agencji Bezpieczeństwa Wewnętrznego (druk sejmowy nr 2295 w VII kadencji Sejmu RP). Z uzasadnienia do wspomnianego projektu ustawy wynika, iż dotychczasowy art. 18 ustawy o ABW oraz AW, ustanawiający zasady przekazywania przez Szefa ABW informacji innym organom, został przeniesiony z rozdziału „Organizacja ABW oraz AW” do rozdziału z postanowieniami ogólnymi (projektowany art. 5 ustawy o ABW oraz AW). Zaproponowana zmiana dotyczyła m.in. ograniczenia możliwości żądania przez Prezydenta RP oraz Prezesa Rady Ministrów od Szefa ABW niektórych kategorii informacji przez wyłączenie informacji o osobach udzielających Agencji pomocy w wykonywaniu czynności operacyjno-rozpoznawczych oraz informacji o szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych, a także o stosowanych w związku z ich prowadzeniem środkach i metodach. Uzasadniano to następująco: *szczególną wrażliwością tego typu informacji i koniecznością dołożenia najwyższych starań w celu ich ochrony*. Z powyższego faktu można zatem wysnuć wniosek, iż skoro w 2014 r. proponowano wprowadzenie takiego przepisu do ustawy o ABW oraz AW, to w obowiązujących wówczas przepisach (które obowiązują również

¹⁵ Szerzej na ten temat zob. M. Bożek, *Sejmowa kontrola działalności służb specjalnych i jej ograniczenia wynikające z ustaw kompetencyjnych. Zarys problemu na tle uwarunkowań normatywnych*, „Studia Iuridica Lublinensia” 2013, t. 20.

i obecnie) nie było takiego zakazu i przekazywanie informacji w trybie art. 18 ustawy o ABW oraz AW nie było obwarowane ograniczeniami wynikającymi z art. 39 ust. 3 ustawy o ABW oraz AW. Dodanie tego przepisu miało zatem na celu wprowadzenie *novum* w postaci ograniczenia w przekazywaniu informacji, w trybie art. 5 ustawy o ABW oraz AW (zastępującego dotychczasowy art. 18 ustawy o ABW oraz AW).

Podsumowanie

Podsumowując powyższe rozważania, wyraźnie należy podkreślić, iż na podstawie art. 18 ustawy o ABW oraz AW Szefowie Agencji są uprawnieni, a wręcz zobowiązani, do przekazywania podmiotom uprawnionym informacji mogących mieć istotne znaczenie dla bezpieczeństwa i pozycji międzynarodowej Rzeczypospolitej Polskiej. Co więcej, przekazywanie tych informacji — w trybie art. 18 ustawy o ABW oraz AW — nie napotyka na ograniczenia co do zakresu, w jakim mają być przekazane, w przeciwnym bowiem razie ograniczałoby to skuteczną realizację zadań organów władzy wykonawczej uprawnionych do otrzymywania tych informacji. W przypadku braku uznania przez Szefa ABW informacji za „istotną” albo gdy odbiorcą informacji ma być podmiot niezaliczony do podmiotów uprawnionych wymienionych w art. 18, a informacje mające być przedmiotem przekazania są zaklasyfikowane jako informacje niejawne, to przy ich przekazywaniu w innym trybie należy każdorazowo rozważyć ich zakres i ustalić, czy przekazanie ich nie podlega zakazom ze wspomnianego art. 39 ust. 3 ustawy o ABW oraz AW.

Magdalena Gołaszewska

Rozdział 2.

Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny

Wstęp

Na pierwszy plan w działalności Agencji Bezpieczeństwa Wewnętrznego, już nawet wnioskując z samej nazwy instytucji, wysuwa się zagadnienie bezpieczeństwa wewnętrznego państwa. Potwierdzenie tej tezy odnajdziemy w art. 1 ustawy o ABW oraz AW, który stanowi, iż Agencja Bezpieczeństwa Wewnętrznego jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Jednakże tak ogólne sformułowanie pozwala jedynie na wskazanie ogólnego zarysu obszaru działalności tej instytucji, a doprecyzowanie zakresu jej działania wynika z art. 5 ust. 1 ustawy o ABW oraz AW. Z analizy tego przepisu wynika, iż oprócz zwalczania przestępstw wymienionych w ust. 1 pkt 2 ustawy o ABW oraz AW i ujawniania mienia zagrożonego przypadkiem w związku z tymi przestępstwami, rozpoznawania, zapobiegania i wykrywania zagrożeń godzących w bezpieczeństwo systemów teleinformatycznych (ust. 1 pkt 2 a), realizowania zadań związanych z ochroną informacji niejawnych (ust. 1 pkt 3), uzyskiwania i przetwarzania informacji mogących mieć znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego (ust. 1 pkt 4) i innych działań określonych w ustawach i umowach międzynarodowych (ust. 1 pkt 5) zadaniem Agencji Bezpieczeństwa Wewnętrznego jest rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa. Dlatego też już samo umiejscowienie tego zadania jako pkt 1 w art. 5 ust. 1 ustawy o ABW oraz AW, wymienającym poszczególne zadania ustawowe, wskazuje również

na priorytetowe czy wręcz podstawowe znaczenie tej tematyki we właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego.

Czym jednak jest dokładnie owo „bezpieczeństwo wewnętrzne” i jakie zagrożenia przeciw niemu skierowane stanowią zasadnicze kierunki zainteresowania Agencji Bezpieczeństwa Wewnętrznego? Odpowiedź na to pytanie nie wynika wprost jedynie z lektury przepisów prawa, ale wymaga poczynienia dodatkowych rozważań na gruncie teoretycznym oraz odniesienia do dotychczasowej praktyki funkcjonowania tej służby.

O ile łatwo jest bowiem odkodować zakres właściwości Agencji Bezpieczeństwa Wewnętrznego w ramach zadania wymienionego w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, albowiem zostało ono sformułowane przy pomocy wskazania rozpoznawania, zapobiegania i wykrywania konkretnych przestępstw oraz ścigania ich sprawców, to konstrukcja pkt 1 może nastroczać pewne problemy interpretacyjne z uwagi na zawarte w jego treści ogólne sformułowania (klauzule generalne), które nie zostały legalnie zdefiniowane.

Celem niniejszego rozdziału jest zatem próba sprecyzowania zakresu działań podejmowanych przez Agencję Bezpieczeństwa Wewnętrznego w celu rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne oraz porządek konstytucyjny państwa, które na użytek niniejszego rozdziału zostały określone jako „działania prewencyjne” oraz przedstawienie środków służących do realizacji tego zadania. W niniejszej pracy wykorzystano, oprócz metody dogmatycznej polegającej na analizie przepisów prawa i tekstów z literatury prawniczej, także analizę porównawczą rozwiązań przyjętych w polskich służbach specjalnych, służbach innych państw europejskich oraz analizę historyczną polskiego systemu prawnego w przeszłości i wpływu zmian na obecne rozwiązania prawne w omawianym zakresie.

Bezpieczeństwo wewnętrzne państwa i porządek konstytucyjny jako pojęcia wyznaczające właściwość Agencji Bezpieczeństwa Wewnętrznego w zakresie działań prewencyjnych

Bez wątpienia punktem wyjścia do dalszych rozważań winno być przybliżenie znaczenia terminu „bezpieczeństwo”, który zgodnie z definicją słownikową rozumiany jest jako stan niezagrożenia, spokoju, pewności¹. Pojęcie to jest też definiowane jako teoria i praktyka zapewniania możliwości przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności przez wykorzystywanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukcja ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów².

¹ *Słownik języka polskiego*, t. 1, s. 139.

² <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html>, [dostęp: 14 IV 2021].

Próbując zdefiniować sformułowanie „bezpieczeństwo wewnętrzne państwa”, należy zauważyć, iż już samo jego znaczenie językowe wskazuje, iż obejmuje ono funkcjonowanie państwa w jego sferze wewnętrznej. O bezpieczeństwo wewnętrzne dba się w obrębie granic państwowych³. Wspomniane ujęcie bezpieczeństwa wewnętrznego jest spójne z klasyczną definicją pojęcia „państwo” autorstwa Jerzego Jellinka, zgodnie z którą państwo jest konglomeratem trzech elementów: terytorium, ludności i władzy⁴.

Na pierwszy rzut oka wydaje się, że termin „bezpieczeństwo wewnętrzne” można zdefiniować na zasadzie prostego rozróżnienia sfery wewnętrznego działania państwa od jego stosunków zewnętrznych (bezpieczeństwo zewnętrzne). Przez wiele lat taki podział był stosowany i niekwestionowany; w sferze wewnętrznej zapewniano porządek i bezpieczeństwo na określonym terytorium przy użyciu prawa i instytucji je egzekwujących, a w sferze zewnętrznej ochraniało terytorium i zamieszkującą je ludność przy użyciu sił zbrojnych. Tym samym przez bezpieczeństwo wewnętrzne rozumiano wszystko to, co wiązało się ze stabilnością i porządkiem na danym terytorium; działania te należały do właściwości organów policji, bezpieczeństwa (służby kontrwywiadowcze) i innych podmiotów zajmujących się zwalczaniem skutków katastrof, zaś przez bezpieczeństwo zewnętrzne rozumiano ochronę i obronę przed zagrożeniami ze środowiska międzynarodowego, za które odpowiadały siły zbrojne i służby wywiadowcze.

Należy zaznaczyć, iż „bezpieczeństwo wewnętrzne” nie jest pojęciem ściśle zdefiniowanym w przepisach prawa, jednakże podejmując próbę opisanego terminu i analizując system prawa pod kątem „bezpieczeństwa wewnętrznego”, należy rozpocząć rozważania od przepisów Konstytucji RP⁵. Lektura przepisów ustawy zasadniczej prowadzi do wniosku, iż pojęcie „bezpieczeństwo wewnętrzne” nie zostało w niej zdefiniowane legalnie, ale odnajdziemy w jej treści użyte kilka razy sformułowanie „bezpieczeństwo” lub „bezpieczeństwo państwa”. Pojęciem „bezpieczeństwo wewnętrzne” posłużył się prawodawca jedynie w dwóch przepisach — w art. 135 statuującym Radę Bezpieczeństwa Narodowego jako organ doradczy Prezydenta Rzeczypospolitej Polskiej w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa i w art. 146 ust. 4 pkt 7, wskazującym na zadanie Rady Ministrów w zakresie zapewnienia bezpieczeństwa wewnętrznego oraz porządku publicznego.

Można również dodać, iż inne akty prawa powszechnie obowiązującego także jedynie posługują się sformułowaniem „bezpieczeństwo wewnętrzne”, ale go nie definiują w swojej treści. Takie przepisy możemy odnaleźć np. w *ustawie z dnia 6 czerwca 1997 r. Kodeks karny*⁶, w art. 112, który dotyczy popełnienia prze-

³ K.P. Marczuk, *Bezpieczeństwo wewnętrzne w perspektywie kosmopolityzmu*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, t. 11/14, s. 167.

⁴ Tamże.

⁵ Dz.U. 1997, nr 78, poz. 483 z późn. zm.

⁶ Dz.U. 2020, poz. 1444.

stępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej oraz w *ustawie z dnia 11 września 2019 r. Prawo zamówień publicznych*⁷, w art. 405 dotyczącym wykluczenia wykonawców z postępowania o udzielenie zamówienia w dziedzinach obronności i bezpieczeństwa w przypadku uzyskania zawiadomienia od instytucji właściwych w sprawach ochrony bezpieczeństwa wewnętrznego lub zewnętrznego państwa.

Tak więc, jak już wyżej wskazano, ustawodawca posługuje się pojęciem „bezpieczeństwo wewnętrzne”, jednakże nie definiuje go na gruncie przepisów ustawowych. Dlatego też próba sprecyzowania zakresu tego pojęcia wymaga analizy literatury z zakresu prawa konstytucyjnego, administracyjnego, a w szczególności piśmiennictwa z dziedziny problematyki bezpieczeństwa państwa. W literaturze odnajdziemy bowiem twierdzenie, że bezpieczeństwo wewnętrzne państwa związane jest z jego stabilnością, harmonijnością funkcjonowania i rozwoju, zabezpieczeniem istotnych wartości i interesów państwa przed czynnikami (zagrożeniami) wewnętrznymi. Dotyczy ono zapewnienia realizacji interesów zarówno całego państwa, ogółu społeczeństwa, ale i jego poszczególnych obywateli przez dostępny potencjał diagnozowania i reagowania na wszelkie zagrożenia wewnętrzne godzące w te interesy⁸. W wielu innych publikacjach pojawiały się kolejne próby zdefiniowania tego pojęcia⁹. Jednakże z uwagi na złożoność problematyki oraz pewną niespójność terminologiczną stworzenie kompleksowej definicji pojęcia „bezpieczeństwo wewnętrzne” wydaje się być zadaniem bardzo trudnym.

Na uwagę zasługuje definicja zaproponowana przez prof. Konstantego Wojtaszczyka, zgodnie z którą „bezpieczeństwo wewnętrzne” to taki stan funkcjonowania państwa, który zapewnia przeciwdziałanie, eliminowanie, ograniczanie zagrożeń dla ustroju konstytucyjnego, porządku wewnętrznego i spokoju oraz umożliwia ochronę interesu publicznego poszczególnych społeczności i każdego obywatela. Bezpieczeństwo wewnętrzne jest obok bezpieczeństwa zewnętrznego jednym z dwóch rodzajów bezpieczeństwa, dla których kryterium wyróżnienia stanowi obszar państwa¹⁰.

Wskazany przez prof. Konstantego Wojtaszczyka oraz opisywany przez innych przedstawicieli doktryny podział na bezpieczeństwo wewnętrzne i zewnętrzne państwa znajduje odzwierciedlenie np. w ustawie o ABW oraz AW (właściwość Agencji Bezpieczeństwa Wewnętrznego w odróżnieniu od zadań Agencji Wywiadu), albowiem działająca na podstawie przepisów tej samej ustawy Agencja Wywiadu jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego

⁷ Dz.U. 2019, poz. 2019 z późn. zm.

⁸ B. Zdrodowski, *Istota bezpieczeństwa państwa*, „Annales Univeristatis Pedagogicae Cracoviensis, Studia de Securitate” 2019, t. 9 (3), <https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/10/4-1.pdf>, [dostęp: 20 IV 2021] s. 57.

⁹ Tak m.in. S. Sulowski, *W poszukiwaniu definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1/09, s. 10–13.

¹⁰ K. Wojtaszczyk, *Istota i dylematy bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1/09, s. 14.

państwa. Powyższe wskazuje, iż ustawodawca wprowadził rozdział bezpieczeństwa wewnętrznego od bezpieczeństwa zewnętrznego państwa m.in. przez ustanowienie dwóch służb przewidzianych do zapewnienia bezpieczeństwa państwa w obu odrębnych aspektach.

Z kolei odnosząc się do kolejnego sformułowania, zawartego w art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW („porządek konstytucyjny”), należy wskazać, iż bez wątpienia odnosi się ono do ochrony wartości określonych w Konstytucji RP. W doktrynie pojęcie to zostało zdefiniowane jako całokształt organów instytucji państwowych i ich poczynań oraz system reguł gwarantujących ciągłość konstytucyjnego ustroju państwa, a w tym ochronę informacji niejawnych, osób, obiektów i urządzeń istotnych dla bezpieczeństwa narodowego, a także wolności, praw oraz obowiązków człowieka i obywatela¹¹.

Należy także podkreślić, iż zgodnie z art. 10 Konstytucji RP ustrój Rzeczypospolitej Polskiej opiera się na podziale i równowadze władzy ustawodawczej, wykonawczej i sądowniczej. Władzę ustawodawczą sprawują Sejm i Senat, wykonawczą Prezydent Rzeczypospolitej Polskiej i Rada Ministrów, a sądowniczą sądy i trybunały. Wszystkie trzy rodzaje władzy (a także inne, niewymienione w tym rozdziale oraz niemieszczące się w klasycznym trójpodziale władzy organy konstytucyjne, jak Rzecznik Praw Obywatelskich, Krajowa Rada Radiofonii i Telewizji) tworzą organizację państwową, tak więc zagrożenie dla funkcjonowania którejkolwiek z nich stanowi zagrożenie dla bezpieczeństwa państwa. Należałoby więc uznać, że pojęcie „bezpieczeństwa państwa” obejmuje swym zakresem pojęcie „porządku konstytucyjnego” jako stanu, w którym najwyższe organy państwa wykonują swoje zadania określone w Konstytucji RP, w sposób określony w tym akcie.

Tak rozumiane bezpieczeństwo państwa jest wartością, którą chronić powinny wszelkie jego organy. Kluczowe kompetencje w zakresie ochrony bezpieczeństwa państwa Konstytucja RP powierza Radzie Ministrów, albowiem w art. 146 nakłada na Radę Ministrów m.in. następujące obowiązki: zapewnienie bezpieczeństwa wewnętrznego państwa i porządku publicznego oraz bezpieczeństwa zewnętrznego państwa. Bez wątpienia działalność Agencji Bezpieczeństwa Wewnętrznego służy wykonaniu jednego ze wskazanych wyżej konstytucyjnych obowiązków Rady Ministrów. Szef Agencji Bezpieczeństwa Wewnętrznego jest bowiem centralnym organem administracji rządowej podporządkowanym bezpośrednio Prezesowi Rady Ministrów, odpowiedzialnym za bezpieczeństwo wewnętrzne państwa oraz porządek konstytucyjny zgodnie z art. 1 i 3 ust. 1–2 ustawy o ABW oraz AW.

Porządek konstytucyjny jest także określany jako stan ładu i funkcjonowania państwa zgodnie z normami określonymi w ustawie zasadniczej¹². Wyraźnym

¹¹ W. Kitler, *Organizacja bezpieczeństwa narodowego RP w kontekście ochrony ładu wewnętrznego państwa*, „Zeszyty Naukowe AON” 2013, t. 4 (93), s. 233.

¹² B. Wiśniewski i in., *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004, s. 12.

przejawem panującego w Rzeczypospolitej Polskiej porządku konstytucyjnego są powstałe na gruncie Konstytucji RP naczelne zasady, które wprost wskazują na chronione w tym zakresie dobra, jakimi są m.in: suwerenność narodu (art. 4), demokratyczne państwo prawne (art. 2), podział władzy i równowaga władz (art. 10), wolności i prawa człowieka i obywatela (rozdział 2), parlamentarna forma rządów, odrębność władzy sądowniczej oraz niezawisłość sądów i trybunałów (art. 173), a także społeczna gospodarka rynkowa (art. 20), własność prywatna (art. 21) oraz wolność gospodarcza (art. 22)¹³.

Dlatego też działania Agencji Bezpieczeństwa Wewnętrznego winny być nakierowane na zapewnienie bezpieczeństwa państwa także i w aspekcie wspomnianych wyżej zasad konstytucyjnych oraz sprawnego funkcjonowania konstytucyjnych organów państwa.

Należy także zwrócić uwagę na to, iż w brzmieniu art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW oprócz wspomnianych już wyżej pojęć podjęto próbę doprecyzowania zakresu tego zadania przez przykładowe wyliczenie pewnych elementów składających się na chronione wartości: *w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność terytorium, a także obronność państwa*. I tak, przez wskazanie wprost w treści art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW na „suwerenność i międzynarodową pozycję” ustawodawca położył szczególny nacisk na działania Agencji Bezpieczeństwa Wewnętrznego nakierowane na suwerenność rozumianą jako niezależność władzy państwowej w stosunkach z innymi państwami i organizacjami międzynarodowymi¹⁴. Można więc stwierdzić, iż priorytetem działania Agencji Bezpieczeństwa Wewnętrznego w tym zakresie winna być zdolność Rzeczypospolitej Polskiej do samodzielnego, niezależnego od innych podmiotów, sprawowania władzy nad określonym terytorium. Wewnętrzna suwerenność państwa przejawia się w tym, że władza państwowa jest najwyższa na danym obszarze i sama decyduje o zakresie swoich kompetencji, a wszystkie inne instytucje i organy funkcjonują za jej zgodą i na warunkach przez nią określonych. Z kolei zewnętrzna suwerenność państwa przejawia się w realizacji przez nie celów niezależnych od innych państw i ochronie interesów danego państwa¹⁵.

Ponadto ochronie winny podlegać także takie wartości, jak: „niepodległość”, czyli niezależność jednego państwa (narodu) od innych państw w sprawach wewnętrznych i zewnętrznych¹⁶ oraz „nienaruszalność” rozumiana jako brak naruszenia, brak pogwałcenia, nietykalność¹⁷ terytorium państwa. Użycie tych zwrotów wskazuje na intencję ustawodawcy w zakresie doprecyzowania katalogu zagrożeń bezpieczeństwa wewnętrznego przez odniesienie do

¹³ W. Kitler, dz. cyt., s. 233.

¹⁴ *Słownik języka polskiego*, t. 3, s. 349.

¹⁵ B. Wiśniewski, *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2013, s. 30.

¹⁶ *Słownik języka polskiego*, t. 2, s. 330.

¹⁷ Tamże, s. 324.

fundamentalnych wartości, które winny podlegać ochronie w odniesieniu do państwa jako instytucji w zakresie jego niezależności od innych państw lub podmiotów zewnętrznych oraz bezpieczeństwa jego terytorium i granic.

W treści analizowanego przepisu mamy także wskazaną „obronność państwa”, która zgodnie ze współcześnie wypracowaną definicją jest dziedziną bezpieczeństwa narodowego i obejmuje zintegrowane przeciwstawianie się zagrożeniom polityczno-militarnym przy wykorzystaniu wszystkich — wojskowych i cywilnych — zasobów państwa, zorganizowanych w system obronności¹⁸. Należy zatem przyjąć, iż oprócz sił zbrojnych Rzeczypospolitej Polskiej także i Agencja Bezpieczeństwa Wewnętrznego pełni rolę w tym obszarze, w szczególności w zakresie rozpoznawania wymienionych zagrożeń w przestrzeni wewnętrznej.

Jak już wyżej wskazano, wyliczenie tych pojęć nie ma charakteru zamkniętego, na co oczywiście wskazuje użyty w treści przepisu zwrot „w szczególności”. Pozwala to także na zakwalifikowanie do tego zakresu innych, niezbędnych wartości, które zostaną uznane za element „bezpieczeństwa wewnętrznego” lub „porządku konstytucyjnego”. Jednakże przy analizowaniu decyzji o podjęciu przez Agencję działań w zakresie zagrożenia, które nie zostało *expressis verbis* sformułowane w treści art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW, należy przeprowadzić głęboką analizę istoty tego zagadnienia w kontekście zakwalifikowania go jako niebezpieczeństwa skierowanego przeciwko bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu państwa. Należy również mieć na uwadze fakt, iż Szef Agencji Bezpieczeństwa Wewnętrznego jako organ władzy publicznej winien działać, na podstawie zasady legalizmu wynikającej z art. 7 Konstytucji RP, na podstawie i w granicach prawa. Zgodnie z założeniami doktryny¹⁹ i linią orzecniczą w tym zakresie²⁰ do działalności organów publicznych nie stosuje się bowiem zasady „co nie jest zakazane jest dozwolone” lecz regułę „dozwolone jest tylko to, co prawo wyraźnie przewiduje”.

Powyższe rozważania prowadzą do wniosku, iż art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW nie definiuje wprost pojęć „bezpieczeństwo wewnętrzne” i „porządek konstytucyjny”, ale w literaturze przedmiotu można znaleźć pogląd, iż takie definicje można odtworzyć pośrednio na podstawie treści wskazanej ustawy, biorąc pod uwagę dziedziny, którymi zajmuje się Agencja Bezpieczeństwa Wewnętrznego (w tym także obejmując swoim zakresem przeciwdziałanie przestępstwom wymienionym w ustawie oraz ochronę informacji niejawnych)²¹.

¹⁸ S. Koziej, *Obronność Rzeczypospolitej Polskiej w latach 1989–2009*, Warszawa 2010, s. 36.

¹⁹ Tak m.in. M. Florczak-Wątor, *Komentarz do art. 7 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radzewicz, WKP, Warszawa 2019, System Lex.

²⁰ Por. m.in. wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 15 stycznia 1997 r., sygn. akt III SA 534/96, „Monitor Podatkowy” 1997/12/374 (Lex 31 185) oraz wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 24 maja 1993 r., sygn. akt III SA 2017/92, OSNSA 1993/4/113 (Lex nr 10 400).

²¹ A. Barcikowski, *Bezpieczeństwo wewnętrzne różne perspektywy analityczne i doktrynalne*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, nr 11/14, s. 16.

Dlatego też „bezpieczeństwo wewnętrzne państwa i porządek konstytucyjny” jako wartości, do ochrony których powołana jest Agencja Bezpieczeństwa Wewnętrznego, można rozumieć jako dążenie do sytuacji, w której organy państwa mogą sprawnie działać i wypełniać prawidłowo swoje obowiązki wynikające z Konstytucji RP.

Działania prewencyjne w zakresie bezpieczeństwa państwa — analiza historyczna i prawnoporównawcza

Skoro już został ustalony teoretyczny zakres pojęć „bezpieczeństwo wewnętrzne” i „porządek konstytucyjny”, możemy przejść do bardziej szczegółowych rozważań na temat zagrożeń, jakie mogą pojawić się w tym obszarze działalności prewencyjnej organów państwowych. Dywagacje te należy rozpocząć od stwierdzenia, iż zagadnienie ochrony bezpieczeństwa państwa, rozumiane jako działanie w zakresie prowadzenia działań prewencyjnych (rozpoznawania i zwalczania zagrożeń), godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny, kształtowało się w polskim prawie w ciągu wielu lat, a historia działań aparatu państwowego w tym zakresie sięga już czasów powojennych.

Tytułem przypomnienia można wskazać, iż w strukturach utworzonego w lipcu 1944 r. Polskiego Komitetu Wyzwolenia Narodowego²² funkcjonował resort bezpieczeństwa, który składał się z wydziału kontrwywiadu i działu zaopatrzenia technicznego. W następnych latach działał on w ramach Ministerstwa Bezpieczeństwa Publicznego utworzonego na podstawie *ustawy z dnia 31 grudnia 1944 r. o powołaniu Rządu Tymczasowy Rzeczypospolitej Polskiej z przekształcenia Polskiego Komitetu Wyzwolenia Narodowego w Rząd Tymczasowy Rzeczypospolitej Polskiej*²³. Mocą *dekretu z dnia 7 grudnia 1954 r. o naczelnym organach administracji państwowej w zakresie spraw wewnętrznych i bezpieczeństwa publicznego*²⁴ sprawy z zakresu bezpieczeństwa publicznego zostały powierzone Komitetowi do spraw Bezpieczeństwa Publicznego. Natomiast w *ustawie z dnia 13 listopada 1956 r. o zmianie organizacji naczelnym organów administracji publicznej w zakresie bezpieczeństwa publicznego*²⁵ sprawy ochrony ustroju ludowo-demokratycznego określonego w Konstytucji Polskiej Rzeczypospolitej Ludowej i interesów państwa przed wrogą działalnością szpiegowską i terrorystyczną powierzono Ministrowi Spraw Wewnętrznych.

Zgodnie zaś z *ustawą z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów* Minister Spraw Wewnętrznych został ustanowiony naczelnym organem administracji państwowej w dziedzinie ochrony bezpieczeństwa państwa i porządku publicznego, a także ochrony przed bezprawnymi zamachami na życie i zdrowie ludzkie oraz

²² Dz.U. 1944, nr 1, poz. 1.

²³ Dz.U. 1994, nr 19, poz. 99.

²⁴ Dz.U. 1954, nr 54, poz. 269 z późn. zm.

²⁵ Dz.U. 1956, nr 54, poz. 241.

dorobek materialny i kulturalny społeczeństwa²⁶. W myśl przepisów tej ustawy do zakresu działania Ministra Spraw Wewnętrznych należały np. sprawy ochrony bezpieczeństwa państwa, w tym zwalczanie szpiegostwa, terroryzmu, dywersji i sabotażu i innych zasad godzących w konstytucyjne zasady ustrojowe Polskiej Rzeczypospolitej Ludowej, jak również koordynowanie działań w zakresie ochrony tajemnicy państwowej i służbowej oraz kontrola ruchu międzynarodowego. Minister Spraw Wewnętrznych wykonywał swoje zadania za pośrednictwem Służby Bezpieczeństwa i Milicji Obywatelskiej, podległych mu jednostek wojskowych oraz straży pożarnej. W ustawie tej wskazano również, iż ochrona bezpieczeństwa państwa i porządku publicznego należała do podstawowych zadań Służby Bezpieczeństwa i Milicji Obywatelskiej.

Z chwilą powołania Urzędu Ochrony Państwa Służba Bezpieczeństwa została rozwiązana. W ustawie z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa²⁷, w art. 1 ust. 1, utworzono Urząd Ochrony Państwa, którego celem działania była ochrona bezpieczeństwa państwa i jego porządku konstytucyjnego. Zgodnie z ust. 2 pkt 1 tego przepisu do zadań Urzędu Ochrony Państwa należało m.in. rozpoznawanie i przeciwdziałanie zagrożeniom godzącym w bezpieczeństwo, obronność, niezależność i całość państwa. To wówczas w zakresie uregulowania właściwości Urzędu Ochrony Państwa pojawiło się sformułowanie „rozpoznawanie i przeciwdziałanie zagrożeniom”, doprecyzowane przez określenie, iż chodzi o zagrożenia „godzące w bezpieczeństwo i obronność państwa”. Na tym etapie funkcjonowania służby mieliśmy już do czynienia z ustawowo wskazanym działaniem w zakresie „zagrożeń”, a dokładniej ich rozpoznawaniem i przeciwdziałaniem ich powstaniu, oraz ogólnym sformułowaniem „bezpieczeństwo państwa i jego porządek konstytucyjny”.

W ustawie o Agencji Bezpieczeństwa Wewnętrznego to zadanie opisano już bardziej szczegółowo i wskazano, iż do zadań Agencji Bezpieczeństwa Wewnętrznego należy rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa.

Z uzasadnienia do projektu ustawy o ABW oraz AW wynika, iż ustawowe zadania Agencji Bezpieczeństwa Wewnętrznego określone zostały jako *zagrożenia godzące w bezpieczeństwo państwa* z przykładowo wskazanymi obszarami, w jakich zagrożenia te mogą wystąpić (np. suwerenność, międzynarodowa pozycja państwa, obronność kraju lub nienaruszalność i niepodzielność jego terytorium). Wskazano również, że do zadań Agencji Bezpieczeństwa Wewnętrznego należy zaliczyć m.in. rozpoznawanie, zapobieganie i zwalczanie zagrożeń porządku konstytucyjnego. A zatem naruszenie norm prawnych, wyrażających nakazy i zakazy określonego postępowania, lub naruszenie przepisów ustaw zawierających określone ograniczenia, których źródłem jest Konstytucja RP,

²⁶ Dz.U. 1983, nr 38, poz. 172 z późn. zm.

²⁷ Dz.U. 1990, nr 30, poz. 180.

należać będzie do właściwości Agencji, jeśli naruszenia tego porządku stanowią zagrożenie dla bezpieczeństwa państwa. Pozostały katalog zadań Agencji Bezpieczeństwa Wewnętrznego obejmować miał dotychczasowe zadania Szefa Urzędu Ochrony Państwa w zakresie nie wkraczającym w kompetencje Szefa Agencji Wywiadu²⁸. Należy dodać, iż zacytowane wyżej brzmienie przepisu określającego działania prewencyjne nie uległo zmianie w ciągu niemal już 20 lat obowiązywania ustawy o ABW oraz AW.

Poruszając się w zakresie działań prewencyjnych, nie sposób nie odnieść się do właściwości pozostałych instytucji działających w Rzeczypospolitej Polskiej w obszarze zapewnienia bezpieczeństwa, a w szczególności do zakresu zadań powierzonych służbom specjalnym. Na wstępie należy zauważyć, iż w polskim systemie prawa nie ma legalnej definicji tego pojęcia, ale w art. 11 ustawy o ABW oraz AW pojawiło się normatywne określenie jego zakresu przez wymienienie służb uznawanych za specjalne, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego. Owa definicja ma charakter *stricte* podmiotowy, jedynie wskazuje poszczególne służby objęte jej zakresem, nie określa zaś ich cech instytucjonalnych czy też ich obszarów działalności.

Z uwagi na fakt, iż w Rzeczypospolitej Polskiej uprawnienia do wykonywania czynności operacyjno-rozpoznawczych mają nie tylko wymienione służby specjalne, ale także inne podmioty (np. Policja, Straż Graniczna, Żandarmeria Wojskowa, Służba Ochrony Państwa), można zatem owe podmioty uprawnione podzielić na dwie kategorie — na służby specjalne, które tradycyjnie wykonują zadania wywiadowcze i kontrwywiadowcze oraz inne służby, które zajmują się szeroko rozumianym bezpieczeństwem państwa, tzw. służby policyjne²⁹.

Służby policyjne wykonują zadania dotyczące bezpieczeństwa i porządku publicznego, w szczególności w zakresie życia, zdrowia i mienia, czyli odpowiadają za bezpieczeństwo państwa w sferze życia publicznego (bezpieczeństwo obywateli). Służby specjalne natomiast zajmują się bezpieczeństwem państwa w zakresie ochrony struktur organizacyjnych państwa, ram instytucjonalnych, w których kształtuje się życie publiczne i gospodarcze kraju (bezpieczeństwo instytucji). W demokratycznym państwie prawnym o kształcie tych ram decydują zasady i normy prawne regulujące organizację i funkcjonowanie systemu organizacyjnego państwa. Całokształt tych zasad i norm wynika przede wszystkim z ustawy zasadniczej i stanowi treść porządku konstytucyjnego państwa³⁰. Na podstawie tak przyjętego podziału wyprowadzono tezę, iż służby specjalne powinny mieć wiedzę o zagrożeniach, zaś służby policyjne mają wykrywać i ścigać sprawców tych zagrożeń (przestępstw)³¹.

²⁸ [https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/\\$file/276.pdf](https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/$file/276.pdf), [dostęp: 23 IV 2021].

²⁹ M. Bożek i in., *Służby specjalne w strukturze władz publicznych*, Lex a Wolters Kluwers business, Warszawa 2014, s. 15.

³⁰ M. Bożek i in., dz. cyt., s. 31.

³¹ Tamże, s. 129.

Na potrzeby niniejszego rozdziału uwagę skupimy na służbach specjalnych, dla porządku wskazując, iż dwie z tych służb zostały powołane do zapewnienia bezpieczeństwa w aspekcie zewnętrznym — Agencja Wywiadu, która działa na mocy przepisów ustawy o ABW oraz AW i jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa (sfera cywilna) oraz Służba Wywiadu Wojskowego, działająca na podstawie przepisów ustawy o SKW oraz SWW³², która jest właściwa w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej (sfera wojskowa).

Pozostałe trzy służby specjalne zajmują się sprawami *stricto* wewnętrznymi, z których oprócz wspomnianej wyżej Agencji Bezpieczeństwa Wewnętrznego Służba Kontrwywiadu Wojskowego na podstawie art. 1 ustawy o SKW oraz SWW jest właściwa 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, zaś Centralne Biuro Antykorupcyjne w myśl ustawy o CBA³³ zostało utworzone jako służba specjalna do zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa.

Powyższe rozważania prowadzą do wniosku, iż zagrożenia godzące w bezpieczeństwo wewnętrzne zostały wprost zapisane przez ustawodawcę jedynie w przepisach kompetencyjnych Agencji Bezpieczeństwa Wewnętrznego, ale podobny zakres działania prewencyjnego, choć nieco inaczej sformułowany, został powierzony także Służbie Kontrwywiadu Wojskowego. Służba ta wprawdzie nie ma w przepisach swojej ustawy kompetencyjnej literalnie wskazanego zadania w postaci rozpoznawania zagrożeń godzących w bezpieczeństwo wewnętrzne, ale zajmuje się także „zagrożeniami wewnętrznymi”, tj. działaniami kontrwywiadowczymi w sferze wojskowej.

Tytułem wyjaśnienia można dodać, że służby policyjne w nieznacznym zakresie mają w swojej właściwości prowadzenie pewnych działań prewencyjnych, lecz nie są one w ich przepisach kompetencyjnych wprost określone jako rozpoznawanie zagrożeń. I tak np. w *ustawie z dnia 6 kwietnia 1990 r. o Policji*³⁴ wskazano wprawdzie, że jest właściwa do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego, w tym zapewnienia spokoju w miejscach publicznych, jednak główną osią jej działania jest ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, a także wykrywanie przestępstw i ściganie ich sprawców. Ponadto Służba Ochrony Państwa na podstawie ustawy z dnia 8 grudnia

³² Dz.U. 2019, poz. 687 z późn. zm.

³³ Tamże, poz. 1921 z późn. zm.

³⁴ Dz.U. 2020, poz. 360 z późn. zm.

2017 r.³⁵ jest właściwa w zakresie ochrony osób i obiektów oraz rozpoznawania i zapobiegania skierowanym przeciwko nim przestępstwom. Powyższe pozwala wnioskować, iż co do zasady rozpoznawanie zagrożeń należy do domeny służb specjalnych, które dodatkowo w tym celu wyposażono w ustawowe uprawnienie do wykonywania czynności analityczno-informacyjnych.

Na podkreślenie zasługuje fakt, iż ustawodawca, określając właściwość ustawową Agencji Bezpieczeństwa Wewnętrznego, wprost wskazał na zagrożenia godzące w „bezpieczeństwo wewnętrzne” państwa i *de facto* stanowi ona największą instytucję zajmującą się ochroną bezpieczeństwa wewnętrznego państwa. Ponadto na Agencję Bezpieczeństwa Wewnętrznego ustawodawca nałożył wyłączny obowiązek stania na straży porządku konstytucyjnego Rzeczypospolitej Polskiej.

Analizując uprawnienia polskich służb specjalnych w zakresie działań prewencyjnych, warto dodać, iż z porównania rozwiązań prawnych dotyczących służb specjalnych funkcjonujących w innych państwach europejskich³⁶ można wyprowadzić wniosek, że w Europie nie istnieje jeden dominujący system organizacji służb specjalnych.

Przyglądając się organizacji systemu służb specjalnych od strony umocowania i kompetencji cywilnych służb odpowiedzialnych za bezpieczeństwo wewnętrzne, wskazać można trzy grupy państw: kraje, w których istnieje wydzielona cywilna służba odpowiedzialna za bezpieczeństwo wewnętrzne, o czysto informacyjnym charakterze; kraje, w których ta sama służba informacyjna odpowiada za wywiad zagraniczny i bezpieczeństwo wewnętrzne państwa; kraje, w których służba odpowiedzialna za bezpieczeństwo wewnętrzne państwa posiada uprawnienia dochodzeniowo-śledcze.

W większości dużych krajów europejskich (np. Niemcy, Włochy, Wielka Brytania) istnieje wyspecjalizowana służba kontrwywiadowcza o charakterze operacyjno-rozpoznawczym i analityczno-informacyjnym, obok której działa wywiad zagraniczny i najczęściej również wyspecjalizowana agencja powołana do ścigania najgroźniejszych form przestępczości (Federalny Urząd Kryminalny w Niemczech, Narodowa Agencja Kryminalna w Wielkiej Brytanii). Pojawiają się też odrębne wyspecjalizowane służby właściwe w obszarze bezpieczeństwa łączności, cyberbezpieczeństwa czy wywiadu elektronicznego (Centrala Łączności Rządowej w Wielkiej Brytanii, Federalny Urząd Bezpieczeństwa Teleinformatycznego w Niemczech). Model drugi (służby wywiadowczo-kontrwywiadowczej) jest charakterystyczny dla krajów małych, które — jak należy domniemywać — z reguły nie mają szczególnie rozległych interesów międzynarodowych. Z krajów średniej wielkości taki model przyjęły Holandia i Grecja, zaś z dużych państw europejskich przyjęła

³⁵ Dz.U. 2021, poz. 575.

³⁶ Szerzej na ten temat m.in. w publikacji P. Burczaniuk i in., *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach*, Agencja Bezpieczeństwa Wewnętrznego, Emów 2017.

go jedynie Hiszpania (Narodowe Centrum Wywiadu podległe Prezesowi Rady Ministrów). Model, w którym służba odpowiedzialna za bezpieczeństwo wewnętrzne posiada uprawnienia dochodzeniowo-śledcze (można nazwać go modelem „policji bezpieczeństwa”), jest rozpowszechniony szczególnie w państwach skandynawskich. Z dużych państw europejskich ma go Francja. W krajach tych służby specjalne posiadają silne związki z policją. Związki te mogą mieć charakter organizacyjny (działanie w ramach struktury policji), prawny (działanie oparte na tej samej pragmatyce co policja) bądź genetyczny (służby specjalne wywodzą się historycznie z policji)³⁷.

Przeprowadzona kwerenda (w tym przegląd stron internetowych służb specjalnych, a w niektórych przypadkach także źródłowych aktów prawnych) pozwala na wyodrębnienie zasadniczych obszarów działalności służb w poszczególnych krajach. Służby w Europie Zachodniej jako najważniejsze obszary swej właściwości identyfikują rozpoznawanie i zwalczanie: terroryzmu, szpiegostwa, cyberprzestępczości i proliferacji. Należy jednak zauważyć, że chociaż tak zdefiniowany profil zainteresowania jest zbliżony z największymi współczesnymi zagrożeniami, to niewątpliwie stanowi odpowiedź na społeczne odczucie zagrożenia związane z bieżącymi wydarzeniami.

Obszary działań prewencyjnych pozostających we właściwości Agencji Bezpieczeństwa Wewnętrznego

Jak już wyżej wskazano, decydujące znaczenia dla prawidłowego zdefiniowania właściwości Agencji Bezpieczeństwa Wewnętrznego ma opisane wyżej pojęcie „bezpieczeństwo wewnętrzne” i w takim ujęciu będzie ono stanowiło przedmiot dalszych rozważań. Jednakże w tym miejscu zasadne wydaje się także zdefiniowanie terminu „zagrożenie” oraz ustalenie relacji, jakie zachodzą między pojęciami „bezpieczeństwo” i „zagrożenie”, aby właściwie ustalić zakres przedmiotowy tego zagadnienia.

Potocznie terminem „bezpieczeństwo” określamy stan bez zagrożeń, brak lęku przed utratą życia, zdrowia lub mienia oraz wiarę, że w wypadku wystąpienia takiego zagrożenia możliwe będzie uzyskanie skutecznej pomocy³⁸. Etymologia wyrazu „bezpieczeństwo” w wielu językach (także w polskim) podkreśla pierwotność poczucia zagrożenia w stosunku do poczucia pewności swego zabezpieczenia („bez pieczy” czyli bez wystarczającej ochrony)³⁹.

Zgodnie z definicją słownikową „zagrożenie” to sytuacja lub stan, które komuś zagrażają lub, w których ktoś czuje się zagrożony⁴⁰, lub też jest ono definiowane jako sytuacja, w której pojawia się zwiększone prawdopodobieństwo

³⁷ Patrz szerzej: tamże.

³⁸ B. Kaczmarczyk, *Bezpieczeństwo i zagrożenia w praktyce*, SA PSP Kraków, 2014, s. 13.

³⁹ B. Wiśniewski, *System bezpieczeństwa państwa...*, s. 37.

⁴⁰ *Słownik języka polskiego*, <http://sjp.pwn.pl>, [dostęp: 27 IV 2021].

powstania stanu niebezpiecznego dla otoczenia⁴¹. W literaturze przedmiotu pojęcie „zagrożenie” rozumiane jest także jako szeroki zespół zjawisk negatywnie ocenianych⁴². Można podsumować, iż „zagrożenie” to sytuacja, która może zakłócić prawidłowe funkcjonowanie podmiotu, która winna być wyprzedzająco zidentyfikowana jako potencjalne, niekorzystne zjawisko.

W świetle przytoczonych wyżej definicji, zestawienie pojęć „bezpieczeństwo” i „zagrożenie” wskazywać może, że mamy do czynienia z dwoma przeciwstawnymi, czy też wykluczającymi się zagadnieniami. W ogólnym ujęciu przez „bezpieczeństwo” można rozumieć brak zagrożeń. Jednakże połączenie tych pojęć w opisie zadania ustawowego Agencji Bezpieczeństwa Wewnętrznego prowadzi do wniosku, iż oba terminy faktycznie się uzupełniają i tworzą logiczną całość wskazującą na główny obszar zainteresowania tej służby.

Przechodząc do bardziej szczegółowych rozważań na temat zagrożeń i ich relacji z poczuciem i zapewnieniem bezpieczeństwa wewnętrznego państwa, należy zaznaczyć, iż ważnym elementem, który pozwala na podjęcie skutecznej reakcji na wypadek wystąpienia zagrożenia jest wskazanie czynności, które zostały przewidziane dla działań Agencji Bezpieczeństwa Wewnętrznego. Analizując przepis art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW, trzeba zauważyć, że ustawodawca, tworząc ten przepis, posłużył się sformułowaniami „rozpoznawanie, zapobieganie i zwalczanie” i wymienił te czynności w logicznym ciągu zdarzeń. Wskazuje to na intencję prawodawcy, by rozpocząć opisywanie działania Agencji Bezpieczeństwa Wewnętrznego w zakresie zagrożeń od ich „rozpoznawania”, czyli językowo od zidentyfikowania kogoś lub czegoś, wyróżniając spośród innych⁴³. Bez wątplenia zapobieganie zjawiskom niekorzystnym, zagrażającym bezpieczeństwu ludzi i państwa, należy rozpocząć od poznania ich źródeł, co daje w większości przypadków możliwość ich eliminacji już we wstępnej fazie (w zarodku). Na tym etapie mamy do czynienia z czynnościami Agencji Bezpieczeństwa Wewnętrznego, które są nakierowane na analizowanie otaczającej rzeczywistości przez pryzmat wartości podlegających ochronie oraz definiowanie potencjalnych zagrożeń, które mogą być przeciw nim skierowane. Prawidłowa identyfikacja zagrożenia, na jego wstępnym etapie i przygotowanie się do jego eliminacji w każdym aspekcie, pozwala na podjęcie wyprzedzających i skutecznych działań. Odpowiednia, a najlepiej wyprzedzająca wiedza, jest podstawowym atutem w skutecznej walce z zagrożeniami.

Ponadto przepis wskazuje także na działanie w zakresie „zapobiegania”, czyli niedopuszczenia do czegoś złego⁴⁴. W tej fazie działania funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego winni zatem podejmować czynności,

⁴¹ *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2008, s. 172–173.

⁴² R. Zięba, *Bezpieczeństwo a terroryzm — aspekty teoretyczne*, w: *Terroryzm: globalne wyzwanie*, red. K. Kowalczyk, W. Wróblewski, Wydawnictwo Adam Marszałek, Toruń 2006, s. 29.

⁴³ *Słownik języka polskiego*, zob. <http://sjp.pwn.pl> [dostęp: 27 IV 2021].

⁴⁴ Tamże.

aby nie dopuścić do tego, by zidentyfikowane już uprzednio niebezpieczeństwo faktycznie zaistniało. Finalnie owo działanie może także wejść w fazę „zwalczania”, czyli wystąpienia przeciwko komuś lub czemuś, przewyciężenia czegoś⁴⁵. W przypadku zaistnienia zidentyfikowanego zagrożenia niezbędne jest podejmowanie czynności w celu jego eliminacji. Należy podkreślić, iż realność bądź możliwość wystąpienia niepożądanego zdarzenia czy zjawiska zmusza państwo do podjęcia wysiłku na rzecz podjęcia środków zaradczych. Bezpieczeństwo państwa pozostaje w dialektycznym związku z zagrożeniami i oznacza jego zdolność do przeciwstawienia się nim⁴⁶.

Podsumowując, w omawianym przepisie ustawy o ABW oraz AW mamy do czynienia z zagrożeniami godzącymi w zdefiniowane już wyżej bezpieczeństwo wewnętrzne państwa i porządek konstytucyjny oraz podejmowanymi wobec nich działaniami — pierwsze i podstawowe zadanie to zdefiniowanie konkretnego zagrożenia, uświadomienie sobie jego specyfiki i możliwości wystąpienia, a następnie podejmowanie właściwych działań w celu niedopuszczenia do jego zaistnienia bądź uniknięcia ewentualnych jego skutków.

Opisane wyżej zadanie ustawowe Agencji Bezpieczeństwa Wewnętrznego w zakresie działań prewencyjnych pozwala postawić tezę, iż ABW jest powołana do rozpoznawania, zapobiegania i zwalczania „wszelkich” zagrożeń godzących w bezpieczeństwo wewnętrzne i porządek konstytucyjny. Z przepisu wynika jedyne ustawowe ograniczenie w postaci „godzenia w bezpieczeństwo wewnętrzne i porządek konstytucyjny”. Działania prewencyjne w zakresie monitorowania życia społecznego i politycznego pod kątem zagrożeń można określić mianem czynności rozpoznawczych, profilaktycznych lub wyprzedzających.

W literaturze przedmiotu działania prewencyjne określane są też jako działania kontrwywiadowcze w rozumieniu instytucjonalnym, w odróżnieniu od działań o charakterze policyjnym wykonywanych przez służby specjalne. Są one prowadzone w celu identyfikacji wrogich podmiotów oraz zbierania dowodów przestępczej działalności, aby na ich podstawie można było zastosować właściwe środki karne lub administracyjne. Do zadań kontrwywiadu należy także zbieranie i analizowanie danych niezbędnych do zapewnienia bezpieczeństwa państwa⁴⁷.

W literaturze przedmiotu można również spotkać stwierdzenie, iż kontrwywiad ma trzy główne zadania, tj.: zapewnienie fizycznego bezpieczeństwa informacji; identyfikowanie i zatrzymywanie własnych obywateli, którzy szpiegują dla obcego rządu; identyfikowanie obcych agentów pracujących przeciwko interesom państwa oraz podejmowanie próby ich przekształcenia w podwójnych agentów lub ściganie za szpiegostwo⁴⁸. Ponadto na podstawie fachowej literatury

⁴⁵ Tamże.

⁴⁶ B. Wiśniewski, *System bezpieczeństwa państwa...*, s. 35.

⁴⁷ M. Górka, *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, ŚSP 2'17, s. 108.

⁴⁸ Tamże, s. 108.

można wysnuć wniosek, iż zadania kontrwywiadu pojmowane są jako czynności prowadzone w celu ochrony przed działaniami wywiadowczymi, sabotażem lub zamachami realizowanymi na rzecz lub w imieniu obcych mocarstw, organizacji, osób lub międzynarodowych operacji terrorystycznych⁴⁹. Na marginesie można dodać, iż działania kontrwywiadowcze bywają także określane jako wypełnianie funkcji policji politycznej, której zadania są definiowane jako ochrona przed zamachami zewnętrznymi i wewnętrznymi zagrażającymi państwu, istniejącemu porządkowi prawnemu, politycznemu i ustrojowi społecznemu⁵⁰.

Do podstawowych działań Agencji Bezpieczeństwa Wewnętrznego w obszarze kontrwywiadowczym należy zaliczyć: monitorowanie instytucjonalnej i cudzoziemskiej aktywności na terenie Rzeczypospolitej Polskiej, pod kątem realizacji zadań na rzecz obcych służb specjalnych, ofensywne rozpracowywanie obcych służb specjalnych, a także rozpoznanie osób i innych podmiotów współpracujących z obcymi służbami specjalnymi⁵¹.

W tym zakresie bez wątpienia mieści się zagadnienie związane z szeroko rozumianym szpiegostwem, które jako przestępstwo pozostające we właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego może przybierać następujące formy: kierowanie działalnością obcego wywiadu, organizowanie działalności obcego wywiadu, branie udziału w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, branie udziału w obcym wywiadzie i udzielanie temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, działanie na rzecz obcego wywiadu i udzielanie temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, wejście do systemu informatycznego w celu uzyskania wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, gromadzenie lub przechowywanie wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, zgłoszenie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej⁵².

Opisane szeroko w literaturze przedmiotu aspekty przestępstwa szpiegostwa bez wątpienia należy również odnieść do działania prewencyjnego Agencji Bezpieczeństwa Wewnętrznego w tym zakresie. Priorytetem służby winno być bowiem takie rozpoznanie tego zagrożenia i jego eliminacja, ażeby nie przeszło ono w dalszą fazę jego realizacji, czyli popełnienie czynu karalnego, co będzie wymagało podjęcia czynności procesowych.

Jako element zagrożenia bezpieczeństwa wewnętrznego bez wątpienia należy zakwalifikować także rozpoznawanie zagadnień związanych z działalnością terrorystyczną, jednakże w polskim systemie prawnym pojęcie „terroryzm” nie

⁴⁹ Tamże, s. 108.

⁵⁰ M. Kolaszyński, dz. cyt., s. 113.

⁵¹ S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2002, s. 54.

⁵² Szerzej: P. Burczaniuk, *Przestępstwo szpiegostwa — rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw*, red. P. Burczaniuk, Warszawa 2017, s. 93–96.

zostało legalnie zdefiniowane. Można jedynie wskazać, iż w art. 115 § 20 kodeksu karnego⁵³ zawarto określenie „przestępstwo o charakterze terrorystycznym” jako czyn zabroniony, zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonej czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba takiego czynu.

Samo pojęcie „terroryzm” jest natomiast raczej terminem o charakterze naukowym, obrazującym stan zagrożenia społecznego wywołanego czynem o charakterze terrorystycznym. W literaturze „terroryzm” definiowany jest jako stosowanie gwałtu do osiągnięcia celów politycznych lub ekonomicznych w stosunkach międzynarodowych, forma interwencji dokonywanej przemocą przez specjalne oddziały wojskowe lub policyjne albo przez organizacje terrorystyczne⁵⁴. „Terroryzm” jest także ujmowany jako bezwzględna walka ze strukturami legalnej władzy państwowej, prowadzona z naruszeniem wszelkich konwencji i umów międzynarodowych, a polegająca na skrytobójczym przeprowadzaniu zamachów, których celem jest zabicie jak największej liczby przypadkowych osób lub spowodowanie dużych strat materialnych, ażeby wywołane tym poczucie strachu i przerażenia powodowały taką presję społeczną, by zmusić władze państwowe do spełnienia wszelkich żądań (zaniechanie danego postępowania)⁵⁵.

W świetle powyższego wśród zadań Agencji Bezpieczeństwa Wewnętrznego na pierwszy plan wysuwa się potrzeba prowadzenia działań prewencyjnych, w szczególności w zakresie gromadzenia informacji w celu identyfikowania ewentualnych zagrożeń o charakterze terrorystycznym na terytorium Rzeczypospolitej Polskiej, skierowanych przeciwko działalności państwa i jego obywateli.

Ponadto w obliczu wydarzeń geopolitycznych i postępu technologicznego nie można nie wspomnieć o zagrożeniach wynikających z działań terrorystycznych określanych jako cyberterroryzm, rozumiany jako bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne, będący rezultatem działań subnarodowych grup, podmiotów niepaństwowych bądź obcych służb specjalnych, w celu zastraszenia albo wymuszenia na rządzie lub społeczeństwie danego kraju realizacji daleko idących polityczno-społecznych żądań⁵⁶.

W aspekcie zjawiska terroryzmu należy także wskazać na działania Agencji Bezpieczeństwa Wewnętrznego nakierowane na rozpoznawanie ekstremizmu, w szczególności jego odmiany politycznej, rozumianego jako kompleks poglądów,

⁵³ Dz.U. 2020, poz. 1444 z późn. zm.

⁵⁴ J.E. Osmańczyk, *Encyklopedia spraw międzynarodowych i ONZ*, Warszawa 1974, s. 3509.

⁵⁵ M. Zimny, *Terroryzm samobójczy*, Warszawa 2006, s. 15.

⁵⁶ A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm jako nowe zagrożenia dla bezpieczeństwa międzynarodowego w dobie globalizacji*, w: *Terroryzm w świecie współczesnym*, red. E. Haliżak, Warszawa 2004, s. 324.

idei, postulatów o różnym poziomie spójności wewnętrznej oraz związanych z nimi zachowań, charakteryzujących się skrajnością — patrząc przez pryzmat istniejącego układu sił politycznych⁵⁷. Pełnią one bardzo istotną rolę, ponieważ sprawne funkcjonowanie demokratycznego państwa uzależnione jest w głównej mierze od przestrzegania przez organy władzy publicznej, partie polityczne, jak i obywateli, norm zawartych w ustawie zasadniczej. Z tego powodu działania organizacji ekstremistycznych o charakterze niekonstytucyjnym, czyli odwołujących się w swoich programach do totalitarnych metod i praktyk działania nazizmu, faszyzmu i komunizmu, nienawiści rasowej i narodowej, stosowania przemocy w celu zdobycia władzy lub wpływu na politykę państwa, wymagają od organów państwa podjęcia odpowiednich przeciwdziałań. Z uwagi na fakt, że działalność tych organizacji ukierunkowana jest na zakłócenie funkcjonowania organów władzy publicznej, a w niektórych przypadkach zmierza do zmiany ustroju państwowego, rola Agencji Bezpieczeństwa Wewnętrznego w rozpoznawaniu i zwalczaniu ich działalności jest kluczowa.

Zagadnienie rozprzestrzeniania broni masowego rażenia (BMR) oraz środków jej przenoszenia do tzw. krajów ryzyka (tzw. proliferacja) stanowi także ważny element zainteresowania Agencji Bezpieczeństwa Wewnętrznego, rozumiany jako zagrożenie bezpieczeństwa wewnętrznego. Co do zasady w działalności Agencji Bezpieczeństwa Wewnętrznego proliferacja jest rozpatrywana jako zadanie dotyczące rozpoznawania, zapobiegania i wykrywania przestępstw w zakresie produkcji i obrotu towarami, technologiami i usługami strategicznymi dla bezpieczeństwa państwa oraz nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady w obrocie międzynarodowym (art. 5 ust. 1 pkt 2 lit. d–e), nie można jednak nie wspomnieć o tych zagadnieniach, które winny podlegać zainteresowaniu Agencji Bezpieczeństwa Wewnętrznego już na etapie identyfikacji tego problemu w postaci podjęcia działań prewencyjnych.

Do zagrożeń bezpieczeństwa wewnętrznego należy także zakwalifikować zagadnienia związane z bezpieczeństwem ekonomicznym, które w literaturze przedmiotu zostały podzielone na zagrożenia ekonomiczne zewnętrzne i wewnętrzne. Do zagrożeń wewnętrznych zalicza się świadome działania obcych państw, ich służb specjalnych oraz powiązanych z nimi podmiotów gospodarczych, których celem jest wpływanie na sytuację gospodarczą danego kraju. Zaś za wewnętrzne zagrożenia ekonomiczne uważa się niezgodne z prawem działania rodzimych i zagranicznych przedsiębiorców na rynku krajowym, zwłaszcza próby nielegalnego wzbogacenia się, defraudacje państwowych lub zagranicznych dotacji, spekulację i korupcję⁵⁸.

Można zatem podsumować, iż w tym aspekcie mamy do czynienia z działaniami czynników zewnętrznych i wewnętrznych, których celem jest wywieranie

⁵⁷ R. Herbut, *Ekstremizm*, w: *Słownik politologii*, Wrocław 2003, s. 86–87.

⁵⁸ K.A. Wojtaszczyk, *Istota i dylematy bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, nr 1/09, s. 25–26.

wpływu na sytuację gospodarczą (ekonomiczną) kraju. W tym zakresie możemy wyróżnić bezpieczeństwo energetyczne, działania podejmowane w sektorze finansowym, bankowym i ubezpieczeniowym, w tym zakresie mieści się także korupcja (osłona antykorupcyjna) i przestępczość zorganizowana, które to już jako przestępstwa należą do właściwości Agencji Bezpieczeństwa Wewnętrznego również i w zakresie czynności dochodzeniowo-śledczych.

Działalność Agencji Bezpieczeństwa Wewnętrznego w powyższych obszarach nazywana jest w praktyce „ochroną kontrwywiadowczą” i rozumiana jako zadania związane z szeroko pojętą ochroną interesów kraju przed działaniami zewnętrznymi. Czynności związane z tym zadaniem dotyczą przede wszystkim ochrony podmiotów i instytucji o znaczeniu strategicznym (urzędy, podmioty gospodarcze). W tym aspekcie należy także wskazać, iż duże znaczenie na etapie działań prewencyjnych mają czynności Agencji Bezpieczeństwa Wewnętrznego polegające na prowadzeniu szkoleń dla urzędników państwowych i pracowników instytucji prywatnych, kluczowych dla bezpieczeństwa państwa — w zakresie zagrożeń, z jakimi mogą mieć do czynienia w swojej pracy, w szczególności w kontaktach z przedstawicielami innych państw (tzw. profilaktyka kontrwywiadowcza). W trakcie tych szkoleń przekazywana jest wiedza na temat skali zagrożeń ze strony obcych służb specjalnych oraz podstawowych zasad bezpieczeństwa, jakie powinny być wdrażane w kontaktach z osobami trzecimi, głównie z obcokrajowcami. Działania te stanowią także element koordynacji Agencji Bezpieczeństwa Wewnętrznego w kontaktach z instytucjami i ułatwiają wymianę informacji oraz pozwalają wyprzedzająco na zbudowanie niezbędnego zasobu informacyjnego wśród urzędników państwowych.

Należy dodać, iż w ramach ochrony kontrwywiadowczej zadania podejmowane są dwutorowo. Z jednej strony chronione są podmioty, które mogą stanowić przedmiot zainteresowania obcych służb wywiadowczych, a z drugiej monitorowane są działania podejmowane przez obce służby na terytorium Rzeczypospolitej Polskiej. W pierwszym aspekcie należy wskazać, iż system ochrony kontrwywiadowczej skoncentrowany jest przede wszystkim na urzędach administracji centralnej i terenowej, podmiotach istotnych z punktu widzenia podstawowych interesów państwa oraz ośrodkach naukowych i technicznych zajmujących się badaniami nad technologiami podwójnego zastosowania. W drugim aspekcie przedsięwzięcia funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego zmierzają w szczególności do wykrycia i zneutralizowania prób uzyskiwania informacji metodami niezgodnymi z prawem. Taka aktywność obcych służb może odbywać się m.in. przez: próby nawiązania kontaktu z urzędnikami państwowymi, dążenie do uzyskania informacji objętych klauzulą tajności, starania pozyskania technologii i towarów podwójnego zastosowania oraz działania w sferze gospodarczej, zwłaszcza w sektorze energetycznym, które mogą zagrażać podstawom ekonomicznym Rzeczypospolitej Polskiej⁵⁹.

⁵⁹ M. Kolaszyński, dz. cyt, s. 119–120.

Opisane wyżej dziedziny działalności kontrwywiadowczej Agencji Bezpieczeństwa Wewnętrznego stanowią próbę stworzenia *quasi* katalogu zagrożeń należących do jej właściwości ustawowej. Trudno jest bowiem odnaleźć w literaturze przedmiotu kompleksowe opracowanie dotyczące kwestii zagrożeń bezpieczeństwa wewnętrznego, które enumeratywnie wymienia i opisuje poszczególne zagrożenia wchodzące w zakres tego pojęcia. Jednakże wskazane wyżej pola działalności nie zostały wybrane przypadkowo — znajdują one odzwierciedlenie w dokumentach analitycznych oficjalnie opublikowanych przez Agencję Bezpieczeństwa Wewnętrznego w latach 2009–2014 pt. *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego*. I tak np. w *Raporcie z działalności Agencji Bezpieczeństwa Wewnętrznego w 2011 r.* zawarto informację, iż Agencja Bezpieczeństwa Wewnętrznego badała działalność grup i organizacji, które swoją aktywnością próbowały propagować idee faszystowskie lub komunistyczne, znieważały inne osoby ze względu na ich przynależność narodową, etniczną, rasową, polityczną lub wyznaniową oraz nawoływały do nienawiści wobec takich osób. Kryteria te zostały ustalone na podstawie art. 13 Konstytucji RP⁶⁰. Z kolei w *Raporcie z działalności Agencji Bezpieczeństwa Wewnętrznego w 2012 r.* wskazywano, iż uwaga Agencji skupiała się na rozpoznawaniu zagrożenia związanego z działalnością grup terrorystycznych i ekstremistycznych⁶¹. Z *Raportu z działalności Agencji Bezpieczeństwa Wewnętrznego w 2013 r.* wynika, iż działania Agencji polegały na monitorowaniu podmiotów zajmujących się obrotem komponentami wykorzystywanymi do produkcji materiałów wybuchowych i obserwacji działań osób, które ze względu na swoje zainteresowania i posiadaną specjalistyczną wiedzę były w stanie wyprodukować materiały wybuchowe, które mogły być wykorzystane do przeprowadzenia zamachu terrorystycznego⁶². Z treści ostatniego opublikowanego dokumentu tego typu, tj. z *Raportu z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.*, wynika, iż wskutek działań operacyjno-rozpoznawczych na kierunku kontrwywiadowczym prowadzono działania przeciwko aktywności rosyjskich służb wywiadowczych w Polsce dotyczącej m.in. zabiegania o informacje z zakresu wywiadu politycznego, gospodarczego i naukowo-technicznego oraz dane umożliwiające dotarcie do osób dysponujących wiedzą istotną z punktu widzenia interesów politycznych i bezpieczeństwa Rzeczypospolitej Polskiej. Potwierdzono też działania białoruskich służb specjalnych na terytorium Rzeczypospolitej Polskiej. Zidentyfikowano również zainteresowanie obcych służb wywiadowczych polskim sektorem energetycznym, w tym perspektywami jego rozwoju. Wskazano wówczas na działania

⁶⁰ *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2011 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2012, s. 21.

⁶¹ *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2012 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 15.

⁶² *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2013 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2014, s. 17.

w zakresie zwalczania terroryzmu i przeciwdziałania ekstremizmom, w tym m.in. analizowano działalność islamskich ekstremistów w cyberprzestrzeni⁶³.

W przeciwieństwie do zagadnienia dotyczącego zwalczania stypizowanych przestępstw, wymienionych w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, a także ścigania ich sprawców i ewidentnego przypisania konkretnego czynu karalnego do zakresu kompetencji Agencji Bezpieczeństwa Wewnętrznego, już samo zakwalifikowanie danego zagadnienia jako zagrożenia godzącego w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny wymaga dokonania pewnego procesu myślowego pod kątem analizy przytoczonych wyżej zagadnień, w tym też ewentualnego poszerzenia ich zakresu w danej sytuacji. Przedstawione wyżej kwestie, identyfikowane jako zagrożenia godzące w bezpieczeństwo wewnętrzne państwa, na potrzeby art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW znajdują swoje praktyczne odzwierciedlenie w zadaniach najważniejszych departamentów kierunkowych Agencji Bezpieczeństwa Wewnętrznego. Zgodnie bowiem z *zarządzeniem nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego*⁶⁴ w skład Agencji Bezpieczeństwa Wewnętrznego wchodzi m.in. Departament Kontrywywiadu, Departament Zagrożeń Strategicznych oraz Centrum Antyterrorystyczne. Już same nazwy tych jednostek organizacyjnych poniekąd wskazują na zakres problemów, którymi się zajmują odpowiednio: kontrywywiad (szpiegostwo), zagrożenia strategiczne (bezpieczeństwo ekonomiczne, energetyczne, proliferacja), terroryzm.

Jednakże wydaje się zasadne wnioskowanie, by zakres przestępstw przypisanych do właściwości Agencji Bezpieczeństwa Wewnętrznego posiłkowo wyznaczał także zakres zagadnień, którymi Agencja może zająć się na początkowym etapie ich rozpoznawania, czyli we wstępnej formie działania prewencyjnego, nie wchodząc jeszcze w działania ustawowe pod kątem oceny czynu karalnego popełnionego przez konkretną osobę. Można nawet zaryzykować twierdzenie, iż przestępczość pozostająca we właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego może być także w szerokim rozumieniu zakwalifikowana jako zagrożenie godzące w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny.

Środki służące wykonywaniu działań prewencyjnych przez Agencję Bezpieczeństwa Wewnętrznego

Przechodząc do omówienia środków przewidzianych w Agencji Bezpieczeństwa Wewnętrznego do zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, na wstępie należy wskazać, iż z opisanej już wyżej istoty zagrożeń działania dotyczące ich rozpoznawania, zapobiegania

⁶³ *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r., Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2015, s. 15–17.*

⁶⁴ M.P. 2018, poz. 927.

i zwalczania mają charakter wyprzedzający (prewencyjny). Uzyskana informacja o możliwym zagrożeniu jest kwalifikowana pod kątem właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego, co następnie uruchamia wiele działań, które w przeważającej mierze są niejawnie i nie mogą stanowić przedmiotu szczegółowych rozważań w niniejszym rozdziale.

Od początku funkcjonowania cywilnej służby kontrwywiadowczej do rozpoznawania i zwalczania zagrożeń bezpieczeństwa państwa służyły podobne instrumenty — według ustawy o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń oraz innych działań godzących w bezpieczeństwo państwa lub porządek publiczny funkcjonariusze Służby Bezpieczeństwa mieli prawo wykonywać czynności operacyjno-rozpoznawcze.

W pierwotnej wersji ustawy o Urzędzie Ochrony Państwa⁶⁵ wskazano na wykonywanie czynności operacyjno-rozpoznawczych w celu rozpoznania, zapobiegania i wykrywania przestępstw, lecz już nowelizacja tego aktu⁶⁶ wprowadziła z dniem 12 października 1995 r. przepis, iż Urząd Ochrony Państwa wykonuje czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznania, zapobiegania i wykrywania przestępstw, a także czynności operacyjno-rozpoznawcze, w celu uzyskania informacji istotnych dla ochrony bezpieczeństwa państwa.

Podobnie przedstawia się to zagadnienie także i w obecnym stanie prawnym — w tej kwestii na szczególną uwagę zasługuje art. 21 ust. 1 ustawy o ABW oraz AW, zgodnie z którym w ramach zadań, o których mowa w art. 5 ust. 1, funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego wykonują:

- 1) czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców;
- 2) czynności operacyjno-rozpoznawcze i analityczno-informacyjne w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego.

Już sama redakcja tego przepisu wskazuje na nieco odmienne potraktowanie działań wykrywczych i prewencyjnych w aspekcie przypisanych im środków wykonawczych. W jego treści wskazano bowiem, iż w odniesieniu do przestępstw mamy do czynienia z czynnościami operacyjno-rozpoznawczymi i dochodzeniowo-śledczymi, czyli wprost przypisano te czynności do zadań wykonywanych na podstawie art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW. Nieco inny zabieg legislacyjny został natomiast użyty w odniesieniu do innych zadań, albowiem w treści art. 21 ust. 1 pkt 1 ustawy o ABW oraz AW nie zastosowano wprost odwołania do *zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny* czy też innych zadań wymienionych w pkt 2a–5, lecz wskazano na wykonywanie konkretnych czynności w celu *uzyskiwania i przetwarzania*

⁶⁵ Dz.U. 1990, nr 30, poz. 180.

⁶⁶ Dz.U. 1995, nr 104, poz. 515.

informacji istotnych dla bezpieczeństwa państwa i jego porządku konstytucyjnego. W świetle takiej redakcji przepisu należy jednak wnioskować, iż ustawodawca przyjął, że w zakresie pojęcia „informacje istotne dla bezpieczeństwa państwa i jego porządku konstytucyjnego” mieszczą się informacje niezbędne do rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, o których mowa w art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW. Świadczy o tym także wstęp do wyliczenia zawarty w omawianym przepisie, albowiem odnosi się on bez wątplenia do realizacji wszystkich zadań wymienionych w art. 5 ust. 1, zatem wnioskuje *a contrario*, skoro w pkt 1 wskazano jedynie zadanie dotyczące przestępstw (pkt 2), to pozostałe zadania wymienione w art. 5 ust. 1 pkt 1, 2a–5 ustawy o ABW oraz AW muszą się mieścić w zakresie sformułowania „informacje istotne dla bezpieczeństwa państwa i jego porządku konstytucyjnego”. Przyjęcie odmiennej tezy prowadziłoby do nieuprawnionego wniosku, iż ustawodawca pozostawił poza zakresem regulacji wymienione w pkt 1, 2a–5 zadania Agencji w zakresie przyporządkowania im kategorii czynności przeznaczonych do ich realizacji.

Dlatego też wypada podkreślić, iż w zakresie działań prewencyjnych (zwalczanie zagrożeń) funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego mają prawo wykonywać czynności operacyjno-rozpoznawcze i analityczno-informacyjne.

Dalsze rozważania w tej kwestii należy rozpocząć od przybliżenia charakterystyki czynności operacyjno-rozpoznawczych, które pozwalają na zdobywanie informacji niezbędnych do podejmowania skutecznych działań przez służbę.

Pojęcie „czynności operacyjno-rozpoznawczych” w polskim systemie prawa nie posiada definicji legalnej, lecz w literaturze przedmiotu podjęto próby jego zdefiniowania. I tak np. według T. Hanauska „czynności operacyjno-rozpoznawcze” stanowią odrębny system poufnych bądź tajnych działań, uprawnionych do tego ustawowo organów, prowadzonych poza procesem karnym, lecz zazwyczaj służących aktualnym lub przyszłym celom tego procesu i wykonywanych dla zapobiegania i zwalczania przestępczości oraz innych prawnie określonych negatywnych zjawisk społecznych⁶⁷. W literaturze znajdziemy też sformułowanie, iż czynności operacyjno-rozpoznawcze polegają na ustalaniu faktów dotyczących zdarzeń, które ze względu na swój społecznie szkodliwy charakter zakłócają normalne funkcjonowanie państwa (społeczeństwa)⁶⁸.

Próbę podsumowania dorobku piśmiennictwa w tym zakresie podjął A. Taracha, który stwierdził, iż „czynności operacyjno-rozpoznawcze” to czynności organów państwowych wykonywane tajnie lub poufnie, w oparciu o podstawę ustawową, spełniające funkcję informacyjną, wykrywczą, profilaktyczną i dowodową⁶⁹. W piśmiennictwie fachowym wskazuje się, iż funkcja informacyjna

⁶⁷ T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1996, s. 96.

⁶⁸ M. Bożek, *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej” 2015, nr 1, s. 21–22.

⁶⁹ A. Taracha, *Czynności operacyjno-rozpoznawcze aspekty kryminalistyczne i prawnodowodowe*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006, s. 25.

czynności operacyjno-rozpoznawczych, zwana także rozpoznawczą, polega na zdobywaniu możliwie dużej ilości informacji na temat aktualnych i przyszłych działań; funkcja profilaktyczna tych czynności związana jest z kolei z zapobieganiem popełnieniu przestępstw i może niekiedy pokrywać się z funkcją dowodową (np. w aspekcie ujęcia sprawcy w fazie przygotowania do przestępstwa lub usiłowania jego popełnienia). Funkcja wykrywcza natomiast sprowadza się do wykrywania przestępstw i ich sprawców⁷⁰.

W działaniach Agencji Bezpieczeństwa Wewnętrznego nakierowanych na rozpoznawanie i zwalczanie zagrożeń podstawową rolę odgrywa funkcja informacyjna, która — jak można wnioskować z samej nazwy — pozwala na zdobycie niezbędnych informacji. Jednakże należy dodać, iż w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, a także w innych ustawach kompetencyjnych służb specjalnych, można dostrzec też istotną kwestię odnoszącą się do charakteru czynności operacyjno-rozpoznawczych w zakresie prowadzenia ich nie tylko w celu uzyskiwania informacji o zagrożeniach, lecz również w celu zwalczania przestępstw (funkcja wykrywcza).

Jak już wyżej wskazano, Agencja Bezpieczeństwa Wewnętrznego podejmuje czynności operacyjno-rozpoznawcze zarówno w celu zwalczania przestępstw, jak i zagrożeń oraz uzyskiwania informacji. Dlatego też można podsumować, iż uprawnienie do wykonywania czynności operacyjno-rozpoznawczych można zakwalifikować jako instrument wielowymiarowy, z którego można korzystać przy zwalczaniu przestępstw (działalność w wymiarze wykrywczym), ale także i w związku z rozpoznawaniem zagrożeń (działalność w wymiarze profilaktyczno-kontrwywiadowczym).

Należy podkreślić, iż działania Agencji Bezpieczeństwa Wewnętrznego w zakresie rozpoznawania i zwalczania zagrożeń — w odróżnieniu od rozpoznawania, zapobiegania i wykrywania przestępstw — mają wyłącznie charakter prewencyjny, przedprocesowy i w większości opierają się na czynnościach, które ze swojej istoty cechują się niejawnością. Właściwość w zakresie przestępstw z kolei obejmuje zarówno czynności operacyjno-rozpoznawcze, jak i dochodzeniowo-śledcze, które stanowią *de facto* działania o charakterze wykrywczym, zmierzające do ustalenia i ścigania osoby sprawcy, co zostanie szczegółowo opisane w kolejnym rozdziale.

W ocenie autora niniejszego tekstu nie jest możliwe precyzyjne rozdzielenie działań operacyjnych funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, podejmowanych na podstawie art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW, w pełnym oderwaniu od działań wykonywanych w myśl pkt 2 tego przepisu — owe niwy działalności Agencji wzajemnie się przenikają, w pewnych aspektach nakładają się na siebie, szczególnie na wstępnym poziomie analizowania informacji. Powyższy podział ma znaczenie raczej teoretyczne (poznawcze), natomiast dla funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego wykonujących czynności operacyjno-rozpoznawcze ma on znaczenie drugorzędne,

⁷⁰ Por. M. Bożek i in., dz. cyt., s. 113.

ponieważ podejmowane przez nich działania operacyjne w zakresie właściwości wynikającej z art. 5 ust. 1 ustawy o ABW oraz AW sprowadzają się *de facto* do czynności mających na celu ochronę bezpieczeństwa wewnętrznego państwa.

Przechodząc do wskazania czynności operacyjno-rozpoznawczych, które mogą być podejmowane przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego w zakresie zwalczania zagrożeń, należy zaznaczyć, iż tylko niektóre czynności operacyjno-rozpoznawcze zostały uregulowane na poziomie ustawy, natomiast większość z nich jest szczegółowo unormowana w niejawnych aktach prawnych wydawanych przez Szefa Agencji Bezpieczeństwa Wewnętrznego. Z uwagi na ograniczenia prawne wynikające z przepisów *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*⁷¹ w niniejszym rozdziale zostaną wskazane jedynie te aspekty pracy operacyjnej, które są regulowane w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Ponadto zostaną one ograniczone do tych czynności, które mogą być realizowane w celu wykonywania działań prewencyjnych, o których mowa w art. 5 ust. 1 pkt 1 tej ustawy.

Bez wątplenia na uwagę w tej kwestii zasługuje wspomniane w art. 35 ust. 2–4 ustawy o ABW oraz AW uprawnienie funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz osób udzielających Agencji Bezpieczeństwa Wewnętrznego pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych do posługiwania się dokumentami publicznymi w rozumieniu *ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych*⁷² lub innymi dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi posługuje się przy wykonywaniu zadań służbowych (tzw. dokumenty legalizacyjne), a także kompetencja Agencji Bezpieczeństwa Wewnętrznego do sporządzania i wydawania takich dokumentów na wnioski upoważnionych organów, służb i instytucji państwowych. Jak wskazano w literaturze przedmiotu, tzw. działania maskujące są to czynności mające na celu stworzenie lub wykorzystanie błędnego przeświadczenia osób, wobec których podejmowane są działania operacyjne lub osób postronnych, co do właściwego znaczenia określonych zdarzeń, obiektów lub tożsamości osób uczestniczących. W działaniach maskujących można wykorzystać m.in. legalizację, czyli uzyskanie lub wytworzenie dokumentów legalizacyjnych, zabezpieczających przed zdemaskowaniem rzeczywistych danych⁷³. Stosowanie wspomnianego wyżej maskowania na etapie działań prewencyjnych pozwala ukryć fakt zainteresowania Agencji Bezpieczeństwa Wewnętrznego danym zagadnieniem i umożliwia skuteczne gromadzenie niezbędnych informacji.

Bardzo ważną rolę w działaniach prewencyjnych Agencji Bezpieczeństwa Wewnętrznego odgrywa także instytucja współpracy z osobowymi źródłami informacji i tzw. przedsięwzięcie werbunkowe. Są one bodaj najstarszymi

⁷¹ Dz.U. 2019, poz. 742.

⁷² Dz.U. 2020, poz. 725.

⁷³ Por. M. Kolaszyński, dz. cyt., s. 139.

i „klasycznymi” źródłami poufnych informacji, wykorzystywanymi przez wszystkie polskie służby specjalne⁷⁴. Została ona uregulowana w art. 36 ustawy o ABW oraz AW i sprowadza się do możliwości korzystania z pomocy osób niebędących funkcjonariuszami przy wykonywaniu ustawowych zadań (tzw. tajni współpracownicy, tajni informatorzy). Na poziomie ustawowym wspomniana współpraca została obwarowana obustronnym zakazem ujawniania informacji — w odniesieniu do Agencji Bezpieczeństwa Wewnętrznego dotyczy ona danych o osobie udzielającej pomocy, a w odniesieniu do współpracowników faktu udzielania pomocy i okoliczności związanych z jej udzielaniem. Świadczy to o tym, iż współdziałanie z takimi osobami cechuje się bezwzględną tajnością zarówno w trakcie współpracy, jak i po jej zakończeniu.

Z przeglądu literatury, w szczególności kryminalistycznej, można wnioskować, iż tajnych współpracowników pozyskuje się z różnych środowisk, w tym np. ze środowisk kryminogennych i spośród osób tkwiących w nich⁷⁵. Można również znaleźć informację, iż współpracownicy mogą być werbowani do współpracy przez służbę lub też mogą podejmować taką współpracę z własnej inicjatywy. Zasadą jest, że informator ma tylko jednego prowadzącego, natomiast każdy funkcjonariusz operacyjny powinien mieć kilku stałych informatorów. Niezbędne informacje, wytyczne i wskazówki powinny być przekazywane informatorom przez funkcjonariuszy ustnie, podczas dyskretnych spotkań na neutralnym gruncie⁷⁶. Wskazane wyżej cechy pozwalają na przyjęcie, iż jest to jedna z podstawowych metod pozyskiwania informacji przez służbę. Dzięki odpowiedniemu uplasowaniu współpracowników służba może uzyskać, a następnie przetwarzać, informacje pochodzące bezpośrednio lub pośrednio od grup przestępczych czy też obcych służb.

Inną metodę prowadzenia czynności operacyjno-rozpoznawczych uregulowano w art. 23 ust. 1 pkt 6 ustawy o ABW oraz AW, z którego wynika, iż funkcjonariusze Agencji mają prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych (tzw. obserwacja). Obserwacja stanowi zespół czynności zmierzających do celowego, planowego, kierowanego i systematycznego postrzegania badanego zjawiska, przedmiotu czy zdarzenia, pozwalającego badaczowi na uzyskanie odpowiedzi na interesujące go pytania⁷⁷. Czynności te mają na celu śledzenie osób lub zjawisk po to, by uzyskać informacje, dokonać szczegółowych ustaleń i je udokumentować. Obserwacja może być wykonywana przez funkcjonariuszy osobiście bądź z wykorzystaniem specjalistycznego sprzętu

⁷⁴ Tamże.

⁷⁵ Zob. np. K. Sławik, *Kryminalistyka, przegląd zagadnień*, Warszawa 2002, s. 163.

⁷⁶ K. Ożóg-Wróbel, *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych”, t. 22, 2012, nr 4, s. 128–129.

⁷⁷ A. Żebrowski, *Czynności operacyjno-rozpoznawcze. Regulacje prawne*, Kraków 2000, s. 20.

technicznego. Literatura przedmiotu dostarcza poszerzonej wiedzy w tym zakresie. Wskazuje, że obserwacja może być prowadzona bezpośrednio, tj. przy zastosowaniu bezpośredniego poznania zmysłowego bądź pośrednio, z wykorzystaniem różnego rodzaju aparatury, jak np. kamer, promieniowania podczerwonego i innych urządzeń, zwłaszcza elektronicznych⁷⁸. Ponadto, ze względu na sposób prowadzenia czynności, wyróżniamy obserwację statyczną, dynamiczną, tajną, jawną oraz kombinowaną⁷⁹. Oczywiście obserwacja prowadzona jest w sposób niejawnym, z zachowaniem szczególnych wymogów oraz pełnej dyskrecji. Z uwagi na jej specyfikę — użycie środków technicznych i często brak bezpośredniego kontaktu z osobą obserwowaną — wydaje się ona bardzo uniwersalną metodą, która może zostać zastosowana w większość spraw podlegających rozpoznaniu operacyjnemu.

Metodą, która nabiera w ostatnich latach coraz większego znaczenia ze względu na dokonujący się postęp technologiczny, jest uprawnienie funkcjonariuszy do analizy billingów telefonicznych i logowań telefonów komórkowych na poszczególnych stacjach przekaźnikowych. Czynność ta obecnie pozwala odtworzyć drogę przemieszczania się użytkownika telefonu komórkowego oraz jego spotkania z innymi użytkownikami telefonów komórkowych. W tym aspekcie na uwagę zasługuje art. 28 ustawy o ABW oraz AW, regulujący uprawnienie do uzyskiwania niezbędnych do realizacji zadań, o których mowa w art. 5 ust. 1, danych niestanowiących treści odpowiednio przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, tzw. danych telekomunikacyjnych, danych pocztowych oraz internetowych, o których mowa w *ustawie z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne*⁸⁰ oraz przetwarzania ich bez wiedzy i zgody osoby, której dotyczą. Należy podkreślić, iż wspomniane dane, jak również i te, które Agencja Bezpieczeństwa Wewnętrznego ma prawo uzyskiwać na podstawie art. 28 b ustawy o ABW oraz AW (dane z elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci; dane objęte tajemnicą telekomunikacyjną, w przypadku użytkownika, który nie jest osobą fizyczną — numer zakończenia sieci oraz siedziba lub miejsce wykonywania działalności gospodarczej, firma lub nazwa i forma organizacyjna tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej — także nazwa miejscowości oraz ulicy, przy której znajduje się zakończenie sieci), które na gruncie Dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej (dyrektywa o prywatności i komunikacji elektronicznej) określane są jako dane o ruchu (*traffic data*) oraz dane o lokalizacji (*location data*)⁸¹.

⁷⁸ T. Hanausek, *Zarys taktyki kryminalistycznej*, Warszawa 1994, s. 108.

⁷⁹ Tamże, s. 109.

⁸⁰ Dz.U. 2012, poz. 567.

⁸¹ Dz.U. UE-sp. 13–29.514.

Jak wynika wprost z treści art. 28 i 28b, dane o ruchu i lokalizacji, zwane umownie „danymi bilingowymi”, mogą być wykorzystywane do realizacji wszystkich obszarów właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego określonej w art. 5 ust. 1 ustawy, w tym także i w zakresie zadania polegającego na rozpoznawaniu i zwalczaniu zagrożeń. Z pewnością informacje uzyskane w wyniku analizy danych bilingowych pozwalają na pogłębienie informacji o osobie, która została uprzednio pozyskana w toku czynności operacyjno-rozpoznawczych, pozwalają też na szybkie uzyskanie informacji, a jednocześnie zapewnienie ochrony kierunków i zainteresowań operacyjnych, co także znacząco wpływa na przyspieszenie i skuteczność działań prewencyjnych. Na szczególną uwagę zasługuje fakt, iż dane bilingowe pozwalają uzyskać wiedzę na temat lokalizacji aparatów telefonicznych, co jest szczególnie istotne w działaniach związanych ze szpiegostwem i terroryzmem, a także z zapewnieniem bezpieczeństwa najważniejszych osób w państwie. Ponadto informacje takie są istotne w zapobieganiu i zwalczaniu zagrożeń w cyberprzestrzeni (np. przez ustalenie adresu IP komputera).

Tytułem wyjaśnienia można dodać, iż na poziomie ustawy o ABW oraz AW uregulowano jeszcze kilka aspektów pracy operacyjnej, w tym możliwość korzystania z innych metod, tj.: kontroli operacyjnej (art. 27), zakupu kontrolowanego (art. 29) oraz przesyłki niejawnie nadzorowanej (art. 30). Jednakże wspomniane metody mogą być zastosowane jedynie w przypadku zwalczania przestępstw, i to tylko wymienionych konkretnie w tych przepisach, nie mogą natomiast być wykorzystane w celu wykonywania innych zadań ustawowych Agencji. Z tego powodu nie zostaną one szczegółowo omówione w publikacji dotyczącej działań prewencyjnych.

Należy zauważyć, iż w wyniku wykonywania czynności przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego może dojść do sytuacji, gdy okaże się, że informacje uzyskane w ich toku wskazują, że sprawa będąca ich przedmiotem należy do zakresu działania innych organów, służb lub instytucji. Taki stan został uregulowany przez ustawodawcę w art. 22a ust. 1 ustawy o ABW oraz AW, zgodnie z którym Szef Agencji przekazuje wówczas, z zastrzeżeniem ust. 5–7, uzyskane informacje i materiały właściwemu podmiotowi. Jeżeli informacje i materiały uzyskane przez Agencję Bezpieczeństwa Wewnętrznego wskazują na uzasadnione podejrzenie popełnienia przestępstwa lub przestępstwa skarbowego albo potwierdzają jego popełnienie, Szef Agencji Bezpieczeństwa Wewnętrznego przedstawia je właściwemu prokuratorowi w celu podjęcia decyzji w zakresie ich dalszego procesowego wykorzystania (ust. 3). Natomiast jeśli wskazują na uzasadnione podejrzenie popełnienia wykroczenia lub wykroczenia skarbowego albo potwierdzają jego popełnienie, Szef Agencji Bezpieczeństwa Wewnętrznego zawiadamia organ właściwy dla ścigania sprawcy (ust. 4). Na podkreślenie zasługuje przepis ust. 5, który pozwala Szefowi Agencji Bezpieczeństwa Wewnętrznego na podjęcie decyzji o kontynuowaniu sprawy, nawet jeżeli w toku wykonywania czynności operacyjno-rozpoznawczych ujawnią się okoliczności wskazujące na to, że sprawa będąca przedmiotem tych czynności

nie pozostaje w kompetencji Agencji Bezpieczeństwa Wewnętrznego, o ile jest to uzasadnione bezpieczeństwem państwa. Przepis ten jest bardzo ważny z punktu widzenia właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego z art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW, albowiem pozwala *de facto* na incydentalne poszerzenie zakresu działania Agencji Bezpieczeństwa Wewnętrznego o sprawę, która literalnie nie mieści się w zakresie jej właściwości, ale została oceniona jako taka, która może mieć wpływ na bezpieczeństwo państwa. Na podstawie tego przepisu Szef Agencji Bezpieczeństwa Wewnętrznego ma przyznaną pewną autonomię w decydowaniu o uprawnieniu Agencji Bezpieczeństwa Wewnętrznego do kontynuowania danej sprawy z uwagi na bezpieczeństwo państwa, jednakże nie decyduje samodzielnie, lecz za zgodą Prezesa Rady Ministrów, a w przypadku powołania ministra w celu koordynowania działalności służb specjalnych — za zgodą tego ministra (ust. 6–8). Ze względu na rangę tych spraw i wyjątkowość sytuacji Prezydent Rzeczypospolitej Polskiej na podstawie ust. 6 i 9 jest informowany o wystąpieniu do Prezesa Rady Ministrów o zgodę i jej uzyskaniu na kontynuowanie czynności przez Agencję Bezpieczeństwa Wewnętrznego.

W aspekcie rozpoznawania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny niewątpliwie doniosłą rolę odgrywają także działania o charakterze analityczno-informacyjnym, które zostały wskazane, obok czynności operacyjno-rozpoznawczych, w art. 21 pkt 2 ustawy o ABW oraz AW. Czynności te polegają zasadniczo na gromadzeniu, przetwarzaniu i przekazywaniu informacji istotnych z punktu widzenia bezpieczeństwa państwa innym organom w celu ułatwienia im podejmowania decyzji, a także mają znaczenie dla dalszych działań służby. Jak wskazuje się w literaturze, przy analizowaniu tych czynności, w relacji do innych wykonywanych przez służby specjalne, można zaobserwować, że występują one w podwójnej roli. W pierwszej z nich stanowią zwieńczenie pracy operacyjnej. Wynika to z tego, że informacje zebrane w trakcie czynności operacyjno-rozpoznawczych najczęściej nie nadają się do bezpośredniego przekazania odbiorcom zewnętrznym z uwagi choćby na ich ilość. Dlatego wymagają selekcji, interpretacji oraz możliwie szybkiej analizy, pozwalającej wyselekcjonować wiedzę najbardziej wartościową, a przy tym przekazać ją w sposób spójny i zrozumiały. Tę rolę omawianych czynności określa się jako ich wykorzystanie na poziomie politycznym. Wydaje się, że takim zwieńczeniem pracy operacyjnej będzie też przekazanie tych informacji innym organom w przypadku, gdy będzie to uzasadnione z uwagi na ich kompetencje. Z kolei druga ich rola to wykorzystanie informacji na poziomie operacyjnym, ewentualnie śledczym. W tej sytuacji czynności analityczno-informacyjne są spożytkowane wewnątrz służby i mają na celu ukierunkowanie dalszej działalności operacyjnej lub śledczej⁸².

Czynności analityczno-informacyjne pomimo tego, że pełnią istotną rolę w rozpoznawaniu i zwalczaniu zagrożeń, nie zostaną w tym miejscu

⁸² Por. M. Kolaszyński, dz. cyt., s. 147.

szczegółowo opisane, gdyż będą przedmiotem odrębnego rozdziału. Jedyne sygnalizacyjnie można zaznaczyć, iż wykonywanie tych czynności oraz ich ranga znajdują odzwierciedlenie w strukturze organizacyjnej Agencji Bezpieczeństwa Wewnętrznego — z powołanego już wyżej zarządzenia Prezesa Rady Ministrów w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego wynika, iż w strukturze Agencji Bezpieczeństwa Wewnętrznego wyodrębniono wyspecjalizowaną jednostkę analityczną, jaką jest Departament Informacji, Analiz i Prognoz, do którego podstawowego zakresu działania należy właśnie gromadzenie i przetwarzanie informacji istotnych z punktu widzenia właściwości ustawowej Agencji Bezpieczeństwa Wewnętrznego. Ponadto czynności analityczno-informacyjne są także wykonywane w ramach pracy departamentów kierunkowych (liniowych).

Należy także zwrócić uwagę, iż np. w *Raporcie z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.* podkreślono rolę Agencji Bezpieczeństwa Wewnętrznego w zakresie pozyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, o czym jest mowa w art. 18 ustawy o ABW oraz AW. Wskazano, iż opracowania analityczno-informacyjne Agencji Bezpieczeństwa Wewnętrznego powstają na podstawie wiedzy uzyskanej z rozpracowania operacyjnego, ustaleń o charakterze dochodzeniowo-śledczym, a także z danych pochodzących ze źródeł ogólnodostępnych. Ich celem jest wspieranie procesu decyzyjnego, dokonywanie oceny ryzyka oraz zapobieganie negatywnym skutkom zjawisk i wydarzeń. Agencja, mając świadomość znaczenia funkcji analityczno-informacyjnej i jej wpływu na bezpieczeństwo RP, coraz większy nacisk kładła na opracowywanie analiz strategicznych oraz informacji wyprzedzających⁸³.

W kontekście informacji gromadzonych przez Agencję Bezpieczeństwa Wewnętrznego należy także wskazać na art. 18 ust. 1 ustawy o ABW oraz AW, na podstawie którego Szef Agencji, w zakresie swojej właściwości, przekazuje niezwłocznie Prezydentowi Rzeczypospolitej Polskiej i Prezesowi Rady Ministrów informacje mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej. Obowiązek ten został zmodyfikowany w treści ust. 2, według którego powyższe informacje są przekazywane Prezydentowi Rzeczypospolitej Polskiej w każdym przypadku, kiedy tak zdecyduje, zaś w ust. 3 przewidziano, iż te informacje są przekazywane właściwemu ministrowi, w zakresie jego działania, chyba że Prezes Rady Ministrów zdecyduje inaczej. Na podstawie tego przepisu Szef Agencji Bezpieczeństwa Wewnętrznego jest uprawniony i jednocześnie zobowiązany do przekazywania wskazanym organom informacji, które zostały uzyskane w toku działalności ustawowej Agencji, a które są jednocześnie kwalifikowane jako takie, które mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej. Wprawdzie w cytowanym przepisie nie mamy wprost odniesienia ani do „zagrożenia” ani do „bezpieczeństwa

⁸³ *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014...*, s. 5.

wewnętrznego”, jednak zestawienie tego przepisu z art. 5 ust. 1 ustawy o ABW oraz AW pozwala na postawienie tezy, że owo zadanie Szefa Agencji Bezpieczeństwa Wewnętrznego — jako element działań o charakterze informacyjnym — wpisuje się również w rozpoznawanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny. Przyjęcie odmiennej interpretacji prowadziłoby do nieuprawnionego wniosku, iż w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu nie przewidziano, by tego rodzaju czynności, a dokładniej ich efekty w formie informacji/analiz dotyczących istotnych zagadnień dla bezpieczeństwa państwa i jego pozycji międzynarodowej, były wykorzystywane jako narzędzia dedykowane do rozpoznawania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny. W ocenie autora niniejszego rozdziału przepis art. 18 interpretowany w połączeniu z art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW stanowi *de facto* swoistą podstawę do skutecznego prowadzenia działań prewencyjnych przez gromadzenie informacji i przekazywanie jej właściwym organom państwowym. Można podsumować, iż wskazane wyżej przepisy statuują najbardziej charakterystyczną, swoistą cechę służb specjalnych, która pozwala na wypełnienie jej podstawowej roli w zakresie obowiązku informacyjnego wobec najwyższych organów państwa w celu sprawnego i bezpiecznego funkcjonowania jego instytucji i obywateli.

W aspekcie czynności analityczno-informacyjnych doniosłą rolę odgrywa także przepis art. 33 ustawy o ABW oraz AW, który statuuje uprawnienie Agencji Bezpieczeństwa Wewnętrznego do uzyskiwania informacji, w tym także niejawnie, gromadzenia ich, sprawdzania i przetwarzania — w zakresie właściwości ustawowej. Niewątpliwie zatem wspomniane uprawnienie przysługuje także i w zakresie działań prewencyjnych i dotyczy zarówno informacji pozyskiwanych ze źródeł zewnętrznych, jak i wewnętrznych. Podobną funkcję odgrywa także uprawnienie przewidziane w art. 34 ust. 1 ustawy o ABW oraz AW, dotyczące możliwości zbierania, także niejawnie, w ramach właściwości ustawowej, wszelkich danych osobowych, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, także i danych wrażliwych wskazanych w art. 14 ust. 1 *ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych* przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości⁸⁴, tj. danych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych, a także danych genetycznych, biometrycznych, dotyczących zdrowia, seksualności i orientacji seksualnej osoby fizycznej, a także możliwości korzystania z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzania ich bez wiedzy i zgody osoby, której dotyczą. Przepis ten pozwala nie tylko gromadzić dane osobowe, ale także je przetwarzać, tj. dokonywać wszelkich operacji na tych danych, takich jak np. zbieranie,

⁸⁴ Dz.U. 2019, poz. 125.

utrwalanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, usuwanie lub niszczenie. Wskazane wyżej przepisy pozwalają Agencji Bezpieczeństwa Wewnętrznego na bardzo szeroki dostęp do informacji, w tym także tych uzyskiwanych za pośrednictwem systemów teleinformatycznych, co przekłada się na bardzo szybkie i sprawne działanie, prowadzone czasem nawet bez konieczności wychodzenia z budynku i bez potrzeby nawiązywania kontaktu osobistego z osobami spoza służby, co z kolei umożliwi prowadzenie działań przez funkcjonariuszy z mniejszym ryzykiem ewentualnej dekonspiracji.

Analizując działania funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego w zakresie rozpoznawania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa, podejmowane w formie czynności operacyjno-rozpoznawczych i analityczno-informacyjnych, należy zwrócić uwagę na przewidzianą w art. 40 ust. 1 ustawy o ABW oraz AW rolę Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie koordynowania czynności operacyjno-rozpoznawczych podejmowanych przez służby specjalne, mogących mieć wpływ na bezpieczeństwo państwa. Na podstawie ust. 2 tego przepisu Szef Agencji Bezpieczeństwa Wewnętrznego w celu zapewnienia koordynacji prowadzi centralną ewidencję zainteresowań operacyjnych służb specjalnych. Z uwagi na ograniczenia natury prawnej, a w szczególności niejawni charakter tych czynności oraz regulacji związanej z prowadzeniem wymienionej ewidencji, na potrzeby niniejszego rozdziału można jedynie wskazać, iż takie uprawnienie zostało ustawowo przewidziane i pozostawione je do uregulowania w drodze zarządzenia Prezesa Rady Ministrów, które winno uwzględniać wymogi dotyczące ochrony informacji niejawnych. Z samego brzmienia art. 40 ustawy o ABW oraz AW można jedynie wnioskować, iż ustawodawca dostrzegł potrzebę koordynowania, czyli pewnego uprządkowania działań operacyjnych podejmowanych przez kilka podmiotów, w tym przypadku przez służby specjalne i tę funkcję powierzył właśnie Szefowi Agencji Bezpieczeństwa Wewnętrznego. Wydaje się, że *ratio legis* tego przepisu sprowadzał się do stworzenia pewnego narzędzia do zebrania w jednym miejscu wiedzy na temat działań operacyjnych, co z kolei pozwoli wyeliminować problemy związane z prawidłową wymianą informacji między służbami specjalnymi. Na podkreślenie zasługuje fakt, iż wspomniana ewidencja dotyczy jedynie koordynacji działań podejmowanych przez służby specjalne, a nie wszystkie służby uprawnione do wykonywania czynności operacyjno-rozpoznawczych. Regulacja podstawowa dotycząca tej kwestii, wydana na podstawie art. 40 ust. 3 ustawy o ABW oraz AW, stanowi dokument niejawni i nie może zostać szczegółowo opisana na użytek niniejszego rozdziału.

Na marginesie można również dodać, iż służby specjalne co do zasady dysponują podobnym do Agencji Bezpieczeństwa Wewnętrznego arsenalem środków prawnych do realizacji ustawowych zadań, w tym także w zakresie tzw. działań prewencyjnych — w szczególności przez wykonywanie czynności operacyjno-rozpoznawczych oraz uzyskiwanie i przetwarzanie informacji. Jak już wyżej wskazano, najbardziej zbliżone do regulacji Agencji Bezpieczeństwa

Wewnętrzny jest unormowanie zawarte w art. 25 ustawy o SKW oraz SWW, zgodnie z którym funkcjonariusze Służby Kontrwywiadu Wojskowego mają prawo do wykonywania czynności operacyjno-rozpoznawczych i analityczno-informacyjnych. Podkreślenia wymaga fakt, iż Służba Kontrwywiadu Wojskowego, w odróżnieniu od Agencji Bezpieczeństwa Wewnętrznego, jest służbą wykonującą co do zasady jedynie działania o charakterze prewencyjnym, albowiem nie dysponuje ona uprawnieniem do wykonywania czynności dochodzeniowo-śledczych, a wyniki czynności operacyjno-rozpoznawczych prowadzonych przez tę służbę, już na poziomie procesowym, są opracowywane i waloryzowane przez Żandarmerię Wojskową na podstawie przepisów *ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*⁸⁵.

Podsumowanie

Rozważania w zakresie charakteru i obszarów działań prewencyjnych bez wątpienia prowadzą do konstatacji, iż Agencja Bezpieczeństwa Wewnętrznego jest służbą specjalną dedykowaną do rozpoznawania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny. Pomimo tego, że pojęcia „bezpieczeństwo” i „zagrożenie” słownikowo są przeciwieństwami, to w omawianym aspekcie pozostają one ze sobą we wzajemnej zależności, a wręcz się uzupełniają. Ze względu na to, że wraz z rozwojem cywilizacji pojawiają się nowe zagrożenia poszerza się również znaczenie słowa „bezpieczeństwo”, a tym samym obszar działania Agencji Bezpieczeństwa Wewnętrznego w zakresie zagrożeń bezpieczeństwa wewnętrznego. Dzięki sprawnemu działaniu służb wywiadowczych i kontrwywiadowczych, zwłaszcza w aspekcie działalności prewencyjnej, uzyskana w jej trakcie wiedza na temat otaczających nas negatywnych zjawisk pozwala często uniknąć zagrożenia, jeśli nawet nie całkowicie, to chociaż eliminuje element zaskoczenia. Umożliwia to zatem skuteczne zminimalizowanie ryzyka związanego z pojawieniem się zagrożenia, a jeśli nie dało się uniknąć jego wystąpienia, to pozwala na skuteczne zwalczanie tego zagrożenia. Dzięki wyprzedzającemu posiadaniu właściwych/niezbędnych informacji można się przygotować, nauczyć się podejmować skuteczne i skoordynowane działania, eliminując zagrożenia lub zmniejszając ich skutki.

Można nawet zaryzykować twierdzenie, iż działania prewencyjne służb specjalnych może i nie są efektywne, ale z pewnością efektywne. O ile bowiem przy przestępstwach mamy do czynienia z wykryciem sprawcy, o tyle działalność w zakresie rozpoznawania i zwalczania zagrożeń winna pozostawać utajniona.

Jak już wyżej wskazano, trudno jest jednoznacznie zdefiniować „zagrożenia godzące w bezpieczeństwo wewnętrzne i porządek konstytucyjny państwa”, jednakże przez lata funkcjonowania Agencji Bezpieczeństwa Wewnętrznego udało się wypracować wspomniany wyżej katalog zdarzeń, które winny być

⁸⁵ Dz.U. 2020, poz. 431 z późn. zm.

kwalifikowane jako takie zagrożenia i podlegać działaniom prewencyjnym Agencji Bezpieczeństwa Wewnętrznego.

Można także stwierdzić, iż charakter ustrojowy Agencji Bezpieczeństwa Wewnętrznego oraz konstrukcja obowiązującej ustawy o ABW oraz AW i wynikające z niej uprawnienia nie pozostawiają wątpliwości co do zakresu jej kompetencji w sferze bezpieczeństwa wewnętrznego oraz porządku konstytucyjnego w opisanych wyżej wymiarach (obszarach), dominującej roli w systemie działań prewencyjnych oraz zasadności podejmowania tych działań w celu ochrony wartości fundamentalnych z punktu widzenia bezpieczeństwa państwa jako organizacji, ale także jego obywateli. Skuteczność działania organów państwa możliwa jest dzięki posiadaniu wyprzedzających informacji o potencjalnych zagrożeniach i metodach ich neutralizacji — wiedza w tym zakresie zdobyta przez Agencję Bezpieczeństwa Wewnętrznego i jej przekazanie właściwym podmiotom są niezbędne dla sprawnego funkcjonowania konstytucyjnych organów państwa. Można nawet zaryzykować twierdzenie, iż jest to znacznie bardziej doniosła rola służb specjalnych niż działania w zakresie zwalczania konkretnych przestępstw czy ścigania ich sprawców, co mogłoby czysto teoretycznie zostać powierzone do wykonania służbom policyjnym.

Kluczowe znaczenie posiadania informacji dostrzegali Sun Tzu, który już w VI w. p.n.e. stwierdził, iż najwyższym osiągnięciem jest pokonać wroga bez walki, a sprawą najwyższej wagi jest rozbicie strategii wroga. Według tego chińskiego stratega jest to możliwe dzięki posiadaniu informacji, które nazywał *przewidującą wiedzą*⁸⁶. Nie budzi zatem wątpliwości to, że doniosłe, a wręcz fundamentalne, znaczenie informacji winno wyznaczać pożądany kierunek w ewolucji służb specjalnych, a szczególnie w odniesieniu do Agencji Bezpieczeństwa Wewnętrznego — w zakresie wzmacniania jej roli w aspekcie prowadzenia działań prewencyjnych w systemie organów powołanych do zapewnienia bezpieczeństwa państwa.

⁸⁶ Sun Tzu, *Sztuka wojny*, Przedświt, Warszawa 1994, s. 35.

Tomasz Batory

Rozdział 3.

Zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw

Wstęp

*Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*¹ czyni Agencję Bezpieczeństwa Wewnętrznego organem zobowiązanym do ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Tym samym podstawowym zadaniem ABW jako służby specjalnej jest zwalczanie zagrożeń codziennego, normalnego stanu funkcjonowania państwa². Swoją obowiązkowość ABW realizuje m.in. przez zwalczanie przestępczości zwróconej przeciwko bezpieczeństwu wewnętrznemu państwa.

Celem niniejszego rozdziału jest prezentacja ram prawnych, w ramach których ABW realizuje nałożone na nią zobowiązania, oraz instrumentarium środków służących ich realizacji.

Analiza historyczna

„Bez przeszłości nie ma przyszłości”³, i chciałoby się dodać teraźniejszości, dlatego prezentacja rozwiązań prawnych, jakie ustawodawca przewidział dla ABW, nie może obyć się bez odwołania się do pierwowzoru aktualnie obowiązujących regulacji prawnych, tj. do przepisów ustawy o UOP i zawartych w niej zadań oraz środków tym zadaniom dedykowanych. Powstanie UOP jest

¹ *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U., nr 74, poz. 676).

² M. Bożek, *Instytucjonalny system bezpieczeństwa państwa w świetle Konstytucji RP na tle członkostwa Polski w Unii Europejskiej*, w: *Europa — kontynent ryzyka? Społeczne, polityczne i normatywne uwarunkowania bezpieczeństwa w Europie*, red. M. Bożek, M. Troszyński, Warszawa 2007, s. 101; M. Bożek i in., dz. cyt., s. 28.

³ W. Smith, *Placz aniołów*, Warszawa 2013.

nierozerwalnie związane z wydarzeniami historycznymi 1989 r. w Europie i będącą ich konsekwencją transformacją ustrojową państwa polskiego. Ideą UOP, nowej demokratycznej służby specjalnej, było zapewnienie suwerennemu państwu polskiemu skutecznych instrumentów pozwalających neutralizować zagrożenia zewnętrzne i wewnętrzne. Zgodnie z założeniami ustawodawcy, przyjętymi na podstawie wzorców wypracowanych przez tzw. stare demokracje, nowa służba specjalna miała odgrywać ważną rolę w systemie bezpieczeństwa państwa demokratycznego. Przy czym ustawodawca od początku przypisał służbom specjalnym zadania chronienia państwa przed najpoważniejszymi zagrożeniami, a ponadto nałożył na UOP obowiązki w zakresie działań informacyjnych, procesowych oraz ochronno-kontrolnych. Bieżące potrzeby zapewnienia właściwego funkcjonowania państwa w kontekście zmieniającej się sytuacji wewnętrznej i zewnętrznej wymusiły ewolucję uprawnień polegającą na ich stopniowym rozszerzaniu. Na znaczeniu zyskiwały zadania mające na celu zwalczanie przestępczości międzynarodowej i gospodarczej wymierzonej w fundamentalne interesy państwa polskiego. Rozwinięciu uległ również zakres czynności procesowych przewidzianych dla funkcjonariuszy UOP. Początkowo dotyczyły one jedynie przestępstw szpiegostwa i terroryzmu oraz innych poważnych przestępstw przeciw państwu. Po ostatniej nowelizacji ustawy o UOP⁴ uprawnienia procesowe objęły dodatkowo przestępstwa godzące w podstawy ekonomiczne państwa i mające charakter lub zasięg międzynarodowy, w tym nielegalne wytwarzanie, posiadanie i obrót bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi, psychotropowymi lub materiałami jądrowymi i promieniotwórczymi.

Zestawienie zadań postawionych przed UOP z aktualnymi zadaniami realizowanymi przez ABW prowadzi do wniosku, iż obecnie obowiązujący art. 5 ustawy o ABW oraz AW jest bezpośrednim sukcesorem art. 1 ustawy o UOP. Faktem bezspornym jest, że ustawodawca, konstruując art. 5 ustawy o ABW oraz AW, niewątpliwie wykorzystał zapisy art. 1 ustawy o UOP. Jednak zdaniem krytyków obowiązujących aktualnie regulacji jest to dziedziczenie z dobrodziejstwem inwentarza, powtarzające i utrwalające nieprawidłowe praktyki legislacyjne⁵.

Omówienie główne instytucji

Niewątpliwie usytuowanie służb specjalnych w systemie organów państwowych jest wypadkową wykonywanych przez nie zadań. W państwach demokratycznych główna część aktywności służb specjalnych ogniskuje się wokół funkcji ochrony ustroju demokratycznego, która to funkcja bywa określana

⁴ Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz.U. 1999, poz. 526, 548, 1255; 2000, poz. 852; 2001, poz. 877 i 1149).

⁵ M. Bożek, *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, „Studia Iuridica Lublinensia” 2015.

jako pierwotna i podstawowa w stosunku do pozostałych. Na ogół, choć czynności służb specjalnych mogą pozostawać w sprzeczności z prawem do ochrony prywatności, wolnością i ochroną tajemnicy komunikowania się czy też autonomią informacyjną, są uznawane za konieczne w demokratycznym państwie prawa z uwagi na ochronę bezpieczeństwa państwa, porządku publicznego bądź ochronę wolności i praw człowieka jako jednostki i zbiorowości. Bezpieczne funkcjonowanie państwa staje się bowiem wartością najwyższą i warunkiem *sine qua non* wykonywania pozostałych funkcji⁶. Nie oznacza to oczywiście *carte blanche* dla służb specjalnych i przyznania im możliwości działania zgodnie z zasadą *exitus acta probat*⁷. Dopuszczalność stosowania czynności przez służby specjalne zależy przede wszystkim od przestrzegania przez nie konstytucyjnych wymagań, mających chronić jednostki przed ekscesami w stosowaniu prawa i nadmiernym wkroczeniem w sferę ich prywatności, a ponadto zabezpieczać przed wpływaniem na demokratyczny mechanizm sprawowania władzy w państwie.

Przechodząc do prezentacji art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, będącego *de facto* tematem niniejszego rozdziału, należy wskazać, iż stanowi on ramy prawne, w jakie ujęto działania podejmowane przez ABW w związku z realizacją funkcji ochronnej państwa w aspekcie zwalczania przestępczości.

Do zadań ABW należy zatem:

2) rozpoznawanie, zapobieganie i wykrywanie przestępstw:

- a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa,
- b) godzących w podstawy ekonomiczne państwa,
- c) korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. z 2017 r. poz. 1393 oraz z 2019 r. poz. 371 i 492), jeżeli może to godzić w bezpieczeństwo państwa,
- d) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
- e) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym,
- f) przeciwko wymiarowi sprawiedliwości, określonych w art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 KK, jeżeli pozostają w związku z przestępstwami, o których mowa w lit. a–e oraz ściganie ich sprawców.

⁶ J. Kuciński, *Nauka o państwie*, Wyższa Szkoła Zarządzania i Prawa, Warszawa 2012, s. 56, s. 63–64; s. 80, 85–86; zob. m.in. E. Ura, *Prawne zagadnienia bezpieczeństwa państwa*, Krajowa Agencja Wydawnicza, Rzeszów 1988, s. 11.

⁷ „Cel uświęca środki”, „Heroides” Owidiusz.

Odnosząc się do wyżej wymienionych zapisów art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, należy wskazać, iż wszystkie cztery rodzaje czynności do jakich ustawodawca zobowiązał ABW w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, tj. rozpoznawanie, zapobieganie, wykrywanie i ściganie, odnoszą się do przestępstw skatalogowanych w art. 5 ust. 1 pkt. 2 rzeczonyj ustawy. Tym samym należy uznać, iż ustawodawca uczynił Agencję Bezpieczeństwa Wewnętrznego organem państwa, który oprócz wielu innych zadań realizuje również te polegające na zwalczaniu przestępczości⁸. Kwartet uprawnień, w jaki ustawodawca wyposażył ABW, daje możliwości skutecznej walki z przestępczością *ab ovo usque ad mala*, tj. od zebrania informacji w ramach czynności operacyjno-rozpoznawczych do przeprowadzenia postępowania karnego pod nadzorem prokuratora, skutkującego sporządzeniem aktu oskarżenia.

W przeciwieństwie jednak do Policji⁹ ABW jako służba specjalna nie zajmuje się zwalczaniem każdej przestępczości, lecz tylko jej rodzajów wyszczególnionych w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, a więc godzącej w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny. W art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW ustawodawca doprecyzował zatem zakres przestępstw, wyznaczając ABW specjalne cele (np. przeciwdziałanie i wykrywanie szpiegostwa), które ze względu na znaczenie dla interesów państwa oraz wiążący się z ich specyfiką stopień skomplikowania czynności operacyjnych, uzasadniają nadanie jej odmiennego statusu i zakresu kompetencji. Zadania, jakie ustawodawca nałożył na ABW, wykazują istotne odmienności od celów powołania pozostałych służb specjalnych i formacji policyjnych. Specyfika tych zadań oraz waga interesów, których zabezpieczeniu mają one służyć, wymusza stworzenie adekwatnego otoczenia normatywnego wraz z odpowiednim instrumentarium pozwalającym na sprawne wykonywanie zadań określonych przez ustawodawcę.

Użycie w przepisach ustawy wyżej wymienionych zastrzeżeń zakresowych istotnie zawęży pole działania ABW w zakresie zwalczania przestępczości. Jest to widoczne wprost w art. 5 ust. 1 pkt 2 lit. a, c i d ustawy o ABW oraz AW. Agencja realizuje swe funkcje, jeśli przestępstwa godzą lub mogą godzić w bezpieczeństwo państwa. W wyżej wymienionym przypadku sytuacja jest klarowna, gdyż po wyliczeniu kategorii przestępstw przepis wskazuje wprost, iż godzą one lub mogą godzić w bezpieczeństwo państwa. Jednak wydaje się logicznym, iż i w pozostałych jednostkach redakcyjnych art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW powinno zawęzić się ujęcie przestępstw do kategorii dotyczących ochrony bezpieczeństwa państwa i porządku konstytucyjnego. Przy czym w przypadku art. 5 ust. 1 pkt 2 lit. b i e ustawy o ABW oraz AW zawężenie należy wiązać i wywodzić z ogólnych kompetencji ABW ujętych w art. 1 ustawy o ABW oraz AW, tzn. „ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego”.

⁸ *Konstytucyjne i ustawowe uwarunkowania organizacji i funkcjonowania ABW*, Siedlce 2015.

⁹ *Ustawa o Policji z dnia 6 kwietnia 1990 r.* (Dz.U. 2020, poz. 360) art. 14 (*Czynności służbowe Policji*).

Przechodząc do analizy konstrukcji art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, należy zauważyć, iż lit. a, b i c tego przepisu zawierają zwroty nieookreślone, a mianowicie art. 5 ust. 1 pkt 2 lit. a ustawy o ABW oraz AW zawiera zapis: *i innych przestępstw godzących w bezpieczeństwo państwa*, art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW zawiera zwrot: *przestępstwa godzące w podstawy ekonomiczne państwa*, natomiast art. 5 ust. 1 pkt 2 lit. c ustawy o ABW oraz AW zawiera fragment: *jeśli może to godzić w bezpieczeństwo państwa*. Tym samym przepisy ustawy o ABW oraz AW nie odsyłają do konkretnych przepisów karnych, w których ustawodawca opisuje dane typy przestępstw godzących w bezpieczeństwo państwa lub podstawy ekonomiczne państwa. W tej sytuacji katalog takich przestępstw, których zwalczanie należy do zadań ustawowych ABW, jest bliżej nieokreślony (otwarty). Konstrukcja przepisu art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW przez to, że odnosi się do katalogu otwartego, powoduje, iż ustawodawca, określając kompetencje ABW, posłużył się wyrażeniami pozakodeksowymi, co z kolei oznacza, iż identyfikacja „przestępstw godzących w bezpieczeństwo państwa”, „przestępstw mogących godzić w bezpieczeństwo państwa”, „przestępstw godzących w podstawy ekonomiczne państwa” może napotykać trudności. Przyjęta koncepcja konstrukcji art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW spotkała się z polemiką zarówno ze strony praktyków, jak i teoretyków prawa, szermujących argumentami o jej kolizyjności z zasadami demokratycznego państwa prawnego¹⁰. Zgodnie z tą teorią w państwie odwołującym się na gruncie rozwiązań konstytucyjnych do idei państwa prawa ustawodawca nie powinien używać terminów nieostrych, konstruując przepisy kompetencyjne organów państwowych. Jako argument krytycy redakcji art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW podawali m.in. wyrok Trybunału Konstytucyjnego z dnia 14 grudnia 1999 r. (Sk 14/98 OTK 1999/7/163). Trybunał wskazuje w nim, że użycie przez prawodawcę pojęć nieookreślonych lub klauzul generalnych nie jest równoznaczne z przyznaniem interpretatorowi absolutnej i pozostającej poza wszelką kontrolą swobody w zakresie wykładni tego rodzaju zwrotów, a wręcz przeciwnie, zobowiązuje organ stosujący prawo do szczególnej staranności. Tym samym ustawodawca nie może z powodu niejasnego sformułowania tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki (wyrok TK z dnia 23 marca 2006 r., sygn. K 4/06 OTK-A nr 3/2006 poz. 32, por. wyrok TK z dnia 30 października 2001 r., sygn. K 33/00, OTK ZU nr 7/2001 poz. 217). Krytycy przyjętej przez ustawodawcę, w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, koncepcji granic właściwości działania i norm kompetencyjnych ABW wskazywali¹¹, iż przyjęte rozwiązania, stanowiąc podstawy podejmowanych

¹⁰ Wniosek RPO z dnia 15 listopada 2011 nr RPO-683674-II/II/MK; M. Bożek *Zwalczanie przestępstw...*

¹¹ Wnioski Prokuratora Generalnego z 12 listopada 2015 r. (sygn. akt K 32/15) oraz Rzecznika Praw Obywatelskich z 4 grudnia 2015 r. (sygn. akt K 41/15).

przez ABW konkretnych działań, w tym czynności operacyjnych, nie odpowiadają zasadom rzetelnej legislacji, w tym należytej poprawności, precyzyjności i jasność przepisów stanowiących podstawę wkraczania władzy wykonawczej w sferę konstytucyjnie chronionych praw i wolności. Powyższe argumenty zmateriałyzyowały się w postaci wniosków Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego skierowanych do Trybunału Konstytucyjnego o zbadanie zgodności z Konstytucją RP art. 5 ust. 1 pkt 2 lit. a i c ustawy o ABW oraz AW.

Warto jednak zauważyć, iż Trybunał Konstytucyjny, poddając ocenie art. 5 ust. 1 pkt 2 lit. a ustawy o ABW oraz AW w zakresie, w jakim obejmuje zwrot *i innych przestępstw godzących w bezpieczeństwo państwa*, a także art. 5 ust. 1 pkt 2 lit. c ustawy o ABW oraz AW, uznał je za zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności (zob. wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11). Z uwagi na to, iż argumentacja Trybunału rozstrzyga kontrowersje pojawiające się w odniesieniu do treści art. 5 ust. 1 pkt 2, pozwolę sobie na jej prezentację.

Po pierwsze Trybunał Konstytucyjny uznał, iż:

ustawowa regulacja całego art. 5 (...) jest kompleksowa, spójna, a także konstrukcyjnie, aksjologicznie i prakseologicznie racjonalna (...) Kompleksowość regulacji całego art. 5 ustawy o ABW oraz AW wynika z identyfikowania przez prawodawcę chronionych wartości oraz określenia przedmiotu działania ABW za pomocą zastosowania formuły wyznaczenia zadań tego organu policji bezpieczeństwa — właściwego w sprawach ochrony bezpieczeństwa wewnętrznego i porządku konstytucyjnego naszego państwa.

Po drugie: Trybunał Konstytucyjny stwierdził, iż:

Chronione w art. 5 ustawy o ABW oraz AW wartości są objęte treścią pojęć: bezpieczeństwo państwa, bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, suwerenność i międzynarodowa pozycja państwa, nienaruszalność jego terytorium, obronność państwa, podstawy ekonomiczne państwa, a także m.in. moralność publiczna i sprawność funkcjonowania instytucji państwa, zobowiązania prawnomiędzynarodowe państwa z ich przesłankami aksjologicznymi. Z natury swojej te konstytucyjnie istotne wartości nie mogą być w ustawie szczegółowo wyspecyfikowane, stąd konieczność posłużenia się przez prawodawcę pojęciem ogólnym, „zbierającym” wartości szczególne.

Po trzecie Trybunał Konstytucyjny uznał, iż:

Ustawodawca zadbał o spójność działań realizujących zadania, stosując formułę dopełnienia (pkt 1 „w szczególności...”, pkt 2 lit. a „i innych przestępstw godzących w bezpieczeństwo państwa”), będącą jedyną możliwą do zastosowania przy bogactwie faktycznym i aksjologicznym przedmiotu

regulacji. Kierowanie do ustawodawcy postulatu wyczerpującego wyliczenia typów przestępstw w oderwaniu od ogólnego kwalifikatora („godzenie w bezpieczeństwo państwa”), jeśli w ogóle byłoby możliwe, to ocierałoby się o granice legislacyjnej poprawności. (...) Kompletnie zindywidualizowanie przestępstw w kontekście normy zawartej w art. 5 ustawy o ABW oraz AW prowadziłoby do pozostawienia poza regulacją stanów faktycznych i prawnych „godzących w bezpieczeństwo państwa”, co bezpośrednio naruszałoby art. 1 Konstytucji RP oraz mogłoby także bezpośrednio i pośrednio godzić w wolności naszych obywateli gwarantowane zasadą zaufania obywateli do państwa, w tym kontekście — jego zdolności do skutecznej ochrony wartości zawartych w ust. 1 art. 5 tej ustawy.

Po czwarte Trybunał Konstytucyjny stwierdził, iż:

Treść normatywną, w tym wyznaczenie zakresu typologicznego przestępstw, określa także kompleksowe zestawienie wszystkich typów przestępstw w art. 5 ust. 1 pkt 2 lit. a–e ustawy o ABW oraz AW, tzn. opatrzenie ich kwalifikatorem „bezpieczeństwo państwa” oraz treścią ust. 1, w istocie dookreśla zbiór wszystkich, w tym innych przestępstw, a nie otwiera na zupełnie nowe, nieznanne oderwane od treści tego przepisu przestępstwa...

Powyższy wyrok z uwagi na treść art. 190 ust. 1 Konstytucji RP zamyka kwestię kontestowania treści normatywnych zawartych w art. 5 ust. 1 pkt 2 lit. a i c ustawy o ABW oraz AW z uwagi na ich niekonstytucyjność. Nie zamyka on oczywiście dyskusji przedstawicieli nauki i praktyków dotyczących zasadności i racjonalności obowiązujących regulacji.

Przechodząc do analizy treści art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, należy wskazać, że ustawodawca zgrupował przestępstwa pozostające we właściwości ABW w sześciu jednostkach redakcyjnych oznaczonych literowo od a do f. Analiza zawartości katalogu przestępstw wskazuje, iż kryterium kwalifikacyjnym stał się przedmiot ochrony (zamachu). W doktrynie prawa karnego za przedmiot ochrony (zamachu) uznaje się wszystkie dobra i wartości indywidualne i ogólnospołeczne, które podlegają ochronie przewidzianej przepisami karnymi zawartymi w ustawie Kodeks karny i ustawach szczególnych¹².

Odnosząc się zatem do poszczególnych elementów katalogu, należy zauważyć, iż art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW w lit. a omawianego przepisu grupuje i opisuje czyny przestępcze, które stanowią zagrożenie dla suwerenności Rzeczypospolitej Polskiej. Przedmiotem ochrony są więc: niepodległość, integralność terytorialna, porządek konstytucyjny, niezakłócone działanie organów konstytucyjnych, podstawy bezpieczeństwa i obronności, moc obronna oraz inne komponenty bezpieczeństwa państwa¹³. Przy czym, jak już wcześniej podno-

¹² M. Bożek, *Zwalczanie przestępczości...*

¹³ Zob. S. Hoc, *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2002, s. 44, 48. S. Zalewski, *Służby specjalne w państwie*

szono, ustawodawca, wskazując przestępstwa, których zwalczanie jest celem ABW, posługuje się zarówno sformułowaniami dookreślonymi (szpiegostwo, terroryzm, bezprawne ujawnienie lub wykorzystanie informacji niejawnych), jak i niedookreślonymi: „inne przestępstwa godzące w bezpieczeństwo państwa”. Przy czym, pomimo tego, iż ustawodawca nie zdecydował się na odesłanie wprost do innych aktów prawnych, to przestępstwa „szpiegostwa”, „terroryzmu” oraz „bezprawnego ujawnienia lub wykorzystania informacji niejawnych” są na tyle skonkretyzowane, że można je zdekodować na gruncie obowiązujących ustaw, tj. przede wszystkim Kodeksu karnego.

Odnosząc się zatem do poszczególnych kategorii przestępstw ujętych w art. 5 ust 1 pkt 2 lit. a ustawy o ABW oraz AW, należy wskazać, iż szpiegostwo na gruncie ustawy o ABW oraz AW jest tożsame z przestępstwem opisanym w art. 130 KK¹⁴. Jego formą podstawową jest branie udziału w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej. Formy kwalifikowane to: 1) organizowanie lub kierowanie działalnością obcego wywiadu, 2) branie udziału w obcym wywiadzie albo działanie na jego rzecz i udzielanie temu wywiadowi informacji, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej. Jeżeli wiadomości, których udzielił obcemu wywiadowi sprawca czynu z art. 130 § 2 KK, stanowią tajemnicę państwową, wówczas jego zachowanie należy kwalifikować kumulatywnie z uwzględnieniem art. 130 § 2 KK i art. 265 § 2 KK, a jeśli objęte były tajemnicą służbową — art. 130 § 2 KK i art. 266 § 1 lub 2 KK.

Formami uprzywilejowanymi przestępstwa szpiegostwa są zaś: 1) uzyskiwanie, gromadzenie lub przechowywanie wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej w celu udzielenia ich obcemu

demokratycznym, Akademia Obrony Narodowej — Wydział Wydawniczy, Warszawa 2005, s. 26; por. J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Książka i Wiedza, Warszawa 2007, s. 318; A. Krzak, *Kontrwywiad w: Polskie służby specjalne. Słownik*, red. K. Wojtaszczyk, Oficyna Wydawnicza ASPRA-JR, Warszawa 2011, s. 104; N. Polar, T.B. Allen, *Księga szpiegów. Encyklopedia*, Magnum, Warszawa 2000, s. 305. Zob. J. Widacki, *Dyskretny urok tajnych służb*, w: tenże, *Rozważania o prawie i sprawiedliwości*, Oficyna Wydawnicza AFM, Kraków 2007, s. 59. Tenże, *Przedmowa*, w: M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2006, s. 9. S. Zalewski, *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009, s. 23.

¹⁴ Art. 130 KK § 1: *Kto bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10.* § 2. *Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.* § 3. *Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, wchodzi do systemu informacyjnego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.* § 4. *Kto działalność obcego wywiadu organizuje lub nią kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności.*

wywiadowi, 2) zgłoszenie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej.

Stosownie do postanowień art. 138 § 2 KK komentowany przepis stosuje się odpowiednio do szpiegostwa na szkodę państwa sojuszniczego, zapewniającego wzajemność. Działalność szpiegowska obywatela polskiego podejmowana na rzecz wywiadu państwa obcego i na szkodę państwa niesojuszniczego, jakkolwiek budzić może poważne zastrzeżenia natury moralnej, nie stanowi przestępstwa na gruncie polskiego ustawodawstwa.

Przedmiot ochrony w wypadku szpiegostwa stanowi generalnie bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej, a w szczególności te wszystkie elementy składające się na bezpieczeństwo zewnętrzne, których przekazanie obcym organizacjom wywiadowczym może prowadzić do zagrożenia bezpieczeństwa państwa¹⁵.

Kolejnym przestępstwem ujętym w art. 5 ust 1 pkt 2 lit. a ustawy o ABW oraz AW jest terroryzm. Jednak odmiennie niż w wypadku szpiegostwa pojęcie to nie odnosi się do jednego artykułu KK. Warto zaznaczyć, iż KK nie posługuje się w ogóle nomenklaturą „terroryzm”, ale pojęciem „przestępstwo o charakterze terrorystycznym”. Definicja tego pojęcia została zawarta w art. 115 § 20 KK, zgodnie z którym przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób, 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu¹⁶. Do typowych form zamachów terrorystycznych zalicza się: piractwo powietrzne lub morskie, zamachy bombowe na budynki, samoloty, pociągi, autobusy, dworce lub inne urządzenia użyteczności publicznej, w których znajduje się większa liczba ludzi, zamachy wobec nieokreślonej grupy ludności cywilnej, porwanie osób w celu wymuszenia określonego zachowania władz publicznych.

Dokonując dekodowania przestępstw o charakterze terrorystycznym na podstawie zapisów Kodeksu karnego, mając na względzie typizację przestępstw w części szczególnej owego, należy wskazać, iż chodzi tu o następujące przestępstwa: Art. 118 (Eksterminacja), Art. 118a (Zamach przeciwko ludności), Art. 119 (Przemoc i groźba bezprawna), Art. 120 (Środki masowej zagłady), Art. 127 i 128 (Zamach stanu), Art. 134 (Zamach na życie Prezydenta), Art. 140 (Zamach terrorystyczny), Art. 148 (Zabójstwo), Art. 163 (Spowodowanie niebezpiecznych

¹⁵ P. Kardas, *Komentarz do art. 130 Kodeksu karnego*, LEX/el.

¹⁶ R. Aleksandrowicz, *Pojęcie czynu o charakterze terrorystycznym „de lege lata” i „de lege ferenda” (wybrane zagadnienia)*, „Problemy praworządności” 1988, nr 10. M. Filar, *Terroryzm — problemy definicyjne oraz regulacje prawne w polskim prawie karnym w świetle prawa międzynarodowego i porównawczego*, w: *Terroryzm. Materiały z sesji naukowej*, red. V. Kwiatkowska-Darul, Toruń 2002.

zdarzeń), Art. 164 (Bezpośrednie niebezpieczeństwo), Art. 165 (Inne niebezpieczeństwa), Art. 165a (Sfinansowanie przestępstwa o charakterze terrorystycznym), Art. 166 (Piractwo), Art. 167 (Niebezpieczne urządzenia lub substancje), Art. 170 (Rozbójnictwo morskie), Art. 173 (Katastrofa), Art. 174 (Niebezpieczeństwo katastrofy), Art. 252 (Wzięcie zakładnika), Art. 255a (Rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa), Art. 258 § 2 i § 4 (Zorganizowana grupa i związek przestępczy), Art. 259a (Przekroczenie granicy RP w celu popełnienia przestępstwa o charakterze terrorystycznym).

Kolejnym przestępstwem ujętym w art. 5 ust 1 pkt 2 lit. a ustawy o ABW oraz AW jest bezprawne ujawnienie lub wykorzystania informacji niejawnych, w szczególności przestępstwa przeciwko ochronie informacji. Aktem prawnym regulującym kwestie prawne związane z definicjami i zasadami klasyfikacji informacji niejawnych jest *ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*¹⁷. Jednakże bezprawne ujawnienie lub wykorzystanie informacji niejawnych, w szczególności przestępstwo przeciwko ochronie informacji, jest raczej powszechnie utożsamiane z przestępstwami opisanymi w rozdziale XXXIII KK, tj. przede wszystkim dotyczącymi ochrony informacji o klauzuli „ściśle tajne” i „tajne” — Art. 265 (Tajemnica państwowa), oraz poufne, zastrzeżone i stanowiące tajemnice zawodowe — Art. 266 (Tajemnica służbowa), Art. 267 (Nielegalne uzyskanie informacji), Art. 268a (Szkoda w bazach danych), Art. 269 (Sabotaż komputerowy), Art. 269a (Zakłócanie pracy w sieci), Art. 269b (Bezprawne wykorzystanie programów i danych). Dane, które w omawianym przypadku stanowią przedmiot ochrony, to te, których ujawnienie spowodowałoby poważną szkodę dla Rzeczypospolitej Polskiej (m.in. zagrożenie bezpieczeństwa kraju, zakłócenie funkcjonowania organów sprawiedliwości, niekorzystny wpływ na funkcjonowanie gospodarki narodowej czy utrudnianie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej).

Wreszcie art. 5 ust 1 pkt 2 lit a *in fine* odnosi się do innych przestępstw godzących w bezpieczeństwo państwa. Jak wcześniej wykazano, w nauce prawa i praktyce podkreślano kontrowersyjność tegoż sformułowania. Wydaje się jednak, że w sposób przekonywujący, korzystając z argumentacji TK, wykazano, iż sformułowanie „inne przestępstwa godzące w bezpieczeństwo państwa” pozwala ABW na elastyczne reagowanie na zagrożenia dla bytu i funkcjonowania państwa. Kompletnie zindywidualizowanie przestępstw w kontekście normy zawartej w art. 5 ustawy o ABW oraz AW prowadziłoby do pozostawienia poza regulacją stanów faktycznych i prawnych godzących w bezpieczeństwo państwa. Pomimo tego, że KK nie posługuje się taką terminologią *explicite*, to doktryna zalicza na ogół do kategorii innych przestępstw godzących w bezpieczeństwo państwa: przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne (rozdział XVI); przestępstwa przeciwko Rzeczypospolitej Polskiej (rozdział XVII); przestępstw przeciwko obronności (rozdział XVIII); czy przestępstwa przeciwko bezpieczeństwu powszechnemu (rozdział XX). Przy czym,

¹⁷ Dz.U. 2019, poz. 742.

ze względu na legislacyjny zabieg ustawodawcy, tj. posłużenie się pojęciem nieostrym nie jest to katalog zamknięty.

Przechodząc do omówienia art. 5 ust 1 pkt 2 lit. b, c i d ustawy o ABW oraz AW, należy wskazać, iż ochronie prawnokarnej podlega w nim przede wszystkim bezpieczeństwo ekonomiczne państwa. Nie ulega wątpliwości, że Agencja Bezpieczeństwa Wewnętrznego powinna eliminować zagrożenia dla państwa *sensu largo*, a więc również powinna eliminować sytuacje groźne dla gospodarki narodowej w postaci negatywnych czynników wewnętrznych czy też zewnętrznych. Literatura fachowa i nauka prawa¹⁸ definiują zagrożenia wewnętrzne jako niezgodne z prawem działania rodzimych i zagranicznych przedsiębiorców na rynku krajowym, zwłaszcza próby nielegalnego wzbogacenia się, defraudacje państwowych lub zagranicznych dotacji, spekulację, korupcję, pranie brudnych pieniędzy, przestępczość związaną z wykorzystaniem bankowości elektronicznej. Zalicza się do nich także nielegalne zmony cenowe (przetargowe).

Do zewnętrznych zagrożeń ekonomicznych zalicza się na ogół te zagrożenia, które wynikają z procesów zachodzących w gospodarce światowej, czyli globalizacji wzajemnych współzależności oraz nieprzewidywalności i chaotyczności rynku światowego¹⁹. Należą także do nich świadome działania obcych państw, ich służb specjalnych oraz powiązanych z nimi podmiotów gospodarczych, których celem jest wywieranie wpływu na sytuację gospodarczą danego kraju.

Art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW, jak wcześniej wskazywano, używa pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa”. Jest to sformułowanie pozakodeksowe, którego wykładnią zajęła się nauka prawa. Zdaniem P. Tulei użyte w tym przepisie określenie „podstawy państwa” oznacza zasady ustroju politycznego państwa, główne instytucje ustroju, zasady konstytucyjne, naczelną zasadę konstytucyjną²⁰. Określenie „ekonomiczne podstawy państwa” oznacza z kolei, że chodzi tu o zasady konstytucyjne odnoszące się do aspektów ekonomicznych, finansowych i gospodarczych ustroju państwowego (porządku konstytucyjnego). Termin „podstawy ekonomiczne państwa” można więc utożsamiać z podstawami (zasadami) ustroju gospodarczego państwa (art. 20 i n. Konstytucji RP)²¹.

¹⁸ Ł. Skoneczny, *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej*, PBW 2009, nr 1, s. 25–26; M. Smolak, *Formy zwalczania procederu prania brudnych pieniędzy*, PBW 2013, nr 9, s. 294–305; K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej — skimming*, PBW 2014, nr 10, s. 104–120; G. Borowik, *Zwalczanie zμών cenowych jako zagrożenia ekonomicznych interesów RP — próba oceny skuteczności unormowań prawnych*, PBW 2013, nr 9, s. 167–193.

¹⁹ E. Haliżak, *Ekonomiczne wymiary bezpieczeństwa narodowego i międzynarodowego*, w: *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. D.B. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997, s. 88.

²⁰ P. Tuleja, *Zasady konstytucyjne*, w: *Konstytucjonalizacja zasad i instytucji ustrojowych*, red. P. Sarnecki, Warszawa 1997, s. 25.

²¹ K. Walczuk, M. Bożek, *Konstytucyjne i ustawowe uwarunkowania organizacji i funkcjonowania ABW*, Siedlce 2015, s. 123–124; zob. także: M. Karpiuk, *Zasady ustroju*

Tym niemniej omawiany przepis w dalszym ciągu budzi wątpliwości interpretacyjne, wynikające z jego nieo określoności. Są one związane zarówno z samym jego brzmieniem, jak i ze środkami, jakie ABW może stosować na jego podstawie, realizując w praktyce ochronę ekonomicznych interesów państwa. Wątpliwości te podzielił również Trybunał Konstytucyjny (teza z dnia 15 listopada 2010 r. S 4/10). Zdaniem TK, który przedstawił Sejmowi Rzeczypospolitej Polskiej uwagi dotyczące stwierdzonych uchybień w przepisach ustawy o ABW oraz AW, przepis ten narusza standardy demokratycznego państwa prawnego wynikające z Konstytucji RP i orzecznictwa Trybunału Konstytucyjnego. Zdaniem TK wyrażenie „przestępstwa godzące w podstawy ekonomiczne państwa” uniemożliwia identyfikację typów przestępstw określonych przez ustawę karną. Niemożność identyfikacji typów przestępstw określonych przez ustawę karną, cechująca przepis art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW, powoduje w konsekwencji uchybienie innych powiązanych z nią przepisów ustawy o ABW oraz AW. Tym samym w swej tezie sygnalizacyjnej Trybunał wskazał, że zmiana brzmienia art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW jest niezbędna dla zapewnienia spójności systemu prawnego Rzeczypospolitej Polskiej. Co znamienne, Trybunał nie dokonał jednak oceny konstytucyjnej art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW. Odnosząc się do powyższej argumentacji nie sposób pominąć faktu, iż:

ustawowa regulacja całego art. 5 (...) jest kompleksowa, spójna, a także konstrukcyjnie, aksjologicznie i prakseologicznie racjonalna (...) Kompleksowość regulacji całego art. 5 ustawy o ABW oraz AW wynika z identyfikowania przez prawodawcę chronionych wartości oraz określenia przedmiotu działania ABW za pomocą zastosowania formuły wyznaczenia zadań tego organu policji bezpieczeństwa — właściwego w sprawach ochrony bezpieczeństwa wewnętrznego i porządku konstytucyjnego naszego państwa²².

W świetle powyższych argumentów trudno moim zdaniem zgodzić się z tezą sygnalizacyjną Trybunału Konstytucyjnego z dnia 15 listopada 2010 r. S 4/10.

Przechodząc do konkretnych kategorii przestępstw, jakie doktryna i piśmiennictwo wiążą z pojęciem „przestępstwa godzące w podstawy ekonomiczne państwa”, należy zaliczyć do nich przede wszystkim: przestępstwa z rozdziału XXXVI KK (pt. *Przestępstwa przeciwko obrotowi gospodarczemu*), ale także będą to niektóre przestępstwa z rozdziałów Kodeksu karnego: XXIX (*Przestępstwa przeciwko działalności instytucji państwowych oraz samorządu terytorialnego*), XXXV (*Przestępstwa przeciwko mieniu*), XXXVII (*Przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi*). Wskazać należy także na przestępstwa z ustawy z 10 września 1999 r. — Kodeks karny skarbowy

politycznego państwa w Rzeczypospolitej Polskiej w: M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012, s. 34–50.

²² Zob. wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11.

(tj. Dz.U. 2016, poz. 2137 ze zm.). Zgodnie z art. 53 § 11 KKS przestępstwo skarbowe skierowane przeciwko istotnym interesom finansowym państwa polskiego, o którym mowa w art. 3 § 3 KKS, jest to takie przestępstwo skarbowe, które zagraża Skarbowi Państwa powstaniem uszczerbku finansowego w wysokości co najmniej dziesięciokrotności wielkiej wartości. Wielka wartość jest to wartość, która w czasie popełnienia czynu zabronionego przekracza tysiącrotną wysokość minimalnego wynagrodzenia (art. 53 § 16 KKS).

Art. 5 ust. 1 pkt 2 lit. c ustawy o ABW oraz AW odnosi się do przestępstw korupcyjnych. Jeśli chodzi o definicję legalną korupcji, to została ona ujęta w art. 1 ust 3a ustawy o CBA²³. Jeśli chodzi o zakres podmiotowy tych przestępstw, to ABW zobowiązana jest do zwalczania korupcji tylko osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. 2017, poz. 1393; Dz.U. 2019, poz. 371 i 492). Dodatkową cezurą jest, by przestępstwa wymienionych osób godziły w bezpieczeństwo państwa. Co do wskazania konkretnych przestępstw mieszczących się w zakresie przedmiotowym działania ABW, to należy wskazać, że zdaniem doktryny i piśmiennictwa²⁴ należy do nich zaliczać przestępstwa ujęte w rozdziale XXIX KK (*Przestępstwa przeciwko działalności instytucji państwowych oraz samorządu terytorialnego*), w szczególności zaś przestępstwa stypizowane w art. 228 KK, 229 KK, 230 KK i 231 KK.

Art. 5 ust. 1 pkt 2 lit. d ustawy o ABW oraz AW wskazuje jako zadanie ABW zwalczanie przestępstw dotyczących produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa.

²³ *Korupcją, w rozumieniu ustawy, jest czyn: 1) polegający na obiecywaniu, proponowaniu lub wręczaniu przez jakąkolwiek osobę, bezpośrednio lub pośrednio, jakichkolwiek nienależnych korzyści osobie pełniącej funkcję publiczną dla niej samej lub dla jakiegokolwiek innej osoby, w zamian za działanie lub zaniechanie działania w wykonywaniu jej funkcji; 2) polegający na żądaniu lub przyjmowaniu przez osobę pełniącą funkcję publiczną bezpośrednio, lub pośrednio, jakichkolwiek nienależnych korzyści, dla niej samej lub dla jakiegokolwiek innej osoby, lub przyjmowaniu propozycji lub obietnicy takich korzyści, w zamian za działanie lub zaniechanie działania w wykonywaniu jej funkcji; 3) popełniany w toku działalności gospodarczej, obejmującej realizację zobowiązań względem władzy (instytucji) publicznej, polegający na obiecywaniu, proponowaniu lub wręczaniu, bezpośrednio lub pośrednio, osobie kierującej jednostką niezaliczaną do sektora finansów publicznych lub pracującej w jakimkolwiek charakterze na rzecz takiej jednostki, jakichkolwiek nienależnych korzyści, dla niej samej lub na rzecz jakiegokolwiek innej osoby, w zamian za działanie lub zaniechanie działania, które narusza jej obowiązki i stanowi społecznie szkodliwe odwzajemnienie; 4) popełniany w toku działalności gospodarczej obejmującej realizację zobowiązań względem władzy (instytucji) publicznej, polegający na żądaniu lub przyjmowaniu bezpośrednio lub pośrednio przez osobę kierującą jednostką niezaliczaną do sektora finansów publicznych lub pracującą w jakimkolwiek charakterze na rzecz takiej jednostki, jakichkolwiek nienależnych korzyści lub przyjmowaniu propozycji lub obietnicy takich korzyści dla niej samej lub dla jakiegokolwiek innej osoby, w zamian za działanie lub zaniechanie działania, które narusza jej obowiązki i stanowi społecznie szkodliwe odwzajemnienie.*

²⁴ M. Bożek, *Zwalczanie przestępstw...*

W odróżnieniu od poprzednich punktów są one dekodowane nie tylko na gruncie KK, tj. w art. 121 KK²⁵, ale także w art. 33 *ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa* (Dz.U. 2020, poz. 509)²⁶.

Art. 121 KK kryminalizuje wytwarzanie, gromadzenie, nabywanie, zbywanie, przechowywanie, przewożenie lub przesyłanie środków masowej zagłady lub środków walki bądź prowadzenie badań mających na celu wytwarzanie lub stosowanie takich środków. Pojęcie „środek masowej zagłady” obejmuje broń jądrową, biologiczną i chemiczną. Zakazane „środki walki” to np. wymienione w art. 8 ust. 2 lit. b pkt XIX Statutu MTK stosowanie pocisków, które z łatwością rozszerzają się lub spłaszczają w ciele człowieka, jak np. pociski z twardą łuską, która nie pokrywa w całości rdzenia lub jest ponacinana. Dobrem chronionym w art. 121 KK jest porządek prawny w zakresie ograniczeń w dostępie do zakazanych środków masowej zagłady lub środków walki. Przepisy te mają zapobiegać niebezpieczeństwu rozległych zamachów na życie i zdrowie człowieka. Ustawa o obrocie dotyczy: 1) produktów podwójnego zastosowania — produktów podwójnego zastosowania w rozumieniu art. 2 pkt 1 rozporządzenia nr 428/2009; 2) uzbrojenia — broni, amunicji, materiałów wybuchowych, wyrobów, ich części i technologii wskazanych w wykazie określonym w przepisach wydanych na podstawie art. 6a ust. 3; 3) towarów o znaczeniu strategicznym — towarów o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa, będących produktami podwójnego zastosowania lub uzbrojeniem.

Art. 33 *ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa*, kryminalizuje obrót wymienionymi kategoriami towarów bez zezwolenia lub

²⁵ Art. 121. § 1. *Kto, wbrew zakazom prawa międzynarodowego lub przepisom ustawy, wytwarza, gromadzi, nabywa, zbywa, przechowuje, przewozi lub przesyła środki masowej zagłady lub środki walki bądź prowadzi badania mające na celu wytwarzanie lub stosowanie takich środków, podlega karze pozbawienia wolności od roku do lat 10. § 2. Tej samej karze podlega, kto dopuszcza do popełnienia czynu określonego w § 1.*

²⁶ Art. 33. 1. *Kto dokonuje obrotu bez zezwolenia lub, chociażby nieumyślnie, wbrew warunkom określonym w zezwoleniu, podlega karze pozbawienia wolności od roku do lat 10. 2. Jeżeli sprawca, dokonujący obrotu wbrew warunkom określonym w zezwoleniu, działa nieumyślnie i przywrócił stan, o którym mowa w art. 31 ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2a. Kto zamieszcza nieprawdziwe lub niepełne informacje we wniosku o wydanie zezwolenia na obrót podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 3. Karze określonej w ust. 1 podlega, kto dopuszcza do popełnienia czynu określonego w ust. 1 lub 2. 4. W razie skazania za przestępstwo określone w ust. 1, 2 lub 3 sąd może orzec przepadek towarów o znaczeniu strategicznym lub innych przedmiotów służących lub przeznaczonych do popełnienia albo pochodzących bezpośrednio lub pośrednio z przestępstwa, w tym środków płatniczych i papierów wartościowych, chociażby nie stanowiły one własności sprawcy.*

choćby nieumyślnie, wbrew warunkom określonym w zezwoleniu. Kryminalizowane jest również zamieszczanie nieprawdziwych lub niepełnych informacji we wniosku o wydanie zezwolenia na obrót.

Art. 5 ust. 1 pkt 2 lit. e ustawy o ABW oraz AW wskazuje jako zadanie ABW zwalczanie przestępstw nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym. Są one dekodowane na gruncie KK, *ustawy z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym* (tj. Dz.U. 2017, poz. 290 ze zm.) oraz *ustawy z 29 lipca 2005 r. o przeciwdziałaniu narkomanii* (tj. Dz.U. 2017, poz. 783 ze zm.).

Na gruncie przepisów KK przyjmuje się, że są to przestępstwa ujęte w art. 263 § 1–2 KK (wytwarzanie, obrót i posiadanie broni palnej i amunicji). Typy przestępstw określone w art. 263 KK łączą dobro chronione, którym jest porządek publiczny zagrożony naruszeniem zasad wytwarzania i obrotu bronią palną lub amunicją, a także posiadanie broni palnej lub amunicji przez osoby do tego nieuprawnione. W sytuacji braku definicji legalnej tych pojęć w KK należy odwołać się do regulacji zawartych w treści BrońU.

Również ze względu na brak w KK definicji legalnej pojęć „środki odurzające” i „substancje psychotropowe” należy odwołać się do regulacji zawartych w treści NarkU, tj. do art. 4 NarkU, zawierającego definicje pojęć: „wytwarzanie”, „przewóz”, „środki odurzające”, i „substancje psychotropowe”. Celem NarkU jest zapobieganie i przeciwdziałanie zjawisku narkomanii przez ustalenie sfery prohibicji w zakresie produkcji i obrotu środkami odurzającym. Pomimo rozbieżności w rozumieniu przedmiotu ochrony należy przychylić się do stanowiska, iż jest nim zdrowie publiczne (społeczeństwa jako całości) chronione przed niekontrolowaną produkcją i rozpowszechnianiem środków odurzających. Na gruncie przepisów NarkU przyjmuje się, że w zakresie kompetencyjnym ABW pozostają przestępstwa ujęte w art. 53 (wytwarzanie środków odurzających etc.), art. 54 (wyrabianie przyrządów służących produkcji środków odurzających etc.), art. 55 (przewóz i wywóz środków odurzających) art. 56 (Wprowadzenie do obrotu i uczestniczenie w obrocie) NarkU. Z zastrzeżeniem, że muszą dotyczyć obrotu międzynarodowego.

Art. 5 ust. 1 pkt 2 lit. f ustawy o ABW oraz AW wskazuje jako zadanie ABW zwalczanie przestępstw przeciwko wymiarowi sprawiedliwości. Przy czym lit. f jest jedyną jednostką redakcyjną art. 5 ust 1 pkt 2 ustawy o ABW oraz AW, w której ustawodawca *explicite* odnosi się do konkretnych jednostek redakcyjnych KK. Wskazuje mianowicie precyzyjnie, iż chodzi o: art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 KK. Przy czym dodatkowym kwalifikatorem jest tu związek z przestępstwami, o których mowa w lit. a–e. Przedmiotem ochrony jest w omawianym przypadku niewątpliwie prawidłowe funkcjonowanie państwa w aspekcie konstytucyjnej władzy sądowniczej i walki z bezprawnymi zamachami na nią kierowanymi. W zakres przestępstw przeciwko

wymiarowi sprawiedliwości, do zwalczania których ustawodawca zobowiązał ABW, wchodzą zatem: wywieranie groźbą bezprawną lub przemocą wpływu na czynności sądu (art. 232, KK), fałszywe zeznania (art. 233 KK), fałszywe oskarżenie (art. 234 KK), tworzenie fałszywych dowodów dla podjęcia ścigania o przestępstwo, w tym przestępstwo skarbowe, wykroczenie, przewinienie dyscyplinarne (art. 235 KK), zatajenie dowodów niewinności osoby podejrzanej (art. 236 § 1 KK), poplecznictwo — udaremnianie lub utrudnianie postępowania karnego (art. 239 § 1 KK). Przy czym muszą one pozostawać w związku z przestępstwami, o których mowa w lit. a–e art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW.

Ustawodawca, postawiwszy przed ABW konkretne zadania, wyposażył również Agencję w instrumenty, dzięki którym może zakładane zadania i cele zrealizować. Należy zauważyć, że ustawa o ABW oraz AW ma charakter kompleksowy. Ustawodawca najpierw w art. 5 ustawy o ABW oraz AW komponuje według reguł aksjologicznych zestaw wartości oraz określa przedmiot działania ABW za pomocą zastosowania formuły wyznaczenia zadań tego organu bezpieczeństwa państwa, a następnie w art. 21 ustawy o ABW oraz AW wskazuje instrumentarium umożliwiające ich realizację. Zgodnie z brzmieniem art. 21 ustawy o ABW oraz AW w granicach zadań, o których mowa w art. 5 ust. 1, funkcjonariusze ABW wykonują czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców.

Pojęcie „czynności operacyjno-rozpoznawcze” nie zostało dotychczas zdefiniowane. Nie ma także powszechnie akceptowanej w doktrynie definicji tych czynności. We wcześniejszej literaturze pod pojęciem „czynności operacyjno-rozpoznawcze” rozumiano taktyczno-rozpoznawcze czynności nieprocesowe, które praktyka służby śledczej ukształtowała jako czynności uzupełniające lub wykonawcze w stosunku do czynności procesowych i zadań postępowania przygotowawczego. Kwestia ta była przedmiotem dyskusji teoretyków prawa²⁷ począwszy od lat 50. XX w. Wśród głosów znaczących w dyskusji trzeba wymienić L. Schaffa, J. Krwawicza, J. Widackiego oraz przede wszystkim A. Tarachę.

Uwzględniając dorobek i poglądy wymienionych wyżej autorów, przez „czynności operacyjno-rozpoznawcze” należy generalnie rozumieć wyraźnie określone w ustawie niejawne działania wyspecjalizowanych służb i organów państwowych, których celem jest: wykrywanie negatywnych zjawisk godzących w porządek publiczny i bezpieczeństwo publiczne, identyfikacja grup i środowisk przestępczych, ustalanie źródeł dowodowych, zabezpieczanie środków dowodowych i przeprowadzanie dowodów podlegających wykorzystaniu w procesie

²⁷ L. Schaff, *O niektórych problemach dotyczących zakresu postępowania przygotowawczego*, NP 1957, nr 12. Nieco odmienne spojrzenie na tę kwestię prezentują: J. Krwawicz (M. Lipka, J. Krwawicz, *O rozpracowaniach operacyjnych*, Warszawa 1963, s. 3–4), J. Widacki (*Kryminalistyka*, red. J. Widacki, Warszawa 1999, s. 110 i n.) oraz A. Taracha (A. Taracha, *Czynności operacyjno-rozpoznawcze...*, s. 25).

karnym, pozyskiwanie podmiotów współpracujących z organami ścigania oraz ujawnianie okoliczności sprzyjających popełnianiu czynów nieakceptowanych społecznie.

Kompetencje do prowadzenia czynności operacyjno-rozpoznawczych przewidziano w przepisach aż ośmiu ustaw regulujących zadania 10 służb, tj. Policji²⁸, CBA²⁹, SG³⁰, ABW, AW, SWW³¹, SKW³², KAS³³, ŻW³⁴, SOP³⁵. Obecnie w Polsce uprawnionych do ich stosowania jest 10 formacji. Pięć z nich to służby określone ustawowo jako specjalne, następne to: Policja, Straż Graniczna, Żandarmeria Wojskowa, Służba Celną oraz Krajowa Administracja Skarbowa, Służba Ochrony Państwa.

W praktyce każda ze służb posiadających uprawnienia do ich wykonywania reguluje istotę tych czynności w swoich przepisach wewnętrznych o charakterze niejawnym. Tylko niektóre najbardziej złożone czynności operacyjno-rozpoznawcze są określone ustawowo zarówno co do ich celów, podstaw prawnych i faktycznych, jak i sposobu prowadzenia (kontrola operacyjna, zakup kontrolowany, kontrolowane przyjęcie lub wręczenie korzyści majątkowej, zbieranie i przetwarzanie danych telekomunikacyjnych, współpraca z osobowymi źródłami informacji)³⁶. Jednakże w literaturze fachowej zwraca się uwagę na niejednorodność przepisów w poszczególnych ustawach kompetencyjnych. Każdy z aktów prawnych posługuje się inną metodyką oraz katalogiem przestępstw, w przypadku których dopuszcza się prowadzenie poszczególnych czynności, co powoduje praktyczne trudności związane z dopuszczalnością wykorzystania tak

²⁸ Ustawa o Policji z dnia 6 kwietnia 1990 r. (Dz.U. 2020, poz. 360), art. 14 ust. 1, art. 19, 19 a, 19 b, 20, 20 a–e, 20 b, 20 c, 20 d, 21, 21 a–n, 22.

²⁹ Ustawa o Centralnym Biurze Antykorupcyjnym z dnia 9 czerwca 2006 r. (Dz.U. 2019, poz. 1921), art. 13 ust 1.

³⁰ Ustawa o Straży Granicznej z dnia 12 października 1990 r., tj. z dnia 28 stycznia 2020 r. (Dz.U. 2020, poz. 305), art. 1 ust 4.

³¹ Ustawa o służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego z dnia 9 czerwca 2006 r. (Dz.U. 2019, poz. 687), art. 26.

³² Ustawa o służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego z dnia 9 czerwca 2006 r. (Dz.U. 2019, poz. 687), art. 25.

³³ Ustawa o Krajowej Administracji Skarbowej z dnia 16 listopada 2016 r., tj. z dnia 1 marca 2021 r. (Dz.U. 2021, poz. 422), art. 2 ust. 1.

³⁴ Ustawa o Żandarmerii Wojskowej i Wojskowych Organach Porządkowych z dnia 24 sierpnia 2001 r. (Dz.U. 2020, poz. 431), art. 3 ust. 1.

³⁵ Ustawa o służbie Ochrony Państwa z dnia 8 grudnia 2017 r. (Dz.U. 2021, poz. 575), art. 3 ust. 1.

³⁶ S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, Lex/el. 2012, teza 2 do art. 13; zob. także A. Dermont, B.K. Rowiński, *Czynności operacyjno-rozpoznawcze w świetle ustawy z 14 lipca 1983*, „Problemy Kryminalistyki” 1985, nr 169; T. Hanausek, *Kryminalistyka a praca operacyjna*, „Problemy Kryminalistyki” 1982, nr 183; S. Koebecke, *Przyczynek do rozważań o teorii pracy operacyjnej*, „Problemy Kryminalistyki” 1981, nr 150; A. Taracha, *Czynności operacyjno-rozpoznawcze a ochrona praw jednostki*, „Problemy Praworządności” 1988, nr 8–9; T. Grzegorzcyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2011, s. 653.

pozyskanych materiałów w postępowaniu karnym. Kwestia ta stała się kanwą do ożywionej dyskusji doktrynalnej, co skutkuje bogatą literaturą fachową³⁷.

Ustawa o ABW oraz AW przewiduje, że w sprawach o przestępstwa, o których mowa w art. 5 ust. 1 pkt 2 rzeczony ustawy, w ramach czynności operacyjno-rozpoznawczych mogą być dokonywane czynności ujęte w rozdziale 4 ustawy o ABW oraz AW (pt. *Uprawnienia funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), a konkretniej opisane w art. 27–34 i 36 ustawy o ABW oraz AW. Generalnie jest to bardzo szeroki zestaw narzędzi umożliwiający, jak się wydaje, realizację w pełni zadań ABW zawartych w art. 5 ust. 1 ustawy o ABW oraz AW. Do środków operacyjno-rozpoznawczych, jakimi ABW/funkcjonariusze ABW mogą się posługiwać, należą: zarządzenie kontroli operacyjnej; uzyskiwanie danych niestanowiących treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną; zakup kontrolowany; niejawne nadzоровanie wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa; kontrola korespondencji; żądanie przedstawienia informacji o systemach informatycznych; blokada dostępności w systemie teleinformatycznym określonych danych informatycznych, mających związek ze zdarzeniem o charakterze terrorystycznym, lub określonych usług teleinformatycznych, służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym; uzyskiwanie i przetwarzanie informacji niejawnych; korzystanie z przetwarzanych przez banki informacji stanowiących tajemnicę bankową oraz informacji dotyczących umów o: rachunek papierów wartościowych, rachunek pieniężny, ubezpieczenia lub innych dotyczących obrotu instrumentami finansowymi, świadczenia usług płatniczych lub zawieranych z uczestnikami funduszy inwestycyjnych, a w szczególności z przetwarzanych przez uprawnione podmioty danych osób, które zawarły takie umowy, korzystać z pomocy osób niebędących funkcjonariuszami Agencji.

Pod pojęciem „czynności dochodzeniowo-śledcze” należy rozumieć czynności podejmowane w ramach dochodzenia (art. 325a i n. KPK) i śledztwa (art. 309 i n. KPK). Chodzi tutaj o czynności procesowe w postępowaniu karnym. Pod pojęciem „czynności procesowe w postępowaniu karnym” należy rozumieć określone przez prawo karne procesowe zachowanie się uczestnika postępowania, wywołujące przewidziane przez to prawo skutki prawne³⁸.

Stosowanie tych uprawnień jest najbardziej widocznym rezultatem działalności ABW. Obecnie spośród polskich służb specjalnych jedynie Agencja

³⁷ A. Taracha, *Czynności...*, s. 155–218; K.T. Boratyńska, *Wokół problematyki związanej z wykorzystaniem dowodowych materiałów operacyjnych*, w: *Praktyczne elementy przestępczości zorganizowanej i terroryzmu*, red. L. Paprzycki, Z. Rau, Oficyna a Wolters Kluwer business, Warszawa 2009, s. 145–153. E. Gruza, *Czynności operacyjno-rozpoznawcze w: Kryminalistyka — czyli rzecz o metodach śledczych*, red. E. Gruza, M. Goc, J. Moszczyński, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008, s. 61–62.

³⁸ T. Grzegorzczak, J. Tylman, *Polskie postępowanie karne*, s. 399.

Bezpieczeństwa Wewnętrznego oraz Centralne Biuro Antykorupcyjne³⁹ w ramach swoich ustawowych kompetencji mają uprawnienia śledcze. Tym samym CBA, podobnie jak ABW, realizuje swoje zadania zarówno w wymiarze operacyjno-rozpoznawczym jak i dochodzeniowo-śledczym. Przy czym zadania CBA zostały skonstruowane w sposób diametralnie odmienny od zadań ABW⁴⁰. Przyjęty model wynika zapewne z innych zasad programowych konstytuujących ABW i CBA. O ile ABW jest dedykowaną w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, to CBA jest służbą specjalną do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, właściwą także do zwalczania działalności godzącej w interesy ekonomiczne państwa. Zakres działania ABW jest nieporównywalnie szerszy i wymusza tym samym większą elastyczność, dynamizm oraz konieczność reakcji na pojawiające się zagrożenia dla bytu i funkcjonowania państwa.

Realizacja czynności dochodzeniowo-śledczych budzi kontrowersje od samego początku ich wypełniania przez UOP/ABW. Krytycy przyjętych rozwiązań wskazują, iż są to uprawnienia bardziej charakterystyczne dla służb policyjnych niż specjalnych. W związku z tym pojawiły się postulaty przyznania

³⁹ Ustawa o CBA, art. 13 ust. 1.

⁴⁰ Art. 2 ust 1 pkt 1 Ustawy o CBA: do zadań CBA, w zakresie właściwości określonej w art. 1 ust. 1, należy: 1) rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko: a) działalności instytucji państwowych oraz samorządu terytorialnego, określonych w art. 228–231 *ustawy z dnia 6 czerwca 1997 r. — Kodeks karny*, a także o którym mowa w art. 14 *ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne* (Dz.U. 2017, poz. 1393; 2019, poz. 371, 492), b) wymiarowi sprawiedliwości, określonych w art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1, wyborom i referendum, określonych w art. 250a, porządkowi publicznemu, określonych w art. 258, wiarygodności dokumentów, określonych w art. 270–273 i art. 277 a § 1, mieniu, określonych w art. 286, obrotowi gospodarczemu, określonych w art. 296–297, art. 299 i art. 305, obrotowi pieniędzmi i papierami wartościowymi, określonych w art. 310 *ustawy z dnia 6 czerwca 1997 r. — Kodeks karny*, a także o których mowa w art. 586–592 *ustawy z dnia 15 września 2000 r. — Kodeks spółek handlowych* (Dz.U. 2019, poz. 505, 1543 i 1655) oraz określonych w art. 179–183 *ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi* (Dz.U. 2018, poz. 2286, 2243, 2244; 2019, poz. 730, 875, 1655), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa, c) finansowaniu partii politycznych, określonych w art. 49 d i 49 f *ustawy z dnia 27 czerwca 1997 r. o partiach politycznych* (Dz.U. 2018, poz. 580), jeżeli pozostają w związku z korupcją, d) obowiązkom podatkowym i rozliczeniom z tytułu dotacji i subwencji, określonych w rozdziale 6 *ustawy z dnia 10 września 1999 r. — Kodeks karny skarbowy* (Dz.U. 2018, poz. 1958 z późn. zm.), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa, e) zasadom rywalizacji sportowej, określonych w art. 46–48 *ustawy z dnia 25 czerwca 2010 r. o sporcie* (Dz.U. 2019, poz. 1468 i 1495), f) obrotowi lekami, środkami spożywcymi specjalnego przeznaczenia żywieniowego, wyrobami medycznymi określonymi w art. 54 *ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych* (Dz.U. 2019, poz. 784, 999, 1096 i 1590) — oraz ściganie ich sprawców.

służbom specjalnym jedynie tradycyjnej roli służb wywiadowczych i kontrwywiadowczych, która polega na identyfikowaniu i monitorowaniu zagrożeń dla bezpieczeństwa państwa⁴¹. Spełnianie takiej funkcji, określanej niekiedy jako funkcja informacyjna, nie wymaga stosowania czynności dochodzeniowo-śledczych. Służby dla zdobycia informacji stosują wyłącznie metody operacyjne i analityczne. W razie stwierdzenia przestępstwa nie prowadzą postępowania przygotowawczego, tylko przekazują materiały do prokuratury lub policji.

Nie podzielając powyższego poglądu, należy wskazać na niefunkcjonalność i niepraktyczność proponowanego modelu. Wydaje się, że zdecydowanie skuteczniejsza jest służba, które realizuje powierzone jej zadania zgodnie ze starorzymską zasadą *ab ovo usque ad mala*. W wypadku ABW dzieje się tak z uwagi na wyposażenie jej w zakresie art. 5 ust. 1 ustawy o ABW oraz AW w kwartet uprawnień dotyczących rozpoznawania, zapobiegania, wykrywania i ścigania przestępstw. W ten sposób ABW posiada instrumenty, dzięki którym może eliminować realne i potencjalne zagrożenia dla bezpieczeństwa państwa, co stanowi istotę bytu i działalność służb specjalnych.

Hipotetyczne zagrożenia związane z ewentualnym zagrożeniem dla praw i swobód obywatelskich, wynikające z połączenia w ABW funkcji operacyjno-rozpoznawczych i dochodzeniowo-śledczych, mogą w łatwy sposób zostać wyeliminowane przez stworzenie odpowiednich gwarancji normatywnych co do trybu stosowania czynności (co już występuje w ustawie o ABW oraz AW i aktach wykonawczych i, jak się wydaje, sprawdza się w praktyce).

Czynności dochodzeniowo-śledcze podejmowane przez funkcjonariuszy ABW i CBA stanowią realizację uprawnień procesowych przysługujących im na podstawie odpowiednio: art. 21 ust. 3 ustawy o ABW oraz AW i art. 13 ust. 3 ustawy o CBA, a także w wypadku obu służb — art. 312 KPK.

Kwestia organów uprawnionych do prowadzenia postępowania karnego (śledztwa i dochodzenia) została uregulowana w art. 311 KPK. Przepis ten normuje zasady prowadzenia śledztwa, uznając że organem je prowadzącym jest prokurator. Jednocześnie jednak prokurator został upoważniony do powierzenia policji śledztwa w całości, w części lub tylko w celu wykonania poszczególnych czynności. Prokurator może zastrzec do osobistego wykonania jakąkolwiek czynność śledztwa. Zakres powierzanego policji śledztwa ulega ograniczeniom w wypadkach określonych w art. 309 pkt 2 i 3 KPK, gdyż wówczas możliwe jest już tylko zlecenie dokonania poszczególnych czynności. Niezależnie od zakresu powierzonych policji czynności, w każdym śledztwie prokurator może zastrzec, że pewne czynności wykona osobiście.

⁴¹ T. Hanausek, *Kryminalistyka...*, s. 86. Obszerniej na temat rozważań definicyjnych nad pojęciem przeszukania zob. Z. Uniszewski, *Przeszukanie. Problematyka kryminalistyczna*, Wydawnictwo Neriton, Warszawa 2000, s. 41–46, 98, 99. P. Sarnecki, *Artykuł 50*, w: L. Garlicki, *Konstytucja Rzeczypospolitej Polskiej. Komentarz III*, Wydawnictwo Sejmowe, Warszawa 2003, s. 3.

Z kolei zapis art. 312 KPK nadaje uprawnienia policji, wynikające z przepisów Kodeksu postępowania karnego, organom Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Centralnego Biura Antykorupcyjnego oraz Żandarmerii Wojskowej. Uprawnienia procesowe tych organów obejmują wyłącznie ściganie przestępstw określonych w dotyczących ich ustawach kompetencyjnych. Wyjątkowo jedynie, w sytuacji tożsamości podmiotowej dotyczącej osoby sprawcy, możliwe jest łączne prowadzenie przez dany organ postępowania także o przestępstwa niewymienione w takiej ustawie. Uprawnienia takie przysługują również innym organom na podstawie przepisów szczególnych. Wykonywanie czynności procesowych przez organ do tego nieuprawniony może spowodować uznanie ich za bezskuteczne.

Agencja Bezpieczeństwa Wewnętrznego jest uprawniona także do prowadzenia dochodzenia. Zgodnie bowiem z art. 325a § 1 KPK dochodzenie prowadzi policja lub organy, o których mowa w art. 312 KPK, czyli także ABW, chyba że prowadzi je prokurator. Przepisy dotyczące śledztwa stosuje się odpowiednio do dochodzenia, jeżeli przepisy rozdziału 36a KPK, poświęconego dochodzeniu, nie stanowią inaczej. Przepisy rozdziału 36a KPK nie regulują w pełni instytucji dochodzenia. Zastosowanie więc mają odpowiednie przepisy dotyczące śledztwa. W szczególności dotyczy to art. 312, 314, 315–318 KPK.

W związku z powyższym do czynności procesowych, wykonywanych przez funkcjonariuszy ABW na podstawie art. 312 KPK, w związku z art. 311 KPK, zalicza się przede wszystkim: przesłuchiwanie podejrzanych i świadków (art. 177 KPK), konfrontowanie osób przesłuchiwanych (art. 172 KPK), dokonywanie okazania osób (art. 173 KPK), wzywanie i przesłuchiwanie podejrzanych i świadków (art. 177 KPK), oględziny miejsca, osób i rzeczy (art. 207 KPK), przeprowadzenie eksperymentu, doświadczenia lub odtworzenia przebiegu zdarzeń (art. 211 KPK), przeszukiwanie osób, pomieszczeń i zatrzymywanie rzeczy — po uzyskaniu postanowienia sądu lub prokuratora albo bez takiego postanowienia w przypadkach niecierpiących zwłoki (art. 217 KPK), zatrzymywanie osób podejrzanych (art. 244 KPK), prawo do przeprowadzenia czynności sprawdzających informacje zawarte w zawiadomieniu o przestępstwie (art. 307 KPK), prawo podejmowania w każdej sprawie czynności niecierpiących zwłoki dla zabezpieczenia śladów i dowodów przestępstwa (art. 308 KPK). Agencja Bezpieczeństwa Wewnętrznego wykonuje również czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie postępowania karnego, Kodeksie karnym wykonawczym, ustawie o ABW oraz AW (art. 21 ust. 2). Przykładem mogą być uregulowania art. 311 KPK. Zgodnie z tym przepisem śledztwo prowadzi prokurator, który może powierzyć policji przeprowadzenie śledztwa w całości lub w określonym zakresie albo dokonanie poszczególnych czynności śledztwa. W wypadkach określonych w art. 309 pkt 2 i 3 KPK można powierzyć policji jedynie dokonanie poszczególnych czynności śledztwa (art. 311 § 1–2 KPK). Wskazane powierzenie nie może obejmować czynności związanych z przedstawieniem zarzutów, zmianą lub uzupełnieniem postanowienia o przedstawieniu zarzutów oraz zamknięciem śledztwa (art. 311 § 3 KPK). W sytuacji opisanej

w art. 311 § 2 KPK policja może dokonać innych jeszcze czynności, jeżeli wyłoni się taka potrzeba (art. 311 § 4 KPK). Postanowienia art. 311 KPK mają odpowiednie zastosowanie do ABW (art. 312 KPK).

Kwestię wykonywania przez funkcjonariuszy ABW czynności dochodzeniowo-śledczych służących realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW, reguluje art. 23 ustawy o ABW oraz AW.

Na jego podstawie funkcjonariusze ABW, mają prawo:

- 1) wydawania osobom poleceń określonego zachowania się w granicach niezbędnych do wykonania czynności określonych w pkt 2–5a lub wykonywania innych czynności służbowych podejmowanych w zakresie i w celu realizacji ustawowych zadań ABW lub w celu uniknięcia bezpośredniego zagrożenia bezpieczeństwa osób lub mienia, gdy jest to niezbędne do sprawnego i zgodnego z prawem wykonywania tych czynności albo uniknięcia zatarcia śladów przestępstwa;
- 2) legitymowania osób w celu ustalenia ich tożsamości;
- 3) zatrzymywania osób w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego;

Przy czym osobie zatrzymanej, lub wobec której dokonano przeszukania, przysługują uprawnienia odpowiednio osoby zatrzymanej lub osoby, której prawa zostały naruszone, przewidziane w przepisach Kodeksu postępowania karnego. Zatrzymanie osoby może być zastosowane tylko wówczas, gdy inne środki okazały się bezcelowe lub nieskuteczne. Osoba zatrzymana może być okazywana, fotografowana lub daktyloskopowana tylko wtedy, gdy jej tożsamości nie można ustalić w inny sposób. Osobę zatrzymaną należy niezwłocznie poddać, w razie uzasadnionej potrzeby, badaniu lekarskiemu lub udzielić jej pierwszej pomocy medycznej. Czynności wobec osoby zatrzymanej powinny być wykonywane w sposób możliwie najmniej naruszający dobra osobiste osoby, wobec której zostały podjęte. Na sposób przeprowadzenia czynności wobec osoby zatrzymanej przysługuje zażalenie do prokuratora właściwego ze względu na miejsce przeprowadzenia czynności w terminie siedmiu dni od dnia dokonania czynności. Do zażalenia stosuje się przepisy Kodeksu postępowania karnego w zakresie dotyczącym postępowania odwoławczego.

- 4) przeszukiwania osób i pomieszczeń w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego;
- 5) dokonywania kontroli osobistej, a także przeglądania zawartości bagaży i sprawdzania ładunków w portach i na dworcach lub innych miejscach odprawy podróżnych, lub bagaży oraz w środkach transportu lądowego, powietrznego i wodnego, w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary lub w związku z realizacją zadań określonych w art. 5 ust. 1 pkt 1–2b i 5 ustawy o ABW oraz AW;
- 5a) dokonywania sprawdzenia prewencyjnego na zasadach i w sposób określony w art. 43a ustawy o ABW oraz AW;

- 6) obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych podejmowanych na podstawie ustawy;
- 7) żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielenia nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa;
- 8) zwracania się o niezbędną pomoc do innych, niż wymienieni w pkt 7, przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa.

Podsumowanie

Niniejszy rozdział jest próbą, z uwagi na ogromny zakres przedmiotowy podjętej tematyki, syntetycznego przedstawienia aspektów prawnych realizacji przez ABW zadań w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw ujętych w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW środków służących ich realizacji.

ABW posiada najszerszy w ujęciu przedmiotowym zakres zadań i uprawnień spośród polskich służb specjalnych. Także jako jedyna, oprócz CBA, posiada uprawnienia dochodzeniowo-śledcze. Co, jak wspomniano, niejednokrotnie bywa kwestionowane⁴² i podważane. Konstrukcja obecnych przepisów regulujących zadania ABW/UOP była przedmiotem krytyki niemal od daty wejścia w życie ustawy o UOP, tj. od 1990 r. Głównym i powtarzającym się zarzutem jest używanie w art. 5 ustawy o ABW oraz AW wyrażeń nieostrych, co może skutkować zamachem na standardy demokratycznego państwa prawa⁴³. Tymczasem ponad 30-letnie doświadczenie funkcjonowania omawianych przepisów nie znajduje potwierdzenia dla takich tez. Mimo to krytycy obecnie obowiązujących regulacji⁴⁴ postulują zmianę art. 5 ust 1 pkt 2 ustawy o ABW oraz AW przez ograniczenie do absolutnego minimum stosowania terminów nieostrych oraz wprowadzenie odesłania do konkretnych przepisów (Kodeksu karnego i innych ustaw), w których ustawodawca opisuje dane typy czynów zabronionych (przestępstw i przestępstw skarbowych). Postulowane zmiany mają być remedium na możliwość niewłaściwej interpretacji przepisów kompetencyjnych ABW⁴⁵. Za wzór rozwiązań w tym zakresie, spełniających przede wszystkim

⁴² B. Sprengel, *Ustrój organów administracji bezpieczeństwa i porządku publicznego*, Włocławek 2004.

⁴³ Wniosek Rzecznika Praw Obywatelskich z 4 grudnia 2015 r. (sygn. akt K 41/15).

⁴⁴ M. Bożek, *Zwalczanie przestępczości...*

⁴⁵ Tamże.

kryterium powiązania czynności rozpoznawania, zapobiegania i wykrywania przestępstw z penalizacją czynów w przepisach karnych, są przywoływane odpowiednio ustawa o CBA, ustawa o SKW oraz SWW. W obu tych aktach zadanie rozpoznawania, zapobiegania i wykrywania przestępstw zostało określone przez przywołanie nazewnictwa i numeracji poszczególnych jednostek redakcyjnych przepisów Kodeksu karnego i Kodeksu karnego skarbowego oraz ustaw szczególnych zawierających przepisy karne. Teoretycznie nie sposób nie podzielić akceptacji dla takiej formy regulacji, jednak w praktyce nie można się z nią zgodzić. Długoletnie doświadczenia praktyczne w zakresie funkcjonowania obecnych przepisów nie dostarczają dowodów na nadużywanie obecnie obowiązujących rozwiązań. Konstrukcja zadań ABW zawarta w art. 5 ustawy o ABW oraz AW, pomimo że odmienna obecnie od konstrukcji zadań innych partnerskich służb specjalnych, spełnia swoją rolę, pozwalając na elastyczne reagowanie i podejmowanie działań przez Agencję w każdym wypadku zagrożenia dla bezpieczeństwa państwa. Dodatkowo wydaje się, że wobec doprecyzowania zakresów przedmiotowych CBA, SKW, SWW oraz innych zadań kompetencyjnych AW oraz policji pada argument o tym, że nowe ujęcie art. 5 ustawy o ABW oraz AW wpłynie na wyeliminowanie sporów kompetencyjnych między służbami, gdyż już obecnie kompetencje wydają się odpowiednio wyodrębnione, a spory kompetencyjne praktycznie nie istnieją. Zadania nałożone na Agencję Bezpieczeństwa Wewnętrznego wykazują istotne odmienności od celów powołania pozostałych służb i formacji policyjnych. Specyfika tych zadań oraz waga interesów, których zabezpieczeniu mają one służyć, wymusza stworzenie adekwatnego otoczenia normatywnego wraz z odpowiednim instrumentarium pozwalającym na sprawne wykonywanie zadań określonych przez ustawodawcę.

Konkluzją niniejszej pracy jest zatem brzmiący być może prowokacyjnie wobec dorobku doktryny i piśmiennictwa, ale podyktowany dotychczasową dobrą praktyką funkcjonowania art. 5 ust 1 pkt 2 ustawy o ABW oraz AW, wniosek *de lege ferenda*, brzmiący *nihil novi*, tzn. optujący za pozostawieniem zapisów art. 5 ust 1 pkt 2 rzeczonyj ustawy w obecnym kształcie.

Gracjan Poterała

Rozdział 4.

Zadania ABW w zakresie bezpieczeństwa teleinformatycznego państwa

Wstęp

Pojęcie „bezpieczeństwo teleinformatyczne państwa” nie zostało wprowadzone dotychczas zdefiniowane na gruncie prawa polskiego, jednakże z całą pewnością należy stwierdzić, że jego zakres odnosi się do wielu aspektów szeroko rozumianego bezpieczeństwa narodowego. Bezpieczeństwo narodowe, jak wskazuje M. Nowiński¹, jest *pojęciem o najszerzym zakresie przedmiotowym, które obejmuje również inne rodzaje bezpieczeństwa, jak: bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne oraz bezpieczeństwo zewnętrzne*. Wydaje się, iż przywołany powyżej podział bezpieczeństwa narodowego jest poglądem słusznym i popartym wieloma przykładami. A. Grzelak w komentarzu do art. 73² Traktatu o funkcjonowaniu Unii Europejskiej³:

(...) bezpieczeństwo narodowe (ang. *national security*) najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa, która obejmuje problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa. Państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór wartości wewnętrznych, które jego zdaniem powinny być chronione przed zagrożeniami. Bezpieczeństwo narodowe postrzegane jest zatem

¹ M. Nowiński, *Pojęcie bezpieczeństwa narodowe w prawie europejskim i międzynarodowym w kontekście uprawnień służb specjalnych*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota”, Warszawa 2017, s. 11.

² A. Grzelak, *Komentarz do art. 72 i komentarz do art. 73*, w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, red. A. Wróbel, N. Półtorak, D. Miąsik, Warszawa 2012.

³ Wersja skonsolidowana Dz.Urz. UE C 83 z 30 III 2010.

jako zdolność narodu (państwa) do obrony terytorium i wartości. Termin „bezpieczeństwo narodowe” zawiera w sobie zatem te aspekty, które w kontekście art. 72 nazywane są „bezpieczeństwem wewnętrznym”, chociaż intuicyjnie wydaje się pojęciem szerszym, i dotyczy również kwestii bezpieczeństwa w aspekcie militarnym.

Jednakże, z uwagi na charakter zagrożeń dotyczących systemów teleinformatycznych jednoznaczne przyporządkowanie ich do któregoś z wymienionych rodzajów bezpieczeństwa państwa, stanowiących elementy bezpieczeństwa narodowego, może okazać się niemożliwe. Zagrożenia dotyczące bezpieczeństwa systemów teleinformatycznych ze względu na fakt, iż ich głównym nośnikiem są sieci teleinformatyczne, mogą mieć charakter zarówno wewnętrzny, jak i zewnętrzny. W niektórych przypadkach, pomimo stwierdzenia, że takie zagrożenie pochodzi z urządzenia znajdującego się w sieci wewnętrznej danego państwa, może się jednak okazać, że był to jedynie „przekaznik” albo „wykonawca poleceń”⁴, płynących z zupełnie innego miejsca na świecie.

Samo pojęcie „bezpieczeństwo teleinformatyczne” wywodzi się z *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. 2019, poz. 742) i dotyczy bezpieczeństwa systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych.

Warto zauważyć, że technologie informacyjno-komunikacyjne stały się nieodłącznym elementem życia i funkcjonowania człowieka w XXI w., a ich rozwój wydaje się obecnie procesem naturalnym, wynikającym z potrzeby tworzenia coraz to doskonalszych i bardziej innowacyjnych rozwiązań mających na celu zaspokojenie potrzeb społeczeństwa i gospodarki. Analiza zagadnienia bezpieczeństwa teleinformatycznego państwa powinna obejmować nie tylko kwestie ochrony informacji niejawnych, ale również bezpieczeństwo innych systemów teleinformatycznych. W tym miejscu wydaje się, że prawidłowe zrozumienie problematyki bezpieczeństwa teleinformatycznego państwa wymaga określenia zakresu tego pojęcia. Rozważania na temat bezpieczeństwa teleinformatycznego państwa należałoby więc rozpocząć od wskazania elementów składających się na ten rodzaj bezpieczeństwa oraz dokonania analizy powstawania kolejnych regulacji prawnych wynikających *de facto* z rozwoju technologii informacyjno-komunikacyjnych.

Definicja pojęcia „technologie informacyjno-komunikacyjne”, która wskazywałaby konkretne rozwiązania techniczne stanowiące zakres przedmiotowy tego terminu, mogłaby szybko stać się nieaktualna z uwagi na tempo rozwoju nowoczesnych technologii. Biorąc powyższe pod uwagę, uniwersalna definicja pojęcia „technologie informacyjno-komunikacyjne” powinna mieć charakter ogólny, niezależny od upływu czasu i rozwoju technologicznego.

Jako przykład uniwersalnego określenia pojęcia „technologie informacyjno-komunikacyjne” można przywołać definicję M. Matusiak, w której wskazano, iż:

⁴ Komputer zombi.

pojęcie technologie informacyjno-komunikacyjne (*Information and Communication Technology* — ICT) nazywane też technologiami informacyjnymi (IT), są technologiami związanymi ze zbieraniem, przechowywaniem, przetwarzaniem, przesyłaniem, rozdzielaniem i prezentacją informacji (tj. tekstów, obrazów, dźwięku). Obejmują one w szczególności technologie komputerowe (sprzęt i oprogramowanie) i technologie komunikacyjne. Technologie informacyjne to także dziedzina wiedzy obejmująca: informatykę, telekomunikację i inne technologie powiązane z informacją. Dostarczają one narzędzi, za pomocą których można pozyskiwać informacje, selekcjonować je, analizować, przetwarzać i przekazywać odbiorcom⁵.

Z powyższej definicji wynika, iż pojęcia „technologie informacyjno-komunikacyjne” (ICT) i „technologie informacyjne” (IT) mogą być używane zamiennie, dlatego też na potrzeby niniejszego tekstu wszystkie technologie informacyjno-komunikacyjne będą nazywane technologiami informacyjnymi.

Rozwój technologii informacyjnych nie dotyczy wyłącznie usług i rozwiązań technologicznych przeznaczonych dla społeczeństwa i podmiotów gospodarczych, ale w znacznym stopniu dotyczy również administracji publicznej. Pierwszym krokiem w tym zakresie było uchwalenie przez Sejm Rzeczypospolitej Polskiej *ustawy z dnia 21 grudnia 2001 r. o zmianie ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania ministrów, ustawy o działach administracji rządowej*⁶ oraz *o zmianie niektórych ustaw*. Przedmiotowa ustawa nowelizowała m.in. *ustawę z dnia 4 września 1997 r. o działach administracji rządowej* w zakresie wprowadzenia nowego działu administracji rządowej „informatyzacja” oraz określenia zakresu spraw objętych tym działem, do których zaliczono kwestie:

- 1) infrastruktury informatycznej oraz systemów i sieci teleinformatycznych,
- 2) technologii i technik informacyjnych oraz standardów informatycznych,
- 3) informatyzacji administracji rządowej i samorządowej,
- 4) wspierania inwestycji w dziedzinie informatyki,
- 5) edukacji informacyjnej oraz usług teleinformatycznych i multimedialnych,
- 6) zastosowań informatyki w społeczeństwie informacyjnym, w szczególności w gospodarce, bankowości i edukacji,
- 7) realizacji zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji.

Wprowadzenie do polskiego porządku prawnego przepisów regulujących na poziomie ustawowym kwestie związane z rozwojem nowoczesnych technologii oraz wyspecjalizowanie odrębnego działu administracji rządowej, właściwego do realizacji tych zadań, wydaje się z perspektywy czasu działaniem właściwym. Kolejnym znaczącym krokiem podjętym przez ustawodawcę w drodze do informatyzacji administracji publicznej i implementacji nowoczesnych technologii

⁵ *Innowacje i transfer technologii. Słownik pojęć*, red. K.B. Matusiak, Warszawa 2011, s. 290.

⁶ Dz.U. 2001, poz. 1800.

w sektorze publicznym było uchwalenie *ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*⁷, która to ustawa, jak wskazuje uzasadnienie:

stanowi kolejny krok w kierunku pełnej realizacji przyjętego przez Sejm Rzeczypospolitej Polskiej i Radę Ministrów planu działania w zakresie rozwoju społeczeństwa informacyjnego i integracji Polski z Unią Europejską. (...) Projekt ustawy, stanowiącej rozwinięcie i uszczegółowienie na płaszczyźnie normatywnej wymienionych wyżej tendencji i dążeń, zakłada osiągnięcie minimalnego stanu zgodności technicznej komponentów sprzętowych i programowych systemów teleinformatycznych — takiego, który umożliwi współpracę systemów teleinformatycznych używanych przez różne podmioty publiczne do realizacji właściwych im zadań publicznych. Podkreślenia wymaga okoliczność, że dzięki osiągnięciu takiego stanu stanie się możliwy sprawny przepływ informacji między podmiotami publicznymi w zakresie realizowanych przez nie zadań, co bezpośrednio przełoży się na zwiększenie szybkości i skuteczności działania tych podmiotów⁸.

Przedmiotowa ustawa, z uwagi na zakres regulowanej materii, wielokrotnie posługuje się pojęciem „system teleinformatyczny”, które nie jest nowe dla polskiego systemu prawnego, na co wskazuje sposób zdefiniowania go w art. 3 pkt 3 tej ustawy przez odesłanie do art. 2 pkt 3 *ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz.U. nr 144, poz. 1204).

Z kolei art. 2 pkt 3 u. św. elektr. stanowi, że określenie „system teleinformatyczny” oznacza *zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne*. Warto również nadmienić, że pomimo upływu 19 lat od czasu uchwalenia tej ustawy przedmiotowa definicja uległa tylko drobnym zmianom wynikającym z uchwalenia w 2004 r. ustawy *Prawo telekomunikacyjne* i wprowadzeniu w niej pojęcia „telekomunikacyjne urządzenie końcowe”. Analizując definicje pojęć „technologie informacyjno-komunikacyjne” oraz „system teleinformatyczny”, można dojść do wniosku, iż wszelkie definicje terminów z zakresu nowych technologii powinny mieć charakter uniwersalny, opisujący je przez wskazanie ogólnych rozwiązań technologicznych, gdyż może to spowodować dezaktualizację definicji w krótkim czasie.

Jednakże wraz z rozwojem systemów teleinformatycznych przez administrację publiczną oraz implementacją nowych technologii w sektorze publicznym przez długi okres nie dostrzegano problematyki zagrożeń dla bezpieczeństwa

⁷ Dz.U. 2005, poz. 565.

⁸ [https://orka.sejm.gov.pl/Druki4ka.nsf/\(\\$vAllByUnid\)/7CF4C722BFCE7A7EC1256D910029F45D/\\$file/1934-ustawa.rtf](https://orka.sejm.gov.pl/Druki4ka.nsf/($vAllByUnid)/7CF4C722BFCE7A7EC1256D910029F45D/$file/1934-ustawa.rtf), [dostęp: 25 VI 2021].

tych systemów teleinformatycznych, co skutkowało brakiem kompleksowych uregulowań prawnych dotyczących tej materii.

Wydaje się, iż punktem zwrotnym zarówno dla Polski, jak i całej Europy, który pokazał, w jakim stopniu prawidłowe funkcjonowanie państwa jest uzależnione od bezpieczeństwa krytycznych dla tego państwa systemów teleinformatycznych, były wydarzenia w Estonii w kwietniu 2007 r.

Wiosną 2007 r. doszło do pierwszego w historii ataku pochodzącego z cyberprzestrzeni, skierowanego przeciw niepodległemu państwu. Przyczyną takiego zmasowanego cyberataku był konflikt o podłożu historycznym, wywołany przygotowaniem do przeniesienia z centrum Tallina pomnika upamiętniającego sowieckich żołnierzy, poległych podczas walk o to miasto podczas drugiej wojny światowej. Sprzeciw wobec planów przeniesienia pomnika na miejscowy cmentarz wojskowy wyrazili działacze mniejszości rosyjskiej w Estonii. Początkowo ich protest miał charakter pokojowy. Dopiero oficjalne stanowisko władz rosyjskich w kwestii miejsca usytuowania przedmiotowego pomnika doprowadziło do międzypaństwowego kryzysu, a w rezultacie do fali zamieszek na ulicach Tallina. Jednakże w przypadku tego konfliktu to nie ulice estońskiej stolicy były głównym teatrem działań Rosjan.

Polem bitwy elektronicznej stał się estoński internet. 27 kwietnia o godzinie 22.30 serwis rządu zaczęły bombardować tzw. ataki *denial of services* (DoS). Dziś wiadomo, że te cyberataki, prowadzone przez wielu niezależnych hakerów, rozpoczęła rosyjska organizacja „Nasi”, podporządkowana Kremlowi (ona sama twierdzi, że jest niezależna od rosyjskiego rządu). Od tamtego wieczora fala cyberataków na infrastrukturę informatyczną nasilała się, unieruchamiając strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Cyberataki osiągnęły apogeum 9 maja (rosyjski Dzień Zwycięstwa), gdy ich celem stał się też sektor prywatny. Sytuacja zaczęła przypominać powieść *science fiction*: dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi *online* i wstrzymać transakcje zagraniczne. Zamarła też strona największego dziennika „Postimees”⁹.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Jednym z aspektów bezpieczeństwa teleinformatycznego państwa jest bezpieczeństwo systemów teleinformatycznych dopuszczonych do przetwarzania informacji niejawnych. Zagadnienie bezpieczeństwa teleinformatycznego w kontekście ochrony informacji niejawnych ma zdecydowanie dłuższą historię, niż ma to miejsce w przypadku systemów i sieci, w których przetwarzane są wyłącznie informacje nieoznaczone klauzulą tajności.

⁹ <https://www.tygodnikpowszechny.pl/dni-ktore-wstrzasnely-estonia-136573>, [dostęp: 25 VI 2021].

W polskim systemie prawnym regulacje z zakresu bezpieczeństwa teleinformatycznego systemów i sieci dopuszczonych do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych pojawiły się po raz pierwszy w *ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*¹⁰ w rozdziale 10 (*Bezpieczeństwo systemów i sieci teleinformatycznych*)¹¹. Przepisy te zostały następnie uchylone w związku z wejściem w życie z dniem 2 stycznia 2011 r. *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*¹², która w art. 190 uchyliła *ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. 2005, poz. 1631 z późn. zm.).

Obecnie obowiązująca *ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* w rozdziale ósmym (*Bezpieczeństwo teleinformatyczne*), obejmującym przepisy zawarte w art. 48–53, reguluje zagadnienie bezpieczeństwa teleinformatycznego systemów i sieci, w których przetwarzane są informacje niejawne. Analizując przedmiotowe przepisy, można dojść do wniosku, iż stanowią one regulacje o charakterze uniwersalnym i ponadczasowym, gdyż pomimo upływu ponad 10 lat od dnia uchwalenia tych przepisów znowelizowany został wyłącznie art. 53 ust. 5 pkt 2¹³, dotyczący opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego. Nowelizacja tego przepisu nie dotyczyła kwestii *stricte* merytorycznych, lecz miała charakter dostosowujący. Jej skutkiem była zmiana jednej z wytycznych do wydania przez Prezesa Rady Ministrów rozporządzenia określającego szczegółowy sposób i tryb ustalania wysokości oraz poboru opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego.

Należy w tym miejscu nadmienić, iż właściwość Agencji Bezpieczeństwa Wewnętrznego w kontekście zarówno szeroko rozumianej ochrony informacji niejawnych, jak i realizacji zadań z zakresu bezpieczeństwa teleinformatycznego w tym aspekcie, wynika z art. 5 ust. 1 pkt 3 ustawy o ABW oraz AW i art. 10 ust. 3 u. inf. niejaw. Przedmiotowy przepis ustawy o ochronie informacji niejawnych wskazuje, że Agencja Bezpieczeństwa Wewnętrznego realizuje zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, niewymienionych w ust. 2. Natomiast ust. 2 przywołanego przepisu określa właściwość Służby Kontrwywiadu Wojskowego wyłącznie wobec podmiotów i osób wykonujących zadania o charakterze innym niż cywilnym, tj. Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, ataszatów obrony

¹⁰ Dz.U. 1999, poz. 95.

¹¹ Art. 60–64 ustawy o ochronie informacji niejawnych.

¹² Dz.U. 2011, poz. 1228.

¹³ Nowelizacja art. 53 ust. 5 pkt 2 wynikała z art. 129 pkt 2 *ustawy z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę — Prawo o szkolnictwie wyższym i nauce* (Dz.U. 2010, poz. 1669).

w placówkach zagranicznych oraz żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione powyżej. W związku z powyższym należy stwierdzić, iż zadania Agencji Bezpieczeństwa Wewnętrznego, jak i Służby Kontrwywiadu Wojskowego, w zakresie bezpieczeństwa teleinformatycznego państwa są analogiczne, a jedyna różnica to właściwość podmiotowa w tym zakresie.

Analizując przepisy u. inf. niejaw., na wstępie wskazać należy, iż o fakcie uregulowania kwestii zasad *ochrony informacji niejawnych* w systemach teleinformatycznych stanowi art. 1 ust. 1 pkt 7 tej ustawy. Dodatkowo zagadnienia z zakresu bezpieczeństwa teleinformatycznego systemów, w których przetwarzane są informacje niejawne, wymagało zdefiniowania na poziomie ustawowym pojęć specyficznych dla tego rodzaju systemów. Na potrzeby zdefiniowania w ustawie o ochronie informacji niejawnych pojęcia „system teleinformatyczny”¹⁴ ustawodawca posłużył się odesłaniem do definicji tego pojęcia w rozumieniu art. 2 pkt 3 u. św. elektr. (Dz.U. 2019, poz. 123). Ponadto, z uwagi na szczególne wymagania dotyczące ochrony informacji niejawnych w systemach i sieciach teleinformatycznych w ustawie o ochronie informacji niejawnych, odpowiednio w art. 2 pkt 7–12, zdefiniowano również pojęcia: „dokument szczególnych wymagań bezpieczeństwa”, „dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego”, „akredytacja bezpieczeństwa teleinformatycznego”, „certyfikacja” oraz „audyt bezpieczeństwa systemu teleinformatycznego”.

Najistotniejszym elementem procedury dopuszczenia systemu teleinformatycznego do przetwarzania informacji niejawnych jest akredytacja bezpieczeństwa teleinformatycznego. Sposób dokonywania akredytacji systemu teleinformatycznego zależy przede wszystkim od najwyższej klauzuli informacji, które będą mogły być przetwarzane w danym systemie teleinformatycznym.

Agencja Bezpieczeństwa Wewnętrznego jest właściwa do przeprowadzenia akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych, w których będą przetwarzane informacje niejawne o klauzuli „poufne” lub wyższej¹⁵ w podmiotach pozostających w jej właściwości, z uwagi na podział wynikający z art. 10 ust. 2 i 3 u. inf. niejaw. Natomiast w przypadku systemów teleinformatycznych, w których będą przetwarzane informacje niejawne o klauzuli „zastrzeżone”, akredytacji dla takiego systemu udziela kierownik jednostki organizacyjnej przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego¹⁶.

Potwierdzeniem udzielenia przez Agencję Bezpieczeństwa Wewnętrznego akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego¹⁷. Natomiast sama akre-

¹⁴ Ustawa o ochronie informacji niejawnych, art. 2 pkt 6.

¹⁵ Tamże, art. 48 ust. 3.

¹⁶ Tamże, art. 48 ust. 9.

¹⁷ Tamże, art. 48 ust. 5.

dytacja bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych udzielana jest na czas określony, nie dłuższy niż pięć lat¹⁸.

Jednakże, aby świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego mogło zostać wydane, niezbędne jest zatwierdzenie przez Agencję Bezpieczeństwa Wewnętrznego dokumentacji bezpieczeństwa systemu teleinformatycznego oraz pozytywny wynik audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez Agencję Bezpieczeństwa Wewnętrznego¹⁹. Wyjątek od tej reguły może stanowić sytuacja, gdy akredytacji bezpieczeństwa systemu teleinformatycznego podlega system, w którym przetwarzane będą informacje niejawne oznaczone klauzulą „poufne” lub niższą. W takiej sytuacji Agencja Bezpieczeństwa Wewnętrznego może odstąpić od przeprowadzania audytu bezpieczeństwa takiego systemu teleinformatycznego²⁰.

Oprócz przepisów ustawy o ochronie informacji niejawnych istotną rolę w zakresie regulacji dotyczących bezpieczeństwa teleinformatycznego państwa odgrywa również *rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*²¹, którego podstawę do wydania stanowi art. 49 ust. 9 u. inf. niejaw. Rozporządzenie to określa podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne. Ponadto, przedmiotowe rozporządzenie wskazuje zakres niezbędnych danych, jakie powinna zawierać dokumentacja bezpieczeństwa systemów teleinformatycznych oraz określa sposób opracowania tej dokumentacji.

Kolejnym z istotnych aspektów bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych jest zagadnienie ochrony elektromagnetycznej. Ochrona elektromagnetyczna systemu teleinformatycznego jest stosowana w celu przeciwdziałania i zapobiegania naruszeniu poufności i dostępności informacji niejawnych przetwarzanych w systemie teleinformatycznym. Naruszenie poufności informacji niejawnych w kontekście bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych należy rozumieć jako ujawnienie informacji niejawnych podmiotom do tego nieuprawnionym²², do czego może dojść na skutek wykorzystania elektromagnetycznej emisji ujawniającej, która pochodzi z elementów systemu w systemie teleinformatycznym przetwarzającym informacje niejawne²³. Środki ochrony elektromagnetycznej stosuje się w systemach teleinformatycznych

¹⁸ Tamże, art. 48 ust. 2.

¹⁹ Tamże, art. 48 ust. 6.

²⁰ Tamże, art. 48 ust. 8.

²¹ Dz.U. 2011, poz. 948.

²² *Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*, § 2 pkt 9.

²³ Tamże, § 8 ust. 1.

przetwarzających informacje niejawne o klauzuli „poufne” lub wyższej, które dobiera się na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, z uwzględnieniem zaleceń w zakresie bezpieczeństwa teleinformatycznego, o których mowa w art. 52 ust. 3 u. inf. niejaw., udzielanych przez Agencję Bezpieczeństwa Wewnętrznego.

Ponadto, ochrona elektromagnetyczna dotyczy również sytuacji, w której mogłoby dojść do naruszenia dostępności informacji niejawnych, tj. właściwości określającej, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym²⁴, przez wystąpienie zakłócenia pracy tych systemów teleinformatycznych za pomocą emisji lub impulsów elektromagnetycznych o dużej mocy. W takim przypadku środki ochrony elektromagnetycznej dobierane są na podstawie wyników szacowania ryzyka, tj. całościowego procesu analizy i oceny ryzyka dla bezpieczeństwa informacji niejawnych.

Jednakże, aby ochrona elektromagnetyczna systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej była właściwie, realizowana musi być ona z wykorzystaniem środków ochrony elektromagnetycznej, które podlegały badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonej przez Agencję Bezpieczeństwa Wewnętrznego. Z kolei urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają w pierwszej kolejności badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego.

Reasumując, Szef Agencji Bezpieczeństwa Wewnętrznego pełni rolę organu „regulacyjnego” w zakresie bezpieczeństwa teleinformatycznego przeznaczonych do przetwarzania informacji niejawnych, a zadania realizowane przez Agencję Bezpieczeństwa Wewnętrznego dotyczą w szczególności procesu dopuszczania systemów teleinformatycznych i urządzeń do przetwarzania informacji niejawnych. Natomiast w zakresie samego bezpieczeństwa teleinformatycznego poszczególnych systemów teleinformatycznych odpowiedzialność ciąży na kierowniku jednostki organizacyjnej, w której funkcjonuje konkretny system teleinformatyczny.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

Pierwszym aktem prawnym rangi ustawowej, który wprowadzał w polskim systemie prawnym regulacje dotyczące cyberprzestrzeni była *ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*²⁵. Należy jednak zauważyć, że przedmiotowa nowelizacja oprócz dodania przepisów

²⁴ Tamże, § 2 pkt 1.

²⁵ Dz.U. 2011, poz. 1323.

wskazujących, że przesłanką wprowadzenia któregoś ze stanów nadzwyczajnych mogą być zdarzenia w cyberprzestrzeni, oraz definiujących pojęcie „cyberprzestrzeń” w poszczególnych zmienianych ustawach, nie wprowadziła żadnych nowych narzędzi, które pozwoliłyby podjąć działania przez organy kierujące działaniami w czasie stanu nadzwyczajnego²⁶.

Pierwszą ustawą, która uregulowała zagadnienie rozpoznawania, zapobiegania i wykrywania zagrożeń godzących w bezpieczeństwo teleinformatyczne państwa w zakresie systemów teleinformatycznych, które nie są akredytowane do przetwarzania informacji niejawnych, była *ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*²⁷. Przedmiotowa ustawa określiła zasady prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie ich realizacji, a także wprowadziła zmiany w przepisach regulujących zagadnienia dotyczące zagrożeń o charakterze terrorystycznym. Ponadto w ramach prac legislacyjnych nad projektem tej ustawy dostrzeżono konieczność uregulowania na poziomie ustawowym możliwości wystąpienia zdarzenia o charakterze terrorystycznym albo wystąpienia takiego zdarzenia, którego celem mogą stać się systemy teleinformatyczne istotne z punktu widzenia funkcjonowania państwa.

W tym zakresie *ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* wprowadziła na poziomie ustawowym przepisy określające spójny i jednolity system wprowadzania stopni alarmowych, w tym również stopni alarmowych dotyczących cyberprzestrzeni Rzeczypospolitej Polskiej (stopnie alarmowe CRP).

Przed wejściem w życie ustawy o działaniach antyterrorystycznych kwestia stopni alarmowych była uregulowana w przepisach *ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*²⁸ oraz w przepisach wykonawczych wydanych na podstawie art. 7 ust. 4 tejże ustawy, uprawniającego Prezesa Rady Ministrów do określenia w drodze zarządzenia, z zachowaniem przepisów o ochronie informacji niejawnych, wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego, z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego, oraz organów odpowiedzialnych za ich uruchamianie. Przedmiotowe akty prawne, tj. zarządzenia Prezesa Rady Ministrów nr 74 z 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego²⁹ oraz nr 18 z 2 marca 2016 r.

²⁶ Art. 8 *ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej* (Dz.U. 2017 poz.1897), art. 9 *ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (Dz.U. 2017, poz. 1928) i art. 9–14 *ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz.U. 2017, poz. 1932).

²⁷ Dz.U. 2016, poz. 904.

²⁸ Dz.U. 2013, poz. 1166; 2015, poz. 1485; 2016, poz. 266.

²⁹ *Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.*

w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego³⁰ określały sposób i tryb wprowadzania stopni alarmowych CRP. Zasadniczą różnicą między systemami stopni alarmowych było to, że system stosowany przed wejściem w życie *ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, wprowadzony zarządzeniem, obejmował wyłącznie sferę administracji rządowej, natomiast aktualny system, uregulowany na poziomie ustawowym, jest już powszechnie obowiązujący³¹.

Wskazuje na to również uzasadnienie do projektu ustawy o działaniach antyterrorystycznych, w którym projektodawca stwierdza, iż *ustawa wprowadzi powszechnie obowiązujący i dostosowany do wymogów NATO czterostopniowy system stopni alarmowych na wypadek zagrożeń terrorystycznych oraz stopni alarmowych w cyberprzestrzeni*³².

Z punktu widzenia bezpieczeństwa teleinformatycznego państwa to właśnie uregulowanie na poziomie ustawowym zagadnienia dotyczącego systemu stopni alarmowych CRP jest najbardziej istotną zmianą wprowadzoną przez ustawę o działaniach antyterrorystycznych. Przed wejściem w życie tych przepisów zagadnienie to było uregulowane w załączniku nr 1 do zarządzenia Prezesa Rady Ministrów nr 18 z 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.

Stopnie alarmowe CRP określają poziom zagrożenia wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo związane są bezpośrednio z wystąpieniem takiego zdarzenia. Przyjęty system określa cztery rodzaje stopni alarmowych CRP tj.:

- 1) pierwszy stopień alarmowy CRP (stopień ALFA-CRP),
- 2) drugi stopień alarmowy CRP (stopień BRAVO-CRP),
- 3) trzeci stopień alarmowy CRP (stopień CHARLIE-CRP),
- 4) czwarty stopień alarmowy CRP (stopień DELTA-CRP)³³.

Istotna rola w procedurze wprowadzania, zmieniania i odwoływania stopnia alarmowego CRP została powierzona Szefowi Agencji Bezpieczeństwa Wewnętrznego, którego opinia jest niezbędna do wprowadzenia, zmieniania i odwołania stopnia alarmowego CRP zarówno przez Prezesa Rady Ministrów, jak i ministra właściwego do spraw wewnętrznych, w przypadkach niecierpiących zwłoki.

W kontekście stopni alarmowych CRP ustawa o działaniach antyterrorystycznych wprowadziła również przepis obligujący Szefa ABW do powołania

³⁰ <https://czarnocin.bip.gov.pl/fobjects/download/154968/zarządzenie-nr-18-prezesa-rady-ministrow-z-dnia-2-marca-2016-r-pdf.html>, [dostęp: 25 VI 2021].

³¹ P. Łabuz, T. Safjański, W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz*, Warszawa 2019.

³² <https://orka.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/%-24File/516-uzas.docx>, [dostęp: 25 VI 2021].

³³ *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, art. 15 ust. 2.

sztabu koordynacyjnego w przypadku wprowadzenia stopnia alarmowego CRP³⁴. W skład sztabu koordynacyjnego wchodzi przedstawiciele wyznaczeni przez służby specjalne oraz przedstawiciele policji, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Generalnego Inspektora Informacji Finansowej, Krajowej Administracji Skarbowej, Żandarmerii Wojskowej oraz Rządowego Centrum Bezpieczeństwa³⁵. Przepisy tej ustawy dają ponadto Szefowi Agencji Bezpieczeństwa Wewnętrznego uprawnienie do powoływania do udziału w pracach sztabu koordynacyjnego, w zależności od rodzaju zdarzenia o charakterze terrorystycznym, dodatkowych członków sztabu koordynacyjnego spośród przedstawicieli innych organów administracji publicznej oraz przedstawiciela Prokuratora Generalnego, wyznaczonych przez te organy³⁶. Przepisy *ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* określają również zadania sztabu koordynacyjnego, do których należy rekomendowanie zmiany lub odwołania stopnia alarmowego oraz określenie form i zakresu współdziałania służb i organów wchodzących w skład sztabu koordynacyjnego i biorących udział w jego pracach³⁷.

Z punktu widzenia bezpieczeństwa teleinformatycznego państwa ustawa o działaniach antyterrorystycznych wprowadziła również istotne zmiany w ustawie o ABW oraz AW³⁸, polegające na rozszerzeniu katalogu zadań Agencji Bezpieczeństwa Wewnętrznego o rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej³⁹. Oprócz rozszerzenia zadań Agencji Bezpieczeństwa Wewnętrznego ustawa o działaniach antyterrorystycznych rozszerzyła zakres uprawnień i obowiązków Szefa Agencji Bezpieczeństwa Wewnętrznego⁴⁰. Powyższe zmiany zostaną szerzej omówione w części dotyczącej przepisów regulujących zagadnienie bezpieczeństwa teleinformatycznego państwa zawartych w ustawie o ABW oraz AW.

³⁴ Tamże, art. 17 ust. 1.

³⁵ Tamże, art. 5 ust. 1 w związku z art. 17 ust. 1 te samej ustawy.

³⁶ Tamże, art. 17 ust. 2 w związku z art. 6 ust. 2 pkt 2 te samej ustawy.

³⁷ Tamże, art. 17 ust. 3.

³⁸ Tamże, art. 38.

³⁹ *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, art. 5 ust. 1 pkt. 2 a.

⁴⁰ Tamże, art. 32 a i art. 32 b–32 d.

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2020, poz. 27 z późn. zm.)

Określenie roli Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa teleinformatycznego państwa nastąpiło w ramach przepisów zmieniających inne ustawy, zawartych w ustawie o działaniach antyterrorystycznych⁴¹. Ustawa ta znowelizowała ustawę o ABW oraz AW przez rozszerzenie zadań Agencji Bezpieczeństwa Wewnętrznego o przepis wskazujący, iż do zadań tej służby specjalnej należy rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 *ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. 2019, poz. 1398)⁴². Przepis ten po raz pierwszy w polskim systemie prawnym wskazywał podmiot odpowiedzialny za określony zakres bezpieczeństwa teleinformatycznego państwa.

Zadania przekazane do realizacji Agencji Bezpieczeństwa Wewnętrznego mają charakter prewencyjny. Przemawia za tym sposób, w jaki zostały uregulowane, w szczególności fakt, iż mają dotyczyć rozpoznawania, zapobiegania i wykrywania zagrożeń skierowanych przeciwko bezpieczeństwu teleinformatycznemu państwa, a więc wiążą się bezpośrednio z przeciwdziałaniem wystąpienia tych zagrożeń.

W ramach określenia wymienionych zadań Agencji Bezpieczeństwa Wewnętrznego ustawodawca wskazał także katalog podmiotów, w zakresie których systemów informatycznych mają być one realizowane. Podmioty te można podzielić na dwie grupy, którymi są: organy administracji publicznej oraz podmioty umieszczone na prowadzonym przez dyrektora Rządowego Centrum Bezpieczeństwa jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

W ramach poszczególnych uprawnień przyznanych Szefowi Agencji Bezpieczeństwa Wewnętrznego w przepisach ustawy o działaniach antyterrorystycznych, nowelizujących ustawę o Agencji Bezpieczeństwa Wewnętrznego, dodano art. 32a–32e. W tych przepisach jednoznacznie wskazano Agencję Bezpieczeństwa Wewnętrznego jako jedyny organ administracji publicznej, który w 2016 r. w zakresie swojej właściwości posiadał narzędzia pozwalające na podjęcie realnych działań w zakresie bezpieczeństwa teleinformatycznego państwa w kontekście systemów teleinformatycznych, które nie są akredytowane do przetwarzania

⁴¹ *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, art. 38.

⁴² *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, art. 5 ust. 1 pkt. 2 a.

informacji niejawnych. Jak już wcześniej wskazano, w zakresie bezpieczeństwa systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych uprawnienia Szefa ABW zostały określone w *ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. 2019, poz. 742).

Uprawnienia Szefa ABW w zakresie prewencji dotyczącej bezpieczeństwa teleinformatycznego państwa wprowadziły nieznane dotychczas w polskim systemie prawnym narzędzie umożliwiające przeprowadzenie oceny bezpieczeństwa systemu teleinformatycznego w celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym w cyberprzestrzeni, dotyczących najistotniejszych z punktu widzenia funkcjonowania państwa systemów teleinformatycznych oraz ścigania ich sprawców. Zakresem przedmiotowym oceny poziomu bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia ciągłości funkcjonowania państwa, zostały objęte systemy teleinformatyczne organów administracji publicznej lub sieci teleinformatyczne objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemy teleinformatyczne właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym, lub dane przetwarzane w tych systemach⁴³. Ocena bezpieczeństwa systemów teleinformatycznych dokonywana przez Szefa ABW przeprowadzana jest zgodnie z rocznym planem. Przedmiotowy plan jest opracowywany corocznie do 30 września i określa zakres oceny bezpieczeństwa w następnym roku kalendarzowym⁴⁴. Plan oceny bezpieczeństwa sporządzany jest w uzgodnieniu z ministrem właściwym do spraw informatyzacji, a podmioty zarządzające systemami ujętymi w tym planie są informowane przez Agencję Bezpieczeństwa Wewnętrznego o włączeniu ich systemu do planu. Ponadto przepisy regulujące tryb sporządzania planu oceny bezpieczeństwa systemów teleinformatycznych zawierają regulację określającą tryb przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych *ad hoc*, wskazując na możliwość jej przeprowadzenia z pominięciem planu. Rozwiązanie to wydaje się o tyle istotne, że pozwala na podjęcie przez Szefa ABW odpowiednich działań w przypadku uzyskania ważnych informacji o zagrożeniach dotyczących systemów teleinformatycznych istotnych z punktu widzenia funkcjonowania państwa.

Chociaż ocena bezpieczeństwa systemów teleinformatycznych, o której mowa w art. 32a ustawy o ABW oraz AW, przeprowadzana przez Szefa ABW, jest swego rodzaju audytem bezpieczeństwa systemów teleinformatycznych, to nie należy jej mylić z audytem bezpieczeństwa teleinformatycznego, o którym mowa w art. 48 ust. 6 pkt 2 u. inf. niejaw. Ocenie bezpieczeństwa systemów teleinformatycznych, przeprowadzanej przez Szefa Agencji Bezpieczeństwa

⁴³ *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, art. 32 a ust. 1.

⁴⁴ Tamże, art. 32 a ust. 2.

Wewnętrznego, bliżej jest do tzw. testów penetracyjnych, świadczonych jako usługa komercyjna przez wiele podmiotów prywatnych⁴⁵.

Przepisy ustawy o ABW oraz AW precyzyjnie określają sposób i cel przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych, wskazując że polega ona na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego, których celem jest przede wszystkim identyfikacja podatności systemu teleinformatycznego. Przez podatność, której wykrycie jest głównym celem przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych, ustawodawca rozumie słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która mogłaby zostać wykorzystana w przypadku zagrożenia dla takiego systemu teleinformatycznego, płynącego z cyberprzestrzeni. Ponadto ustawodawca precyzyjnie wskazał cechy systemów teleinformatycznych, których naruszenie może stanowić podatność stanowiącą zagrożenie dla bezpieczeństwa tego systemu teleinformatycznego. Cechami systemu teleinformatycznego, które są naruszane w przypadku wystąpienia zagrożenia i podlegają badaniu podczas oceny bezpieczeństwa systemu teleinformatycznego, są jego integralność, poufność, rozliczalność i dostępność⁴⁶.

Kolejnym istotnym aspektem przeprowadzania przez Szefa Agencji Bezpieczeństwa Wewnętrznego oceny bezpieczeństwa systemów teleinformatycznych jest fakt, iż systemy teleinformatyczne, podlegające badaniu w czasie jego przeprowadzania, zazwyczaj funkcjonują w sposób standardowy i wykonują przewidziane dla nich zadania. Projektodawca wprowadził więc w przepisach regulujących sposób przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych swego rodzaju wytyczne określające sposób przeprowadzania takiej oceny. Tym samym powinna być ona realizowana z uwzględnieniem zasad minimalizacji zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności. Ustawodawca wprowadził też w omawianych przepisach dodatkową regulację, wskazującą wprost na kategoryczny zakaz przeprowadzania oceny bezpieczeństwa systemu teleinformatycznego w sposób, który może doprowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie teleinformatycznym podlegającym tej ocenie⁴⁷.

Z uwagi na fakt, iż systemy teleinformatyczne podlegające ocenie bezpieczeństwa różnią się od siebie zarówno w zakresie budowy, jak i posiadanych funkcjonalności, a także mając na względzie, że osoby przeprowadzające ocenę bezpieczeństwa takiego systemu nie posiadają dostępu do dokumentacji ocenianego systemu, istnieje ogromne niebezpieczeństwo doprowadzenia do zakłócenia pracy ocenianego systemu albo uszkodzenia danych przetwarzanych w ocenianych systemach. Kompromisem między bezpieczeństwem ocenianego systemu

⁴⁵ Np. PwC Polska, zob. <https://www.pwc.pl/pl/uslugi/testy-penetracyjne-bezpieczenstwo-informatyczne.html>, [dostęp: 25 VI 2021].

⁴⁶ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 a ust. 4.

⁴⁷ Tamże, art. 32 a ust. 5.

teleinformatycznego a przeprowadzeniem rzetelnej i obiektywnej oceny takiego systemu jest uregulowanie przez ustawodawcę obowiązku uzgodnienia między Agencją Bezpieczeństwa Wewnętrznego i podmiotem odpowiedzialnym za oceniany system teleinformatyczny ramowych warunków przeprowadzenia tej oceny, w tym w szczególności daty rozpoczęcia, harmonogramu oraz zakresu i rodzaju testów bezpieczeństwa przeprowadzanych w ramach oceny bezpieczeństwa⁴⁸. Uzgodnienie dokonywane przed rozpoczęciem oceny bezpieczeństwa systemu teleinformatycznego ma na celu minimalizację ryzyka wystąpienia negatywnych skutków dla takiego systemu w związku z przeprowadzaną oceną. Aby proces uzgadniania sposobu przeprowadzenia oceny bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia funkcjonowania państwa ustandaryzować i ułatwić jego przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego, a także ułatwić współpracę między służbą przeprowadzającą ocenę i podmiotem, którego system teleinformatyczny podlega ocenie, ustawodawca zawarł w art. 32a ust. 14 ustawy o ABW oraz AW upoważnienie do wydania stosownego rozporządzenia. Przedmiotowa kwestia została więc uregulowana w *rozporządzeniu Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym*⁴⁹. Przedmiotowy akt wykonawczy oprócz określenia warunków i trybu przeprowadzania oceny bezpieczeństwa, a także czynności niezbędnych do przeprowadzania oceny bezpieczeństwa, wyznacza również wzór porozumienia zawierającego ramowe warunki przeprowadzenia oceny.

Analizując zagadnienie przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego oceny bezpieczeństwa systemu teleinformatycznego, wskazać należy, że w celu uzyskania skuteczności podejmowanych działań, które umożliwią odzworowanie realnego zagrożenia dla takiego systemu teleinformatycznego, niezbędne są odpowiednie narzędzia, które posiadają funkcjonalności analogiczne do narzędzi używanych przez osoby podejmujące próby przełamania zabezpieczeń systemu teleinformatycznego i uzyskania nieuprawnionego dostępu do jego zasobów.

W przypadku Agencji Bezpieczeństwa Wewnętrznego należy mieć jednak na uwadze art. 7 Konstytucji RP, który jednoznacznie wskazuje, że organy władzy publicznej działają na podstawie i w granicach prawa, a jak wskazuje art. 269b § 1 KK, wytwarzanie, pozyskiwanie narzędzi służących do przełamania zabezpieczeń systemów teleinformatycznych stanowi znamiona czynu zabronionego.

W związku z powyższym ustawa o ABW oraz AW zawiera przepis określający kontratyp wobec czynu polegającego na wytwarzaniu lub pozyskiwaniu urządzenia lub programów komputerowych, o których mowa w art. 269b KK. Ponadto przepis ten umożliwi ich używanie w celu określenia podatności ocenianego systemu teleinformatycznego, pod kątem ewentualnej możliwości popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo

⁴⁸ Tamże, art. 32 a ust. 6.

⁴⁹ Dz.U. 2016, poz. 1076.

§ 2 w związku z § 1, art. 269 § 2 albo art. 269a KK⁵⁰. Przepis ten w sposób jednoznaczny określa katalog narzędzi, jakie mogą być używane podczas przeprowadzania oceny bezpieczeństwa systemu teleinformatycznego. Przyznane w ten sposób uprawnienie pozwala na wykorzystanie środków technicznych, które mogą zostać użyte w przypadku wystąpienia realnego zagrożenia, płynącego z cyberprzestrzeni, dla takiego systemu, co znacznie zwiększa wartość przeprowadzonej oceny bezpieczeństwa takiego systemu teleinformatycznego.

W związku z umożliwieniem korzystania podczas przeprowadzania oceny bezpieczeństwa systemu teleinformatycznego z urządzeń lub oprogramowania służących m.in. do przełamywania zabezpieczeń i uzyskiwania dostępu do zasobów systemów teleinformatycznych ustawodawca przewidział i uregulował zagadnienie ewentualnego uzyskania takiego dostępu przez osoby bezpośrednio przeprowadzające ocenę bezpieczeństwa systemu teleinformatycznego do informacji nieprzeznaczonych dla tej osoby albo do całości lub części systemu teleinformatycznego podlegającego ocenie bezpieczeństwa⁵¹. W przepisach został również uregulowany sposób postępowania z informacjami uzyskanymi przez Agencję Bezpieczeństwa Wewnętrznego w związku z przeprowadzaniem oceny bezpieczeństwa systemu teleinformatycznego, wskazujący wprost, iż stanowią one tajemnicę prawnie chronioną i nie mogą zostać wykorzystane do realizacji innych zadań ABW. Informacje te, niezależnie od formy, w jakiej zostały utrwalone, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu⁵². Natomiast sposób dokonywania zniszczenia materiałów zawierających informacje uzyskane przez Agencję Bezpieczeństwa Wewnętrznego, w związku z przeprowadzaniem oceny bezpieczeństwa systemu teleinformatycznego, szczegółowo reguluje *rozporządzenie Prezesa Rady Ministrów z dnia 18 lipca 2016 r. w sprawie sposobu niszczenia materiałów zawierających informacje uzyskane w wyniku przeprowadzonej przez Agencję Bezpieczeństwa Wewnętrznego oceny bezpieczeństwa oraz wzorów druków wymaganej dokumentacji* (Dz.U 2016, poz. 1055), do wydania którego upoważnia art. 32 a. ust. 13 ustawy o ABW oraz AW. Przedmiotowe rozporządzenie precyzyjnie reguluje sposób dokonania zniszczenia uzyskanych materiałów, wskazując na odpowiednie sposoby postępowania zarówno w przypadku materiałów i dokumentów, jak również informacji utrwalonych na nośnikach danych.

Wyniki przeprowadzonej oceny bezpieczeństwa systemu teleinformatycznego mogą mieć znaczenie nie tylko dla podmiotu, którego system podlegał ocenie, ale również dla innych systemów teleinformatycznych. Podmiot, którego system teleinformatyczny podlegał ocenie bezpieczeństwa, otrzymuje podsumowanie czynności przeprowadzonych w ramach oceny bezpieczeństwa tego systemu teleinformatycznego oraz wskazanie wykrytych podatności ocenianego

⁵⁰ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 a ust. 7.

⁵¹ Tamże, art. 32a ust. 8.

⁵² Tamże, art. 32a ust. 9.

systemu⁵³. Gdy podczas przeprowadzania oceny systemu dojdzie do wykrycia podatności, która w ocenie Agencji Bezpieczeństwa Wewnętrznego może występować również w innych systemach teleinformatycznych, służba ta jest obowiązana do niezwłocznego poinformowania o tym fakcie ministra właściwego do spraw informatyzacji wraz ze wskazaniem ewentualnej możliwości wystąpienia tej podatności w innych systemach teleinformatycznych⁵⁴. Takie rozwiązanie pozwala, w przypadku wykrycia nieznannej podatności, na wdrożenie działań pozwalających na zabezpieczenie systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, przed ewentualnymi zagrożeniami pochodzącymi z cyberprzestrzeni, jeszcze przed odkryciem i wykorzystaniem tej podatności w sposób zagrażający bezpieczeństwu tych systemów.

Przepisy regulujące zagadnienie przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia bezpieczeństwa państwa, zawierają również normę upoważniającą Szefa Agencji Bezpieczeństwa Wewnętrznego do określenia, w drodze zarządzenia, rodzajów testów bezpieczeństwa, dokonywanych w ramach oceny bezpieczeństwa, z uwzględnieniem potrzeby kompletności dokonywanej oceny. Przeniesienie tego zakresu regulacji na poziom aktu wewnętrznego, jakim jest zarządzenie Szefa Agencji Bezpieczeństwa Wewnętrznego, stanowi uelastycznienie zakresu działań Agencji Bezpieczeństwa Wewnętrznego i pozwala na dynamiczne dostosowywanie zakresu testów bezpieczeństwa dokonywanych w ramach oceny bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, w przypadku zidentyfikowanych podatności, których nie wykrywały dotychczas przeprowadzane testy bezpieczeństwa.

Kolejnym z uprawnień przyznanych Szefowi ABW w ramach nowelizacji ustawy o ABW oraz AW jest umożliwienie przyspieszenia podjęcia i realizacji ustawowych zadań ABW w przypadku wystąpienia zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa lub danych przetwarzanych w tych systemach. Uprawnienie to pozwala Szefowi Agencji Bezpieczeństwa Wewnętrznego na żądanie od podmiotu, którego system teleinformatyczny lub dane były obiektem zdarzenia o charakterze terrorystycznym, udzielenia szczegółowych informacji dotyczących takiego systemu teleinformatycznego. Informacje, jakich może żądać w takim wypadku Szef ABW, dotyczą budowy, funkcjonowania i zasad eksploatacji systemów teleinformatycznych, w tym mogą obejmować hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemu oraz ich używanie⁵⁵. Żądanie przekazania tych informacji ma na celu umożliwienie Agencji Bezpieczeństwa Wewnętrznego realizacji jej ustawowego zadania, określonego w art. 5 ust. 1 pkt 2 a ustawy o ABW oraz AW, polegającego na zapobieganiu i reagowaniu na zdarzenia o charakterze terrorystycznym

⁵³ Tamże, art. 32 a ust. 10.

⁵⁴ Tamże, art. 32 a ust. 11.

⁵⁵ Tamże, art. 32 b ust. 1.

dotyczące systemów istotnych z punktu widzenia funkcjonowania państwa lub danych przetwarzanych w tych systemach, a także na zapobieganiu i wykrywaniu przestępstw o charakterze terrorystycznym w tym obszarze oraz ściganiu ich sprawców. Przedmiotowe uprawnienie stanowi w istocie podstawę prawną do umożliwienia podjęcia przez Agencję Bezpieczeństwa Wewnętrznego kompleksowych i niczym nieograniczonych działań w ramach takiego systemu. Z uwagi na charakter informacji i danych przekazywanych na żądanie Szefa Agencji Bezpieczeństwa Wewnętrznego oraz mając na względzie konieczność zachowania najwyższego poziomu bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, ustawodawca przewidział uniwersalne rozwiązanie dla ochrony tych informacji i danych, wskazując iż podlegają one ochronie przewidzianej w przepisach o ochronie informacji niejawnych i mogą być udostępniane jedynie funkcjonariuszom ABW prowadzącym w danym postępowaniu czynności operacyjno-rozpoznawcze oraz ich przełożonym, uprawnionym do sprawowania nadzoru nad tymi czynnościami⁵⁶. Jednocześnie w przedmiotowych przepisach uregulowano kwestię ewentualnej odpowiedzialności odszkodowawczej Skarbu Państwa za szkody wyrządzone naruszeniem obowiązku zachowania w tajemnicy danych i informacji przekazanych Szefowi Agencji Bezpieczeństwa Wewnętrznego na zasadach określonych w Kodeksie cywilnym⁵⁷.

Do katalogu uprawnień o charakterze *quasi* prewencyjnym, przyznanych Szefowi ABW w zakresie bezpieczeństwa teleinformatycznego państwa, należy zaliczyć również przepisy regulujące zasady zarządzania i realizacji blokady dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym. Zarządzenie i realizacja takiej blokady dostępności są dokonywane w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców. Blokada dostępności w systemie teleinformatycznym może dotyczyć określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. Wskazać w tym miejscu należy, iż przepisy regulujące zagadnienie blokady dostępności danych lub usług w systemie teleinformatycznym zostały skonstruowane w sposób analogiczny jak uregulowany w art. 27 ustawy o ABW oraz AW tryb i sposób zarządzania kontroli operacyjnej, która jest jednym z uprawnień służb specjalnych najgłębiej ingerującym w prawo do prywatności i tajemnicę korespondencji. Taki sposób uregulowania uprawnienia do zarządzania blokadą dostępności określonych danych i usług wskazuje na rozważę ustawodawcy, która w szczególności została wykazana przez wprowadzenie wielostopniowego mechanizmu kontroli wniosków Szefa ABW w sprawie zastosowania blokady dostępności określonych

⁵⁶ Tamże, art. 32 b ust. 2.

⁵⁷ Tamże, art. 32 b ust. 3.

danych i usług. Wniosek Szefa ABW wymaga pisemnej zgody Prokuratora Generalnego⁵⁸, a o jego rozstrzygnięciu decyduje w formie postanowienia Sąd Okręgowy w Warszawie⁵⁹. Ustawodawca w omawianych przepisach określił także wymagania formalne dla wniosków składanych przez Szefa ABW⁶⁰, tryb i sposób rozpatrywania ich przez sąd⁶¹ oraz środki odwoławcze w postaci zażalenia na postanowienie sądu przysługujące Szefowi Agencji Bezpieczeństwa Wewnętrznego i Prokuratorowi Generalnemu⁶². Ponadto upoważnił Prezesa Rady Ministrów do określenia, w drodze rozporządzenia, sposobu dokumentowania blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków⁶³.

Blokadę dostępności określonych danych i usług sąd zarządza na okres nie dłuższy niż 30 dni. Jednakże blokada ta może zostać jednorazowo przedłużona na okres nie dłuższy niż trzy miesiące, a tryb składania wniosku o przedłużenie blokady dostępności określonych danych i usług jest analogiczny do trybu składania wniosku o zarządzenie zastosowania takiej blokady⁶⁴.

Podmiotem realizującym postanowienie sądu w zakresie dokonania blokady dostępności określonych danych i usług jest usługodawca świadczący usługi drogą elektroniczną, który jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu⁶⁵.

Przepisy regulujące kwestię zarządzania blokady dostępności określonych danych i usług, analogicznie jak w przypadku przepisów dotyczących kontroli operacyjnej, zawierają również regulacje umożliwiające Szefowi Agencji Bezpieczeństwa Wewnętrznego podjęcie odpowiednich działań w przypadkach niecierpiących zwłoki, gdy mogłoby to spowodować wystąpienie zdarzenia o charakterze terrorystycznym. Tryb postępowania w takim przypadku został ograniczony do obowiązku uzyskania przez Szefa Agencji Bezpieczeństwa Wewnętrznego pisemnej zgody Prokuratora Generalnego, która umożliwia zarządzenie blokady dostępności określonych danych i usług. Jednakże tryb ten wymaga jednoczesnego zwrócenia się z wnioskiem o wydanie postanowienia w tej sprawie do Sądu Okręgowego w Warszawie⁶⁶.

Blokada dostępności określonych danych i usług jest zarządzana na określony czas, po upływie którego dostęp do tych danych i usług powinien zostać odblokowany. Ustawodawca przewidział w analizowanych przepisach również inne sytuacje, które powodują zaprzestanie blokowania dostępności tych danych i usług. Jedną z nich jest nieudzielenie przez Sąd Okręgowy w Warszawie zgody

⁵⁸ Tamże, art. 32 c ust. 1.

⁵⁹ Tamże, ust. 3.

⁶⁰ Tamże, ust. 6.

⁶¹ Tamże, ust. 9.

⁶² Tamże, ust. 10.

⁶³ Tamże, ust. 14.

⁶⁴ Tamże, ust. 7.

⁶⁵ Tamże, ust. 5.

⁶⁶ Tamże, ust. 4.

na zarządzoną przez Szefa Agencji Bezpieczeństwa Wewnętrznego blokadę dostępności w trybie podejmowania działań niecierpiących zwłoki, w terminie pięciu dni od złożenia tego wniosku. Kolejną z przesłanek powodujących zaprzestanie blokowania dostępności danych i usług jest nieudzielenie przez sąd zgody na przedłużenie blokady⁶⁷. Zastosowanie blokady dostępności określonych danych i usług jest uprawnieniem o charakterze wyjątkowym i powinno być stosowane jedynie w wypadkach, gdy zaistniała sytuacja nie pozwala na użycie innych dostępnych środków. Ustawodawca przewidział więc specjalny tryb informowania o zastosowaniu blokady dostępności. W wypadku skorzystania z tego narzędzia, gdy usługodawca świadczący usługi drogą elektroniczną, który został zobowiązany do zrealizowania czynności z zakresu zablokowania określonych danych lub usług, ma siedzibę na terytorium Rzeczypospolitej Polskiej, Szef Agencji Bezpieczeństwa Wewnętrznego jest obowiązany do powiadomienia ministra właściwego do spraw informatyzacji⁶⁸.

Realizacja przez Agencję Bezpieczeństwa Wewnętrznego zadań o charakterze analityczno-informacyjnym odbywa się również w kontekście występowania zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa. Gromadzenie informacji w tym zakresie zostało powierzono Szefowi Agencji Bezpieczeństwa Wewnętrznego przez nałożenie na ten organ obowiązku prowadzenia rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej⁶⁹. W rejestrze tym gromadzone są szczegółowe dane dotyczące zarówno systemu teleinformatycznego, którego dotyczyło naruszenie bezpieczeństwa, jak i dane dotyczące samego naruszenia, w tym m.in. data i czas jego wykrycia oraz prawdopodobna początkowa data i czas tego naruszenia⁷⁰, identyfikacja źródła zdarzenia naruszającego bezpieczeństwo systemu⁷¹, opis stwierdzonego zdarzenia oraz sposób działania podmiotu powodującego naruszenie bezpieczeństwa⁷², a także opis szkód w systemie powstałych lub mogących powstać wskutek zdarzenia naruszającego bezpieczeństwo systemu⁷³.

Wszystkie dane gromadzone w przedmiotowym rejestrze pochodzą od administratorów systemu teleinformatycznego, w którym doszło do naruszenia bezpieczeństwa, zobowiązanych do ich przekazywania niezwłocznie po wykryciu zdarzenia naruszającego bezpieczeństwo tego systemu. Ze względu na zakres zadań powierzonych ministrowi kierującemu działem administracji „informatyzacja” przepisy dotyczące przedmiotowego rejestru wskazują na obowiązek udostępnienia mu zgromadzonych tam danych. Prowadzenie przez Szefa Agencji

⁶⁷ Tamże, ust. 11.

⁶⁸ Tamże, ust. 12.

⁶⁹ Tamże, art. 32 d ust. 1.

⁷⁰ Tamże, ust. 2 pkt 2.

⁷¹ Tamże, ust. 2 pkt 3.

⁷² Tamże, ust. 2 pkt 4.

⁷³ Tamże, ust. 2 pkt 5.

Bezpieczeństwa Wewnętrznego tego rejestru ma na celu zgromadzenie danych w zakresie pojawiających się naruszeń bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, a ich analiza może okazać się pomocna w przygotowaniu i wydaniu przez Szefa Agencji Bezpieczeństwa Wewnętrznego rekomendacji, które stanowią kolejne z narzędzi prewencyjnych w kontekście bezpieczeństwa teleinformatycznego państwa.

Wydawanie rekomendacji dotyczących bezpieczeństwa teleinformatycznego państwa przez Szefa Agencji Bezpieczeństwa Wewnętrznego to kolejne z narzędzi o charakterze prewencyjnym w zakresie utrzymania bezpieczeństwa teleinformatycznego państwa. W przypadku wystąpienia zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, Szef Agencji Bezpieczeństwa Wewnętrznego przeprowadza analizę takiego zdarzenia i wydaje rekomendacje dla podmiotów zarządzających systemami teleinformatycznymi, istotnymi z punktu widzenia funkcjonowania państwa. Przedmiotowe rekomendacje mają na celu podniesienie poziomu bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, oraz zapewnienie odpowiedniego poziomu integralności, poufności, rozliczalności i dostępności tych systemów⁷⁴. Z uwagi na różnorodność charakteru i budowy systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, ustawodawca przewidział możliwość wniesienia do Szefa ABW zastrzeżenia do wydanych rekomendacji w zakresie przedstawionych w tym dokumencie sposobów podniesienia poziomu bezpieczeństwa systemów teleinformatycznych. Możliwość przedstawienia zastrzeżeń wynika z faktu, iż wskazany w rekomendacjach sposób podniesienia bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, w określonych sytuacjach i przy określonej konfiguracji takiego systemu może wpłynąć negatywnie na jego funkcjonowanie lub bezpieczeństwo takiego systemu⁷⁵. Przedstawienie zastrzeżeń do rekomendacji nie stanowi środka zwalniającego podmiot zarządzający systemem teleinformatycznym, istotnym z punktu widzenia funkcjonowania państwa, z obowiązku ich wprowadzenia. Wobec zgłoszonych zastrzeżeń Szef ABW niezwłocznie przedstawia swoje stanowisko, w którym podtrzymuje swoje rekomendacje albo przekazuje zmienione rekomendacje⁷⁶.

Podmioty zarządzające systemami teleinformatycznymi, istotnymi z punktu widzenia funkcjonowania państwa, które otrzymały rekomendacje wydane przez Szefa ABW, są obowiązane w terminie miesiąca od dnia ich otrzymania do poinformowania Szefa ABW o sposobie i zakresie ich uwzględnienia⁷⁷. Narzędziem, jakie ustawodawca przewidział dla Szefa ABW w sytuacji, gdyby podmiot zarządzający systemem teleinformatycznym, istotnym z punktu widzenia

⁷⁴ Tamże, art. 32 e ust. 1.

⁷⁵ Tamże, ust. 2.

⁷⁶ Tamże, ust. 3.

⁷⁷ Tamże, ust. 4.

funkcjonowania państwa, nie uwzględnił rekomendacji bezpieczeństwa, jest możliwość wystąpienia do podmiotu sprawującego nadzór nad podmiotem, który nie uwzględnił rekomendacji bezpieczeństwa, z informacją o ich nieuwzględnieniu lub wnioskiem, by ów organ nadzorujący podjął odpowiednie działania mające na celu wykonanie rekomendacji⁷⁸.

Innym aktem prawnym rangi ustawowej, który rozszerzył zakres narzędzi prewencyjnych przewidzianych dla Szefa ABW, służących podniesieniu poziomu bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, była *ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018, poz. 1560), która oprócz regulacji dotyczących ustanowienia krajowego systemu cyberbezpieczeństwa, wprowadziła również w art. 79 zmiany w ustawie o ABW oraz AW polegające na dodaniu art. 32 aa.

Przedmiotowy przepis ustanowił uprawnienie dla ABW do wdrożenia, prowadzenia i koordynowania funkcjonowania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet. Działanie przedmiotowego systemu ma na celu zapobieganie i przeciwdziałanie oraz zwalczanie zdarzeń o charakterze terrorystycznym, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych. Zakres podmiotowy systemów, które mają być włączone do systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, jest analogiczny jak w przypadku innego narzędzia o charakterze prewencyjnym powierzono Szefowi ABW, jakim jest ocena bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa. Do katalogu systemów teleinformatycznych, w których ma być wdrożony system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, należą systemy teleinformatyczne organów administracji publicznej lub sieci teleinformatyczne objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemy teleinformatyczne właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym⁷⁹.

Mechanizm przyłączania poszczególnych podmiotów do systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet jest analogiczny jak w przypadku oceny bezpieczeństwa systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, i też odbywa się na podstawie rocznego planu. Ponadto ustawodawca przewidział możliwość włączenia podmiotów do tego systemu z pominięciem planu, co wskazuje na działania mające na celu uelastycznienie sposobu rozbudowy przedmiotowego systemu i możliwość szybkiego reagowania w wyjątkowych sytuacjach⁸⁰.

⁷⁸ Tamże, ust. 5.

⁷⁹ Tamże, art. 32 aa ust. 1.

⁸⁰ Tamże, ust. 2.

Jednocześnie przepisy regulujące kwestię wdrożenia systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet jednoznacznie wskazały, iż przystąpienie przez podmiot do tego systemu jest obligatoryjne, a przepisy określiły tryb, w jakim podmiot, który ma zostać przyłączony do tego systemu, jest o tym fakcie informowany oraz sposób uzgadniania warunków technicznych, niezbędnych do dokonania tego przyłączenia⁸¹. Ponadto przepisy regulujące zagadnienie systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet zawierają upoważnienie do wydania przez Prezesa Rady Ministrów aktu wykonawczego regulującego warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w którym zostały w szczególności określone czynności niezbędne do uruchomienia tego systemu i jego utrzymania. W celu ustandaryzowania zakresu i sposobu uzgadniania kwestii technicznych i organizacyjnych dotyczących zawarcia porozumienia w sprawie przyłączenia poszczególnych podmiotów do wdrożenia systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet opracowano przedmiotowe rozporządzenie określające wzór tego porozumienia.

Pewnym wyjątkiem w zakresie obligatoryjności przystąpienia do przedmiotowego systemu są sytuacje, w których podmiotem przystępującym ma być podmiot podległy Ministrowi Obrony Narodowej lub przez niego nadzorowany. Wdrożenie systemu ostrzegania w takim podmiocie może nastąpić wyłącznie za zgodą Ministra Obrony Narodowej⁸².

Pomimo tego, iż przyłączenie podmiotu do systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, wskazanego w rocznym planie, jest obowiązkowe, może wystąpić sytuacja, w której porozumienie określające wszystkie kwestie techniczne i organizacyjne dokonania tego przyłączenia nie zostanie zawarte z powodu przyczyn leżących po stronie tego podmiotu. W takim wypadku ABW informuje o tym fakcie podmiot nadzorujący ten podmiot lub ministra właściwego do spraw informatyzacji⁸³.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2020, poz. 1369)

Ustawa o krajowym systemie cyberbezpieczeństwa stanowiła implementację do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii⁸⁴. Przedmiotowa ustawa uregulowała przede wszystkim organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu. Krajowy system cyberbezpieczeństwa

⁸¹ Tamże, ust. 7.

⁸² Tamże, ust. 5.

⁸³ Tamże, ust. 8.

⁸⁴ Dz.Urz. UE L 194 z 19.07.2016, s. 1.

został oparty na trzech zespołach CSIRT⁸⁵ poziomu krajowego. Jednym z CSIRT-ów poziomu krajowego jest CSIRT GOV — Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa ABW.

Pozostałe CSIRT-y tworzące krajowy system cyberbezpieczeństwa to CSIRT NASK i CSIRT MON, prowadzone odpowiednio przez Naukową i Akademicką Sieć Komputerową — Państwowy Instytut Badawczy oraz Ministra Obrony Narodowej⁸⁶.

Zakres zadań poszczególnych CSIRT-ów jest zbliżony, a jedyną znaczącą różnicą jest ich zakres właściwości podmiotowej w kontekście obsługi incydentów. W kontekście bezpieczeństwa teleinformatycznego państwa pozostającego we właściwości Szefa ABW należy wskazać, iż CSIRT GOV koordynuje obsługę incydentów zgłaszanych przez niektóre jednostki sektora finansów publicznych.

Przyjęty przez ustawodawcę sposób określenia zakresu podmiotowego poszczególnych CSIRT-ów, polegający na wprowadzeniu odesłania do *ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych*, ma zasadniczą zaletę, tj. uwzględnia wszystkie jednostki sektora publicznego bez obaw o ewentualną możliwość pozostawienia jakiegokolwiek jednostki publicznej poza właściwością któregokolwiek z CSIRT-ów. Jednakże rozwiązanie to ma również wady, które wyraźnie widać na przykładzie właściwości CSIRT-u GOV, do zadań którego należy koordynacja obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 *ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych*, z wyjątkiem wymienionych w art. 26 ust. 5 i 6 *ustawy o krajowym systemie cyberbezpieczeństwa*, a także jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane⁸⁷. Jak już wskazano powyżej, określenie właściwości poszczególnych CSIRT-ów stanowi kompromis między kompletnością katalogu podmiotów objętych właściwością poszczególnych CSIRT-ów a jego czytelnością. Oprócz koordynacji obsługi incydentów zgłaszanych przez wymienione wyżej jednostki sektora finansów publicznych do właściwości CSIRTu GOV należy również koordynacja obsługi incydentów zgłaszanych przez Narodowy Bank Polski, Bank Gospodarstwa Krajowego. Ponadto ustawa o krajowym systemie cyberbezpieczeństwa potwierdziła właściwość Szefa ABW wobec podmiotów, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 *ustawy o zarządzaniu kryzysowym*, a także podmiotów, które pozostają we właściwości CSIRT NASK w przypadku, gdy incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług

⁸⁵ Ang. *Computer Security Incident Response Team* (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego).

⁸⁶ *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, art. 2 pkt 2 i 3.

⁸⁷ Tamże, art. 26 ust. 7.

wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy, o zarządzaniu kryzysowym.

Inną kwestią, która jest niezmiernie istotna z punktu widzenia bezpieczeństwa państwa, jest wyłączenie stosowania ustawy o krajowym systemie cyberbezpieczeństwa wobec podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa ABW lub Szefa AW⁸⁸. Przedmiotowe wyłączenie nie powoduje wyłomów w krajowym systemie cyberbezpieczeństwa w zakresie podmiotów objętych sektorem „ochrona zdrowia”, a także pozwala na realizację przez ABW oraz AW zadań wynikających z art. 35 ust. 1 ustawy o ABW oraz AW w zakresie ochrony m.in. danych identyfikujących funkcjonariuszy tych agencji.

Właściwość Szefa ABW w zakresie zdarzeń w cyberprzestrzeni mających charakter terrorystyczny, wskazaną wprost w art. 5 ust. 1 pkt 2a ustawy o ABW oraz AW, potwierdza również ustawa o krajowym systemie cyberbezpieczeństwa, wskazując CSIRT GOV jako zespół właściwy do koordynacji obsługi incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy o działaniach antyterrorystycznych. Jedyny wyjątek w tym zakresie stanowią incydenty związane ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 5 ust. 1 pkt 2 a ustawy o SKW oraz SWW, które pozostają we właściwości CSIRT MON. Ponadto, ustawodawca przewidział obowiązek przekazania koordynacji obsługi incydentu związanego ze zdarzeniem o charakterze terrorystycznym do CSIRT MON lub CSIRT GOV⁸⁹.

Zakończenie

Analizując aspekty prawne realizacji przez ABW zadań w zakresie bezpieczeństwa teleinformatycznego państwa oraz przyznane w tym zakresie środki i narzędzia służące zapewnieniu bezpieczeństwa teleinformatycznego systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, należy stwierdzić, iż Szef ABW jest organem administracji publicznej, posiadającym najszersze uprawnienia w zakresie czuwania nad bezpieczeństwem teleinformatycznym tych systemów. Wśród tych systemów należy wyróżnić systemy teleinformatyczne akredytowane do przetwarzania informacji niejawnych, systemy teleinformatyczne organów administracji publicznej oraz systemy teleinformatyczne najważniejszych jednostek sektora finansów publicznych. W zakresie właściwości Szefa ABW pozostają również systemy teleinformatyczne lub sieci teleinformatyczne, objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5 b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym. We właściwości Szefa ABW pozostają też zdarzenia o charakterze terrorystycznym w cyberprzestrzeni. Dodatkowo ABW wykonuje wiele zadań o charakterze prewencyjnym

⁸⁸ Tamże, art. 1 ust. 2 pkt 3.

⁸⁹ Tamże, art. 27 ust. 3.

w zakresie systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa.

Jednakże, nawet pomimo dość szerokich uprawnień oraz możliwości, należy wyraźnie stwierdzić, iż bezpieczeństwo systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa, jest nieustannie zagrożone, a rozwiązania legislacyjne nigdy nie zapewnią pełnego spektrum zabezpieczenia tych systemów, dlatego niezbędna jest stała analiza nowych zagrożeń pochodzących z cyberprzestrzeni oraz wprowadzanie takich rozwiązań legislacyjnych, które umożliwią jak najpełniejsze zabezpieczenie tych systemów. Cyberbezpieczeństwo Rzeczypospolitej Polskiej jest nowym frontem walki, jednak nie można do niego stosować rozwiązań i koncepcji, które dotychczas zdawały egzamin w przypadku standardowych zagrożeń bezpieczeństwa państwa.

Marcin Nowiński
Mateusz Wieczerza

Rozdział 5.

Zadania służb specjalnych w obszarze ochrony informacji niejawnych ze szczególnym uwzględnieniem aspektów międzynarodowych

Uwagi wstępne

Pod pojęciem „ochrona informacji niejawnych” należy rozumieć, w ujęciu ogólnym, zespół działań właściwych organów państwa mających na celu ich zabezpieczenie przed nieuprawnionym ujawnieniem.

Współczesne wyzwania związane z tą sferą należy analizować w sposób kompleksowy, uwzględniający nie tylko formalne aspekty ochrony informacji niejawnych (np. prawidłowa klasyfikacja informacji niejawnych czy organizacja systemu ich ochrony w jednostkach organizacyjnych, w których są one przetwarzane), lecz również fakt, iż system ochrony informacji niejawnych służy przede wszystkim zagwarantowaniu właściwego poziomu ochrony wartości, o których mowa w art. 5 ustawy o ABW oraz AW — bezpieczeństwa wewnętrznego, porządku konstytucyjnego, niepodległości czy integralności terytorialnej.

Zapewnienie efektywnego systemu ochrony informacji niejawnych służy przede wszystkim realizacji zadań kontrwywiadowczych, związanych z neutralizacją aktywności obcych służb specjalnych przez uniemożliwienie czy znaczne obniżenie prawdopodobieństwa uzyskania przez nie dostępu do informacji, którym w myśl *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*¹ nadana została klauzula tajności.

Biorąc pod uwagę fakt, iż specyfika zagrożeń związanych z możliwością uzyskania dostępu do informacji niejawnych przez podmioty nieuprawnione stanowić może zagrożenie dla wszystkich wartości wymienionych w art. 5 ustawy o ABW oraz AW, zasadne wydaje się zaklasyfikowanie wymienionego

¹ Dz.U. 2019, poz. 742.

ryzyka jako godzącego w bezpieczeństwo narodowe, stanowiące kategorię szerszą niż poszczególne komponenty wymienione we wspomnianym przepisie.

Zadania służb specjalnych, w szczególności ABW, w omawianym obszarze podzielić można na dwa podstawowe rodzaje:

- zadania o charakterze ochronnym, podejmowane w wymiarze wewnętrznym, polegające na zagwarantowaniu prawidłowego funkcjonowania systemu ochrony informacji niejawnych;
- zadania związane z zapewnieniem efektywnych sposobów wymiany informacji niejawnych z partnerami zagranicznymi w celu aktywnego przeciwdziałania zidentyfikowanym zagrożeniom dla bezpieczeństwa narodowego.

Celem niniejszego rozdziału jest zatem dokonanie opisu podstawowych zagrożeń mogących skutkować nieuprawnionym ujawnieniem informacji niejawnych przez przyzmat pojęcia bezpieczeństwa narodowego, omówienie ustawowych instrumentów, jakie wykorzystywać może ABW w celu ich rozpoznawania i zwalczania oraz charakterystyka najważniejszych zadań służb specjalnych w drugiej z wymienionych powyżej kategorii — wymiany informacji niejawnych w wymiarze międzynarodowym, w szczególności w oparciu o bilateralne umowy o ochronie informacji niejawnych oraz umowy o współpracy w zwalczaniu przestępczości zorganizowanej.

Rys historyczny

Należy wskazać, że do chwili wejścia w życie *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, ochronę informacji niejawnych w Rzeczypospolitej Polskiej gwarantowała *ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*². Warto zaznaczyć, że ta ustawa w okresie swego obowiązywania doczekała się 23 nowelizacji. Charakter powyższych zmian był różnorodny, obejmował zmiany o charakterze porządkującym, wynikające z nowelizacji bądź uchwalania nowych ustaw, aż po zasadnicze zmiany merytoryczne samej ustawy o ochronie informacji niejawnych. Obowiązująca przez ponad 10 lat ustawa o ochronie informacji niejawnych pozwoliła stworzyć wspólny system ochrony informacji niejawnych oraz odegrała istotną rolę w okresie akcesji Polski do NATO. Należy zauważyć, że już ustawa z 1999 r., jako pierwsza po 1989 r., regulowała sferę wymiany informacji niejawnych w stosunkach międzynarodowych, definiując iż służby ochrony państwa (którymi zgodnie z art. 2 pkt 3 były Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego), zgodnie z art. 14 ust. 1 pkt 4, były właściwe do ochrony informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi. Ponadto, zgodnie z art. 15 tej ustawy, w stosunkach międzynarodowych szefowie Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego pełnili funkcję krajowej

² Dz.U. 2005, nr 196, poz. 1631 z późn. zm. Uchylona przez *ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*.

władzy bezpieczeństwa. Analogicznie art. 24 ówczesnej ustawy stanowił, że materiały otrzymywane z zagranicy oraz wysyłane za granicę, w celu wykonania umów międzynarodowych, oznaczają się odpowiednią do ich treści klauzulą tajności, określoną w ustawie oraz jej zagranicznym odpowiedniku. Innym przepisem odnoszącym się do sfery międzynarodowej wymiany informacji niejawnych był art. 25 ust. 2 pkt 3, który wskazywał, że chronione bez względu na upływ czasu pozostają informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia. Art. 28 ust. 2 wskazywał z kolei, że jeżeli z zawartych przez Rzeczpospolitą Polską umów międzynarodowych wynika, na zasadzie wzajemności, obowiązek dopuszczenia do informacji niejawnych obywateli obcych państw, mających wykonywać w Rzeczypospolitej Polskiej pracę w interesie innego państwa lub organizacji międzynarodowej, postępowania sprawdzającego nie przeprowadza się. Wspomniane regulacje nie wyczerpują całego katalogu przepisów ówczesnej ustawy odnoszącej się do sfery międzynarodowej wymiany informacji niejawnych, ale ukazują spektrum regulacyjne w tamtym akcie prawnym, w którym po raz pierwszy przedmiotowe kwestie zostały szczegółowo uregulowane.

Warto przy tym zauważyć, że ustawa z 1999 r. była w pewnej mierze wzorowana na rozwiązaniach zawartych w dokumencie C-M (55) 15 (*Final*), określającym politykę bezpieczeństwa Sojuszu Północnoatlantyckiego, opracowanym w 1955 r. W samym NATO, wobec narastającego przeświadczenia, że liczące blisko 50 lat rozwiązania są już przestarzałe, przyjęto w 2002 r. nowy dokument regulujący politykę bezpieczeństwa — C-M (2002) 49, który wprowadza zasady znacznie bardziej elastyczne i umożliwia szerokie stosowanie zarządzania ryzykiem w miejsce dawniej obowiązujących standardów minimalnych. W tym kierunku szły też zmiany wprowadzane przez dyrektywy wykonawcze i wytyczne Biura Bezpieczeństwa NATO, a także dokumenty dotyczące polityki bezpieczeństwa Unii Europejskiej. Były one wykorzystywane w bieżącej działalności polskich krajowych władz bezpieczeństwa, jednak wdrażanie nowoczesnych rozwiązań jest w znacznym stopniu warunkowane zmianami na poziomie ustawy. Z biegiem czasu jednak wiele jej przepisów stało się przestarzałymi i niefunkcjonalnymi, w szczególności wobec dokonującego się ogromnego postępu technologicznego, zwłaszcza w zakresie środków łączności oraz systemów teleinformatycznych.

Objęcie przez Rzeczpospolitą Polską przewodnictwa w Radzie Unii Europejskiej w 2011 r. postawiło przed polską administracją państwową wiele wyzwań wymagających podjęcia pilnych kroków. Jednym z nich było postulowane przez Ministerstwo Spraw Zagranicznych dostosowanie polskiego systemu ochrony informacji niejawnych do reguł i praktyki obowiązującej w instytucjach Unii Europejskiej i w krajach członkowskich. Dotyczyło to szczególnie możliwości znacznie bardziej elastycznego traktowania zasad ochrony informacji o niskich klauzulach tajności, co w strukturach unijnych umożliwia szybkie, bieżące wykorzystywanie tych informacji w pracy grup roboczych oraz ich sprawne przekazywanie i przetwarzanie w systemach teleinformatycznych. System

ochrony informacji niejawnych w Polsce wymagał zatem reform bardzo daleko idących, co uzasadniało konieczność opracowania nowej ustawy, która poprawiłaby jakość prawa normującego ochronę informacji niejawnych w Rzeczypospolitej Polskiej³.

Odpowiedzią na te problemy oraz dylematy było opracowanie nowej ustawy o ochronie informacji niejawnych (*ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*), która jest obecnie obowiązującym aktem prawnym i której istotne regulacje zostaną szczegółowo przedstawione w dalszej części.

Ochrona informacji niejawnych a pojęcie „bezpieczeństwa narodowego”

Dokonanie szczegółowej charakterystyki zadań służb specjalnych w obszarze ochrony informacji niejawnych, z uwzględnieniem międzynarodowego wymiaru tego problemu, w pierwszej kolejności wymaga podkreślenia, iż zdolność państwa do ich skutecznej realizacji jest jednym z zadań organów władzy publicznej dotyczących sfery bezpieczeństwa narodowego.

Pojęcie „bezpieczeństwo narodowe” zdefiniować można jako pewien obiektywny stan, w którym dane państwo jest wolne od zagrożeń o charakterze wewnętrznym i zewnętrznym. Ewolucja występujących aktualnie w tej sferze zagrożeń związana jest z dogłębną redefinicją specyfiki stosunków międzynarodowych po zakończeniu zimnej wojny. Przyjmowany tradycyjnie podział na zagrożenia o charakterze wewnętrznym oraz zewnętrznym traci obecnie na znaczeniu, a czynników stwarzających zagrożenie dla bezpieczeństwa narodowego nie sposób jednoznacznie przyporządkować do jednej z tych kategorii.

O ile przedstawienie szczegółowej charakterystyki nowych rodzajów zagrożeń dla bezpieczeństwa narodowego przekracza zakres niniejszego rozdziału, o tyle wskazać należy, iż istotne znaczenie z punktu widzenia ochrony informacji niejawnych mają następujące problemy:

- zagrożenia dla bezpieczeństwa narodowego nie są związane wyłącznie z działalnością państw i ich organów, lecz również aktorów pozapaństwowych (np. organizacji terrorystycznych czy ponadnarodowych korporacji dążących do uzyskania informacji za pomocą szpiegostwa przemysłowego);
- rozwój środków technicznych służących do przetwarzania informacji sprawia, iż zmianie ulega zarówno sam charakter informacji, jak i sposoby sprawowania nad nimi kontroli;
- transgraniczny charakter współczesnych wyzwań w obszarze bezpieczeństwa narodowego wymaga stworzenia nie tylko systemu gwarantującego bezpieczeństwo informacji niejawnych, ale również możliwość ich efektywnej wymiany między państwami.

Pojęcie „bezpieczeństwo narodowe” oraz składające się nań elementy w początkach XXI w. różnią się znacząco od tego, w jaki sposób było ono

³ Uzasadnienie projektu ustawy o ochronie informacji niejawnych oraz o zmianie niektórych ustaw. Sejm RP VI kadencji. Nr druku 2791.

rozumiane w XX stuleciu, gdy jego najbardziej istotnym aspektem było bezpieczeństwo militarne. Mając na uwadze ewolucję, o której mowa wyżej, tytułem przykładu wyróżnić można następujące komponenty pojęcia „bezpieczeństwo narodowe”⁴:

- bezpieczeństwo polityczne — ochrona systemu politycznego przed nieuprawnioną ingerencją zarówno wewnętrzną, jak i zewnętrzną;
- bezpieczeństwo gospodarcze — zdolność systemu gospodarczego do zapewnienia funkcjonowania społeczeństwa oraz stopień, w jakim właściwe organy państwa mogą swobodnie podejmować decyzje co do najważniejszych kierunków polityki gospodarczej czy finansowej. Za jeden z elementów bezpieczeństwa gospodarczego uznać można bezpieczeństwo energetyczne, rozumiane jako zdolność państwa do zapewnienia dostępu do surowców energetycznych wyłącznie na podstawie kryteriów rynkowych, w sposób wolny od wpływu innych państw czy podmiotów pozapaństwowych;
- bezpieczeństwo powszechne — rozumiane jako zapewnienie fizycznego bezpieczeństwa obywateli, podstawowych funkcji infrastrukturalnych czy komunikacyjnych (np. bezpieczeństwo środków transportu czy ochrona granic);
- cyberbezpieczeństwo — ochrona systemów informatycznych, zarówno państwowych, jak i prywatnych, przed nieuprawnioną ingerencją podmiotów państwowych lub pozapaństwowych.

Z tego względu istotne znaczenie ma postrzeganie uwarunkowań związanych z ochroną informacji niejawnych w sposób szeroki, uwzględniający zarówno zmianę podstawowych paradygmatów stosunków międzynarodowych i globalnego systemu bezpieczeństwa, jak i rosnące w bezprecedensowym tempie znaczenie informacji dla bezpieczeństwa państwa. Uzyskanie dostępu do informacji niejawnych może być celem nie tylko organów innego państwa, lecz również aktorów pozapaństwowych, np. organizacji terrorystycznych czy korporacji działających w wymiarze globalnym.

Analiza najważniejszych aspektów specyfiki obszaru bezpieczeństwa narodowego prowadzi do wniosku, iż intensyfikacja zagrożeń związanych z możliwością bezprawnego ujawnienia informacji niejawnych czy wejścia w ich posiadanie przez nieuprawniony podmiot związana jest z trzema grupami czynników:

- ewolucją zagrożeń dla bezpieczeństwa narodowego związaną z zagrożeniami hybrydowymi i asymetrycznymi;
- rosnącą rolą informacji w kształtowaniu polityki państwa oraz rozszerzeniem obszarów, w których waga określonych informacji uzasadnia nadanie im klauzuli tajności;

⁴ R. Holmes Kim, *What is National Security?* The Heritage Foundation, dostępne w Internecie: www.heritage.org/sites/default/files/201910/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf, [dostęp: 31 V 2021].

- rozwojem technologicznym wiążącym się z powszechnym wykorzystywaniem środków komunikacji elektronicznej, Internetu oraz systemów informatycznych w toku realizacji zadań organów władzy publicznej.

Zagrożenia dla bezpieczeństwa narodowego należy zatem postrzegać jako czynniki mogące mieć negatywny wpływ na immanentne elementy składowe państwa (niepodległość, integralność terytorialną, suwerenność, porządek konstytucyjny czy bezpieczeństwo obywateli). Sfera ochrony informacji niejawnych stanowi jeden z jego najbardziej istotnych komponentów. Problematyka ochrony informacji niejawnych powinna być zatem analizowana przede wszystkim przez pryzmat realizacji podstawowych funkcji państwa w obszarze bezpieczeństwa narodowego.

Aspekty prawne

Zdefiniowanie interakcji zachodzących między wymienionymi pojęciami jest utrudnione z uwagi na fakt, iż „informacje niejawne” to termin prawny — zarówno sama definicja, jak i sposoby m.in. ich klasyfikowania, przetwarzania i ochrony, są szczegółowo określone w *ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji*, w przeciwieństwie do terminu „bezpieczeństwo narodowe”, którego ramy znaczeniowe mogą być określone wyłącznie w sposób pośredni, z uwagi na brak definicji legalnej tego pojęcia.

Zgodnie z definicją zawartą w art. 1 ust. 1 u. inf. niejaw., pod pojęciem „informacje niejawne” należy rozumieć informacje, 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. Z definicji tej wynika zatem, iż kluczowym kryterium ochrony informacji niejawnych jest interes państwa⁵.

Jak wskazano wyżej, w polskim systemie prawnym nie występuje definicja legalna pojęcia „bezpieczeństwo narodowe”. Niemniej jednak, rozważania istotne dla interpretacji tego pojęcia zawarte są w wydanych 6 października 2020 r. orzeczeniach w połączonych sprawach C-511/18, C-512/18 i C-520/18 *La Quadrature du Net* i in. oraz w sprawie C-623/17 *Privacy International*.

Podkreślenia wymaga również fakt, iż pojęcie „bezpieczeństwo narodowe” występuje w art. 4 ust. 2 TFUE. Zgodnie z tym przepisem Unia szanuje równość Państw Członkowskich wobec Traktatów, jak również ich tożsamość narodową, nierozzerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym w odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza te mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo

⁵ I. Stankowska, *Komentarz do ustawy o ochronie informacji niejawnych*, Lexis Nexis, Warszawa 2011, wyd. 1, s. 16.

narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego.

Precyzyjne określenie klauzuli bezpieczeństwa narodowego, o którym mowa w art. 4 ust. 2 TFUE, sprawia liczne problemy interpretacyjne, w szczególności w toku postępowań przed TSUE, prowadzonych na skutek kierowanych przez Państwa Członkowskie pytań prejudycjalnych dotyczących kwestii zastosowania prawa UE do instrumentów ustawodawczych dotyczących sfery bezpieczeństwa narodowego.

Trybunał nie dokonał dotychczas szczegółowej wykładni omawianego przepisu, niemniej jednak w kontekście niniejszego rozdziału istotne znaczenie mają uwagi zaprezentowane we wspomnianych orzeczeniach z 6 października 2020 r. W pkt. 135 wyroku w sprawach C-511/18, C-512/18 i C/520/18 TSUE wskazał, iż odpowiedzialność Państw Członkowskich za sferę bezpieczeństwa narodowego, o której mowa w art. 4 ust. 2 TFUE, obejmuje pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, a także zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna.

Powyższe rozważania Trybunału można uznać za pośrednią, abstrakcyjną definicję pojęcia „bezpieczeństwo narodowe”. Nie zawiera ona katalogu spraw mieszczących się w zakresie tego pojęcia, niemniej jednak wskazuje na kluczowe elementy — jest to m.in. ochrona podstawowych funkcji państwa oraz zapobieganie działalności mogącej poważnie zdestabilizować jego kluczowe elementy składowe, jak struktury konstytucyjne, polityczne czy społeczne.

Mając na uwadze powyższą definicję, ochronę informacji niejawnych należy zaliczyć do spraw mieszczących się w kategorii pojęcia bezpieczeństwa narodowego. Działania uprawnionych organów w tym zakresie mają na celu ochronę podstawowych funkcji państwa, spełnione jest również kryterium możliwości poważnej destabilizacji kluczowych elementów państwa w razie ich nieuprawnionego ujawnienia.

Zadania ABW oraz wybrane instrumenty ich realizacji w obszarze ochrony informacji niejawnych wynikające z ustawy o ABW

Ustawowe zadania ABW w obszarze ochrony informacji niejawnych wynikają z art. 5 ust. 1 pkt 2 lit. a ustawy, zgodnie z którym do zadań ABW należy rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa, terroryzmu, bezprawnego ujawnienia informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa.

Ponadto ochrona informacji niejawnych jest również powiązana z zadaniami ABW o charakterze systemowym, wynikającymi z art. 5 ust. 1 pkt 1 ustawy. Zgodnie z tym przepisem do zadań ABW należy rozpoznawanie, zapobieganie

i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa.

Bezprawne ujawnienie informacji niejawnych jest ściśle związane z działalnością obcych służb specjalnych. Działalność ta może być prowadzona na wielu płaszczyznach (np. w sferze gospodarczej, politycznej czy militarnej) oraz z wykorzystaniem różnorodnych instrumentów (np. pozyskiwanie informacji od źródeł osobowych czy wywiad elektroniczny). Należy w tym miejscu podkreślić, iż działania mające na celu uzyskanie informacji niejawnych innego państwa nie jest wyłącznym celem aktywności służb innych państw — może ona również polegać na prowadzeniu wywiadu jawnoźródłowego (tzw. białego wywiadu) czy też na uzyskiwaniu informacji niepodlegających żadnemu szczególnemu reżimowi ochrony, pozornie niemających związku z bezpieczeństwem państwa, które w powiązaniu z innymi danymi pozwalają na uzyskanie szczegółowej wiedzy o istotnych z punktu widzenia bezpieczeństwa, obronności czy gospodarki aspektach funkcjonowania innego państwa. Bezprawne ujawnienie informacji niejawnych stanowi zatem kwalifikowaną formę zagrożeń związanych z działalnością obcych służb specjalnych.

Zgodnie z systematyką wynikającą z art. 21 ustawy w granicach zadań, o których mowa w art. 5 ust. 1, funkcjonariusze ABW wykonują następujące rodzaje czynności:

1. operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców;
2. operacyjno-rozpoznawcze i analityczno-informacyjne w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego.

ABW wykonuje również czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie postępowania karnego oraz Kodeksie karnym wykonawczym (art. 21 ust. 2).

Precyzyjne zdefiniowanie roli ABW w obszarze ochrony informacji niejawnych wymaga określenia, które z przewidzianych w ustawie instrumentów, służących realizacji ustawowych zadań tego organu, mogą być wykorzystywane do celów związanych z rozpoznawaniem, zapobieganiem i wykrywaniem przestępstwa bezprawnego ujawnienia informacji niejawnych — zadanie ABW wynikające z art. 5 ust. 1 pkt 2 lit. a ustawy. Analiza przepisów ustawy wskazuje, iż do katalogu tego należą następujące instrumenty:

- a) zastosowanie urządzeń uniemożliwiających telekomunikację

Zgodnie z art. 26 a ustawy w celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1 i 2, Szef ABW może zarządzić o zastosowaniu przez ABW urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez ABW, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Mając na uwadze specyfikę tego instrumentu, należy przyjąć, iż jest on dostosowany w szczególności do zwalczania zagrożeń o charakterze terrorystycznym, np. przez uniemożliwienie wykorzystywania urządzeń telekomunikacyjnych na danym obszarze, co mogłoby mieć związek np. z uzyskaniem przez właściwe organy informacji o planowanym w konkretnym miejscu i czasie ataku terrorystycznym.

W ujęciu teoretycznym możliwa jest również sytuacja, w której wykorzystanie tego rodzaju urządzeń będzie miało na celu np. uniemożliwienie przesłania obcej służbie informacji niejawnych drogą elektroniczną. Niemniej jednak, mając na uwadze specyfikę tego instrumentu, przyjąć należy, iż jego podstawowym celem jest zapobieganie zdarzeniom o charakterze terrorystycznym.

b) kontrola operacyjna oraz pozyskiwanie tzw. metadanych telekomunikacyjnych

Uregulowana w art. 27 ustawy o ABW oraz AW kontrola operacyjna jest kluczowym instrumentem realizacji ustawowych zadań ABW. Z uwagi na fakt, iż wiąże się ona z wysokim stopniem ingerencji w podstawowe prawa i wolności gwarantowane na mocy Konstytucji RP, jej stosowanie możliwe jest wyłącznie po spełnieniu ustawowych przesłanek oraz po wyczerpaniu określonego w wymienionym przepisie trybu.

Zgodnie z art. 27 ust. 1 sąd może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia, zarządzić kontrolę operacyjną — gdy inne środki okazały się bezskuteczne albo będą nieprzydatne — przy wykonywaniu czynności operacyjno-rozpoznawczych podejmowanych przez ABW w celu rozpoznawania, zapobiegania i wykrywania przestępstw, o których mowa m.in. w art. 5 ust. 1 pkt 2 lit. a (bezprawne ujawnienie informacji niejawnych, szpiegostwo oraz terroryzm).

W doktrynie działania te określa się jako zespół niejawnych i niekonwencjonalnych działań prowadzonych przez uprawnione organy w celu uzyskania, sprawdzenia i wykorzystania informacji o pozostających w prawie uzasadnionym zainteresowaniu osobach, miejscach bądź zdarzeniach⁶.

Zamknięty katalog szczegółowych sposobów prowadzenia kontroli operacyjnej zawarty został w art. 27 ust. 6 ustawy — zgodnie z tym przepisem kontrola operacyjna prowadzona jest niejawnie i polega na:

- 1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
- 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
- 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;

⁶ T. Hanausek, *Kryminalistyka, Zarys wykładu*, w: *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Komentarz*, red. B. Opaliński, M. Rogalski, P. Szustakiewicz, Legalis, Kraków 2005.

- 4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
- 5) uzyskiwaniu dostępu i kontroli zawartości przesylek.

Zastosowanie wskazanych powyżej instrumentów pozwala na precyzyjne odtworzenie zachowań osoby objętej kontrolą. W kontekście rozpoznawania i zwalczania przestępstw polegających na bezprawnym ujawnieniu informacji niejawnych kontrola operacyjna umożliwi przede wszystkim ustalenie, czy w danej sytuacji doszło faktycznie do ujawnienia informacji niejawnych przedstawicielowi obcej służby, czy też doszło do przekazania innych danych, co samo w sobie może wypełniać znamiona przestępstwa szpiegostwa, niemniej jednak nie będzie stanowiło przestępstwa bezprawnego ujawnienia informacji niejawnych.

Zastosowanie kontroli operacyjnej w kontekście realizacji zadań związanych z ochroną informacji niejawnych należy traktować jako finalny etap procesu działań operacyjno-rozpoznawczych związanych z wykryciem powiązań określonych osób z przedstawicielami zagranicznych służb specjalnych. Instrument ten należy traktować jako środek komplementarny w stosunku do pozyskiwania przez ABW tzw. metadanych zgodnie z art. 28 ustawy.

Zgodnie z tym przepisem ABW może uzyskiwać dane niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1, niestanowiące treści przekazu telekomunikacyjnego, określone w art. 180 c i 180 d ustawy z dnia 16 lipca 2004 r. — *Prawo telekomunikacyjne* (Dz.U. 2021, poz. 576).

Zgodnie z zawartym w art. 180 c katalogiem obowiązkami zatrzymywania danych, wynikającym z art. 180 a ust. 1, objęte są dane niezbędne do:

- 1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
 - a) inicjującego połączenie,
 - b) do którego kierowane jest połączenie;
- 2) określenia:
 - a) daty i godziny połączenia oraz czasu jego trwania,
 - b) rodzaju połączenia,
 - c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Art. 180 d zobowiązuje z kolei przedsiębiorców telekomunikacyjnych do zapewnienia warunków dostępu i utrwalania oraz udostępniania uprawnionym podmiotom, a także sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3–5 (dane objęte tajemnicą telekomunikacyjną), 161 (warunki przetwarzania danych osobowych) oraz 179 ust. 9 (dane z elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci).

Kontrola operacyjna oraz uzyskiwanie metadanych telekomunikacyjnych w kontekście zwalczania zagrożeń związanych z bezprawnym ujawnieniem informacji niejawnych należy traktować jako instrumenty mogące przyczynić się do ich neutralizacji na różnych etapach rozwoju tych zagrożeń. Wykorzystanie

metadanych może przyczynić się do ustalenia faktu utrzymywania przez określoną osobę kontaktów z przedstawicielami służb obcych państw, niemniej jednak nie pozwalają one na określenie dokładnego charakteru tych relacji ani ewentualnie rodzaju przekazywanych im informacji. Z tego względu kontrola operacyjna powinna w tym przypadku pełnić rolę instrumentu o charakterze subsydiarnym, stosowanego wówczas, gdy wykorzystanie innych metod nie pozwala na jednoznaczne określenie, czy w danym przypadku doszło do bezprawnego ujawnienia lub wykorzystania informacji niejawnych.

Zadania ABW oraz SKW w sferze ochrony informacji niejawnych w wymiarze międzynarodowym

Krajowa władza bezpieczeństwa

Podział kompetencji ABW i SKW w obszarze ochrony informacji niejawnych wynika z art. 10 u. inf. niejaw. Zgodnie z art. 10 ust. 1, ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości, określonej w ust. 2 i 3 tego przepisu:

- 1) prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
- 2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
- 3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;
- 4) zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską i innymi państwami lub organizacjami międzynarodowymi;
- 5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

U. inf. niejaw. wprowadziła wyraźne rozgraniczenie kompetencji ABW i SKW w obszarze ochrony informacji niejawnych — SKW realizuje zadania w odniesieniu do Ministerstwa Obrony Narodowej i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej, ataszatów obrony w placówkach zagranicznych oraz żołnierzy w służbie czynnej, wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione powyżej (art. 10 ust. 2).

ABW realizuje z kolei zadania w sferze ochrony informacji niejawnych w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, które nie zostały wymienione w art. 10 ust. 2.

W ujęciu ogólnym należy zatem uznać, iż właściwość ABW obejmuje sferę cywilną, zaś właściwość SKW dotyczy sfery wojskowej.

Jednoznaczne zdefiniowanie właściwości tych organów miało na celu uniknięcie występujących w czasie obowiązywania poprzedniej ustawy o ochronie informacji niejawnych sporów kompetencyjnych między tymi organami, prowadzących np. do sytuacji równoległego prowadzenia czynności z zakresu ochrony informacji niejawnych w stosunku do tego samego podmiotu. Zabieg ten należy uznać za korzystny z punktu widzenia pewności prawa oraz stabilizacji zakresu praw i obowiązków podmiotów objętych u. inf. niejaw. — ewentualne naruszenie

przepisów o właściwości stanowi kwalifikowaną wadę decyzji administracyjnej, stanowiącą przesłankę jej nieważności (art. 156 § 1 pkt 1 KPA)⁷.

Niezależnie od problemów związanych z zakresem właściwości ABW i SKW, z punktu widzenia problematyki prezentowanej w niniejszym rozdziale najbardziej istotnym przepisem kompetencyjnym jest art. 10 ust. 1 pkt 4 u. inf. niejaw., zgodnie z którym organy te zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi.

Zgodnie z art. 11 ust. 1 u. inf. niejaw. funkcję krajowej władzy bezpieczeństwa pełni Szef ABW. Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego (NATO), Unii Europejskiej lub innym organizacjom międzynarodowym, które ustawodawca określa mianem informacji niejawnych międzynarodowych (art. 11 ust. 2).

W odniesieniu do podmiotów należących do sfery wojskowej, wymienionych w art. 10 ust. 2, Szef ABW pełni funkcję krajowej władzy bezpieczeństwa za pośrednictwem Szefa SKW (art. 11 ust. 3).

Rozwiązanie polegające na utworzeniu jednej krajowej władzy bezpieczeństwa jest odmienne od modelu przyjętego na gruncie poprzedniej u. inf. niejaw. — zgodnie z jej art. 15 funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych pełnił Szef ABW oraz Szef SKW.

Utworzenie jednolitej krajowej władzy bezpieczeństwa związane było z koniecznością dostosowania systemu ochrony informacji niejawnych do standardów UE oraz NATO — w państwach należących do tych organizacji dominującym modelem jest powierzenie tej funkcji jednemu organowi odpowiadającemu w sposób kompleksowy za ochronę informacji otrzymywanych od innych państw czy organizacji międzynarodowych oraz za współpracę z nimi. Wprowadzenie modelu jednolitej krajowej władzy bezpieczeństwa prowadzić miało również do ułatwienia bieżącej współpracy z partnerami zagranicznymi oraz do wprowadzenia jednolitych standardów w zakresie informacji niejawnych wymienianych z organizacjami międzynarodowymi czy też z innymi państwami w ramach współpracy bilateralnej⁸.

Uregulowania odnoszące się do sposobu funkcjonowania oraz zadań krajowej władzy bezpieczeństwa w ramach NATO zawarte zostały w dokumencie C-M (2002) 49 z dnia 17 czerwca 2002 r. Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego (*Security within the North Atlantic Treaty Organization*) wraz ze zmianami wynikającymi z dokumentu C-M (2002) 49-REV 1 z 20 listopada 2020 r. Dokument ten ustanawia podstawowe zasady i minimalne standardy bezpieczeństwa, które mają być stosowane przez Państwa

⁷ I. Stankowska, *Komentarz...*, s. 46–47.

⁸ Tamże, s. 51.

Członkowskie NATO oraz organy cywilne i wojskowe tej organizacji w celu zapewnienia tego samego poziomu ochrony informacji niejawnych.

Zgodnie z art. 2 dokumentu Państwa Członkowskie NATO zobowiązują się do utworzenia krajowej władzy bezpieczeństwa (*National Security Authority*), odpowiedzialnej za wdrożenie odpowiednich środków zapewniających bezpieczeństwo informacji niejawnych przetwarzanych w związku ze współpracą w ramach tej organizacji.

Zadania krajowej władzy bezpieczeństwa wymienione zostały w załączniku B do wspomnianego dokumentu. Punkt 3 załącznika B zawiera powtórzenie zobowiązania Państw Członkowskich NATO do utworzenia krajowej władzy bezpieczeństwa odpowiedzialnej za ochronę informacji niejawnych NATO. Organ ten pełni funkcję głównego punktu kontaktowego dla Biura Bezpieczeństwa NATO (*NATO Office of Security — NOS*) w zakresie wszystkich spraw dotyczących bezpieczeństwa w ramach NATO.

Katalog zadań krajowej władzy bezpieczeństwa zawarty został w punkcie czwartym załącznika B, zgodnie z którym organ ten jest odpowiedzialny za:

- a) bezpieczeństwo informacji niejawnych NATO przetwarzanych przez organy krajowe, zarówno wojskowe, jak i cywilne, w kraju i za granicą;
- b) prowadzenie okresowych inspekcji środków bezpieczeństwa mających na celu zapewnienie ochrony informacji niejawnych NATO wprowadzonych przez organy krajowe, na wszystkich szczeblach, zarówno w sferze cywilnej, jak i wojskowej, w celu zapewnienia, iż są one chronione w sposób zgodny z wymogami NATO. W przypadku organów posiadających dostęp do informacji oznaczonych klauzulami CTS lub ATOMAL inspekcje odbywają się co najmniej raz na 24 miesiące, chyba że w tym okresie zostaną one przeprowadzone przez Biuro Bezpieczeństwa NATO;
- c) zapewnienie, iż dokument *Personnel Security Clearance* (PSC)⁹ został wydany wszystkim obywatelom danego państwa, których obowiązki służbowe wymagają dostępu do informacji oznaczonych klauzulą *NATO COFIDENTIAL* lub wyższą, zgodnie z Polityką Bezpieczeństwa NATO (*NATO Security Policy*);
- d) zapewnienie opracowania odpowiednich planów bezpieczeństwa, mających na celu zapobieżenie uzyskaniu dostępu do informacji niejawnych NATO przez osoby nieuprawnione w razie sytuacji kryzysowej;
- e) wyrażenie zgody na utworzenie lub likwidację krajowych rejestrów informacji oznaczonych jako COSMIC. Krajowa władza bezpieczeństwa informuje Biuro Bezpieczeństwa NATO o utworzeniu oraz likwidacji tych rejestrów.

Podsumowując, Szef ABW, pełniący funkcję krajowej władzy bezpieczeństwa, jest organem odpowiedzialnym za sprawowanie kompleksowego nadzoru

⁹ Zgodnie z definicją dokumentu PSC, zawartą w pkt 2 załącznika C — Bezpieczeństwo osobowe (*Personnel Security*) stanowi formalne potwierdzenie krajowej władzy bezpieczeństwa, lub innego właściwego organu, zdolności danej osoby do dostępu do informacji niejawnych NATO o klauzuli *NATO CONFIDENTIAL* lub wyższej.

nad systemem ochrony informacji niejawnych w stosunkach z innymi państwami oraz organizacjami międzynarodowymi.

Przyznanie Szefowi ABW funkcji krajowej władzy bezpieczeństwa postrzegać należy jako jeden z aspektów realizacji rozumianych w sposób szeroki zadań o charakterze kontrwywiadowczym. W tym kontekście należy uznać, iż rola Szefa ABW nie sprowadza się wyłącznie do zapewnienia odpowiedniego poziomu ochrony informacji niejawnych wytwarzanych przez organy polskie, lecz ma na celu zapewnienie bezpieczeństwa informacji niejawnych innych państw oraz organizacji międzynarodowych, przede wszystkim NATO.

Przypisanie wspomnianej roli Szefowi ABW stanowi swego rodzaju rozszerzenie ustawowej roli ABW jako organu odpowiedzialnego za zapewnienie bezpieczeństwa wewnętrznego państwa. Ograniczenie ustawowego zakresu kompetencji ABW wyłącznie do działań podejmowanych na terenie RP wynika z art. 5 ust. 2, zgodnie z którym jej działalność poza granicami Rzeczypospolitej Polskiej może być prowadzona w związku z jej działalnością na terytorium państwa wyłącznie w zakresie realizacji zadań określonych w art. 5 ust. 1 pkt 2.

Sprawowanie funkcji krajowej władzy bezpieczeństwa nie stanowi co prawda *per se* działalności poza granicami RP, o której mowa w przywołanym przepisie, niemniej jednak stanowi ona wyjątek od zasady, w myśl której ABW nie działa co do zasady poza granicami państwa, jest organem o charakterze *stricte* wewnętrznym, a podjęcie współpracy z podmiotami zewnętrznymi — właściwymi organami i służbami innych państw — może nastąpić wyłącznie po uzyskaniu zgody Prezesa Rady Ministrów.

Powierzenie Szefowi ABW funkcji krajowej władzy bezpieczeństwa wynika z art. 11 u. inf. niejaw. oraz z art. 5 ust. 1 pkt 3 ustawy o ABW oraz AW. W tym kontekście charakterystyczny jest swoisty brak spójności pomiędzy art. 8 ustawy o ABW oraz AW, regulującym kwestie współpracy międzynarodowej, a art. 11 u. inf. niejaw. Pierwszy z tych przepisów *expressis verbis* dopuszcza możliwość podejmowania współpracy wyłącznie z organami i służbami innych państw po uzyskaniu zgody Prezesa Rady Ministrów, pomijając tym samym organizacje międzynarodowe.

Z drugiej strony, sprawowanie funkcji krajowej władzy bezpieczeństwa w sposób naturalny wiąże się z koniecznością współdziałania z właściwymi organami NATO czy UE, jak wskazano chociażby w przywołanym dokumencie NATO C-M (2002) 49.

Wykładnia funkcjonalna powyższych przepisów powinna prowadzić do wniosku, iż mają one charakter rozłączny — zadania związane ze sprawowaniem funkcji krajowej władzy bezpieczeństwa wynikające z u. inf. niejaw. mają charakter autonomiczny w stosunku do przepisów ustawy o ABW oraz AW, regulujących warunki oraz sposób prowadzenia współpracy międzynarodowej. Niemniej jednak, mając na uwadze spójność przepisów ustawy o ABW oraz AW i u. inf. niejaw., korzystne byłoby dokonanie zmian w art. 8 ustawy o ABW oraz AW przez dodanie przepisu przewidującego możliwość współpracy Szefa ABW z organizacjami międzynarodowymi, co stanowiłoby swego rodzaju łącznik między omawianymi przepisami.

Charakterystyczne jest, iż ograniczenie podmiotów zagranicznych, z którymi ustawodawca dopuszcza prowadzenie współpracy, nie ma zastosowania w przypadku Centralnego Biura Antykorupcyjnego — zgodnie z art. 2 ust. 2 ustawy o CBA Szef CBA, w celu realizacji zadań CBA, może podejmować współpracę z właściwymi organami i służbami innych państw oraz organizacjami międzynarodowymi.

Biorąc pod uwagę fakt powierzenia Szefowi ABW funkcji krajowej władzy bezpieczeństwa, zawarcie przepisu dopuszczającego możliwość współpracy z organizacjami międzynarodowymi w ustawie o CBA i brak tego rodzaju przepisu w ustawie o ABW oraz AW może budzić wątpliwości. O ile, jak wskazano powyżej, zadania w tym obszarze należy traktować jako mające charakter autonomiczny w stosunku do przepisów ustawy o ABW oraz AW, regulujących współpracę międzynarodową, o tyle przyznanie CBA uprawnienia do prowadzenia tego rodzaju współpracy z organizacjami międzynarodowymi i brak analogicznego przepisu w ustawie o ABW oraz AW jest nieuzasadnione, zważywszy na charakter zadań realizowanych przez te organy.

Aspekty prawnomiędzynarodowe wymiany informacji niejawnych — umowy o wzajemnej ochronie i wymianie informacji niejawnych

Prowadzenie współpracy międzynarodowej w obszarze wymiany informacji niejawnych wymaga stworzenia podstaw formalnoprawnych, które umożliwią określenie zasad, na podstawie których prowadzona będzie wymiana informacji niejawnych. Instrumentem prawnym służącym prowadzeniu takiej współpracy przez Rząd Rzeczypospolitej Polskiej ze swoimi zagranicznymi odpowiednikami są umowy międzynarodowe.

Należy również wskazać, że właściwość Szefa ABW w zakresie czynności związanych z zawieraniem umów międzynarodowych, dotyczących wzajemnej ochrony i wymiany informacji niejawnych, wynika z następujących przepisów:

- art. 5 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz.U. 2020, poz. 127 z późn. zm.) — minister kierujący działem administracji rządowej właściwy do spraw, których dotyczy umowa międzynarodowa, po uzgodnieniu projektu umowy i instrukcji negocjacyjnej z ministrem właściwym do spraw zagranicznych oraz z innymi zainteresowanymi ministrami, składa Prezesowi Rady Ministrów wniosek o udzielenie zgody na rozpoczęcie negocjacji umowy międzynarodowej. Przepisy ustawy odnoszące się do ministra stosuje się odpowiednio do kierownika centralnego organu administracji rządowej (art. 4 ustawy);
- art. 5 ust. 1 pkt 3 ustawy o ABW oraz AW — do zadań ABW należy realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;
- art. 11 ust. u. inf. niejaw. — Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Biorąc pod uwagę powyższe podstawy prawne, należy wskazać na kilka istotnych aspektów związanych z międzynarodową wymianą informacji niejawnych prowadzoną na podstawie umów międzynarodowych. Wymiana ta możliwa jest na podstawie różnych rodzajów umów międzynarodowych, które w zależności od zakresu przedmiotowego oraz podmiotowego mogą regulować całościowo lub fragmentarycznie międzynarodową wymianę informacji niejawnych. W odniesieniu do wymienionych rodzajów umów międzynarodowych w pierwszej kolejności należy wspomnieć, że zasadniczo wymiana i ochrona wzajemnie wymienianych informacji niejawnych powinna się odbywać na podstawie kompleksowych umów międzynarodowych o wzajemnej ochronie informacji niejawnych, które są procedowane w oparciu o regulacje wynikające z *ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych*¹⁰. Istotnym elementem tych umów jest fakt, iż podlegają one procedurze ratyfikacji. Ponadto mogą być umowami kompleksowymi regulującymi, co do zasady, zarówno sferę „cywilną”, jak i sferę „wojskową”, jak również mogą być ograniczone w swoim zakresie podmiotowym, np. wyłącznie do sfery „wojskowej” wymiany informacji niejawnych. Szczegółowe informacje o konstrukcji prawnej wymienionych umów międzynarodowych, ich procedowaniu, jak również o poszczególnych regulacjach prawnych zostaną przedstawione w dalszej części niniejszego rozdziału.

Jednakże warto zaznaczyć, że oprócz kompleksowych umów międzynarodowych, dedykowanych wzajemnej ochronie informacji niejawnych, regulacje odnoszące się do ochrony informacji niejawnych występują również w innych umowach międzynarodowych. Przykładem takich umów odnoszących się do przedmiotowej kwestii są umowy międzynarodowe o współpracy w zwalczaniu przestępczości zorganizowanej. Rząd Rzeczypospolitej Polskiej od lat 90. XX w. zawarł kilkadziesiąt takich umów, których głównym celem jest rozwój współpracy wobec wzrostu przestępczości, szczególnie jej zorganizowanych form oraz wzmocnienie w powyższym kontekście współpracy organów ochrony bezpieczeństwa porządku publicznego w celu skutecznego zwalczania przestępczości. Należy też zauważyć, że po stronie polskiej wśród organów właściwych do współpracy zazwyczaj znajdują się następujące podmioty: minister właściwy do spraw wewnętrznych, minister właściwy do spraw instytucji finansowych, minister właściwy do spraw finansów publicznych, Szef Agencji Bezpieczeństwa Wewnętrznego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Generalny Inspektor Informacji Finansowej¹¹. Strona partnerska wskazuje zwykle odpowiedniki organów polskich, zgodnie z własnym uznaniem i prawem krajowym. Oprócz wymiany informacyjnej dla celów zwalczania przestępczości

¹⁰ Dz.U. 2020, poz. 127.

¹¹ Por. z Umową między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o współpracy w zakresie zwalczania przestępczości zorganizowanej i innych rodzajów przestępczości, podpisaną w Brasiliu dnia 9 X 2006 r. (Dz.U. 2016, poz. 1323) oraz z Umową zawartą między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o współpracy w zwalczaniu przestępczości zorganizowanej oraz innego rodzaju przestępczości, podpisaną w Warszawie dnia 7 XI 2011 r. (Dz.U. 2017, poz. 1609).

istotą przedmiotowej współpracy jest możliwość wspólnego podejmowania różnych form współpracy operacyjnej, mającej na celu usprawnienie współpracy w zwalczaniu przestępczości. Powyższe działania, z uwagi na ich specyfikę, wymagają wymiany informacji niejawnych, dlatego umowy te (zawierane co do zasady na szczeblu rządowym oraz podlegające procedurze ratyfikacyjnej) zawierają regulacje dedykowane zasadom ochrony informacji niejawnych.

Należy dodać, że wraz z rozwojem tego rodzaju umów międzynarodowych, wynikającym z upływu czasu, nowych zagrożeń i okoliczności, wspomniane umowy również ewoluowały, a wraz z nimi także regulacje odnoszące się do ochrony informacji niejawnych. Takie regulacje w tego rodzaju umowach, które zawierano w okresie wcześniejszym, obejmowały bardzo podstawowe zobowiązanie właściwych organów stron do zapewnienia ochrony przekazywanych sobie wzajemnie informacji niejawnych. Ponadto w tego rodzaju przepisach znajdowała się także np. tzw. tabela ekwiwalentności klauzul tajności, która zawierała poszczególne klauzule tajności nadawane informacjom niejawnym oraz ich odpowiedniki w państwie drugiej strony. Regulacje te uwzględniają również zasadę, zgodnie z którą wszelkie informacje niejawne, przekazane przez właściwy organ jednej strony właściwemu organowi drugiej strony, mogą być udostępnione innym podmiotom niż wymienione w umowie oraz podmiotom państw trzecich, właściwym w sprawach ochrony bezpieczeństwa i porządku publicznego, wyłącznie za zgodą właściwego organu strony przekazującej. Ponadto, w wypadku narażenia na ujawnienie lub ujawnienia informacji niejawnych przekazywanych przez właściwy organ jednej strony, właściwy organ strony przyjmującej jest zobowiązany powiadomić niezwłocznie o tym zdarzeniu właściwy organ strony przekazującej, jednocześnie właściwy organ strony przyjmującej jest zobligowany poinformować właściwy organ strony przekazującej o okolicznościach zdarzenia i jego skutkach oraz działaniach podjętych w celu zapobieżenia występowaniu w przyszłości tego rodzaju zdarzeń¹².

Z biegiem czasu zakres przedmiotowy wspomnianych regulacji o ochronie informacji niejawnych w umowach o współpracy w zwalczaniu przestępczości został rozszerzony i w aktualnie procedowanych umowach (które nie weszły jeszcze w życie, ale są procedowane) projekt takich regulacji obejmuje swym zakresem następujące kwestie:

- 1) zobowiązanie do uregulowania kwestii ochrony informacji niejawnych wymienianych między właściwymi organami stron docelowo w odrębnej umowie, przy jednoczesnym zastrzeżeniu, iż do czasu jej wejścia w życie do ochrony informacji niejawnych stosuje się zasady określone w niniejszej umowie;
- 2) doprecyzowanie trybu wymiany informacji niejawnych, przez wskazanie, że w ramach współpracy w zakresie realizacji postanowień niniejszej umowy, właściwe organy stron mogą wymieniać informacje niejawne bezpośrednio;

¹² Por. np. z art. 13 Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o współpracy w zwalczaniu przestępczości, podpisanej w Dubrowniku dnia 9 VII 2010 r. (Dz.U. 2015, poz. 400).

- 3) zapewnienie przez właściwe organy stron co najmniej takiej samej ochrony wymienianym lub wytworzonym w wyniku ich wspólnej działalności informacjom niejawnym, niezależnie od ich formy, nośnika i sposobu utrwalenia, w tym również przedmiotom lub dowolnym ich częściom także w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem, jaka obowiązuje na podstawie prawa wewnętrznego strony, która je otrzymała;
- 4) wskazanie w umowie tabeli ekwiwalentności klauzul tajności w państwach stron oraz zobowiązanie stron do traktowania określonych w tej tabeli klauzul tajności jako równorzędnych;
- 5) wskazanie, że dostęp do informacji niejawnych, przekazanych przez właściwy organ drugiej strony, przyznawany jest wyłącznie osobom upoważnionym do dostępu do informacji niejawnych o określonej klauzuli tajności zgodnie z prawem wewnętrznym strony, która je otrzymała;
- 6) określenie, że powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem wewnętrznym każdej ze stron, a powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczba kopii i tłumaczeń jest natomiast ograniczona do liczby wymaganej dla celów służbowych;
- 7) wskazanie, że informacje niejawne o klauzuli „ściśle tajne” są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ strony, która je przekazała;
- 8) zobowiązanie, że informacje niejawne są niszczone zgodnie z prawem wewnętrznym strony, która je otrzymała, w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie, a informacje niejawne o klauzuli „ściśle tajne” nie są niszczone, gdyż są one zwracane właściwemu organowi strony, która je przekazała;
- 9) wskazanie, że właściwy organ, który otrzymał informacje niejawne od właściwego organu drugiej strony wykorzystuje je wyłącznie w celach, dla których zostały one przekazane;
- 10) zobowiązanie, że informacje niejawne, przekazane przez właściwy organ jednej strony, mogą być udostępnione innym podmiotom niż wymienione w umowie oraz podmiotom państw trzecich wyłącznie za zgodą właściwego organu strony, która przekazuje informacje niejawne;
- 11) określenie standardów postępowania w przypadku naruszenia zasad bezpieczeństwa dotyczących informacji niejawnych, w tym ujawnienia lub narażenia na ujawnienie przekazanych informacji niejawnych, przez wskazanie, że właściwy organ strony, która je otrzymała, zgodnie z prawem wewnętrznym powiadomi właściwy organ drugiej strony o takim zdarzeniu, jego okolicznościach i skutkach oraz działaniach podjętych w celu zapobieżenia występowaniu w przyszłości tego rodzaju zdarzeń, ponadto wskazano, że każdy przypadek narażenia na ujawnienie lub ujawnienia informacji niejawnych będzie wyjaśniany zgodnie z prawem wewnętrznym strony, na terytorium której zdarzenie miało miejsce.

Należy jednocześnie pamiętać, że w sytuacji, w której z danym państwem jest procedowana umowa o współpracy w zwalczaniu przestępczości,

a wcześniej została już zawarta i obowiązuje między tymi samymi stronami umowa o wzajemnej ochronie informacji niejawnych, pożądanym jest, aby w umowie o współpracy w zwalczaniu przestępczości został umieszczony przepis o ochronie informacji niejawnych, który w tej kwestii odsyła do właściwej przedmiotowo umowy o wzajemnej ochronie informacji niejawnych.

Istotnym problemem, jaki pojawił się w toku praktyki i stosowania wymienionych umów o współpracy w zwalczaniu przestępczości oraz umów o wzajemnej ochronie informacji niejawnych, jest wątpliwość, czy w przypadku gdy organy właściwe, na podstawie umowy o współpracy w zwalczaniu przestępczości (zasadniczo chodzi o organy ochrony bezpieczeństwa i porządku publicznego, a w szczególności Komendanta Głównego Policji i Komendanta Głównego Straży Granicznej), do prowadzenia współpracy ze swoimi odpowiednikami drugiej strony (np. w zakresie współpracy operacyjnej), która wymaga wymiany informacji niejawnych, są zobligowane zastosować się do postanowień umów o wzajemnej ochronie informacji niejawnych (w kwestii ochrony informacji niejawnych), czy może przyjąć, iż te organy ochrony bezpieczeństwa i porządku publicznego są uprawnione do bezpośredniej wymiany informacji niejawnych, czy też powinny stosować tryb określony w umowie o wzajemnej ochronie informacji niejawnych. Należy wspomnieć, że przekazywanie informacji niejawnych w oparciu o tryb określony w wymienionej umowie odbywa się, co do zasady, drogą dyplomatyczną, z uwzględnieniem możliwości przekazywania informacji niejawnych za pomocą systemów bezpiecznej łączności, sieci lub innych środków elektromagnetycznych dopuszczonych do użytku zgodnie z prawem krajowym stron. Krajowe władze bezpieczeństwa poinformują się wzajemnie o zatwierdzonych systemach. W przypadku informacji niejawnych o klauzuli „zastrzeżone” mogą być one przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem krajowym strony wytwarzającej. Wobec powyższego, w drodze wzajemnych ustaleń między przedstawicielami Szefa ABW jako krajowej władzy bezpieczeństwa oraz przedstawicielami Ministra Spraw Wewnętrznych i Administracji (jako podmiotu wiodącego w zakresie procedowania umów o współpracy w zakresie zwalczania przestępczości) przyjęto, że z uwagi na istotę oraz praktykę w zakresie współpracy, np. operacyjnej, prowadzonej przez organy ochrony bezpieczeństwa i porządku publicznego, na podstawie umów o współpracy w zwalczaniu przestępczości, organy te są uprawnione do wymiany informacji niejawnych bezpośrednio (z ich zagranicznymi odpowiednikami wskazanymi w poszczególnych umowach). Takie rozwiązanie znalazło swoje potwierdzenie we wszystkich nowo procedowanych umowach o wzajemnej ochronie informacji niejawnych, w których znajduje się przepis, w podstawie którego organy bezpieczeństwa i porządku publicznego stron mogą wymieniać informacje niejawne bezpośrednio, w razie takiej konieczności¹³.

¹³ Tytułem przykładu można wskazać art. 8 ust. 5 obowiązującej Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o wzajemnej ochronie informacji niejawnych, podpisanej w Warszawie dnia 27 XI 2018 r. (Dz.U. 2019, poz. 2040).

Innym przykładem umów międzynarodowych, które w swym zakresie przedmiotowym również odnoszą się do ochrony informacji niejawnych, są umowy międzynarodowe w dziedzinie obronności procedowane przez Ministra Obrony Narodowej jako podmiot wiodący. W tych umowach zasadniczo znajduje się przepis dedykowany ochronie informacji niejawnych, jednakże w swej treści stanowi on, że ochrona informacji niejawnych wymienianych między stronami, dotyczących przedmiotu tychże umów, będzie uregulowana w odrębnej umowie¹⁴. Tymi umowami odrębnymi są oczywiście umowy kompleksowe o wzajemnej ochronie informacji niejawnych, które szczegółowo zostaną przedstawione w dalszej części tego tekstu.

Warto zaznaczyć, że warunkiem *sine qua non* rozwoju współpracy politycznej i gospodarczej z innymi państwami jest niejednokrotnie stworzenie odpowiednich podstaw prawnych, regulujących zasady ochrony informacji niejawnych wymienianych w relacjach bilateralnych. Stąd właśnie wynika potrzeba zawierania z poszczególnymi państwami umów międzynarodowych o wzajemnej ochronie informacji niejawnych. Takie umowy regulują swym zakresem przedmiotowym aspekty prawne współpracy właściwych polskich podmiotów z ich zagranicznymi odpowiednikami upoważnionymi, zgodnie ze swoim prawem krajowym, do przetwarzania informacji niejawnych. Takie umowy stanowią podstawę do nawiązania ściślejszej współpracy różnych sektorów gospodarczych poszczególnych krajów, w tym w zakresie obronności i bezpieczeństwa wewnętrznego, zwłaszcza w zwalczaniu najgroźniejszych form przestępczości, oraz przeciwdziałania terroryzmowi. Uregulowanie powyższych kwestii jest przede wszystkim istotne dla rozwoju współpracy gospodarczej, gdyż stworzy polskim i zagranicznym przedsiębiorcom podstawy prawne do zawierania kontraktów, których realizacja wiąże się z dostępem do informacji niejawnych lub wytwarzaniem takich informacji. Wejście w życie umów o wzajemnej ochronie informacji niejawnych otwiera nowe perspektywy dla polskiego przemysłu zbrojeniowego, umożliwiając przedsiębiorcom z tego sektora uczestnictwo w przetargach związanych z dostępem do informacji niejawnych organizowanych w innych krajach, jak również pozwala na udostępnienie oferty rynku zagranicznego Siłom Zbrojnym Rzeczypospolitej Polskiej.

Warto dodać, że umowy o wzajemnej ochronie informacji niejawnych, co do zasady podlegają ratyfikacji. Związanie przedmiotowymi umowami następuje przez ratyfikację w trybie artykułu 89 ustęp 2 Konstytucji RP, zgodnie z postanowieniami artykułu 12 ustęp 2 ustawy o umowach międzynarodowych.

Wybór trybu tzw. małej ratyfikacji poparty jest potrzebą uznania tego rodzaju umów za źródło prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej, gdyż ich postanowienia będą miały zastosowanie do szerokiego kręgu podmiotów (organy administracji państwowej, przedsiębiorcy). W związku

¹⁴ Np. art. 6 Umowy Ramowej między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o dwustronnej współpracy obronnej, podpisanej w Warszawie dnia 1 XII 2010 r. (Dz.U. 2016, poz. 264).

z faktem, iż zgodnie z artykułem 87 ustęp 1 Konstytucji RP źródłem prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej są wyłącznie ratyfikowane umowy międzynarodowe, a nie występują przesłanki ratyfikacji takich umów za uprzednią zgodą wyrażoną w ustawie, związanie Rzeczypospolitej Polskiej przedmiotowymi umowami następuje najczęściej w drodze ratyfikacji bez uprzedniej zgody wyrażonej w ustawie.

Poniżej przedstawiono charakterystykę najważniejszych elementów umów o wzajemnej ochronie i wymianie informacji niejawnych przez pryzmat charakterystycznych elementów preambuły, celów i podstawowych zobowiązań stron (z uwzględnieniem różnic dotyczących umów zawieranych z państwami UE i z pozostałymi państwami, w szczególności w obszarze ochrony danych osobowych), klauzul tajności oraz postanowień dotyczących przetwarzania i wymiany informacji.

Umowy tego rodzaju odpowiadać muszą krajowym regulacjom o ochronie informacji niejawnych — z tego względu dokładny kształt zobowiązań stron, czy też przyjęte definicje, muszą być sformułowane na odpowiednim poziomie ogólności.

Cele umowy oraz podstawowe zobowiązania stron

W większości zawieranych przez Polskę umów o wymianie i wzajemnej ochronie informacji niejawnych określenie przedmiotu umowy oraz podstawowych zobowiązań stron poprzedzone jest preambułą, mającą na celu przedstawienie okoliczności jej zawierania oraz dookreślenie celów przyświecających umowie.

Do najczęściej występujących elementów preambuły zaliczyć należy podkreślenie dążenia do rozwoju współpracy między państwami, dążenie do zapewnienia właściwej ochrony informacjom niejawnym wymienianym na podstawie umowy oraz zastrzeżenie, iż umowa nie narusza właściwych przepisów prawa międzynarodowego ani prawa krajowego stron.

W kontekście rozważań prezentowanych w niniejszym rozdziale należy podkreślić, iż w umowie między RP a Królestwem Szwecji¹⁵ wyrażone zostało *expressis verbis* powiązanie ochrony informacji niejawnych ze sferą bezpieczeństwa narodowego. Zgodnie z preambułą do tej umowy władze RP i Królestwa Szwecji zawierają ją w interesie bezpieczeństwa narodowego, pragnąc zagwarantować wzajemną ochronę wszystkich informacji, które zostały zaklasyfikowane jako informacje niejawne zgodnie z prawem krajowym jednej ze stron i przekazane drugiej stronie, kierując się w tym celu zamiarem stworzenia regulacji w zakresie wzajemnej ochrony informacji niejawnych, które obowiązywać będą w odniesieniu do wszelkiej współpracy dwustronnej związanej z wymianą informacji niejawnych.

¹⁵ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Szwecji o wzajemnej ochronie informacji niejawnych z dnia 6 IX 2007 r. (Dz.U. 2008, poz. 1282).

To, iż interes bezpieczeństwa narodowego zawarty został w preambule do wspomnianej umowy, nie zaś np. w przepisie określającym zobowiązania stron, wynika z faktu, iż pojęcie „bezpieczeństwo narodowe” nie posiada jednolitej definicji ani na gruncie prawa krajowego większości państw, ani też na gruncie prawa międzynarodowego. Odwołanie się do tego pojęcia w preambule świadczy zatem o tym, iż bezpieczeństwo narodowe traktować należy jako pewien ogólny cel, którego realizacji służyć ma zawarcie umowy, nie zaś wyraz konkretnych zobowiązań stron.

Zawarcie w preambule odniesienia do tego pojęcia należy ocenić pozytywnie — materialnym celem zawierania tego rodzaju umów jest stworzenie na płaszczyźnie bilateralnej rozwiązań, pozwalających na skuteczną wymianę informacji niejawnych oraz zobowiązujących strony do zapewnienia właściwego poziomu ich ochrony, co z kolei stanowi jeden z dostępnych poszczególnym państwom instrumentów, mających na celu zapewnienie bezpieczeństwa narodowego.

Zobowiązania stron w większości przypadków polegają na podejmowaniu działań, których celem jest zapewnienie ochrony otrzymanym informacjom niejawnym, co najmniej takiej samej, jaka zagwarantowana jest w odniesieniu do ich własnych informacji niejawnych o równorzędnej klauzuli tajności.

Kolejnym zobowiązaniem stron jest ograniczenie możliwości wykorzystywania informacji niejawnych, uzyskanych na podstawie umowy, wyłącznie w uzgodnionych celach. Umowy tego rodzaju wykluczają również możliwość udostępniania otrzymanych informacji niejawnych stronom trzecim bez uprzedniej zgody właściwego organu drugiej strony (tzw. zasada strony trzeciej).

W przypadku umów zawieranych z Państwami Członkowskimi UE w tego rodzaju umowach nie wprowadza się przepisów regulujących zagadnienie ochrony danych osobowych przetwarzanych w związku z ich wykonywaniem. Ochrona danych osobowych regulowana jest bowiem na poziomie prawa UE przez tzw. RODO (rozporządzenie ogólne o ochronie danych)¹⁶ oraz dyrektywę 2016/680¹⁷.

Postanowienia tego rodzaju niezbędne są z kolei w wypadku umów z państwami niebędącymi członkami UE. Przepisy te dotyczą w szczególności przetwarzania danych osobowych w związku z wizytami przedstawicieli upoważnionych organów państw na terytorium państwa będącego drugą stroną umowy. Tytułem przykładu, zgodnie z art. 10 ust. 4 umowy zawartej między

¹⁶ *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 IV 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)*; Dz.Urz. UE L 119 z 4 V 2016 r., s. 1.

¹⁷ *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 IV 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW*, Dz.Urz. UE L 119 z 4 V 2016 r., s. 89.

Rządem RP a Gabinetem Ministrów Ukrainy¹⁸ do ochrony danych osobowych, przekazywanych w związku z organizacją wizyt, o których mowa powyżej, stosuje się następujące postanowienia:

- dane osobowe przekazane na podstawie tej umowy mogą być wykorzystywane wyłącznie w celu określonym przez upoważniony podmiot je przekazujący i na warunkach określonych przez ten podmiot;
- danych osobowych przekazanych na podstawie tej umowy nie przechowuje się dłużej, aniżeli jest to niezbędne dla osiągnięcia celu przetwarzania;
- w przypadku przekazania danych, których nie wolno było przekazać zgodnie z prawem krajowym państwa strony, upoważniony podmiot przekazujący dane osobowe zawiadamia o tym upoważniony podmiot je otrzymujący, który jest zobowiązany do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;
- upoważniony podmiot przekazujący dane osobowe odpowiada za ich merytoryczną poprawność i jeśli okaże się, że przekazane zostały dane nieprawdziwe lub niekompletne, zawiadamia o tym upoważniony podmiot otrzymujący dane osobowe, który jest zobowiązany do ich sprostowania lub usunięcia;
- upoważnione podmioty przekazujące i otrzymujące dane osobowe są zobowiązane do ich rejestrowania, przekazywania, otrzymywania i usuwania;
- upoważnione podmioty przekazujące i otrzymujące dane osobowe są zobowiązane do skutecznego zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.

Analogiczne postanowienia zawarte zostały m.in. w umowach z Czarnogórą¹⁹, Serbią²⁰, Wietnamem²¹ czy Azerbejdżanem²².

Klauzule tajności

Jedną z najważniejszych zasad wzajemnej ochrony i wymiany informacji niejawnych jest zasada równorzędności klauzul tajności — informacje oznaczone określoną klauzulą tajności są chronione na takich samych zasadach, jak krajowe informacje niejawne drugiej strony, noszące analogiczną klauzulę.

¹⁸ Umowa między Rządem Rzeczypospolitej Polskiej a Gabinetem Ministrów Ukrainy o wzajemnej ochronie informacji niejawnych z dnia 27 VIII 2015 r. (Dz.U. 2017, poz. 81).

¹⁹ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Czarnogóry o wzajemnej ochronie informacji niejawnych z dnia 18 XI 2014 r. (Dz.U. 2016, poz. 246), Legalis.

²⁰ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o wzajemnej ochronie informacji niejawnych z dnia 11 VI 2015 r. (Dz.U. 2016, poz. 795), Legalis.

²¹ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych z dnia 9 IX 2010 r. (Dz.U. 1 III 2012), Lex.

²² Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych z dnia 31 V 2019 r. (Dz.U. 16 III 2020), Lex.

W ujęciu praktycznym określenie wzajemnych relacji między poszczególnymi klauzulami w umowach określane jest w tabeli wskazującej klauzule, które stanowią swoje jednoznaczne odpowiedniki. O ile wskazanie równorzędnych klauzul nie rodzi trudności w procesie zawierania umów z państwami, których przepisy prawa krajowego wyróżniają, podobnie jak u. inf. niejaw., cztery klauzule tajności, o tyle problematyczne może okazać się określenie poziomu ochrony informacji oznaczonych klauzulą niewystępującą w systemie drugiej strony umowy.

Przykładem ilustrującym drugi przypadek, związany z różnicami występującymi w strukturze klauzul tajności umawiających się stron, jest tabela zawarta w art. 3 umowy zawartej między władzami RP i Wielkiej Brytanii²³. Zgodnie z jej art. 3, w rozumieniu niniejszej umowy, niżej wymienione klauzule tajności są równorzędne:

Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej	Rzeczypospolita Polska
<i>UK TOP SECRET</i>	ŚCIŚLE TAJNE
<i>UK SECRET</i>	TAJNE
Brak odpowiednika (patrz część 2 niniejszego rozdziału)	POUFNE
<i>UK OFFICIAL SENSITIVE</i>	ZASTRZEŻONE

Z uwagi na fakt, iż w prawie wewnętrznym Wielkiej Brytanii nie istnieje odpowiednik polskiej klauzuli „poufne”, informacje oznaczone tą klauzulą traktowane są przez stronę brytyjską jako *UK SECRET* (art. 3 ust. 2).

Jeżeli zatem określona klauzula nie posiada odpowiednika w systemie prawnym drugiej strony, to zgodnie z wypracowaną praktyką informacje oznaczone tą klauzulą chronione są tak jak informacje noszące klauzulę o jeden poziom wyższą.

Wymiana oraz przetwarzanie informacji niejawnych

Informacje niejawne wymieniane na podstawie bilateralnych umów o wzajemnej ochronie i wymianie informacji niejawnych przekazywane są co do zasady drogą dyplomatyczną. Niektóre umowy dopuszczają jednak wyjątek od tej zasady — przykładowo, zgodnie z art. 9 umowy z Francją²⁴ zarówno informacje oznaczone klauzulą „ściśle tajne”, jak również „tajne” i „poufne”, w indywidualnych przypadkach, za obopólną zgodą krajowych władz bezpieczeństwa lub właściwych organów bezpieczeństwa stron, możliwe jest ich przekazanie

²³ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o wzajemnej ochronie informacji niejawnych z dnia 18 VIII 2006 r. (Dz.U. 2007, nr 140, poz. 985).

²⁴ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Francuskiej o wzajemnej ochronie informacji niejawnych z dnia 28 V 2008 r. (Dz.U. 2009, poz. 394).

w inny sposób. Warto także dodać, że w „najnowszych” zawieranych umowach międzynarodowych występuje postanowienie (o czym wspomniano wcześniej), że *Organy uprawnione do wymiany informacji niejawnych na podstawie innych umów międzynarodowych, zawartych między Stronami, mogą wymieniać informacje niejawne bezpośrednio*²⁵.

Umowy wprowadzają również wymogi w odniesieniu do możliwości przekazywania informacji niejawnych drogą elektroniczną. Ten sposób przekazywania informacji dopuszczalny jest wyłącznie w formie w pełni zaszyfrowanej, z wykorzystaniem metod szyfrowania oraz urządzeń zatwierdzonych przez właściwe organy stron. Postanowienia tego rodzaju znajdują się m.in. w umowach ze Szwecją, Francją, Finlandią²⁶ czy Włochami²⁷.

W odniesieniu do kwestii związanych z tłumaczeniem, powielaniem czy niszczeniem informacji niejawnych postanowienia omawianych umów w większości wypadków zastrzegają, iż czynności te prowadzone są zgodnie z prawem krajowym strony otrzymującej.

Najdalej idące obostrzenia występują w przypadku dokonywania wymienionych czynności w odniesieniu do informacji oznaczonych klauzulą „ściśle tajne”. Tak np. zgodnie z art. 8 umowy z Austrią²⁸ informacje noszące tę klauzulę są powielane tylko po uprzednim uzyskaniu pisemnej zgody wydanej przez ich wytwórcę. Analogiczne rozwiązanie przyjęto w umowie z Włochami (art. 3 ust. 5), Finlandią (art. 8 ust. 1) czy Portugalią²⁹.

Ponadto informacje oznaczone klauzulą „ściśle tajne” nie podlegają zniszczeniu — są one zwracane stronie przekazującej (art. 6 ust. 3 umowy z Francją, czy art. 8 ust. 5 umowy z Finlandią).

Kolejną zasadą mającą na celu zapewnienie właściwego poziomu ochrony informacji niejawnych, przekazywanych drugiej stronie umowy, jest ograniczenie możliwości ich powielania — liczba kopii powinna być ograniczona do liczby wymaganej dla celów służbowych (art. 7 ust. 2 umowy ze Szwecją, art. 9 ust. 1 umowy z Wielką Brytanią).

²⁵ Por. z art. 8 ust. 6 Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych, podpisanej w Baku dnia 31 V 2019 r. (Dz.U. 2020, poz. 447) LEX.

²⁶ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Finlandii o wzajemnej ochronie informacji niejawnych z dnia 25 V 2017 r. (Dz.U. 2008, poz. 780), Legalis.

²⁷ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Włoskiej w sprawie wzajemnej ochrony informacji niejawnych z dnia 11 II 2005 r. (Dz.U. 2007, nr 30, poz. 196), Legalis.

²⁸ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federalnym Republiki Austrii o wzajemnej ochronie informacji niejawnych z dnia 4 XII 2013 r. (Dz.U. 2014, poz. 1746), Legalis.

²⁹ Umowa między Rzeczpospolitą Polską a Republiką Portugalską o wzajemnej ochronie informacji niejawnych z dnia 2 VIII 2007 r. (Dz.U. 2009, nr 154, poz. 1228), Legalis.

Istotne znaczenie mają przepisy regulujące tryb postępowania w razie naruszenia bezpieczeństwa przez utratę informacji niejawnych lub wystąpienia podejrzenia, iż zostały one ujawnione osobom nieuprawnionym. W takim wypadku właściwy organ bezpieczeństwa strony otrzymującej (w przypadku Polski będzie to Szef ABW, w przypadku innych państw zazwyczaj organ pełniący funkcję krajowej władzy bezpieczeństwa) niezwłocznie zawiadamia właściwy organ strony przekazującej.

W dalszej kolejności właściwe organy strony otrzymującej (w razie potrzeby we współpracy z właściwym organem strony przekazującej) prowadzą czynności mające na celu wyjaśnienie okoliczności sprawy oraz informują stronę przekazującą o ich wynikach, szkodach związanych z naruszeniem bezpieczeństwa oraz środkach zastosowanych w celu ich minimalizacji.

Wnioski końcowe

Umowy o wzajemnej ochronie informacji niejawnych pozostają podstawowym instrumentem współpracy bilateralnej, pozwalającym na prowadzenie efektywnej współpracy w obszarze politycznym, gospodarczym czy ekonomicznym. Ponadto wymiana tego rodzaju informacji możliwa jest również na podstawie umów regulujących inne zagadnienia, w szczególności umowy o współpracy w zwalczaniu przestępczości zorganizowanej.

Wymiana informacji niejawnych może być uregulowana w sposób kompleksowy (na podstawie umów o wzajemnej ochronie informacji niejawnych) bądź w sposób fragmentaryczny, dotyczący określonej sfery współpracy bilateralnej, jak np. w przypadku drugiego rodzaju umów wymienionych powyżej.

Należy podkreślić, iż pożądanymi byłyby, aby RP posiadała umowy międzynarodowe dedykowane wzajemnej ochronie informacji niejawnych z jak największą liczbą państw, z którymi prowadzona jest współpraca międzynarodowa, co pozwoliłoby stworzyć odpowiednie i bezpieczne ramy współpracy w zakresie wymiany i ochrony informacji niejawnych. Praktyka pokazuje, że pomimo prężnych działań ze strony polskiej krajowej władzy bezpieczeństwa nie wszystkie państwa, z którymi RP prowadzi współpracę międzynarodową w omawianym zakresie wykazują odpowiednią determinację, aby takie umowy międzynarodowe zawrzeć. Warto zaznaczyć, iż z każdym rokiem przybywa umów międzynarodowych dotyczących wzajemnej ochrony informacji niejawnych zawieranych przez władze RP, a ponadto umowy zawarte wiele lat temu, które uległy dezaktualizacji, są również zmieniane i dostosowywane do aktualnych standardów prawnych, jak również bieżących potrzeb.

Należy też podkreślić, że centralnym organem odpowiedzialnym za wymianę informacji niejawnych w stosunkach międzynarodowych, zarówno z państwami, jak i organizacjami międzynarodowymi, jest Szef ABW pełniący funkcje krajowej władzy bezpieczeństwa. Kompetencje tego organu w tej sferze wynikają zarówno z ustawy o ABW, jak i z u. inf. niejaw.

Zadania Szefa ABW w omawianym obszarze postrzegać należy jako zadania dotyczące sfery bezpieczeństwa narodowego w szerokim rozumieniu. O ile ochrona informacji niejawnych w wymiarze krajowym jest ściśle powiązana z realizacją zadań o charakterze kontrwywiadowczym, to przypisanie temu organowi funkcji krajowej władzy bezpieczeństwa traktować należy jako rozszerzenie jego ustawowej roli na sferę międzynarodową.

Rola Szefa ABW w sferze międzynarodowej wymiany informacji niejawnych nie ma zatem charakteru wyłącznie pasywnego, ograniczonego jedynie do zapewnienia odpowiedniego poziomu ochrony informacji niejawnych wymienianych z partnerami zagranicznymi. Ma ona charakter aktywny — pozwala na kształtowanie przez ten organ międzynarodowych instrumentów pozwalających na skuteczne przeciwdziałanie zagrożeniom dla bezpieczeństwa narodowego, np. o charakterze terrorystycznym czy wyzwaniom związanym z działalnością obcych służb specjalnych skierowaną przeciw państwom NATO czy UE.

Zważywszy na intensyfikację współpracy z państwami obszaru euroatlantyckiego, należy uznać, iż umowy o wzajemnej ochronie i wymianie informacji niejawnych będą odgrywały coraz istotniejszą rolę, stając się instrumentem mocno wspomagającym prowadzenie polityki zagranicznej oraz pozwalającym na pogłębienie poziomu współpracy z określonymi państwami w obszarze ekonomicznym czy technologicznym.

Roman Brzozowski

Rozdział 6.

Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW

Wstęp do zagadnienia

Punktem wyjścia do rozważań nad zagadnieniem dotyczącym czynności wykonywanych przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, o których mowa w art. 21 ustawy o ABW oraz AW¹, w kontekście zadań ABW, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW, należy, w mojej ocenie, uczynić stwierdzenie, iż zakres uprawnień funkcjonariuszy służb specjalnych wynika przede wszystkim z przyjętego w Polsce modelu służb specjalnych. Wspierając się w tym zakresie dorobkiem piśmiennictwa, przytoczyć trzeba w tym miejscu tezę Martina Bożka² odnoszącą się właśnie do kwestii odpowiedniego klasyfikowania modelu polskich służb specjalnych:

W związku z charakterem zadań i kompetencji służb specjalnych w Polsce i na świecie można mówić o dwóch modelach ich funkcjonowania. Pierwszym, w którym służby specjalne pełnią wyłącznie funkcje informacyjne, a tym samym nie dysponują narzędziami karnej reakcji na jakieś zdarzenie. (...) W drugim modelu funkcje służb specjalnych polegają zarówno na uzyskiwaniu, analizowaniu i przekazywaniu informacji o zagrożeniach, jak i na rozpoznawaniu i wykrywaniu przestępstw oraz ściganiu ich sprawców.

W polskim porządku prawnym normatywne pojęcie „służby specjalne” wynika z art. 11 ustawy o ABW oraz AW, w którym wyodrębniono dwie grupy organów państwowych: te, którym ustawodawca nadaje miano służb specjalnych, tj.: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu,

¹ Dz.U. 2020, poz. 27 z późn. zm.

² M. Bożek, *Współczesny model polskich służb specjalnych. Służby informacyjne czy policyjne?* ZNAON 2005, nr 1, s. 92 i n.

Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego oraz te, którym to miano nie przysługuje. Do tej drugiej grupy służb i instytucji, mogących również podejmować zadania na rzecz ochrony bezpieczeństwa państwa, ale niebędących służbami specjalnymi, zostały zaliczone m.in.: policja, Straż Graniczna, Żandarmeria Wojskowa, Służba Więzienna, Służba Ochrony Państwa, Krajowa Administracja Skarbowa czy służby rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej.

„Ustawy kompetencyjne”³ przed szczegółowym omówieniem uprawnień funkcjonariuszy służb specjalnych wskazują na rodzaje wykonywanych przez nich działań — określanych jako czynności. Służby specjalne, jeśli by rozpatrywać je *in gremio*, mają uprawnienia do stosowania czynności operacyjno-rozpoznawczych, analityczno-informacyjnych, dochodzeniowo-śledczych i kontrolnych. Taki wachlarz stosowanych czynności przysługuje jedynie dwom służbom specjalnym: ABW i CBA. Uprawnienia do stosowania wszystkich czynności, oprócz dochodzeniowo-śledczych, posiada SKW, natomiast służby wywiadowcze (AW i SWW) są uprawnione jedynie do wykonywania czynności operacyjno-rozpoznawczych i analityczno-informacyjnych⁴.

Odnosząc to do wskazanych wyżej modeli funkcjonowania służb specjalnych, należy zauważyć, iż w związku z posiadaniem przez ABW i CBA kompetencji w zakresie ścigania karnego model funkcjonowania obu tych formacji określa się jako model o charakterze mieszanym (informacyjno-policyjnym)⁵. Zatem oprócz zadań typowo informacyjnych przysługują tym służbom kompetencje charakterystyczne dla policyjnych organów śledczych.

Z kolei na gruncie europejskim przykładem praktycznego zastosowania modelu funkcjonowania służby specjalnej o charakterze mieszanym jest francuska odpowiedniczka ABW, tj. Generalna Dyrekcja Bezpieczeństwa Wewnętrznego (*Direction Générale de la Sécurité Intérieure* — DGSI), jedyna francuska służba odpowiedzialna za bezpieczeństwo wewnętrzne państwa. Odpowiada ona za pozyskiwanie, konsolidację i wykorzystywanie informacji istotnych z punktu widzenia bezpieczeństwa narodowego lub fundamentalnych interesów państwa. W zakresie swojej właściwości współpracuje z policją na zasadach określonych w kodeksie postępowania karnego. W celu podkreślenia owego mieszanego (informacyjno-policyjnego) charakteru zadań i kompetencji tej służby warto odwołać się do literatury przedmiotu⁶:

³ Zob.: art. 21 ust. 1 pkt 1 i 2 oraz art. 22 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; art. 13 ust. 1 pkt 1–3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. 2019, poz. 1921 z późn. zm.), art. 25 i art. 26 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2019, poz. 687 z późn. zm.).

⁴ M. Kolaszyński, dz. cyt., s. 129.

⁵ M. Bożek i in., dz. cyt., s. 30.

⁶ P. Burczaniuk i in., *Analiza rozwiązań...*, s. 20–22.

(...) głównym założeniem prac nad utworzeniem DGSI było połączenie elementów służby wywiadowczej z organem dochodzeniowo-śledczym, co w rezultacie miało doprowadzić do stworzenia instytucji zdolnej do prowadzenia kompleksowych, dwutorowych działań zarówno w sferze wywiadowczej, jak i postępowania karnego. DGSI jest jedyną służbą upoważnioną do prowadzenia postępowań przygotowawczych w sprawach o szpiegostwo, bezprawne ujawnienie informacji niejawnych, ataki na System Automatycznego Przetwarzania Danych, ataki wymierzone w sieci teleinformatyczne użytkowane przez organy administracji rządowej oraz przez najważniejszych operatorów sieci komunikacyjnych, a także w sprawach dotyczących działań podejmowanych przeciwko urzędniom znajdującym się w tzw. strefach ograniczonego dostępu. Od 2011 r. (...) służba jako jedyna jest upoważniona do przeciwdziałania proliferacji broni masowego rażenia.

Utworzenie zatem w maju 2014 r. DGSI, z przekształcenia jej w oparciu o wspomniany model informacyjno-policyjny z Centralnej Dyrekcji Wywiadu Wewnętrzznego (*Direction Centrale du Renseignement Intérieur* — DCRI), wskazuje, iż w Europie uprawnienia śledcze mają w swoich kompetencjach nie tylko służby specjalne krajów położonych na wschód od Polski czy też służby amerykańskie, jak Federalne Biuro Śledcze, zaś funkcjonowanie Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego według tego modelu nie stanowi wyjątku w krajach należących do Unii Europejskiej czy Paktu Północnoatlantyckiego.

Pozostałe polskie służby specjalne, tj. AW, SKW oraz SWW, realizujące zadania kontrwywiadowcze i wywiadowcze, są reprezentantami pierwszego ze wspomnianych wyżej modeli funkcjonowania służb specjalnych, których rola polega na identyfikowaniu i monitorowaniu zagrożeń dla bezpieczeństwa państwa i informowaniu o nich najwyższych władz państwowych. Służby te nie realizują zadań polegających na wykrywaniu przestępstw i ściganiu ich sprawców, w konsekwencji zatem nie jest konieczne wyposażenie ich w możliwość stosowania czynności dochodzeniowo-śledczych.

Nawiązując jeszcze do aspektu *stricte* informacyjnego polskich służb specjalnych, wskazać należy, iż realizacja zadań ustawowych przez wszystkie służby specjalne odbywa się w drodze czynności operacyjno-rozpoznawczych i analityczno-informacyjnych, co wynika z poszczególnych ustaw kompetencyjnych. To znaczy, że funkcjonariusze każdej z nich są uprawnieni do ich wykonywania. Zatem:

sকoro realizacja zadań (...) służb specjalnych (...) odbywa się poprzez czynności operacyjno-rozpoznawcze i analityczno-informacyjne, to należy przyjąć, że działania ABW, AW, SKW i SWW ukierunkowane na realizację ich zadań (z wyłączeniem prowadzenia czynności dochodzeniowo-śledczych i działalności w zakresie zadań związanych z ochroną informacji niejawnych) mają albo charakter operacyjno-rozpoznawczy, albo analityczno-informacyjny. *A contrario* co nie jest w działalności

ABW, AW, SKW i SWW pracą analityczno-informacyjną jest działaniem operacyjno-rozpoznawczym (z wyłączeniem czynności dochodzeniowo-śledczych, działań o charakterze administracyjnym, logistycznym typu przetarg w zakresie sprzętu, budowa obiektów, załatwianie spraw kadrowych itp.)⁷.

Po wstępnym zainicjowaniu problematyki polegającym na wskazaniu zależności między przyjętym modelem funkcjonowania służby specjalnej a charakterem realizowanych przez nią zadań oraz zakresem uprawnień przyznanych funkcjonariuszom danej formacji, w dalszej części niniejszego rozdziału zostaną przedstawione w kontekście historycznym regulacje prawne odnoszące się do wymienionych wyżej rodzajów czynności, a następnie czynności funkcjonariuszy ABW w obecnie obowiązującym porządku prawnym, z jednoczesnym ich porównaniem z rozwiązaniami przewidzianymi w innych ustawach kompetencyjnych służb specjalnych.

Analiza historyczna zagadnienia

Z treści art. 6 ust. 1 *ustawy z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych*⁸ wynika, że funkcjonariusze Służby Bezpieczeństwa i Milicji Obywatelskiej w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń oraz innych działań godzących w bezpieczeństwo państwa lub porządek publiczny, wykonują czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-prawne.

Zakres praw i obowiązków funkcjonariuszy Służby Bezpieczeństwa został natomiast określony w art. 20 *ustawy o urzędzie Ministra Spraw Wewnętrznych*, zgodnie z którym przepisy *ustawy o służbie funkcjonariuszy Milicji Obywatelskiej* oraz o zaopatrzeniu emerytalnym funkcjonariuszy Milicji Obywatelskiej i ich rodzin, jak również o odszkodowaniach przysługujących w razie wypadków i chorób pozostających w związku ze służbą w Milicji Obywatelskiej, stosuje się do funkcjonariuszy Służby Bezpieczeństwa.

Zaznaczyć należy, iż na gruncie *ustawy o urzędzie Ministra Spraw Wewnętrznych* wykonywanie czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz administracyjno-prawnych było związane ze sprawami pozostającymi w zakresie działania *Ministra Spraw Wewnętrznych*, których katalog określono w art. 2 ust. 1 i 2.

Nowe przepisy *ustawy o urzędzie Ministra Spraw Wewnętrznych*, zastępujące kilkakrotnie nowelizowaną *ustawę z dnia 31 stycznia 1959 r. o służbie funkcjonariuszy Milicji Obywatelskiej*⁹, zostały wprowadzone 1 stycznia 1986 r., gdy

⁷ J. Wygoda, *Pojęcie czynności operacyjno-rozpoznawczych w ustawodawstwie polskim — propozycja wykładni Teza nr 2*, „Wojskowy Przegląd Prawniczy” 2017, nr 1 (5), LEX.

⁸ Dz.U. 1983, nr 38, poz. 172.

⁹ Dz.U. 1973, nr 23, poz. 136 z późn. zm.

weszła w życie ustawa z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej Polskiej Rzeczypospolitej Ludowej¹⁰.

W odniesieniu do pojęcia „czynności operacyjno-rozpoznawcze” ustawa ta wskazywała tylko na samą kategorię czynności prawnej jako możliwości podejmowania takich działań służących określonym celom. Pomija się w jej treści aspekt definiowania legalnego, a nawet jego zakresu znaczeniowego, ustawodawca wymienia je obok czynności dochodzeniowo-śledczych i administracyjno-porządkowych. Nadano im jednak wyrazistą i rozległą ramę prawną, a przez fakt normotwórczy otrzymały one formalny charakter¹¹. Nie określono wówczas jednak ich metod.

Wykonywanie czynności operacyjno-rozpoznawczych służyło, w myśl art. 2 ust. 1 pkt 1 ustawy o urzędzie Ministra Spraw Wewnętrznych, ochronie bezpieczeństwa państwa, w tym zwalczaniu szpiegostwa, terroryzmu, dywersji i sabotażu oraz innych czynów godzących w konstytucyjne zasady ustrojowe Polskiej Rzeczypospolitej Ludowej, jak również koordynowaniu działań w zakresie ochrony tajemnicy państwowej i służbowej oraz kontroli ruchu międzynarodowego.

Z kolei w art. 6 ust. 3 ustawy o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów ustawodawca odniósł się do czynności dochodzeniowo-śledczych, stanowiąc iż uprawnienia procesowe funkcjonariuszy Milicji Obywatelskiej, wynikające z przepisów Kodeksu postępowania karnego i przepisów Kodeksu postępowania w sprawach o wykroczeniach, przysługują również funkcjonariuszom Służby Bezpieczeństwa. Natomiast w ust. 2 wskazano, iż funkcjonariusze Służby Bezpieczeństwa i Milicji Obywatelskiej wykonują również czynności na polecenie sądów i organów prokuratury w zakresie określonym w odrębnych przepisach.

Stosownie do art. 2 ust. 1 pkt 2 i 4 ustawy o urzędzie Ministra Spraw Wewnętrznych, wykonywanie czynności procesowych (dochodzeniowo-śledczych) służyło natomiast ochronie życia, zdrowia i mienia obywateli oraz mienia społecznego przed bezprawnymi zamachami naruszającymi te dobra, a także zwalczaniu innych przestępstw i wykroczeń.

W przypadku zaś czynności administracyjno-prawnych, aktualnie określanych jako czynności administracyjno-porządkowe, ich wykonywanie na gruncie ustawy o urzędzie Ministra Spraw Wewnętrznych przez funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej, stosownie do art. 2 ust. 1 pkt 3 i 5, było związane z ochroną porządku publicznego, w tym ochroną ładu i spokoju w miejscach publicznych oraz środkach komunikacji publicznej, a także z bezpieczeństwem w ruchu drogowym oraz ochroną granic państwowych, w tym organizowaniem kontroli ruchu granicznego, zabezpieczaniem nienaruszalności znaków i urzędzeń granicznych.

¹⁰ Dz.U. 1985, nr 38, poz. 181.

¹¹ A. Dana, *Prawo o czynnościach operacyjno-rozpoznawczych*, „Prokuratura i Prawo” 2021, nr 3, Legalis.

Funkcjonariusze Służby Bezpieczeństwa i Milicji Obywatelskiej, zgodnie z art. 7 ust. 1 ustawy o urzędzie Ministra Spraw Wewnętrznych, wykonując czynności, o których mowa w art. 6, mieli w szczególności prawo: legitymowania lub w inny sposób ustalania tożsamości osoby, zatrzymywania osób w trybie i wypadkach określonych w przepisach Kodeksu postępowania karnego, zatrzymywania osób naruszających lub zagrażających porządkowi i bezpieczeństwu publicznemu, przeszukiwania osób i pomieszczeń w trybie i wypadkach określonych w odrębnych przepisach, dokonywania kontroli osobistej i przeglądania zawartości bagaży czy żądania niezbędnej pomocy od kierowników instytucji państwowych i jednostek gospodarki społecznej.

Chociaż wspomnianym wyżej uprawnieniom nie poświęcono w ustawie o urzędzie Ministra Spraw Wewnętrznych zbyt wiele miejsca, to jednak — jak pisał Jan Widacki¹²:

postępem wobec stanu sprzed 1983 roku było to, że w ogóle pojawiła się regulacja ustawowa (często zresztą nieprzestrzegana) rozmaitych działań organów bezpieczeństwa, operujących w sferze praw i wolności obywatelskich. Była to jednak ustawa regulująca funkcjonowanie organów totalitarnego państwa ze specyficznym dla takiego państwa podejściem do praw i swobód obywatelskich.

W 1989 roku stało się jasne, że ustawę tę należy zmienić, że musi być postawiony pierwszy krok w kierunku przebudowy aparatu bezpieczeństwa i dostosowania go do standardów państwa demokratycznego.

W ramach realizacji powyższego celu 6 kwietnia 1990 r. została uchwalona ustawa o Urzędzie Ochrony Państwa, która weszła w życie 10 maja 1990 r.¹³ Następnego dnia mianowano jego pierwszego szefa, którym został Krzysztof Kozłowski. W lipcu 1990 r. rozpoczęto proces weryfikacji, zaś 31 lipca 1990 r. rozwiązano Służbę Bezpieczeństwa i zorganizowano Urząd Ochrony Państwa. W latach 1990–1996 Urząd Ochrony Państwa był wydzielonym pionem w Ministerstwie Spraw Wewnętrznych, a na jego czele stał szef podległy ministrowi. Po reformie administracyjnej, która weszła w życie w dwóch etapach (1 października 1996, 1 stycznia 1997), Urząd Ochrony Państwa stał się samodzielną instytucją Rzeczypospolitej Polskiej. Od 1 października 1996 r. nadzór nad nim przejął Prezes Rady Ministrów, a ponadto od 1 stycznia 1997 r. powołany został minister-koordynator służb specjalnych.

Zgodnie z art. 1 ust. 2 ustawy o Urzędzie Ochrony Państwa do zadań Szefa Urzędu Ochrony Państwa należało: (1) rozpoznawanie i przeciwdziałanie zagrożeniom godzącym w bezpieczeństwo, obronność, niezależność, całość i międzynarodową pozycję państwa; (2) zapobieganie i wykrywanie przestępstw szpiegostwa i terroryzmu oraz innych przestępstw godzących w bezpieczeństwo

¹² J. Widacki, *Prehistoria UOP*, „Przegląd Bezpieczeństwa Wewnętrznego” 2010, wydanie specjalne, s. 19.

¹³ Dz.U. 1990, nr 30, poz. 180.

państwa oraz ściganie ich sprawców; (3) zapobieganie i wykrywanie przestępstw godzących w podstawy ekonomiczne państwa i ściganie ich sprawców; (4) zapobieganie i wykrywanie przestępstw o charakterze lub zasięgu międzynarodowym, w tym nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi, psychotropowymi lub materiałami jądrowymi i promieniotwórczymi oraz ściganie ich sprawców; (5) rozpoznawanie i przeciwdziałanie naruszeniom tajemnicy państwowej; (6) przygotowywanie dla najwyższych organów władzy i administracji państwowej informacji i analiz istotnych dla bezpieczeństwa państwa; (7) zapewnienie kryptograficznej ochrony wiadomości stanowiących tajemnicę państwową i służbową, przekazywanych przez techniczne środki łączności na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych.

W ramach zadań określonych w powyższy sposób — stosownie do treści art. 6 ust. 1 ustawy o UOP — wykonywał on czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznania, zapobiegania i wykrywania przestępstw, a także czynności operacyjno-rozpoznawcze w celu uzyskiwania informacji istotnych dla ochrony bezpieczeństwa państwa.

W tym miejscu warto nadmienić, iż z dniem 8 listopada 2001 r. wszedł w życie art. 6a¹⁴ ustawy o UOP regulujący materię zbierania i przetwarzania danych osobowych, który został dodany *ustawą z dnia 6 lipca 2001 r. o zmianie ustaw o: powszechnym obowiązku obrony Rzeczypospolitej Polskiej; odszkodowaniach*

¹⁴ 1. Urząd Ochrony Państwa w celu realizacji ustawowych zadań może zbierać, także niejawnie, z zachowaniem ograniczeń wynikających z art. 10 ust. 1, dane osobowe, w tym również dane wskazane w art. 27 i 28 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz.U. 1997, nr 133, poz. 883; 2000, nr 12, poz. 136, nr 50, poz. 580, nr 116, poz. 1216; 2001, nr 42, poz. 474, nr 49, poz. 509), a także korzystać z danych o osobie, w tym również w formie zapisu elektronicznego, uzyskanych przez organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz przetwarzać je w rozumieniu ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której dane te dotyczą.

2. Administrator danych, o których mowa w ust. 1, jest obowiązany udostępnić dane osobowe, z zastrzeżeniem ust. 4, na podstawie imiennego upoważnienia Szefa Urzędu Ochrony Państwa lub upoważnionego funkcjonariusza, okazanego przez funkcjonariusza wraz z legitymacją służbową. Fakt udostępnienia tych danych stanowiących tajemnicę państwową podlega ochronie na podstawie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95, z 2000 r. nr 12, poz. 136 i nr 39, poz. 462 oraz z 2001 r. nr 22, poz. 247, nr 27, poz. 298 i nr 56, poz. 580).

3. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór upoważnienia, o którym mowa w ust. 2, uwzględniając wyłącznie niezbędne dane upoważnionego funkcjonariusza oraz szczegółowe warunki wydawania upoważnień w imieniu Szefa Urzędu Ochrony Państwa przez jego zastępcę lub innego funkcjonariusza.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, warunki i tryb przekazywania Urzędowi Ochrony Państwa informacji o osobie, uzyskanych przez inne organy uprawnione do wykonywania czynności operacyjno-rozpoznawczych, w czasie wykonywania tych czynności, uwzględniając wymagania wynikające z przepisów o ochronie informacji niejawnych.

przysługujących w razie wypadków i chorób pozostających w związku ze służbą w Milicji Obywatelskiej; zaopatrzeniu inwalidów wojennych i wojskowych oraz ich rodzin; uposażeniu żołnierzy; Policji; Urzędzie Ochrony Państwa; Państwowej Straży Pożarnej; kontroli skarbowej; zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin; zaopatrzeniu emerytalnym funkcjonariuszy Policji, Urzędu Ochrony Państwa, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej i Służby Więziennej oraz ich rodzin; zakwaterowaniu Sił Zbrojnych Rzeczypospolitej Polskiej; Służbie Więziennej; Inspekcji Celnej¹⁵.

Możliwość zbierania (również niejawnie) wszelkich danych osobowych, w tym także danych wrażliwych — jeżeli takie działania są uzasadnione charakterem realizowanych zadań, stanowi szczególną kategorię uprawnień analityczno-informacyjnych, która to kategoria na gruncie ówczesnej ustawy o Urzędzie Ochrony Państwa nie została wprost wyrażona w jej przepisach prawnych, jak to się stało w odniesieniu do czynności operacyjno-rozpoznawczych oraz czynności dochodzeniowo-śledczych. Zatem czynności operacyjno-rozpoznawcze polegające na zbieraniu i przetwarzaniu danych osobowych, o których mowa w art. 6a ustawy o UOP, stanowiły *de facto* czynności analityczno-informacyjne — niewyrażone wprost na gruncie ustawy o Urzędzie Ochrony Państwa — i były wykonywane, stosownie do art. 6 ust. 1 ustawy o UOP *in fine*, w celu uzyskiwania informacji istotnych dla ochrony bezpieczeństwa państwa.

W art. 6 ust. 1 ustawy o UOP oprócz czynności operacyjno-rozpoznawczych wymieniono również kategorię czynności dochodzeniowo-śledczych, których wykonywanie przez funkcjonariuszy UOP miało na celu rozpoznanie, zapobieganie i wykrywanie przestępstw, jak również ściganie ich sprawców, co wynikało już jednak z przytoczonej wyżej regulacji art. 1 ust. 2 ustawy o UOP, a dokładnie z treści punktów od 2 do 4.

Stosownie do art. 6 ust. 2 ustawy o UOP Urząd Ochrony Państwa wykonywał również czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie postępowania karnego, zaś zgodnie z ust. 3 funkcjonariusze Urzędu Ochrony Państwa wykonywali czynności tylko w zakresie właściwości tego urzędu i w tym zakresie przysługiwały im uprawnienia procesowe policjantów, wynikające z przepisów kodeksu postępowania karnego.

Przykładem innych uprawnień funkcjonariuszy Urzędu Ochrony Państwa, o których stanowi art. 7 ust. 1 ustawy o UOP, z których mogli oni korzystać, wykonując czynności, o których mowa w art. 6, były m.in. prawo zatrzymywania osób oraz przeszukiwania osób i pomieszczeń w trybie i w wypadkach określonych w przepisach kodeksu postępowania karnego.

W odróżnieniu od ustawy o urzędzie Ministra Spraw Wewnętrznych w ustawie o UOP wskazano niektóre metody i środki pracy operacyjnej (np. kontrola korespondencji, stosowanie środków technicznych umożliwiających w sposób tajny uzyskiwanie informacji, współpraca z osobowymi źródłami informacji).

¹⁵ Dz.U., nr 81, poz. 877.

Nie przyznawano im jeszcze wtedy funkcji dowodowej. Pełniły one jednak funkcję rozpoznawczą, profilaktyczną oraz wykrywczą.

Ustawa o Urzędzie Ochrony Państwa w ciągu ponad dziesięcioletniego okresu jej obowiązywania podlegała kilku nowelizacjom. Z punktu widzenia uprawnień funkcjonariuszy UOP istotnym będzie wspomnieć w tym miejscu o *ustawie z dnia 21 lipca 1995 r. o zmianie ustaw o: urzędzie Ministra Spraw Wewnętrznych, Policji, UOP, Straży Granicznej oraz niektórych innych ustaw*¹⁶, w której dokonano rozbudowy ustawowej regulacji dotyczącej czynności operacyjno-rozpoznawczych. Przede wszystkim wprowadzono dwie nowe instytucje: zakup kontrolowany i przesyłkę niejawnie nadzorowaną. Ponadto rozszerzono katalog przestępstw pozwalających na zastosowanie kontroli korespondencji. Za Mateuszem Kolaszyńskim¹⁷ wskazać należy, iż:

znowelizowane ustawy kompetencyjne *expressis verbis* wyrażały możliwość wykorzystywania określonych czynności operacyjnych w procesie karnym, co stanowiło wyraźne podkreślenie tendencji do zacierania niegdyś ostrej granicy między czynnościami operacyjnymi i procesowymi. Jednym z przejawów tej tendencji było poddanie dwóch nowych czynności operacyjnych kontroli wewnątrzadministracyjnej sprawowanej przez ministra spraw wewnętrznych i Prokuratora Generalnego. Następne istotne przeobrażenie w zakresie kontroli nad czynnościami operacyjno-rozpoznawczymi nastąpiło w latach 2001–2002, kiedy kontrola operacyjna została poddana zewnętrznej kontroli sprawowanej przez sądy.

Zasygnalizowane zmiany z początku XXI w. zostały wprowadzone m.in. przez nową *ustawę kompetencyjną z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*¹⁸. Dodać należy, iż ABW została utworzona 29 czerwca 2002 r., po rozwiązaniu Urzędu Ochrony Państwa, w miejsce którego utworzono dwie odrębne agencje, tj. Agencję Bezpieczeństwa Wewnętrznego oraz Agencję Wywiadu. Jako służba specjalna Agencja Bezpieczeństwa Wewnętrznego podlega kontroli cywilnej — jest nadzorowana przez Prezesa Rady Ministrów¹⁹ i kontrolowana przez Sejm.

Czynności funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego

Jak już to wcześniej zasygnalizowano we *Wstępie* do zagadnienia, ustawy kompetencyjne, przed szczegółowym omówieniem uprawnień funkcjonariuszy służb specjalnych, wskazują na rodzaje wykonywanych przez nich działań — określanych jako czynności.

¹⁶ Dz.U., nr 104, poz. 515.

¹⁷ M. Kolaszyński, dz. cyt., s. 132–133.

¹⁸ Dz.U., nr 74, poz. 676.

¹⁹ Art. 3 *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego mogą podejmować działania operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców. Natomiast wykonywanie czynności operacyjno-rozpoznawczych i analityczno-informacyjnych może mieć miejsce w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego²⁰.

Agencja Bezpieczeństwa Wewnętrznego może też realizować czynności na polecenie sądu lub prokuratora w zakresie przewidzianym w Kodeksie postępowania karnego i Kodeksie karnym wykonawczym. Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego mogą podejmować działania jedynie w zakresie właściwości tej Agencji i w ramach tego zakresu przysługują im uprawnienia procesowe policji, określone przepisami Kodeksu postępowania karnego²¹.

Z przytoczonej regulacji art. 21 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wynikają dwa ograniczenia w wykonywaniu przez Agencję Bezpieczeństwa Wewnętrznego wszystkich czynności. Po pierwsze, uprawnienia funkcjonariuszy limitowane są granicami zadań wyznaczonych przez przepisy prawa. Niedopuszczalne jest więc wykonywanie jakichkolwiek czynności bez związku z realizacją zadań, które ustawodawca nałożył na Agencję Bezpieczeństwa Wewnętrznego, a których otwarty katalog został wskazany w art. 5 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Zadania te są realizowane przez Agencję Bezpieczeństwa Wewnętrznego w kilku podstawowych obszarach, a mianowicie: kontrwywiadu, bezpieczeństwa ekonomicznego państwa, przeciwdziałania terroryzmowi i proliferacji broni masowego rażenia, przeciwdziałania przestępczości zorganizowanej o charakterze międzynarodowym, ochrony cyberprzestrzeni oraz ochrony informacji niejawnych. Czynności te natomiast stanowią środki służące do realizacji zadań Agencji Bezpieczeństwa Wewnętrznego w zakresie: obowiązków informacyjnych względem najwyższych organów władzy państwowej, zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, rozpoznawania, zapobiegania i wykrywania przestępstw ujętych w art. 5 ust. 1 pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, bezpieczeństwa teleinformatycznego państwa polskiego oraz ochrony informacji niejawnych, w tym również w aspekcie międzynarodowym.

Drugim ograniczeniem wykonywania czynności przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego jest wskazany w ustawie cel ich podjęcia. Mają oni bowiem prawo podejmowania czynności w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców, jak również w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego.

²⁰ Art. 21 ust. 1 pkt 1 i 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

²¹ Tamże, ust. 2 i 3.

Oznacza to, iż:

zarówno czynności operacyjno-rozpoznawcze, jak i dochodzeniowo-śledcze muszą być wykonywane w określonym celu. Celem tym jest rozpoznawanie, zapobieganie i wykrywanie przestępstw oraz ścigania ich sprawców. Czynności operacyjno-rozpoznawcze mogą być jeszcze podejmowane w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego. Natomiast czynności analityczno-informacyjne mogą być realizowane tylko w celu wskazanym w poprzednim zdaniu²².

Czynności operacyjno-rozpoznawcze nie zostały zdefiniowane ustawowo. Są to czynności upoważnionych organów państwowych, które polegają na zasadniczo niejawnym i poufnym, pozaprocesowym działaniu uprawnionych ustawowo służb, nakierowanym na realizację ich zadań związanych z zapobieganiem przestępczości i innym negatywnym zjawiskom społecznym oraz z ich zwalczaniem. Wykonywane są poza procesem karnym, choć służą realizacji zadań prowadzonego lub przyszłego postępowania karnego²³.

Cecha niejawności czynności operacyjno-rozpoznawczych (oznaczonych klauzulami „tajne” i „ściśle tajne”) jest podkreślona w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w której zawarto regulacje dotyczące udostępniania informacji o pracy operacyjnej na zewnątrz (na żądanie prokuratora lub sądu). Na podstawie bowiem przepisu art. 39 ust. 1, oprócz wyjątków określonych w ustawie (ust. 3), w szczególności dotyczących czynności operacyjno-rozpoznawczych, Szef Agencji Bezpieczeństwa Wewnętrznego w zakresie swojego działania może zezwolić funkcjonariuszom i pracownikom Agencji Bezpieczeństwa Wewnętrznego oraz byłym funkcjonariuszom i pracownikom, po ustaniu stosunku służbowego lub stosunku pracy w Agencji Bezpieczeństwa Wewnętrznego, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych, na udzielenie informacji niejawnej określonej osobie lub instytucji.

Wśród funkcji pełnionych przez czynności operacyjno-rozpoznawcze należy wskazać funkcję rozpoznawczą (polegającą na rozpoznawaniu czynników oraz środowisk kryminogennych i przestępczych), funkcję wykrywczą (związaną z wykrywaniem przestępstw i ich sprawców), funkcję dowodową (sprowadzającą się do udowadniania winy sprawcom przestępstw), funkcję zapobiegawczą (dotyczącą zapobiegania popełnieniu określonych przestępstw lub neutralizowania pewnych zagrożeń)²⁴.

²² B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis.

²³ Por.: *Kryminalistyka*, red. J. Widacki, Warszawa 1999, s. 110; B. Hołyst, *Kryminalistyka*, Warszawa 2016, s. 47 Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, s. 67.

²⁴ A. Taracha, *Czynności operacyjno-rozpoznawcze...*, s. 25.

W przypadku służb specjalnych należy ponadto zwrócić szczególną uwagę na funkcję informacyjną czynności operacyjno-rozpoznawczych. Wynika ona wprost z przepisów regulujących działalność tych służb, które wykonują czynności operacyjno-rozpoznawcze i analityczno-informacyjne w celu uzyskiwania i przetwarzania informacji istotnych dla bezpieczeństwa państwa i jego porządku konstytucyjnego²⁵.

Przyjmuje się, że czynności operacyjno-rozpoznawcze są samodzielną, różną od czynności dochodzeniowo-śledczych formą aktywności służb policyjnych, wywiadowczych i kontrwywiadowczych²⁶.

Za Adamem Tarachą można wskazać w ramach płaszczyzny prawnej i taktyczno-kryminalistycznej na cztery obszary odmienności między czynnościami operacyjno-rozpoznawczymi a czynnościami dochodzeniowo-śledczymi. Pierwszy z nich dotyczy możliwości wykorzystania wyników w postępowaniu karnym. Do niedawna na gruncie kryminalistyki panował pogląd, iż taką funkcję posiadają jedynie czynności dochodzeniowo-śledcze. Obecnie ta różnica uległa wyraźnemu zatarciu. Wynika to przede wszystkim z nadania przez ustawodawcę niektórym metodom operacyjno-rozpoznawczym waloru dowodowego. W ramach drugiego kryterium wskazuje się, że działania operacyjne są objęte większym stopniem utajnienia („ściśle tajne”) niż czynności procesowe, których dotyczy jedynie tajemnica służbowa (tajemnica śledztwa). Ponadto działalność operacyjna znacznie częściej nosi cechy podstępny i w odróżnieniu od tych drugich nie podlega rygorom procesowym oraz nie odnosi się do niej gwarancje procesowe. Ostatnią znaczącą różnicą jest brak obowiązku ze strony osób fizycznych do udzielania informacji funkcjonariuszom przeprowadzającym czynności operacyjno-rozpoznawcze. Wynika to z faktu, że na uczestnikach tych działań nie ciąży obowiązek jakim podlegają świadkowie w procesie karnym. Właśnie brak tych obowiązków po stronie osób udzielających informacji, a także niedopuszczalność stosowania, z pewnymi wyjątkami, przymusu odróżniają najmocniej czynności operacyjno-rozpoznawcze od procesowych²⁷.

Czynności operacyjno-rozpoznawcze stanowią główny składnik procesu wykrywczego i charakteryzują się tajnością *ex ante* wobec wszystkich osób poddawanych takim działaniom. Taka działalność (...) pozostaje w naturalnym konflikcie z niektórymi prawami jednostki. Odwołując się do konstytucyjnych podstaw dopuszczalności czynności operacyjno-rozpoznawczych jako udzielenia określonego organowi administracji publicznej uprawnień do posługiwania się nimi, należy wskazać na treść art. 31 ust. 3 Konstytucji RP statuującą zasadę proporcjonalności. Zgodnie z jego treścią ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są

²⁵ M. Bożek i in., dz. cyt., s. 113–114.

²⁶ M. Chrabkowski, *Wykorzystywanie materiałów kontroli operacyjnej w postępowaniu przygotowawczym*, Szczytno 2009, s. 27.

²⁷ M. Kolaszyński, dz. cyt., s. 130–131.

konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw²⁸.

W praktyce każdej ze służb posiadających uprawnienia do wykonywania czynności operacyjno-rozpoznawczych określa się ich istotę oraz sposób przeprowadzenia — w przepisach wewnętrznych, niejawnych (metody pracy operacyjnej). Tylko niektóre najbardziej złożone metody pracy operacyjnej są określone ustawowo zarówno co do ich celów, podstaw prawnych i faktycznych oraz sposobu prowadzenia (tj. kontrola operacyjna, zakup kontrolowany, kontrolowane przyjęcie lub wręczenie korzyści majątkowej, zbieranie i przetwarzanie danych telekomunikacyjnych czy współpraca z osobowymi źródłami informacji)²⁹.

Na kwestię konieczności prawnej regulacji czynności operacyjno-rozpoznawczych zwrócił uwagę Jerzy Konieczny, formułując definicję tych czynności, które są, według niego, umocowanymi ustawowo, z reguły niejawnymi działaniami organów państwowych, realizowanymi w celach informacyjnych, prewencyjnych, wykrywczych lub dowodowych, a w przypadku służb wywiadowczych mających ponadto znaczenie polityczne, militarne i gospodarcze³⁰.

Dla porządku wskazać należy w tym miejscu na nieudaną próbę normatywnego zdefiniowania pojęcia „czynności operacyjno-rozpoznawczych”, podjętą w projekcie ustawy o czynnościach operacyjno-rozpoznawczych³¹. Zgodnie z art. 2 ust. 1 pkt 1–3 projektu ustawy czynności operacyjno-rozpoznawcze są zespołem przedsięwzięć jawnych i niejawnych prowadzonych wyłącznie w celu: 1) rozpoznania, zapobiegania i wykrywania przestępstw, 2) odnajdywania osób ukrywających się przed organami ścigania lub wymiarem sprawiedliwości oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginięcie jest wynikiem przestępstwa, a także odnajdywania rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem, 3) ustalenia tożsamości osób i zwłok, w przypadku uzasadnionego podejrzenia przestępczego działania.

Wskazuje się w literaturze przedmiotu³², iż owa praktyka prawnej regulacji czynności operacyjno-rozpoznawczych powinna występować w połączeniu z ogólną kontrolą nad działaniami operacyjnymi, sprawowaną przez sądy i inne organy państwa. W związku z tym wskazane wyżej metody pracy operacyjnej, z wyjątkiem współpracy z osobowymi źródłami informacji, są sklasyfikowane jako czynności poddane kontroli sądowej i prokuratorskiej (kontroli

²⁸ A. Dana, dz. cyt., Legalis.

²⁹ S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym...*

³⁰ J. Konieczny, *Czynności operacyjno-rozpoznawcze*, w: *Kryminalistyka*, red. J. Widacki, Wydawnictwo C.H. Beck, Warszawa 2008, s. 125.

³¹ Druk sejmowy nr 1570 z dnia 26 I 2007 r. oraz druk sejmowy nr 353 z dnia 7 II 2008 r.

³² M. Kolaszyński, dz. cyt., s. 137–143.

zewnątrzadministracyjnej), w przeciwieństwie do pozostałych, wymienionych dalej metod pracy operacyjnej, nieobjętych zewnętrzną kontrolą.

Pierwsza z metod pracy operacyjnej to kontrola operacyjna, która prowadzona jest niejawnie i polega na: (1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych, (2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu, lub miejsc innych niż miejsca publiczne, (3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, (4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych oraz (5) uzyskiwaniu dostępu i kontroli zawartości przesyłek³³.

Druga metoda to zakup kontrolowany, która polega na dokonaniu w sposób niejawni nabycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi albo których wytwarzanie, posiadanie, przewożenie lub obrót którymi są zabronione, a także przyjęciu lub wręczeniu korzyści majątkowej³⁴.

Trzecia metoda to przesyłka (dostawa) niejawnie nadzorowana, która jest działaniem podejmowanym w celu stwierdzenia tożsamości uczestników przestępstwa w sytuacji, gdy określone przedmioty są nielegalnie przemieszczane, przechowywane lub dochodzi do obrotu nimi³⁵.

Odnosząc się do trzech wymienionych metod pracy operacyjnej wskazać trzeba, iż poza objęciem ich kontrolą prokuratorską, a w wypadku kontroli operacyjnej — także sądową, odróżnia je od pozostałych metod pracy operacyjnej to, iż są to metody subsydiarne (pomocnicze), to jest mogą być stosowane tylko w ostateczności, gdy inne czynności operacyjne okazały się bezskuteczne lub nieprzydatne. Dodatkowo ich zastosowanie jest możliwe jedynie wobec określonego katalogu przestępstw a informacje zdobyte za ich pomocą mogą mieć wartość dowodową w procesie karnym³⁶.

Na szczególną uwagę zasługuje natomiast zbieranie i przetwarzanie danych telekomunikacyjnych³⁷. Do 7 lutego 2016 r. była to metoda pracy operacyjnej nieobjęta kontrolą zewnętrzną. Jednakże sytuacja uległa zmianie wraz z wyrokiem Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. K 23/11)³⁸. Przepis art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w brzmieniu przed zmianami wprowadzonymi *ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*³⁹,

³³ Art. 27 ust. 6 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

³⁴ Tamże, art. 29 ust. 1.

³⁵ Tamże, art. 30 ust. 1.

³⁶ E. Gruza, dz. cyt., s. 61–64.

³⁷ Art. 28 i 28 a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

³⁸ Dz.U. 2014, poz. 1055.

³⁹ Dz.U. 2016, poz. 147.

przez to, że nie przewidywał niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180 c i 180 d ustawy — Prawo telekomunikacyjne, został uznany za niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP. W uzasadnieniu tego wyroku Trybunał Konstytucyjny wyjaśnił, że przepis ten, w przeciwieństwie do przepisów *ustawy z dnia 6 kwietnia 1990 r. o Policji* czy *ustawy z dnia 28 września 1991 r. o kontroli skarbowej*, regulujących kwestie udostępniania danych telekomunikacyjnych, *expressis verbis* wyłącza obowiązek uzyskania zgody sądu, tj. wydania postanowienia wyrażającego zgodę na udostępnienie funkcjonariuszom Agencji Bezpieczeństwa Wewnętrznego danych telekomunikacyjnych. Ustawodawca nie przewidział jednocześnie innego, alternatywnego mechanizmu niezależnej kontroli nad pozyskiwaniem tych danych przez funkcjonariuszy ABW, który mógłby zostać uznany za spełniający standard konstytucyjny.

W związku z powyższym wskazać należy również na uprawnienie Agencji Bezpieczeństwa Wewnętrznego do uzyskiwania — w celu realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu — danych: (1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy — Prawo telekomunikacyjne, (2) o których mowa w art. 161 ustawy — Prawo telekomunikacyjne, (3) w przypadku użytkownika, który nie jest osobą fizyczną — numeru zakończenia sieci oraz siedziby lub miejsca wykonywania działalności gospodarczej, nazwy firmy lub nazwy i formy organizacyjnej tego użytkownika, (4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej — także nazwy miejscowości i ulicy, przy której znajduje się zakończenie sieci udostępnione użytkownikowi, oraz ich przetwarzania bez wiedzy i zgody osoby, której dotyczy⁴⁰.

Natomiast wśród metod pracy operacyjnej nieobjętych kontrolą zewnętrzną można wymienić obserwację⁴¹, która polega na obserwowaniu i rejestrowaniu przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych podejmowanych na podstawie ustawy.

Trybunał Konstytucyjny w wyroku z 20 kwietnia 2004 r. (sygn. K 45/02), dotyczącym stosowania tej czynności przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego uznał, że to uprawnienie ogranicza konstytucyjne prawo do prywatności zawarte w artykułach 47, 49 i 51 ust. 2 Konstytucji RP. W wyroku tym nie zakwestionowano okoliczności, iż przeciwdziałanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa wymaga podjęcia przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego wideoobserwacji. Jednak wskazano, iż zakwestionowany przepis nie spełnia zasady proporcjonalności w zakresie ingerencji w prawa i wolności jednostki. Znowelizowana ustawa o Agencji Bezpieczeństwa Wewnętrznego

⁴⁰ Art. 28 b *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

⁴¹ Tamże, art. 23 ust. 1 pkt 6.

oraz Agencji Wywiadu⁴² zezwala na wykonywanie obserwacji jedynie w ramach czynności operacyjno-rozpoznawczych⁴³ oraz czyni zadość postulowanej przez Trybunał Konstytucyjny zasadzie proporcjonalności⁴⁴. Spełniony został także wymóg zapewnienia środka odwoławczego. Na sposób przeprowadzenia obserwacji przysługuje, w terminie siedmiu dni od dnia, kiedy podmiot dowiedział się o dokonanych wobec niego czynnościach, zażalenie do prokuratora właściwego ze względu na miejsce ich przeprowadzania⁴⁵. Natomiast materiały z tych czynności, które nie stanowią informacji potwierdzających popełnienie przestępstwa lub nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznie protokolarnemu, komisijnemu zniszczeniu⁴⁶.

Jako kolejne metody pracy operacyjnej nieobjęte kontrolą zewnętrzną można wskazać współpracę z osobowymi źródłami informacji⁴⁷ i przedsięwzięcia werbunkowe, polegające na zbieraniu informacji na temat osoby, z wykorzystaniem wyników obserwacji, wywiadu czy wskazań osób współpracujących z funkcjonariuszami (osoba niebędąca funkcjonariuszem).

Przy wykonywaniu swoich zadań Agencja Bezpieczeństwa Wewnętrznego może korzystać z pomocy osób niebędących jej funkcjonariuszami. Osoby takie pozyskują i przekazują Agencji Bezpieczeństwa Wewnętrznego informacje i materiały, które następnie są wykorzystywane w ujawnianiu działalności obcych służb wywiadowczych lub zwalczania przestępczości, w szczególności gospodarczej i zorganizowanej. Osoby udzielające pomocy są rodzajem własnego źródła informacji o zagrożeniach, które Agencja Bezpieczeństwa Wewnętrznego ma za zadania rozpoznawać i zwalczać. Zabronione jest ujawnianie danych o osobie udzielającej Agencji pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych. Ujawnienie danych o takich osobach może nastąpić jedynie w przypadkach określonych w ustawie⁴⁸. Osoba taka nie może ujawniać faktu udzielania pomocy ani okoliczności związanych z jej udzielaniem. Osobom udzielającym pomocy może być przyznane wynagrodzenie wypłacane z funduszu operacyjnego⁴⁹.

W ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu⁵⁰ przewidziano również wyłączenie współpracy z enumeratywnie wymienioną

⁴² Ustawa z dnia 25 listopada 2004 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U.2004, nr 267, poz. 2647).

⁴³ Art. 23 ust. 1 pkt 6 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁴⁴ Tamże, art. 23 ust. 6.

⁴⁵ Tamże, art. 23 ust. 7.

⁴⁶ Tamże, art. 23 ust. 8.

⁴⁷ Tamże, art. 36 ust. 1–3.

⁴⁸ Tamże, art. 39 ust. 4.

⁴⁹ B. Opaliński, M. Rogalski P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego...*

⁵⁰ Art. 37 ustawy o ABW oraz AW.

grupą podmiotów. Dotyczy to m.in. posłów i senatorów, osób zajmujących kierownicze stanowiska państwowe, sędziów, prokuratorów i adwokatów.

Do metod pracy operacyjnej nieobjętych zewnętrzną kontrolą zalicza się także działania maskujące. Są to czynności mające na celu stworzenie lub wykorzystywanie błędnego przeświadczenia osób, wobec których podejmowane są działania operacyjne albo osób postronnych, co do właściwego znaczenia określonych zdarzeń, obiektów lub tożsamości osób uczestniczących. W działaniach maskujących można wykorzystywać m.in. legalizację, czyli uzyskanie lub wytworzenie dokumentów legalizacyjnych, zabezpieczających przed zdemaskowaniem rzeczywistych danych⁵¹.

Powyższe działania znajdują umocowanie w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu⁵², która przewiduje uprawnienia ABW o charakterze operacyjno-rozpoznawczym, polegające na ochronie środków, form i metod realizacji zadań oraz zgromadzonych informacji i danych identyfikujących funkcjonariuszy. Ochrona ta polega przede wszystkim na utajnieniu środków, form i metod, informacji i ich źródeł oraz danych funkcjonariuszy.

W świetle powyższego czynności operacyjno-rozpoznawcze stanowią zasadniczy środek, przy pomocy którego Agencja Bezpieczeństwa Wewnętrznego może realizować swoje zadania ustawowe. Dzięki nim ABW może nie tylko zdobywać informacje o zagrożeniach, lecz przede wszystkim korzystać z nich w celu rozpoznawania, zapobiegania i wykrywania przestępstw. W kontekście art. 21 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, czynności operacyjno-rozpoznawcze mogą więc mieć — w zależności od realizowanego zadania ustawowego — charakter wykrywczo-dowodowy (*w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców*) lub informacyjny (*w celu uzyskiwania i przetwarzania informacji*)⁵³.

Pod pojęciem „czynności dochodzeniowo-śledcze” należy rozumieć czynności podejmowane w ramach dochodzenia⁵⁴ oraz śledztwa⁵⁵. Chodzi tutaj o czynności procesowe w postępowaniu karnym. Pod pojęciem „czynności procesowe” w postępowaniu karnym należy rozumieć określone przez prawo karne procesowe zachowanie się uczestnika postępowania wywołujące przewidziane przez to prawo skutki prawne⁵⁶.

Cele czynności procesowych mogą być przejęte z Kodeksu postępowania karnego, w którym są wyznaczone cele postępowania przygotowawczego. Są

⁵¹ B. Kurzępa, *Podstęp w toku czynności karnoprocessowych i operacyjnych*, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora”, Toruń 2003, s. 194–195.

⁵² Art. 35 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁵³ M. Bożek, *Upewnienia operacyjne służb specjalnych jako środki umożliwiające ingerencję w wolności i prawa jednostki (zarys problemu)*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 17 (9), s. 91.

⁵⁴ Art. 325 a i n. ustawy z dnia 6 czerwca 1997 r. — Kodeks postępowania karnego (Dz.U. 2021, poz. 534).

⁵⁵ Art. 309 i n. Kodeksu postępowania karnego.

⁵⁶ T. Grzegorzczak, J. Tylman, *Polskie postępowanie karne*, Warszawa 2011, s. 399.

nimi: (1) ustalenie, czy został popełniony czyn zabroniony i czy stanowi on przestępstwo, (2) wykrycie i w razie potrzeby ujęcie sprawcy, (3) zebranie niezbędnych danych dotyczących sprawcy, (4) wyjaśnienie okoliczności sprawy, w tym ustalenie osób pokrzywdzonych i rozmiarów szkody, (5) zebranie, zabezpieczenie i utrwalenie, w niezbędnym zakresie, dowodów dla sądu⁵⁷.

Funkcjonariusze ABW wykonują również czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie postępowania karnego oraz w *ustawie z dnia 6 czerwca 1997 r. — Kodeks karny wykonawczy*⁵⁸. Przykładem mogą być uregulowania art. 311 kodeksu postępowania karnego. Zgodnie z tym przepisem śledztwo prowadzi prokurator, który może powierzyć policji przeprowadzenie śledztwa w całości lub w określonym zakresie albo dokonanie poszczególnych czynności śledztwa. W wypadkach określonych w art. 309 pkt 2 i 3 Kodeksu postępowania karnego można powierzyć policji jedynie dokonanie poszczególnych czynności śledztwa⁵⁹. Wskazane powierzenie nie może obejmować czynności związanych z przedstawieniem zarzutów, zmianą lub uzupełnieniem postanowienia o przedstawieniu zarzutów oraz zamknięciem śledztwa⁶⁰. W sytuacji opisanej w art. 311 § 2 Kodeksu postępowania karnego policja może dokonać innych jeszcze czynności, jeżeli wyłoni się taka potrzeba⁶¹. Postanowienia art. 311 Kodeksu postępowania karnego mają odpowiednie zastosowanie do Agencji Bezpieczeństwa Wewnętrznego⁶².

Do innych czynności procesowych wykonywanych przez funkcjonariuszy ABW, uregulowanych w Kodeksie postępowania karnego, zalicza się przede wszystkim: (1) przesłuchiwanie podejrzanych i świadków (art. 177), (2) konfrontowanie osób przesłuchiwanych (art. 172), (3) dokonywanie okazania osób (art. 173), (4) oględziny miejsca, osób i rzeczy (art. 207), (5) przeszukiwanie osób, pomieszczeń i zatrzymywanie rzeczy (art. 217), (6) zatrzymywanie osób podejrzanych (art. 244), (7) przeprowadzenie eksperymentu, doświadczenia lub odtworzenia przebiegu zdarzeń (art. 211), (8) prawo do przeprowadzenia czynności sprawdzających w zakresie informacji zawarte w zawiadomieniu o przestępstwie (art. 307), (9) prawo podejmowania czynności niecierpiących zwłoki dla zabezpieczenia śladów i dowodów przestępstwa (art. 308).

Funkcjonariusze ABW wykonują czynności tylko w zakresie właściwości tej Agencji i w tym zakresie przysługują im uprawnienia procesowe policji, wynikające z przepisów Kodeksu postępowania karnego. Dodać należy w tym miejscu, iż „wykonywanie czynności procesowych przez organ do tego nieuprawniony może spowodować uznanie ich za bezskuteczne, co oznacza, że nie będą one stanowiły dowodu w sprawie”⁶³.

⁵⁷ Art. 297 § 1 Kodeksu postępowania karnego.

⁵⁸ Dz.U. 2021, poz. 53.

⁵⁹ Art. 311 § 1–2 Kodeksu postępowania karnego.

⁶⁰ Tamże, art. 311 § 3.

⁶¹ Tamże, art. 311 § 4.

⁶² Tamże, art. 312 pkt 1.

⁶³ *Kodeks postępowania karnego. Komentarz*, red. J. Skorupka, art. 312, Legalis.

Funkcjonariusze ABW są uprawnieni także do prowadzenia dochodzenia. Dochodzenie prowadzi policja lub organy, o których mowa w art. 312 Kodeksu postępowania karnego, czyli także ABW, chyba że prowadzi je prokurator⁶⁴. Przepisy dotyczące śledztwa stosuje się odpowiednio do dochodzenia, jeżeli przepisy rozdziału 36a Kodeksu postępowania karnego, poświęconego dochodzeniu, nie stanowią inaczej. Przepisy rozdziału 36a Kodeksu postępowania karnego nie regulują w pełni instytucji dochodzenia. Zastosowanie więc mają odpowiednie przepisy dotyczące śledztwa. W szczególności dotyczy to art. 312, 314, 315–318 Kodeksu postępowania karnego.

Uprawnienia o charakterze procesowym wynikają także z ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Spośród przedstawionych uprawnień funkcjonariuszy ABW w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu znajduje się odwołanie bezpośrednio do tych związanych z zatrzymaniem osoby podejrzanej oraz prawem przeszukiwania osób i pomieszczeń w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego⁶⁵.

Natomiast takie uprawnienia, jak: (1) wydawanie osobom poleceń określonego zachowania się w granicach niezbędnych do wykonania czynności określonych w art. 23 ust. 1 pkt 2–5a lub wykonywania innych czynności służbowych, podejmowanych w zakresie i w celu realizacji ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego lub w celu uniknięcia bezpośredniego zagrożenia bezpieczeństwa osób lub mienia, gdy jest to niezbędne do sprawnego i zgodnego z prawem wykonywania tych czynności albo uniknięcia zatarcia śladów przestępstwa, (2) legitymowanie osób w celu ustalenia ich tożsamości, (3) dokonywanie kontroli osobistej⁶⁶, a także przeglądanie zawartości bagaży i sprawdzanie ładunków⁶⁷ w portach i na dworcach lub innych miejscach odprawy podróżnych, lub bagażu oraz w środkach transportu lądowego, powietrznego i wodnego, w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary lub w związku z realizacją zadań określonych w art. 5 ust. 1 pkt 1–2b i 5, czy też (4) dokonywanie sprawdzenia prewencyjnego na zasadach i w sposób określony w art. 43a, mają charakter uprawnień procesowych i administracyjno-porządkowych⁶⁸.

Ponadto funkcjonariusze ABW mają prawo przeprowadzania doprowadzenia, o którym mowa w art. 4 pkt 2 lit. a ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej⁶⁹ lub konwoju, o którym mowa w art. 4 pkt 3 tej ustawy.

⁶⁴ Art. 325 a § 1 Kodeksu postępowania karnego.

⁶⁵ Art. 23 ust. 1 pkt 3 i 4 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁶⁶ Tamże, art. 23 a w związku z art. 23 c.

⁶⁷ Tamże, art. 23 b w związku z art. 23 c.

⁶⁸ Por.: Rozporządzenie Rady Ministrów z dnia 7 I 2020 r. w sprawie przeprowadzania i dokumentowania niektórych czynności przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego (Dz.U. 2020, poz. 64).

⁶⁹ Dz.U. 2018, poz. 1834; 2019, poz. 15.

Wskazać należy również, iż zmiany w przepisach prawa odnoszące się do granic uprawnień dochodzeniowo-śledczych były także rezultatem orzeczeń Trybunału Konstytucyjnego.

W kwestii wydawania poleceń określonego zachowania się Trybunał Konstytucyjny stwierdził, że w ramach czynności dochodzeniowo-śledczych uprawnienia do wydawania poleceń określonego zachowania się są usprawiedliwione. Jednakże polecenia dotyczą sfery wolności człowieka, dlatego ustawodawca powinien wytyczyć w sposób jednoznaczny granicę dopuszczalnej ingerencji funkcjonariusza i przewidzieć odpowiednie środki proceduralne umożliwiające kontrolę zasadności wydanego polecenia⁷⁰.

W związku z przywołanym wyrokiem Trybunału Konstytucyjnego w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu⁷¹ sprecyzowano okoliczności, w jakich funkcjonariusze mogą wydawać *polecenia określonego zachowania*. Uznano, że mogą one być wydawane tylko wtedy, gdy dotyczą wykonywania ustawowych zadań ABW i w granicach niezbędnych do legitymowania osób w celu ustalenia ich tożsamości, a także zatrzymywania osób, przeszukiwania osób i pomieszczeń, dokonywania kontroli osobistej i przeglądania zawartości bagaży albo w celu uniknięcia bezpośredniego zagrożenia bezpieczeństwa osób lub mienia. Wprowadzono też procesową kontrolę *sposobu przeprowadzenia czynności* realizowanych przez funkcjonariuszy ABW. Osobie, której wydano takie polecenie, przysługuje prawo do złożenia zażalenia do właściwego miejscowo prokuratora, w trybie przepisów Kodeksu postępowania karnego.

W odniesieniu zaś do kontroli osobistej Trybunał Konstytucyjny stwierdził, że przepis uprawniający m.in. funkcjonariuszy ABW i CBA do przeprowadzenia kontroli osobistej, przeszukania osób i pojazdów, nie określając granic tych czynności, jest niezgodny z Konstytucją. Przeszukanie osoby jest czymś więcej niż oględzinami ciała. *Najbardziej zaawansowany stopień* takiego przeszukania może oznaczać daleko idącą ingerencję w nietykalność osobistą przeszukiwanego. Kontrola osobista zaś jest samodzielną, pozaprocesową (operacyjną) czynnością, podejmowaną — co do zasady — w związku z zaistnieniem uzasadnionego podejrzenia popełnienia czynu zabronionego. Istnieje też pogląd, że kontrola osobista to przeszukanie prowadzone jedynie poza procesem karnym i nienormowane w Kodeksie postępowania karnego⁷².

Na mocy nowelizacji ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu dookreślono przepisy dotyczące dokonywania kontroli osobistej oraz przeglądania zawartości bagaży w związku z realizacją zadań,

⁷⁰ Por.: Wyrok Trybunału Konstytucyjnego z dnia 20 IV 2004 r., sygn. K 45/02, OTK-A 2004/4/30 (Dz.U.2004, nr 109, poz. 1159).

⁷¹ Art. 23 ust. 1 pkt 1 *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* w brzmieniu nadanym ustawą z dnia 25 XI 2004 r. (Dz.U., nr 267, poz. 2647), która weszła w życie dnia 1 I 2005 r.

⁷² Por. wyrok Trybunału Konstytucyjnego z dnia 14 XII 2017 r., sygn. K 17/14, OTK-A 2018/4 (Dz.U. 2017, poz. 2405).

które znajdują się we właściwości rzeczowej ABW⁷³. Zgodnie z obowiązującymi przepisami przez kontrolę osobistą rozumie się sprawdzenie: (1) zawartości odzieży i obuwia osoby kontrolowanej oraz przedmiotów, które znajdują się na jej ciele, bez odsłaniania przykrytej odzieżą powierzchni ciała, (2) zawartości podręcznego bagażu oraz innych przedmiotów, które posiada przy sobie osoba kontrolowana, (3) zawartości odzieży i obuwia osoby kontrolowanej i przedmiotów, które znajdują się na jej ciele, z odsłonięciem przykrytych odzieżą powierzchni ciała w celu oraz w zakresie niezbędnym do odebrania broni lub innych poszukiwanych przedmiotów, w przypadku gdy ujawniono ich posiadanie przez osobę kontrolowaną podczas sprawdzenia, o którym mowa w pkt 1 lub 2, i gdy do ich odebrania nie jest wystarczające zastosowanie czynności określonych w pkt 1 i 2, (4) jamy ustnej, nosa, uszu oraz włosów osoby kontrolowanej, (5) miejsc intymnych osoby kontrolowanej, w szczególności uzasadnionych przypadkach.

Czynności procesowe zarówno te regulowane przepisami kodeksu postępowania karnego, jak i te wynikające z ustawy o ABW oraz AW, przewidują procedurę zewnętrznego nadzorowania przez prokuraturę lub sąd rezultatów działalności służb specjalnych. Natomiast czynności operacyjne podlegają w zasadzie nadzorowi wewnętrznemu, a w wyjątkowych tylko przypadkach zewnętrznej kontroli. Zasadniczym celem czynności procesowych jest zwalczanie przestępczości i ściganie konkretnych sprawców przestępstw. Pozwala to już na samym początku prowadzić działania śledcze oraz wspomagające je czynności operacyjne w odpowiednim kierunku. Dzięki temu już w późniejszych etapach postępowania procesowego można ponownie dokonać kontroli legalności i zasadności przebiegu czynności operacyjnych prowadzonych na użytek działań śledczych⁷⁴.

Z kolei czynności analityczno-informacyjne, jak już wyżej wspomniano, służą — obok czynności operacyjno-rozpoznawczych — realizacji zadań ustawowych przez wszystkie służby specjalne. W związku z tym działania służb specjalnych ukierunkowane na realizację tych zadań (z wyłączeniem prowadzenia czynności dochodzeniowo-śledczych i działalności w zakresie zadań związanych z ochroną informacji niejawnych) mają albo charakter operacyjno-rozpoznawczy, albo analityczno-informacyjny. Wobec tego to, co nie jest działaniem operacyjno-rozpoznawczym w działalności służb, stanowi ich pracę analityczno-informacyjną.

⁷³ Art. 23a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu dodany ustawą z dnia 14 grudnia 2018 r. (Dz.U. 2018 r., poz. 2399), która weszła w życie dnia 25 XII 2018 r.

⁷⁴ J. Mąka, *Wyzwania stojące przed służbami specjalnymi — 20 lat temu i obecnie*, „Przeгляд Bezpieczeństwa Wewnętrznego” 2011, wydanie specjalne, s. 162.

W literaturze przedmiotu⁷⁵ wskazuje się, iż:

funkcja analityczno-informacyjna służb specjalnych polega na dostarczaniu władzom państwowym i działającym na ich rzecz podmiotom wiedzy niezbędnej do podejmowania optymalnych decyzji z punktu widzenia interesów państwa, czyli zgodnych z polską racją stanu. (...) Katalog zainteresowań analityczno-informacyjnych służb specjalnych ma w tym względzie charakter otwarty. To znaczy, że dotyczy on każdego podmiotu, którego działalność generuje lub może generować zagrożenia dla bezpieczeństwa RP oraz każdego zdarzenia, które ma wpływ na to bezpieczeństwo. Takie podejście zakłada zmienność zainteresowań podmiotowych i przedmiotowych służb specjalnych, tak w sensie kierunków, jak i intensywności rozpoznania, zależnych od dynamicznych zmian zachodzących w otoczeniu, zarówno w kraju jak i za granicą. Za znacznie szerszym, niż w przypadku funkcji represyjnej, katalogiem zainteresowań służb na płaszczyźnie informacyjno-analitycznej przemawia przede wszystkim fakt, że tylko pewna grupa zagrożeń dla bezpieczeństwa państwa, w tym jego bezpieczeństwa ekonomicznego, wiąże się z działalnością sprzeczną z obowiązującym prawem, czyli prościej — zagrożenia te nie zawsze są wynikiem działalności przestępczej.

W przypadku ABW zadania tej formacji w zakresie pracy analityczno-informacyjnej polegają na uzyskiwaniu, analizowaniu, przetwarzaniu i przekazywaniu właściwym organom informacji, które mogą mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego⁷⁶.

Informacje te są przekazywane niezwłocznie przez Szefa ABW, w zakresie jego właściwości, Prezydentowi RP i Prezesowi Rady Ministrów⁷⁷. Są to informacje, które mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP. Obowiązek ten został zmodyfikowany w sytuacjach, gdy informacje te są przekazywane Prezydentowi RP w każdym przypadku⁷⁸, kiedy tak zdecyduje, oraz gdy informacje są przekazywane właściwemu ministrowi, w zakresie jego działania, chyba że Prezes Rady Ministrów zdecyduje inaczej⁷⁹.

Z powyższego wynika, iż obowiązek przekazywania informacji przez Szefa ABW został zróżnicowany co do trybu i podmiotów uprawnionych do ich otrzymywania. Ustawodawca opisał podstawowy tryb *ex officio* (z urzędu) stosowany wobec szerszego kręgu podmiotów uprawnionych (Prezydent RP, Prezes Rady Ministrów, ministrowie). Przewidziano również dodatkowy tryb *petitio* (na żądanie), który ma zastosowanie wyłącznie wobec Prezydenta RP. W obu sytuacjach nałożono na Szefa ABW obowiązek przekazywania stosownych informacji

⁷⁵ K. Bodziony, *Rola służb specjalnych w systemie instytucji odpowiedzialnych za bezpieczeństwo ekonomiczne państwa*, „Przegląd Bezpieczeństwa Wewnętrznego” 2012, nr 7 (4), s. 139.

⁷⁶ Art. 5 ust. 1 pkt 4 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁷⁷ Tamże, art. 18 ust. 1.

⁷⁸ Tamże, art. 18 ust. 2.

⁷⁹ Tamże, art. 18 ust. 3.

podmiotom uprawnionym, przy czym w drugiej z nich dzieje się tak w każdym przypadku, gdy Prezydent RP tak zdecyduje. Przyjęte rozwiązanie podkreśla niewątpliwie rolę Prezydenta RP w systemie organów państwa. Z kolei wskazanie przez ustawodawcę, iż przekazywanie przez Szefa ABW uzyskanych informacji podmiotom uprawnionym winno następować niezwłocznie, świadczy o randze tych informacji dla bytu i funkcjonowania państwa, która to ulega jeszcze wzmocnieniu na skutek wąskiego zakresienia katalogu ich odbiorców.

Granice wskazanego obowiązku informacyjnego Szefa ABW zostały zdefiniowane przez pryzmat ich właściwości. W wypadku Szefa ABW owe granice wytycza art. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, statuując ABW jako organ właściwy w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Skoro zatem ABW jest właściwa w powyższym zakresie, to tym bardziej właściwy jest Szef ABW jak centralny organ administracji rządowej, działający przy pomocy ABW, będącej urzędem administracji rządowej⁸⁰.

Wskazać należy, iż sformułowany w powyższy sposób obowiązek informacyjny został wprost nazwany jako zadanie Szefa ABW, obok innych zadań uregulowanych w art. 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, już na etapie prac legislacyjnych nad projektem ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w latach 2001–2002. W uzasadnieniu do tego projektu ustawy (IV.276) można przeczytać, iż *odrębnym zadaniem Szefów ABW i AW jest przygotowywanie dla najwyższych organów władzy wykonawczej, tj. Prezydenta RP i Prezesa Rady Ministrów, informacji dotyczących zagrożeń bezpieczeństwa Państwa oraz zagrożeń porządku konstytucyjnego*. Jest to zatem na gruncie obowiązującej obecnie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, jak również i w przeszłości, jedyne zadanie Szefa ABW, które może wypełniać, pod warunkiem sprawnego i skutecznego realizowania zadań ustawowych przez podległy mu urząd.

Fundamentalne znaczenie powyższego obowiązku informacyjnego wynika jednak nie tylko z okoliczności potraktowania go przez ustawodawcę jako zadania Szefa ABW, pośród innych zadań ustawowych, ale także z ulokowania tej regulacji w rozdziale 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, odnoszącym się do organizacji ABW. Wspomniany obowiązek informacyjny został bowiem zamieszczony pośród przepisów dotyczących powoływania i odwoływania Szefa ABW, czy też wydawania przez niego aktów kierowania wewnętrznego. Mianowicie, przez wykonywanie przez Szefa ABW dyspozycji art. 18 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, możliwe jest realizowanie konstytucyjnych obowiązków przez Prezydenta RP jako najwyższego przedstawiciela Rzeczypospolitej Polskiej, gwaranta ciągłości władzy państwowej, strażnika suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium. Analogiczne informacje przekazywane przez Szefa ABW umożliwiają Prezesowi

⁸⁰ Tamże, art. 3 ust. 1.

Rady Ministrów realizację jego konstytucyjnego obowiązku, czyli prowadzenia polityki wewnętrznej i zagranicznej Rzeczypospolitej Polskiej.

W świetle powyższego zatem, należy stwierdzić, iż wspomniany rozdział trzeci ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zawiera fundamenty prawne dla funkcjonowania Szefa ABW oraz podległego mu urzędu, do których zalicza się także powyższy obowiązek informacyjny. W tym kontekście za uzasadnione uznać należy stwierdzenie, iż wypełnianie tego zadania informacyjnego przez Szefa ABW stanowi kwintesencję działalności Agencji Bezpieczeństwa Wewnętrznego, tj. informowanie konstytucyjnych organów władzy wykonawczej o zagrożeniach bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

W odniesieniu do uprawnień funkcjonariuszy realizujących czynności analityczno-informacyjne wskazać należy na uprawnienie⁸¹, zgodnie z którym Agencja Bezpieczeństwa Wewnętrznego w zakresie swojej właściwości może uzyskiwać (także niejawnie) informacje, gromadzić je, sprawdzać oraz przetwarzać. W związku z tą regulacją w literaturze przedmiotu wskazuje się, iż:

w zależności od źródła pochodzenia informacje uzyskiwane przez ABW można podzielić na informacje pozyskiwane ze źródeł zewnętrznych oraz wewnętrznych. Zgodnie z tym podziałem o informacji można mówić jako informacji przetwarzanej poza ABW i kierowanej do niej w drodze oficjalnych lub nieoficjalnych kontaktów oraz o informacji uzyskiwanej przez funkcjonariuszy ABW w ramach własnych czynności (operacyjno-rozpoznawczych, analityczno-informacyjnych). (...) Zgodnie z administracyjnoprosesową oraz karnoprosesową zasadą przestrzegania z urzędu właściwości rzeczowej, ABW powinny być przekazywane informacje o sprawach pozostających w jej zainteresowaniu z uwagi na jej ustawowe zadania (...). Odmiennie przedstawia się kwestia zdobywania informacji przez czynności własne funkcjonariuszy. W tych przypadkach wymagana jest konkretna podstawa prawna umożliwiająca pozyskiwanie, gromadzenie i przetwarzanie informacji⁸².

Szczególną kategorią uprawnień analityczno-informacyjnych ABW jest uprawnienie⁸³ polegające na możliwości zbierania, także niejawnie, wszelkich danych osobowych, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, danych wskazanych w art. 14 ust. 1⁸⁴ *ustawy z dnia 14 grudnia*

⁸¹ Tamże, art. 33.

⁸² B. Opaliński, M. Rogalski P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego...*

⁸³ Art. 34 *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

⁸⁴ Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi wrażliwymi”.

2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości⁸⁵, a także korzystania z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzania ich bez wiedzy i zgody osoby, której te dane dotyczą.

W związku z powyższym administrator zbioru danych jest obowiązany na podstawie imiennego upoważnienia wydanego przez Szefa ABW do udostępniania danych osobowych, którymi zarządza. Administrator zbioru danych udostępnia również Szefowi ABW w drodze teletransmisji informacje zgromadzone w zbiorach danych, jeżeli jednostka organizacyjna ABW, będąca odbiorcą informacji, spełnia łącznie następujące warunki: (1) posiada urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał; (2) posiada zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania, a (3) specyfika lub zakres wykonywanych zadań uzasadnia takie udostępnienie.

Do istotnych uprawnień⁸⁶ analityczno-informacyjnych funkcjonariuszy ABW należy zaliczyć także uprawnienia dotyczące żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielenia nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa. Dodatkowo funkcjonariusze ABW wykonujący czynności analityczno-informacyjne mają prawo⁸⁷ zwracać się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, a w nagłych wypadkach do każdej osoby, o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa.

W literaturze przedmiotu⁸⁸ podnosi się, iż w przypadku uprawnienia do stosowania czynności analityczno-informacyjnych zauważalna jest skromna podstawa ustawowa. W znikomym stopniu ustawy kompetencyjne regulują kwestie sposobu przetwarzania informacji i dokumentowania tego procesu, w czym zawiera się również brak regulacji dotyczących zasad tworzenia baz danych, dostępu do nich i sposób sprawowania kontroli w tej materii.

Wśród czynności wykonywanych przez służby specjalne, z wyłączeniem Agencji Wywiadu oraz Służby Wywiadu Wojskowego (służb o charakterze ściśle wywiadowczym), we *Wstępie* do zagadnienia wymieniono również czynności kontrolne. Przechodząc do ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, wskazać należy w pierwszej kolejności, iż ustawodawca nie posłużył się na gruncie jej regulacji pojęciem „czynności kontrolne”, niemniej

⁸⁵ Dz.U. 2019, poz. 125.

⁸⁶ Art. 23 ust. 1 pkt 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁸⁷ Tamże, art. 23 ust. 1 pkt 8.

⁸⁸ M. Kolaszyński, dz. cyt., s. 148–149.

jednak uprawnienie funkcjonariuszy ABW do ich stosowania nie budzi żadnych wątpliwości. Uprawnienie to jest bowiem ściśle powiązane z wykonywaniem zadań w zakresie ochrony informacji niejawnych. W katalogu ustawowych zadań ABW wymieniono, w zakresie właściwości tej instytucji, realizację zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych⁸⁹. Działania te podejmowane są w trzech obszarach: bezpieczeństwa osobowego, bezpieczeństwa przemysłowego oraz kontroli ochrony informacji niejawnych.

W związku z tym ABW odpowiada za zapewnienie właściwej ochrony informacji niejawnych, zwłaszcza oznaczonych klauzulą „tajne” i „ściśle tajne”. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*⁹⁰ określa zasady ich ochrony, rodzaje i sposób przeprowadzania postępowań sprawdzających oraz procedury ochrony fizycznej i teleinformatycznej. Nadanie niektórym informacjom niejawnym klauzuli „tajne” lub „ściśle tajne” wynika z konieczności ochrony przed poważną lub wyjątkowo poważną szkodą dla Rzeczypospolitej Polskiej. Dostęp do tego typu danych mogą uzyskać wyłącznie osoby uprawnione oraz dające rękojmię zachowania tajemnicy, co potwierdza się w ramach postępowania sprawdzającego. Jeśli zostaną ujawnione informacje, że osoba posiadająca poświadczenie bezpieczeństwa, nie daje rękojmi zachowania tajemnicy, przeprowadza się wobec niej kontrolne postępowanie sprawdzające. Instytucje i firmy, które są w posiadaniu informacji niejawnych, podlegają kontroli w zakresie ich ochrony. Kontrola obejmuje: badanie prawidłowości przetwarzania informacji niejawnych, organizacji ich ochrony, prowadzenia szkoleń w zakresie ochrony informacji niejawnych, prowadzenia postępowań sprawdzających, ochrony informacji niejawnych w systemach teleinformatycznych, czy stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Agencja Bezpieczeństwa Wewnętrznego prowadzi także postępowania w zakresie bezpieczeństwa przemysłowego wobec przedsiębiorców starających się o dostęp do informacji niejawnych w związku z wykonywaniem umów lub zadań wynikających z przepisów prawa.

W ramach współpracy międzynarodowej Polska jest zobowiązana zapewnić jednolity stopień bezpieczeństwa informacji klasyfikowanych, które są wymieniane z zagranicznymi partnerami. Szef Agencji Bezpieczeństwa Wewnętrznego pełni funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych, tzn. odpowiada za wdrażanie uzgodnionych zasad i środków ochrony informacji niejawnych.

Obecnie Szef Agencji Bezpieczeństwa Wewnętrznego pełni funkcję krajowej władzy bezpieczeństwa. W odniesieniu natomiast do sfery związanej

⁸⁹ Art. 5 ust. 1 pkt 3 *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

⁹⁰ Dz.U. 2019, poz. 742.

z obronnością funkcję tę sprawuje Szef Agencji Bezpieczeństwa Wewnętrznego za pośrednictwem Szefa Służby Kontrwywiadu Wojskowego.

Czynności wykonywane przez funkcjonariuszy na gruncie ustawy o Centralnym Biurze Antykorupcyjnym oraz ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego

Na gruncie ustawy o Centralnym Biurze Antykorupcyjnym można wyróżnić cztery rodzaje czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze, analityczno-informacyjne i kontrolne. Czynności podejmowane przez Centralne Biuro Antykorupcyjne mogą być realizowane jedynie w granicach jego zadań przewidzianych w art. 2 ustawy o Centralnym Biurze Antykorupcyjnym. Podobnie jak Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne może także wykonywać czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie postępowania karnego oraz Kodeksie karnym wykonawczym⁹¹. Funkcjonariuszom Centralnego Biura Antykorupcyjnego przysługują w zakresie właściwości Centralnego Biura Antykorupcyjnego uprawnienia procesowe policji określone przepisami Kodeksu postępowania karnego⁹².

Czynności operacyjno-rozpoznawcze są wykonywane przez Centralne Biuro Antykorupcyjne w celu zapobiegania popełnianiu przestępstw, ich rozpoznania i wykrywania⁹³.

Czynności dochodzeniowo-śledcze Centralne Biuro Antykorupcyjne może wykonywać, jeżeli istnieje uzasadnione podejrzenie popełnienia przestępstwa, w celu ścigania jego sprawców⁹⁴.

Czynności analityczno-informacyjne są wykonywane w celu uzyskiwania i przetwarzania informacji istotnych dla zwalczania korupcji w instytucjach państwowych oraz samorządzie terytorialnym, a także działalności godzącej w interesy ekonomiczne państwa⁹⁵. W zakresie przewidzianym dla czynności analityczno-informacyjnych mogą być wykonywane czynności kontrolne.

Czynności kontrolne mogą być wykonywane w celu ujawnienia przypadków korupcji w instytucjach państwowych i samorządzie terytorialnym, a także nadużyć osób pełniących funkcje publiczne oraz działalności godzącej w interesy ekonomiczne państwa⁹⁶. Czynności kontrolne polegają również na badaniu i kontroli określonych przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem państwowym lub komunalnym oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych

⁹¹ Art. 13 ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym.

⁹² Tamże, art. 13 ust. 3.

⁹³ Tamże, art. 13 ust. 1 pkt 1.

⁹⁴ Tamże *in fine* ustawy o Centralnym Biurze Antykorupcyjnym.

⁹⁵ Art. 13 ust. 1 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym

⁹⁶ Tamże, art. 13 ust. 1 pkt 2.

i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych, a także na badaniu prawidłowości realizacji umów o partnerstwie publiczno-prywatnym⁹⁷. Zaznaczyć należy, iż w przeciwieństwie do ustawy o Centralnym Biurze Antykorupcyjnym, ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego nie posługują się pojęciem „czynności kontrolne”.

Funkcjonariusze Centralnego Biura Antykorupcyjnego, wykonując czynności służące realizacji zadań przewidzianych w art. 2 ustawy o Centralnym Biurze Antykorupcyjnym, korzystają z uprawnień, które wynikają przede wszystkim z art. 14 ust. 1 pkt 1–8 ustawy o Centralnym Biurze Antykorupcyjnym oraz z aktów wykonawczych do tej ustawy⁹⁸.

Funkcjonariusze Centralnego Biura Antykorupcyjnego, wykonując czynności służące realizacji zadań, o których mowa w art. 2 ust. 1 pkt 1, mają prawo: (1) wydawania osobom poleceń określonego zachowania się w granicach niezbędnych do wykonania czynności określonych w pkt 2–5a lub wykonywania innych czynności służbowych podejmowanych w zakresie i w celu realizacji ustawowych zadań CBA, lub w celu uniknięcia bezpośredniego zagrożenia bezpieczeństwa osób lub mienia, gdy jest to niezbędne do sprawnego i zgodnego z prawem wykonywania tych czynności albo uniknięcia zatarcia śladów przestępstwa; (2) legitymowania osób w celu ustalenia ich tożsamości; (3) zatrzymywania osób w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego; (4) przeszukiwania osób i pomieszczeń w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego; (5) dokonywania kontroli osobistej⁹⁹, a także przeglądania zawartości bagaży i sprawdzania ładunków¹⁰⁰ w portach i na dworcach lub w innych miejscach odprawy podróźnych, lub bagaży oraz w środkach transportu lądowego, powietrznego i wodnego, w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary lub w związku z realizacją zadań określonych w art. 2 ust. 1 pkt 1–2 i 7; (6) dokonywania sprawdzenia prewencyjnego na zasadach i w sposób określony w art. 30a; (7) obserwowania i rejestrowania, przy użyciu środków technicznych, obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych podejmowanych na podstawie ustawy; (8) żądania niezbędnej pomocy od instytucji państwowych,

⁹⁷ Tamże, art. 31 ust. 2.

⁹⁸ *Rozporządzenie Rady Ministrów z dnia 31 I 2020 r. w sprawie przeprowadzania i dokumentowania niektórych czynności przez funkcjonariuszy Centralnego Biura Antykorupcyjnego* (Dz.U. 2020, poz. 205) oraz *rozporządzenie Rady Ministrów z dnia 4 VIII 2006 r. w sprawie udzielania funkcjonariuszom Centralnego Biura Antykorupcyjnego niezbędnej pomocy przez instytucje państwowe, organy administracji rządowej i samorządu terytorialnego, przedsiębiorców, jednostki organizacyjne, organizacje społeczne oraz obywateli* (Dz.U., nr 142, poz. 1018).

⁹⁹ Art. 14 aa w związku z art. 14 ac ustawy o Centralnym Biurze Antykorupcyjnym.

¹⁰⁰ Tamże, art. 14 ab w związku z art. 14 ac.

organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielenia nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa; (9) zwracania się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, jak również zwracania się do każdej osoby o udzielenie pomocy, w ramach obowiązujących przepisów prawa.

Ponadto funkcjonariusze Centralnego Biura Antykorupcyjnego mają prawo przeprowadzania doprowadzenia, o którym mowa w art. 4 pkt 2 lit. A ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej¹⁰¹ lub konwoju, o którym mowa w art. 4 pkt 3 tej ustawy.

Z uwagi na to, że wymienione wyżej uprawnienia mogą być realizowane w ramach czynności służących wykonywaniu ustawowych zadań przez Centralne Biuro Antykorupcyjne: operacyjno-rozpoznawczych, dochodzeniowo-śledczych, analityczno-informacyjnych i kontrolnych, to należałoby je traktować jako odrębną kategorię, to jest uprawnień o charakterze porządkowo-administracyjnym¹⁰².

Uprawnienia funkcjonariuszy Agencji Wywiadu, podobnie jak w przypadku Agencji Bezpieczeństwa Wewnętrznego, zostały uregulowane w rozdziale czwartym ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W granicach zadań Agencji Wywiadu¹⁰³ jej funkcjonariusze mogą dokonywać czynności operacyjno-rozpoznawczych oraz analityczno-informacyjnych¹⁰⁴.

Funkcjonariusze Agencji Wywiadu, wykonując powyższe czynności, mają prawo żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielania nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa¹⁰⁵. Ponadto Agencja Wywiadu może zwracać się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, jak również ma prawo zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa¹⁰⁶.

Podobnie jak Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu realizuje wspomniany wyżej obowiązek informacyjny, polegający na niezwłocznym przekazywaniu, w zakresie jego właściwości, Prezydentowi RP

¹⁰¹ Dz.U. 2018, poz. 1834; 2019, poz. 15.

¹⁰² Por. M. Bożek, *Pozycja prawna Agencji Bezpieczeństwa Wewnętrznego (struktura, zadania, zakres uprawnień)*, Emów 2003, s. 39 i n.

¹⁰³ Art. 6 ust. 1 pkt 1–9 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

¹⁰⁴ Tamże, art. 22.

¹⁰⁵ Tamże, art. 24 ust. 1 pkt 1.

¹⁰⁶ Tamże, art. 24 ust. 1 pkt 2.

i Prezesowi Rady Ministrów informacji, które mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej.

W ramach wspólnoty informacyjnej organy administracji rządowej przekazują Szefowi Agencji Wywiadu informacje istotne dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej, w szczególności dotyczące: (1) zagrożeń zewnętrznych godzących w bezpieczeństwo, obronność, niepodległość oraz integralność terytorialną i nienaruszalność granic Rzeczypospolitej Polskiej; (2) zagrożeń międzynarodowych sojuszy, układów politycznych i układów wojskowych, których Rzeczpospolita Polska jest stroną; (3) międzynarodowego terroryzmu i ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej; (4) międzynarodowego handlu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa Rzeczypospolitej Polskiej oraz dla utrzymania międzynarodowego pokoju i bezpieczeństwa; (5) realizacji umów międzynarodowych dotyczących rozbrojenia i zagrożeń związanych z rozprzestrzenianiem broni masowej zagłady oraz środków jej przenoszenia; (6) zagrożeń występujących w rejonach konfliktów i kryzysów międzynarodowych; (7) zagrożeń realizacji celów polityki zagranicznej Rzeczypospolitej Polskiej; (8) zagrożeń interesów ekonomicznych Rzeczypospolitej Polskiej¹⁰⁷.

Organy administracji rządowej przekazują Szefowi Agencji Wywiadu powyższe informacje niezwłocznie po ich uzyskaniu, w miarę możliwości w treści i formie, w jakiej je uzyskały. Informacje te Szef Agencji Wywiadu przekazuje organom wymienionym w art. 18, a także Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Służby Kontrwywiadu Wojskowego lub Szefowi Służby Wywiadu Wojskowego, w zakresie ich właściwości¹⁰⁸.

Podobnie jak w przypadku ABW, funkcjonariusze Agencji Wywiadu mogą podejmować współpracę z osobowymi źródłami informacji, z zastrzeżeniem enumeratywnie wskazanych wyłączeń podmiotowych.

Uprawnienia funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach są uregulowane w rozdziale trzecim *ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*¹⁰⁹. W granicach swoich zadań¹¹⁰ funkcjonariusze Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego mogą wykonywać czynności operacyjno-rozpoznawcze i analityczno-informacyjne¹¹¹, a ponadto w przypadku Służby Kontrwywiadu Wojskowego również czynności wynikające z ustawy o ochronie informacji niejawnych.

¹⁰⁷ Tamże, art. 41 ust. 1.

¹⁰⁸ Tamże, art. 41 ust. 2 i 3.

¹⁰⁹ Dz.U. 2019, poz. 687.

¹¹⁰ Art. 5 i art. 6 ust. 1 *ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*.

¹¹¹ Tamże, art. 25 pkt 1 i 2 oraz art. 26 pkt 1 i 2.

Analiza przepisów przedmiotowej ustawy dotyczących uprawnień funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego wskazuje na liczne podobieństwa do odpowiednich regulacji ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Przykładowo, można wskazać na uprawnienia funkcjonariuszy obu służb do: żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej — wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielania nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa¹¹²; zwracania się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, jak również do zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa¹¹³; posługiwania się dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, jakimi się posługuje przy wykonywaniu zadań służbowych¹¹⁴; korzystania z pomocy osób niebędących funkcjonariuszami¹¹⁵; czy zbierania, także niejawnie, wszelkich danych osobowych, jeżeli jest to uzasadnione charakterem realizowanych zadań, oraz przetwarzania ich bez wiedzy i zgody osoby, której te dane dotyczą¹¹⁶.

¹¹² Tamże art. 28 ust. 1 pkt 1.

¹¹³ Tamże, art. 28 ust. 1 pkt 2.ego

¹¹⁴ Tamże, art. 39 ust. 2–6.

¹¹⁵ Tamże, art. 40 w związku z art. 41.

¹¹⁶ Tamże, art. 38.

Michał Kamiński

Rozdział 7.

Prawne aspekty współpracy międzynarodowej służb specjalnych

Pojęcie „służby specjalne”

W wielu dostępnych opracowaniach wskazuje się na niejednoznaczność pojęcia „służby specjalne”. Zazwyczaj określa się tym terminem wywiad i kontrwywiad¹. Słownik terminów z zakresu bezpieczeństwa narodowego wydany przez Akademię Obrony Narodowej podaje: „służby specjalne” (ang. *special services*) — *ogólna nazwa dla cywilnych i wojskowych służb organizujących i prowadzących działania wywiadowcze i kontrwywiadowcze*². Wśród spotykanych w doktrynie definicji pojęcia „służby specjalne” można znaleźć taką, która będzie stawiała na pierwszym miejscu kwestię zbierania informacji: *służby specjalne to zorganizowane zazwyczaj przez państwo struktury ukierunkowane na niejawne pozyskiwanie informacji istotnych z punktu widzenia bezpieczeństwa organizatora tej działalności (państwa) bądź przeciwdziałanie ich zdobywaniu przez podobne struktury identyfikowane jako obce*³, jak również definicję uwypuklającą aspekt tajności działania — *służby specjalne to instytucje usytuowane w strukturze aparatu władzy państwowej organizacyjnie samodzielne lub wchodzące w skład innej jednostki państwowej, np. ministerialnej, instytucje uprawnione do prowadzenia różnych działań o charakterze tajnym*⁴. Wielość

¹ S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2005, s. 13; G. Rydlewski, *Służby specjalne w systemie bezpieczeństwa wewnętrznego*, w: *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 228.

² *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. P. Balcerowicz, Warszawa 2008, s. 123–124.

³ S. Zalewski, *Ewolucja modelu polskich służb specjalnych 1990–2002*, Warszawa 2002, s. 34.

⁴ J. Larecki, *Wielki leksykon służb specjalnych świata. Organizacje wywiadu, kontrwywiadu i policji politycznych świata terminologia profesjonalna i żargon operacyjny*, Warszawa 2007 s. 621.

i różnorodność dostępnych definicji może prowadzić do konkluzji, że pojęcia tego nie można w jednoznaczny, uniwersalny sposób zdefiniować⁵.

Wobec braku zgodności przedstawicieli doktryny w kwestii definicji pojęcia „służby specjalne” jedynym sposobem ustalenia zakresu podmiotowego tego terminu jest wskazanie katalogu służb państwowych, którym ustawodawca nadał taki status⁶. Obecnie funkcjonują w Polsce trzy służby państwowe określone *expressis verbis* przez ustawodawcę w aktach prawnych, regulujących ich status i funkcjonowanie (czyli w ustawach kompetencyjnych), jako służby specjalne. Ustawodawca określił tak: Centralne Biuro Antykorupcyjne, Służbę Kontrwywiadu Wojskowego oraz Służbę Wywiadu Wojskowego. Co interesujące, ustawodawca nie przypisał wprost statusu służb specjalnych ABW oraz AW w przepisach powołujących te organy. Oczywiście nie oznacza to, że służby te, pełniące funkcje cywilnego kontrwywiadu i wywiadu, są pozbawione tego statusu.

Dlatego należy uznać, iż rzeczywista, pełna definicja podmiotowa pojęcia „służby specjalne” w Polsce jest zawarta w przepisach określających szczególne formy kontroli i nadzoru nad tymi służbami ze strony ciał wchodzących w zakres władzy wykonawczej i ustawodawczej, tj. Kolegium do Spraw Służb Specjalnych i Sejmowej Komisji do Spraw Służb Specjalnych⁷.

Zakres właściwości Kolegium do Spraw Służb Specjalnych został określony w art. 11 ustawy o ABW oraz AW. W świetle przyjętego w tym przepisie rozwiązania miano „służby specjalne” przysługuje wyłącznie pięciu służbom: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Wywiadu Wojskowego oraz Służbie Kontrwywiadu Wojskowego⁸. Dlatego dalsze rozważania będą się odnosiły do tych pięciu podmiotów.

Podstawy ustawowe współpracy międzynarodowej służb specjalnych

Służby specjalne w Polsce stanowią część systemu organów władzy publicznej. Szefowie wszystkich pięciu służb specjalnych są centralnymi organami administracji rządowej, wykonującymi swoje zadania przy pomocy urzędów, jakimi są służby (ABW, AW, CBA, SKW i SWW)⁹, co jednoznacznie wpisuje służby specjalne w konstytucyjnie wyodrębniony segment władzy wykonawczej. Oznacza to, że stosuje się do nich zawarta w art. 7 Konstytucji RP norma, statuująca zasadę legalizmu, zwaną też zasadą praworządności¹⁰, zgodnie z którą organy

⁵ M. Jakubowska, *Agencja Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa państwa*, w: *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość — teraźniejszość — przyszłość. Materiały i studia*, Warszawa–Szczecin 2012, s. 9.

⁶ M. Bożek i in., dz. cyt.

⁷ M. Kolaszyński, dz. cyt., s.14–15.

⁸ M. Bożek i in., dz. cyt.

⁹ M. Kolaszyński, dz. cyt., s. 44.

¹⁰ M. Florczak-Wątor, *Komentarz...*

władzy publicznej działają na podstawie i w granicach prawa. Jak stwierdza Wiesław Skrzydło w swoim komentarzu do tego przepisu:

W państwie demokratycznym, w którym rządzi prawo, organy władzy publicznej mogą powstać tylko na podstawie prawa, a normy prawne muszą określać ich kompetencje, zadania i tryb postępowania, wyznaczając tym samym granice ich aktywności. Organy te mogą działać tylko w tych granicach. O ile jednostka ma swobodę działania zgodnie z zasadą, że co nie jest wyraźnie zabronione przez prawo, jest dozwolone, to organy władzy publicznej mogą działać tylko tam i o tyle, o ile prawo je do tego upoważnia (...) ¹¹.

Z zasady legalizmu wynika zatem, iż kompetencji organów władzy publicznej nie można domniemywać, muszą one zawsze wynikać z obowiązujących przepisów.

Wobec powyższego prowadzenie współpracy międzynarodowej przez służby specjalne musi się zawsze odbywać na podstawie i w granicach obowiązującego prawa. Musi przede wszystkim w każdym przypadku istnieć podstawa prawna do nawiązania współpracy międzynarodowej przez służbę specjalną oraz muszą zostać spełnione przewidziane prawem warunki do nawiązania takiej współpracy.

Podstawę taką mogą stanowić przepisy aktów będących źródłami prawa powszechnie obowiązującego na terenie Rzeczypospolitej Polskiej. Logiczne wydaje się, by zagadnienie to zostało uregulowane w tzw. ustawach kompetencyjnych, powołujących do istnienia służby specjalne i określających ich zadania, strukturę, kompetencje oraz prawa i obowiązki ich personelu.

Tak jest w istocie. Każda z trzech ustaw kompetencyjnych regulujących status pięciu polskich służb specjalnych zawiera przepis regulujący kwestię podejmowania przez te służby współpracy międzynarodowej.

W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu ¹² jest to art. 8. Zgodnie z treścią jego ust. 1, Szefowie Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, każdy w zakresie swojej właściwości, w celu realizacji zadań Agencji mogą podejmować współdziałanie z właściwymi organami i służbami innych państw. Przepis ten wskazuje przesłanki materialne, które uzasadniają podjęcie przez ABW lub AW współpracy międzynarodowej. Współpraca musi się mieścić w zakresie właściwości jednej z agencji oraz służyć konkretnemu celowi, w postaci realizacji jej zadań.

Właściwość Agencji Bezpieczeństwa Wewnętrznego została określona w art. 1 ustawy o ABW oraz AW. Zgodnie z treścią tego przepisu ABW jest

¹¹ W. Skrzydło, *Komentarz do art. 7 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX 2013.

¹² *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U., nr 74, poz. 676).

właściwa w zakresie ochrony bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego.

Natomiast zgodnie z art. 2 ustawy o ABW oraz AW ta ostatnia jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa.

Zadania ABW są szczegółowo wymienione w art. 5 ustawy o ABW oraz AW. Obejmują: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa (punkt 1), a także rozpoznawanie, zapobieganie i wykrywanie określonych przestępstw oraz ściganie ich sprawców (punkt 2), rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo teleinformatycznej infrastruktury krytycznej (punkt 2a), ujawnianie mienia zagrożonego przypadkiem w związku z przestępstwami wymienionymi w punkcie 2 (punkt 2 b), realizowanie w zakresie swojej właściwości zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych (punkt 3), uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (punkt 4) oraz podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (punkt 5).

Właściwość Agencji Wywiadu została natomiast określona w art. 2 ustawy o ABW oraz AW, zgodnie z którym Agencja ta jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa. Zadania AW zostały zaś wymienione w art. 6 ust. 1 ustawy o ABW oraz AW. Zadania te obejmują: uzyskiwanie, analizowanie przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego (punkt 1), rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej (punkt 2), ochronę zagranicznych przedstawicielstw Rzeczypospolitej Polskiej i ich pracowników przed działaniami obcych służb specjalnych i innymi działaniami mogącymi przynieść szkodę interesom Rzeczypospolitej Polskiej (punkt 3), zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej (punkt 4), rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej (punkt 5), rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia (punkt 6), rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa, oraz podejmowanie działań mających na celu eliminowanie tych zagrożeń (punkt 7), rozpoznawanie, przeciwdziałanie i zapobieganie

zdarzeniom o charakterze terrorystycznym, wymierzonym przeciwko obywatelom lub mieniu Rzeczypospolitej Polskiej poza granicami państwa, z wyłączeniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko personelowi lub mieniu Sił Zbrojnych Rzeczypospolitej Polskiej (punkt 7a), prowadzenie wywiadu elektronicznego (punkt 8) oraz podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (punkt 9).

Zgodnie z ust. 2 art. 8 omawianej ustawy, podjęcie współpracy międzynarodowej przez ABW lub AW może nastąpić po spełnieniu przesłanki formalnej w postaci uzyskania przez Szefa Agencji zgody Prezesa Rady Ministrów. Przepis nie określa, w jakiej formie następuje wyrażenie zgody przez Prezesa Rady Ministrów na podjęcie przez ABW i AW współpracy międzynarodowej, z czego należy wyprowadzić wniosek, iż może to nastąpić w dowolnej formie.

Przepis art. 8 ustawy o ABW oraz AW jest najstarszym i najdłużej obowiązującym w polskim prawie przepisem regulującym kwestię warunków dopuszczalności podejmowania współpracy międzynarodowej przez służby specjalne. Obowiązuje od chwili wejścia w życie ustawy o ABW oraz AW, czyli od 29 czerwca 2002 r. Co istotne, analogicznej regulacji nie zawierała uchylona na mocy przepisów ustawy o ABW oraz AW *ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa*¹³. Oznacza to, że była to pierwsza regulacja zasad i trybu nawiązywania współpracy międzynarodowej przez służby specjalne. W chwili uchwalenia ustawy o ABW oraz AW przez Sejm, druga, obok likwidowanego wówczas Urzędu Ochrony Państwa, polska służba specjalna, jaką były Wojskowe Służby Informacyjne, działała bez podstawy prawnej, wyrażonej w odrębnej ustawie kompetencyjnej. Ustawa o Wojskowych Służbach Informacyjnych została uchwalona przez Sejm dopiero rok później¹⁴.

W uzasadnieniu do projektu ustawy o ABW oraz AW zawarto następujące zdanie, wyjaśniające potrzebę wprowadzenia do tej ustawy regulacji, która znalazła się w jej art. 8:

Uwzględniając konieczność coraz szerszej współpracy międzynarodowej w dziedzinie zapobiegania, przeciwdziałania oraz wykrywania najważniejszych przestępstw takich jak terroryzm, handel narkotykami, nielegalne rozprzestrzenianie broni ABC i technologii rakietowych, handel materiałami rozszczepialnymi, pranie brudnych pieniędzy na wielką skalę przyznano Szefowi Agencji kompetencje do współdziałania z właściwymi organami i służbami innych państw, jednocześnie wprowadzając wymóg poinformowania Prezesa Rady Ministrów o zamiarze podjęcia takiej współpracy¹⁵.

¹³ Tekst jednolity: Dz.U. 1999, nr 51, poz. 526; nr 53, poz. 548; nr 110, poz. 1255; 2000, nr 73, poz. 852 oraz 2001, nr 106, poz. 1149; nr 81, poz. 877.

¹⁴ *Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych* (Dz.U., nr 139, poz. 1326; nr 179, poz. 1750 oraz 2004, nr 19, poz. 177; nr 171, poz. 1800; nr 273, poz. 2703).

¹⁵ Druk nr 276 Sejmu IV kadencji, s. 57.

Uzasadnienie dość nieprecyzyjnie odnosi się do treści przepisu art. 8 ustawy o ABW oraz AW. Jak wskazano wyżej, warunkiem podjęcia przez ABW albo AW współpracy ze służbą lub organem innego państwa nie jest jedynie poinformowanie Prezesa Rady Ministrów o zamiarze nawiązania współpracy, lecz uzyskanie jego zgody, co zakłada konieczność aktywnej interakcji ze strony Prezesa Rady Ministrów.

Zastanawiające jest, dlaczego ustawodawca dostrzegł konieczność unormowania zagadnienia podejmowania współpracy międzynarodowej przez służby specjalne dopiero po 12 latach od przemian ustrojowych, w wyniku których doszło do powołania Urzędu Ochrony Państwa. Trudno sądzić, że przez 12 lat istnienia UOP nie powstała nigdy potrzeba prowadzenia przez tę instytucję współpracy międzynarodowej. Kwestia ta znajdowała się zatem w swoistej „szarej strefie”, nieregulowanej przez ustawodawcę.

Warto zauważyć, że cywilna służba specjalna, jaką był Urząd Ochrony Państwa, w zakresie wyposażenia w kompetencje do prowadzenia współpracy międzynarodowej została potraktowana przez ustawodawcę zupełnie inaczej niż powołana tego samego dnia (6 kwietnia 1990) najważniejsza polska służba powołana do ochrony bezpieczeństwa obywateli oraz do utrzymywania bezpieczeństwa i porządku publicznego, jaką była i jest policja. W jej przypadku *współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów*¹⁶ znalazło się od początku wśród ustawowych zadań tej formacji.

Trudno dzisiaj rozstrzygnąć, dlaczego na początku lat 90. XX w. ustawodawca uznał, że tworzony wówczas UOP nie potrzebuje, w przeciwieństwie do policji, ustawowej regulacji dotyczącej współpracy z odpowiednimi służbami innych państw. Być może na początku lat 90. wydawało się, że zadania realizowane przez służby specjalne w demokratycznym państwie, związane z ochroną bezpieczeństwa i suwerenności państwa, po odcięciu całej rozbudowanej sfery działań policji politycznej, realizowanych przez Służbę Bezpieczeństwa w okresie PRL, będą ograniczały się głównie do sfery wywiadowczo-kontrwywiadowczej, a zatem realizowane będą w znacznej mierze w opozycji do działań innych państw, czy to przez zwalczanie działań szpiegowskich obcych służb na swoim terytorium (kontrwywiad), czy przez zdobywanie informacji na terenie innych państw, w sposób nierzadko naruszający obowiązujące tam prawo (wywiad). Takie ujęcie zadań służb specjalnych mogło prowadzić do wniosku, że służby specjalne powinny realizować swoje zadania samodzielnie. Być może również współpracę międzynarodową służb specjalnych postrzegano wówczas negatywnie, na podstawie doświadczeń z czasów PRL jako czynnik ograniczający suwerenność państwa. W przypadku policji, zajmującej się generalnym zwalczaniem przestępczości oraz ściganiem sprawców przestępstw, potrzeba prowadzenia współpracy międzynarodowej była czymś oczywistym. Ponadto

¹⁶ Art. 1 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst pierwotny: Dz.U., nr 30, poz. 179).

międzynarodowa współpraca służb policyjnych odbywa się jawnie i w sposób zinstytucjonalizowany, czego przejawem jest działalność Międzynarodowej Organizacji Policji Kryminalnych — Interpol, do której polska policja dołączyła już w 1990 r. Nie da się tego samego powiedzieć o współpracy służb specjalnych świata zachodniego.

W następnych latach okazało się, że ważnym obszarem działania służb specjalnych jest również rozpoznawanie zagrożeń dla podstawowych interesów ekonomicznych państwa, jak też rozpoznawanie przestępczości zorganizowanej w jej najbardziej wyrafinowanych formach, mających charakter lub zasięg międzynarodowy, a współcześnie istotną rolę w efektywnym wykonywaniu przedsięwzięć w obszarze bezpieczeństwa państwa odgrywa współdziałanie z zagranicznymi służbami partnerskimi¹⁷.

Nie bez znaczenia była integracja Polski z organizacjami międzynarodowymi świata zachodniego, w tym odpowiadającymi za bezpieczeństwo zbiorowe. Polska stała się członkiem NATO 12 marca 1999 r. Wcześniej, 22 stycznia 1999 r., została uchwalona ustawa o ochronie informacji niejawnych¹⁸, dostosowująca system ochrony informacji niejawnych w Polsce do standardów NATO. Na mocy tej ustawy służby specjalne — Urząd Ochrony Państwa i Wojskowe Służby Informacyjne — zyskały status Krajowych Władz Bezpieczeństwa, właściwych w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych¹⁹. Wprowadzenie tych przepisów spowodowało faktycznie konieczność podjęcia przez te służby współpracy ze swoimi odpowiednikami w innych krajach NATO.

W chwili podjęcia prac nad ustawą o ABW oraz AW jej twórcy musieli już sobie zdawać sprawę, że nowo powstałe służby będą musiały prowadzić współpracę z organami i służbami innych państw. Postanowiono zatem kwestię tę uregulować prawnie.

Wprowadzanie do ustawy o ABW oraz AW przepisu art. 8 wpisało się w trend zwiększania cywilnej, demokratycznej kontroli nad służbami specjalnymi.

Ukształtowany w Polsce po 1990 r. system nadzoru nad działalnością służb specjalnych zakłada, że swoją rolę w tym zakresie posiada każda z trzech władz: władza wykonawcza wyznacza kierunki działalności służb specjalnych i utrzymuje nad nimi bieżący nadzór, władza ustawodawcza zajmuje się funkcjonowaniem tajnych służb przez uchwalanie przepisów dotyczących ich zadań i uprawnień, ustalanie budżetu, żądanie informacji i przesłuchiwanie osób z kierownictwa służb, zaś władza sądownicza sprawuje nadzór nad stosowaniem części metod operacyjno-rozpoznawczych oraz osądza ewentualne nadużycia funkcjonariuszy służb²⁰. Od 1996 r. organem posiadającym decydującą rolę w wyznaczaniu kierunków zadań, nadzorze koordynacji działań oraz nadzorze

¹⁷ S. Zalewski, *Służby specjalne...*, s. 51.

¹⁸ Dz.U. nr 15, poz. 45.

¹⁹ Art. 15 *ustawy z dnia 22 stycznia 1999 o ochronie informacji niejawnych*.

²⁰ T. Kuć, *Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego”, nr 16/17, s. 190.

nad służbami specjalnymi stał się Prezes Rady Ministrów. Uprawnienia nadzorcze Prezesa Rady Ministrów wobec cywilnych służb specjalnych znalazły się wówczas zarówno w ustawie o UOP, jak też w przepisach ustawy o działach administracji rządowej²¹, w myśl której w zakresie zadań premiera znalazło się nadzorowanie organów administracji rządowej, nieujętej w zakresie działów administracji.

Wprowadzony w 2002 r. przepis art. 8 ustawy o ABW oraz AW oznacza dalsze umocnienie nadzoru konstytucyjnego organu władzy wykonawczej, jakim jest Prezes Rady Ministrów, nad działalnością służb specjalnych. Prezes Rady Ministrów może udzielić Szefowi ABW albo AW, na jego wniosek, zgody na podjęcie współpracy ze wskazaną służbą lub organem innego państwa, ale może też tej zgody odmówić i współpraca taka wówczas nie może zostać nawiązana. Podejmując decyzję w tej sprawie, Prezes Rady Ministrów może zbadać istnienie przesłanek, o których mowa w ust. 1 art. 8 ustawy o ABW oraz AW, tzn. czy planowana współpraca mieści się w zakresie właściwości danej Agencji oraz służy realizacji jej zadań, ale również czy jest zgodna z aktualnym kierunkiem polityki zagranicznej Rzeczypospolitej Polskiej. W celu umożliwienia Prezesowi Rady Ministrów dokonania rzetelnej oceny powyższych przesłanek prawidłowo sformułowany wniosek szefa danej służby powinien zawierać: nazwę obcej służby lub organu, z którym określona agencja planuje nawiązać współpracę, związałą informację na temat tej instytucji i jej kompetencji, zakres planowanej współpracy oraz uzasadnienie, wskazujące potencjalne korzyści, jakie planowana współpraca międzynarodowa ma przynieść. Jest to więc skuteczny mechanizm nadzoru nad działalnością służb specjalnych.

O przepisie art. 8 ustawy o ABW oraz AW można powiedzieć, że wyznaczył pewien trend w zakresie sposobu uregulowania kwestii nawiązywania współpracy w ustawach kompetencyjnych służb specjalnych.

W kolejnej po ustawie o ABW oraz AW *ustawie z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych* znalazł się art. 6 o następującej treści: *Szef WSI w celu realizacji zadań WSI, po uzyskaniu zgody Ministra Obrony Narodowej, może podejmować współdziałanie i zawierać porozumienia z właściwymi organami, służbami i instytucjami krajowymi oraz zagranicznymi*. Oprócz wskazania innego organu właściwego do wyrażania zgody na współpracę służby (Minister Obrony Narodowej zamiast Prezesa Rady Ministrów), co miało związek z innym umiejscowieniem służby w strukturze organów administracji rządowej, przepis ten różni się od analogicznej regulacji zawartej w ustawie o ABW oraz AW tym, że jako przedmiot zgody wyrażanej przez organ nadzorczy wskazuje nie tylko podejmowanie współdziałania, ale również zawieranie porozumień, zaś wśród podmiotów, których dotyczy zgoda, wymienia obok organów i służb instytucje, a ponadto reguluje nawiązywanie współpracy zarówno z podmiotami krajowymi, jak i zagranicznymi. Ustawa o WSI utrzymała się w obrocie prawnym

²¹ Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (tekst jednolity: Dz.U. 2016, poz. 543).

jedynie przez trzy lata, utraciła bowiem moc z dniem 30 września 2006 r. na podstawie art. 3 ustawy — Przepisy wprowadzające ustawę o SKW oraz SWW i ustawę o służbie w SKW oraz SWW²².

Zlikwidowane Wojskowe Służby Informacyjne zostały zastąpione przez nowo utworzone Służbę Kontrywywiadu Wojskowego i Służbę Wywiadu Wojskowego. W regulującej ich działanie ustawie kompetencyjnej znalazł się również przepis regulujący podejmowanie współdziałania z podmiotami zagranicznymi, tym razem w sposób bardziej zbliżony do regulacji zawartej w ustawie o ABW oraz AW. Zgodnie z art. 9 ust. 1 ustawy o SKW oraz SWW²³ Szefowie SKW i SWW, każdy w zakresie swojej właściwości, w celu realizacji zadań podległych sobie służb mogą podejmować współpracę z właściwymi organami i służbami innych państw. Zgodnie z art. 9 ust. 2 tej ustawy podjęcie współpracy, o której mowa w ust. 1, może nastąpić po uzyskaniu zgody Prezesa Rady Ministrów. Dodatkowo przepis ten nakłada na Prezesa Rady Ministrów obowiązek zasięgnięcia opinii Ministra Obrony Narodowej, przed wyrażeniem zgody. Taka konstrukcja trybu wyrażenia zgody na podjęcie przez SKW albo SWW współpracy międzynarodowej wynika z faktu, że zgodnie z art. 3 ust. 2 ustawy o SKW oraz SWW Szefowie tych służb podlegają Ministrowi Obrony Narodowej, z zastrzeżeniem określonych w tej ustawie uprawnień Prezesa Rady Ministrów lub Ministra Koordynatora Służb Specjalnych, w przypadku jego powołania. Wyrażanie zgody na podjęcie przez którąś z wojskowych służb specjalnych współpracy międzynarodowej stanowi w świetle powyższego jedną z kompetencji zastrzeżonych w ustawie o SKW oraz SWW dla Prezesa Rady Ministrów. Przyznanie tej kompetencji premierowi świadczy o dużym znaczeniu przypisywanym przez ustawodawcę współpracy międzynarodowej służb specjalnych. Zarazem jednak ustawodawca uznał, że organ, któremu bezpośrednio podlegają szefowie obu tych służb, czyli Minister Obrony Narodowej, z uwagi na sprawowanie bezpośredniego nadzoru nad działalnością służb wojskowych, również powinien mieć udział w procesie decyzyjnym dotyczącym tej kwestii. Dlatego sformułowano w art. 9 ust. 2 ustawy o SKW oraz SWW obowiązek zasięgnięcia przez Prezesa Rady Ministrów opinii Ministra Obrony Narodowej.

W przypadku piątej służby specjalnej — powstałego w 2006 r., podobnie jak dwie omówione wyżej służby wojskowe, Centralnego Biura Antykorupcyjnego — kwestię podejmowania i prowadzenia przez tę służbę współpracy międzynarodowej uregulowano początkowo w sposób odmienny niż w przypadku czterech pozostałych służb specjalnych. W tekście pierwotnym *ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*²⁴ do kwestii tej odnosił się przepis art. 2 ust. 2, który stanowił: *CBA współdziałała w zakresie swojej właściwości z organizacjami międzynarodowymi na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów*. Przepis ten odsyłał zatem do odrębnych przepisów, a także umów i porozumień międzynarodowych,

²² Dz.U. 2006, nr 104, poz. 711.

²³ Tekst jednolity: Dz.U. 2019, poz. 687.

²⁴ Dz.U. 2006, nr 104, poz. 708.

jako podstawy prawnej prowadzenia przez CBW współpracy międzynarodowej, nie przewidując dla organu nadzorującego CBA kompetencji w zakresie wyrażania zgody na taką współpracę. Jako partnerów współdziałania wskazano nie służby lub organy innych państw, lecz organizacje międzynarodowe.

Pomimo tego, iż SKW, SWW oraz CBA powstały w tym samym roku, to kwestię podejmowania przez te służby współpracy międzynarodowej uregulowano w ich ustawach kompetencyjnych zupełnie inaczej. O ile przepis art. 9 ustawy o SKW i SWW jest ewidentnie wzorowany na przepisie art. 8 ustawy o ABW oraz AW, to wzorem dla stworzenia pierwotnej wersji przepisu art. 2 ust. 2 ustawy o CBA wydaje się być raczej art. 1 ust. 2 pkt 7 ustawy o Policji, choć trzeba pamiętać, że przepis ustawy o Policji przewidywał możliwość współdziałania z policjami innych państw, zaś omawiany przepis ustawy o CBA wskazywał jako jedynego partnera współdziałania organizacje międzynarodowe. Pewną ciekawostką może być fakt, że na etapie prac parlamentarnych nad projektem ustawy o CBA początkowo art. 2 ust. 2 odnosił się do współdziałania tej służby nie tylko z organizacjami międzynarodowymi, lecz również krajowymi organami administracji rządowej i samorządowej²⁵. Na etapie prac parlamentarnych nad projektem fragment ten został wykreślony.

Wskazany wyżej stan prawny uległ zmianie z dniem 2 września 2010 r., wraz z wejściem w życie *ustawy z dnia 5 sierpnia 2010 r. o zmianie ustawy o Centralnym Biurze Antykorupcyjnym oraz ustawy o sporcie*²⁶. Art. 2 ustawy o CBA zyskał wówczas następujące brzmienie: *Szef Centralnego Bura Antykorupcyjnego w celu realizacji zadań CBA może podejmować współpracę z właściwymi organami i służbami innych państw oraz z organizacjami międzynarodowymi*. Oprócz tego, po art. 2 dodano artykuł 2a o treści: *Podjęcie współpracy, o której mowa w ust. 2 może nastąpić po uzyskaniu zgody Prezesa Rady Ministrów*. Tym samym, do ustawy o CBA wprowadzono przepisy regulujące zagadnienie warunków i trybu podejmowania przez tę służbę współpracy międzynarodowej w sposób analogiczny, jak w przypadku pozostałych czterech służb specjalnych, tzn. uzależniając możliwość podjęcia takiej współpracy od wcześniejszej zgody Prezesa Rady Ministrów. Jedyna różnica polega na tym, że wśród podmiotów zagranicznych, z którymi służba może podejmować współpracę, ustawodawca wymienił, obok właściwych organów i służb innych państw, również organizacje międzynarodowe. Ta grupa podmiotów została niejako przeniesiona do nowej wersji ustawy o CBA z wcześniejszej wersji przepisu art. 2. Tym sposobem służba ta, w wyniku nowelizacji ustawy o CBA z 2010 r., zyskała nowe możliwości współpracy międzynarodowej, nie tracąc zarazem dotychczasowych.

W komentarzu do ustawy o CBA jego autorzy (Stanisław Hoc i Przemysław Szustakiewicz) odnoszą się do sytuacji prawnej CBA po 2010 r., stwierdzając iż: *Aktualnie dozwolone jest podejmowanie współpracy z właściwymi organami*

²⁵ [https://orka.sejm.gov.pl/Druki5ka.nsf/0/C7181EB8C7824F41C125710A0045AD56/\\$file/275.pdf](https://orka.sejm.gov.pl/Druki5ka.nsf/0/C7181EB8C7824F41C125710A0045AD56/$file/275.pdf), [dostęp: 31 V 2021].

²⁶ Dz.U. 2010, nr 151, poz. 1014.

*i służbami innych państw oraz z organizacjami międzynarodowymi, ale po uzyskaniu zgody Prezesa Rady Ministrów. Jest to rozwiązanie prawidłowe, powstaje jednak pytanie, dlaczego twórcy ustawy o CBA nie pamiętali o konieczności takiej kompetencji*²⁷. Komentarz podaje również informację, iż z danych o wynikach działalności CBA w 2011 r. wynika, że w 2011 r. CBA uzyskało zgodę Prezesa Rady Ministrów na podejmowanie współpracy w zakresie zwalczania korupcji i działalności godzącej w interesy ekonomiczne państwa, prewencji, edukacji i informacji antykorupcyjnej z organami i służbami 37 państw oraz z 10 organizacjami i instytucjami pozarządowymi.

Wobec powyższego uprawnione będzie twierdzenie, że od 2010 r. funkcjonuje w Polsce w miarę spójny system regulacji ustawowych dotyczących podejmowania współpracy międzynarodowej przez służby specjalne. Służby te (ABW, AW, SKW, SWW i CBA) mogą podejmować w zakresie swojej właściwości i w celu realizacji swoich zadań współdziałanie z właściwymi organami i służbami innych państw (CBA dodatkowo z organizacjami międzynarodowymi). Oprócz tego istnieje spójny system cywilnego nadzoru nad prowadzeniem przez służby specjalne współpracy międzynarodowej, polegający na wymogu wydania przez Prezesa Rady Ministrów zgody na jej podjęcie (w przypadku SKW i SWW w procesie decyzyjnym uczestniczy dodatkowo, przez wydanie opinii, Minister Obrony Narodowej). Należy uznać, że w celu efektywnego wykonania swych nadzorczych kompetencji Prezes Rady Ministrów przed wydaniem decyzji w przedmiocie zgody na współpracę międzynarodową powinien dokonać oceny zaistnienia ustawowych przesłanek podjęcia przez daną służbę współpracy międzynarodowej z zagranicznym podmiotem. Ocenie Prezesa Rady Ministrów powinno w szczególności podlegać to, czy współdziałanie mieści się w zakresie właściwości danej służby, czy służy realizacji jej zadań, a także czy obca służba lub organ, z którym planuje współpracę polska służba, jest służbą właściwą, czyli czy jej kompetencje korelują z kompetencjami polskiej służby oraz celem podejmowanej współpracy. Organ nadzorczy, podejmując decyzję w sprawie wydania zgody na współpracę, może i powinien również wziąć pod uwagę i to, czy nawiązanie tej współpracy odpowiada kierunkowi polityki zagranicznej prowadzonej przez Rzeczpospolitą Polską (za której prowadzenie, zgodnie z art. 146 ust. 1 Konstytucji RP, odpowiada Rada Ministrów).

Z treści przepisów art. 8 ustawy o ABW oraz AW, art. 9 ustawy o SKW oraz SWW i art. 2 ust. 2 i 2a ustawy o CBA nie wynika, czy zgoda Prezesa Rady Ministrów na współdziałanie z obcym podmiotem powinna mieć charakter incydentalny czy stały, wobec czego należy przyjąć, że dopuszczalne są obie sytuacje, w zależności od treści złożonego przez szefa danej służby wniosku oraz decyzji organu nadzorczego. Z treści wskazanych przepisów nie wynika także, czy współdziałanie polskiej służby specjalnej z obcym podmiotem, na które wyraża zgodę Prezes Rady Ministrów, może dotyczyć wszystkich zadań danej służby,

²⁷ S. Hoc, P. Szustakiewicz, *Komentarz do art. 2 ustawy o Centralnym Biurze Antykorupcyjnym*, w: *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, LEX/el., 2012.

tylko niektórych, czy może tylko konkretnej sprawy. Wobec tego należy uznać, że wszystkie te opcje są możliwe, w zależności od sposobu sformułowania przez szefa danej służby wniosku do Prezesa Rady Ministrów, jak też od treści zgody udzielonej przez Prezesa Rady Ministrów. Naturalnym ograniczeniem zakresu współpracy będzie zakres kompetencji służby zagranicznej, rzadko bowiem zdarza się, by kompetencje służb z różnych państw, nawet zajmujących analogiczne miejsca w strukturze systemów bezpieczeństwa swoich państw, pokrywały się ze sobą.

Jak wskazano już wyżej, przy okazji omawiania art. 8 ustawy o ABW oraz AW, nie ma wymogów prawnych odnoszących się do formy wniosku o udzielenie zgody na współpracę, jak też samej zgody, odnosi się to również do analogicznych przepisów ustawy o SKW oraz SWW, jak też ustawy o CBA.

W komentarzu do art. 8 ustawy o ABW oraz AW autorstwa P. Opalińskiego, M. Rogalskiego i P. Szustakiewicza, który — z uwagi na analogiczną formę zapisu — należałoby odnieść również do art. 9 ustawy o SKW oraz SWW i art. 2 oraz art. 2 ust. 2 i 2a ustawy o CBA, wspomniani autorzy, próbując wskazać moment, w którym służba powinna uzyskać zgodę Prezesa Rady Ministrów na prowadzenie współpracy międzynarodowej, stwierdzają, co następuje: *Przyjąć należy, że trzeba uzyskać zgodę Prezesa Rady Ministrów nie tylko przed podjęciem już faktycznej (realnej współpracy), ale także na prowadzenie rozmów i uzgodnień z właściwymi organami i służbami innych państw dotyczących prowadzenia tej współpracy*²⁸. Wydaje się jednak, że uznawanie, iż zgoda Prezesa Rady Ministrów jest wymagana na każdy kontakt polskich służb ze służbą obcą, byłoby nadmierowe i nie odpowiadało realiom, np. w zakresie pracy wywiadowczej. Uzasadnione wydaje się, z uwagi na ekonomię działania organu nadzorczego, aby służby występowały o zgodę na współpracę ze służbami, co do których istnieje już wiedza na temat chęci współpracy z ich strony, co wymaga jakiejś formy kontaktu. Niewątpliwie jednak wypada się zgodzić, że podjęcie rozmów na temat ram i trybu planowanej współpracy, a tym bardziej podjęcie przez polską służbę współdziałania z obcą służbą w zakresie realizacji swoich zadań ustawowych, powinno być już poprzedzone wcześniejszym uzyskaniem zgody na współpracę międzynarodową.

Omówiony mechanizm udzielania przez Prezesa Rady Ministrów zgody na podejmowanie przez służby specjalne współpracy międzynarodowej stanowi jeden z elementów uprawnień nadzorczych tego organu nad służbami specjalnymi, służących zapewnieniu możliwości wykonywania jego konstytucyjnych prerogatyw, obejmujących zgodnie z art. 148 Konstytucji RP m.in. zapewnienie wykonywania polityki Rady Ministrów i określanie sposobów jej wykonywania, podczas gdy do konstytucyjnych zadań Rady Ministrów należy zapewnianie bezpieczeństwa wewnętrznego i zewnętrznego państwa oraz porządku publicznego²⁹.

²⁸ B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, s. 32.

²⁹ P. Burczaniuk, *System nadzoru i kontroli nad służbami specjalnymi w Polsce — stan obecny na tle analizy prawno-porównawczej wybranych państw. Postulaty de lege ferenda*,

Rola Ministra-Koordynatora Służb Specjalnych

W chwili obecnej, uprawnienia nadzorcze Prezesa Rady Ministrów w zakresie podejmowania przez służby specjalne współpracy międzynarodowej są wykonywane przez inny organ — Ministra-Koordynatora Służb Specjalnych. Przesądza o tym przepis § 5 pkt 3 *rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra — członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych*³⁰. Zgodnie z treścią tego przepisu do zadań ministra w zakresie koordynowania działalności służb specjalnych należy wyrażanie zgody na współdziałanie Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu z właściwymi organami i służbami innych państw, a w przypadku Centralnego Biura Antykorupcyjnego także z organizacjami międzynarodowymi. Tym samym Prezes Rady Ministrów, w drodze rozporządzenia wydanego na podstawie art. 33 ust. 1 *ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów*³¹, pozwalającego szefowi rządu na ustalenie szczegółowego zakresu działania ministra, a także obsługującego go ministerstwa, przeniósł swoją kompetencję do wyrażania zgody na podejmowanie współpracy międzynarodowej przez cywilne służby specjalne na inny naczelny organ administracji rządowej.

Piotr Burczaniuk w swoim rozdziale poświęconym systemowi nadzoru i kontroli nad służbami specjalnymi w Polsce uznał Ministra-Koordynatora Służb Specjalnych za jeden z najistotniejszych elementów związanych z nadzorem i kontrolą nad służbami specjalnymi, umiejscowionych w ramach egzekutywy. Do jego cech charakterystycznych zaliczył niestałość tego urzędu, w pełni uzależnionego od woli Prezesa Rady Ministrów, (...) *który na podstawie art. 148 Konstytucji RP powierza mu wykonywanie zadań delegowanych z pierwotnych uprawnień samego szefa rządu, w sposób określony w art. 33 ust. 1 Ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów, tj. przez wydanie rozporządzenia określającego zakres jego działania co czyni go tzw. ministrem bez teki*³².

Tomasz Kuć uznał możliwość powołania Ministra-Koordynatora Służb Specjalnych za próbę rozwiązania problemu dotyczącego realnych możliwości wykonywania przez Prezesa Rady Ministrów osobistego nadzoru nad bieżącą pracą służb specjalnych wobec konieczności kierowania całością prac rządu³³.

Pomimo tego, iż zadania realizowane przez Ministra-Koordynatora są uzależnione od zakresu upoważnienia udzielonego mu przez Prezesa Rady Ministrów w wydanym przez niego rozporządzeniu, to ustawy kompetencyjne służb specjalnych wiążą z jego powołaniem pewne prerogatywy, automatycznie przechodzące z Prezesa Rady Ministrów na jego osobę bądź włączają go wraz

w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, Warszawa 2017, s. 30–32.

³⁰ Dz.U. 2019, poz. 2273.

³¹ Dz.U. 2021, poz. 178 i 1192.

³² P. Burczaniuk, dz. cyt., s. 37.

³³ T. Kuć, dz. cyt., s. 194.

z powołaniem w istniejące procedury nadzorcze³⁴. Wśród tych prerogatyw, do których zalicza się koordynowanie współpracy służb specjalnych w celu realizacji ustawowych zadań czy wyrażanie zgody na kontynuowanie sprawy nie pozostającej w zakresie kompetencji danej służby, nie ma jednak udzielania zgody na współpracę międzynarodową³⁵. Ustawodawca nie uznał zatem wyrażania zgody na podejmowanie przez służby specjalne współdziałania z właściwymi służbami i organami innych państw za element niezbędnego instrumentarium, w które koniecznie musi zostać wyposażony minister powołany w celu koordynacji działania służb specjalnych.

Pierwszym wydanym po wejściu w życie ustawy o ABW oraz AW aktem prawnym powołującym ministra właściwego do spraw koordynacji służb specjalnych było *rozporządzenie Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie szczegółowego zakresu działania Ministra-członka Rady Ministrów — Koordynatora Służb Specjalnych, Zbigniewa Wassermanna*³⁶. Pomimo iż ocenia się, że ten akt prawny dał ówczesnemu koordynatorowi wiele formalnych instrumentów stwarzających możliwość realnej kontroli całości działań służb specjalnych, w tym służb wojskowych³⁷, nie przeniósł on na Ministra-Koordynatora Służb Specjalnych kompetencji Prezesa Rady Ministrów do wyrażania zgody na podejmowanie przez służby specjalne współdziałania z zagranicznymi podmiotami. Przepis § 2 pkt 4 wspomnianego rozporządzenia stanowił jednak, iż do zakresu działania ministra należy koordynowanie współdziałania służb specjalnych z właściwymi organami i służbami innych państw. Analogiczne rozwiązania zostały zawarte w dwóch rozporządzeniach Prezesa Rady Ministrów regulujących zakres działania tego ministra: z 3 sierpnia 2006 r.³⁸ i 21 września 2007 r.³⁹, w których przepis mówiący o kompetencji ministra w zakresie koordynacji współdziałania z właściwymi organami i służbami innych państw został oznaczony jako § 2 punkt 4.

Po raz pierwszy do przeniesienia kompetencji Prezesa Rady Ministrów do wyrażania zgody na współpracę służb specjalnych z podmiotami zagranicznymi doszło w przepisach *rozporządzenia Prezesa Rady Ministrów z dnia 24 listopada 2011 r. w sprawie szczegółowego zakresu działania Jacka Cichockiego — Ministra Spraw Wewnętrznych — w zakresie koordynacji służb specjalnych*⁴⁰. W rozporządzeniu tym znalazł się przepis § 1 ust. 2 pkt 4, zaliczający do zadań

³⁴ Por. P. Burczaniuk, dz. cyt., s. 37.

³⁵ Tamże, s. 37–38.

³⁶ Dz.U. 2006, nr 141, poz. 998.

³⁷ T. Kuć, dz. cyt., s. 195.

³⁸ *Rozporządzenie Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie szczegółowego zakresu działania Ministra-członka Rady Ministrów — Koordynatora Służb Specjalnych, Zbigniewa Wassermanna* (Dz.U. 2006, nr 141, poz. 998).

³⁹ *Rozporządzenie Prezesa Rady Ministrów z dnia 21 września 2007 r. w sprawie szczegółowego zakresu działania Ministra-członka Rady Ministrów — Koordynatora Służb Specjalnych, Zbigniewa Wassermanna* (Dz.U. 2007, nr 178, poz. 1255).

⁴⁰ Dz.U. 2011, nr 254, poz. 1524.

ministra powołanego do koordynacji służb specjalnych, wykonywanych w imieniu Prezesa Rady Ministrów oraz z jego upoważnienia, wyrażanie zgody na współdziałanie z właściwymi organami i służbami innych państw przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, a w przypadku Centralnego Biura Antykorupcyjnego także z organizacjami międzynarodowymi. Warto zauważyć, że do scedowania kompetencji premiera w zakresie wyrażania zgody na współdziałanie z podmiotami zagranicznymi doszło wyłącznie w odniesieniu do cywilnych służb specjalnych. W stosunku do służb wojskowych miała zastosowanie nadal regulacja ustawowa, zgodnie z którą zgodę na współpracę międzynarodową wyrażał Prezes Rady Ministrów po zasięgnięciu opinii Ministra Obrony Narodowej. Identyczny przepis znalazł się również w kolejnym rozporządzeniu Prezesa Rady Ministrów, które powierzało zadanie koordynacji służb specjalnych następnemu ministrowi spraw wewnętrznych⁴¹, jak i następnym, które po rekonstrukcji rządu powierzyło ponownie zadanie koordynacji służb specjalnych Jackowi Cichockiemu, już jako ministrowi bez teki⁴².

Zmiana rządu spowodowana werdyktem wyborczym z jesieni 2016 r. (właściwie 2015 r. — przyp. autora) *stała się przyczynkiem do kolejnej zmiany koncepcji prowadzenia nadzoru nad służbami specjalnymi przez egzekutywę. Sprowadza się ona do scedowania zasadniczej części prerogatyw i obowiązków szefa rządu na członka Rady Ministrów zajmującego się jedynie kontrolą i nadzorem nad służbami*⁴³. Rzeczywiście, na mocy przepisów *rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra — Członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych*⁴⁴, nowo powołany minister otrzymał wyjątkowo szerokie kompetencje w zakresie nadzoru nad służbami specjalnymi, a także w zakresie kontroli i koordynowania ich działalności. W przepisach omawianego rozporządzenia zadania Ministra-Koordynatora zostały podzielone na grupy według kryterium przedmiotowego. Zadania nadzorcze wyszczególniono w przepisie § 2, kontrolne w § 3, koordynacyjne w § 4, pozostałe zadania w § 5. Wyrażanie przez ministra zgody na współdziałanie Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu z właściwymi organami i służbami innych państw, a w przypadku Centralnego Biura Antykorupcyjnego także z organizacjami międzynarodowymi, zostało zaliczone do grupy zadań koordynacyjnych i uregulowane w przepisie § 4 pkt 3. Nie jest to jedyne zawarte w tekście omawianego rozporządzenia zadanie Ministra-Koordynatora związane ze współpracą międzynarodową. Innym jego zadaniem, z obszaru koordynowania działalności

⁴¹ *Rozporządzenie Prezesa Rady z dnia 28 lutego 2013 r. w sprawie szczegółowego zakresu działania Bartłomieja Sienkiewicza — Ministra Spraw Wewnętrznych — w zakresie koordynacji służb specjalnych* (Dz.U. 2013, poz. 22).

⁴² *Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2014 r. w sprawie szczegółowego zakresu działania Ministra — Członka Rady Ministrów Jacka Cichockiego w zakresie koordynacji służb specjalnych* (Dz.U. poz. 1276).

⁴³ T. Kuć, dz. cyt., s. 198.

⁴⁴ Dz.U. 2015, poz. 1921.

służb specjalnych, zostało bowiem *zapewnienie optymalnych warunków dla współpracy służb specjalnych ze służbami innych państw i organizacjami międzynarodowymi*. Natomiast do zadań ministra w zakresie nadzoru nad działalnością służb specjalnych zaliczono uregulowane w § 2 pkt 6 *wyznaczanie celów i kierunków rozwoju współpracy międzynarodowej służb specjalnych oraz dokonywanie oceny efektów tej współpracy*. Ponadto Minister-Koordynator Służb Specjalnych, niezależnie od wskazanych uprawnień koordynacyjnych i nadzorczych w stosunku do służb specjalnych, otrzymał również uprawnienie do samodzielnego prowadzenia współpracy międzynarodowej z organami innych państw oraz instytucjami międzynarodowymi zajmującymi się nadzorem, koordynacją i kontrolą służb specjalnych (§ 5 pkt 1). W świetle powyższego uprawnione będzie twierdzenie, iż Minister-Koordynator Służb Specjalnych otrzymał w 2015 r. zestaw kompetencji pozwalających objąć efektywnym nadzorem obszar prowadzonej przez służby specjalne współpracy międzynarodowej. Wśród narzędzi, w jakie szef rządu wyposażył Ministra-Koordynatora, była kompetencja do wyrażania zgody na współdziałanie z zagranicznymi podmiotami, ograniczona jednak tylko do służb cywilnych, podobnie jak miało to miejsce w przypadku rozporządzeń statuujących kompetencje poprzednich ministrów właściwych w zakresie koordynacji działań służb specjalnych: Jacka Cichockiego i Bartłomieja Sienkiewicza. Z kolei zadania dotyczące wyznaczania celów i kierunków rozwoju współpracy międzynarodowej służb specjalnych oraz dokonywania oceny rezultatów tej współpracy, a także zapewnienia optymalnych warunków dla współpracy służb specjalnych ze służbami innych państw i organizacjami międzynarodowymi, objęły już wszystkie służby specjalne, z wojskowymi włącznie.

Powyższe kompetencje Ministra-Koordynatora Służb Specjalnych obowiązują do chwili obecnej, bowiem identyczne, jak omówione wyżej, przepisy znalazły się w treści dwóch kolejnych rozporządzeń Prezesa Rady Ministrów ustalających szczegółowy zakres działania tego organu, w ramach dwóch kolejnych składów Rady Ministrów powołanych od tego czasu — z 13 grudnia 2017 r.⁴⁵ i 18 listopada 2019 r.⁴⁶

Porównanie z regulacjami prawnymi innych służb

Omówione wyżej rozwiązania prawne, polegające na wprowadzeniu ustawowego wymogu uzyskania zgody organu nadzorującego na współdziałanie służby z podmiotem zagranicznym są charakterystyczne wyłącznie dla ustaw

⁴⁵ *Rozporządzenie Prezesa Rady Ministrów z dnia 13 grudnia 2017 r. w sprawie szczegółowego zakresu działania Ministra — Członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych* (Dz.U. 2017, poz. 2332).

⁴⁶ *Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra — Członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych* (Dz.U. 2019, poz. 2273).

kompetencyjnych polskich służb specjalnych. W przypadku ustaw kompetencyjnych służb odpowiedzialnych za ochronę bezpieczeństwa i porządku publicznego, podległych ministrowi spraw wewnętrznych, ustawodawca zdecydował się na inne rozwiązanie, polegające na przypisaniu tym służbom generalnej kompetencji do prowadzenia współpracy międzynarodowej. Szczegółowe rozwiązania legislacyjne w tym zakresie są różne.

W przypadku *ustawy z dnia 6 kwietnia 1990 r. o Policji*⁴⁷ *współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi, a także z organami instytucjami Unii Europejskiej na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów* znalazło się, jako pkt 7, wśród 11 w chwili obecnej zadań tej formacji, skatalogowanych w art. 1 ust. 2. Oprócz tego ustawodawca nałożył na policję, odrębnym przepisem (art. 2 ust. 3), obowiązek realizacji zadań wynikających z przepisów prawa Unii Europejskiej oraz umów i porozumień międzynarodowych, na zasadach w nich określonych.

Nieco inne rozwiązanie legislacyjne przyjęto w ustawie o Straży Granicznej⁴⁸. W ustawie tej nie wpisano współpracy międzynarodowej do katalogu zadań służby, zawartego w art. 1 ust. 2 i ust. 2a omawianej ustawy. Uregulowano to zagadnienie w odrębnym przepisie art. 1 ust. 3 o treści: *Straż Graniczna w zakresie określonym w ust. 2 i 2a współdziała z właściwymi organami i instytucjami Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi, w tym z Międzynarodową Organizacją Policji Kryminalnej — Interpol.* W przypadku ustawy o Straży Granicznej ustawodawca nie potraktował zatem prowadzonej przez tę służbę współpracy międzynarodowej jako zadania, a jedynie jako przysługujące jej narzędzie, służące realizacji jej ustawowych zadań. Jednocześnie do ustawy o Straży Granicznej wprowadzono analogiczną do art. 1 ust. 3 ustawy o Policji regulację art. 1 ust. 2a, nakładającą na Straż Graniczną obowiązek realizacji zadań wynikających z przepisów prawa Unii Europejskiej oraz umów i porozumień międzynarodowych.

W najnowszej *ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, współdziałanie z organami i służbami innych państw oraz organizacjami międzynarodowymi na podstawie umów i porozumień oraz odrębnych przepisów* zaliczono do kompetencji komendanta tej służby, wymienionych w art. 14 omawianej ustawy kompetencyjnej (pkt 5).

W żadnej z wymienionych trzech ustaw nie uzależniono podjęcia przez służbę współdziałania z właściwą służbą lub organem innego państwa od wymogu wcześniejszego uzyskania zgody organu nadzorującego tę służbę, pomimo iż ustawy te określają status komendantów policji, Straży Granicznej i Służby Ochrony Państwa jako centralnych organów administracji rządowej, podległych ministrowi właściwemu do spraw wewnętrznych.

Ustawy o Policji i Służbie Ochrony Państwa uzależniają jednak możliwość podejmowania przez te służby współpracy z odpowiednimi służbami i organami

⁴⁷ Dz.U. 2020, poz. 360.

⁴⁸ Tamże, poz. 305.

innych państw oraz organizacjami międzynarodowymi od istnienia niezależnej podstawy prawnej w postaci zawartej umowy, porozumienia lub odrębnych przepisów. Ustawa o Straży Granicznej takiego wymogu nie stawia, wymagając jedynie, by współdziałanie z zagranicznym podmiotem służyło realizacji zadań tej służby.

Szukając odpowiedzi na pytanie, dlaczego ustawodawca zdecydował się na odmienne niż w przypadku służb ochrony bezpieczeństwa i porządku publicznego uregulowanie kwestii podejmowania przez służby specjalne współdziałania z podmiotami zagranicznymi, uzależniając podjęcie przez te służby współdziałania od wcześniejszej zgody Prezesa Rady Ministrów, wskazać można na prawdopodobne przekonanie o szczególnym znaczeniu takiej współpracy dla najbardziej żywotnych interesów państwa, co uzasadnia objęcie jej szczególnym nadzorem organu władzy politycznej. Z drugiej strony, można wskazać na przekonanie, że współpraca służb specjalnych, z uwagi na jej niejawny charakter, ma mniej formalny charakter niż w przypadku służb policyjnych, wobec czego oparcie takiej współpracy na umowach i porozumieniach międzynarodowych lub odrębnych przepisach, jak w przypadku policji i SOP, nie byłoby rozwiązaniem efektywnym.

Analiza dostępnych informacji na temat aktów prawnych regulujących działalność służb specjalnych w krajach Europy Zachodniej prowadzi do wniosku, że kwestie dopuszczalności podejmowania przez służby specjalne współpracy międzynarodowej zostały uregulowane w różny sposób.

W przypadku Francji do zadań Generalnej Dyrekcji Bezpieczeństwa Wewnętrznego (*Direction Generale de la Securite Interieure* — DGSI) należy zapewnienie niezbędnych instrumentów komunikacji z innymi służbami i organami, zarówno francuskimi, jak i zagranicznymi, oraz ustanawianie w tym celu oficerów łącznikowych. Brakuje jednak wymogu uzyskania zgody organu nadzorującego (w tym wypadku ministra spraw wewnętrznych) na możliwość podjęcia współpracy ze służbami partnerskimi⁴⁹.

W Hiszpanii do zadań Narodowego Centrum Wywiadu (*Centro Nacional de Inteligencia* — CNI), pełniącego w tym kraju funkcje wywiadu i kontrwywiadu, zalicza się wspieranie współpracy ze służbami wywiadowczymi innych państw lub organizacjami międzynarodowymi, w celu skutecznej realizacji swoich celów, zgodnie z ramami wyznaczonymi przez rząd⁵⁰.

W przypadku Królestwa Niderlandów, na mocy jednej ustawy — o służbach wywiadowczych i bezpieczeństwa z 2002 r. — uregulowano działalność dwóch służb specjalnych: cywilnej — Generalnej Służby Bezpieczeństwa i Wywiadu (*Algemeene Inlichtingen — en Veiligheidsdienst* — AIVD) oraz wojskowej — Agencji Wywiadu Obronnego (*Militaire*

⁴⁹ P. Burczaniuk i in., *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach*, Emów 2017, s. 21.

⁵⁰ Tamże, s. 28.

Inlichtingen — en Veiligheidsdienst — MIVD)⁵¹. Wymieniona ustawa nakłada na szefów obu służb obowiązek utrzymywania kontaktów z zagranicznymi służbami partnerskimi. Zarówno AIVD, jak i MIVD, przysługuje prawo udzielania służbom specjalnym innych państw informacji istotnych z punktu widzenia realizacji ich zadań, a także wsparcia o charakterze technicznym lub innego rodzaju, o ile nie zagraża to dobrom chronionym przez służby holenderskie i nie utrudnia realizacji ich zadań. Właściwy minister nadzorujący daną służbę może upoważniać szefów służb do wydawania zgody na udzielenie informacji obcym służbom lub udzielenie im informacji w nagłych wypadkach⁵².

W Niemczech z kolei, Federalny Urząd Ochrony Konstytucji może nawiązać z organem lub służbą obcego państwa współpracę, polegającą na wymianie informacji wywiadowczych po spełnieniu pewnych warunków. Ustawa o współpracy między Republiką Federalną a krajami związkowymi w zakresie dotyczącym ochrony konstytucji oraz o Urzędzie Ochrony Konstytucji stanowi, że aby wymiana danych była dopuszczalna, jeśli występuje potrzeba zweryfikowania informacji o możliwym istnieniu poważnego zagrożenia dla bezpieczeństwa Republiki Federalnej Niemiec oraz innego państwa, druga strona gwarantuje przestrzeganie obowiązujących w Niemczech standardów konstytucyjnych, cele współpracy i dalsze wykorzystywanie danych zostają określone w formie pisemnej przed rozpoczęciem współpracy między służbami i wreszcie musi zostać wydana zgoda Ministerstwa Spraw Wewnętrznych. Zasadniczo dopuszczalna jest współpraca Urzędu Ochrony Konstytucji ze służbami Państw Członkowskich NATO i Unii Europejskiej. Na współpracę ze służbami z państw spoza tego obszaru Ministerstwo Spraw Wewnętrznych może wyrazić zgodę w sytuacjach wyjątkowych — w przypadku czynności prowadzonych w celu zapobieżenia popełnieniu poważnych przestępstw przeciwko istnieniu lub bezpieczeństwu państwa albo organizacji międzynarodowej. Zgodnie z postanowieniami swojej ustawy kompetencyjnej Urząd Ochrony Konstytucji może uczestniczyć we wspólnych przedsięwzięciach (forach współpracy) służb specjalnych, pod warunkiem że dane przekazane przez tę służbę nie mogą zostać przekazane stronie trzeciej bez jej zgody i mogą zostać wykorzystane wyłącznie w celach, w jakich zostały przekazane⁵³.

Umowy międzynarodowe jako podstawa prawna współpracy międzynarodowej służb specjalnych

Zgodnie z treścią art. 87 Konstytucji RP źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są, oprócz Konstytucji, ustaw i rozporządzeń, ratyfikowane umowy międzynarodowe. Źródłami prawa powszechnie obowiązującego są wszystkie ratyfikowane umowy międzynarodowe, niezależnie od tego,

⁵¹ Tamże, s. 29.

⁵² Tamże, s. 35.

⁵³ Tamże, s. 45.

czy ich ratyfikacja wymagała uprzedniej zgody wyrażonej w ustawie i niezależnie od trybu wyrażenia zgody na ich ratyfikację. Pozostałe umowy międzynarodowe, które nie podlegają ratyfikacji, mają status odpowiadający aktom prawa wewnętrznego, opisanym w art. 93 Konstytucji RP, które wiążą tylko jednostki organizacyjne podległe organowi, który akt wydał. Akty te jednak pozostają wiążące dla Rzeczypospolitej Polskiej w relacjach międzynarodowych. Umowy międzynarodowe ratyfikowane przez prezydenta za uprzednią zgodą wyrażoną w ustawie, w trybie przewidzianym w art. 89 ust. 1 Konstytucji RP, a zatem umowy dotyczące pokoju, sojuszy, układów politycznych lub układów wojskowych, wolności, praw lub obowiązków obywatelskich określonych w Konstytucji, członkostwa Rzeczypospolitej Polskiej w organizacji międzynarodowej, znacznego obciążania państwa pod względem finansowym i wreszcie spraw uregulowanych w ustawie lub, w których Konstytucja wymaga ustawy zgodnie z unormowaniem zawartym w art. 91 ust. 2 Konstytucji, mają pierwszeństwo przed ustawą, jeśli ustawy tej nie da się pogodzić z umową⁵⁴. Natomiast pozostałe ratyfikowane umowy międzynarodowe mają w hierarchii źródeł prawa pozycję niższą od ustaw, a zatem muszą być zgodne z ustawami⁵⁵.

Skoro umowy międzynarodowe mogą stanowić źródło prawa powszechnie obowiązującego, mogą również nakładać prawa i obowiązki na organy i służby państwowe, w tym służby specjalne. Mogą zatem również stanowić podstawę prawną do prowadzenia przez służby specjalne współpracy międzynarodowej.

Tak jest w istocie. Dotyczy to przede wszystkim umów bilateralnych. Przyczyną tego stanu rzeczy jest okoliczność, że sposób opracowywania umów wielostronnych, co najczęściej odbywa się w ramach organizacji międzynarodowych, oraz ich otwarcie do podpisu przed dużą liczbą państw (nawet praktycznie nieograniczoną, jak w przypadku umów przyjmowanych w ramach systemu prawnego Organizacji Narodów Zjednoczonych), mających zróżnicowane interesy i odmienne systemy prawne, wymusza najczęściej wysoki poziom ogólności tych umów. Natomiast zawarcie umowy dwustronnej umożliwia szczegółowe uregulowanie współpracy organów i instytucji dwóch mających wspólne interesy krajów w określonym obszarze.

Wpływ na działalność służb specjalnych mają przede wszystkim dwie grupy zawieranych przez Rzeczpospolitą Polską umów międzynarodowych — umowy o współpracy w zakresie zwalczania przestępczości oraz umowy o ochronie informacji niejawnych.

Umowy o współpracy w zakresie zwalczania przestępczości są zawierane w celu umożliwienia skutecznej współpracy organów i służb odpowiedzialnych za zwalczanie poważnych przestępstw. Regulują one współpracę organów

⁵⁴ Por. P. Radziewicz, *Komentarz do art. 89 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej...*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziewicz.

⁵⁵ Por. tenże, *Komentarz do art. 91 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej...*

ścigania zasadniczo na etapie przedprocesowym, gdyż współpracę procesową regulują odrębne umowy o wzajemnej pomocy w sprawach karnych. Niezbędnym elementem tego rodzaju umów jest określenie katalogu przestępstw, przy zwalczaniu i zapobieganiu których strony umowy planują współpracować. Zazwyczaj katalog ten obejmuje przestępczość zorganizowaną, terroryzm i inne poważne przestępstwa występujące w obrocie międzynarodowym, jak nielegalny obrót bronią, amunicją, środkami odurzającymi, nielegalną migracją czy handel ludźmi. Najważniejszym celem przedmiotowych umów jest umożliwienie wymiany informacji między organami obu stron uprawnionymi do zwalczania przestępstw, dlatego zawierają zawsze przepis wskazujący organy właściwe do współpracy na ich podstawie. Oprócz szefów służb podległych ministrowi właściwemu do spraw wewnętrznych i finansów publicznych na liście tych organów systematycznie zamieszcza się szefów służb specjalnych posiadających uprawnienia dochodzeniowo-śledcze, czyli do 2002 r. Szefa Urzędu Ochrony Państwa, od 2002 r. Szefa Agencji Bezpieczeństwa Wewnętrznego, zaś po 2006 r. również Szefa Centralnego Biura Antykorupcyjnego. Oprócz wymiany informacyjnej umowy tego rodzaju przewidują często różne formy współpracy operacyjnej właściwych organów, jak: przesyłka niejawnie nadzorowana, działania pod przykryciem, obserwacja, wspólne patrole czy pościg transgraniczny (ostatnie formy współpracy są możliwe do realizacji w ramach współpracy z krajami graniczącymi z Polską). Inne spotykane w tego rodzaju umowach formy współpracy to powoływanie grup roboczych w celu realizacji postanowień umowy, prowadzenie współpracy naukowo-technicznej, wymiana doświadczeń czy ekspertów. Standardowo w tego typu umowach reguluje się również zagadnienia ochrony informacji niejawnych oraz danych osobowych wymienianych przy ich realizacji. Jeśli z danym państwem zawarto wcześniej umowę o ochronie informacji niejawnych, umowa o zwalczaniu przestępczości zawiera najczęściej przepis odsyłający do postanowień umowy o ochronie informacji niejawnych. Inne spotykane w tego typu umowach uregulowania to np. szczególne regulacje dotyczące zwalczania terroryzmu czy upoważnienie organów właściwych na podstawie danej umowy do współpracy do zawierania porozumień wykonawczych, regulujących w sposób szczegółowy zasady i tryb współpracy między nimi.

Służby specjalne mogą prowadzić współpracę na podstawie przedmiotowych umów z organami państwa drugiej strony, wskazanymi do jej wykonywania w treści umowy. Jeśli umowa zawiera przepis upoważniający organy właściwe do współpracy do zawierania na jej podstawie pisemnych porozumień z organami drugiej strony, szef polskiej służby specjalnej może zawierać takie porozumienia z organami drugiej strony. Sam fakt wymieniania dwóch organów jako właściwych do współpracy w treści umowy może jednak nie wystarczyć do jej nawiązania. Warunkiem niezbędnym nawiązania takiej współpracy jest jednak posiadanie przez obie te instytucje odpowiadających sobie kompetencji. Przeszkodą w wykonywaniu przez polskie służby specjalne umów o zwalczaniu przestępczości, jako efektywnego narzędzia prowadzenia współpracy międzynarodowej, jest fakt, że kraje, z którymi Polska zawiera tego typu umowy, nie zawsze zgłaszają po swojej

stronie służby specjalne jako organy właściwe do prowadzenia na ich podstawie współpracy. Wynika to z okoliczności, że przyznawanie służbom specjalnym kompetencji do wykrywania przestępstw i ścigania ich sprawców nie jest częstym rozwiązaniem. Jako przykłady umów o zwalczaniu przestępczości, w których jako organy właściwe do współpracy ze strony drugiego państwa wskazano służby specjalne bądź inne organy odpowiedzialne za bezpieczeństwo państwa, można wymienić umowy z: Estonią⁵⁶, Rumunią⁵⁷, Słowacją⁵⁸, Wietnamem⁵⁹ czy Brazylią⁶⁰ oraz większość zawartych przez Polskę umów z krajami z obszaru dawnego ZSRR.

Internetowa Baza Traktatowa Ministerstwa Spraw Zagranicznych wymienia 44 podpisane umowy o zwalczaniu przestępczości, w tym 43 które weszły w życie i 39 opublikowanych w „Dzienniku Ustaw”⁶¹.

Drugą grupą umów bilateralnych istotnych dla współpracy międzynarodowej służb specjalnych są umowy o wzajemnej ochronie informacji niejawnych. Celem tego rodzaju umów jest zapewnienie ochrony informacjom niejawnym wytworzonym w toku współpracy lub wymienianym między ich stronami. Umowy tego rodzaju, zawarte przez Rzeczpospolitą Polską z innymi państwami lub organizacjami międzynarodowymi, stanowią jednocześnie podstawę do wymiany informacji niejawnych. Świadczy o tym m.in. brzmienie art. 5 ust. 5 *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*⁶², który nakazuje oznaczanie informacji niejawnych przekazywanych do Polski przez inne państwa lub organizacje międzynarodowe polskim odpowiednikiem ich klauzuli tajności, czy też art. 34 ust. 4 i 11 tej ustawy, według których dostęp do informacji niejawnych może wynikać z zawartej przez Rzeczpospolitą Polską umowy międzynarodowej. Również w treści poprzednio obowiązującej *ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* znajdował się zapis (art. 24), z którego wynikało, iż wymiana informacji niejawnych z zagranicą następuje w celu wykonania umów międzynarodowych.

⁵⁶ Umowa. między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o współpracy w zakresie zwalczania przestępczości zorganizowanej oraz innej przestępczości, podpisana w Warszawie dnia 26 VI 2003 r. (Dz.U. 2004, nr 216, poz. 2195; 2008, nr 12, poz. 71).

⁵⁷ Umowa podpisana w Warszawie dnia 11 VII 2001 r. między Rządem RP a Rządem Rumunii o współpracy w zwalczaniu przestępczości zorganizowanej, terroryzmu i innych rodzajów przestępstw (Dz.U. 2004, nr 154, poz. 1625).

⁵⁸ Umowa między RP a Republiką Słowacką o współpracy w zwalczaniu przestępczości oraz o współdziałaniu na terenach przygranicznych, podpisana w Warszawie dnia 23 III 2004 r., podpisana w Warszawie dnia 23 III 2004 r. (Dz.U. 2007, nr 85, poz. 568; 2011, nr 249, poz. 1497).

⁵⁹ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o współpracy w zwalczaniu przestępczości zorganizowanej, podpisana w Warszawie dnia 28 VII 2003 r. (Dz.U. 2004, nr 216, poz. 2197).

⁶⁰ Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o współpracy w zakresie zwalczania przestępczości zorganizowanej oraz innych rodzajów przestępczości, podpisana w Brasiliu dnia 9 października 2006 r. (Dz.U. 2016 poz. 1323 oraz z 2017 r. poz. 207)

⁶¹ <https://traktaty.msz.gov.pl/umowa-1>, [dostęp: 28 V 2021].

⁶² Dz.U. 2010, nr 182, poz. 1228.

Umowy o ochronie informacji niejawnych są istotne dla współpracy międzynarodowej służb specjalnych nie tylko jako podstawa do wymiany informacji niejawnych, która jest niezbędna dla efektywnej współpracy międzynarodowej służb specjalnych, ale również jako podstawa prawna do bezpośredniej współpracy wskazanych w nich właściwych organów. Organy te to krajowe władze bezpieczeństwa.

Pojęcie krajowej władzy bezpieczeństwa zostało zdefiniowane w polskim prawie w art. 11 ust. 2 *ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*. Zgodnie z jego treścią: *Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych NATO, Unii Europejskiej lub innych organizacji międzynarodowych*. Stosownie natomiast do art. 11 ust. 1 wymienionej ustawy funkcję Krajowej Władzy Bezpieczeństwa pełni Szef Agencji Bezpieczeństwa Wewnętrznego. Na gruncie poprzedniej *ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*⁶³, która utraciła moc z dniem 2 stycznia 2011 r., funkcje krajowych władz bezpieczeństwa pełnili kolejno: Szef UOP (w latach 1999–2002), Szef WSI (w latach 1999–2006), Szef ABW (od 2002) oraz Szef SKW (w latach 2006–2011).

Krajowe władze bezpieczeństwa są standardowo wskazywane w treści dwustronnych umów o ochronie informacji niejawnych jako właściwe organy do wykonywania umowy albo po prostu „krajowe władze bezpieczeństwa” (co jest możliwe, jeśli system prawny drugiej strony umowy również operuje tym pojęciem). Przepisy umów o ochronie informacji niejawnych nakładają na wskazane w nich właściwe organy (krajowe władze bezpieczeństwa) wiele obowiązków, których wykonywanie wymaga od nich utrzymywania stałych kontaktów z ich zagranicznymi odpowiednikami. W niektórych przypadkach umowy o ochronie informacji niejawnych zawierają upoważnienia do zawierania przez właściwe organy porozumień wykonawczych⁶⁴.

Do chwili obecnej podpisano 40 tego rodzaju umów, przy czym 38 opublikowanych w „Dzienniku Ustaw” ma moc obowiązującą⁶⁵. Związanie Rzeczypospolitej Polskiej umowami tego rodzaju standardowo następuje w trybie tzw. małej ratyfikacji.

Umowy wielostronne, z uwagi na swój charakter, nie wskazują organów poszczególnych państw właściwych do ich wykonywania. Niektóre multilateralne konwencje międzynarodowe z zakresu zwalczania terroryzmu zawierają jednak przepisy zobowiązujące ich strony do wyznaczenia punktów

⁶³ Tekst pierwotny: Dz.U., nr 15, poz. 95, tekst jednolity: Dz.U. 2005, nr 196, poz. 1631; 2006, nr 104, poz. 708 i 711; nr 149, poz. 1078; nr 218, poz. 1592; nr 220, poz. 1600; 2007, nr 25, poz. 162; 2008, nr 171, poz. 1056; 2009, nr 178, poz. 1375.

⁶⁴ Przykładem jest Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Albanii o wzajemnej ochronie informacji niejawnych, podpisana w Tiranie dnia 21 IX 2004 r. (Dz.U. 2005, nr 247, poz. 2093).

⁶⁵ <https://traktaty.msz.gov.pl/umowa-1>, [dostęp: 31 V 2021]

kontaktowych, odpowiedzialnych za wysyłanie i przyjmowanie w imieniu państwa informacji na temat zjawisk, których zwalczaniu służy dana konwencja. Informacje na temat danych punktu kontaktowego są składane u depozytariusza określonej konwencji.

Przykładem takiej konwencji wielostronnej jest Międzynarodowa konwencja w sprawie zwalczania aktów terroryzmu jądrowego, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych 13 kwietnia 2005 r.⁶⁶ Art. 7 ust. 4 wymienionej konwencji nakłada na jej państwa-strony obowiązek poinformowania Sekretarza Generalnego Narodów Zjednoczonych o swoich organach i punktach kontaktowych odpowiedzialnych za wysyłanie i odbieranie informacji, o których wymianie mówią przepisy tej konwencji. W notyfikacji złożonej 6 maja 2010 r. Sekretarzowi Generalnemu Narodów Zjednoczonych Rzeczpospolita Polska poinformowała, że jej punktem kontaktowym na podstawie niniejszej konwencji będzie Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego⁶⁷.

Omówiwszy rolę umów międzynarodowych dla współpracy służb specjalnych z podmiotami zagranicznymi, można postawić pytanie: czy wymienienie szefa służby specjalnej w treści ratyfikowanej umowy międzynarodowej jako organu właściwego do współpracy, w ramach tej umowy, z wymienionymi w niej organami innych państw, może stanowić podstawę prawną do nawiązania takiej współpracy, alternatywną wobec zgody na współdziałanie, udzielonej przez Prezesa Rady Ministrów? Na pytanie to trudno jest udzielić jednoznacznej odpowiedzi.

Wykładnia językowa art. 8 ustawy o ABW oraz AW, art. 9 ustawy o SKW oraz SWW i art. 2a ustawy o CBA sugerowałyby odpowiedź negatywną. Również analiza porównawcza ustaw kompetencyjnych służb specjalnych z przepisami ustaw o Policji oraz o Służbie Ochrony Państwa prowadzi do podobnego wniosku. Regulacja kwestii dopuszczalności podejmowania współpracy międzynarodowej jest w obu tych grupach ustaw wyraźnie odmienna, bowiem ustawy wymienionych służb ochrony bezpieczeństwa i porządku publicznego dopuszczają wprost współdziałanie policji i SOP z podmiotami zagranicznymi na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów, zaś w przypadku służb specjalnych zgoda Prezesa Rady Ministrów pozostaje jedyną przesłanką umożliwiającą nawiązanie przez te służby współpracy międzynarodowej.

Trudno jednak wskazać cel, jakiemu to zróżnicowanie miałyby służyć. Prezes Rady Ministrów bierze przecież czynny udział w procedurach służących związaniu Rzeczypospolitej Polskiej umową międzynarodową wraz z innymi organami władzy wykonawczej. *Ustawa z dnia 14 kwietnia 2000 r. o umowach międzynarodowych*⁶⁸ przewiduje, iż rozpoczęcie negocjacji umowy międzynarodowej następuje po uzyskaniu przez właściwego ministra zgody Prezesa

⁶⁶ Dz.U. 2010, nr 112, poz. 740.

⁶⁷ *Treaty series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations 2010*, s. 351, <https://treaties.un.org/doc/Publication/UNTS/Volume%202673/v2673.pdf>, [dostęp: 29 V 2021].

⁶⁸ Tekst jednolity: Dz.U. 2020, nr 127; 2019, poz. 2020.

Rady Ministrów. Podpisanie umowy międzynarodowej, podobnie jak przekazanie jej Prezydentowi do ratyfikacji, następuje po wyrażeniu w formie uchwały zgody przez Radę Ministrów. Prezydent otrzymuje umowę międzynarodową do ratyfikacji bądź po wyrażeniu przez Sejm zgody w formie ustawy (procedura tzw. dużej ratyfikacji), bądź po złożeniu przez rząd Sejmowi zawiadomienia o zamiarze ratyfikacji (procedura tzw. małej ratyfikacji). W przypadku związania Rzeczypospolitej Polskiej umową międzynarodową w formie zatwierdzenia w procedurze jej przyjęcia uczestniczy jedynie Rada Ministrów.

Niezależnie jednak od przyjętego trybu związanie Rzeczypospolitej Polskiej umową międzynarodową angażuje nieporównanie więcej organów władzy wykonawczej, a w przypadku trybu ratyfikacji także ustawodawczej, niż przewidziany w ustawach kompetencyjnych służb specjalnych tryb uzyskiwania zgody Prezesa Rady Ministrów na współdziałanie, a sam Prezes Rady Ministrów bierze aktywny udział w tych procedurach. Można by zatem rozważyć, czy wobec niezbędnego udziału decyzyjnego samego Prezesa Rady Ministrów, jak i Rady Ministrów, w procedurach służących związaniu Rzeczypospolitej Polskiej umową międzynarodową, w momencie ratyfikacji umowy międzynarodowej przewidującej współpracę polskich służb specjalnych ze wskazanymi w jej treści służbami i organami innego państwa, istnieje już faktyczna zgoda Prezesa Rady Ministrów na taką współpracę. Teza ta jest dodatkowo wzmocniana przez przyjęcie w polskim porządku konstytucyjnym koncepcji bezpośredniego obowiązywania umów międzynarodowych w systemie prawnym oraz pierwszeństwo postanowień umowy międzynarodowej, ratyfikowanej za uprzednią zgodą wyrażoną w ustawie, przed postanowieniami ustawy⁶⁹.

Z uwagi na jednoznaczne brzmienie zapisów ustaw kompetencyjnych służb specjalnych autor niniejszego rozdziału doradzałby jednak występowanie z ostrożności do Prezesa Rady Ministrów (lub w obecnym stanie prawnym do Ministra-Koordynatora Służb Specjalnych, w przypadku służb cywilnych) o zgodę na współpracę również z organami i służbami, które wskazane są jako organy właściwe do współpracy w ratyfikowanej przez Rzeczpospolitą Polską umowie międzynarodowej, która wskazuje jako organ właściwy do współpracy po polskiej stronie szefa danej służby specjalnej.

Można by jednak rozważyć, w świetle przytoczonych wyżej argumentów, możliwość dodania do ustaw kompetencyjnych służb specjalnych zawartych przez Rzeczpospolitą Polską umów i porozumień międzynarodowych oraz odrębnych przepisów jako samoistnych przesłanek pozwalających na podjęcie przez określoną służbę współpracy z właściwymi służbami i organami innych państw oraz organizacjami międzynarodowymi. Zgoda Prezesa Rady Ministrów pozostałaby w ustawach kompetencyjnych jako alternatywna podstawa podjęcia przez określoną służbę współpracy międzynarodowej w sytuacji, gdy nie występuje samoistna podstawa prawna takiej współpracy zawarta w umowie

⁶⁹ Niektóre umowy o zwalczaniu przestępczości były przyjmowane w trybie tzw. dużej ratyfikacji.

międzynarodowej lub odrębnych przepisach. Niniejsza koncepcja mogłaby zostać rozpatrzona jako wniosek *de lege ferenda*.

Współpraca służb specjalnych z organizacjami międzynarodowymi

Jak wskazano wyżej, jedyną służbą specjalną, posiadającą w swojej ustawie kompetencyjnej przepis umożliwiający prowadzenie współpracy z organizacjami międzynarodowymi, jest Centralne Biuro Antykorupcyjne.

Tymczasem specyfika współpracy międzynarodowej prowadzonej w ramach kluczowych dla bezpieczeństwa i pozycji międzynarodowej Rzeczypospolitej Polskiej organizacji międzynarodowych, jakimi są NATO i Unia Europejska, wymusza niejednokrotnie angażowanie w tę współpracę służb wywiadu i kontrwywiadu, zarówno cywilnego, jak i wojskowego.

W przypadku NATO należy w pierwszej kolejności wskazać na niezwykle istotną dla funkcjonowania tej organizacji rolę systemu ochrony informacji niejawnych, w którym kluczową rolę odgrywają krajowe władze bezpieczeństwa Państw Członkowskich. Zgodnie z przyjętym przez Radę Północnoatlantycką dokumentem: „Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego”⁷⁰ każde Państwo Członkowskie NATO wyznacza krajową władzę bezpieczeństwa odpowiedzialną za bezpieczeństwo informacji niejawnych paktu. Krajowa władza bezpieczeństwa służy za główny punkt kontaktowy Biura Bezpieczeństwa NATO (struktury sojuszu odpowiedzialnej za ochronę informacji niejawnych). Reprezentanci krajowych władz bezpieczeństwa wszystkich Państw Członkowskich NATO wchodzi w skład Komitetu Bezpieczeństwa — organu powoływanego przez Radę Północnoatlantycką, odpowiedzialnego za bieżącą aktualizację polityki bezpieczeństwa NATO oraz zatwierdzanie różnego rodzaju dokumentów i instrukcji dotyczących ochrony informacji niejawnych.

Oprócz tego funkcjonują w ramach NATO struktury angażujące do współpracy zarówno cywilne, jak i wojskowe służby wywiadu i kontrwywiadu. W dniu 5 stycznia 2016 r. pojawiła się w mediach informacja o objęciu przez Agencję Wywiadu przewodnictwa w Cywilnym Komitecie Wywiadowczym NATO — powstałej w 2010 r. jednej z trzech głównych struktur wywiadowczych NATO, obok Wojskowego Komitetu Wywiadowczego (*Military Intelligence Committee* — MIC) i Rady Zarządzającej ds. Wywiadu (*Intelligence Steering Board* — ISB)⁷¹. Również Agencja Bezpieczeństwa Wewnętrznego informowała na swojej

⁷⁰ *Document C-M (2002)49 — REV1 Security Within the North Atlantic Treaty Organisation (NATO)*, niepubl.

⁷¹ Zespół W polityce, *Agencja Wywiadu przewodniczy w 2016 roku Cywilnemu Komitetowi Wywiadowczemu NATO*, 5 stycznia 2016 r., <https://wpolityce.pl/polityka/277139-agencja-wywiadu-w-2016-roku-przewodniczy-cywilnemu-komitetowi-wywiadowczemu-nato>, [dostęp: 30 V 2021].

stronie internetowej o swoim aktywnym uczestnictwie w Cywilnym Komitecie Wywiadowczym⁷².

W 2017 r. w wyniku reformy strukturalnej sojusz powołał do życia Połączony Pion Wywiadu i Bezpieczeństwa (JISD) w Kwaterze Głównej NATO, w którym po raz pierwszy w historii w Kwaterze Głównej NATO utworzono połączony pion cywilno-wojskowy⁷³.

Jednym z przejawów współpracy służb specjalnych w ramach NATO było również powołanie przez Polskę i Słowację, jako państwa ramowe, w 2015 r. Centrum Eksperckiego Kontrwywiadu NATO w Krakowie⁷⁴.

Odnosząc się do możliwości współpracy służb specjalnych z organami i instytucjami Unii Europejskiej, art. 4 ust. 2 *Traktatu o Unii Europejskiej* stanowi, iż Unia szanuje funkcje państwa w zakresie zapewnienia bezpieczeństwa publicznego, a w szczególności bezpieczeństwo narodowe pozostaje w sferze wyłącznej odpowiedzialności Państw Członkowskich, zdaje się sugerować, że sfera działania służb specjalnych znajduje się w całości poza zakresem kompetencji Unii Europejskiej.

W rzeczywistości sytuacja jest bardziej skomplikowana. Zgodnie z art. 4 ust. 2 TFUE jedną z dziedzin, do których stosują się kompetencje dzielone między Unią a państwami członkowskimi, jest Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości. Przestrzeń Wolności Bezpieczeństwa i Sprawiedliwości jest szczegółowo uregulowana w tytule V TFUE. Obejmuje ona współpracę w zakresie polityk dotyczących kontroli granicznej, azyłu i imigracji, współpracę sądową w sprawach cywilnych, współpracę wymiarów sprawiedliwości w sprawach karnych oraz współpracę policyjną. Zgodnie z art. 73 TFUE, znajdującym się w przepisach ogólnych Działu V, *Państwa Członkowskie mogą organizować między sobą i na swoją odpowiedzialność uznane przez nie za stosowne formy współpracy i koordynacji między właściwymi służbami ich administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego*. Przepisem określającym zakres wpływu Unii Europejskiej na politykę karną państw członkowskich jest art. 83 TFUE, który pozwala organom Unii na ustanowienie norm minimalnych odnoszących się do określania przestępstw oraz kar w dziedzinach

⁷² <https://www.abw.gov.pl/pl/wolnytekst/318,NATO.html>, [dostęp: 30 V 2021].

⁷³ A. Freytag von Loringhoven, *Nowa era działalności wywiadowczej NATO*, w: *Przegląd NATO*, 2019 r. <https://www.nato.int/docu/review/pl/articles/2019/10/29/nowa-era-dzialalnosci-wywiadowczej-nato/index.html>, [dostęp: 30 V 2021].

⁷⁴ Kwestie dotyczące działania wymienionego Centrum zostały uregulowane w umowie międzynarodowej: Memorandum o Porozumieniu między Ministrem Obrony Narodowej Rzeczypospolitej Polskiej Ministrem Obrony Republiki Słowackiej, Ministerstwem Obrony Republiki Chorwacji, Ministerstwem Obrony Republiki Czeskiej, Federalnym Ministerstwem Obrony Republiki Federalnej Niemiec, Ministerstwem Obrony Węgier, Ministerstwem Obrony Republiki Włoskiej, Ministerstwem Obrony Republiki Litewskiej, Ministerstwem Obrony Narodowej Rumunii, Ministerstwem Obrony Republiki Słowenii dotyczącym utworzenia, administracji i działania Centrum Eksperckiego Kontrwywiadu NATO, podpisanym w Norfolk dnia 29 IX 2015 r. (M.P. 2016, poz. 590).

szczególnie poważnej przestępczości o wymiarze transgranicznym, obejmujących: terroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcję, fałszowanie środków płatniczych, przestępczość komputerową i przestępczość zorganizowaną. Należy zauważyć, że rozpoznawanie, zapobieganie, wykrywanie oraz ściganie sprawców znacznej części z wymienionych przestępstw znajduje się we właściwości Agencji Bezpieczeństwa Wewnętrznego.

Zgodnie z art. 87 ust. 1 TFUE Unia rozwija współpracę policyjną obejmującą wszystkie właściwe organy Państw Członkowskich, w tym służby policji, służby celne oraz inne organy ścigania wyspecjalizowane w zapobieganiu przestępstwom lub ich wykrywaniu i ściganiu. Pojęcie innych organów ścigania wyspecjalizowanych w zapobieganiu przestępstwom lub ich wykrywaniu i ściganiu może obejmować również służby specjalne posiadające tego rodzaju uprawnienia. Wobec powyższego nie ma przeszkód, aby Agencja Bezpieczeństwa Wewnętrznego oraz Centralne Biuro Antykorupcyjne partycypowały, w zakresie swojej właściwości, w pewnych elementach współpracy policyjnej w ramach Unii Europejskiej.

Zgodnie natomiast z ust. 2 i 3 art. 87 TFUE Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, mogą ustanawiać środki dotyczące: gromadzenia, przechowywania, przetwarzania, analizowania i wymiany istotnych informacji, wspierania szkolenia pracowników, jak również współpracy w zakresie wymiany pracowników, wyposażenia i badań w dziedzinie kryminalistyki oraz wspólnych technik śledczych dotyczących wykrywania poważnych form przestępczości zorganizowanej. Rada, stanowiąc zgodnie ze specjalną procedurą ustawodawczą, może natomiast ustanowić środki dotyczące współpracy operacyjnej między organami, o których mowa w niniejszym rozdziale. Rada stanowi jednomyślnie po konsultacji z Parlamentem Europejskim.

Centralną instytucją europejską w ramach współpracy policyjnej jest Euro-pol, o którym mowa w art. 88 TFUE. Zgodnie z treścią jego ust. 1: *Zadaniem Europolu jest wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania Państw Członkowskich, jak również ich wzajemnej współpracy w zapobieganiu i zwalczaniu poważnej przestępczości dotyczącej dwóch lub więcej Państw Członkowskich, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką Unii*. Struktura, funkcjonowanie oraz zakres działań i zadań Europolu są regulowane *Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującym i uchylającym decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW*⁷⁵. Zgodnie z art. 7 ust. 2 wymienionego rozporządzenia *Każde państwo członkowskie ustanawia lub wyznacza jednostkę krajową, która jest organem łącznikowym między Europolem a właściwymi organami tego państwa członkowskiego*. Na terytorium Rzeczypospolitej Polskiej punktem kontaktowym w zakresie wymiany informacji z Europolem

⁷⁵ (Dz.Urz. UE, Seria L Nr 135, s. 53 oraz z 2018 r. Nr 235, s. 1).

jest Biuro Międzynarodowej Współpracy Komendy Głównej Policji. Komórka ta koordynuje i nadzoruje wszystkie działania w ramach międzynarodowej współpracy operacyjnej i pozaoperacyjnej⁷⁶. W celu zapewnienia ABW możliwości współpracy z członkami Europolu Szef ABW zawarł 26 lipca 2010 r. z Komendantem Głównym Policji porozumienie⁷⁷, na podstawie którego Komenda Główna Policji pośredniczy we współpracy prowadzonej przez ABW z partnerami zagranicznymi będącymi członkami Europolu.

Jako akt prawa europejskiego z zakresu współpracy policyjnej, dotyczący właściwości kompetencyjnej ABW i mogący stanowić dla niej samoistną podstawę do współpracy z właściwymi organami i służbami innych państw, wskazać należy np. *Decyzję Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, w szczególności w zakresie terroryzmu i przestępczości zorganizowanej*⁷⁸. Celem niniejszej decyzji jest intensyfikacja współpracy transgranicznej między organami policyjnymi i sądowymi państw UE, aby skuteczniej zwalczać terroryzm i przestępczość transgraniczną. Przepisy tego aktu prawnego dotyczą w szczególności zautomatyzowanej wymiany informacji w związku z istotnymi wydarzeniami i w celu zwalczania terroryzmu oraz innych form transgranicznej współpracy policyjnej. Nakładają na Państwa Członkowskie obowiązek wzajemnego dostarczania sobie danych nieosobowych i danych osobowych do celów prewencji kryminalnej oraz ochrony porządku i bezpieczeństwa publicznego podczas istotnych wydarzeń o wymiarze transgranicznym. Zgodnie z art. 16 ust. 1 wymienionej decyzji do celów zapobiegania przestępstwom terrorystycznym Państwa Członkowskie mogą dostarczać, zgodnie z prawem krajowym, w indywidualnych przypadkach, nawet bez otrzymania stosownego wniosku, krajowym punktom kontaktowym pozostałych Państw Członkowskich dane osobowe i informacje, o ile jest to konieczne z uwagi na szczególne okoliczności, dające podstawy do przypuszczenia, że osoby, których dane dotyczą, dopuszczają się przestępstw o charakterze terrorystycznym. Stosownie do art. 16 ust. 3 wymienionej decyzji każde Państwo Członkowskie ma obowiązek wyznaczyć krajowy punkt kontaktowy, który odpowiada za wymianę danych z krajowymi punktami kontaktowymi innych Państw Członkowskich. Uprawnienia krajowych punktów kontaktowych określa właściwe prawo krajowe. Zgodnie z art. 5 ust. 3 ustawy o ABW oraz AW zadania punktu kontaktowego, o którym mowa w art. 16 ust. 3 decyzji Rady 2008/615/WSiSW, wykonuje Szef Agencji Bezpieczeństwa Wewnętrznego.

Należy wspomnieć również o obowiązującej wciąż *decyzji ramowej Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany*

⁷⁶ <https://info.policja.pl/inf/wspolpraca-miedzynarod/72445,Wspolpraca-miedzynarodowa.html>, [dostęp: 30 V 2021].

⁷⁷ Porozumienie w sprawie zapewnienia przez Komendę Główną Policji udziału Agencji Bezpieczeństwa Wewnętrznego we współpracy prowadzonej w ramach Międzynarodowej Organizacji Policji Kryminalnych Interpol i Europejskiego Urzędu Policji — Europol, niepubl.

⁷⁸ Dz.Urz. UE Seria L Nr 210 z 6 VIII 2008 r., s. 1.

*informacji i danych wywiadowczych między organami ścigania Państw Członkowskich Unii Europejskiej*⁷⁹, która określa zasady, według których organy ścigania Państw Członkowskich (...) mogą dokonywać skutecznej i sprawnej wymiany istniejących informacji i danych wywiadowczych w celu prowadzenia dochodzeń karnych lub operacji wywiadowczych w sprawie przestępstw (art. 1 ust. 1). „Informacje lub dane wywiadowcze” są definiowane w treści decyzji jako *każdy rodzaj informacji lub danych w posiadaniu organów ścigania i każdy rodzaj informacji lub danych w posiadaniu władz publicznych lub podmiotów prywatnych, które są dostępne organom ścigania bez stosowania środków przymusu* (...). Niniejsza decyzja ramowa została implementowana do polskiego porządku prawnego przepisami ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi⁸⁰, której art. 1 ust. 2 wymienia wśród podmiotów uprawnionych do wymiany informacji z organami państw członkowskich Unii Europejskiej, organami ścigania państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi, Agencję Bezpieczeństwa Wewnętrznego oraz Centralne Biuro Antykorupcyjne.

Wśród organów i instytucji Unii Europejskiej znajdują się gremia, których zakres właściwości dotyka zagadnień pozostających w zakresie właściwości służb specjalnych i w których pracach biorą udział przedstawiciele służb specjalnych. Wymienić można chociażby wśród organów Rady:

- Grupę Roboczą ds. Terroryzmu — organ przygotowawczy Rady, który przygotowuje i całościowo ukierunkowuje prace Rady w dziedzinie zwalczania terroryzmu; do jego zadań należy wymiana informacji i ocen na temat zagrożeń terrorystycznych, przeciwdziałanie radykalizacji postaw i werbunkowi potencjalnych terrorystów oraz wyszukiwanie najlepszych krajowych rozwiązań w walce z terroryzmem;⁸¹,
- Komitet Bezpieczeństwa Rady — powstały na mocy przepisów bezpieczeństwa Rady o ochronie informacji niejawnych UE, analizuje wszelkie kwestie ochrony informacji niejawnych UE i w razie potrzeby udziela Radzie zaleceń. Omawia m.in. przepisy i strategie UE w tej dziedzinie, umowy o wymianie informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi, a także zasady wymiany informacji niejawnych między instytucjami, organami i agencjami UE; składa się z przedstawicieli krajowych organów bezpieczeństwa lub innych stosownych organów państw członkowskich⁸².

Wymienić należy również strukturę wchodzącą w skład Europejskiej Służby Działań Zewnętrznych, jaką jest Centrum Sytuacyjno-Wywiadowcze INTCEN

⁷⁹ Dz.Urz. UE Seria L Nr 386, s. 89 oraz z 2007 r., Nr 75, s. 26.

⁸⁰ Dz.U. 2020, poz. 158.

⁸¹ <https://www.consilium.europa.eu/pl/council-eu/preparatory-bodies/working-party-terrorism/>, [dostęp: 30 V 2021].

⁸² <https://www.consilium.europa.eu/pl/council-eu/preparatory-bodies/security-committee/>, [dostęp: 30 V 2021].

(*EU Intelligence and Situation Centre*), wytwarzające analizy wywiadowcze na potrzeby Europejskiej Służby Działań Zewnętrznych, Komisji i Państw Członkowskich, głównie na podstawie informacji otrzymanych od służb wywiadowczych państw członkowskich⁸³.

Opisana wyżej współpraca służb specjalnych z instytucjami organizacji międzynarodowych odbywa się w interesie państwa polskiego i jego bezpieczeństwa. Przy obecnym poziomie integracji naszego państwa ze strukturami międzynarodowymi świata zachodniego oraz pogłębianiu integracji międzynarodowej w ramach tych struktur, również w obszarze bezpieczeństwa, jest ona wręcz nieunikniona. Niestety, ustawodawstwo krajowe zdaje się nie nadążać za tymi trendami.

W świetle powyższego zapewnienie zgodności stanu faktycznego ze stanem prawnym wymaga zapisania w ustawach kompetencyjnych wszystkich służb specjalnych możliwości współpracy z organizacjami międzynarodowymi.

Podsumowanie — wnioski *de lege ferenda*

Przedstawione w niniejszym rozdziale omówienie podstaw i ram prawnych współpracy międzynarodowej służb specjalnych oraz niektórych praktycznych problemów dotyczących tej współpracy prowadzi do wniosków o zasadności podjęcia dyskusji na temat zasadności zmian w regulujących te kwestie przepisach ustaw kompetencyjnych tych służb.

W szczególności zasadnym postulatem *de lege ferenda* wydaje się ustawowe uregulowanie możliwości współdziałania Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego z organizacjami międzynarodowymi. Przypisanie takiej kompetencji wyłącznie Centralnemu Biuro Antykorupcyjnemu, a pozbawienie jej pozostałych służb specjalnych, nie znajduje merytorycznego uzasadnienia. Co więcej, jak wykazano wyżej, nie odpowiada potrzebom praktyki, bowiem faktyczna współpraca pozostałych służb specjalnych z agendami NATO czy Unii Europejskiej ma w rzeczywistości miejsce i jest niezbędna, jeśli Rzeczpospolita Polska ma efektywnie uczestniczyć w pracach tych organizacji w zakresie spraw dotyczących szeroko rozumianego bezpieczeństwa. Dlatego postulat ten nie powinien budzić wątpliwości.

Innym postulatem, który można by poddać dyskusji, jest wprowadzenie do ustaw kompetencyjnych służb specjalnych przepisów pozwalających na podejmowanie przez te służby współpracy międzynarodowej na podstawie zawartych przez Rzeczpospolitą Polską umów i porozumień międzynarodowych oraz odrębnych przepisów. Jak wykazano wyżej, rozwiązanie takie nie doprowadziłoby do ograniczenia wpływu Prezesa Rady Ministrów na zakres prowadzonej

⁸³ *Joint answer given by High Representative/Vice-President Ashton on behalf of the Commission Written questions: E-006018/12, E-006020/12, https://www.europarl.europa.eu/doceo/document/E-7-2012-006018-ASW_CS.html?redirect, [dostęp: 30 V 2021].*

przez służby specjalne współpracy międzynarodowej, bowiem szef rządu oraz Rada Ministrów w każdym przypadku wyrażają zgodę na związanie Rzeczypospolitej Polskiej umową międzynarodową w określonym kształcie. W sytuacji, gdy stanowiąca źródło prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej, a zarazem będąca zaciągniętym przez Rzeczypospolitą Polską zobowiązaniem w porządku prawnomiędzynarodowym, umowa przewiduje możliwość współpracy polskiej służby specjalnej z organem lub służbą innego państwa, wymaganie dodatkowej zgody Prezesa Rady Ministrów na nawiązanie takiej współpracy wydaje się nadmiarowe.

Umożliwienie służbom współpracy międzynarodowej na podstawie odrębnych przepisów objęłoby np. działania Szefa Agencji Bezpieczeństwa Wewnętrznego jako krajowej władzy bezpieczeństwa w stosunkach międzynarodowych, której kompetencje określają krajowe i międzynarodowe przepisy o ochronie informacji niejawnych.

Zgoda Prezesa Rady Ministrów pozostałaby w takiej sytuacji warunkiem podejmowania przez służby specjalne współpracy z właściwymi służbami i organami innych państw w sytuacji, gdy nie ma podstawy dla takiej współpracy w zawartej przez Rzeczypospolitą Polską umowie międzynarodowej lub odrębnych przepisach, a interes bezpieczeństwa Rzeczypospolitej Polskiej wymaga nawiązania takiej współpracy. Sytuacje takie byłyby nadal częste, bowiem jak wykazano wyżej, wskazywanie przez inne państwa służb specjalnych jako organów właściwych do współpracy na podstawie np. umów o współpracy w zakresie zwalczania przestępczości zdarza się relatywnie rzadko. W konsekwencji w wyniku przyjęcia postulowanego rozwiązania dotychczasowy tryb podejmowania przez służby współdziałania ze służbami innych państw byłby stosowany do współpracy służb specjalnych *sensu stricto*, obejmującej głównie niejawne działania wywiadowcze i kontrwywiadowcze. Z kolei współpraca *de facto* policyjna, wynikająca z posiadania przez Agencję Bezpieczeństwa Wewnętrznego i Centralne Biuro Antykorupcyjne uprawnień dochodzeniowo-śledczych, jak również współpraca administracyjna, wynikająca z przypisania Szefowi ABW roli krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych, odbywałyby się na zasadach podobnych, jak w przypadku służb ochrony bezpieczeństwa i porządku publicznego.

Model obowiązujących w Polsce przepisów dotyczących podejmowania przez służby specjalne współpracy międzynarodowej powstał prawie 20 lat temu. Być może nadchodzi właściwy moment, aby podjąć dyskusję nad zasadnością jego zmiany w celu dostosowania do wyzwań współczesności oraz uwzględnienia dwóch dekad doświadczeń.

Magdalena Gołaszewska

Rozdział 8.

Problematyka ochrony środków, form i metod realizacji zadań w praktyce funkcjonowania służb specjalnych

Wstęp

W literaturze przedmiotu możemy odnaleźć dwie klasyczne sfery tajnych działań prowadzonych przez służby — pozyskiwanie informacji i ochrona własnych zasobów informacyjnych¹. Tak więc, działalność służb, szczególnie w aspekcie wykonywania przez nie czynności operacyjno-rozpoznawczych, które co do zasady mają niejawnny charakter, a także uzyskiwanych w ich toku informacji, stanowiących sedno działań tych służb, winna podlegać szczególnej ochronie, określanej także jako tzw. szczelność informacyjna. Jednakże poziom wspomnianej ochrony zależny jest od zakresu i charakteru działań podejmowanych przez poszczególne formacje — nieco inaczej układa się wspomniane zagadnienie w odniesieniu do tzw. służb policyjnych (np. policja, Straż Graniczna), a inaczej wobec służb specjalnych wymienionych w art. 11 ustawy o ABW oraz AW², tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego. W odróżnieniu od służb policyjnych, które co do zasady zajmują się wykrywaniem przestępstw i ściganiem ich sprawców (działalność wykrywcza), zasadniczym elementem wspólnym działalności służb specjalnych jest prowadzenie działań o charakterze prewencyjnym i informacyjnym³. Dlatego też można podsumować, iż przeważająca rola czynności informacyjnych stanowi charakterystyczny wyróżnik służb specjalnych od służb policyjnych. Należy także dodać, iż co do zasady służby policyjne zajmują się

¹ Zob. S. Zalewski, *Służby specjalne w państwie demokratycznym*, Akademia Obrony Narodowej, Warszawa 2005, s. 17.

² Dz.U. 2020, poz. 27 z późn. zm.

³ Zob. M. Bożek i in., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Lex a Wolters Kluwer business, Warszawa 2014, s. 29–32.

bezpieczeństwem obywateli, zaś służby specjalne cechuje zasadniczo dbanie o bezpieczeństwo państwa i jego instytucji. A zatem, im wyższy stopień skomplikowania zadań i celów działania danej służby, tym wyższy winien być poziom stosowanych w niej zabezpieczeń w ramach tzw. systemu ochronnego.

Należy także wspomnieć, iż zgodnie z definicją słownikową pojęcie „ochrona” oznacza zabezpieczenie przed czymś niekorzystnym, złym lub niebezpiecznym⁴. W kontekście przytoczonego wyżej znaczenia językowego warto jednak zastanowić się, na czym dokładnie polega owa ochrona w kontekście realizacji zadań przez służby specjalne i jakie konkretne wartości podlegają zabezpieczeniu w tej kwestii? Wydaje się, że na tak postawione pytanie można nawet pokusić się o odpowiedź, że wszystko, co dotyczy sfery działań służb specjalnych, powinno podlegać takiej ochronie — począwszy od życia i zdrowia funkcjonariuszy, a także ich danych osobowych, przez informacje uzyskiwane w toku czynności, szczegóły co do prowadzenia czynności, a skończywszy na fizycznym zabezpieczeniu budynków, w których wykonywane są zadania służbowe. Jednakże odpowiedź na to pytanie nie jest tak oczywista, albowiem regulacja w tym zakresie w ustawach pragmatycznych służb specjalnych jest bardzo ogólna, nie zawiera definicji legalnych ani szczegółowych rozwiązań w tym zakresie. Punkt wyjścia do dalszych rozważań stanowić będzie art. 35 ust. 1 ustawy o ABW oraz AW⁵, zgodnie z którym Agencja Bezpieczeństwa Wewnętrznego w związku z wykonywaniem swoich zadań zapewnia ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy Agencji. Z przywołanego wyżej przepisu można wyprowadzić trzy podstawowe aspekty, w których ustawodawca nałożył na Agencję Bezpieczeństwa Wewnętrznego obowiązek zapewnienia ochrony: bezpieczeństwo personalne (bezpieczeństwo funkcjonariuszy i pracowników oraz ich danych osobowych), bezpieczeństwo fizyczne (bezpieczeństwo obiektów, obszarów i urządzeń) oraz bezpieczeństwo informacyjne (bezpieczeństwo wykonywanych czynności, w tym szczegółowych form i zasad prowadzenia czynności operacyjno-rozpoznawczych oraz bezpieczeństwo zgromadzonych informacji). Niniejszy rozdział ma na celu przybliżenie ochrony środków, form i metod realizacji zadań w praktyce funkcjonowania służb specjalnych we wskazanych wyżej aspektach.

W niniejszej pracy oprócz metody dogmatycznej, polegającej na analizie przepisów prawa i tekstów z literatury prawniczej, wykorzystano także analizę porównawczą rozwiązań przyjętych w polskich służbach specjalnych z uwzględnieniem historycznego ujęcia omawianych instytucji, a także przytoczono wnioski wypływające z analizy orzecznictwa sądowo-administracyjnego dotyczącego przedmiotowej kwestii.

⁴ *Słownik języka polskiego*, <http://sjp.pwn.pl>, [dostęp: 17 VI 2021].

⁵ Dz.U. 2020, poz. 27 z późn. zm.

Ramy prawne systemu ochronnego w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i ustawach innych służb specjalnych — aspekt prawno-porównawczy i historyczny

Podstawową regulację, w której ustawodawca nałożył na Agencję Bezpieczeństwa Wewnętrznego obowiązek zapewnienia ochrony kwestii wrażliwych dla jej funkcjonowania, stanowi wskazany już wyżej art. 35 ust. 1 ustawy o ABW oraz AW. Jednakże na podkreślenie zasługuje konstatacja, iż ustawodawca we wskazanym przepisie wprowadził wprawdzie wspomniany wyżej obowiązek ochronny, jednakże uczynił to w drodze bardzo ogólnego przepisu, nie dookreślając jednak narzędzi służących do jego realizacji. Z przytoczonego wyżej brzmienia art. 35 ust. 1 ustawy o ABW oraz AW można jednak wywnioskować, iż oprócz obiektów i danych funkcjonariuszy ochroną objęte są następujące aspekty — środki, formy i metody wykonywania działań. Z uwagi na powyższe zróżnicowanie określeń „metoda”, „środek”, „forma” w kontekście czynności wykonywanych przez służbę należy wskazać, iż pojęcie „metoda” słownikowo oznacza świadomie stosowany sposób postępowania, mający prowadzić do osiągnięcia zamierzonego celu; „środek” oznacza coś, co umożliwi lub zrobienie czegoś, zaś „forma” może być rozumiana jako postać, wygląd czegoś bądź układ skoordynowanych elementów, czy też sposób postępowania, zachowania się. Należy także dodać, iż w literaturze kryminalistycznej „metoda” określa się celowo wykorzystywaną kombinację środków i zachowań, które przy zastosowaniu posiadanej wiedzy i zdobytego doświadczenia ułatwiają realizację założonych celów, a „środek” stanowi zwarty element, specjalnie stosowany przy realizacji konkretnych zamierzeń, przy czym zazwyczaj są to środki techniczne, ułatwiające pozyskiwanie i zapisywanie informacji (np. urządzenia bezpośredniego podsłuchu, kamery). Wskazane wyżej rozróżnienie terminologiczne, sformułowane w treści art. 35 ust. 1 ustawy o ABW oraz AW, wydaje się zatem być świadomym zabiegiem ustawodawcy, zmierzającym do poszerzenia zakresu obowiązywania tego przepisu przez wprowadzenie kilku kategorii chronionych wartości, nieco doprecyzowujących tak ogólne brzmienie tej normy.

Należy dodać, iż w kolejnych jednostkach redakcyjnych omawianego przepisu uregulowano uprawnienie do posługiwania się dokumentami uniemożliwiającymi ustalenie danych identyfikujących funkcjonariusza oraz środków, jakimi posługuje się on przy wykonywaniu zadań służbowych (tzw. dokumentami legalizacyjnymi) w przypadku wykonywania czynności operacyjno-rozpoznawczych. Wskazano również, iż funkcjonariusze przy wykonywaniu czynności operacyjno-rozpoznawczych mogą posługiwać się środkami identyfikacji elektronicznej, zawierającymi dane inne niż identyfikujące funkcjonariusza (tzw. legalizacyjne środki identyfikacji elektronicznej). Analogiczne uprawnienie co do posługiwania się dokumentami legalizacyjnymi i legalizacyjnymi środkami identyfikacji elektronicznej wprowadzono także wobec osób udzielających pomocy Agencji Bezpieczeństwa Wewnętrznego przy wykonywaniu czynności operacyjno-rozpoznawczych.

Ponadto w ust. 6 tego przepisu wskazano, iż nie popełnia przestępstwa osoba, która: poleca sporządzenie lub kieruje sporządzeniem dokumentów legalizacyjnych; sporządza takie dokumenty; udziela pomocy przy sporządzeniu tych dokumentów; wydaje legalizacyjne środki identyfikacji elektronicznej, a także funkcjonariusz lub osoba udzielająca pomocy Agencji, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami legalizacyjnymi oraz legalizacyjnymi środkami identyfikacji elektronicznej. Wprowadzone przez ustawodawcę kontraty, czyli okoliczności wyłączające bezprawność czynu, pozwalają w imieniu prawa na wykonywanie wymienionych czynności, składających się na instytucję legalizacji, które bez zastosowania niniejszego przepisu powodowałyby jednak odpowiedzialność karną. Można zatem podsumować, iż zarówno sama instytucja legalizacji, jak i wzmocnienie jej kontratypami, stanowią element systemu ochronnego, pozwalający na ukrywanie prawdziwych tożsamości funkcjonariuszy i osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych, co znacznie podnosi poziom zabezpieczenia danych funkcjonariuszy oraz wpływa pozytywnie na bezpieczeństwo wykonywanych przez nich czynności.

Należy także wskazać na art. 43 ust. 1 ustawy o ABW oraz AW, obligujący do zapewnienia ochrony wykorzystywanych urządzeń oraz obszarów i obiektów, a także przebywających w nich osób, przez wewnętrzną służbę ochrony. Na podstawie ust. 2 funkcjonariusze wykonujący zadania w zakresie ochrony, w granicach chronionych obszarów i obiektów, mają prawo do: ustalania uprawnień osób do przebywania na obszarach lub w obiektach chronionych, legitymowania osób w celu ustalenia ich tożsamości, wydawania poleceń dotyczących określonego zachowania się w granicach chronionych obszarów i obiektów, w tym ich opuszczenia, ujęcia osób stwarzających bezpośrednie zagrożenie życia lub zdrowia ludzkiego, a także dla chronionego mienia, w celu niezwłocznego oddania tych osób policji lub innym właściwym organom, dokonywania sprawdzenia prewencyjnego, a także sprawdzania bagaży, środków transportu i ładunków, usunięcia pojazdów z miejsca postoju, zniszczenia, unieruchomienia lub przejścia kontroli lotu bezzałogowego statku powietrznego, w tym modelu latającego — jeżeli jest to niezbędne do zapewnienia bezpieczeństwa chronionych urządzeń, a także obszarów, obiektów oraz przebywających w nich osób.

Mając na uwadze przytoczone wyżej przepisy, można wskazać, iż na gruncie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu mamy do czynienia z dwoma podstawowymi przepisami „ochronnymi” — jednym, ogólnym, odnoszącym się do nakazu zabezpieczenia szczegółów dotyczących wykonywanych zadań, zgromadzonych informacji, obiektów a także danych identyfikujących funkcjonariuszy oraz drugim, doprecyzowującym aspekt zapewnienia fizycznej ochrony budynków i osób. Ogólne ramy systemu ochronnego bez wątplenia wskazują na podstawowy jego aspekt, tj. posługiwanie się dokumentami legalizacyjnymi i legalizacyjnymi środkami identyfikacji elektronicznej. Wszystkie służby specjalne dysponują takim uprawnieniem, które dotyczy nie tylko funkcjonariuszy, ale także i osób udzielających im pomocy

w wykonywaniu zadań. Dopełnienie tych przepisów stanowi art. 39 ust. 1 i 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w którym zawarto uprawnienie Szefa Agencji Bezpieczeństwa Wewnętrznego do wydawania zezwolenia aktualnym funkcjonariuszom i pracownikom oraz byłym funkcjonariuszom Agencji Bezpieczeństwa Wewnętrznego oraz Urzędu Ochrony Państwa i byłym pracownikom tych instytucji na udzielenie informacji niejawniej podmiotom zewnętrznym. Należy także dodać, iż w ust. 3 tego przepisu wskazano na przypadki, w których nie jest dopuszczalne wydanie zgody na udzielenie informacji niejawniej podmiotom zewnętrznym — wprowadzono bowiem bezwzględny zakaz udostępniania informacji o: osobie, jeżeli zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych, szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych; stosowanych w związku z ich prowadzeniem środków i metodach; osobie udzielającej pomocy Agencji Bezpieczeństwa Wewnętrznego oraz Urzędowi Ochrony Państwa. W kolejnych jednostkach redakcyjnych tego przepisu wskazano jednak przypadki wyjątkowego ujawnienia najbardziej chronionych informacji, do czego może dojść jedynie na żądanie prokuratora lub sądu, zgłoszone w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych bądź też na żądanie prokuratora lub sądu, uzasadnione podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Tak więc można stwierdzić, iż analizowany wyżej przepis wpisuje się także w konstrukcję systemu ochronnego i umożliwia zachowanie szczelności informacyjnej, wprowadza bowiem odrębne, autonomiczne uprawnienie Szefa Agencji Bezpieczeństwa Wewnętrznego do podejmowania decyzji o zakresie udostępnianych informacji niejawnych, które nie jest obwarowane sformalizowaną procedurą i zasadniczo nie przewiduje kwestionowania odmowy udzielenia zezwolenia, a ponadto wprowadza bezwzględny zakaz udostępniania pewnych informacji poza strukturę służby specjalnej.

Należy także wspomnieć, iż w treści art. 19 ust. 3 ustawy o ABW oraz AW ustawodawca zawarł upoważnienie ustawowe (tzw. delegację ustawową) do uregulowania przez szefa służby, w drodze zarządzenia, sposobów, metod i form wykonywania zadań w podległej mu instytucji, w zakresie nieobjętym innymi przepisami. Wprawdzie regulacja wydana na takiej podstawie stanowić będzie akt prawny o charakterze wewnętrznym, ale z uwagi na fakt wydania go na podstawie upoważnienia ustawowego można twierdzić, iż taki akt prawny będzie miał jednak pewnego rodzaju umocowanie ustawowe. Zarządzenia Szefa Agencji Bezpieczeństwa Wewnętrznego wydawane na tej podstawie prawnej dopełniają regulacje powszechnie obowiązujące w zakresie szczegółów funkcjonowania służby, w tym także w aspektach podlegających powinności zachowania wysokiego poziomu ochrony.

Wskazany wyżej model tzw. systemu ochronnego znajduje odzwierciedlenie również w regulacjach prawych dotyczących pozostałych służb specjalnych. Po

pierwsze, z racji usytuowania w tej samej ustawie, należy wskazać, iż ta sama regulacja dotyczy Agencji Wywiadu (wspólne przepisy). Ponadto wspomniany model znajduje odzwierciedlenie w przepisach ustawy o CBA⁶ i ustawy o SKW oraz SWW⁷, w których to dostrzegamy podobną konstrukcję przepisów „ochronnych”, jak ta w ustawie o ABW oraz AW. Podstawowym przepisem w tym zakresie jest odpowiednio art. 24 ust. 1 ustawy o CBA i art. 39 ust. 1 ustawy o SKW oraz SWW, z których wynika nakaz zapewnienia ochrony środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy danej służby. Ponadto przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze każdej ze służb oraz osoby udzielające służbom pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych mogą posługiwać się dokumentami legalizacyjnymi oraz legalizacyjnymi środkami identyfikacji elektronicznej (ust. 2–3). W kolejnych jednostkach redakcyjnych wymienionych przepisów uregulowano także okoliczności wyłączające bezprawność czynu związanego z wydawaniem i posługiwaniem się dokumentami legalizacyjnymi. Z kolei w art. 30 ust. 1 ustawy o CBA i w art. 44 ustawy o SKW oraz SWW wskazano obowiązek zapewnienia ochrony własnych urządzeń oraz obszarów i obiektów, a także przebywających w nich osób i wskazano formy zapewnienia tej ochrony. W art. 28 ust. 1 ustawy o CBA i w art. 43 ust. 1 ustawy o SKW oraz SWW odnajdziemy regulację dotyczącą udzielania przez szefa służby zezwolenia funkcjonariuszom i pracownikom oraz byłym funkcjonariuszom i pracownikom, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych, na udzielenie informacji niejawnej określonej osobie lub instytucji, która jest zbudowana analogicznie jak regulacja w ustawie o ABW oraz AW — zarówno w zakresie danych podlegających bezwzględnemu zakazowi udostępnienia, jak i wyjątków od tego zakazu. Należy także dodać, iż w ustawach pragmatycznych innych służb specjalnych zawarto również analogiczne upoważnienia do uregulowania, w drodze zarządzenia, sposobów, metod i form wykonywania zadań (art. 10 ust. 3 ustawy o CBA oraz art. 20 ust. 3 ustawy o SKW oraz SWW).

Wskazane wyżej rozważania prowadzą do wniosku, iż potrzeba ochrony działalności służb specjalnych, a w szczególności gromadzonych informacji, wydaje się niezbędna i winna być oczywista. Jednakże owo zagadnienie, w przypadku działalności poprzednika prawnego Agencji Bezpieczeństwa Wewnętrznego, nie pojawiło się jednak w przepisach pierwotnej wersji *ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa*⁸. We wspomnianej ustawie ustawodawca nie wprowadził bowiem wprost przepisu, który statuowałby tę ochronę. Przepis taki został dodany dopiero *ustawą z dnia 21 lipca 1995 r. o zmianie ustaw: o Urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa,*

⁶ Dz.U. 2019, poz. 1921 z późn. zm.

⁷ Dz.U. 2019, poz. 687 z późn. zm.

⁸ Dz.U. 1990, nr 30, poz. 180.

o Straży Granicznej oraz niektórych innych ustaw⁹, która wprowadziła analogiczne przepisy również i w odniesieniu do działalności policji i Straży Granicznej. W myśl art. 11 a ust. 1, w związku z wykonywaniem zadań wymienionych w art. 1 ust. 2 Urząd Ochrony Państwa zapewniał ochronę form i metod realizacji zadań, informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy. Dopełnienie tego przepisu zostało zawarte w kolejnych ustępach, które wskazywały na możliwość posługiwania się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi posługuje się przy wykonywaniu zadań służbowych, a także wprowadzały tę możliwość wobec osób udzielających pomocy Urzędowi Ochrony Państwa. Także i ustawa o WSI¹⁰, która dotyczyła działalności poprzednika prawnego Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego, w art. 34 ust. 1 zawierała przepis dotyczący zapewnienia ochrony danych identyfikujących żołnierzy Wojskowych Służb Informacyjnych i osób, które udzielały im pomocy przy wykonywaniu zadań, a także form, metod i sposobów wykonywania zadań, zgromadzonych informacji oraz ochrony własnych urzędzeń, obiektów i obszarów. Ponadto, w ust. 2–6 regulowała uprawnienia w zakresie dokumentów legalizacyjnych. Natomiast w art. 37 zawarty był przepis dotyczący zezwalania żołnierzom Wojskowych Służb Informacyjnych, pracownikom Wojskowych Służb Informacyjnych oraz byłym żołnierzom i pracownikom na udzielenie informacji niejawniej podmiotom zewnętrznym.

Jak wynika z przytoczonych wyżej rozważań, ramy prawne w omawianym zakresie są niemal analogiczne w odniesieniu do wszystkich służb specjalnych, a także były w podobny sposób ukształtowane w aktach prawnych normujących działania ich poprzedników prawnych.

Praktyczne aspekty funkcjonowania systemu ochronnego w służbach specjalnych na przykładzie działalności Agencji Bezpieczeństwa Wewnętrznego

Przechodząc do omówienia praktycznego wymiaru poszczególnych elementów wspomnianego wyżej „systemu ochronnego” w służbach specjalnych, należy wskazać, iż z pewnością podstawową rolę w zabezpieczeniu informacji odgrywają przepisy *ustawy z dnia 5 sierpnia 2020 r. o ochronie informacji niejawnych*¹¹. Przepisy wspomnianej ustawy wprowadzają bowiem kompleksowy system ochrony informacji i materiałów, którym nadano klauzule tajności, obowiązujący w polskim porządku prawnym — nie tylko w odniesieniu do służb specjalnych, ale także i wobec innych podmiotów publicznych i niepublicznych, które

⁹ Dz.U. 1995, nr 104, poz. 515.

¹⁰ Dz.U. 2003, nr 139, poz. 1326 z późn. zm.

¹¹ Dz.U. 2019, poz. 742.

przetwarzają informacje niejawne. Ustawodawca mocą przepisów tej ustawy, w celu zapewnienia bezpieczeństwa państwa, przez ochronę najważniejszych zasobów informacyjnych wykreował swoiste instrumenty zapewniające bezpieczeństwo wyspecyfikowanych informacji. Nie budzi bowiem wątpliwości, iż skuteczne działanie państwa czy też poszczególnych jego organów wymaga ograniczenia dostępu czy wręcz utajnienia pewnych informacji, ażeby potencjalny przeciwnik nie był w stanie dotrzeć do ich treści, a tym samym nie mógł przeciwdziałać podjętym działaniom. Dlatego też w ustawie wprowadzono klauzule tajności, określono materialne przesłanki nadawania poszczególnych klauzul i formalne aspekty ich nadawania. Z uwagi zaś na niejawność większości działań podejmowanych przez służby, w szczególności w zakresie czynności operacyjno-rozpoznawczych, sam fakt nadania klauzuli tajności informacjom uzyskiwanym w ich toku, a co za tym idzie ściśle reglamentowany dostęp do ich treści — zgodnie z zasadą *need to know*, wynikającą z art. 4 ust. 1 u. inf. niejaw., iż informacje niejawne udostępniane są wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku — stanowi podstawowy instrument do zapewnienia właściwego poziomu ochrony w wielu aspektach działalności służb specjalnych.

Należy także wskazać, iż jeden z instrumentów do realizacji obowiązku ochronnego został wskazany w art. 35 ust. 2–6 ustawy o ABW oraz AW jako instytucja legalizacji, na którą składa się możliwość posługiwania się dokumentami legalizacyjnymi oraz legalizacyjnymi środkami identyfikacji elektronicznej przy wykonywaniu czynności operacyjno-rozpoznawczych przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz osoby udzielające im pomocy. Jak już wyżej wskazano, legalizacja sprowadza się do przyznania uprawnienia do sporządzenia, wydania i posługiwania się dokumentami legalizacyjnymi oraz legalizacyjnymi środkami identyfikacji elektronicznej, które *de facto* stanowią fikcyjne dokumenty, służące do ukrycia prawdziwej tożsamości funkcjonariuszy oraz osób udzielających im pomocy w związku z wykonywaniem przez nich czynności operacyjno-rozpoznawczych. Mogą one dotyczyć, co oczywiste, nie tylko osób fizycznych, lecz także wszelkich innych podmiotów prawa, np. podmiotów gospodarczych lub osób prawnych. Są to dokumenty wydawane w sytuacjach prawnie dopuszczalnych (tzw. ustawywy kontratyp pozakodeksowy), aby nadać legalny charakter nieprawdziwym danym w nim zawartym¹². Należy jednak podkreślić, iż wskazane wyżej przypadki, dopuszczające możliwość posłużenia się fikcyjną tożsamością oraz dokumentami i środkami je potwierdzającymi, obejmują jedynie wykonywanie czynności operacyjno-rozpoznawczych. A zatem, wnioskując *a contrario*, należy stwierdzić, iż nie jest możliwe wydanie dokumentów legalizacyjnych w celu innym niż wykonywanie czynności operacyjno-rozpoznawczych i wobec innych funkcjonariuszy niż

¹² Zob. R. Lizak, *Dokumenty legalizacyjne w służbach specjalnych*, „Prokuratura i Prawo” 2013, t. 2, s. 142–153.

funkcjonariusze operacyjni i osoby udzielające im pomocy. Tak więc poza tą regulacją tej instytucji pozostają wszyscy inni funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, wykonujący służbę w pionie śledczym czy logistycznym, ale także i ci funkcjonariusze z pionów operacyjnych, którzy w danym momencie nie wykonują czynności operacyjno-rozpoznawczych. Wykluczona jest bowiem możliwość posłużenia się dokumentami legalizacyjnymi poza czynnościami operacyjno-rozpoznawczymi, czyli na użytek czynności dochodzeniowo-śledczych czy też innych czynności administracyjnych (urzędowych).

Jednakże, z uwagi na wysoki poziom informatyzacji systemów państwowych oraz przetwarzanie danych funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, jako obywateli Rzeczypospolitej Polskiej, w wielu takich systemach (np. PESEL¹³, Rejestr Dowodów Osobistych¹⁴, Centralny Rejestr Ubezpieczonych¹⁵, Centralny Rejestr Podmiotów — Krajowej Ewidencji Podatników¹⁶, System Informacji Medycznej¹⁷) wydaje się zasadne, aby dotychczas funkcjonujące aspekty bezpieczeństwa personalnego zostały jednak rozszerzone wobec wszystkich funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego i ich rodzin przez możliwość stosowania środków w celu ukrywania faktu służby wobec każdego funkcjonariusza, a nie tylko wobec funkcjonariuszy wykonujących czynności operacyjno-rozpoznawcze i to wyłącznie w związku z wykonywaniem tych czynności. W celu wzmocnienia poziomu bezpieczeństwa ochrony danych funkcjonariuszy służb specjalnych niezbędne jest rozdzielenie przepisów odnoszących się do legalizacji związanej z czynnościami operacyjno-rozpoznawczymi od przepisów obejmujących możliwość ukrywania faktu służby przez wprowadzenie nowej instytucji prawnej tzw. maskowania (legendowania), polegającej na szeroko rozumianej ochronie danych identyfikujących funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz innych służb specjalnych, nie tylko w związku z wykonywaniem czynności operacyjno-rozpoznawczych, ale *a priori* w związku z samym faktem pełnienia służby w danej formacji. Istotność kwestii zabezpieczenia zasobów kadrowych znajduje bowiem swoje uzasadnienie w zakresie zasadności zapewnienia fizycznego bezpieczeństwa danej osoby oraz jej najbliższych. Jak już wyżej wskazano, dane każdego funkcjonariusza podlegają gromadzeniu, przetwarzaniu i udostępnianiu na takich samych zasadach jak dane wszystkich obywateli Rzeczypospolitej Polskiej, tym samym niezbędne jest wprowadzenie mechanizmów minimalizujących ryzyko zidentyfikowania powiązań danych obywatela, będącego jednocześnie funkcjonariuszem, z miejscem jego służby.

¹³ Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. 2021, poz. 510).

¹⁴ Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. 2021, poz. 816).

¹⁵ Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. 2021, poz. 423 z późn. zm.).

¹⁶ Ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz.U. 2020, poz. 170 z późn. zm.).

¹⁷ Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2021, poz. 666 z późn. zm.).

W świetle powyższego zasadne wydaje się zatem wypracowanie rozwiązania, które w sposób kompleksowy podniesie poziom bezpieczeństwa danych funkcjonariuszy służb specjalnych. W toku działań legislacyjnych podejmowanych przez Agencję Bezpieczeństwa Wewnętrznego postulowano wprowadzenie nowych przepisów dotyczących maskowania (legendowania) przez umożliwienie sporządzania i wydawania oraz posługiwania się dokumentami ukrywającymi fakt służby funkcjonariusza w Agencji Bezpieczeństwa Wewnętrznego, a także przez stworzenie dedykowanych funkcjonalności w systemach teleinformatycznych, w których przetwarzane są dane funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, obejmujące w szczególności bezpieczne zarządzanie tymi danymi. Proponowano też umożliwienie stosowania uprawnień administracyjno-porządkowych i określanie przez Szefa Agencji Bezpieczeństwa Wewnętrznego stref ochronnych wokół obszarów lub obiektów oraz ustalanie ograniczeń w zagospodarowaniu i korzystaniu z terenów w tych strefach. Należy bowiem podkreślić, iż warunkiem koniecznym dla efektywnej i skutecznej realizacji zadań spoczywających na Agencji Bezpieczeństwa Wewnętrznego (ale również na innych służbach specjalnych), oprócz posiadania niezbędnych instrumentów w postaci uprawnień, środków finansowych, kompetentnego personelu oraz wspomagających narzędzi technicznych, jest bowiem bezpieczeństwo funkcjonariuszy (ale także i członków ich rodzin), a aktualnie obowiązujące przepisy ustawowe nie pozwalają na podejmowanie działań „maskujących” przez dokonywanie w tym celu niezbędnych działań w systemach teleinformatycznych ani nie zawierają instytucji maskowania (legendowania), umożliwiającej ukrywanie faktu służby w związku z wszelkimi czynnościami podejmowanymi przez funkcjonariuszy, w tym m.in. w zakresie wystawiania zaświadczeń o miejscu pracy, uzyskiwaniu dochodów, które są niezbędne w wielu sprawach życia codziennego i rodzinnego.

Należy także wskazać, iż uprawnienie w zakresie wprowadzania danych osobowych do systemów informatycznych oraz kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych organów państwowych i jednostek samorządu terytorialnego, innych państwowych lub komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych, realizujących zadania publiczne przysługuje już funkcjonariuszom Centralnego Biura Śledczego Policji na podstawie art. 18 a *ustawy z dnia 25 czerwca 1997 r. o świadku koronnym*¹⁸. Przepis ten pozwala na wprowadzanie fikcyjnych danych do systemów teleinformatycznych, we współdziałaniu z właściwymi organami państwa, nie tylko prowadzącymi takie systemy, ale także z innymi organami, które mogą udzielić pomocy w danej sprawie. Wprawdzie ustawa o świadku koronnym nie definiuje owej „pomocy”, ale wydaje się to zabiegiem słusznym, gdyż jej forma będzie zależała od wielu okoliczności, takich jak np.: charakterystyka danego systemu ewidencyjnego, rodzaj wprowadzanych informacji czy zakres

¹⁸ Dz.U. 2016, poz. 1197.

podmiotowy (liczba osób objętych nadaniem fikcyjnej tożsamości)¹⁹. Wobec powyższego Agencja Bezpieczeństwa Wewnętrznego podejmowała próby zastosowania analogicznego rozwiązania w zakresie wprowadzania danych do systemów i rejestrów w swojej ustawie pragmatycznej, a także zgłaszała propozycje legislacyjne dotyczące uregulowania tego zagadnienia w poszczególnych ustawach regulujących działania konkretnych rejestrów państwowych. Wprawdzie do chwili obecnej nie udało się wprowadzić do ustawy o ABW oraz AW instytucji maskowania ani ogólnego przepisu dotyczącego możliwości wprowadzania danych osobowych funkcjonariuszy w systemach teleinformatycznych, to jednakże *ustawą z dnia 9 października 2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw*²⁰ wprowadzono stosowny przepis w *ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia*²¹, który wprowadza minimalne wymagania dla systemów teleinformatycznych regulowanych tą ustawą, uwzględniające bezpieczeństwo przetwarzania i udostępniania danych dotyczących funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz innych służb specjalnych i członków ich rodzin w zakresie ochrony tych danych, przewidzianej w art. 35 ust. 1 ustawy o ABW oraz AW, a także analogicznych przepisach zawartych w ustawach pragmatycznych innych służb specjalnych.

W aspekcie bezpieczeństwa danych osobowych funkcjonariuszy i osób udzielających pomocy przy wykonywaniu czynności oraz bezpieczeństwa zgromadzonych informacji wskazywany już wielokrotnie przepis art. 35 ust. 1 ustawy o ABW oraz AW należy interpretować łącznie z art. 39 ust. 1 ustawy o ABW oraz AW, który wprowadza szczególną regulację dotyczącą udostępniania informacji o czynnościach operacyjno-rozpoznawczych podmiotom zewnętrznym, tj. osobom spoza struktury służb specjalnych i innym instytucjom przez mechanizm uzyskania zezwolenia Szefa Agencji Bezpieczeństwa Wewnętrznego na udzielenie niejawnej informacji określonej osobie lub instytucji.

Należy jednak dodać, iż na podstawie ust. 3 wspomnianego przepisu informacji o osobach, jeżeli zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych, informacje o osobach udzielających pomocy Agencji oraz jej poprzednikowi prawnemu, informacje o szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz o stosowanych w związku z ich prowadzeniem środkach i metodach, a w niektórych przypadkach również o rezultatach tych czynności, są objęte ustawowym bezwzględny zakazem ich udostępniania. Ustawodawca przewidział jedynie nieliczne przypadki, w których osoby spoza służb mogą mieć dostęp do takich informacji. Zgodnie zaś z art. 39 ust. 3 i 4 ustawy o ABW oraz AW takie informacje mogą zostać udostępnione wyłącznie na żądanie prokuratora albo sądu, zgłoszone

¹⁹ M. Gabriel-Węglowski, *Ustawa o świadku koronnym. Komentarz. Zarys instytucji w Europie*, Lex 2011, [dostęp: 17 VI 2021].

²⁰ Dz.U. 2015, poz. 1991 z późn. zm.

²¹ Dz.U. 2021, poz. 666 z późn. zm.

w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych, a także na żądanie prokuratora lub sądu, uzasadnione podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Należy jednak wskazać, iż zastosowanie art. 39 ust. 1 ustawy o ABW oraz AW przez wydanie przez Szefa Agencji Bezpieczeństwa Wewnętrznego zezwolenia na udostępnienie informacji niejawnej nie oznacza, że informacje przez fakt przekazania przestają być objęte ochroną wynikającą z nadanej klauzuli tajności. Nadal podlegają one ochronie jako informacje niejawne, a zatem podlegają nadal wszelkim rygorom wynikającym z ustawy o ochronie informacji niejawnych, w tym m.in. w zakresie zakazu dalszego ich udostępnienia.

W kontekście stosowania art. 39 ust. 1 ustawy o ABW oraz AW jako elementu systemu ochronnego, co już wyżej zasygnalizowano, przepisy ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, jak również i przepisy innych ustaw pragmatycznych, stanowią przejaw swoistej autonomii szefa służb w zakresie udostępnienia lub odmowy udostępnienia wobec konkretnych informacji niejawnych²². Wspomniany przepis nie wprowadza bowiem szczegółowego trybu udzielania takiego zezwolenia przez szefa służby, czy też nie przewiduje możliwości odwołania się od odmowy udzielenia zezwolenia na udostępnienie informacji niejawnych podmiotom zewnętrznym. Mechanizm ten pozwala zatem na swoiste filtrowanie przez Szefa Agencji Bezpieczeństwa Wewnętrznego informacji niejawnych pod kątem możliwości i zasadności ich udostępnienia poza strukturę służby, co wpływa także na podniesienie skuteczności systemu ochronnego.

Należy także zwrócić uwagę na problemy dotyczące skutecznego zapewnienia bezpieczeństwa informacyjnego w kontekście wnioskowania o udostępnienie informacji publicznych dotyczących działalności służb specjalnych. W tym obszarze ścierają się bowiem dwie wartości — z jednej strony mamy ustawowy nakaz ochrony pewnych informacji (ustawa o ochronie informacji niejawnych oraz art. 35 ust. 1 i art. 39 ust. 1–3 ustawy o ABW oraz AW), a z drugiej strony oczekiwania społeczne i nadzór obywatelski wcielany w życie na podstawie przepisów Konstytucji Rzeczypospolitej Polskiej²³ oraz *ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej*²⁴. Na podstawie tych przepisów informacje dotyczące działalności Agencji Bezpieczeństwa Wewnętrznego, z uwagi na fakt, że jest ona urzędem administracji publicznej, finansowanym ze środków publicznych, podlegają udostępnieniu jako informacje publiczne. Wprawdzie

²² M. Bożek, *Sejmowa kontrola działalności służb specjalnych i jej ograniczenia wynikające z ustaw kompetencyjnych. Zarys problemu na tle uwarunkowań normatywnych*, „Studia Iuridica Lublinensia” 2013, t. 20, s. 62–66.

²³ Dz.U. 1997, poz. 78 z późn. zm.

²⁴ Dz.U. 2020, poz. 2176.

w ustawie o dostępie do informacji publicznej ustawodawca wprowadził podstawę prawną do odmowy udostępnienia informacji publicznej z uwagi na ograniczenia wynikające z przepisów o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych (art. 5 ust. 1 ustawy o dostępie do informacji publicznej), jednakże problemy w działalności służb w kontekście udostępniania informacji pojawiły się w odniesieniu do wniosków o dostęp do informacji publicznej, które zawierały pytania o informacje z zakresu ustawowej działalności służb specjalnych, które w przeważającej mierze dotyczyły działań operacyjnych, ale nie były oznaczone klauzulą tajności. W przypadku tych informacji i wydawanych przez szefa służby decyzji odmawiających ich udostępnienia, z uwagi na ograniczenia prawne wynikające z art. 35 ust. 1 i art. 39 ustawy o ABW oraz AW, pojawiały się wątpliwości i zarzuty wnioskodawców co do prawidłowości działania organu, które następnie były rozstrzygane przez sądy administracyjne w toku kontroli sądowo-administracyjnej. Można powiedzieć nawet, iż na tym tle ukształtowała się pewna linia orzecznicza, albowiem w uzasadnieniach do wyroków w tych sprawach²⁵ Naczelny Sąd Administracyjny stwierdził, iż w niektórych przypadkach samo wskazanie konkretnych zagrożeń, związanych z ewentualnym udostępnieniem żądanych informacji, mogłoby prowadzić do ujawnienia informacji objętych odmową. Ponadto Naczelny Sąd Administracyjny stwierdził, że Agencja Bezpieczeństwa Wewnętrznego jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, a katalog jej zadań określa art. 5 ust. 1 ustawy o ABW oraz AW, zaliczając do nich m.in. rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa. Naczelny Sąd Administracyjny podkreślił, że zakwalifikowanie informacji z zakresu 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. inf. niejaw.

Z kolei art. 39 ust. 3 ustawy o ABW oraz AW potwierdza, że podane w nim informacje ustawodawca traktuje jako szczególnie zasługujące na ochronę przed ujawnieniem. W ocenie sądu przepisy te powinny być powiązane z regulacjami ustawy o ochronie informacji niejawnych. Naczelny Sąd Administracyjny dodał również, że przepisy art. 35 i art. 39 ustawy o ABW oraz AW stanowią wprawdzie przepisy kompetencyjne, a nie materialnoprawne, ale mogą one stanowić podstawę odmowy udostępnienia informacji publicznej, gdyż mogą być one współstosowane z przepisami ustawy o ochronie informacji niejawnych. W świetle powyższego można zatem stwierdzić, iż cytowane wyżej przepisy, pomimo

²⁵ Wyrok NSA z dnia 8 III 2017 r., I OSK 1312/15, Lex nr 2 267 585, wyrok NSA z dnia 6 IX 2016 r., I OSK 291/15, Lex nr 1 988 083, wyrok NSA z dnia 6 IX 2016 r., I OSK 210/15, Lex nr 2 143 005.

ich bardzo ogólnego brzmienia, poparte dotychczasową praktyką służb, znajdującą odzwierciedlenie w orzecznictwie sądów, mogą zostać potraktowane jako swoisty mechanizm prawnej ochrony zgromadzonych informacji, uzupełniający przepisy ustawy o ochronie informacji niejawnych.

W aspekcie praktycznego wymiaru funkcjonowania systemu ochronnego warto także dodać, iż wspomniany już wcześniej art. 19 ust. 3 ustawy o ABW oraz AW, upoważniającego szefa służby do uregulowania, w drodze zarządzenia, szczegółowych kwestii dotyczących wykonywania zadań, nie wskazuje jednak na to, jakich zadań służby może dotyczyć zarządzenie ani też jakie czynności funkcjonariuszy powinny być w nim uregulowane. Oznacza to zatem, że w drodze takiego zarządzenia można uregulować wszelkie czynności podejmowane przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, które nie zostały uregulowane w innych przepisach, a ich realizacja przybiera postać *sposobów, form i metod*. Z uwagi na niejawny charakter czynności operacyjno-rozpoznawczych i brak szczegółowej regulacji tego zagadnienia na poziomie ustawowym Szef Agencji Bezpieczeństwa Wewnętrznego (oraz szefowie pozostałych służb specjalnych) na podstawie ustawowych upoważnień reguluje szczegółowe zasady i formy prowadzenia działań operacyjno-rozpoznawczych w drodze niejawnych zarządzeń. Ze względu na klauzulę nadaną takim dokumentom nie są możliwe w niniejszym rozdziale dalsze rozważania dotyczące ich treści, jednakże oczywistym jest, że przepisy wewnętrznych aktów prawnych, w tym także w zakresie wykonywania czynności operacyjno-rozpoznawczych, nie mogą być sprzeczne z ogólnymi rozwiązaniami przyjętymi w aktach powszechnie obowiązujących. W świetle powyższych dywagacji można wysnuć wniosek, iż przepis upoważniający do wydania aktu wewnętrznego może zostać uznany także jako odrębna forma ochrony, wprawdzie część z tych aktów jest wydawana jako dokumenty jawne, natomiast pozostałe, z uwagi zaś na zawartość treściową, przyjmują postać dokumentów oznaczonych klauzulą tajności, co w oczywisty sposób ogranicza krąg ich potencjalnych odbiorców i mieści się w kategorii dodatkowego, obok obowiązujących przepisów ustawy o ochronie informacji niejawnych, zabezpieczenia informacji dotyczących najbardziej wrażliwych aspektów działania służby.

Odnosząc się do bezpieczeństwa w aspekcie fizycznej ochrony obiektów, jak już wyżej wskazano, art. 43 ustawy o ABW oraz AW statuuje obowiązek zapewnienia ochrony wykorzystywanych urządzeń oraz obszarów i obiektów, wykonywany przy pomocy funkcjonariuszy wewnętrznej służby ochrony. W ust. 2 tego przepisu wymieniono dedykowane w tym celu uprawnienia, polegające m.in. na: legitymowaniu osób w celu ustalenia tożsamości, wydawaniu poleceń dotyczących określonego zachowania czy ujęciu osób stwarzających zagrożenia życia lub zdrowia ludzkiego i chronionego mienia. Jednakże przez lata funkcjonowania tego przepisu obserwowano zachodzący postęp technologiczny i dostrzeżono, iż wymienione w nim aktywności nie w pełni odpowiadają aktualnym potrzebom ochronnym. Uznano wówczas zasadność wprowadzenia zmiany w tym przepisie w aspekcie możliwości przeciwdziałania używaniu nowego narzędzia, które

stało się coraz bardziej popularne i dostępne na rynku. *Ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*²⁶ dokonano nowelizacji wspomnianego przepisu ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i wprowadzono kolejne uprawnienie w zakresie fizycznej ochrony obiektów i obszarów przez możliwość zniszczenia, unieruchomienia lub przejęcia kontroli lotu bezzałogowego statku powietrznego, w tym modelu latającego.

Podsumowanie

Służby specjalne, wykonując powierzone im ustawowe zadania niezbędne do prawidłowego funkcjonowania państwa, które w przeważającej mierze mają charakter niejawny, winny być bez wątpienia wyposażone w instrumenty prawne pozwalające im na zachowanie tzw. szczelności informacyjnej i zapewnienie jak najwyższego poziomu bezpieczeństwa życia i zdrowia ich funkcjonariuszy. Nieuprawnione ujawnienie zgromadzonych informacji, czy też danych funkcjonariuszy wykonujących czynności służbowe, może powodować kompromitację podejmowanych działań, ale także może narażać życie i zdrowie wykonujących je funkcjonariuszy. W świetle powyższych rozważań można wysnuć wnioski, iż zagadnienie funkcjonowania tzw. systemu ochronnego w służbach specjalnych, pomimo oczywistego i fundamentalnego znaczenia tego zagadnienia dla bezpieczeństwa służby, które także pośrednio wpływa na bezpieczeństwo państwa, jest regulowane w sposób bardzo ogólny w ustawach pragmatycznych. Wprawdzie z tych przepisów można wywnioskować zakres ochrony i zapewnić jej odpowiedni poziom, to jednakże, w świetle postępującej informatyzacji i związanych z nią zmian w systemach teleinformatycznych, zasadne wydaje się sformułowanie postulatów *de lege ferenda*.

Przede wszystkim w obliczu zmian technologicznych i informatyzacji niemal wszystkich dziedzin życia, w tym także w zakresie funkcjonowania rejestrów państwowych, zasadny wydaje się postulat doprecyzowania kolejnych form ochrony danych funkcjonariuszy na poziomie ustawowym przez wprowadzenie mechanizmów umożliwiających podejmowanie szeroko rozumianych działań maskujących (legendujących) w odniesieniu do danych osobowych funkcjonariuszy służb specjalnych i ich rodzin w aspekcie ukrywania faktu służby bądź też przynajmniej wprowadzenie w ustawach pragmatycznych przepisu zawierającego upoważnienie do wydania aktu prawnego w tym zakresie przez szefa właściwej służby. Pozwoli to na pogłębienie zakresu systemu ochronnego i umożliwi zapewnienie ochrony na wyższym poziomie, również i w aspektach pozaoperacyjnych, które aktualnie pozostają poza regulacją ustawową. Niezbędne jest też, o czym wspomniano już wyżej, podjęcie inicjatywy legislacyjnej, zmierzającej do uchwalenia przepisów umożliwiających funkcjonariuszom Agencji Bezpieczeństwa Wewnętrznego i innych służb specjalnych wprowadzanie danych osobowych do systemów teleinformatycznych i innych

²⁶ Dz.U. 2016, poz. 904 z późn. zm.

zbiorów ewidencyjnych organów państwowych, jednostek samorządu terytorialnego oraz innych podmiotów niepaństwowych realizujących zadania publiczne w celu sporządzania i wydawania dokumentów legalizacyjnych.

Ponadto w celu zapewnienia szczelności informacyjnej i skuteczniejszej ochrony informacji dotyczących najbardziej wrażliwych działań służb specjalnych oraz uniknięcia wikłania służb specjalnych w długotrwałe procesy sądowe w zakresie odmowy dostępu do informacji publicznej, które powodują nieuzasadnione, a wręcz szkodliwe, zainteresowanie podmiotów zewnętrznych zagadnieniami, które nie powinny być analizowane w przestrzeni publicznej, zasadne wydaje się wprowadzenie w przepisach ustawy o dostępie do informacji publicznej wyłączenia spod jej zakresu obowiązywania informacji jawnych dotyczących działalności ustawowej służb specjalnych bądź też wprowadzenia odrębnej kategorii tajemnicy w postaci „tajemnicy służb specjalnych”, która obejmowałaby podstawę prawną do odmowy udostępnienia informacji, które nie są oznaczone klauzulą tajności, ale zawierają informacje dotyczące wrażliwych aspektów funkcjonowania służb specjalnych. Wprowadzenie systemowego rozwiązania w tym zakresie pozwoli na sprawne i obiektywne rozstrzygnięcie spraw związanych z odmową udostępniania takich informacji na podstawie ustawy o dostępie do informacji publicznej, co w świetle wagi tych informacji i powinności ich ochrony przez służbę nieco wypacza, skądinąd słuszną, ideę dostępu do informacji o sprawach publicznych.

W świetle powyższych rozważań można skonstatować, iż funkcjonujący aktualnie system ochronny wprawdzie spełnia swoje podstawowe zadania w sferze bezpieczeństwa fizycznego, personalnego i informacyjnego w służbach specjalnych, ale uwzględnienie postulatów legislacyjnych pozwoli na jego rozbudowanie i skuteczniejsze funkcjonowanie na przyszłość, co znacząco wpłynie na poprawę bezpieczeństwa funkcjonariuszy i ich rodzin, a tym samym na sprawniejsze wykonywanie działań przez służby specjalne w obszarze zapewnienia bezpieczeństwa państwa.

Piotr Burczaniuk

Rozdział 9.

Problematyka tworzenia prawa wewnętrznego służb specjalnych na przykładzie ABW

Wstęp

Niniejszy rozdział ma na celu przybliżenie problematyki tworzenia prawa wewnętrznego służb specjalnych ze szczególnym uwzględnieniem doświadczeń wynikających z kreacji tego rodzaju prawa w Agencji Bezpieczeństwa Wewnętrznego. Co istotne, przedmiotowe zagadnienie nie spotkało się do chwili obecnej z szerszą analizą prowadzoną w obszarze nauk teoretyczno-prawnych bądź dogmatycznych, choć dotyka — jak się wydaje — istotnego problemu badawczego, jakim jest wyznaczenie zakresu i sposobu konstruowania przepisów prawa wewnętrznego, związanych z funkcjonowaniem służb specjalnych. W tym kontekście zagadnienie to jest szczególnie interesujące z perspektywy zmian, jakie zaszły w obszarze kreacji tego rodzaju prawa wraz z przyjęciem katalogu źródeł prawa przez Konstytucję RP z 1997 r. i zauważalnym wówczas problemem kwalifikacji poszczególnych norm prawnych według podziału na obowiązujące powszechnie i wewnątrznie, co *może w niektórych przypadkach rodzić pewne kontrowersje i spory. (...) Dopiero — jak można sądzić — orzecznictwo Trybunału Konstytucyjnego, sądów oraz dorobek doktryny pozwoli na wyostrenie granic pomiędzy tymi rodzajami norm*¹. Niniejszy tekst stanowi więc głos w tej dyskusji, formułowany z perspektywy ponad dwudziestoletniego obowiązywania wskazanej dychotomii norm.

W niniejszym rozdziale problematyka tworzenia prawa wewnętrznego została przedstawiona głównie z wykorzystaniem metody prawno-porównawczej oraz dogmatycznej, wspartej analizą historyczną poszczególnych instytucji. Na podstawie wskazanej metodologii w pierwszej kolejności ukazano miejsce

¹ Uzasadnienie do druku nr 1397 dostępne jest *online*. Protokół dostępu: [https://orka.sejm.gov.pl/RejestrD.nsf/wgdruku/1397/\\$file/1397.pdf](https://orka.sejm.gov.pl/RejestrD.nsf/wgdruku/1397/$file/1397.pdf), [dostęp: 18 VIII 2021].

aktu prawa wewnętrznego w systemie źródeł prawa zbudowanym przez Konstytucję RP z 1997 r., z rozbudowaną analizą samego pojęcia prawa wewnętrznego. W części trzeciej, bazując na tak zarysowanym zakresie przedmiotowym, przedstawiono rys historyczny znaczenia prawa wewnętrznego dla kształtowania zasad ustrojowych funkcjonowania służb specjalnych po 1945 r. W czwartej części natomiast zaprezentowane zostały obowiązujące materialne podstawy kreacji prawa wewnętrznego służb specjalnych, zaś w części piątej przybliżono aspekty proceduralne kreacji tego rodzaju prawa. W ostatniej części zwrócono uwagę na zagadnienie ogłaszania prawa w służbach specjalnych, ze szczególną analizą problematyki ogłaszania prawa niejawnego. Rozdział został zwieńczony podsumowaniem.

Miejsce aktu prawa wewnętrznego w systemie źródeł prawa

Punktem wyjścia do rozważań o miejscu aktu prawa wewnętrznego w systemie źródeł prawa musi stać się analiza przepisów rozdziału trzeciego Konstytucji RP, wprowadzającego dychotomiczny podział źródeł prawa na dwie kategorie — aktów prawa powszechnie obowiązującego i aktów prawa wewnętrznego.

Zgodnie z art. 87 ust. 1 Konstytucji RP źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. W świetle cytowanego przepisu oraz innych postanowień Konstytucji RP, w szczególności charakteryzujących zadania organów trójdzielnej władzy, wskazać należy, iż prawodawca konstytucyjny przyjął podmiotowo przedmiotowy system źródeł prawa powszechnie obowiązującego, na który składają się w aspekcie przedmiotowym określone (wymienione powyżej) formy aktów prawnych, a w aspekcie podmiotowym określone organy konstytucyjne upoważnione do kreacji tych konkretnych form aktów prawnych w procedurach do nich przypisanych. Cechą tak zdefiniowanych aktów prawa powszechnie obowiązującego, na co wskazuje się w doktrynie, jest to, że *mogą wiązać każdy podmiot pozostający pod władzą publiczną RP; mogą być także podstawą decyzji i innego rodzaju władczych rozstrzygnięć wobec jednostki lub innego podmiotu podobnego*².

Z kolei, zgodnie z art. 93 ust. 1 Konstytucji RP uchwały Rady Ministrów oraz zarządzenia Prezesa Rady Ministrów i ministrów mają charakter wewnętrzny i obowiązują tylko jednostki organizacyjnie podległe organowi wydającemu te akty. Na kanwie brzmienia tego przepisu, uwzględniając konstrukcję aktów prawa powszechnie obowiązującego, omówienie problematyki aktów prawa

² *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziejewicz, WKP, Warszawa 2019, art. 87 [online]; protokół dostępu: <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587806681/604121/tuleja-piotr-red-konstytucja-rzeczypospolitej-polskiej-komentarz?cm=URELATIONS>, [dostęp: 26 IV 2021]. Szersza analiza aktów prawa powszechnie obowiązującego pozostaje poza zakresem przedmiotowym niniejszego rozdziału.

wewnętrznego wymaga poruszenia zagadnień koncentrujących się na wskazaniu dopuszczalnych form, w których akty prawa wewnętrznego mogą być konstruowane; organów, które są upoważnione do ich stanowienia i wreszcie zakresu merytorycznego, który może być przedmiotem ich regulacji.

W doktrynie prawniczej³ i orzecznictwie Trybunału Konstytucyjnego jednoznacznie wskazuje się:

że system aktów prawa wewnętrznego ma — w przeciwieństwie do systemu aktów będących źródłami prawa powszechnie obowiązującego — charakter systemu otwartego, w każdym razie w zakresie podmiotowym. Trzon tego systemu stanowią akty wymienione w art. 93 ust. 1, ale nie ma konstytucyjnego zakazu, by przepisy ustawowe upoważniały także inne podmioty do stanowienia zarządzeń czy uchwał, bądź też nawet aktów inaczej nazwanych, ale też odpowiadających charakterystyce aktu o charakterze wewnętrznym⁴.

Analizowany przepis konstytucyjny znajduje więc zastosowanie podmiotowe, zakresowo wykraczające poza wymienione w nim organy (Prezesa Rady Ministrów, ministrów i Radę Ministrów) oraz formy (uchwały i zarządzenia). Można więc wyprowadzić wniosek, iż od strony podmiotowej stanowienie prawa wewnętrznego przynależy szeroko rozumianym organom administracji publicznej i nie jest uzależnione od oznaczonego w jego tytule rodzaju aktu. Jak wskazuje M. Haczkowska, *zakresu podmiotowego nie można jednak rozciągać na podmioty o charakterze prywatnoprawnym, takie jak spółki prawa handlowego, stowarzyszenia, fundacje, a także podmioty publiczne posiadające ustawowo lub nawet konstytucyjnie zagwarantowaną autonomię, jak np. uczelnie wyższe*⁵. Od strony przedmiotowej zaś zaliczenie aktu stanowienia prawa jako prawa wewnętrznego wiąże się z koniecznością wypełniania przez niego cech charakterystycznych dla tego rodzaju źródła prawa, do których zaliczyć należy przede wszystkim wymóg adresacji wyłącznie do *jednostek organizacyjnie podległych organowi wydającemu te akty*, co po pierwsze oznacza, iż nie mogą stanowić podstawy do rekonstrukcji norm powszechnie obowiązujących, po drugie zaś, iż zakres adresatów tych norm jest silnie ograniczony do zakresu definicyjnego organizacyjnej podległości. W tym miejscu przytoczyć należy stanowisko Trybunału Konstytucyjnego, który w swoim orzecznictwie zarysował trzy wymiary więzi rozumianej pod pojęciem „organizacyjnej podległości”:

- 1) tzw. hierarchiczne podporządkowanie, w znaczeniu przyjętym w prawie administracyjnym:

³ Por. m.in. M. Haczkowska, w: R. Balicki i in., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2014, art. 93, tekst dostępny *online*. Protokół dostępu: <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587599077/396517/haczkowska-monika-red-konstytucja-rzeczypospolitej-polskiej-komentarz?cm=URELATIONS>, [dostęp: 27 IV 2021].

⁴ Tak wyrok TK z 1 XII 1998 r., K 21/98, OTK 1998, nr 7, poz. 116.

⁵ Zob. przypis 491.

wyrażające jednostronną zależność organu niższego stopnia od organu stopnia wyższego lub podmiotu podległego od podmiotu zwierzchniego. Na tę zależność składają się dwa elementy: zależność osobowa i zależność służbowa. Zależność osobowa rozpoczyna się z chwilą nawiązania stosunku pracy osoby pełniącej funkcje organu, a kończy w momencie jego ustania. Jej treścią jest regulowanie stosunków osobowych w czasie trwania stosunku pracy (awansowanie, nagradzanie, przeniesienie na inne stanowisko, odpowiedzialność służbowa, porządkowa, odpowiedzialność dyscyplinarna). Niekiedy rozszerza się pojęcie zależności osobowej przez włączenie do niej dyspozycyjności pracownika. Zależność osobowa łączy się ściśle z zależnością służbową. Podległość służbowa w systemie hierarchicznego podporządkowania wyraża się w możliwości wydawania poleceń służbowych przez organ wyższy organowi niższemu. Kierowanie organem niższym w obrębie zależności służbowej odbywa się za pomocą aktów dwójakiego rodzaju: aktów generalnych (okólników, wytycznych, instrukcji, zarządzeń) oraz aktów indywidualnych (poleceń służbowych). Stosunek organizacyjny, wyrażający się w hierarchicznym podporządkowaniu, jest stosunkiem między organami administracji publicznej. Jego treść podobna jest do treści stosunków powstających między pracownikami urzędów a ich zwierzchnikami służbowymi⁶;

- 2) więź ustrojowo-prawną, która kształtowana jest przepisem o charakterze ustrojowym, budującym normę, której dyspozycja kształtuje zależność podległości jednego podmiotu (organu) pod drugi podmiot (organ), między którymi nie zachodzi klasyczny administracyjny stosunek hierarchicznego podporządkowania. Jak wskazano w orzecznictwie Trybunału Konstytucyjnego, relacja taka zachodzi między np. Najwyższą Izbą Kontroli a Sejmem RP, między którymi podległość ta została wprost ustalona w konstytucji⁷;
- 3) więź funkcjonalną, która jest kształtowana między konstytucyjnym organem państwowym a podmiotami prywatnymi, tworzącymi łączny funkcjonalny związek systemowy oparty na realizacji tożsamego zadania kierunkowego, przyjmującego postać konstytucyjnego zadania publicznego. Ukształtowanie tego sposobu rozumienia pojęcia organizacyjnej podległości ukształtował Trybunał Konstytucyjny, rozpatrując problematykę uchwał Rady Polityki Pieniężnej i Zarządu Narodowego Banku Polskiego w kontekście konstytucyjnego katalogu źródeł prawa, uznając je za akty prawne o charakterze wewnętrznym. Pozycja banków komercyjnych wobec NBP została przez Trybunał utożsamiona z organizacyjną podległością w ramach opisanego w doktrynie prawniczej systemu prawa bankowego. Jak wskazano w orzeczeniu Trybunału:

⁶ Wyrok Trybunału Konstytucyjnego z dnia 28 VI 2000 r., sygn. K 25/99, OTK 2000, nr 5, poz. 141.

⁷ Szerzej na ten temat w wyroku Trybunału Konstytucyjnego z dnia 1 XII 1998 r., sygn. K 21/98, OTK 1998, nr 7, poz. 116.

wiodąca rola banku centralnego jako banku banków powoduje, że mimo samodzielności i formalnej niezależności banków komercyjnych, w zakresie polityki pieniężnej są one poddane zależności, pozwalającej na określenie jej funkcjonalną podległością. Zdaniem Trybunału, w tym wypadku podległość organizacyjna powinna być rozumiana szerzej, a więc również jako obejmująca podległość funkcjonalną. Dostrzegając niebezpieczeństwo „rozchwiania” konstytucyjnej koncepcji prawa wewnętrznego, Trybunał Konstytucyjny ogranicza możliwość takiej interpretacji do specyficznej sytuacji, gdy mianowicie podmiotem jest konstytucyjna instytucja — Narodowy Bank Polski, zaś przedmiotem konstytucyjnie określone zadania publiczne. Tylko więc spełnienie łącznie obu przesłanek, podmiotowej i przedmiotowej, pozwala na przyjęcie ich jako kryteriów podległości organizacyjnej do wydawania aktów normatywnych o wewnętrznym charakterze⁸.

Warto zwrócić uwagę, na co wskazuje P. Radzewicz, analizując orzeczenie Trybunału Konstytucyjnego z 19 października 2010 r. w sprawie o sygn. K 35/09⁹, iż art. 93 Konstytucji stanowi również jeden ze środków ochrony samodzielności statusu organu przed narzucaniem mu przez organ, wobec którego nie pozostaje on w relacji organizacyjnej podległości, aktów prawa wewnętrznego. Założenie to w sposób oczywisty podkreśla autonomię organu w zakresie kreacji aktów prawa wewnętrznego, określającego tryb jego pracy bądź organizacji i środek ochrony przed narzucaniem takich aktów prawnych niejako „z zewnątrz”¹⁰.

Wszystkie opisane powyżej rodzaje więzi stanowią, zdaniem TK, uzasadnienie do wydawania aktów prawa wewnętrznego.

W uzupełnieniu zwrócić należy uwagę na oczywiste rozdzielenie aktów prawa wewnętrznego jako źródeł prawa będących wynikiem procesu tworzenia prawa, dających tym samym podstawę do wyprowadzania z nich norm generalnych i abstrakcyjnych, od aktów stosowania prawa, którymi w określonym stanie faktycznym ustalana jest przez organ decyzyjny norma indywidualno-konkretna. Świadomość tego rozróżnienia jest istotna, gdyż w wyjątkowych sytuacjach, związanych przykładowo z tożsamością nazwy rodzaju aktu, np. decyzją, ustalenie jego charakteru jako aktu tworzenia lub stosowania prawa, a w konsekwencji rodzaju zawartych w nim norm, będzie wymagało szczególowej analizy jego postanowień.

⁸ Wyrok Trybunału Konstytucyjnego z dnia 28 VI 2000 r., sygn. K 25/99, OTK 2000, nr 5, poz. 141.

⁹ Wyrok Trybunału Konstytucyjnego z dnia 19 X 2010 r., sygn. K 35/09, OTK-A 2010, nr 8, poz. 77.

¹⁰ P. Radzewicz, zob. *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radzewicz, WKP, Warszawa 2019, art. 93, tekst dostępny online; protokół dostępu: <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587806687/604127/tuleja-piotr-red-konstytucja-rzeczypospolitej-polskiej-komentarz?cm=URELATIONS>, [dostęp: 29 IV 2021].

Znaczenie prawa wewnętrznego dla kształtowania zasad ustrojowych funkcjonowania służb specjalnych — rys historyczny

Ukształtowany w sposób opisany powyżej aktualny katalog źródeł prawa stanowi swoiste *novum* wobec modelu przyjętego w tym zakresie przez *Konstytucję Polskiej Rzeczypospolitej Ludowej z dnia 22 lipca 1952 r.*¹¹ i utrzymanego przez *Ustawę Konstytucyjną z dnia 17 października 1992 r. o wzajemnych stosunkach między władzą ustawodawczą i wykonawczą Rzeczypospolitej Polskiej oraz o samorządzie terytorialnym*¹² tzw. Małą Konstytucję, które w katalogu aktów wykonawczych mieściły zarówno rozporządzenia, jak i uchwały Rady Ministrów oraz zarządzenia Prezydenta, Prezesa Rady Ministrów i ministrów. Ten fakt prawny jest szczególnie istotny z perspektywy analizy historycznej regulacji ustrojowych służb specjalnych w Polsce po drugiej wojnie światowej i swoistego wpływu tego „dziedzictwa” na prawne funkcjonowanie służb specjalnych współcześnie.

W tym miejscu wskazać bowiem należy, iż kształtowanie służb specjalnych, cywilnych i wojskowych, w okresie PRL, sprowadzające się do określania ich struktury organizacyjnej, zasad pracy, w tym przede wszystkim pracy operacyjnej oraz statusu prawnego ich funkcjonariuszy, przybierało postać zarządzeń kształtowanych w strukturze resortu spraw wewnętrznych lub obrony narodowej, które jako niejawne (głównie ściśle tajne) akty prawne przybierały formę instrukcji, wytycznych lub rozkazów, w tym rozkazów personalnych. Regulacja ustawowa wyodrębniająca na poziomie ustawowym Służbę Bezpieczeństwa została wprowadzona dopiero ustawą z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów¹³. Przepisami tymi, które uznać należy za ustrojowe, aparat państwowy „przyznał się” do istnienia SB, tworząc jednocześnie „oficjalnie” dwa lata później, *ustawą z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej Polskiej Rzeczypospolitej Ludowej*¹⁴, korpus jej funkcjonariuszy. Obie wymienione ustawy nie obejmowały treścią delegacji do kształtowania aktów prawnych rangi zarządzenia. Ich kreacja była elementem ustrojowo naturalnym, wynikającym z opisanego wyżej konstytucyjnego katalogu źródeł prawa tego okresu. Jednocześnie, co warto podkreślić, służby wojskowe przez cały okres PRL funkcjonowały na zasadach jednostek organizacyjnych, wyodrębnionych w strukturze Sztabu Generalnego Wojska Polskiego, i przez cały ten okres prawna podstawa ich działania opierała się wyłącznie na aktach prawnych rangi zarządzenia, w tym wypadku Ministra Obrony Narodowej, Szefa Sztabu Generalnego czy też szefów poszczególnych zarządów.

Wraz ze zmianami ustrojowymi, które zaszły po 1989 r., nastąpił okres tworzenia służb specjalnych, które miały realizować swoje zadania w warunkach

¹¹ Dz.U. 1952, nr 33, poz. 232.

¹² Dz.U. 1992, nr 84, poz. 426.

¹³ Dz.U. 1983, nr 38, poz. 172.

¹⁴ Dz.U. 1985, nr 38, poz. 181.

i w sposób odpowiadający standardowi demokratycznego państwa prawnego. Z punktu widzenia przedmiotu rozważań niniejszego rozdziału, koncentrującego się na problematyce tworzenia prawa wewnętrznego służb specjalnych, kluczowego znaczenia nabiera ustanowienie 6 kwietnia 1990 r. ustawy o Urzędzie Ochrony Państwa¹⁵, na mocy, której powołano rzeczoną służbę, rozwiązując Służbę Bezpieczeństwa i wprowadzając regulacje dotyczące statusu jej funkcjonariuszy. Co ważne, pierwotna wersja przedmiotowej ustawy nie obejmowała treścią delegacji upoważniających do kreowania aktów normatywnych w formie zarządzeń. Aktualność zachowuje w tym zakresie uzasadnienie poczynione wcześniej, którego sedno koncentruje się na obowiązującym wówczas katalogu konstytucyjnych źródeł prawa. Stosowne zmiany w tym zakresie, oddające zmiany konstytucyjne wprowadzone przez nową konstytucję, zostały wprowadzone dopiero ustawą z 6 lipca 2001 r.¹⁶ Jak wskazywano w jej uzasadnieniu, ustawa ta to *wyodrębniona merytorycznie część realizacji obowiązków w zakresie dostosowaniu aktów normatywnych organów administracji rządowej do Konstytucji Rzeczypospolitej Polskiej stanowiący wykonanie obowiązku nałożonego na Radę Ministrów przepisem art. 241 ust. 6 Konstytucji RP*¹⁷.

W tym kontekście wskazać należy, iż na mocy art. 241 ust. 6 Konstytucji RP Rada Ministrów została zobowiązana do ustalenia, w okresie dwóch lat od dnia wejścia w życie Konstytucji RP, które z uchwał Rady Ministrów oraz zarządzeń ministrów lub innych organów administracji rządowej, podjęte lub wydane przed dniem wejścia w życie Konstytucji, wymagają — stosownie do warunków określonych w art. 87 ust. 1 i art. 92 Konstytucji — zastąpienia ich przez rozporządzenia wydane na podstawie upoważnienia ustawy, której projekt w odpowiednim czasie Rada Ministrów przedstawi Sejmowi. W tym samym okresie Rada Ministrów przedstawić miała Sejmowi projekt ustawy określającej, które akty normatywne organów administracji rządowej, wydane przed dniem wejścia w życie Konstytucji, stają się uchwałami albo zarządzeniami w rozumieniu art. 93 Konstytucji. Jak wskazywano dalej w przytoczonym uzasadnieniu:

¹⁵ Tekst pierwotny ogłoszony w Dz.U. 1990 r., nr 30, poz. 180.

¹⁶ *Ustawa z dnia 6 lipca 2001 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, ustawy o odszkodowaniach przysługujących w razie wypadków i chorób pozostających w związku ze służbą w Milicji Obywatelskiej, ustawy o zaopatrzeniu inwalidów wojennych i wojskowych oraz ich rodzin, ustawy o uposażeniu żołnierzy, ustawy o Policji, ustawy o Urzędzie Ochrony Państwa, ustawy o Państwowej Straży Pożarnej, ustawy o kontroli skarbowej, ustawy o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin, ustawy o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Urzędu Ochrony Państwa, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej i Służby Więziennej oraz ich rodzin, ustawy o zakwaterowaniu Sił Zbrojnych Rzeczypospolitej Polskiej, ustawy o Służbie Więziennej oraz ustawy o Inspekcji Celnej* (Dz.U 2001, nr 81, poz. 877).

¹⁷ Uzasadnienie do druku nr 1397 [online]. Protokół dostępu: [https://orka.sejm.gov.pl/RejestrDrukow/wgdruku/1397/\\$file/1397.pdf](https://orka.sejm.gov.pl/RejestrDrukow/wgdruku/1397/$file/1397.pdf), [dostęp: 18 VIII 2021].

realizując tak wyznaczony zakres zadań, organy administracji rządowej dokonały przeglądu uchwał i rozporządzeń Rady Ministrów oraz rozporządzeń i zarządzeń Prezesa Rady Ministrów, ministrów i innych organów administracji rządowej, podjętych lub wydanych przed dniem 17 października 1997 r. w zakresie służb mundurowych. W toku tych prac przygotowawczych dokonano przeglądu wszystkich obowiązujących aktów normatywnych, były wśród nich zarówno akty normatywne publikowane, jak i niepublikowane. W wyniku przeprowadzenia tego przeglądu wydzielono akty normatywne zawierające normy o charakterze powszechnie obowiązującym w rozumieniu art. 87 Konstytucji oraz akty zawierające normy o charakterze wewnętrznym w rozumieniu art. 93 Konstytucji. Były wśród nich także akty o charakterze mieszanym, tj. zawierające zarówno normy powszechnie obowiązujące, jak i o charakterze wewnętrznym oraz akty o charakterze konkretno-indywidualnym wydane lub uchwalone w formie zarządzenia lub uchwały. Akty prawne tego rodzaju ze względu na ich nienormatywny charakter nie są objęte regulacją niniejszego projektu ustawy. (...) Jeżeli akt prawny wydany został na podstawie upoważnienia ustawowego, przez organ właściwy do wydawania danego rodzaju aktu oraz w formie prawnej wskazanej w Konstytucji, to pozostaje on w obiegu prawnym bez konieczności dokonywania zmian w podstawie prawnej do jego wydania, ponieważ Konstytucja RP nie nakłada takiego obowiązku oraz nie określa skutku w postaci uchylecia takiego aktu, mimo że upoważnienie ustawowe nie zawiera wytycznych. W tej grupie aktów normatywnych znalazły się zarówno akty normatywne o charakterze powszechnie obowiązującym w rozumieniu art. 87 Konstytucji, jak również akty normatywne o charakterze wewnętrznym — uchwały Rady Ministrów oraz zarządzenia ministrów, które spełniają wymagania sformułowane w art. 93 ust. 1 i 3 Konstytucji. (...) W projekcie zaproponowano brzmienie upoważnień ustawowych do wydania aktów normatywnych, których materia regulowana była dotychczas przez akty prawne wadliwe konstytucyjnie w zakresie formy prawnej. W celu zastąpienia aktów, które zawierają normy powszechnie obowiązujące (a nie są rozporządzeniami), co zgodnie z systemem źródeł prawa wymaga formy rozporządzenia, projekt proponuje wprowadzenie upoważnień ustawowych do ich wydania. W ten sposób projekt ustawy umożliwi wydanie stosownych rozporządzeń. (...) W przypadku ustalenia, że akt normatywny skierowany jest jedynie do organów podległych organowi stanowiącemu ten akt i zawiera normy o charakterze wewnętrznym, a nie ma formy uchwały lub zarządzenia albo gdy obowiązujące zarządzenie lub uchwała nie zostały wydane na podstawie ustawy, zaproponowano w projekcie brzmienie upoważnień ustawowych do wydania odpowiednio — uchwał Rady Ministrów lub zarządzeń ministra lub kierownika urzędu centralnego. Zgodnie bowiem z dyspozycją art. 241 ust. 6 uchwały i zarządzenia mają odpowiadać wymogom art. 93 Konstytucji. Te zaś mają być wydane na podstawie ustawy. (...) Projektodawcy przyjmują więc, że przekształcenie aktów normatywnych organów administracji rządowej w uchwały i zarządzenia w rozumieniu art. 93 Konstytucji (art. 241 ust. 6 zdanie drugie) nastąpi poprzez zmianę lub sformułowanie brakujących upoważnień

ustawowych do wydawania tych aktów. Taki sposób postępowania wynika z art. 93 Konstytucji, tj. z konieczności zapewnienia ustawowej podstawy obowiązywania tych aktów, a przez to stwarza możliwość dokonywania w nich zmian lub ich zastępowania oraz publikowania. Nie jest to więc rozwiązanie doraźne, jednorazowe, a dające trwałe podstawy (mechanizm) obecności tych aktów w systemie źródeł prawa. Wydane na podstawie tych upoważnień uchwały albo zarządzenia zastąpią obowiązujące akty prawne niespełniające wymogów określonych w Konstytucji¹⁸.

Warto zwrócić uwagę, iż projektodawca rządowy zdawał sobie sprawę z trudności kwalifikacji poszczególnych norm prawnych według podziału na obowiązujące powszechnie i wewnątrz, wskazując w cytowanym uzasadnieniu, iż ich rozróżnienie *może w niektórych przypadkach rodzić pewne kontrowersje i spory. Jest to bowiem rozróżnienie wprowadzone dopiero przez obecną Konstytucję, nie mogła więc wykształcić się odpowiednia praktyka. Dopiero — jak można sądzić — orzecznictwo Trybunału Konstytucyjnego, sądów oraz dorobek doktryny pozwoli na wyostrenie granic pomiędzy tymi rodzajami norm*¹⁹.

Na mocy przedmiotowej ustawy wprowadzono do ustawy o Urzędzie Ochrony Państwa 43 nowe delegacje ustawowe do wydania rozporządzeń oraz dziewięć delegacji do kreacji aktów prawa wewnętrznego w formie zarządzenia, różnicujące się adresatem delegacji, w dwóch przypadkach wskazując Prezesa Rady Ministrów, zaś w siedmiu Szefa Urzędu Ochrony Państwa. W ten sposób ustawodawca upoważnił do określenia, w drodze zarządzenia, przez:

1. Prezesa Rady Ministrów:
 - 1) szczegółowych zadań Szefa Urzędu Ochrony Państwa (art. 3 ust. 2 ustawy o UOP);
 - 2) stanowisk służbowych i stopni etatowych stanowiących tajemnicę państwową, uwzględniając zaszerogowanie tych stanowisk do grup uposażenia i przypisanych im stopni etatowych (art. 88 ust. 2 ustawy o UOP);
2. Szefa Urzędu Ochrony Państwa:
 - 1) regulaminu organizacyjnego Urzędu Ochrony Państwa oraz regulaminów jednostek organizacyjnych, uwzględniając ich strukturę wewnętrzną i szczególne zadania (art. 3 ust. 4 ustawy o UOP),
 - 2) tworzenia zespołów o charakterze stałym lub doraźnym, określając ich nazwę, skład osobowy oraz szczegółowy zakres i tryb działania (art. 3 ust. 5 ustawy o UOP),
 - 3) tworzenia, przekształcania i likwidacji ośrodków szkolenia, określając ich strukturę, zadania i szczególne zasady funkcjonowania (art. 3 ust. 6 ustawy o UOP),
 - 4) powoływania kolegialnych organów doradczych i opiniodawczych, określając ich nazwę, skład osobowy oraz szczegółowy zakres i tryb działania (art. 5a ust. 3 ustawy o UOP),

¹⁸ Tamże.

¹⁹ Tamże.

- 5) sposobu i trybu wykonywania wewnętrznej kontroli w Urzędzie Ochrony Państwa, a w szczególności jednostki właściwe do prowadzenia i dokumentowania kontroli (art. 5a ust. 4 ustawy o UOP),
- 6) powoływania komisji egzaminacyjnych, w ramach szkoleń korpusowych, określając ich skład osobowy, a także ustalania terminów egzaminów, wzoru zaświadczenia o zdaniu egzaminu oraz sposobu wynagradzania członków komisji (art. 38a ust. 2 ustawy o UOP),
- 7) wysokości funduszu na nagrody i zapomogi, z jednoczesnym ustaleniem wysokości środków finansowych przeznaczonych na nagrody roczne, nagrody uznaniowe i zapomogi (art. 97 ust. 3 ustawy o UOP).

Wprowadzony analizowaną ustawą dostosowującą model konstrukcyjny delegacji, upoważniających do kreacji aktów prawa wewnętrznego w służbach specjalnych, opierający się z jednej strony na dość wyraźnie zarysowanym zakresie przedmiotowym — różnicującym się wobec zakresu przedmiotowego aktów prawa powszechnie obowiązującego w postaci rozporządzeń, oraz swoicie dualistycznym zakresie podmiotowym — upoważniającym z jednej strony organ nadzoru lub z drugiej szefa służby, stał się wzorcowy dla późniejszych rozwiązań przyjmowanych w przepisach ustrojowych i pragmatycznych służb specjalnych. Pierwsza z kolejnych takich ustaw, tj. *ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych*²⁰, zawierała w ramach objętych nią przepisów ustrojowych i pragmatycznych poświęconych tej służbie 11 delegacji do wydania rozporządzeń oraz 18 delegacji do wydania aktów prawa wewnętrznego, w tym: jedną adresowaną do Prezesa Rady Ministrów i 10 adresowanych do Ministra Obrony Narodowej.

Aktualne podstawy kreacji prawa wewnętrznego służb specjalnych

Opisany powyżej model konstrukcyjny aktów prawa wewnętrznego został adoptowany z ustaw o UOP i WSI do aktualnie obowiązujących aktów prawnych regulujących ustrój i pragmatykę służb specjalnych, tj. do ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego i do ustawy o Centralnym Biurze Antykorupcyjnym. Wymienione akty ustawowe zawierają upoważnienia do kreowania aktów prawa wewnętrznego w zakresie podmiotowym i przedmiotowym, upoważniającym do kreacji przez:

1. Prezesa Rady Ministrów (służby cywilne) / Ministra Obrony Narodowej (służby wojskowe):
 - 1) statutu, który określa organizację wewnętrzną służby (art. 20 ust. 1 ustawy o ABW oraz AW; art. 21 ust. 1 ustawy o SKW oraz SWW — po uzyskaniu zgody Prezesa Rady Ministrów; art. 11 ust. 1 ustawy o CBA);
 - 2) (niepodlegające ogłoszeniu) sposobu i trybu realizacji przez szefów obowiązków w zakresie przekazywania uzyskanych informacji innym właściwym organom, służbom lub instytucjom, z uwzględnieniem

²⁰ Tekst pierwotny ogłoszony w Dz.U. 2003, nr 139, poz. 1326.

przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (art. 22a ust. 9 ustawy o ABW oraz AW; art. 27 ust. 9 ustawy o SKW oraz SWW — za zgodą Prezesa Rady Ministrów);

- 3) (z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych) sposobu współdziałania właściwych organów, służb i instytucji państwowych z Szefem ABW przy prowadzeniu rejestru sporządzonych i wydanych dokumentów uniemożliwiających ustalenie danych identyfikujących funkcjonariuszy i pracowników tych organów, służb lub instytucji oraz osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych oraz środków, którymi posługują się przy wykonywaniu zadań służbowych (art. 35 ust. 7 ustawy o ABW oraz AW);
 - 4) (z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych) sposobu współdziałania służb specjalnych z Szefem ABW w zakresie prowadzenia centralnej ewidencje zainteresowań operacyjnych służb specjalnych (40 ust. 3 ustawy o ABW oraz AW);
 - 5) zakresu i trybu współdziałania oraz szczegółowego rozdziału kompetencji pomiędzy ABW, AW, SKW, SWW i CBA (art. 42 ust. 2 ustawy o ABW oraz AW);
 - 6) (uwzględniając wymogi dotyczące ochrony informacji niejawnych) warunków, zakresu i trybu: współdziałania szefów CBA, ABW, SKW oraz Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej i Szefa Krajowej Administracji Skarbowej w zakresie zwalczania korupcji w instytucjach państwowych i samorządzie terytorialnym oraz życiu publicznym i gospodarczym, a także działalności godzącej w interesy ekonomiczne państwa; koordynacji działań o charakterze operacyjno-rozpoznawczym i informacyjno-analitycznym podejmowanych przez wskazane organy, mogące mieć wpływ na realizację zadań CBA określonych w art. 2 ust. 1 i 2 ustawy o CBA — mając na uwadze zapewnienie sprawności i skuteczności tych postępowań (art. 29 ust. 3 ustawy o CBA).
2. Ministra Obrony Narodowej (służby wojskowe):
- 1) (niepodlegające ogłoszeniu) form i trybu współdziałania SKW i SWW (art. 8 ustawy o SKW oraz SWW);
 - 2) (niepodlegające ogłoszeniu) zakresu i trybu współdziałania SKW i SWW ze Sztabem Generalnym Wojska Polskiego i innymi komórkami organizacyjnymi Ministerstwa Obrony Narodowej oraz Dowódcą Generalnym Rodzajów Sił Zbrojnych, Dowódcą Operacyjnym Rodzajów Sił Zbrojnych, Dowódcą Wojsk Obrony Terytorialnej, Szefem Inspektoratu Wsparcia Sił Zbrojnych, dowódcami garnizonów wojskowych i jednostek wojskowych (art. 10 ust. 2 ustawy o SKW oraz SWW);
 - 3) (niepodlegające ogłoszeniu) sposobu i trybu tworzenia zespołów zadaniowych, o których mowa w ust. 1a, oraz wyznaczania żołnierzy pełniących służbę w oddziałach lub pododdziałach SZ RP do składu takich zespołów (art. 10 ust. 3 ustawy o SKW oraz SWW);

- 4) (niepodlegające ogłoszeniu) z ministrem właściwym do spraw zagranicznych, form i trybu współdziałania SKW i SWW z organami, służbami i instytucjami podległymi ministrowi właściwemu do spraw zagranicznych, uwzględniając właściwość tych organów, służb i instytucji (art. 10 ust. 4 ustawy o SKW oraz SWW);
 - 5) trybu i sposobu powoływania jednostek organizacyjnych SKW i SWW, wchodzących w skład jednostek wojskowych SZ RP realizujących zadania za granicą, uwzględniając konieczność zapewnienia bezpieczeństwa i zdolności bojowej tych jednostek oraz przepisy regulujące funkcjonowanie jednostek Sił Zbrojnych (art. 22 ust. 4 ustawy o SKW oraz SWW);
 - 6) szczegółowego ceremoniału składania przysięgi (art. 6 ust. 2 ustawy o służbie SKW oraz SWW).
3. Szefa danej służby:
- 1) (stanowiące informacje niejawne) szczegółowych zasad tworzenia funduszu operacyjnego i gospodarowania tym funduszem (art. 9 ust. 4 ustawy o ABW oraz AW; art. 11 ustawy o SKW oraz SWW; art. 4 ust. 3 ustawy o CBA);
 - 2) regulaminów organizacyjnych jednostek organizacyjnych służb, w których określają jej strukturę wewnętrzną i szczegółowe zadania (art. 20 ust. 2 ustawy o ABW oraz AW; art. 21 ust. 1 ustawy o SKW oraz SWW — po uzyskaniu zgody Ministra Obrony Narodowej; art. 4 ust. 2 ustawy o CBA);
 - 3) upoważnienia do tworzenia, przekształcania i likwidowania ośrodków szkolenia służb, określając ich strukturę, zadania oraz zasady funkcjonowania w zakresie nieobjętym innymi przepisami (art. 20 ust. 3 ustawy o ABW oraz AW; art. 21 ust. 4 ustawy o SKW oraz SWW);
 - 4) form i trybu szkolenia funkcjonariuszy (art. 11 ust. 3 ustawy o CBA);
 - 5) rodzaju dokonywanych przez ABW w ramach oceny bezpieczeństwa testów bezpieczeństwa, uwzględniając potrzebę kompletności dokonywanej oceny bezpieczeństwa (art. 32a ustawy o ABW oraz AW);
 - 6) (z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych) szczegółowego trybu wydawania i przechowywania dokumentów, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza lub osób udzielających pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych, oraz posługiwania się tymi dokumentami (art. 35 ust. 8 ustawy o ABW oraz AW; art. 39 ust. 7 ustawy o SKW oraz SWW; art. 24 ust. 5 ustawy o CBA);
 - 7) (z zachowaniem wymogów dotyczących ochrony informacji niejawnych) sposobu prowadzenia przez ABW centralnego rejestru dokumentów, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza lub osób udzielających pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych (art. 35 ust. 9 ustawy o ABW oraz AW);
 - 8) obiegu informacji, w tym niejawnych, w podległych służbach (art. 38 ustawy o ABW oraz AW; art. 27 ustawy o CBA);
 - 9) znaków lub innych dokumentów identyfikacyjnych funkcjonariuszy (art. 48 ust. 6 ustawy o ABW oraz AW — fakultatywne; art. 52 ust. 4 ustawy o CBA — obligatoryjne);

- 10) sposobu organizacji służby i jej pełnienia w systemie skoszarowanym, z uwzględnieniem czasu pełnienia tej służby oraz porządku dnia (art. 70 ust 2 ustawy o ABW oraz AW — fakultatywne; art. 29 ust. 2 ustawy o służbie SKW oraz SWW — obligatoryjnie);
- 11) upoważnienia do powoływania komisji egzaminacyjnych na pierwszy stopień w korpusie chorążych lub oficerów, określając ich skład osobowy, a także ustalając terminy egzaminów i określając wzór zaświadczenia o zdaniu egzaminu oraz wysokość wynagrodzenia członków komisji (art. 71 ust. 2 ustawy o ABW oraz AW; art. 30 ust. 2 ustawy o służbie SKW oraz SWW);
- 12) ceremoniału składania przysięgi (art. 21 ust. 2 ustawy o CBA);
- 13) przypadków, w których uzyskanie zezwolenia lub wykonanie obowiązku poinformowania o wyjeździe za granicę dzieci pozostających na jego utrzymaniu albo współmałżonka nie jest wymagane, a także obowiązków funkcjonariusza wyjeżdżającego za granicę i powracającego z zagranicy (art. 82 ust. 3 ustawy o ABW oraz AW; art. 41 ust. 3 ustawy o służbie SKW oraz SWW; art. 74 ust. 3 ustawy o CBA);
- 14) wykazu państw, których terytoria w całości lub w części zostały uznane za strefę działań wojennych na podstawie odrębnych przepisów, lub państwa, na których terytoriach występują warunki stwarzające bezpośrednie zagrożenie dla życia lub zdrowia, z zachowaniem wymogów dotyczących ochrony informacji niejawnych (art. 85a ust. 2 ustawy o ABW oraz AW; art. 44a ustawy o służbie SKW oraz SWW);
- 15) norm wyposażenia i uzbrojenia oraz szczegółowych zasad dostępu do wyposażenia i uzbrojenia, jego przyznawania i użytkowania (art. 78 ust. 2 ustawy o CBA; w ABW, AW, SKW i SWW — rozporządzenie);
- 16) upoważnienia do ustanawiania, odznaki i oznak noszonych na mundurze (art. 87 ust. 3 ustawy o ABW oraz AW — fakultatywne; art. 46 ust. 3 ustawy o służbie SKW oraz SWW — fakultatywne);
- 17) trybu przydzielania lokalu mieszkalnego w nowym miejscu pełnienia służby, szczegółowych zasad zwracania udzielonej pomocy finansowej oraz zasad zwalniania zajmowanych lokali mieszkalnych lub domów w nowym miejscu pełnienia służby (art. 110 ust. 3 ustawy o ABW oraz AW; art. 70 ust. 3 ustawy o służbie SKW oraz SWW);
- 18) (stanowiące informacje niejawne) stanowisk służbowych i stopni etatowych, zaszeregowania tych stanowisk do grup uposażenia i przypisanych im stopni etatowych (art. 116 ust. 3 ustawy o ABW oraz AW; art. 76 ust. 4 ustawy o służbie SKW oraz SWW);
- 19) dodatków o charakterze stałym płatnych z dołu (art. 120 ABW oraz AW — fakultatywne; art. 80 ustawy o służbie SKW oraz SWW — fakultatywne);
- 20) wysokości funduszu na nagrody i zapomogi, ustalając jednocześnie wysokość środków finansowych przeznaczonych na nagrody roczne, uznaniowe i zapomogi oraz warunki zwiększania wysokości funduszu na nagrody uznaniowe i zapomogi (art. 125 ust. 3 ustawy o ABW oraz

AW; art. 85 ust. 3 ustawy o służbie SKW oraz SWW; art. 93 ust. 4 ustawy o CBA);

- 21) (z zachowaniem przepisów o ochronie informacji niejawnych) sposobu stwierdzania przebywania na zwolnieniu lekarskim funkcjonariusza w przypadkach uzasadnionych charakterem, miejscem, sposobem lub rodzajem zadań służbowych przez nich wykonywanych (art. 136c ust. 3 ustawy o ABW oraz AW; art. 96c ust. 3 ustawy o służbie SKW oraz SWW; art. 102c ust. 2 ustawy o CBA).

Wszystkie opisane powyżej upoważnienia do kreacji prawa wewnętrznego należy uznać za upoważnienia o charakterze szczególnym (konkretnym), wskazującym bezsporny zakres spraw przekazanych do uregulowania w danym akcie. Jak wskazano w punkcie drugim niniejszego rozdziału, kreacja prawa wewnętrznego może mieć i przeważnie ma oparcie wyłącznie w normie kompetencyjnej danego organu konstrukcyjnie tworzącej element stosunku hierarchicznego podporządkowania. W tym zakresie normę taką uznać należy za podstawę ogólną do kreacji aktów prawa wewnętrznego, z wyłączeniem zakresów merytorycznych delegowanych do uregulowania w opisanych powyżej upoważnieniach szczegółowych. Do podstaw takich w przypadku służb specjalnych należą:

- 1) art. 19 ust. 3 ustawy o ABW oraz AW, zgodnie z którym szefowie obu Agencji, każdy w zakresie swojej właściwości, w drodze zarządzeń, określają sposoby, metody i formy wykonywania zadań w Agencji w zakresie nieobjętym innymi przepisami;
- 2) art. 20 ust. 3 ustawy o SKW oraz SWW, zgodnie z którym szefowie SKW i SWW, każdy w zakresie swojej właściwości, w drodze zarządzeń niepodlegających ogłoszeniu, określają sposoby, metody i formy wykonywania zadań w służbach w zakresie nieobjętym innymi przepisami;
- 3) art. 10 ust. 3 ustawy o CBA, zgodnie z którym Szef CBA, w drodze zarządzenia, określa sposoby, metody i formy wykonywania zadań przez CBA.

Aspekty proceduralne tworzenia prawa wewnętrznego w służbach specjalnych

Analizując zagadnienie wymogów proceduralnych tworzenia prawa wewnętrznego służb specjalnych, wskazać należy na zasadnicze elementy tego zagadnienia. Po pierwsze konstrukcyjnie, co wydaje się oczywiste, procedura tworzenia tego prawa nakierowana powinna być na zagwarantowanie opisanych w punkcie drugim niniejszego rozdziału wymogów materialnych założonych przez Konstytucję. Na tym tle, dokonując analizy obowiązującego systemu prawnego, wyraźnie zarysowuje się dualistyczne zróżnicowanie tej procedury, zdeterminowane rodzajem podmiotu upoważnionego przez delegację ustawową do jego kreacji. Klarownie bowiem da się zauważyć szczegółowo doprecyzowana procedura tworzenia zarządzeń Prezesa Rady Ministrów i jednocześnie daleko niedoprecyzowane proceduralnie zasady tworzenia prawa wewnętrznego w formie zarządzeń szefa danej służby.

Zgodnie z § 19 Reg. RM²¹ projekty zarządzeń Prezesa Rady Ministrów są elementem konstrukcyjnym definicji projektu dokumentu rządowego, a przez to zostały włączone w procedurę określoną Dziełem III tego aktu prawnego, tj. postępowanie z projektami dokumentów rządowych, na którą składa się sformalizowany tryb i zasady opracowania, prowadzenia procesu uzgodnień, konsultacji publicznych lub opiniowania oraz wnoszenia do rozpatrzenia takiego projektu²². Co istotne, w ramach tej procedury projekt takiego zarządzenia podlega obligatoryjnym uzgodnieniom pod względem prawnym z Rządowym Centrum Legislacji, które opracowuje wobec niego stanowisko prawno-legislacyjne. Wskazany powyżej, dalece sformalizowany tryb procedury legislacyjnej projektów zarządzeń Prezesa Rady Ministrów, nakierowany jest w szczególności na weryfikację realizacji wyznaczonych konstytucją standardów stawianych tym aktem.

Kierując się w stronę wojskowych służb specjalnych, wskazać należy, iż procedury legislacyjne kreacji zarządzeń Ministra Obrony Narodowej określone zostały na poziomie kierowanego przez niego resortu w decyzji Nr 5/MON Ministra Obrony Narodowej z dnia 29 stycznia 2018 r. w sprawie opracowywania, uzgadniania, wydawania i ogłaszania aktów normatywnych oraz innych dokumentów w resorcie obrony narodowej²³. Jak wskazano w § 1 tej decyzji, określa ona sposób i tryb opracowywania, uzgadniania, wydawania i ogłaszania aktów normatywnych z zakresu właściwości Ministra Obrony Narodowej, w tym też zarządzeń tego ministra dotyczących funkcjonowania służb specjalnych w sprawach wymienionych w punkcie czwartym niniejszego rozdziału. Decyzja nie znajduje jednak zastosowania do aktów prawa wewnętrznego, kreowanego przez szefów służb wojskowych. Co prawda, w słowniczku zawartym w § 2 tej decyzji, definiując pojęcie jednostki organizacyjnej, wskazano, iż obejmuje ono jednostkę organizacyjną podległą ministrowi lub przez niego nadzorowaną, właściwą merytorycznie dla danej sprawy, oraz Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego, jednakże dalsze postanowienia tego aktu prawnego odnoszą się do tej jednostki jako podmiotu istotnego dla procedury kreacji aktów prawa wewnętrznego Ministra Obrony Narodowej, w tym jego zarządzeń, ale nie zarządzeń kreowanych przez podległych mu szefów służb. W ten sposób dojść można do wniosku o braku przyjęcia na potrzeby wojskowych służb specjalnych szczegółowych rozwiązań proceduralnych — ujętych w formę aktu prawnego, mającego za przedmiot kreację prawa wewnętrznego w tych służbach.

Na tym tle spośród cywilnych służb specjalnych zarówno Centralne Biuro Antykorupcyjne (od 2013), jak i Agencja Bezpieczeństwa Wewnętrznego (od 2015), posiadają akty normatywne przybierające postać swoistej samoregulacji ustanawiającej procedurę tworzenia prawa wewnętrznego.

²¹ M.P. 2016, poz. 1006.

²² Szczegółowe rozważania dotyczące przebiegu rządowego procesu legislacyjnego nie są przedmiotem niniejszego rozdziału.

²³ Dz.Urz. MON 2018, poz. 5 z późn. zm.

W Centralnym Biurze Antykorupcyjnym regulacje w tym zakresie zostały przyjęte zarządzeniem Nr 6/13 Szefa Centralnego Biura Antykorupcyjnego z dnia 4 kwietnia 2013 r. w sprawie metod i form wykonywania w Centralnym Biurze Antykorupcyjnym zadań w zakresie legislacji, wydawania pełnomocnictw i upoważnień oraz koordynacji pomocy prawnej²⁴, które obowiązywało do 6 maja 2021 r., kiedy to weszło w życie zarządzenie Nr 7/21 Szefa Centralnego Biura Antykorupcyjnego z dnia 30 kwietnia 2021 r. w sprawie zasad procedowania projektów aktów prawnych oraz wydawania pełnomocnictw i upoważnień²⁵. W słowniczku zawartym w § 2 tego zarządzenia oddzielono od siebie terminologicznie pojęcia: „projekt aktu normatywnego” (jako projekt zarządzenia Szefa CBA lub porozumienia zawieranego przez Szefa CBA, z wyjątkiem porozumień cywilnoprawnych), „projekt aktu wewnętrznego” (jako projekt decyzji Szefa CBA w sprawie innej niż rozstrzygnięcie w indywidualnej sprawie funkcjonariusza) oraz „projekt aktu zewnętrznego” (jako projekt ustawy, rozporządzenia, uchwały Rady Ministrów, zarządzenia Prezesa Rady Ministrów albo ministra, stanowiska rządu lub umowy międzynarodowej). Zgodnie z § 5 tego zarządzenia projekt aktu normatywnego opracowuje i uzgadnia właściwa merytorycznie jednostka albo zespół powołany w tym celu przez Szefa CBA, w skład którego wchodzi funkcjonariusz Biura Prawnego CBA. Jak wskazuje § 6 zarządzenia, opracowany projekt aktu normatywnego jest przekazywany kierownikom jednostek, których właściwości dotyczy projektowany akt normatywny oraz dyrektorowi Biura Prawnego CBA, w celu zasięgnięcia ich opinii. Jak wskazuje § 7 zarządzenia, jeżeli w trakcie uzgodnień nie dojdzie do ustalenia brzmienia projektu aktu normatywnego akceptowanego przez wszystkich zainteresowanych kierowników jednostek, sporządza się tabelę rozbieżności, zawierającą zestawienie zgłoszonych i nieuwzględnionych uwag wraz z ewentualnym stanowiskiem Biura Prawnego CBA, zaś w celu uzgodnienia ostatecznego brzmienia projektu aktu normatywnego można zwołać konferencję uzgodnieniową, w której będą uczestniczyć przedstawiciele jednostek zgłaszających uwagi do projektu. Brak uzgodnienia wymaga podjęcia ostatecznej decyzji przez Szefa CBA. Projekt aktu normatywnego w ostatecznym brzmieniu jest przekazywany, w celu akceptacji, kierownikom jednostek, w których ten został opracowany i których zadań dotyczy, oraz podlega zatwierdzeniu pod względem prawnym, legislacyjnym i redakcyjnym przez dyrektora Biura Prawnego CBA lub naczelnika Wydziału Prawno-Legislacyjnego w Biurze Prawnym CBA. Akt normatywny po podpisaniu podlega rejestracji w Biurze Prawnym CBA, odpowiednio w prowadzonym w wersji elektronicznej rejestrze jawnych lub niejawnych aktów normatywnych i wewnętrznych.

W Agencji Bezpieczeństwa Wewnętrznego regulacje ustanawiające procedury legislacyjne zostały przyjęte zarządzeniem nr 38 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 14 października 2015 r. w sprawie procedury legislacyjnej

²⁴ Dz.Urz. CBA 2013, poz. 6 z późn. zm.

²⁵ Dz.Urz. CBA 2021, poz. 7.

w *Agencji Bezpieczeństwa Wewnętrznego*²⁶, które obowiązywało do 10 lutego 2019 r., kiedy to weszło w życie zarządzenie nr 11 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 5 lutego 2019 r. w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego²⁷. Zgodnie z § 1 tego zarządzenia określa ono sposób i tryb m.in. opracowywania założeń, projektowania, uzgadniania i wydawania aktów prawnych Szefa ABW związanych z organizacją i funkcjonowaniem ABW, w tym aktów normatywnych i porozumień, których stroną jest Szef ABW. W kolejnych jednostkach redakcyjnych starano się, podobnie jak w przypadku zarządzenia CBA, wprowadzić porządek znaczeniowy kluczowych dla regulacji pojęć, różnicując w tym wypadku znaczenie pojęcia: „akt prawny Szefa ABW”, „akt normatywny Szefa ABW” oraz „akt indywidualny Szefa ABW”. W tym zakresie w słowniczku objętym § 2 zdefiniowano w pkt 3 pojęcie „aktu prawnego Szefa ABW” jako prawną formę działania Szefa ABW (element materialny), w szczególności zarządzenie, decyzja, wytyczne, obwieszczenie i porozumienie (element formalny). Jednocześnie w pkt 1 § 2 zawarto definicję pojęcia „akt normatywny Szefa ABW”, jako aktu prawnego Szefa ABW ustanawiającego normy prawne o charakterze generalnym i abstrakcyjnym (element materialny), w szczególności zarządzenie (element formalny), systemowo powiązane z aktami prawnymi powszechnie obowiązującymi (element materialny). Jak się wydaje, podstawowym celem tak sformułowanych definicji było czytelne oddzielenie od siebie aktów prawnych będących aktami normatywnymi, które dają podstawę do konstruowania norm prawnych, cechujących się generalnością i abstrakcyjnością (determinując jednocześnie ich formę prawną jako zarządzeń), których warunkiem obowiązywania jest ich ogłoszenie we właściwym dzienniku urzędowym, od aktów prawnych Szefa nieposiadających tych cech. Wprowadzone definicje miały zwrócić uwagę na istnienie aktów prawnych (niebędących aktami normatywnymi), które charakteryzują się tzw. mieszanym typem normowania. Ponadto Szef ABW w swoim zarządzeniu wyraźnie wskazał przez przepis § 1a, iż nie znajduje ono zastosowania do aktów prawnych będących wynikiem procesu stosowania prawa, tj.:

- 1) aktów indywidualnych stosowania prawa administracyjnego, wydawanych w związku z realizacją zadań przez właściwe jednostki organizacyjne ABW, w szczególności decyzji administracyjnych, postanowień, zaświadczeń i zezwoleń oraz innych rozstrzygnięć wydawanych w trybie Kodeksu postępowania administracyjnego i innych ustaw, a także upoważnień o charakterze administracyjnym;
- 2) aktów indywidualnych stosowania prawa cywilnego, w szczególności umów i pełnomocnictw;
- 3) aktów Szefa ABW wydawanych w ramach wykonywanych przez funkcjonariuszy ABW czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych albo analityczno-informacyjnych, w tym wydawanych w związku z ich realizacją upoważnień.

²⁶ Dz. Urz. ABW 2015, poz. 24.

²⁷ Dz. Urz. ABW 2021, poz. 4.

Szczegółowe postanowienia dotyczące procedury kreacji aktów prawnych Szefa ABW, związanych z organizacją i funkcjonowaniem ABW, zostały zawarte w rozdziale piątym analizowanego zarządzenia.

Zgodnie z § 20 tego zarządzenia jednostka merytoryczna (czyli jednostka organizacyjna ABW właściwa regulaminowo w zakresie spraw, które są lub mają być przedmiotem uregulowania w akcie prawnym Szefa ABW) dokonuje bieżącego przeglądu tych aktów i niezwłocznie informuje Biuro Prawne ABW o potrzebie wydania lub dokonania nowelizacji tych aktów, opracowując wstępny projekt aktu prawnego Szefa ABW wraz z uzasadnieniem. Co istotne, w załączniku nr 2 do zarządzenia określono wzór graficznej formy aktu prawnego Szefa ABW, w tym układ jego przepisów.

Następnie, na podstawie treści § 21 tego zarządzenia, jednostka merytoryczna uzgadnia wewnętrznie wstępny projekt aktu prawnego Szefa ABW z innymi jednostkami organizacyjnymi ABW, właściwymi w sprawach objętych przedmiotem tego projektu, zaś projekt, który będzie powodować skutki finansowe lub kadrowe podlega uzgodnieniu odpowiednio z Biurem Finansów ABW i Biurem Kadr ABW. Po zakończeniu uzgodnień wewnętrznych jednostka merytoryczna sporządza nową wersję projektu aktu prawnego Szefa ABW, uwzględniającego uwagi zgłoszone do tego projektu, który po ostatecznym uzgodnieniu jest przesyłany do Biura Prawnego ABW celem dokonania ostatecznej oceny pod względem prawnym, legislacyjnym i redakcyjnym. Po zakończeniu tej procedury wersja elektroniczna projektu jest formatowana w Biurze Prawnym ABW zgodnie z szablonem projektu aktu prawnego dostępnym na stronie podmiotowej Biuletynu Informacji Publicznej Kancelarii Prezesa Rady Ministrów, i w tej postaci podlega akceptacji pod względem merytorycznym:

- 1) w przypadku aktów prawnych Szefa ABW niezawierających informacji niejawnych, imienną pieczętką i podpisem na odwrocie ostatniej strony roboczego wydruku tego projektu;
- 2) w przypadku aktów prawnych Szefa ABW zawierających informacje niejawne, imienną pieczętką i podpisem na odwrocie ostatniej strony dokumentu papierowego, który ma być przedłożony do podpisu Szefa ABW.

Po akceptacji merytorycznej dyrektor albo zastępca dyrektora Biura Prawnego ABW oraz naczelnik albo zastępca naczelnika Wydziału I Biura Prawnego ABW potwierdzają zgodność projektu pod względem prawnym, legislacyjnym i redakcyjnym:

- 1) w przypadku aktów prawnych Szefa ABW niezawierających informacji niejawnych, nanosząc klauzulę „za zgodność pod względem prawnym i redakcyjnym”, opatrzoną imienną pieczętką i podpisem na odwrocie ostatniej strony roboczego wydruku tego projektu;
- 2) w przypadku aktów prawnych Szefa ABW zawierających informacje niejawne, nanosząc klauzulę „za zgodność pod względem prawnym i redakcyjnym” opatrzoną imienną pieczętką i podpisem na odwrocie ostatniej strony dokumentu papierowego, który ma być przedłożony do podpisu Szefa ABW.

Co ważne, dokonywanie zmian w projekcie aktu prawnego Szefa ABW zaakceptowanego w sposób, o którym mowa w ust. 1 i 2, jest niedopuszczalne.

Zgodnie z § 26 tego zarządzenia akty prawne Szefa ABW niezawierające informacji niejawnych sporządza się w postaci dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym Szefa ABW, co realizuje obowiązek wynikający z art. 2a ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, zakładający, iż akty normatywne i inne akty prawne podlegające ogłoszeniu ogłasza się w formie dokumentu elektronicznego w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne²⁸, chyba że ustawa stanowi inaczej. Z kolei akty prawne Szefa ABW zawierające informacje niejawne sporządza się w postaci dokumentu papierowego, co jest bezpośrednim następstwem wymogów wynikających z zasad ochrony informacji niejawnych.

Wszystkie akty prawne Szefa ABW podlegają rejestracji w Rejestrze Przepisów Szefa ABW, prowadzonym przez Biuro Prawne ABW, w którym przechowuje się też oryginały aktów prawnych Szefa ABW wytworzonych zarówno w postaci dokumentów elektronicznych (sporządzając ich kopie zapasowe, co najmniej raz w miesiącu) oraz w postaci dokumentów papierowych.

Problematyka ogłaszania prawa w służbach specjalnych

Zgodnie z art. 88 ust. 1 Konstytucji RP warunkiem wejścia w życie ustaw, rozporządzeń oraz aktów prawa miejscowego jest ich ogłoszenie. Jak wskazuje się w doktrynie, *ogłoszenie aktu normatywnego jest doniosłą prawnie czynnością konwencjonalną, która stanowi ostatni etap postępowania prawodawczego (...). W tym sensie ogłoszenie ma nie tylko znaczenie informacyjne, ale też należy je traktować jako odrębny etap szeroko pojętego trybu stanowienia krajowych aktów prawa powszechnie obowiązującego*²⁹. Na mocy art. 88 Konstytucji RP została więc ustanowiona bezwzględna zasada ogłaszania aktów normatywnych o charakterze powszechnie obowiązującym w oficjalnym dzienniku promulgacyjnym, czyniąc z faktu ogłoszenia niezbędny warunek wejścia w życie i obowiązywania tych aktów prawnych. Zasada konieczności ogłaszania prawa wpisuje się tym samym w standard wyznaczany zasadą demokratycznego państwa prawnego. Zwraca uwagę, iż samo ogłoszenie realizuje dwa dodatkowe swoiste postulaty, które można by określić jako *pro* i *contra* obywatel. Z jednej bowiem strony, przez ogłoszenie materializuje się postulat jawności prawa i jego dostępności dla obywatela, z drugiej jednak strony akt normatywny poddany promulgacji wiąże

²⁸ Dz.U. 2021, poz. 670.

²⁹ P. Radziejewicz, zob. *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziejewicz, wyd. 2, Warszawa 2019, LEX/el. 2021, art. 88 [online]. Protokół dostępu: <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587806682/650745/tuleja-piotr-red-konstytucja-rzeczypospolitej-polskiej-komentarz-wyd-ii?cm=URELATIONS>, [dostęp: 4 VI 2021].

i wywołuje skutki prawne, co przekłada się na obowiązek przestrzegania norm prawnych z niego wynikających, wywołując brak możliwości zasłaniania się — zgodnie z łacińską *paremia ignorantia iuris nocet* — faktem jego nieznanomości przez obywatela.

Analizując dalej postanowienia Konstytucji RP, zwrócić należy uwagę, iż delegacją zawartą w jej art. 88 ust. 2 przekazano do uregulowania jako materię ustawową zasady i tryb ogłaszania aktów normatywnych. Ustawodawca zrealizował tę dyspozycję, która zawiera stosowne postanowienia w tym zakresie, jak również zasady i tryb wydawania dzienników urzędowych, przez urzędowe ogłaszanie aktów³⁰. Zwrócić należy uwagę, iż zasady i tryb ogłaszania umów międzynarodowych zostały określone w *ustawie z 14 kwietnia 2000 r. o umowach międzynarodowych*³¹, zaś zasady i tryb ogłaszania aktów normatywnych i niektórych aktów prawnych Unii Europejskiej oraz zasady i tryb wydawania „Dziennika Urzędowego Unii Europejskiej” określają przepisy Unii Europejskiej.

Punktem wyjścia do dalszych rozważań, istotnych z perspektywy tematu niniejszego rozdziału, skoncentrowanego na problematyce tworzenia prawa wewnętrznego w służbach specjalnych, staje się szczegółowa analiza wskazanej ustawy o ogłaszaniu aktów normatywnych i jej wpływu na ogłaszanie prawa wewnętrznego służb specjalnych. Zgodnie z jej art. 2 ogłoszenie aktu normatywnego w dzienniku urzędowym jest obowiązkowe, zaś odrębna ustawa może wyłączyć obowiązek ogłoszenia aktu normatywnego niezawierającego przepisów powszechnie obowiązujących. Zwraca uwagę fakt, iż przyjęte przez ustawę brzmienie tego przepisu rozszerza wyrażoną w Konstytucji RP zasadę konieczności ogłaszania prawa, oprócz aktów normatywnych o charakterze powszechnie obowiązującym, na wszystkie krajowe akty normatywne. Ponadto art. 2 wprowadza *de iure* dwa warunki, których łączne spełnienie znosi obowiązek ogłoszenia aktu normatywnego w dzienniku urzędowym — po pierwsze, dany akt nie może zawierać żadnej normy, która przyjmuje cechy powszechności (*a contrario*, może więc zawierać wyłącznie regulacje o charakterze wewnętrznym); po drugie, musi istnieć wyraźne upoważnienie ustawowe wyłączające obowiązek ogłoszenia danego aktu. Jak wskazuje G. Wierczyński, *w ten sposób zasada wyrażona w tym przepisie odbiera organom wydającym akty wewnętrznie obowiązujące możliwość decydowania o tym, jaki akt zostanie ogłoszony w dzienniku urzędowym i przekazuje ją ustawodawcy. Jak każdy wyjątek, przypadki takie muszą być interpretowane ściśle. W przypadku braku wyraźnego postanowienia ustawodawcy organ wydający akt wewnętrznie obowiązujący nie może samodzielnie przyjąć, że dany akt nie zostanie ogłoszony*³².

³⁰ Dz.U. 2019, poz. 1461 z późn. zm.

³¹ Dz.U. 2020, poz. 127 z późn. zm.

³² G. Wierczyński, zob. *Komentarz do ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych*, w: *Redagowanie i ogłaszanie aktów normatywnych. Komentarz*, wyd. 2, Warszawa 2016, art. 2 [online]. Protokół dostępu: <https://https-sip-lex-pl>.

Biorąc pod uwagę rozważania prowadzone w czwartym punkcie niniejszego rozdziału, wskazać należy, iż do aktów prawnych o charakterze wewnętrznym, które przedmiotem regulacyjnym obejmują działalność służb specjalnych, wobec których ustawodawca wprowadził ustawowe ograniczenie ich ogłoszenia, należą zarządzenia wydawane przez:

1. Prezesa Rady Ministrów (służby cywilne) / Ministra Obrony Narodowej (służby wojskowe), określające sposób i tryb realizacji przez szefów obowiązków w zakresie przekazywania uzyskanych informacji innym właściwym organom, służbom lub instytucjom, uwzględniając przepisy u. inf. niejaw. (art. 22a ust. 9 ustawy o ABW oraz AW; art. 27 ust. 9 ustawy o SKW oraz SWW — za zgodą Prezesa Rady Ministrów);
2. Ministra Obrony Narodowej (służby wojskowe), określające:
 - 1) formy i tryb współdziałania SKW i SWW (art. 8 ustawy o SKW oraz SWW);
 - 2) zakres i tryb współdziałania SKW i SWW ze Sztabem Generalnym Wojska Polskiego i innymi komórkami organizacyjnymi Ministerstwa Obrony Narodowej oraz Dowódcą Generalnym Rodzajów Sił Zbrojnych, Dowódcą Operacyjnym Rodzajów Sił Zbrojnych, Dowódcą Wojsk Obrony Terytorialnej, Szefem Inspektoratu Wsparcia Sił Zbrojnych, dowódcami garnizonów wojskowych i jednostek wojskowych (art. 10 ust. 2 ustawy o SKW oraz SWW);
 - 3) sposób i tryb tworzenia zespołów zadaniowych, o których mowa w ust. 1a, oraz wyznaczania żołnierzy pełniących służbę w oddziałach lub pododdziałach SZ RP do składu takich zespołów (art. 10 ust. 3 ustawy o SKW oraz SWW);
 - 4) wydawane w porozumieniu z ministrem właściwym do spraw zagranicznych, formy i tryb współdziałania SKW i SWW z organami, służbami i instytucjami podległymi ministrowi właściwemu do spraw zagranicznych, uwzględniając właściwość tych organów, służb i instytucji (art. 10 ust. 4 ustawy o SKW oraz SWW).

Co ważne, żadne z zarządzeń, do których kreacji jest upoważniony na mocy delegacji szczególnej lub ogólnej szef danej służby, nie korzysta z ustawowego wyjątku jego ogłoszenia. Zwrócić jednak należy uwagę na szczególnie istotną z perspektywy działalności służb specjalnych regulację art. 22 ust. 5 u. ogłasz. aktów, zgodnie z którą Minister Obrony Narodowej, minister właściwy do spraw wewnętrznych, minister właściwy do spraw zagranicznych, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu lub Szef Centralnego Biura Antykorupcyjnego wydają w postaci papierowej, w razie potrzeby, wyodrębnioną edycję dziennika urzędowego z aktami prawnymi zawierającymi informacje niejawne. W ten sposób akty normatywne o charakterze wewnętrznym,

kreowane przez szefów służb specjalnych, zawierające informacje, które zgodnie z *ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*³³ zostały zaklasyfikowane jako informacje „zastrzeżone”, „poufne”, „tajne” lub „ściśle tajne”, podlegają ogłoszeniu w wydodrębnionej edycji dziennika urzędowego. Dodać należy, iż nie ma w tym kontekście znaczenia, czy informacje zostały oznaczone jako niejawne na podstawie kryteriów wskazanych przez wskazaną ustawę, czy też wynikają z określenia zakresu informacji objętych danym aktem zdeterminowanym delegacją ustawową do jego wydania np. art. 9 ust. 4 ustawy o ABW oraz AW; art. 11 ustawy o SKW oraz SWW; art. 4 ust. 3 ustawy o CBA upoważniający do wydania, stanowiących informację niejawną, szczegółowych zasad tworzenia funduszu operacyjnego i gospodarowania tym funduszem. Na kanwie powyższego, w szczególności brzmienia art. 22 ust. 5 u. ogłasz. aktów oraz analizy brzmienia poszczególnych delegacji do wydania takich aktów, wskazać należy moim zdaniem na brak trafności prezentowanego w doktrynie stanowiska³⁴, zgodnie z którym zaklasyfikowanie aktu prawnego o charakterze wewnętrznym jako aktu niejawnego stanowi ustawową okoliczność warunkującą jego wyłączenie spod publikacji.

Od 1 stycznia 2012 r., kiedy to dodano do ustawy o ogłaszaniu aktów normatywnych przepis art. 2 a, akty normatywne i inne akty prawne podlegające ogłoszeniu ogłasza się w formie dokumentu elektronicznego w rozumieniu *ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*. Ponadto dzienniki urzędowe wydaje się w postaci elektronicznej, zaś dla każdego dziennika urzędowego wydawanego w postaci elektronicznej organ wydający prowadzi odrębną stronę internetową.

Akty prawa wewnętrznego, będące przedmiotem analizy tego rozdziału, ogłaszane są w dzienniku urzędowym właściwym dla organu wydającego dany akt i tak: zarządzenia Prezesa Rady Ministrów ogłaszane są w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” (art. 10 ust. 1 pkt 2 u. ogłasz. aktów), zaś zarządzenia Ministra Obrony Narodowej i szefów służb specjalnych w wydawanych przez nich dziennikach urzędowych ministrów kierujących działaniami administracji rządowej oraz w dziennikach urzędowych urzędów centralnych (art. 12 ust. 1 pkt 1 u. ogłasz. aktów).

W CBA, zgodnie z § 10 zarządzenia nr 7/21 Szefa CBA w sprawie zasad procedowania projektów aktów prawnych oraz wydawania pełnomocnictw i upoważnień, akt normatywny po podpisaniu podlega rejestracji w Biurze Prawnym CBA odpowiednio w prowadzonym w wersji elektronicznej rejestrze, jawnych lub niejawnych aktów normatywnych i wewnętrznych. Następnie Biuro

³³ Dz.U. 2019, poz. 742.

³⁴ Pogląd taki prezentuje G. Wierczyński, zob.: *Komentarz do ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych*, w: *Redagowanie i ogłaszanie aktów normatywnych. Komentarz*, wyd. 2, Warszawa 2016, art. 2 [online]. Protokół dostępu: <https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/commentary/587687091/501004/wierczynski-grzegorz-komentarz-do-ustawy-o-oglaszaniu-aktow-normatywnych-i-niektorych-innych...?cm=U-RELATIONS>, [dostęp: 4 VI 2021].

Prawne CBA publikuje podpisany akt normatywny w „Dzienniku Urzędowym CBA”, przy czym niejawni akt normatywny publikuje się w wyodrębnionej edycji „Dziennika Urzędowego CBA”. Zgodnie z § 11 ust. 2 i 3 tego zarządzenia niejawni akt normatywny publikuje się w wyodrębnionej edycji „Dziennika Urzędowego CBA”, która polega na wydrukowaniu dwóch egzemplarzy niejawnego aktu normatywnego opatrzonego nagłówkiem według wzoru określonego w załączniku i opatrzeniu go przez Biuro Prawne CBA datą oraz kolejną pozycją.

Z kolei w ABW, zgodnie z § 32 zarządzenia nr 11 Szefa ABW w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego, w „Dzienniku Urzędowym ABW”, wydawanym przez Biuro Prawne ABW, ogłasza się akty normatywne Szefa ABW i inne akty prawne podlegające ogłoszeniu, o których mowa w art. 12 u. ogłasz. aktów. Ponadto w „Dzienniku Urzędowym ABW” mogą być ogłaszane niebędące aktami normatywnymi akty prawne Szefa ABW, zawierające w szczególności obwieszczenia i ogłoszenia. W zarządzeniu przesądzono jednoznacznie, iż w „Dzienniku Urzędowym ABW” nie ogłasza się niebędących aktami normatywnymi aktów prawnych Szefa ABW:

- 1) aktów generalnych albo aktów indywidualnych stosowania prawa administracyjnego, w szczególności decyzji administracyjnych, postanowień, zaświadczeń i zezwoleń oraz innych rozstrzygnięć wydawanych w trybie Kodeksu postępowania administracyjnego i innych ustaw, a także upoważnień o charakterze administracyjnym;
- 2) aktów indywidualnych stosowania prawa cywilnego, w szczególności umów i pełnomocnictw;
- 3) dotyczących ochrony środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy ABW, w szczególności zawierających dane osobowe tych funkcjonariuszy, z wyłączeniem danych osobowych Szefa ABW, Zastępców Szefa ABW, dyrektorów jednostek organizacyjnych ABW i ich zastępców oraz funkcjonariuszy ABW działających w sferze publiczno-prawnej.

„Dziennik Urzędowy ABW” wydaje się w postaci elektronicznej z tym, że wyodrębnioną jego edycję z aktami normatywnymi Szefa ABW, zawierającymi informacje niejawni, Biuro Prawne ABW wydaje w postaci papierowej. Zgodnie z § 34 wyodrębnioną edycję „Dziennika Urzędowego ABW” wydaje się nie rzadziej niż raz w miesiącu.

Dodać należy, iż analiza stanu faktycznego prowadzi do wniosku, iż szefowie obu wojskowych służb specjalnych nie prowadzą dziennika urzędowego a kreowane przez siebie akty normatywne ogłaszają w „Dzienniku Urzędowym Ministra Obrony Narodowej”. Szef Agencji Wywiadu zaś nie prowadzi aktywnie dziennika urzędowego, bowiem analiza treści w nim zamieszczanych prowadzi do wniosku, iż ostatnie ogłoszone akty prawne pochodzą z 2011 r.

Podsumowanie

W niniejszym rozdziale przybliżono problematykę tworzenia prawa wewnętrznego służb specjalnych, ze szczególnym uwzględnieniem doświadczeń wynikających z kreacji tego rodzaju prawa w Agencji Bezpieczeństwa Wewnętrznego, omawiając miejsce aktu prawa wewnętrznego w systemie źródeł prawa zbudowanym przez Konstytucję RP z 1997 r. Przedstawiono zarys historyczny znaczenia prawa wewnętrznego dla kształtowania zasad ustrojowych funkcjonowania służb specjalnych po 1945 r., materialne podstawy kreacji prawa wewnętrznego służb specjalnych, aspekty proceduralne kreacji tego rodzaju prawa oraz zagadnienie ogłaszania prawa w służbach specjalnych ze szczególną analizą problematyki ogłaszania prawa niejawnego.

Podsumowując tak zarysowane tematycznie rozważania podjęte w pięciu częściach niniejszego rozdziału, wskazać należy, iż punktem zwrotnym w zakresie kreacji prawa wewnętrznego stało się przyjęcie nowej Konstytucji RP, w której w ramach katalogu źródeł prawa wyraźnie rozdzielono akty prawne obowiązujące powszechnie i wewnątrznie. Ten fakt prawny miał kluczowe znaczenie z perspektywy tworzenia prawa wewnętrznego w służbach specjalnych, którego ilość i znaczenie po tym okresie uległo znacznemu zmniejszeniu i swoistemu wypieraniu przez akty prawne rangi rozporządzenia. Ponadto zakładane przez prawodawcę w 2001 r. przewidywania, iż w krótkim czasie, w wyniku działalności orzeczniczej Trybunału Konstytucyjnego, sądów powszechnych czy też dorobku doktryny, nastąpi swoiście samoczynne zarysowanie granic pomiędzy zakresem regulacyjnym rozporządzeń i zarządzeń, należy uznać za złudne. Proces ten bowiem, pomimo upływu 20 lat wciąż trwa, przekładając się nieustannie na problemy legislatorów projektujących regulacje aktów prawa wewnętrznego służb specjalnych.

Bianka Skowronek

Rozdział 10.

Charakterystyka stosunku służbowego funkcjonariuszy ABW ze szczególnym uwzględnieniem analizy fakultatywnych i obligatoryjnych przesłanek zwolnienia ze służby na podstawie wybranych orzeczeń sądów administracyjnych

Charakterystyka stosunku służbowego funkcjonariuszy ABW jako relacji łączącej funkcjonariusza ze służbą mundurową

Charakter stosunku służbowego osób pełniących służbę w formacjach mundurowych zaliczany jest do prawa publicznego, a w jego ramach do prawa administracyjnego. Jest to stosunek łączący funkcjonariusza z daną formacją mundurową. Powstanie stosunku służbowego, jego zmiana oraz ustanie opiera się na wydanych przez organ administracji decyzjach administracyjnych, zwanych rozkazami. Wydawane przez organ decyzje mają charakter jednostronnych aktów prawnych, których treść determinowana jest przepisami kodeksu postępowania administracyjnego¹, tzw. pragmatyk służbowych, tj. ustaw regulujących powstanie i funkcjonowanie służb mundurowych, oraz wydanych na ich podstawie aktów wykonawczych.

W pragmatykach służbowych uregulowane zostały zarówno warunki i tryb przyjmowania do służby, jej przebieg, przesłanki zwolnienia ze służby, zasady odpowiedzialności dyscyplinarnej, jak i uprawnienia funkcjonariuszy związane z uposażeniem oraz innymi świadczeniami związanymi ze służbą. Obecnie w Polsce pragmatyki służbowe regulują funkcjonowanie m.in. takich służb, jak: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, policja, Straż Graniczna, Państwowa Straż Pożarna, Siły Zbrojne Rzeczypospolitej Polskiej, Służba Więzienna, Straż Marszałkowska.

¹ Zob. *Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego* (Dz.U. 2020, poz.256, ze zm.).

Wymienione formacje tradycyjnie zalicza się do katalogu tzw. służb mundurowych lub inaczej zmilitaryzowanych. Służby mundurowe wykonują zadania z zakresu szeroko pojętej ochrony bezpieczeństwa państwa w jego zewnętrznym i wewnętrznym aspekcie. Przy czym wskazać należy, że zarówno termin „służba”, jak i „stosunek służbowy”, chociaż stanowią pojęcia języka prawnego, to nie mają definicji ustawowych. W systemie prawnym brakuje ustawowego katalogu podmiotów zaliczanych do tych służb. Zdefiniowany prawnie został natomiast katalog służb specjalnych. Zgodnie z treścią art. 11 *ustawy z dnia 24 maja 2020 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*² do służb specjalnych zaliczamy: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Wywiadu Wojskowego, Służbę Kontrwywiadu Wojskowego i Centralne Biura Antykorupcyjne.

Należy przyjąć, że termin „służba” wywodzi się od słowa „służyć”, rozumianego jako *poświęcenie jakiejś idei lub dobru*³. Wobec powyższego warunkiem *sine qua non* uznania danej aktywności za służbę będzie pełnienie jej dla dobra wspólnego. Według definicji słownikowej wyraz „służba” oznacza pracę w urzędzie państwowym, instytucji użyteczności publicznej, wojsku itp. Natomiast termin „służbowy” oznacza: dotyczący pracy w urzędzie, instytucji, wojsku⁴. Z kolei pojęcie „mundurowy” odnosi się do zewnętrznego aspektu przynależności do danej formacji, którą jest mundur, oznaczający: *ubiór lub jego części służące do oznaczeniu przynależności do określonej jednostki organizacyjnej lub wykonywania określonych funkcji lub służby*⁵. Zgodnie z definicją słownikową „zmilitaryzowanie” oznacza: *wprowadzenie w jakimś podmiocie zasad organizacyjnych takich jak w wojsku*⁶.

Mając na uwadze powyższe, przedstawiciele doktryny, w tym M. Liwo, wskazują, że: *za służby mundurowe uznać należy wskazane przez ustawodawcę podmioty publiczne o szczególnej organizacji — na wzór wojskowy — podlegające naczelnym organom administracji rządowej, realizujące ustawowo określone zadania w ramach służby publicznej związane z zapewnieniem określonego rodzaju bezpieczeństwa i porządku na podstawie przyznanych uprawnień i prawnych form działania właściwych administracji*⁷.

² Dz.U. 2020, poz. 27, ze zm.

³ P. Wojtunik, *Pojęcie, źródła prawa i przedmiot prawa stosunków służbowych*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 8, s. 202.

⁴ *Słownik języka polskiego*, PWN, Warszawa 2005, s. 933.

⁵ Zob. *ustawa z dnia 21 grudnia 1978 r. o odznakach i mundurach* (Dz.U. 2016, poz. 38). Należy zauważyć, że niektóre służby zaliczane do mundurowych nie będą podlegały obowiązkowi umundurowania. Funkcjonariusze CBA nie podlegają umundurowaniu. Również funkcjonariusze pozostałych służb specjalnych, z uwagi na specyfikę wykonywanych zadań, często o charakterze niejawnym, co do zasady nie będą nosić munduru.

⁶ J. Bralczyk, *Słownik 100 tysięcy potrzebnych słów*, PWN, Warszawa 2007, s. 1007.

⁷ M. Liwo, *Służby mundurowe jako kategoria języka prawniczego*, „Przegląd Prawa Publicznego” 2015, nr 2, s. 20.

Zważywszy na charakter i doniosłość zadań wykonywanych przez służby mundurowe, stosunek prawny łączący funkcjonariusza z daną formacją mundurową został oparty na szczególnych zasadach, odróżniających go od innych form zatrudnienia, opartych na prawie pracy lub prawie cywilnym⁸. Zauważa się, że: *stosunek służbowy to kategoria stosunku prawnego zachodzącego między określonymi podmiotami, którego treść jest regulowana przepisami prawa publicznego (administracyjnego, konstytucyjnego), ale również prawa pracy. Jego treścią są prawa i obowiązki stron, a przedmiotem zachowanie wymagane od osoby zobowiązanej, odniesione do treści służby*⁹.

W opinii Trybunału Konstytucyjnego cechami charakterystycznymi dla stosunków służbowych w formacjach zmilitaryzowanych są: pełna dyspozycyjność i zależność od władzy służbowej¹⁰. W orzecznictwie sądowym przyjmuje się, że osoby podejmujące służbę, w odróżnieniu od zatrudnianych na podstawie umownego stosunku pracy, pozostają z władzą służbową w takim stosunku podporządkowania, która charakteryzuje się wysoką dyspozycyjnością zarówno co do sposobu wykonywania służby, w tym pod względem pory i miejsca świadczenia służby, jak i innych warunków należących do treści stosunku prawnego¹¹. Ponadto specyfika służby w formacjach mundurowych obejmuje wykonywanie zadań w trudnych warunkach, nierzadko związanych z bezpośrednim narażeniem życia i zdrowia¹². W zamian za spełnienie wymogu szczególnego poświęcenia oraz podporządkowania państwu, mając na uwadze zasady słuszności, zapewnia funkcjonariuszom wiele uprawnień i uprzywilejowanych świadczeń¹³.

Mając na uwadze powyższe, do cech charakterystycznych stosunku służbowego należy zaliczyć takie elementy, jak:

- 1) obowiązek poświęcenia,
- 2) wyjątkowa dyspozycyjność i obowiązek podporządkowania,
- 3) przyznanie funkcjonariuszom szczególnych uprawnień związanych z wykonywaniem służby,

⁸ Należy wskazać, że mianem „stosunki służbowe” lub „pracownicze stosunki służbowe” określane są niekiedy również stosunki zatrudnienia oparte częściowo na prawie pracy, a częściowo na pragmatykach (np. mianowanie, powołanie). Zatrudnienie na takiej podstawie ma charakter mieszany, albowiem niektóre rozstrzygnięcia pracodawców (organów) w stosunku do pracowników mogą być przedmiotem decyzji administracyjnej, a niektóre rozstrzygnięcia będą właściwe dla prawa pracy. Jednakże z uwagi na przedmiot niniejszego rozdziału, dotyczący charakterystyki stosunku służbowego w służbie mundurowej, stosunki zatrudnienia tego rodzaju nie będą omawiane.

⁹ Zob. T. Kuczyński, E. Mazurek-Jasińska, J. Stelina, *Stosunek służbowy*, w: *System prawa administracyjnego*, t. 11, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2011, C.H. Beck, s. 7.

¹⁰ Wyrok TK z dnia 14 XII 1999 r., SK 14/98.

¹¹ Wyrok NSA z 23 XI 2017 r. I OSK 269/16 oraz Uchwała NSA z dnia 5 XII 1991 r., I PZP 60/9.

¹² Wyrok TK z dnia 23 IX 1997 r., K 25/96.

¹³ Uchwała SN z 18 XII 1992 r., III AZP 27/92.

4) administracyjno-prawne uregulowanie stosunku prawnego funkcjonariusza¹⁴.

Nieodłącznym elementem stosunku służbowego jest gotowość funkcjonariuszy do wyjątkowego poświęcenia, która sprowadza się do ofiarowania, w imię wykonywania obowiązków służbowych, ich najcenniejszych dóbr indywidualnych, tj. życia i zdrowia. Za normatywny wyraz gotowości poświęcenia się, jako nieodłącznego elementu świadczenia służby, uznać należy treść roty ślubowania składanego przez funkcjonariuszy służb mundurowych. Treść roty ślubowania w poszczególnych służbach związana jest z wypełnianymi przez nie zadaniami i pozwala na zdefiniowanie dóbr prawnie chronionych, które uzasadniają wprowadzenie zobowiązania funkcjonariuszy do gotowości narażenia życia i zdrowia w imię ochrony tych dóbr. Złożenie roty ślubowania jest warunkiem *sine qua non* powstania stosunku służbowego w formacjach mundurowych, albowiem osoba, która dostanie rozkaz o mianowaniu, a nie złoży ślubowania nie może pełnić służby¹⁵.

Funkcjonariusze ABW oraz AW składają ślubowanie według następującej roty:

Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego (Agencji Wywiadu), ślubuję: służyć wiernie Narodowi, chronić ustanowiony Konstytucją RP porządek prawny, strzec bezpieczeństwa Państwa i jego obywateli, nawet z narażeniem życia. Wykonując powierzone mi zadania, ślubuję pilnie przestrzegać prawa, dochować wierności konstytucyjnym organom Rzeczypospolitej Polskiej, przestrzegać dyscypliny służbowej oraz wykonywać rozkazy i polecenia przełożonych. Ślubuję strzec tajemnicy prawnie chronionej, honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej¹⁶.

W orzecznictwie sądów administracyjnych nie budzi wątpliwości fakt, że osoby pełniące służbę w formacjach zmilitaryzowanych są zobowiązane do dochowania roty ślubowania, albowiem treść roty nie ma jedynie wymiaru symbolicznego, lecz stanowi oświadczenie woli, w którym świadomie zobowiązują się do wykonywania określonych zadań. Wobec powyższego funkcjonariusze pełniący służbę nie mogą uchylić się od skutków złożonej przysięgi¹⁷.

Kolejną, niezwykle istotną cechą stosunku służbowego jest dyspozycyjność i obowiązek podporządkowania. W służbach mundurowych dyspozycyjność jest rozumiana w dwóch aspektach. Z jednej strony oznacza uprawnienie właściwych przełożonych do kształtowania warunków służby podwładnego funkcjonariusza w zależności od potrzeb danej formacji, z drugiej strony do wykonywania służby w nielimitowanym czasie służby. Czas pełnienia służby funkcjonariusza

¹⁴ P. Szustakiewicz, *Istota stosunku służbowego*, w: *Stosunek służbowy w formacjach mundurowych*, red. W. Maciejko, P. Szustakiewicz, Legalis, Warszawa 2016.

¹⁵ Wyrok WSA w Warszawie z 13 XI 2009 r., II SA/WA 1009/09.

¹⁶ Zob. art. 47 ustawy o ABW oraz AW.

¹⁷ Zob. wyroki: NSA z dnia 24 I 2007 r., I OSK 664/06, WSA w Gdańsku z 19 I 2005 r., II SA/GD 3180/02, NSA z 10 II 2012 r., I OSK 1056/11.

jest bowiem określany wymiarem jego obowiązków¹⁸. Szczególna dyspozycyjność wynika z zadań powierzanych służbom mundurowym, które są doniosłe zarówno dla państwa, jak i jego obywateli, i nie może zostać od nich oddzielona.

Z pojęciem „dyspozycyjność” ściśle powiązane jest pojęcie „podporządkowanie”, które oznacza obowiązek wykonywania poleceń przełożonych. Jak wskazuje P. Szustakiewicz: *Cechą charakterystyczną formacji umundurowanych jest obowiązek wykonywania rozkazów lub poleceń. Przepisy, które zezwalają funkcjonariuszom na niewykonanie rozkazu są absolutnym wyjątkiem i nie mogą być nadużywane. Charakter służb zmilitaryzowanych nie pozwala na dyskusję lub stosowanie nad rozkazami, takie postępowanie byłoby zaprzeczeniem mechanizmu funkcjonowania tych formacji*¹⁹. Osoba, która wstępuje do służby nie może „negocjować” warunków pełnienia służby (np. wysokości uposażenia lub godzin wykonywania obowiązków służbowych — ani na początku służby, ani w trakcie służby). Warunki służby są dokładnie określone w przepisach prawa administracyjnego. Ewentualne osiągnięcie celów zakładanych przez funkcjonariusza, tj. np. uzyskanie wyższego uposażenia czy zmiany miejsca pełnienia służby, jest uzależnione od spełnienia przez niego przesłanek określonych w przepisach kształtujących stosunek służbowy²⁰.

W zamian za gotowość do poświęcenia, poddania się szczególnej dyscyplinie służbowej oraz wykonywanie zadań, w warunkach mogących skutkować narażeniem życia lub zdrowia, funkcjonariusze służb mundurowym otrzymują wiele uprawnień, które co do zasady nie występują w sferze umownych (pracowniczych lub cywilnych) stosunków zatrudnienia. Do szczególnych uprawnień należy m.in.: wyłączenie z powszechnego systemu emerytalnego (w tym prawo do odejścia na tzw. wcześniejszą emeryturę oraz odmienne zasady naliczania świadczeń emerytalnych), prawo do otrzymania lokalu mieszkalnego w miejscu służby lub ekwiwalentu w przypadku braku możliwości przyznania takiego lokalu, pomoc finansowa na uzyskanie lokalu mieszkalnego w miejscu służby, świadczenie rozłąkowe, ekwiwalent za umundurowanie, dodatkowy urlop ze względu na wiek, staż lub warunki służby, świadczenia związane z odejściem ze służby. Do szczególnych uprawnień należy zaliczyć również większą niż w przypadku innych zatrudnionych stabilizację stosunku służbowego, wyrażającą się w możliwości zwolnienia funkcjonariusza wyłącznie w przypadkach enumeratywnie wskazanych w przepisach pragmatycznych.

Stosunek służbowy funkcjonariusza ABW powstaje w drodze mianowania, poprzedzonego dobrowolnym zgłoszeniem się do służby. Wyrazem aktu mianowania jest wydanie rozkazu personalnego, który określa dzień przyjęcia do służby oraz stanowisko w służbie. Jak podkreślił Naczelny Sąd Administracyjny:

¹⁸ Zob. art. 51 ust. 1 ustawy o ABW oraz AW.

¹⁹ P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych i żołnierzy zawodowych jako sprawa administracyjna*, Warszawa 2012, Difin, s. 21.

²⁰ Zob. tenże, *Zagadnienie unifikacji przepisów regulujących stosunek służbowy funkcjonariuszy służb mundurowych*, „Przegląd Bezpieczeństwa Wewnętrznego” 2019, nr 21, s. 84.

mianowanie w służbach mundurowych jest indywidualnym aktem administracyjnym, a więc jednostronnym władczym działaniem organu administracyjnego. Rozkaz o mianowaniu jest decyzją administracyjną, w rozumieniu art. 104 kodeksu postępowania administracyjnego, która rozstrzyga sprawę indywidualną polegającą na nawiązaniu pomiędzy osobą fizyczną a organem stosunku służbowego²¹. Rozkaz o mianowaniu, jak każda decyzja administracyjna powinien oprócz wymogów określonych w przepisach pragmatycznych, zawierać obligatoryjne elementy decyzji określone w art. 107§ 1 kodeksu postępowania administracyjnego²².

Po przyjęciu do służby, wszystkie istotne zmiany w zakresie stosunku służbowego funkcjonariusza ABW (np. zmiana miejsca pełnienia służby, stanowiska służbowego, zmiana uposażenia), aż do rozwiązania tego stosunku, będą określone w rozkazach personalnych. Jak wskazuje A. Korcz-Maciejko:

Rozkazy personalne są to decyzje o charakterze władczym, wydane przez właściwe organy, jednostronnie kształtujące sytuację prawną funkcjonariusza. Rozkaz jako szczególna postać polecenia służbowego w administracji publicznej wyposażono w odrębną nazwę tego aktu, podkreślającą, że wydano go w sferze szczególnej, związanej z wykonywaniem władztwa publicznego. (...) Z mocy szczególnego przepisu, jest decyzją administracyjną o ile jego przedmiot obejmuje sprawy kluczowe dla wykonywania służby, tzn. mianuje na funkcjonariusza, zmienia podstawowe elementy stosunku służbowego lub zwalnia ze służby²³.

²¹ Zob. wyrok NSA z dnia 15 VI 2010, sygn. akt I OSK 1705/09.

²² Zgodnie z treścią Art. 107. § 1 Kodeksu postępowania administracyjnego decyzja zawiera:

- 1) oznaczenie organu administracji publicznej;
- 2) datę wydania;
- 3) oznaczenie strony lub stron;
- 4) powołanie podstawy prawnej;
- 5) rozstrzygnięcie;
- 6) uzasadnienie faktyczne i prawne;
- 7) pouczenie, czy i w jakim trybie służy od niej odwołanie oraz o prawie do zrzeczenia się odwołania i skutkach zrzeczenia się odwołania;
- 8) podpis z podaniem imienia i nazwiska oraz stanowiska służbowego pracownika organu upoważnionego do wydania decyzji, a jeżeli decyzja wydana została w formie dokumentu elektronicznego — kwalifikowany podpis elektroniczny;
- 9) w przypadku decyzji, w stosunku do której może być wniesione powództwo do sądu powszechnego, sprzeciw od decyzji lub skarga do sądu administracyjnego — pouczenie o dopuszczalności wniesienia powództwa, sprzeciwu od decyzji lub skargi oraz wysokości opłaty od powództwa lub wpisu od skargi lub sprzeciwu od decyzji, jeżeli mają one charakter stały, albo podstawie do wyliczenia opłaty lub wpisu o charakterze stosunkowym, a także możliwości ubiegania się przez stronę o zwolnienie od kosztów albo przyznanie prawa pomocy.

²³ A. Korcz-Maciejko, *Prawny charakter rozkazu personalnego*, „Administracja: teoria, dydaktyka, praktyka” 2013, nr 3, s. 134.

Rozkazy personalne, pomimo tego, iż wydawane są w sferze wewnętrznej działania administracji służb mundurowych, korzystają z gwarancji procesowych, umożliwiających kontrolę ich legalności. Kontrolę legalności rozkazów sprawują wojewódzkie sądy administracyjne oraz Naczelny Sąd Administracyjny w trybie określonym w przepisach procedury sędowo-administracyjnej²⁴.

Podstawy rozwiązania stosunku służbowego w służbach mundurowych

W porównaniu z innymi stosunkami zatrudnienia pragmatyki służbowe znacząco ograniczają swobodę stron w zakresie możliwości rozwiązania stosunku służbowego. Strony stosunku służbowego nie są uprawnione do jego rozwiązania w drodze wypowiedzenia lub porozumienia stron, które to czynności prawne stanowią podstawowe modele rozwiązywania pracowniczych lub cywilnych stosunków zatrudnienia. Rozwiązanie stosunku służbowego jest możliwe tylko w przypadku wystąpienia okoliczności wskazanych w ustawach pragmatycznych i następuje w drodze zwolnienia ze służby lub stwierdzenia wygaśnięcia stosunku służbowego.

Z jednej strony ograniczenia rozwiązania stosunku służbowego zapewniają funkcjonariuszom stabilizację zatrudnienia, a z drugiej strony chronią interes publiczny, utożsamiany w tym wypadku z interesem służby, zapewniając nieprzerwane i sprawne działanie formacji mundurowych. Jak wskazuje P. Szustakiewicz:

dokładne określenie przesłanek rozwiązania stosunku służbowego funkcjonariuszy chroni ich przed nieuzasadnionym, woluntarystycznym zwolnieniem. Przełożeni są związani przepisami pragmatycznymi i nie mogą działać jedynie na podstawie swojej woli. Takie rozwiązanie sprzyja stabilności i jakości służby funkcjonariuszy, którzy mogą skoncentrować się na wykonywaniu zadań służbowych, a nie zabezpieczeniu bytu swojego i rodziny w razie niespodziewanego i nieuzasadnionego zwolnienia²⁵.

W przepisach pragmatycznych ustawodawca wskazał *ex lege* okoliczności faktyczne, które nakładają na organ obowiązek rozwiązania stosunku służbowego (przesłanki obligatoryjnego zwolnienia ze służby), a także takie, które w razie ich zaistnienia, dają mu taką możliwość (przesłanki fakultatywnego zwolnienia ze służby). Katalog przesłanek zwolnienia ze służby jest katalogiem zamkniętym, co oznacza, że organ nie może zwolnić funkcjonariusza na innej podstawie, niż została wymieniona w przepisach prawa. Przesłanki fakultatywnego oraz obligatoryjnego zwolnienia ze służby przewidują przepisy wszystkich

²⁴ Tylko w nielicznych ściśle określonych przypadkach, wymienionych w ustawie pragmatycznej, do postępowań w sprawach związanych z prawami i obowiązkami funkcjonariuszy zastosowanie będą miały przepisy procedury cywilnej (np. sprawy związane z uprawnieniami rodzicielskimi).

²⁵ P. Szustakiewicz, *Stosunki służbowe...*, s. 274.

pragmatyk służbowych, co jednak nie oznacza, że sposób ustania stosunku służbowego został w nich uregulowany w ten sam sposób.

Jednakże każdorazowo, w przypadku zaistnienia jednej z obligatoryjnych przesłanek zwolnienia ze służby, właściwy w sprawie przełożony będzie miał obowiązek wydać decyzję o zwolnieniu ze służby. Treść takiej decyzji nie będzie zatem w żaden sposób zdeterminowana dokonaną przez niego oceną stanu faktycznego. Losy stosunku służbowego będą w takiej sytuacji konsekwencją określenia przez ustawodawcę *a priori* skutków prawnych wynikających z zaistniałych okoliczności. Postępowanie, w przypadku wystąpienia obligatoryjnej przesłanki zwolnienia ze służby, będzie ograniczone jedynie do wykazania, że przesłanka zwolnienia wystąpiła. W takim postępowaniu właściwy w sprawie przełożony nie jest zobowiązany ani uprawniony do tego, by brać pod uwagę wystąpienie innych okoliczności związanych ze służbą (tj. np. staż służby funkcjonariusza lub otrzymane przez niego dotychczas w służbie nagrody i wyróżnienia)²⁶.

W przypadku wystąpienia jednej z fakultatywnych przesłanek zwolnienia ze służby organ nie będzie obowiązany, lecz tylko uprawniony do wydania decyzji w sprawie zwolnienia ze służby. Podjęcie decyzji o rozwiązaniu stosunku służbowego na podstawie przesłanki fakultatywnej mieści się w granicach uznania administracyjnego, czyli swobodnej oceny okoliczności faktycznych, które mają wpływ na sprawność realizacji zadań danej formacji. Rolą organu będzie w tym przypadku ustalenie to, czy okoliczności danej sprawy uzasadniają dalsze trwanie stosunku służbowego czy też jego rozwiązanie. Przy podejmowaniu decyzji w przypadku fakultatywnego zwolnienia ze służby organ będzie badał te okoliczności z uwzględnieniem art. 7 Kodeksu postępowania administracyjnego, zgodnie z którym rozstrzygając sprawę w drodze decyzji administracyjnej, organ administracji publicznej musi mieć na względzie interes społeczny i słuszny interes strony.

Jak wskazuje P. Szustakiewicz:

Postępowanie w przypadku wystąpienia przesłanek fakultatywnych jest znacznie bardziej skomplikowane niż w sytuacji, gdy wystąpią przesłanki obligatoryjne. Przełożony nie może poprzestać jedynie na ustaleniu wystąpienia jednej z przesłanek fakultatywnego zwolnienia ze służby, ale powinien także wskazać okoliczności, które wpłynęły na to, że zdecydował się na zwolnienie funkcjonariusza. Rozkaz o zwolnieniu ma bowiem charakter uznaniowy, stąd powinny być wobec niego zastosowane wszystkie reguły odnoszące się do decyzji uznaniowej. Rozkaz o zwolnieniu z powodu wystąpienia przesłanki powinien zawierać przekonujące uzasadnienie, wskazujące, dlaczego dany funkcjonariusz nie może nadal pełnić służby²⁷.

Z kolei w orzecznictwie sądów administracyjnych powszechnie przyjmuje się, że kontrola decyzji opartej na uznaniu administracyjnym ma ograniczony

²⁶ Zob. *Komentarz do art. 60 ustawy o Agencji Bezpieczeństwa oraz Agencji Wywiadu*, B. Opaliński, M. Rogalski, P. Szustakiewicz, Legalis, Warszawa 2017.

²⁷ Tamże.

zakres. Sprowadza się ona do zbadania, czy zaskarżona decyzja nie nosi cech dowolności, tj. czy organ administracji wybrał prawnie dopuszczalny sposób rozstrzygnięcia oraz czy wyboru takiego dokonał po ustaleniu i rozważeniu okoliczności istotnych dla sprawy. Kontrola sądowno-administracyjna nie obejmuje natomiast oceny, w jaki sposób organy administracji, realizując określoną politykę stosowania prawa, wypełniają treść pozasystemowych kryteriów słusznościowych czy celowościowych²⁸. W konsekwencji, w sprawach dotyczących fakultatywnego zwolnienia funkcjonariusza ze służby sądy administracyjne badają jedynie, czy decyzja o rozwiązaniu stosunku służbowego nie jest arbitralna lub czy nie została podjęta przy użyciu niedozwolonych kryteriów. Nie mogą natomiast wkraczać w kompetencje merytoryczne właściwych organów i przesądzać, czy dana osoba powinna nadal pozostać funkcjonariuszem danej formacji, czy też może zostać wykluczona z tego grona.

Reasumując, jak wskazuje P. Wiczorek, przesłanki fakultatywnego i obligatoryjnego zwolnienia ze służby można scharakteryzować w następujący sposób:

uzasadnione wydaje się stwierdzenie, że katalogi fakultatywnych jak i obligatoryjnych podstaw zwolnienia funkcjonariusza ze służby mają podstawę w ochronie interesu publicznego. W konsekwencji należy przyjąć, że obligatoryjne przesłanki zwolnienia ze służby zawierają wiążącą ocenę ustawodawcy, że określone zdarzenia naruszają interes publiczny w takim stopniu, iż dla jego ochrony należy poświęcić interes indywidualny. Idąc tym tokiem myślenia, należy stwierdzić, że fakultatywne podstawy zwolnienia ze służby zostały określone przez prawodawcę jako jedynie potencjalnie godzące w interes służby. Ustawodawca nie przesądza apriorycznie, jak to ma miejsce w przypadku obligatoryjnych przesłanek zwolnienia ze służby, że naruszenie to wyklucza dalsze pełnienie służby²⁹.

Obligatoryjne i fakultatywne przesłanki rozwiązania stosunku służbowego w ABW, z uwzględnieniem analizy porównawczej ustaw pragmatycznych pozostałych służb specjalnych

Przepis art. 44 ustawy o ABW oraz AW określa wymagania, jakie powinien spełniać funkcjonariusz ABW oraz AW. Zgodnie z treścią tego przepisu służbę w ABW oraz AW może pełnić osoba:

- 1) posiadająca obywatelstwo polskie;
- 2) korzystająca z pełni praw publicznych;
- 3) wykazująca nieskazitelną postawę moralną, obywatelską i patriotyczną;
- 4) dająca rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych;

²⁸ Zob. m.in. wyrok NSA z dnia 19 V 2011 r. I OSK 301/11.

²⁹ M. Wiczorek, *Charakter prawny stosunków służbowych funkcjonariuszy służb mundurowych*, Wydawnictwo Adam Marszałek, Toruń 2017, s. 235.

- 5) posiadająca co najmniej wykształcenie średnie lub średnie branżowe i określone kwalifikacje zawodowe oraz zdolność fizyczną i psychiczną do służby w formacjach uzbrojonych, wymagających szczególnej dyscypliny służbowej, której gotowa jest się podporządkować.

Przedmiotowy przepis określa podstawowe warunki, jakie powinien spełnić kandydat do służby w ABW oraz osoba pozostająca w służbie. Nie ulega zatem wątpliwości, że utrata którejs z powyższych przesłanek będzie stanowić podstawę do zwolnienia ze służby. Katalog obligatoryjnych oraz fakultatywnych przesłanek zwolnienia ze służby będzie zatem nawiązywał w sposób oczywisty do wymienionych wymagań.

Obligatoryjne przesłanki zwolnienia ze służby

Obligatoryjne przesłanki zwolnienia ze służby funkcjonariusza ABW zostały określone w art. 60 ust. 1 ustawy o ABW oraz AW. Zgodnie z treścią powyższego przepisu funkcjonariusza ABW obligatoryjnie zwalnia się w następujących przypadkach:

- 1) orzeczenia trwałej niezdolności do służby przez komisję lekarską właściwej Agencji;
- 2) nieprzydatności do służby, stwierdzonej w opinii służbowej w okresie służby przygotowawczej;
- 3) wymierzenia kary dyscyplinarnej wydalenia ze służby;
- 4) skazania prawomocnym wyrokiem sądu za przestępstwo umyślne ścigane z oskarżenia publicznego;
- 5) utraty obywatelstwa polskiego.

Dodatkowo przesłanką obligatoryjnego zwolnienia ze służby będzie zwolnienie funkcjonariusza w przypadku pisemnego zgłoszenia przez niego wystąpienia ze służby, czyli tzw. zwolnienie na raport. Zgodnie z treścią art. 60 ust. 3 ustawy o ABW oraz AW: *Funkcjonariusza zwalnia się ze służby w terminie do 6 miesięcy od dnia pisemnego zgłoszenia przez niego wystąpienia ze służby.*

Katalog obligatoryjnych przesłanek zwolnienia ze służby został podobnie ukształtowany w innych służbach specjalnych. Identyczne uregulowania zawierają przepisy ustawy o służbie w SKW i SWW³⁰. Z kolei katalog ten został poszerzony o dodatkowe przesłanki w odniesieniu do funkcjonariuszy CBA. Zgodnie z treścią art. 64. ust. 1 *ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*³¹ oprócz przesłanek wskazanych powyżej funkcjonariusza CBA zwalnia się ze służby także w przypadku:

- 1) nabycia obywatelstwa innego państwa;
- 2) podania nieprawdy w oświadczeniu składanym na podstawie art. 10 *ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne*, stwierdzonego w drodze postępowania dyscyplinarnego;

³⁰ Dz.U. 2020, poz. 1221, ze zm.

³¹ Dz.U. 2019, poz. 1921, ze zm.

- 3) skazania prawomocnym wyrokiem za przestępstwo skarbowe;
- 4) objęcia kierowniczego stanowiska państwowego albo funkcji z wyboru w organach samorządu terytorialnego.

Obligatoryjną przesłanką zwolnienia ze służby w ABW oraz w pozostałych służbach specjalnych jest orzeczenie właściwej komisji lekarskiej o trwałej niezdolności do służby. Nie budzi wątpliwości fakt, że funkcjonariusz musi posiadać zdolność fizyczną oraz psychiczną do pełnienia służby. Orzeczenie właściwej komisji lekarskiej o braku takiej zdolności będzie zawsze skutkowało koniecznością zwolnienia funkcjonariusza ze służby. Przepis ten został sformułowany w sposób kategoryczny, nie pozostawia organowi żadnej innej możliwości wyboru w przypadku ziszczenia się normy prawnej w nim zawartej³². Decyzja o zwolnieniu ze służby będzie zatem decyzją związaną, uzależnioną od orzeczenia innego organu — komisji lekarskiej. Przy czym istotne jest, aby orzeczenie komisji wskazywało na takie upośledzenie czynności organizmu, które jest trwałe i nie rokuje poprawy.

Jak wyjaśnił Naczelny Sąd Administracyjny w wyroku z 5 lipca 2006 r. (I OSK 1338/05), wydanym na gruncie analogicznego przepisu *ustawy z dnia 6 kwietnia 1990 r. o Policji*³³: (...) *o treści orzeczenia komisji lekarskiej decyduje ocena stopnia i trwałości niezdolności do służby. W tym zakresie istotne znaczenie ma stopień naruszenia sprawności organizmu badanego i możliwości przywrócenia w drodze leczenia sprawności niezbędnej do dalszego pełnienia służby. (...) jeżeli nie ma takich pozytywnych prognoz co do stanu zdrowia, gdyż stwierdzone u badanego schorzenia nie pozwalają w ogóle na pełnienie służby, to funkcjonariusza uznaje się za całkowicie niezdolnego do służby.* Jeżeli komisja lekarska ABW uzna funkcjonariusza za trwale niezdolnego do służby, niezwłocznie zwalnia się go od zajęć służbowych na okres do dnia zwolnienia ze służby³⁴.

Przesłanką obligatoryjnego zwolnienia ze służby w ABW oraz w pozostałych służbach specjalnych jest skazanie prawomocnym wyrokiem sądu za przestępstwo umyślne ścigane z oskarżenia publicznego. W wypadku wystąpienia tej przesłanki zwolnienia organ również jest związany treścią innego orzeczenia — wyroku sądowego. Postępowanie w przedmiocie zwolnienia ze służby w takim wypadku ogranicza się do stwierdzenia istnienia prawomocnego orzeczenia, którego skutkiem jest wydanie rozkazu o zwolnieniu ze służby. W przypadku zaistnienia takiej przesłanki organ administracyjny ogranicza swoją aktywność w postępowaniu do włączenia do akt sprawy prawomocnego wyroku skazującego za przestępstwo umyślne. Przy czym, organ nie bada okoliczności zmierzających do scharakteryzowania funkcjonariusza i jego dotychczasowego przebiegu służby, albowiem elementy te nie mogą mieć żadnego znaczenia prawnego³⁵.

³² Zob. wyrok NSA z dnia 12 VI 2007 r. I OSK 1170/06.

³³ Dz.U. 2020, poz. 360, ze zm.

³⁴ Zob. *rozporządzenie Prezesa Rady Ministrów z dnia 2 VII 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* (Dz.U. 2013, poz. 862, ze zm.).

³⁵ Zob. wyrok NSA z dnia 8 IV 2011 r. I OSK 34/11, wydany na gruncie ustawy o Policji.

Kara wydalenia ze służby jest najsurowszą z przewidzianych w katalogu kar dyscyplinarnych określonych w przepisach pragmatycznych. Orzeczenie kary wydalenia ze służby będzie miało miejsce w przypadku, gdy działanie lub zaniechanie funkcjonariusza w taki sposób naruszyło interes służby, że jednocześnie nie jest możliwe dalsze jej pełnienie.

Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 września 2016 r. (sygn. akt II SA/Wa 856/16): *Postępowanie w przedmiocie zwolnienia ze służby polega jedynie na sprawdzeniu, czy w przypadku danej osoby zostało wydane orzeczenie dyscyplinarne, czy orzeczono w nim karę wydalenia ze służby oraz czy jest ono prawomocne. Przy czym, bezzasadne jest w tym trybie podważanie treści orzeczenia dyscyplinarnego, bowiem postępowanie w sprawie zwolnienia nie służy dodatkowej weryfikacji orzeczenia dyscyplinarnego.*

Zdarzają się sytuacje, gdy delikt dyscyplinarny popełniony przez funkcjonariusza będzie skutkował wszczęciem dodatkowo postępowania karnego. Jednakże ustalenie przez sąd karny, że funkcjonariusz nie dopuścił się przestępstwa, nie będzie automatycznie skutkowało brakiem odpowiedzialności dyscyplinarnej. Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 8 września 2010 r. (sygn. akt VIII SA/Wa 404/10):

Zauważyć w tym miejscu należy, że odpowiedzialność dyscyplinarna związana może być z czynami, które nie podlegają odpowiedzialności karnej. Odpowiedzialność dyscyplinarna jest bowiem niezależna od odpowiedzialności karnej. W ramach postępowania dyscyplinarnego mieści się także odpowiedzialność za czyny nie mające znamion przestępstw, a które uchybiają godności lub regułom wykonywania zawodu. Uznanie przez organ orzekający w postępowaniu dyscyplinarnym oczywistości popełnienia przez funkcjonariusza przestępstwa jest czymś odmiennym od uznania go winnym popełnienia przestępstwa przez sąd w postępowaniu karnym. W postępowaniu dyscyplinarnym odmiennie niż w procedurze karnej nie obowiązuje także zasada domniemania niewinności i tłumaczenia wszelkich nie dających się usunąć wątpliwości na korzyść obwinionego. Oczywiście, nie można kwestionować postanowienia o umorzeniu postępowania karnego, z którego wynika, że skarżący nie popełnił przestępstwa w rozumieniu kodeksu karnego. Niemniej jednak, postanowienie o umorzeniu tegoż postępowania nie oznacza braku możliwości uznania skarżącego winnym naruszenia dyscypliny służbowej z powodu jego niewątpliwie nagannego zachowania i w konsekwencji — wymierzenia mu z tego powodu kary wydalenia ze służby.

Przesłanką obligatoryjnego zwolnienia ze służby jest utrata obywatelstwa polskiego. Osoba, która w trakcie służby przestanie być obywatelem polskim, nie będzie mogła w tej służbie pozostać. Zgodnie z obecnie obowiązującymi przepisami Konstytucji RP oraz *ustawy z dnia 2 kwietnia 2009 r. o obywatelstwie polskim*³⁶ jedyną możliwością utraty obywatelstwa polskiego jest jego zrzeczenie się na własną prośbę, po uzyskaniu zgody Prezydenta RP.

³⁶ Dz.U. 2020, poz. 347.

Z kolei nabycie obywatelstwa innego kraju (dodatkowo) nie będzie przesłanką obligatoryjnego zwolnienia ze służby również w ABW, AW, SKW i SWW. Prawo do posiadania podwójnego obywatelstwa w wymienionych formacjach ustawodawca wprowadził wraz z wejściem w życie *ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*³⁷. W uzasadnieniu projektu do tej ustawy ustawodawca wskazał, że celem wprowadzenia takiego rozwiązania jest pozyskiwanie do służby w tych formacjach osób, które mogą ułatwić rozpoznanie środowisk radykalnych z innych krajów, w tym międzynarodowych organizacji terrorystycznych³⁸. Należy zauważyć, że nabycie obywatelstwa innego kraju stanowi nadal przesłankę obligatoryjnego zwolnienia ze służby w CBA, albowiem ustawa o działaniach antyterrorystycznych nie wprowadziła zmian w przedmiocie obligatoryjnych przesłanek zwolnienia ze służby w tej formacji.

Następną przesłanką obligatoryjnego zwolnienia ze służby jest nieprzydatność do służby stwierdzona w opinii w okresie służby przygotowawczej. Procedura opiniowania funkcjonariuszy ABW została uregulowana w przepisach *rozporządzenia Prezesa Rady Ministrów z dnia 3 marca 2011 r. w sprawie opiniowania funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz wzoru formularza opinii służbowej*³⁹. Natomiast terminy opiniowania zostały określone w art. 53 ust. 1 ustawy o ABW oraz AW.

Opiniowanie w służbie przygotowawczej ma na celu sprawdzenie czy dana osoba, pomimo pozytywnego wyniku postępowania kwalifikacyjnego, skonfrontowana z obiektywnymi wyzwaniami służby, jest w stanie należycie realizować obowiązki służby. Z tego powodu częstotliwość opiniowania w służbie przygotowawczej jest znacznie większa niż w służbie stałej. Należy wskazać, że zgodnie z utrwalonym poglądem orzecznictwa opinia służbowa nie stanowi decyzji administracyjnej. Funkcjonariusz ABW, który nie zgadza się z treścią opinii służbowej, wydanej przez bezpośredniego przełożonego, ma prawo do złożenia do wyższego przełożonego odwołania od opinii służbowej w terminie 30 dni od jej otrzymania. Jeżeli odwołanie nie zostanie uwzględnione, funkcjonariusz może w terminie 14 dni złożyć wniosek do Szefa ABW o ponowne rozpatrzenie uwag odwołania. Niemniej jednak po wyczerpaniu „trybu wewnętrznego”, opinia służbowa nie może zostać zaskarżona do sądu administracyjnego. Zdaniem NSA: *Sprawa opiniowania służbowego funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego nie jest sprawą administracyjną, a opinia służbowa nie ma cech rozstrzygnięcia sprawy administracyjnej ani w znaczeniu procesowym ani materialnym (...) Odwołanie od opinii służbowej oraz wniosek o ponowne rozpatrzenie*

³⁷ Dz.U. 2016, poz. 904, ze zm.

³⁸ Przed uchwaleniem ustawy o działaniach antyterrorystycznych nabycie obywatelstwa innego kraju stanowiło obligatoryjną przesłankę zwolnienia ze służby w ABW, AW, SKW i SWW. Obecnie jest to przesłanka fakultatywnego zwolnienia ze służby w tych formacjach.

³⁹ Dz.U. 2014, poz. 46, ze zm.

*takiego odwołania należy traktować jedynie jako środki prawne uruchamiające wewnętrzną kontrolę postępowania opiniodawczego*⁴⁰.

Mając na uwadze powyższe, w przypadku zaskarżenia rozkazu personalnego o zwolnieniu ze służby do sądu administracyjnego, postępowanie sądowe w takiej sprawie zostanie ograniczone do badania, czy wydano ostateczną opinię oraz oceny trybu prawidłowości wydania takiej opinii. Sąd nie będzie natomiast badał merytorycznych przesłanek, uzasadniających nieprzydatność funkcjonariusza do służby, określonych w wydanej opinii służbowej.

Zwolnienie funkcjonariusza w związku z pisemnym wystąpieniem ze służby jest obligatoryjną przesłanką zwolnienia ze służby, mającą źródło w inicjatywie samego funkcjonariusza. W przypadku sporządzenia przez funkcjonariusza ABW raportu o zwolnieniu ze służby organ zobligowany jest do wydania rozkazu w sprawie zwolnienia ze służby w terminie sześciu miesięcy od daty złożenia tego wniosku. Przy czym organ nie jest związany terminem rozwiązania stosunku służbowego, zaproponowanym przez funkcjonariusza w raporcie.

Organ wyznacza termin zwolnienia ze służby, kierując się interesem służby i mając na względzie sprawne wykonywanie zadań danej formacji. Jak wskazał WSA w Warszawie, w wyroku z dnia 14 listopada 2018 r. (II SA/Wa 293/2018: *Nie stanowi naruszenia prawa, określenie przez Szefa Agencji Bezpieczeństwa Wewnętrznego w rozkazy personalnym o zwolnieniu ze służby innej daty zwolnienia niż określona w raporcie przez funkcjonariusza, o ile data ta mieści się w terminie 6 miesięcy od dnia pisemnego zgłoszenia przez niego wystąpienia ze służby*. Termin zwolnienia ze służby w przypadku złożenia przez funkcjonariusza raportu o zwolnienie w ABW, AW, SKW, SWW wynosi sześć miesięcy, natomiast w przypadku funkcjonariuszy CBA termin ten jest krótszy i wynosi trzy miesiące od daty pisemnego wystąpienia ze służby.

Podkreślić należy też, że zgodnie z utrwalonym w orzecznictwie poglądem (pomimo tego, iż co do zasady do stosunku służbowego stosuje się przepisy procedury administracyjnej): *pisemne zgłoszenie przez funkcjonariusza wystąpienia ze służby, na podstawie art. 60 ust. 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu jest oświadczeniem woli, do którego ma zastosowanie art. 61 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny*⁴¹. Przyjęte przez NSA stanowisko oznacza, że ograniczone są możliwości odwołania takiego oświadczenia woli przez funkcjonariusza. Odwołanie oświadczenia o zwolnieniu ze służby może bowiem zostać uznane za skuteczne tylko w przypadku, gdyby doszło do adresata wraz z oświadczeniem woli lub wcześniej⁴². Zdaniem NSA przyjęty pogląd wiąże się z koniecznością ochrony prawidłowego wykonywania zadań przez ABW:

⁴⁰ Zob. postanowienie NSA z dnia 12 IV 2013 r., sygn. akt. I OSK 302/13.

⁴¹ Zob. uchwała NSA z dnia 5 XII 2011 r., I OPS 4/1.

⁴² Zgodnie z art. 61 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2020, poz. 1740, ze zm.): *Oświadczenie woli, które ma być złożone innej osobie, jest złożone z chwilą, gdy doszło do niej w taki sposób, że mogła zapoznać się z jego treścią. Odwołanie*

(...) należy bowiem pamiętać, że złożenie przez funkcjonariusza oświadczenia woli o wystąpieniu ze służby wywołuje skutki prawne w sferze interesów obu stron stosunku służbowego. Przede wszystkim obliguje organ do rozwiązania stosunku służbowego w terminie przewidzianym w ustawie. Z drugiej zaś strony podnieść należy, że przepisy Kodeksu cywilnego przewidujące możliwość uchylecia się od skutków złożonego oświadczenia woli zapewniają wystarczające gwarancje ochrony funkcjonariusza, którego oświadczenie o wystąpieniu ze służby dotknięte było wadami⁴³.

W ustawie o ABW oraz AW przewidziana została jeszcze jedna przesłanka obligatoryjnego zwolnienia ze służby, która jest uregulowana poza katalogiem określonym w art. 60 ust. 1 ustawy o ABW oraz AW. Zgodnie z treścią art. 54 ust. 3 ustawy o ABW oraz AW:

funkcjonariusza zwalnia się ze służby, jeżeli po przeniesieniu do dyspozycji Szefa ABW zostanie mu zaproponowane nowe stanowisko służbowe, a funkcjonariusz odmówi przyjęcia tej propozycji kadrowej. W związku z powyższym, organ zobligowany jest do zwolnienia funkcjonariusza, który w trakcie pozostawania w dyspozycji, nie zgodzi się na przyjęcie zaoferowanej mu propozycji kadrowej. Przy czym funkcjonariusza takiego zwalnia się ze służby z zachowaniem 6 lub 3 miesięcznego okresu ochronnego, określonego w art. 60 ust. 3 ustawy o ABW oraz AW, w zależności od tego czy funkcjonariusz pozostaje w trakcie wystąpienia przesłanki zwolnienia w służbie przygotowawczej czy stałej.

Fakultatywne przesłanki zwolnienia ze służby

Fakultatywne przesłanki zwolnienia ze służby w ABW zostały określone w art. 60 ust. 2 ustawy o ABW oraz AW. Zgodnie z treścią tego przepisu funkcjonariusza można zwolnić ze służby w ABW w przypadku:

- 1) niewywiązywania się z obowiązków służbowych w okresie odbywania służby stałej, stwierdzonego w dwóch kolejnych opiniach, między którymi upłynęło co najmniej sześć miesięcy,
- 2) skazania prawomocnym wyrokiem sądu za przestępstwo inne niż umyślne ścigane z oskarżenia publicznego,
- 3) objęcia kierowniczego stanowiska państwowego albo objęcia funkcji z wyboru w organach samorządu terytorialnego,
- 4) nabycia prawa do emerytury w pełnym wymiarze, określonego w przepisach odrębnych,
- 5) gdy wymaga tego ważny interes służby,
- 6) likwidacji jednostki organizacyjnej Agencji lub jej reorganizacji, połączonej ze zmniejszeniem obsady etatowej, jeżeli przeniesienie funkcjonariusza do

takiego oświadczenia jest skuteczne, jeżeli doszło jednocześnie z tym oświadczeniem lub wcześniej.

⁴³ Tamże, uchwała NSA z dnia 5 XII 2011 r., I OPS 4/1.

innej jednostki organizacyjnej Agencji lub na niższe stanowisko służbowe nie jest możliwe,

- 7) dwukrotnego nieusprawiedliwionego niestawienia się na badania, o których mowa w art. 59 ust. 1a, lub niepoddania się im albo w przypadku dwukrotnego nieusprawiedliwionego niestawienia się na obserwację w podmiocie leczniczym, w przypadku wyrażenia zgody przez funkcjonariusza, chyba że skierowanie do komisji lekarskiej nastąpiło na wniosek funkcjonariusza,
- 8) upływu 12 miesięcy od dnia zaprzestania służby z powodu choroby,
- 9) nabycia obywatelstwa innego państwa.

W ustawie o służbie w SKW oraz SWW powyższe przesłanki zostały uzupełnione o dodatkową przesłankę fakultatywnego zwolnienia ze służby, tj. nieobecność funkcjonariusza w służbie przez okres powyżej trzech miesięcy z powodu tymczasowego aresztowania. Należy wskazać, że w ustawie o ABW oraz AW nieobecność funkcjonariusza w służbie powyżej trzech miesięcy z powodu tymczasowego aresztowania stanowi przesłankę stwierdzenia wygaśnięcia stosunku służbowego, o ile wcześniej nie nastąpiło zwolnienie ze służby⁴⁴.

W ustawie o CBA występują pewne różnice w określeniu przesłanek fakultatywnego zwolnienia ze służby w stosunku do pozostałych służb specjalnych. W pierwszej kolejności na uwagę zwraca fakt, że w przypadku funkcjonariuszy CBA ustawodawca nie przewidział fakultatywnej przesłanki zwolnienia ze służby z uwagi na „ważny interes” służby. Ponadto w przypadku funkcjonariuszy CBA oprócz przesłanek analogicznych, do określonych w ustawie o ABW oraz AW, fakultatywne zwolnienie funkcjonariusza ze służby może nastąpić również w przypadku:

- 1) tymczasowego aresztowania (niezależnie od okresu),
- 2) wniesienia aktu oskarżenia w przypadku umyślnego przestępstwa ściganego z oskarżenia publicznego,
- 3) niezłożenia w terminie oświadczenia, o którym mowa w art. 10 *ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne*,
- 4) popełnienia przestępstwa ściganego z oskarżenia publicznego, w sytuacji gdy okoliczności jego popełnienia nie budzą wątpliwości.

Wobec powyższego należy stwierdzić, że odpowiedzialność funkcjonariuszy CBA z jednej strony została zaostrzona w stosunku do funkcjonariuszy pozostałych służb specjalnych, albowiem sam fakt niezłożenia w terminie oświadczenia majątkowego lub wniesienie aktu oskarżenia w wypadku umyślnego przestępstwa, ściganego z oskarżenia publicznego, mogą stanowić podstawę do zwolnienia ze służby w tej formacji. Z drugiej strony, ustawodawca nie przewidział możliwości zwolnienia funkcjonariuszy CBA z uwagi na „ważny interes służby”, która to przesłanka, w związku z brakiem definicji legalnej, stanowi najdalej idące uprawnienie w ramach dyskrecjonalnej władzy organu w zakresie podstaw zwolnieniowych.

⁴⁴ Zob. art. 61 pkt. 2 ustawy o ABW oraz AW.

Przesłanką fakultatywnego zwolnienia ze służby we wszystkich służbach specjalnych jest niewywiązywanie się z obowiązków służbowych w okresie odbywania służby stałej, stwierdzone w dwóch kolejnych opiniach. Przy czym, w przypadku funkcjonariuszy ABW, AW, SKW i SWW pomiędzy wydaniem kolejnych dwóch opinii musi upłynąć okres co najmniej sześciu miesięcy. Ustawodawca założył zatem, że w tym stosunkowo długim okresie funkcjonariusz ma możliwość zmiany swojego postępowania, co może skutkować wydaniem pozytywnej opinii służbowej. Natomiast w ustawie o CBA nie wprowadzono minimalnego okresu, który musi upłynąć między wydanymi opiniami służbowymi.

Należy mieć na uwadze fakt, że w przypadku wystąpienia obligatoryjnej przesłanki zwolnienia ze służby ustawodawca posługuje się terminem opinii o „nieprzydatności do służby” w toku służby przygotowawczej, natomiast w wypadku opinii dokonywanej w toku służby stałej ustawodawca posługuje się terminem: „niewywiązywania się z obowiązków służbowych”. Według opinii M. Wieczorka ustawodawca słusznie wprowadził zróżnicowanie terminologiczne wymienionych przypadków zwolnienia ze służby. Opinia w służbie przygotowawczej ma bowiem na celu przede wszystkim ustalenie przydatności funkcjonariusza do służby. Natomiast opinia wydawana w służbie stałej ma na celu ocenę sposobu wykonywania obowiązków służbowych w okresie objętym opinią⁴⁵.

Zważywszy, iż omawiana przesłanka jest fakultatywną przesłanką zwolnienia ze służby, nawet w przypadku, gdy w stosunku danego funkcjonariusza, w ustawowym okresie, zostaną wydane dwie negatywne opinie służbowe, ale organ uzna, iż z okoliczności sprawy wynika, że postawa funkcjonariusza rokuje, iż w przyszłości będzie on wywiązywał się ze swoich obowiązków służbowych, wówczas nie wszczyna się postępowania w sprawie zwolnienia ze służby. Wobec powyższego wszczęcie procedury zwolnieniowej zależy będzie od dyskrejonalnej władzy właściwego przełożonego, z zastrzeżeniem, iż warunkiem *sine qua non* do ziszczenia się tej władzy będzie zawsze wydanie dwóch negatywnych opinii służbowych.

Przesłanką fakultatywnego zwolnienia ze służby w służbach specjalnych jest również prawomocne skazanie za przestępstwo, inne niż implikujące zwolnienie obligatoryjne (tj. umyślne ścigane z oskarżenia publicznego). W przypadku zaistnienia takiej przesłanki podstawę zwolnienia ze służby stanowić będzie zatem stwierdzone prawomocnym wyrokiem karnym popełnienie przestępstwa nieumyślnego lub przestępstwa umyślnego, ściganego z oskarżenia prywatnego.

Kolejną fakultatywną przesłanką zwolnienia ze służby w ABW, AW, SWW i SKW jest objęcie przez funkcjonariusza kierowniczego stanowiska państwowego albo objęcie funkcji z wyboru w organach samorządu terytorialnego. *Ratio legis* tego przepisu jest zapewnienie apolityczności formacji mundurowych. Zagadnienie to łączy się w sposób oczywisty z zakazem członkostwa funkcjonariuszy w partiach politycznych, a przez to i z ograniczeniem wolności zrzeszania się, zagwarantowanej w art. 58 Konsytucji RP⁴⁶.

⁴⁵ M. Wieczorek, *Charakter prawny...*s. 259.

⁴⁶ Tamże, s. 279.

Ponadto, jak wskazuje P. Szustakiewicz, *oczywistym jest, że objęcie danego stanowiska państwowego lub funkcji w samorządzie terytorialnym może prowadzić do konfliktu interesów i związanego z tym podejrzenia o stronnictwo przy wykonywaniu zadań przez daną służbę. Tak sytuacja może być negatywnie odbierana przez społeczeństwo i jako taka naruszać dobre imię służby*⁴⁷. W tym miejscu warto przypomnieć, iż objęcie przez funkcjonariusza kierowniczego stanowiska państwowego albo objęcie funkcji z wyboru w organach samorządu terytorialnego stanowi obligatoryjną przesłankę do zwolnienia ze służby CBA. Za przyjęciem bardziej rygorystycznych wymogów w stosunku do funkcjonariuszy CBA z całą pewnością przemawia charakter zadań wykonywanych przez tę służbę oraz brzmienie art. 73 ust. 2 ustawy o CBA, który stanowi wprost, że: *funkcjonariusz CBA nie może pełnić funkcji publicznej*.

Pragmatyki służbowe przewidują możliwość dla organu zwolnienia ze służby funkcjonariusza, który osiągnął emeryturę w pełnym wymiarze na podstawie przepisów odrębnych⁴⁸. Nabycie prawa do emerytury w pełnym wymiarze jest zatem w służbach mundurowych zdarzeniem na tyle doniosłym prawnie, że stanowi fakultatywną przesłankę do zwolnienia ze służby. W wyroku z 31 stycznia 2020 r. (II SA/Wa 1457/19) WSA w Warszawie podkreślił, że *specyfika służb mundurowych wymaga, aby funkcjonariusz po stosunkowo długim okresie służby przeszedł na emeryturę, a ustawodawca może wprowadzić pewne ograniczenia, z czego powinien zdawać sobie sprawę funkcjonariusz, który decyduje się świadomie na podjęcie służby*.

Przy czym, decyzję o pozostawieniu funkcjonariusza w służbie lub wszczęciu procedury zwolnieniowej właściwy przełożony podejmie po dokonaniu weryfikacji okoliczności danej sprawy, w tym oceny dalszej przydatności w służbie danego funkcjonariusza, z uwzględnieniem zasad racjonalnej polityki kadrowej, pozwalającej na prawidłową realizację zadań. Nie zawsze bowiem w interesie służby będzie zwolnienie osoby, która osiągnęła pełny wiek emerytalny. Jak słusznie bowiem zauważył WSA w Poznaniu w wyroku z 31 stycznia 2018 r. (sygn. akt IV Sa/Po 960/17)⁴⁹: *to przełożony funkcjonariusza może zadecydować, biorąc pod uwagę wszelkie okoliczności sprawy, czy skorzystać z przysługującego prawa, czy też z uwagi na indywidualne cechy funkcjonariusza, pomimo przewidzianej wyraźnie prawem możliwości przejścia na emeryturę pozostawić funkcjonariusza w służbie*. Zatem zwolnienie funkcjonariusza ze służby w związku z osiągnięciem pełnej wysługi emerytalnej nie będzie zależne od woli funkcjonariusza, czy też wyrażenia przez niego gotowości do dalszej realizacji zadań służbowych, ale od oceny dokonanej przez organ.

⁴⁷ P. Szustakiewicz, *Stosunki służbowe*, s. 289.

⁴⁸ Zob. *ustawa z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin* (Dz.U. 2020, poz. 723, ze zm.).

⁴⁹ Wyrok wydany na gruncie ustawy o Policji.

Przesłanką fakultatywnego zwolnienia ze służby w ABW, AW, SKW oraz SWW jest zwolnienie z uwagi na ważny interes służby. Pojęcie „ważny interes służby” jest terminem nieokreślonym na gruncie przepisów prawa. Z powyższych względów przesłanka ta musi zostać każdorazowo skonkretyzowana na gruncie okoliczności danej sprawy. Przy czym przy odczytywaniu treści powyższego terminu należy sięgnąć przede wszystkim do przepisów regulujących cele i zadania danej służby mundurowej oraz szczególnie status funkcjonariuszy tej formacji.

Nie ulega wątpliwości, że zwolnienie ze służby z uwagi na tę przesłankę stanowi środek gwarantujący formacji mundurowej wypełnienie w optymalny sposób ustawowych zadań przy pomocy osób nie tylko odpowiednio przygotowanych zawodowo, ale i świadomych treści złożonego ślubowania. W rachubę może zatem wchodzić realnie istniejąca przyczyna albo okoliczności czy zdarzenia świadczące o tym, że dalsze pozostawianie funkcjonariusza w służbie koliduje z jej interesem⁵⁰. Naczelny Sąd Administracyjny w wyroku z 5 grudnia 2014 r. (sygn. I OSK 1629/13), wydanym na gruncie analogicznego przepisu ustawy o Policji, wskazał, że: *przez ważny interes służby” uzasadniający zwolnienie ze służby należy rozumieć sytuację, w której pierwszeństwo ochrony przysługuje formacji, nawet gdy następuje kosztem zwalnianego funkcjonariusza.*

Jak słusznie zaznaczył M. Wieczorek: *w pragmatykach, w których zawarty został przepis o możliwości fakultatywnego rozwiązania stosunku służby z uwagi na „ważny interes służby” ustawodawca wyposażył organ właściwy w sprawie osobowej w najdalej idące uprawnienie w zakresie ochrony interesu publicznego, utożsamianego z interesem służby*⁵¹. W praktyce, na podstawie tego przepisu, dokonuje się zwolnień takich funkcjonariuszy, którzy w ocenie przełożonych nie powinni z przyczyn pozamerytorycznych pełnić dalej służby, a nie można ich zwolnić na innej podstawie prawnej⁵².

W orzecznictwie nie budzi wątpliwości fakt, że można zwolnić funkcjonariusza ze względu na ważny interes służby z powodu długotrwałego przebywania na zwolnieniach lekarskich lub innych licznych absencji, pod warunkiem że organ wykaże, iż taka sytuacja w istocie dezorganizuje funkcjonowanie jednostki, w której ten funkcjonariusz pełni służbę⁵³. W wyroku z 9 lutego 2016 r. (sygn. I OSK 2855/14) NSA wskazał, że: *(...) Funkcjonariuszka ABW, która nie podejmuje służby i nie wykonuje żadnych obowiązków służbowych z uwagi na przebywanie na długotrwałych zwolnieniach lekarskich, a ponadto w świetle orzeczeń komisji lekarskich, wykazuje zdolność do pełnienia służby, przy jednoczesnym braku podstaw do zaliczenia do grupy inwalidzkiej nie może skutecznie powoływać się na swój interes.*

⁵⁰ Zob. wyrok NSA z dnia 14 III 2017 r., I OSK 397/16, wydany na gruncie przepisów ustawy o Policji.

⁵¹ M. Wieczorek, *Charakter prawny...*, s. 288.

⁵² Zob. m.in. wyrok NSA z dnia 18 XI 2013 r., I OSK 2281/12, wydany na gruncie przepisów ustawy o Policji.

⁵³ Zob. wyrok NSA z dnia 22 X 2008 r., I OSK 1583/07, oraz wyrok WSA w Warszawie z dnia 24 VI 2014 r., II SA/Wa 721/14.

Przesłanką do zwolnienia ze służby, z uwagi na ważny interes służby, będzie również utrata przez funkcjonariusza poświadczenia bezpieczeństwa, uprawniającego do dostępu do informacji niejawnych. W interesie służby leży bowiem, aby ustawowe zadania Agencji, która jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, realizowane były przez osoby spełniające wymagania stawiane przez przepisy ustawy o ABW oraz AW. Brak po stronie funkcjonariusza uprawnień do dostępu do informacji niejawnych oznaczonych klauzulami „ŚCIŚLE TAJNE” i „TAJNE” oraz „POUFNE” oznacza brak możliwości pełnienia służby w ABW⁵⁴. Podstawą do wszczęcia postępowań zwolnieniowych w takich sprawach są ostateczne decyzje o cofnięciu poświadczeń bezpieczeństwa, wydane zgodnie z przepisami u. inf. niejaw.⁵⁵

Zważywszy, że funkcjonariusz, któremu odebrano poświadczenie bezpieczeństwa, niewątpliwie utracił jeden z warunków *sine qua non* pełnienia służby, o którym mowa w art. 44 pkt. 4 ustawy o ABW oraz AW, zasadne wydaje się rozważenie możliwości wprowadzenia zmian do obowiązujących regulacji prawnych, polegających na uzupełnieniu katalogu obligatoryjnych podstaw zwolnienia ze służby, o przesłankę utraty rękojmi zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych.

Nie budzi bowiem wątpliwości fakt, że osoba, która nie daje rękojmi zachowania tajemnicy w zakresie dostępu do informacji niejawnych, nie może dalej pełnić służby. Postępowanie w sprawie zwolnienia w takim przypadku powinno zatem mieć charakter obligatoryjny, tj. samo wystąpienie powyższej przesłanki powinno stanowić podstawę do zwolnienia ze służby, bez konieczności dokonywania przez organ oceny wszystkich okoliczności sprawy.

Przesłanką fakultatywnego zwolnienia ze służby jest również likwidacja jednostki organizacyjnej lub jej reorganizacja, połączona ze zmniejszeniem obsady etatowej, jeżeli przeniesienie funkcjonariusza do innej jednostki organizacyjnej lub na niższe stanowisko służbowe nie jest możliwe. Powyższa przesłanka do zwolnienia stanowi potwierdzenie tezy o wyjątkowej trwałości stosunku służbowego. Należy bowiem wskazać, że w przypadku reorganizacji lub likwidacji jednostki organ w pierwszej kolejności ma obowiązek zapewnienia funkcjonariuszowi innego stanowiska. Jeżeli jednak okaże się to niemożliwe, do faktycznego zwolnienia dochodzi nie w momencie likwidacji lub reorganizacji jednostki, ale dopiero po upływie okresu ochronnego, określonego w art. 60 ust. 4 ustawy o ABW oraz AW. Przy czym okres ochronny zależy od rodzaju służby funkcjonariusza — w służbie przygotowawczej wynosi on trzy miesiące, natomiast w służbie stałej sześć miesięcy.

Specyfika zadań wykonywanych przez funkcjonariuszy służb mundurowych wymaga, aby służbę pełniły osoby zdrowe i sprawne fizyczne. Dlatego też funkcjonariusze nie tylko przed przyjęciem do służby, ale również w jej trakcie, mają obowiązek poddawać się badaniom lekarskim określającym ich zdolność do służby.

⁵⁴ Zob. wyrok WSA w Warszawie, II SA/Wa 2732/19.

⁵⁵ Dz.U. 2019, poz. 742, ze zm.

W razie wystąpienia okoliczności uprawdopodobniających utratę takiej zdolności właściwy przełożony powinien zainicjować postępowanie przed komisją lekarską w celu ustalenia psychofizycznej przydatności funkcjonariusza do dalszego pełnienia służby. W związku z powyższym przesłanką fakultatywną do zwolnienia ze służby w służbach specjalnych jest dwukrotne nieusprawiedliwione niestawienie się na badania w celu określenia stanu zdrowia oraz ustalenia zdolności fizycznej i psychicznej do służby, jak również związku poszczególnych chorób ze służbą, oraz dwukrotne nieusprawiedliwione niestawienie się na obserwację w zakładzie opieki zdrowotnej, w przypadku wyrażenia zgody przez funkcjonariusza. Przesłanką zwolnienia ze służby na tej podstawie nie będzie sytuacja, w której skierowanie do komisji lekarskiej nastąpiło na wniosek samego funkcjonariusza.

Następną fakultatywną przesłanką do zwolnienia ze służby, która występuje w pragmatykach wszystkich służb specjalnych, jest wpływ 12 miesięcy od dnia zaprzestania służby z powodu choroby. Okres 12 miesięcy jest bardzo długim czasem, w którym funkcjonariusz nie wykonuje swoich zadań służbowych. Nie ulega wątpliwości, że tak długa absencja może mieć negatywny wpływ na pracę danej jednostki i zaburzać jej sprawne funkcjonowanie. Ustawodawca zdecydował się na wprowadzenie relatywnie długiego okresu ochronnego dla funkcjonariusza przed zwolnieniem, co jest kolejnym odzwierciedleniem tezy o wyjątkowej trwałości stosunku służbowego. Wskazać przy tym należy, iż w orzecznictwie przyjmuje się, że przy liczeniu okresu pozwalającego na zwolnienie funkcjonariusza nie chodzi o nieprzerwany okres zwolnienia lekarskiego, ale o nieprzerwany okres niepełnienia służby, której zaprzestanie nastąpiło z powodu choroby. Przełożony powinien wykazać w decyzji o zwolnieniu, że funkcjonariusz mimo krótkotrwałych przerw między zwolnieniami lekarskimi faktycznie nie wykonywał obowiązków służbowych przez okres 12 miesięcy⁵⁶.

Ostatnią z przesłanek fakultatywnego zwolnienia ze służby w ABW, AW, SWW i SKW jest nabycie obywatelstwa innego państwa. Przy czym, w przypadku wszczęcia procedury w przedmiocie zwolnienia ze służby na tej podstawie organ powinien w uzasadnieniu rozkazu wykazać, że w świetle okoliczności faktycznych nabycie obywatelstwa innego państwa będzie miało na tyle negatywny wpływ na interes służby, że uniemożliwia dalsze jej pełnienie. W CBA, jak już wspomniano, nabycie przez funkcjonariusza obywatelstwa innego państwa stanowi obligatoryjną przesłankę do zwolnienia ze służby. Wobec powyższego sam fakt nabycia obywatelstwa innego kraju będzie powodował konieczność zwolnienia funkcjonariusza ze służby w tej formacji.

Podsumowanie

Stosunek prawny, który określa prawa i obowiązki funkcjonariuszy ABW jest stosunkiem o charakterze administracyjnoprawnym. Nazywany jest stosunkiem służbowym i dotyczy funkcjonariuszy służb specjalnych oraz innych

⁵⁶ Zob. wyrok WSA w Warszawie z dnia 8 I 2015 r., II SA/Wa 145/14.

służb mundurowych. Cechami tego stosunku jest brak równoprawności stron (organ w sposób władczy może kształtować sytuację prawną funkcjonariusza), szczególnie rodzaj podporządkowania, ponadprzeciętna dyspozycyjność oraz obowiązek wykonywania zadań służbowych z narażeniem życia lub zdrowia. Sprawy z zakresu stosunku służbowego załatwiane są na podstawie przepisów Kodeksu postępowania administracyjnego oraz przepisów pragmatyk służbowych, a rozstrzygnięcia władcze położonych wobec funkcjonariuszy (decyzje administracyjne) poddawane są kontroli sądów administracyjnych.

Stosunek służbowy cechuje znacznie większa trwałość niż w przypadku stosunków zatrudnienia opartych na prawie pracy lub prawie cywilnym. Funkcjonariusz służb mundurowych może zostać zwolniony ze służby tylko w przypadkach enumeratywnie wymienionych w ustawach pragmatycznych. Trwałość tego stosunku wynika z niezmienności zadań, które państwo powierzyło do wykonywania służbom mundurowym, tj. z zakresu szeroko pojętej ochrony bezpieczeństwa państwa zarówno w jego zewnętrznym, jak i wewnętrznym aspekcie.

Pragmatyki służbowe przewidują obligatoryjne oraz fakultatywne przesłanki zwolnienia ze służby. Przesłanki zwolnienia ze służby w przepisach pragmatycznych służb specjalnych zostały ukształtowane w podobny sposób. W zasadzie tożsame przepisy, regulujące omawianą materię, znajdują się w ustawie o ABW oraz AW oraz w ustawie o służbie w SKW i SWW. Pewne odrębności, w powyższym zakresie, zostały uregulowane w ustawie o CBA. W ustawie o CBA katalog obligatoryjnych oraz fakultatywnych przesłanek do zwolnienia ze służby jest bardziej obszerny niż w pozostałych służbach specjalnych. Niemniej jednak w ustawie o CBA jako jedynej służbie specjalnej ustawodawca nie przewidział możliwości rozwiązania stosunku służbowego z uwagi na „ważny interes służby”.

Należałoby rozważyć zmianę katalogu przesłanek obligatoryjnego zwolnienia ze służby określonych w ustawie o ABW oraz AW. Zasadne wydaje się bowiem wprowadzenie do wspomnianego katalogu przesłanki obligatoryjnego zwolnienia ze służby z uwagi na utratę rękojmi zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych. Funkcjonariusz, który utraci poświadczenie bezpieczeństwa, nie może dalej pełnić służby w ABW, a zatem utrata powyższego atrybutu służby powinna prowadzić do obligatoryjnego rozwiązania stosunku służby.

Renata Klejc

Rozdział 11.

Szef ABW jako podmiot zobowiązany do udostępniania informacji publicznej w trybie *ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej* na tle dotychczasowej praktyki orzeczniczej sądów administracyjnych

Dostęp do informacji publicznej — kontekst konstytucyjny

Prawo dostępu do informacji publicznej jest podmiotowym prawem każdego obywatela o szczególnym znaczeniu ustrojowym. Jako prawo o charakterze politycznym rozpatrywać je należy w kontekście zasad ustrojowych, jakimi są zasada zwierzchniej władzy narodu urzeczywistniona w formach demokracji przedstawicielskiej bądź bezpośredniej (art. 4 Konstytucji RP), sprawowanej w ramach demokratycznego państwa prawnego (art. 4 Konstytucji RP), z istotnym udziałem samorządu terytorialnego (art. 16 ust. 2 Konstytucji RP), a w dalszej kolejności także z udziałem samorządu zawodowego i innych rodzajów samorządu (art. 17 Konstytucji RP). U jego podstaw leżą wartości, wśród których istotną rolę odgrywa jawność ukierunkowana na to, aby działanie instytucji publicznych cechowało się rzetelnością i sprawnością¹ oraz było podejmowane na podstawie i w granicach prawa², z poszanowaniem i ochroną przyrodzonej i niezbywalnej godności człowieka³, przy równym traktowaniu przez władze publiczne⁴, które

¹ Preambuła Konstytucji zakłada m.in., że jej ustanowienie ma zapewnić instytucjom publicznym rzetelność i sprawność działania.

² Art. 7 Konstytucji statuuje zasadę legalizmu, zgodnie z którą organy władzy publicznej mogą działać wyłącznie na podstawie i w granicach prawa.

³ Art. 30 Konstytucji stanowi, iż przyrodzona i niezbywalna godność człowieka stanowi źródło wolności praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych.

⁴ Art. 32 ust. 1 Konstytucji.

to władze nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym⁵.

W literaturze fachowej⁶ podkreśla się, że świadomy udział obywateli w życiu społeczeństwa i państwa jest nieodzowny w ustroju demokratycznym, a jego zakres w ogromnym stopniu zależy od stanu wiedzy całej zbiorowości o problemach narodu i państwa. Dla współdziałania obywateli w procesie rządzenia konieczne jest zatem zapewnienie dostępu do informacji o wykonywaniu zadań publicznych, jak i podejmowanie przez państwo innych działań zmierzających do wymiany informacji między władzą a obywatelami.

Przepis art. 61 Konstytucji RP, który ustanawia prawo dostępu do informacji publicznej, został umieszczony w Rozdziale II ustawy zasadniczej (*Wolności, prawa i obowiązki człowieka i obywatela, podrozdział pt. Wolności i prawa polityczne*), co nie jest przypadkowe, i podkreśla polityczny wymiar prawa, odróżniając je od wolności i praw pokrewnych. Zauważyć bowiem należy, iż prawo dostępu do informacji publicznej, rozumianej jako informacja o działalności organów władzy publicznej, stanowi niezbędną przesłankę zaistnienia społeczeństwa obywatelskiego, co w dalszej kolejności prowadzi do umocnienia demokratycznych zasad funkcjonowania władzy w polskim państwie prawnym. Dostęp do informacji z jednej strony zapewnia zatem możliwość efektywnego sprawowania społecznej kontroli nad działaniami organów władzy publicznej, z drugiej zaś jest warunkiem świadomego uczestnictwa obywateli w podejmowaniu rozstrzygnięć przez władze publiczne.

Usytuowanie prawa do informacji w Konstytucji RP ma ponadto uzasadnienie w ścisłym jego powiązaniu z innymi politycznymi prawami obywatelskimi, jak chociażby z czynnym prawem wyborczym. Jakkolwiek bowiem realizacja prawa do informacji nie wpływa bezpośrednio na prace wymienionych w art. 61 ust. 1 i 2 ustawy zasadniczej organów władzy publicznej ani nie rozciąga się na możliwość wywoływania jakiegokolwiek formy nacisku na przejawy ich działalności, ale może wywołać ten skutek przy wykorzystaniu innych praw obywatelskich. Dlatego też nie do przecenienia jest powszechność i równość dostępu do informacji publicznej w społeczeństwie demokratycznym, w którym obywatele mają prawo być informowani o tym, co i dlaczego czynią władze publiczne.

Przejrzystość procesu decyzyjnego umacnia demokratyczny charakter instytucji oraz zaufanie obywateli do administracji. Owa społeczna kontrola wydaje się być szczególnie istotna w obszarach, w których ingerencja organów władzy publicznej w życie obywateli jest na tyle daleko idąca, że godzi w inne podstawowe prawa obywatelskie, jak to nierzadko dzieje się w odniesieniu do działań służb specjalnych. Oczywiście może mieć ona miejsce przy założeniu, że nie uniemożliwi skutecznego działania służb i nie dotyczy konkretnych prowadzonych postępowań czy stosowanych w nich metod operacyjnych, ale też, że

⁵ Art. 51 ust. 2 Konstytucji.

⁶ W. Skrzydło, *Konstytucja, komentarz do art. 61*, LEX; A. Piskorz-Ryń, zob. w: *Jawność i jej ograniczenia*, red. Z. Kmiecik, Warszawa 2013.

potencjalne ujawnienie wnioskowanych informacji nie zagrozi porządkowi i bezpieczeństwu publicznemu lub nie narazi na szwank działania organów chroniących te wartości⁷, co wymaga wyznaczenia precyzyjnej granicy między informacjami publicznymi, które mogą zostać ujawnione i tymi, które, ze względów ważniejszych niż prawo do informacji, powinny pozostać chronione.

Pojęcie informacji publicznej

Ustawa zasadnicza nie wprowadza wprost pojęcia „informacja publiczna”, niemniej rekonstruując jego znaczenie na podstawie brzmienia art. 61 Konstytucji RP, stwierdzić należy, iż ustawodawca oparł je na odczytywanych łącznie kryteriach podmiotowym i przedmiotowym. Kryterium podmiotowe wskazuje, że informacja taka odnosi się do działalności organów władzy publicznej rozumianych jako organy władzy ustawodawczej, wykonawczej i sądowniczej oraz osób pełniących funkcje publiczne, a także organów samorządu gospodarczego i zawodowego, jak również innych podmiotów wykonujących zadania publiczne. Działalność ta z definicji polega na wykonywaniu zadań publicznych i to bez względu na formę, w jakiej ma to miejsce, a zatem odnosi się do wszelkich przejawów aktywności stosowanych w celu realizacji kompetencji przypisanych tym organom lub osobom. Kryterium przedmiotowe nie zostało określone wprost, niemniej przyjmuje się, że informacja taka winna być przechowywana przez władze publiczne bądź też owe inne podmioty wykonujące zadania publiczne⁸. Zdaniem W. Sokolewicz przyjąć należy, iż zgodnie z intencją ustrojodawcy każda informacja wytworzona, przetworzona lub znajdująca się w posiadaniu władz publicznych bądź innych podmiotów wykonujących zadania publiczne jest *eo ipso* „informacją w sprawach publicznych”⁹.

Pojęcie „informacja publiczna” pojawia się w art. 1 ust. 1 *ustawy z dnia 6 września o dostępie do informacji publicznej*¹⁰. Zgodnie z tym przepisem informację publiczną stanowi każda informacja o sprawach publicznych. W doktrynie¹¹ zwraca się uwagę na błąd logiczny przy definiowaniu tego pojęcia, który polega na wyjaśnianiu definiowanego terminu (*definiendum*) — za pośrednictwem innego, także o nieokreślonym zakresie znaczeniowym (łac. *ignotum per ignotum*). Także art. 6 u. inf. publ., zawierający katalog informacji publicznych podlegających udostępnieniu, mając charakter jedynie przykładowy, na co

⁷ Wyrok NSA z dnia 18 V 2011 r., I OSK 198/11, Centralna Baza Orzeczeń Sądów Administracyjnych.

⁸ M. Jaśkowska, *Dostęp do informacji publicznej w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002, s. 28–29.

⁹ W. Sokolewicz, *Komentarz do art. 61 Konstytucji*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. 4, Warszawa 2005.

¹⁰ *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej* (Dz.U. 2020, poz. 2176).

¹¹ M. Jaśkowska, *Pojęcie informacji publicznej i jej rodzaje*, „Kwartalnik Prawa Publicznego” 2012, nr 3, s. 59.

wskazuje użyty tam zwrot „w szczególności”, nie pozwala na precyzyjne odtworzenie znaczenia tego pojęcia. Na tym tle, głównie w orzecznictwie, wypracowano dwa sposoby definiowania pojęcia „informacja publiczna”.

Pierwszy, spotykający się z szerszą aprobatą, o charakterze podmiotowym, opiera się na założeniu, że zakres przedmiotowy i podmiotowy informacji publicznej wynika z samej Konstytucji RP, a ustawa o dostępie do informacji publicznej, zgodnie z art. 61 ust. 4 Konstytucji RP, określa jedynie tryb jej udzielania. Tym samym pojęcie „informacja publiczna” nie może opierać się wyłącznie na brzmieniu art. 1 ust. 1 u. inf. publ., bez uwzględnienia treści art. 61 ust. 1 i 2 Konstytucji RP. Odwołanie się wyłącznie do wykładni językowej mogłoby bowiem w tym przypadku prowadzić do zawężającego rozumienia tego terminu, a w konsekwencji do przyjęcia, że informacją publiczną jest wyłącznie wiadomość odnosząca się do spraw zbiorowości, nieobejmująca spraw indywidualnych rozstrzyganych decyzją administracyjną. Pozostawałoby to w sprzeczności nie tylko z art. 61 Konstytucji RP, który każdemu gwarantuje dostęp do informacji o działalności podmiotów publicznych i to bez względu na to, kogo ta działalność dotyczy, ale byłoby również niespójne z przepisami ustawy o dostępie do informacji publicznej, w szczególności w kontekście wyłączeń z art. 5 i wyliczenia z art. 6.

Przyjmując takie ujęcie zakłada się, że informacją publiczną jest każda wiadomość wytworzona lub odnoszona do władz publicznych, a także wytworzona lub odnoszona do innych podmiotów wykonujących funkcje publiczne, w zakresie wykonywania przez nie zadań władzy publicznej i gospodarowania mieniem komunalnym lub mieniem Skarbu Państwa¹². Informację publiczną stanowić będzie również treść wszelkiego rodzaju dokumentów odnoszących się do organu władzy publicznej lub podmiotu niebędącego organem władzy publicznej, związanych z nimi bądź w jakikolwiek sposób ich dotyczących. Są nią zarówno treści dokumentów bezpośrednio przez nie wytworzone, jak i te, których używają przy realizacji przewidzianych prawem zadań, nawet gdy nie pochodzą wprost od nich. Niewątpliwie chodzi zatem o dokumenty służące realizacji zadań publicznych przez organ i odnoszące się do niego bezpośrednio. Podkreśla się przy tym, że dokumentów tych nie można sprowadzać do dokumentów urzędowych, co do zasady bowiem udostępnieniu podlegają wszystkie dokumenty znajdujące się w aktach postępowania, niezależnie od tego, czy są to dokumenty urzędowe czy prywatne. Bez znaczenia pozostaje również to, czy dokument znajdujący się w aktach ma charakter „wewnętrzny” czy „roboczy”¹³. Nie ma również znaczenia, jaką formą prawną posługują się organy administracji i czy dotyczy działania administracyjnoprawnego, czy cywilnoprawnego. Zwraca się również uwagę, że decydujące dla uznania informacji za informację

¹² Wyrok WSA w Warszawie z dnia 22 IX 2020 r., II SA/Wa 422/20, Centralna Baza Orzeczeń Sądów Administracyjnych.

¹³ Wyrok NSA z dnia 1 XII 2011 r., I OSK 1550/11, Centralna Baza Orzeczeń Sądów Administracyjnych.

publiczną nie jest jej wytworzenie przez organ władzy publicznej, ale fakt, że została uzyskana bądź przetworzona w celu realizacji zadań publicznych.

W orzecznictwie podkreśla się, że na gruncie ustawy o dostępie do informacji publicznej zobowiązanie do udzielenia informacji ogranicza się do informacji, która znajduje się w posiadaniu organu i której używa on do zrealizowania powierzonych prawem zadań. Informacja ta może dotyczyć tylko faktów zaistniałych, tj. takich, które wystąpiły w chwili udzielania informacji i mają bądź miały wpływ na sferę publiczną. Prawo dostępu do informacji publicznej nie obejmuje natomiast prawa do żądania udzielenia informacji o niezmaterializowanych w jakiegokolwiek postaci zamierzeniach podejmowania określonych działań¹⁴. W tym kontekście warty przytoczenia jest pogląd wyrażony przez NSA, zgodnie z którym dopóki określona informacja istnieje tylko w pamięci przedstawiciela władzy publicznej i nie została utrwalona w jakiegokolwiek formie, tak aby można było w sposób niebudzący wątpliwości odczytać jej treść, dopóty informacja taka nie ma waloru informacji publicznej. Informacja publiczna nie może być w szczególności przedmiotem poszukiwań i dociekań ze strony organu, które prowadziłyby do jej wytworzenia¹⁵. Wniosek nie może dotyczyć również przyszłych działań organów w sprawach indywidualnych ani też być postulatem wszczęcia postępowania w jakiejś innej sprawie, np. cywilnej czy karnej¹⁶. W trybie ustawy o dostępie do informacji publicznej nie można domagać się również dokonywania przez organ wykładni prawa¹⁷ czy też wyjaśniania treści aktów¹⁸, natomiast udostępnieniu podlegają już dane dotyczące projektowania aktów normatywnych, w tym w szczególności dane dotyczące przedmiotu regulacji, podmiotów uczestniczących i odpowiedzialnych za jego tworzenie czy etapów, na jakich proces legislacyjny się znajduje.

Oprócz omówionego wyżej podmiotowego definiowania pojęcia „informacja publiczna” w orzecznictwie niekiedy pojawiało się również ujęcie przedmiotowe, odwołujące się do pojęcia „sprawa publiczna” utożsamianego w sensie prawnym ze wszystkimi działaniami (zaniechaniami) podmiotów realizujących zadania publiczne zaliczane do szeroko rozumianego interesu publicznego¹⁹. Ujęcie to zmierzało do wyłączenia z zakresu udostępnianych informacji spraw niepublicznych, osobistych, prywatnych, jak również dokumentów

¹⁴ Wyrok NSA z dnia 20 VI 2002 r., II SAB 70-71/02, Centralna Baza Orzeczeń Sądów Administracyjnych.

¹⁵ Wyrok NSA z dnia 14 IX 2012 r., I OSK 1177/12, Centralna Baza Orzeczeń Sądów Administracyjnych.

¹⁶ Wyrok WSA w Krakowie z dnia 16 XII 2019 r., II SAB/ Kr 400/19, LEX nr 2 771 558.

¹⁷ Postanowienie NSA z dnia 24 I 2006 r., I OSK 928/05, Centralna Baza Orzeczeń Sądów Administracyjnych.

¹⁸ Wyrok NSA z dnia 27 IX 2002 r., II SAB 180/02, Centralna Baza Orzeczeń Sądów Administracyjnych.

¹⁹ Wyrok NSA z dnia 7 X 2009 r., I OSK 209/09, Centralna Baza Orzeczeń Sądów Administracyjnych.

wewnętrznych, nieodnoszących się do spraw publicznych, jak np. wewnętrzna korespondencja urzędowa²⁰.

Niemniej, jak już wskazywano, ujęcie przedmiotowe nie spotyka się z powszechną aprobatą, bowiem większość doktryny i orzecznictwa opowiada się za szerokim określeniem znaczenia pojęcia „informacja publiczna”, jako bardziej odpowiadającego celowi regulacji. Jak zauważa M. Jaśkowska:

zasadą jest bowiem transparentność działań organów publicznych, a ochrona dóbr innych podmiotów, a także zapobieganie przejawom nadużycia prawa, może być osiągane w innym trybie. Pierwszym z nich służy instytucja odmowy udostępnienia w drodze decyzji z uwagi na tajemnicę prawnie chronione, drugim — odmowa ze względu na brak spełnienia warunków do udzielenia informacji przetworzonej, czy też możliwość odmowy udostępnienia informacji wymagających podejmowania nieproporcjonalnych działań przekraczających proste czynności techniczne²¹.

Przychylając się do poglądu większości, uznać należy, iż ogół działalności Agencji Bezpieczeństwa Wewnętrznego, w tym działalność operacyjna jej funkcjonariuszy, jako dotycząca wykonywania ustawowych uprawnień organu w sferze jego działalności obejmującej ochronę bezpieczeństwa wewnętrznego państwa, mieści się w pojęciu „informacji publicznej”²². Podkreślić jednocześnie należy, iż dysponowanie przez organ informacją o charakterze informacji publicznej nie oznacza automatyzmu w jej udostępnianiu z uwagi na ustawowe ograniczenia w tym zakresie²³. Przepis art. 5 ust. 1 u. inf. publ. stanowi bowiem,

²⁰ W wyroku z dnia 16 VI 2009 r., I OSK 89/09, NSA zaprezentował pogląd, że o zakwalifikowaniu opinii prawnej do dokumentów podlegających udostępnieniu w trybie ustawy o dostępie do informacji publicznej decyduje cel, w jakim została opracowana. Opinia prawna sporządzona na użytek organu administracji publicznej w przedmiocie zasadności wszczęcia w przyszłości postępowania w konkretnej sprawie cywilnej, nie stanowi informacji publicznej w rozumieniu art. 1 ust. 1 ustawy o dostępie do informacji publicznej. W dalszej części uzasadnienia sąd podkreślił, iż: *W rozpoznawanej sprawie żądana opinia prawna zawierała informację, która mogła, ale nie musiała, zostać wykorzystana przez organ administracji publicznej w przyszłości, w celu wszczęcia cywilnych postępowań w konkretnych sprawach przeciwko członkom Wspólnoty Mieszkaniowej. Nie dotyczyła więc ona sfery faktów, lecz sfery zamierzeń. Prawo dostępu do informacji publicznej obejmuje prawo żądania udzielenia informacji o określonych faktach i stanach istniejących w chwili udzielania informacji, nie zaś o niezmaterializowanych w jakiegokolwiek postaci zamierzeniach podejmowania określonych działań.*

²¹ M. Jaśkowska, *Pojęcie informacji publicznej i jej rodzaje*, „Kwartalnik Prawa Publicznego” 2012, nr 3, s. 70.

²² W wyroku z dnia 10 XI 2010 r., II SAB 279/10, WSA w Warszawie stwierdził ponadto, iż *wprawdzie istotą prowadzenia kontroli operacyjnej jest jej niejawność, co wynika z art. 27 ust. 6 ustawy o ABW oraz AW, jednak nie zmienia to faktu, iż tego rodzaju działalność jest wykonywana w ramach zadań publicznych, ochrony bezpieczeństwa państwa i porządku konstytucyjnego. (...) Działalność operacyjna funkcjonariuszy ABW mieści się zatem w pojęciu informacji publicznej.*

²³ Wyrok NSA z 18 V 2011 r., I OSK 198/11, Centralna Baza Orzeczeń Sądów Administracyjnych.

że prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych.

Informacja może mieć zatem charakter publiczny, ale nie podlegać udostępnieniu z uwagi na tajemnice prawnie chronione czy prawo do prywatności. Rozróżnienie to ma o tyle istotne znaczenie, iż w przypadku braku przynajmniej informacji publicznej wystarczy powiadomienie wnioskodawcy o tym fakcie. Wówczas może on bronić swojego stanowiska przez skargę na bezczynność organu²⁴. Natomiast w sytuacji, gdy dana informacja publiczna nie może podlegać udostępnieniu, organ zobowiązany jest wydać decyzję, od której służyć będzie skarga do sądu administracyjnego.

Tryby udostępniania informacji

Ustawa o dostępie do informacji publicznej przewiduje cztery odrębne sposoby udostępniania informacji publicznych. Pierwszy z nich, uznany przez ustawodawcę za podstawowy, to udostępnianie informacji w drodze ich publikacji w urzędowym publikatorze teleinformatycznym — Biuletynie Informacji Publicznej, prowadzonym w formie internetowych stron WWW. Jego uzupełnieniem jest umożliwienie przez ustawodawcę podmiotom zobligowanym do udostępniania informacji publicznych wykorzystania w tym celu wyłożenia lub wywieszenia informacji w miejscach ogólnie dostępnych oraz zainstalowanie w takich miejscach urzędów umożliwiających zapoznanie się z taką informacją. Tryb ten, w przeciwieństwie do udostępniania informacji w BIP, nie ma jednak charakteru obligatoryjnego i decyzję co do jego stosowania pozostawiono w gestii podmiotów zobowiązanych do udostępniania informacji publicznej.

Drugim przewidzianym przez ustawodawcę sposobem jest udzielanie informacji publicznych w postępowaniu wnioskowym, trzecim — umożliwienie wstępu na posiedzenia kolegialnych organów władzy publicznej pochodzących z wyborów powszechnych oraz udostępnianie materiałów, w tym audio-wizualnych i teleinformatycznych, dokumentujących te posiedzenia i w końcu

²⁴ W wyroku z dnia 7 VII 2010 r., I OSK 592/10, jaki zapadł w sporze między Agencją Bezpieczeństwa Wewnętrznego a Helsińską Fundacją Praw Człowieka dotyczącym charakteru informacji na temat liczby wniosków o zarządzenie kontroli operacyjnej NSA zauważył: *w orzecznictwie sądów administracyjnych utrwalił się pogląd, że skargę na bezczynność organu w postępowaniu o udzielenie informacji publicznej można złożyć nie tylko wobec „milczenia” organu, ale również w sytuacji, w której powstał spór między wnioskodawcą a adresatem wniosku, co do charakteru żądanej informacji. (...) Sąd Administracyjny do którego trafiła skarga na bezczynność pełni wobec tego rolę arbitra, który ma przede wszystkim przesądzić, czy wnioskodawca żąda informacji, o której mowa w art. 1 ust. 1 ustawy o dostępie do informacji publicznej i tym samym czy ustawa ta znajduje zastosowanie. Skarga na bez czynność w tego rodzaju sprawach chroni wnioskodawcę przed arbitralną decyzją organu, która uniemożliwia uzyskanie żądanej informacji.*

czwartym sposobem jest umieszczanie informacji publicznych w centralnym repozytorium informacji publicznych.

W związku z tym, że Szef Agencji Bezpieczeństwa Wewnętrznego jest organem zobowiązanym do udostępniania informacji publicznej jedynie z wykorzystaniem pierwszych dwóch wymienionych sposobów, z uwagi na zakres tematyczny niniejszej pracy, to do nich ograniczono omówienie zagadnienia.

Publikacja informacji publicznej w BIP

Jak już wspomniano, BIP tworzony jest w formie elektronicznej i udostępniany pod adresami witryn internetowych poszczególnych podmiotów, co umożliwia powszechny dostęp do bieżących informacji publicznych. Forma ta maksymalizuje krąg podmiotów mogących zapoznać się z opublikowaną informacją, a jej podstawową zaletą z punktu widzenia zainteresowanych jest łatwy, szybki oraz bezpłatny dostęp do informacji publicznej. Dodatkowym jej atutem jest umożliwienie swobodnego dostępu do zamieszczonych informacji, a co za tym idzie brak konieczności składania indywidualnego wniosku, co przekłada się na zminimalizowanie kosztów administracyjnych działania organów publicznych. Efektywności tej formy dostępu sprzyja wprowadzenie ujednoczonego systemu stron w sieci teleinformatycznej.

Organami zobowiązanymi do udostępniania informacji w ten sposób są wszystkie podmioty zobowiązane do udostępniania informacji na gruncie ustawy o dostępie do informacji publicznej. Zakres informacji umieszczanych w BIP obejmuje zagadnienia wymienione w art. 6 u. inf. publ., jakimi są informacje dotyczące polityki wewnętrznej i zagranicznej państwa, podmiotów zaliczanych do władz publicznych i innych podmiotów wykonujących zadania publiczne, zasad funkcjonowania tych podmiotów, danych publicznych i majątku publicznego, w tym w szczególności informacje dotyczące zamówień publicznych. Poza tym podmioty, o których mowa w art. 4 ust. 1 i 2 u. inf. publ., obowiązane są do umieszczania w BIP informacji dotyczących sposobu dostępu do informacji publicznych będących w ich posiadaniu, lecz nieudostępnionych w BIP. W BIP umieszczone mogą być również inne informacje publiczne niesprecyzowane bliżej w ustawie. Tym samym ustawodawca nie stworzył zamkniętego katalogu informacji, które mogą być publikowane.

Z punktu widzenia realizacji prawa dostępu do informacji oraz zapewnienia transparentności działania organów administracji publicznej szczególną uwagę zwrócić należy na treść art. 8 ust. 5 u. inf. publ, który określa zakres czynności, jakie organ powinien podjąć w związku z koniecznością ograniczenia dostępu do informacji z uwagi na wyłączenie jawności. Sytuacja taka wymaga precyzyjnego określenia zakresu wyłączenia, wskazania podstawy prawnej uzasadniającej jej dokonanie, jak również określenia organu lub osoby dokonujących tego wyłączenia. Dodatkowo, w przypadku ograniczenia prawa dostępu do informacji ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy, niezbędne jest określenie podmiotu, w interesie którego wyłączenia dokonano.

W kontekście oceny rzetelności i prawdziwości informacji szczególną uwagę zwrócić należy ponadto na regulację art. 8 ust. 6 u. inf. publ., który obliguje podmioty udostępniające informacje w BIP do oznaczenia podmiotu udostępniającego informację, podania danych określających tożsamość osoby, która wytworzyła informację lub odpowiada za jej treść, dołączenia danych określających tożsamość osoby, która wprowadziła informację do BIP, oznaczenia czasu wytworzenia informacji i czasu jej udostępnienia, jak również zabezpieczenia możliwości identyfikacji czasu rzeczywistego udostępnienia informacji.

Postępowanie wnioskowe

Procedury udostępniania informacji publicznych w BIP oraz w centralnym repozytorium uznane zostały przez ustawodawcę za podstawowe, co ma ten skutek, że dopiero w przypadku nieudostępnienia tam informacji po stronie zainteresowanych aktualizuje się uprawnienie do złożenia wniosku o udostępnienie informacji publicznej²⁵. Jak wskazał WSA w Szczecinie w wyroku z 3 września 2008 r.²⁶:

z art. 8 ust. 1 i art. 10 ust. 1 u. inf. publ. wynika, że BIP jest podstawowym źródłem zapoznania się z informacją publiczną i udostępnienie informacji publicznej w BIP wyłącza obowiązek ponownego jej udostępniania na wniosek zainteresowanego, czy w innych przewidzianych w ustawie formach (np. wyłożenia, wywieszenia). Natomiast wniosek zainteresowanego może spowodować po stronie dysponenta informacji obowiązek jej udostępnienia wyłącznie wtedy, gdy informacja ta nie została wcześniej udostępniona i nie funkcjonuje w obiegu publicznym, co nie pozwala zainteresowanemu zapoznać się z jej treścią inaczej, aniżeli wskutek złożenia wniosku do odpowiedniego organu o udzielenie informacji.

Wojewódzki Sąd Administracyjny w Warszawie za niezasadny uznał także wniosek o udzielenie informacji, którą zainteresowany posiada, stwierdzając że w takim przypadku kwestia dostępu do informacji wydaje się bezprzedmiotowa, a żądanie jako niezmiernie duże do uzyskania pewnych wiadomości wykracza poza przedmiot i cele ochrony przewidziane ustawą o dostępie do informacji publicznej²⁷.

W ustawie o dostępie do informacji publicznej nie wskazuje się jakichkolwiek wymagań formalnych wniosku. W szczególności nie wymaga się uzasadnienia faktycznego ani prawnego, jak również dokładnego zidentyfikowania

²⁵ W wyroku z dnia 26 XI 2013 r., III SAB/ Lu 605/13, WSA w Lublinie stwierdził: *Udostępnienie informacji publicznej w Biuletynie Informacji Publicznej wyłącza obowiązek jej udostępniania na wniosek zainteresowanego. Jeśli informacja publiczna, której domaga się zainteresowany podmiot, została upubliczniona, organ do którego skierowano odpowiedni wniosek, winien jedynie odesłać wnioskodawcę do publikatora.*

²⁶ Wyrok WSA w Szczecinie z dnia 3 IX 2008 r., II SA/Sz 505/08, Legalis nr 994 293.

²⁷ Wyrok WSA w Warszawie z dnia 11 III 2009 r., II SAB/Wa 194/08, Legalis nr 209 176.

wnioskodawcy, a jedynie w miarę precyzyjnego wskazania zakresu żądanych informacji²⁸ oraz miejsca i sposobu ich dostarczenia. Co do zasady wniosek powinien być złożony w formie pisemnej, od której to generalnej reguły ustawodawca przewidział wyjątek, dopuszczając możliwość ustanęgo złożenia wniosku w sytuacji, gdy informacja publiczna może być udzielona niezwłocznie. Przyjmuje się przy tym, że z zachowaniem reguły pisemności złożony jest również wniosek przesłany pocztą elektroniczną i to nawet, gdy do jego autoryzacji nie zostanie użyty podpis elektroniczny²⁹. Odformalizowanie trybu udzielania informacji powoduje zatem, że nie ma przeszkód, aby udzielić informacji na wniosek złożony pocztą elektroniczną, nawet gdy nie można ustalić jego adresata. Problem może jednak rodzić wniosek, który został skierowany w formie elektronicznej i uniemożliwia określenie nadawcy, a zarazem wnioskowana informacja jest informacją przetworzoną lub zachodzi potrzeba odmowy jej udostępnienia lub umorzenia postępowania. W takiej sytuacji podmiot zobowiązany powinien żądać od wnioskodawcy, aby jego wniosek pod względem zawartości odpowiadał wymogom pisma procesowego, o których mowa w art. 64 Kodeksu postępowania administracyjnego³⁰, z uwagi na ewentualność wydania decyzji administracyjnej.

Omawiając kwestię rozpatrywania wniosku o udostępnienie informacji publicznej, należy zaznaczyć, że ustawa reguluje w istocie dwa odmienne postępowania o różnym charakterze prawnym, a mianowicie pierwsze z tych postępowań dotyczy udzielenia informacji publicznej, co ma miejsce w formie czynności materialno-technicznej, drugie zaś toczy się w sprawie wydania decyzji administracyjnej, odmawiającej udzielenia informacji publicznej lub umarzającej postępowanie³¹. Samo złożenie wniosku o udostępnienie informacji publicznej nie wszczyna zatem postępowania administracyjnego, gdyż udostępnienie to nie jest dokonywane w formie decyzji administracyjnej. W postępowaniu tym przepisy Kodeksu postępowania administracyjnego nie znajdują zastosowania, bowiem informacja publiczna jest w takiej sytuacji po prostu udostępniana, co przybiera postać czynności materialno-technicznej. Jak jednak zauważył NSA w wyroku z dnia 10 grudnia 2018 r.³²:

²⁸ W wyroku z dnia 8 III 2017 r., I OSK 1312/15, NSA stwierdził, że niezwrócenie się przez Szefa ABW do wnioskodawcy o wyjaśnienie, co rozumie on przez nazwy własne ORANGE CRUSH, OAKSTAR czy partnerstwo BUFFALOGREEN, świadczy o niezindywidualizowanym sposobie rozpatrzenia sprawy i pewnym automatyzmie działania organu. Organ powinien bowiem ustalić, co przez podane nazwy rozumie wnioskodawca, który żąda informacji, jak również co publicznie przypisywane jest tym pojęciom w dostępnych zasobach.

²⁹ Wyrok WSA w Krakowie z dnia 7 II 2018 r., II SAB/Kr 1/18, Centralna Baza Orzeczeń Sądów Administracyjnych.

³⁰ *Ustawa w dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego* (Dz.U. 2021, poz. 735).

³¹ P. Szustakiewicz, *komentarz do art. 10*, w: M. Bidziński, M. Chmaj, P. Szustakiewicz, *Ustawa o dostępie do informacji publicznej. Komentarz*, wyd. 3, Warszawa 2018, Legalis.

³² Wyrok NSA z dnia 10 XII 2018 r. I OSK 1574/18, Centralna Baza Orzeczeń Sądów Administracyjnych.

sytuacja wygląda inaczej, gdy organ zamierza wydać decyzję o odmowie udostępnienia wnioskowanej informacji publicznej w trybie art. 16 ust. 1 u. inf. publ., bądź też umorzyć postępowanie na mocy art. 14 ust. 2 ustawy o dostępie do informacji publicznej lub też wydać jakiegokolwiek inny akt administracyjny, który wiązałby się z ustaleniem podmiotu, od którego pochodzi wniosek. Wówczas winien wymagać od wnioskodawcy usunięcia braków formalnych wniosku, w tym na przykład w postaci podpisu w trybie art. 64 § 2 kodeksu postępowania administracyjnego, jeśli podanie zostało wniesione drogą elektroniczną, bez bezpiecznego, „weryfikowanego podpisu”.

Jak wyjaśnił dalej NSA, zgodnie z art. 16 ust. 1 i 2 u. inf. publ. odmowa udostępnienia informacji publicznej oraz umorzenie postępowania o udostępnienie informacji w przypadku określonym w art. 14 ust. 2 następują w drodze decyzji, do których stosuje się przepisy Kodeksu postępowania administracyjnego. Jak stwierdził NSA przez pojęcie „stosowanie przepisów k.p.a. do decyzji” nie należy rozumieć jedynie wymogu stosowania przepisów wprost odnoszących się do tej formy działania administracji publicznej (np. art. 107 § 1 k.p.a.), ale także nakaz stosowania wszelkich przepisów regulujących procedurę, która kończy się wydaniem decyzji, a więc i obejmującą tryb postępowania określony w art. 64 k.p.a. oraz przepisów, które normują dalsze postępowanie w sprawie zakończonej wydaniem decyzji.

Ograniczenie dostępu do informacji publicznej

Prawo dostępu do informacji publicznej nie ma charakteru absolutnego. Nie istnieje w szczególności prymat zasady dostępu nad wartościami wskazanymi w art. 61 ust. 3 Konstytucji RP, tj. ochroną porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa. Ma ono służyć tworzeniu społeczeństwa obywatelskiego przez umożliwienie społecznej kontroli działań władzy publicznej, a nie zaspakajaniu interesów indywidualnych, które może odbywać się kosztem interesu ogółu. Z tego względu ważne jest, by ujawnienie niektórych informacji nie zagroziło interesom państwa, a tym samym interesom wspólnoty obywateli, której to państwo jest emanacją³³.

Dopuszczalność ograniczenia prawa do informacji należy jednak rozpatrywać w świetle wspólnych dla całego Rozdziału II Konstytucji RP „zasad ogólnych”, odnoszących się do wolności, praw i obowiązków obywatela. Oznacza to, że ograniczenie musi się odbywać na zasadach określonych w art. 31 ust. 3 Konstytucji RP, a zatem jest możliwe tylko w drodze ustawy i wyłącznie wtedy, gdy jest to konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób oraz bez naruszenia istoty wolności

³³ Wyrok WSA w Warszawie z dnia 27 V 2016 r., II SA/Wa 214/16, Centralna Baza Orzeczeń Sądów Administracyjnych.

i praw. Ponadto na tle orzecznictwa Trybunału Konstytucyjnego zrekonstruowana została dodatkowa przesłanka, a mianowicie, że ograniczenia prawa muszą być proporcjonalne do potrzeby ochrony zagrożonego dobra³⁴.

Ustawa o dostępie do informacji publicznej w art. 2 ust. 1 statuuje zasadę powszechności dostępu do informacji publicznej, wskazując że dostęp do informacji publicznej przysługuje „każdemu”. Regulacja ta stanowi poszerzenie kręgu podmiotów uprawnionych w zastawieniu z art. 61 Konstytucji RP, który zakładał, że prawo do informacji przysługuje wyłącznie obywatelom.

Powszechność dostępu do informacji gwarantuje ponadto zapis art. 2 ust. 2 u. inf. publ., który stanowi, iż udostępnienie informacji publicznej, co do zasady, nie może być uzależnione od wykazania przez wnioskodawcę istnienia po jego stronie interesu prawnego lub faktycznego. W konsekwencji dysponent informacji nie może badać motywów, jakimi kierował się wnioskodawca, występując o udostępnienie określonej informacji. Ta generalna zasada doznaje jednak ograniczenia w art. 3 ust. 1 pkt 1 u. inf. publ., który przewiduje, że prawo do informacji publicznej obejmuje uprawnienie do dostępu do informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego.

Informacja przetworzona (art. 3 ust. 1 pkt 1)

Bezspornie informacja przetworzona stanowi kwalifikowaną formę informacji publicznej. W przeciwieństwie jednak do pojęcia „informacja publiczna” termin „informacja przetworzona” nie został nigdzie przez ustawodawcę zdefiniowany. W uzasadnieniu projektu ustawy o dostępie do informacji publicznej tłumaczono, że z pojęciem informacji przetworzonej wiązać należy postać informacji zagregowanej, syntetycznej lub analitycznej. Takie też znaczenie pojęcia „informacja przetworzona” przyjęła doktryna, czyniąc zarazem zastrzeżenie, że nie jest przetwarzaniem informacji dokonywanie w niej drobnych zmian, czy też pomijanie jej fragmentów w związku z obowiązkiem organu odmowy udzielenia informacji ze względu na ochronę danych osobowych, tajemnice ustawowo chronione, prawo do prywatności itp.³⁵

Odtworzenie znaczenia pojęcia „informacja przetworzona”, wobec braku definicji ustawowej, było wielokrotnie podejmowane w orzecznictwie sądów administracyjnych. Choć wypracowanie jednolitego poglądu w tej kwestii napotyka pewne trudności, niemniej możliwe jest wyodrębnienie pewnych kierunków zapatrywania. Przyjmuje się zatem, że podstawową cechą informacji przetworzonej jest to, że organ w chwili składania wniosku informacji tej wprost nie posiada i dla jej wytworzenia niezbędne jest przeprowadzenie przezeń pewnych działań na informacjach posiadanych, w wyniku czego powstanie informacja nowa

³⁴ Wyrok TK z dnia 25 II 1999 r., K 23/09.

³⁵ M. Jaśkowska, *Dostęp do informacji przetworzonej*, w: *Sądownictwo administracyjne gwarantem wolności i praw obywatelskich 1980–2005*, red. J. Góral, R. Hauser, J. Trzciniński, Warszawa 2005, s. 229.

jakościowo³⁶. Podkreśla się, że przetworzenie jest równoznaczne z koniecznością odpowiedniego zestawienia informacji, samodzielnego ich zredagowania, związanego z koniecznością przeprowadzenia przez zobowiązany podmiot czynności analitycznych, których końcowym rezultatem jest dokument pozwalający na dokonanie przez jednostkę samodzielną interpretacji i oceny. Proces przetwarzania, którego istotnym elementem jest włożenie wysiłku intelektualnego w przygotowanie informacji, musi prowadzić do jakościowo nowej informacji³⁷.

Oprócz owego przymiotu nowości, zwraca się uwagę na znaczną wysokość nakładów wiążących się z pozyskaniem informacji jako kryterium uznania informacji za informację przetworzoną. Jak zauważył NSA w wyroku z 16 października 2018 r.³⁸:

Informacją przetworzoną jest nie tylko jakościowo nowa informacja, która nie istnieje w przyjętej treści i postaci, chociaż jej źródłem są materiały znajdujące się w posiadaniu podmiotu zobowiązanego. W pewnych wypadkach, tj. gdy szeroki zakres wniosku wymagający zgromadzenia, przekształcenia (zanonimizowania) i sporządzenia wielu kserokopii określonych dokumentów, wymaga takich działań organizacyjnych i angażowania środków osobowych, które zakłócają normalny tok działania podmiotu zobowiązanego i utrudniają wykonywanie przypisanych mu zadań, informacja wytworzona w ten sposób, pomimo iż składa się z wielu informacji prostych będących w posiadaniu organu, będzie również informacją przetworzoną. Powstały bowiem w wyniku wskazanych wyżej działań zbiór nie istniał w chwili wystąpienia z żądaniem o udostępnienie informacji publicznej.

W podobnym duchu wypowiedział się WSA w Gliwicach³⁹, stwierdzając że informacja przetworzona może zaistnieć w przypadku zsumowania, często na podstawie różnych kryteriów, pojedynczych wiadomości prostych znajdujących się w posiadaniu podmiotu zobowiązanego, pod warunkiem że działania zmierzające do wytworzenia owej nowej informacji podjęte zostaną „na szeroką skalę”, tzn. np. przy zaangażowaniu znacznej liczby pracowników, w sytuacji gdy niezbędne czynności będą czasochłonne i tym samym uniemożliwiające pracownikom rzetelne wykonywanie ich codziennych służbowych obowiązków, prowadząc do dezorganizacji pracy lub co najmniej oderwania pracowników od ich kompetencji i zadań. Zastrzega się przy tym, że *informacja prosta nie zmienia się w informację przetworzoną poprzez proces anonimizacji, bo czynność ta*

³⁶ Wyrok TK z dnia 18 XII 2018 r., SK 27/14 (Legalis nr 1 856 099), wyrok WSA w Białymstoku z dnia 6 III 2018 r., (Legalis nr 1 742 285).

³⁷ Wyrok WSA we Wrocławiu z dnia 19 XII 2005 r., IV SAB/Wr 47/05, Centralna Baza Orzeczeń Sądów Administracyjnych.

³⁸ Wyrok NSA z dnia 16 X 2018 r., I OSK 2567/16, Centralna Baza Orzeczeń Sądów Administracyjnych.

³⁹ Wyrok WSA w Gliwicach z dnia 14 XI 2017 r., IV SA/GI 407/17, Centralna Baza Orzeczeń Sądów Administracyjnych.

*polega jedynie na jej przekształceniu, a nie przetworzeniu. Podobnie nie stanowi o przetworzeniu informacji sięganie do materiałów archiwalnych*⁴⁰.

Przepis art. 3 ust. 1 pkt 1 u. inf. publ. nie wskazuje, jaki podmiot i na jakim etapie ma wykazać zaistnienie w danym przypadku tej szczególnej istotności dla interesu publicznego.

W orzecznictwie przyjmuje się jednak, że wnioskodawca występujący o udostępnienie informacji publicznej na etapie składania wniosku nie musi wiedzieć, że żądana przez niego informacja ma charakter informacji publicznej przetworzonej, a zatem w momencie formułowania i kierowania wniosku nie musi wskazywać powodów, dla których spełnienie jego żądania będzie szczególnie istotne dla interesu publicznego. To podmioty zobowiązane do udostępnienia informacji publicznej muszą wykazać, że objęte wnioskiem żądanie dotyczy informacji publicznej o charakterze przetworzonym i mogą odmówić jej udostępnienia tylko wtedy, gdy wnioskodawca nie wykaże istnienia interesu publicznego⁴¹.

Skoro zatem od takiego wykazania ustawodawca uzależnił udostępnienie informacji przetworzonej, organ zobowiązany do jej udzielenia powinien wezwać wnioskodawcę do przedstawienia argumentów, uzasadnienia, dlaczego w jego ocenie udostępnienie tej informacji właśnie jemu jest szczególnie istotne dla interesu publicznego.

Tu napotkać można jednak kolejny problem, bowiem przesłanka szczególnej istotności dla interesu publicznego także nie została przez ustawodawcę zdefiniowana.

Próbując sprecyzować ów termin, wskazuje się, że pojęcie „interes publiczny” jest pojęciem niedookreślonym, nieposiadającym zwartej zapisanej formuły na gruncie obowiązującego prawa. Można natomiast przyjąć, że jest on znaczeniowo węższy od funkcjonującego w powszechnym użyciu terminu „interes społeczny”. Dlatego stwierdzono, że odnosi się on w swej istocie do spraw związanych z funkcjonowaniem państwa oraz innych ciał publicznych jako pewnej całości, szczególnie z funkcjonowaniem ich podstawowej struktury, zwłaszcza jeżeli związane jest ono z gospodarowaniem mieniem komunalnym lub majątkiem Skarbu Państwa. Należy wówczas wykazać, że taka informacja nie tylko jest ważna dla dużego kręgu potencjalnych odbiorców, ale również, że jej uzyskanie stwarza realną możliwość wykorzystania uzyskanych danych dla poprawy funkcjonowania organów administracji i lepszej ochrony interesu publicznego. Dlatego też wnioskodawca winien wyjaśnić, w jaki sposób zamierza wykorzystać uzyskane informacje dla poprawy tego interesu lub poprawy funkcjonowania organów administracji publicznej. Uzyskanie informacji przetworzonej

⁴⁰ Wyrok NSA z dnia 9 VIII 2011 r., (Legalis nr 825 623).

⁴¹ Wyroki WSA w Warszawie: z dnia 20 VI 2005 r., II SA/Wa 795/05, Centralna Baza Orzeczeń Sądów Administracyjnych; wyrok z dnia 22 II 2006 r., II SA/Wa 1721/05, Centralna Baza Orzeczeń Sądów Administracyjnych; wyrok z dnia 22 VIII 2007 r., II SA/Wa 1048/07, Centralna Baza Orzeczeń Sądów Administracyjnych.

wiąże się bowiem z poniesieniem określonych środków, zwłaszcza finansowych, często trudnych do pogodzenia z bieżącymi działaniami konkretnych organów. W związku z tym jej udzielenie podmiotom, które nie zapewniają, że zostanie ona wykorzystana w celu usprawnienia funkcjonowania danego organu, przemawia za przyjęciem, że po stronie wnioskodawcy nie występuje szczególnie interes publiczny, uzasadniający udzielenie mu takiej informacji.

W tym kontekście nie ma zatem znaczenia, kto ubiega się o daną informację, ale w jakim celu to czyni. Świadczy o tym wprowadzenie kryterium interesu publicznego i to szczególnie istotnego. To wnioskodawca musi zatem wykazać, że informacje, które zamierza uzyskać, nie dotyczą wyłącznie jego interesu, ale że działa w interesie publicznym, a sprawa, o której chce zostać poinformowany, ma szczególne znaczenie dla funkcjonowania odpowiedniego organu. Brak przekonującej argumentacji po stronie wnioskodawcy skutkować musi wydaniem przez podmiot zobowiązany decyzji o odmowie udostępnienia informacji publicznej.

Ochrona informacji niejawnych i innych informacji prawnie chronionych jako przesłanka odmowy dostępu do informacji publicznej

Obok wydedukowanego z art. 3 ust. 1 pkt 1 u. inf. publ. ograniczenia dostępu do informacji przetworzonej, z uwagi na występujące po stronie wnioskodawcy kryterium braku szczególnej istotności dla interesu publicznego w uzyskaniu dostępu do informacji, przedmiotowa ustawa w art. 5 ust. 1 wprost doprecyzowuje ograniczenia, o których mowa w art. 61 ust. 3 Konstytucji RP, stanowiąc że prawo dostępu do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Ograniczenie to jest szczególnie istotne w kontekście dostępu do informacji publicznych dotyczących obszarów działalności służb specjalnych.

Zgodnie z ustawą o ochronie informacji niejawnych⁴² ochrona informacji niejawnych przybiera dwie postaci. Po pierwsze, w myśl art. 4 ust. 1 u. inf. niejaw. wszelkie informacje niejawne mogą być udostępnione 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. Dla ochrony przewidzianej w tym przepisie wystarczy, że informacja ta posiadać będzie element materialny, jakim jest ustalenie, że jest taką, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie jej opracowywania, oraz niezależnie od formy i sposobu jej wyrażania (art. 1 ust. 1 u. inf. niejaw.). Informacja niejawna w opisanym przypadku jest chroniona bez względu na to, czy

⁴² Ustawa z dnia 10 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019, poz. 742).

osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą. Jest ona bowiem niejawną z uwagi na zagrożenia wynikające z jej treści lub sposobu jej uzyskania, a nie w następstwie klasyfikacji⁴³.

Druga postać ochrony, o szerszym zakresie, jest stosowana w odniesieniu do informacji niejawnych, którym nadano klauzulę tajności. Przewiduje ją art. 8 u. inf. niejaw., zgodnie z którym informacje takie mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności. Informacje takie muszą być ponadto przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności. Muszą być także chronione odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Dla owej szerszej ochrony, wynikającej z art. 8 u. inf. niejaw., wymagane są jednak dwa elementy: materialny i formalny. Element materialny określa art. 1 ust. 1 u. inf. niejaw., wskazujący na możliwość powstania określonej szkody czy zagrożenia dla interesów Rzeczypospolitej Polskiej. Element formalny wyraża się natomiast w klauzuli tajności, nadanej zgodnie z art. 5 ust. 1–4 u. inf. niejaw.

Zauważyć należy, że w konsekwencji współlistnienia dwóch poziomów ochrony informacji niejawnych także zakres kontroli sądu administracyjnego w obu przypadkach, w których organ odmawia dostępu do informacji publicznej, powołując się na ochronę informacji niejawnych, będzie się różnił. Jeżeli ograniczenie w udostępnieniu informacji publicznej wynika z faktu, że informacji tej nadano klauzulę tajności, zakres kontroli sądu administracyjnego będzie węższy. W takiej sytuacji bowiem ograniczenie w udostępnieniu informacji publicznej nie wynika z jej elementu materialnego, ale przede wszystkim jest rezultatem formalnego jej oznaczenia, które odbywa się na zasadach określonych w art. 6 u. inf. niejaw. Zgodnie z brzmieniem art. 6 ust. 1 i 2 u. inf. niejaw. klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Informacje niejawne oznaczone klauzulą tajności podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych do czasu zniesienia lub zmiany tej klauzuli tajności na zasadach określonych w ust. 3, z zastrzeżeniem ust. 6. Osoba, nadająca klauzulę tajności, może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności. Natomiast zniesienie lub zmiana klauzuli tajności są możliwe po wyrażeniu pisemnej zgody przez osobę, która ją nadała, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony, przy czym może mieć to miejsce na skutek zwrócenia się przez odbiorcę materiału do jego

⁴³ Por. wyrok NSA z dnia 21 IX 2012 r., I OSK 1393/12, Centralna Baza Orzeczeń Sądów Administracyjnych; wyrok NSA z dnia 8 III 2017 r., I OSK 1777/15, Centralna Baza Orzeczeń Sądów Administracyjnych.

nadawcy z wnioskiem o dokonanie zmiany klauzuli w trybie art. 9 ust. 1 u. inf. niejaw. W przypadku sporu między nadawcą a odbiorcą w kwestii nadanej klauzuli rozstrzyga go ABW lub SKW bądź Prezes Rady Ministrów, jeżeli stroną sporu jest ABW lub SKW. To oni ostatecznie oceniają prawidłowość oznaczenia danego dokumentu. W ten sposób ustawodawca zawęził możliwość niekontrolowanego i nieuzasadnionego znoszenia klauzuli tajności, jak również jej zawyżenia lub zaniżenia.

Zaznaczyć jednocześnie w tym miejscu należy, że na gruncie u. inf. niejaw. brak jest innych regulacji, które nakazywałyby wytwórcy niejawnego dokumentu zniesienie lub zmianę klauzuli tajności z dokumentu. Zarazem przepisy nie nakazują podania uzasadnienia dla nadania określonej klauzuli tajności, co jest o tyle logiczne, że w rezultacie doprowadziłoby do objęcia uzasadnienia klauzulą. Na mocy ustawy o ochronie informacji niejawnych to zatem autor dokumentu jako osoba posiadająca wiedzę o zagrożeniach, z jakimi ewentualnie wiąże się ujawnienie treści danej informacji, obarczony jest obowiązkiem nadania klauzuli adekwatnej do treści zawartej w dokumencie. Zarazem zauważyć należy, że nadanie klauzuli tajności nie odbywa się w drodze wydania decyzji administracyjnej czy postanowienia, nie jest też aktem, o którym mowa w art. 3 § 2 pkt 4 ustawy Prawo o postępowaniu przed sądami administracyjnymi⁴⁴.

Nie oznacza to jednak, że klauzule tajności, pomimo że stwarzają konkretne sytuacje na niekorzyść obywateli, polegające na odmowie udostępnienia informacji publicznej, wymykają się w ogóle spod kontroli sądu. Gdyby tak było, część działań administracji publicznej, wpływająca na sytuację prawną obywatela, w tym na dostęp do informacji publicznej, pozostawałaby poza kontrolą sądów, co jest nie do zaakceptowania, z uwagi na zasadę art. 45 ust. 1 Konstytucji RP⁴⁵.

Z przytoczonych wyżej względów Trybunał Konstytucyjny uznał, że ocena zgodności z prawem materialnym decyzji o odmowie udostępnienia informacji publicznej z powodu oznaczenia tej informacji jedną z klauzul niejawności, o których mowa w ustawie o ochronie informacji niejawnych, nie jest możliwa bez zbadania prawnych przesłanek oznaczenia tej informacji klauzulą niejawności. W przeciwnym razie sądowa kontrola tego rodzaju decyzji byłaby iluzoryczna.

Także Naczelny Sąd Administracyjny w wyroku z 14 września 2010 r.⁴⁶ potwierdził, że dopuszczalna jest kontrola sądowa materialnych przesłanek utajnienia informacji w ramach spraw, których przedmiotem są akty (decyzje) będące następstwem klauzuli tajności, w tym decyzje o odmowie udzielenia informacji publicznej. Tym samym dopuszczono możliwość badania przez sądy administracyjne materialnych przesłanek utajnienia informacji.

⁴⁴ Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. 2019, poz. 2325, ze zm.).

⁴⁵ Wyrok TK z dnia 15 X 2009 r., K 26/08.

⁴⁶ Wyrok NSA z dnia 14 IX 2010 r., I OSK 1047/10, Centralna Baza Orzeczeń Sądów Administracyjnych.

Realizując to uprawnienie, sądy administracyjne wielokrotnie dokonywały oceny zasadności wydania przez Szefa ABW decyzji o odmowie dostępu do informacji publicznej z uwagi na objęcie jej klauzulą tajności. Na tym tle można już mówić o wykształceniu pewnej linii orzeczniczej, której główne kierunki postaram się zaprezentować poniżej.

W pierwszej kolejności należy zwrócić uwagę na orzeczenia dopuszczające dość szerokie ujęcie informacji, które podlegać powinny ochronie z uwagi na ochronę informacji niejawnych. Przytoczyć w tym miejscu należy chociażby wyrok WSA w Warszawie z 27 maja 2016 r.⁴⁷, w którym sąd stwierdził:

z uwagi na wagę i specyfikę zadań ABW uznać należy, że niejawną nie jest tylko treść informacji zawartej w materiałach pozyskanych w wyniku czynności operacyjno-rozpoznawczych, czy też w ramach współpracy prowadzonej z partnerami zagranicznymi, ale także sposób jej pozyskiwania, a nawet samo potwierdzenie faktu jej posiadania, bowiem fakt ten pośrednio może wskazywać na jedyny możliwy sposób jej uzyskania, jakim jest prowadzenie czynności operacyjno-rozpoznawczych. Wiedza w tym zakresie, jak również informacja na temat możliwości technicznych ABW, ma niebagatelne znaczenie zarówno dla obcych służb wywiadowczych, jak i dla zorganizowanych grup przestępczych, których rozpracowywaniem zajmuje się ABW i w konsekwencji może utrudnić czy wręcz uniemożliwić organowi wykonywanie jego ustawowych działań, a tym samym narazić państwo polskie i jego sojuszników na uszczerbek.

W podobnym duchu WSA w Warszawie wypowiedział się także w wyroku z 29 maja 2017 r.⁴⁸, stwierdzając iż porozumienia ABW z przedsiębiorcą telekomunikacyjnym, operatorem pocztowym i usługodawcą, świadczącym usługi drogą elektroniczną bez wątplenia zawierane są w celu realizacji ustawowych zadań ABW, do których należy rozpoznawanie, zapobieganie i zwalczanie zagrożeń wymienionych w art. 5 ustawy o ABW oraz AW. Tym samym ujawnienie tej informacji może powodować zagrożenie dla bezpieczeństwa państwa. Idąc dalej, sąd uznał, że wprawdzie dane, których upublicznienia domaga się fundacja, stanowią żądanie ujawnienia jedynie informacji statystycznej, niemniej znając liczbę tych porozumień i podmiotów świadczących usługi drogą elektroniczną, w łatwy sposób można określić także, w jakim zakresie ABW korzysta z uprawnień przyznanych przez ustawodawcę w bieżącym czasie (wniosek dotyczył aktualnych porozumień). Z tego względu sąd ocenił, iż udostępnienie żądanej informacji może, w sposób pośredni, ujawnić skalę wykorzystywania form i środków pozostających w dyspozycji i w tym kontekście uznał, że odmowa udostępnienia informacji jest jak najbardziej zasadna, w szczególności jeśli uwzględni się stan niewypowiedzianej, ale rzeczywistej wojny terroryzmu

⁴⁷ Wyrok WSA w Warszawie z dnia 27 V 2016 r., II SA/ Wa 214/16, Centralna Baza Orzeczeń Sądów Administracyjnych.

⁴⁸ Wyrok WSA w Warszawie z dnia 29 V 2017 r., II SA/ Wa 291/17, Centralna Baza Orzeczeń Sądów Administracyjnych.

ze światem demokratycznym, przejawiającej się choćby falą zamachów terrorystycznych nękającą państwa zachodnie Unii Europejskiej, pomimo ustanowienia w niektórych z nich stanu wyjątkowego. Wydarzenia te, w szczególności wobec ich agresywnego charakteru, w ocenie sądu stanowią wystarczającą przesłankę do uznania dopuszczalności zwiększenia działań dyskrejonalnych państw demokratycznych w zakresie bezpieczeństwa wewnętrznego ich obywateli i pozostają w zgodności z zasadą proporcjonalności między prawem do bezpieczeństwa obywateli a obywatelskim prawem do informacji.

Także w wyroku z 27 maja 2017 r. WSA w Warszawie⁴⁹ uznał, że ujawnienie nawet zbiorczych danych dotyczących działań podejmowanych na podstawie ustawy antyterrorystycznej może świadczyć o nasileniu bądź osłabieniu działań ABW w tej materii, zwłaszcza gdy będzie następowało cyklicznie. Bez wątpienia informacja taka jest niezwykle cenna dla ugrupowań mogących prowadzić działalność terrorystyczną w naszym kraju, stanowi bowiem sygnał, że należy działać ostrożnie bądź też swobodniej. Informacja o liczbie podejmowanych czynności może mieć też niebagatelne znaczenie dla obywateli państw obcych, potencjalnie zainteresowanych działalnością terrorystyczną. Mając wiedzę w tym zakresie, osoby takie, znając potencjalne ryzyko, mogą efektywniej zabezpieczyć się przed oddziaływaniem środków posiadanych przez organy państwa, co w konsekwencji może utrudnić organowi wykonywanie jego ustawowych działań w zakresie rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym.

Ponadto, w wyroku z 23 stycznia 2019 r. NSA stwierdził, iż

zważywszy na wagę i specyfikę zadań ABW uznać należy, że niejawną nie jest tylko treść informacji zawartej w materiałach pozyskanych w wyniku czynności operacyjno-rozpoznawczych, czy też w ramach współpracy prowadzonej z partnerami zagranicznymi, ale także sam sposób jej pozyskiwania, a nawet samo potwierdzenie faktu jej posiadania, bowiem fakt ten pośrednio może wskazywać na jedyny możliwy sposób jej użycia, jakim jest prowadzenie czynności operacyjno-rozpoznawczych.

Jak podkreślał sąd, *wiedza w tym zakresie może mieć niebagatelne znaczenie dla zorganizowanych grup przestępczych, których rozpracowywaniem zajmuje się ABW i w konsekwencji może utrudnić czy wręcz uniemożliwić organowi wykonywanie jego ustawowych działań, o których mowa w art. 1 i art. 5 ustawy o ABW oraz AW*⁵⁰.

W nawiązaniu do przytoczonych wyżej orzeczeń szczególną uwagę zwrócić należy na podnoszony przez sądy, sformułowany niezależnie od przepisów Konstytucji RP oraz ustawy o ochronie informacji niejawnych, obowiązek

⁴⁹ Wyrok WSA w Warszawie z dnia 25 V 2017 r., II SA/Wa 146/17, Centralna Baza Orzeczeń Sądów Administracyjnych.

⁵⁰ Wyrok NSA z dnia 23 stycznia 2019 r., I OSK 579/17, Centralna Baza Orzeczeń Sądów Administracyjnych.

ochrony środków, metod i form realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy Agencji, który wynika z art. 35 ust. 1 ustawy o ABW oraz AW⁵¹.

W wyroku z 8 marca 2017 r.⁵² Naczelny Sąd Administracyjny, przywołując art. 35 ust. 1⁵³ i 39 ust. 3⁵⁴ ustawy o ABW oraz AW, wskazał, iż: *informacje wymienione w tych regulacjach stanowią informacje niejawne nie tylko z uwagi na objęcie ich dodatkową ochroną w przepisach tych przewidzianą, ale również z tego względu, że wypełniają pojęcie informacji niejawnych z art. 1 ust. 1 u. inf. niejaw., a zatem takich, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkodę dla Rzeczypospolitej Polskiej*. Jak dalej podkreślał sąd, art. 35 ust. 1 ustawy o ABW oraz AW wskazuje, że ochrona wymienionych w nim informacji następuje w związku z wykonywaniem zadań ABW, co w kontekście art. 1 ustawy o ABW oraz AW, który stanowi, iż ABW jest właściwa w sprawach bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, oraz w kontekście art. 5 ust. 1 ustawy o ABW oraz AW, który określając katalog zadań przypisanych przez ustawodawcę ABW, wskazuje, iż są to m.in. rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także w obronność państwa, prowadzi do wniosku, że zakwalifikowanie informacji z zakresu ochrony obronności i bezpieczeństwa państwa jako tych, których nieuprawnione ujawnienie spowodowałoby

⁵¹ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2020, poz. 27, ze zm.).

⁵² Wyrok NSA z dnia 8 III 2017 r., I OSK 1312/15, Centralna Baza Orzeczeń Sądów Administracyjnych.

⁵³ Art. 35 ust. 1 ustawy o ABW oraz AW: *W związku z wykonywaniem swoich zadań Agencje zapewniają ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy tych Agencji*.

⁵⁴ Art. 39 ust. 1–3 ustawy o ABW oraz AW:

1. Szefowie Agencji, każdy w zakresie swojego działania, mogą zezwalać funkcjonariuszom i pracownikom Agencji oraz byłym funkcjonariuszom i pracownikom, po ustaniu stosunku służbowego lub stosunku pracy w Agencji, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych, na udzielenie informacji niejawnej określonej osobie lub instytucji.
2. Uprawnienie, o którym mowa w ust. 1, wobec byłych funkcjonariuszy i pracowników Urzędu Ochrony Państwa przysługuje Szefowi ABW.
3. Zezwolenie, o którym mowa w ust. 1 i 2, nie może dotyczyć udzielenia informacji o:
 - 1) osobie, jeżeli zostały uzyskane w wyniku prowadzonych przez Agencje albo inne organy, służby lub instytucje państwowe czynności operacyjno-rozpoznawczych;
 - 2) szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz o stosowanych w związku z ich prowadzeniem środkach i metodach;
 - 3) osobie udzielającej pomocy Agencji, o której mowa w art. 36 korzystanie z pomocy innych osób podczas wykonywania zadań, ust. 1;
 - 4) osobie udzielającej pomocy Urzędowi Ochrony Państwa w wykonywaniu czynności operacyjno-rozpoznawczych.

lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej, wynika wprost z brzmienia art. 1 ust. 1, wyłożonego z zastosowaniem katalogu z art. 5 u. inf. niejaw. Dodatkowo art. 39 ust. 3 ustawy o ABW oraz AW potwierdza, że wskazane w nim informacje ustawodawca traktuje jako zasługujące na „szczególną ochronę przed ujawnieniem”.

Zasługująca na aprobatę linia orzecznicza ukształtowała się również w sprawach, w których w trybie dostępu do informacji publicznej osoby fizyczne zwracały się z zapytaniem, czy stosowano wobec nich kontrolę operacyjną⁵⁵. Sądy, podkreślając specyfikę zadań wykonywanych przez ABW, a zarazem zwracając uwagę na konieczność ochrony konstytucyjnych wolności praw obywatela, takich jak wolność podmiotu do ochrony prywatności, autonomii informacyjnej, nienaruszalności mieszkania czy wreszcie godności, stawały na stanowisku, że granicę korzystania z wolności praw wyznaczają ograniczenia wynikające z ustaw regulujących odmienne zasady dostępu do informacji publicznych, w szczególności ustawa o ochronie informacji niejawnych, co, wobec zasadnego zakwalifikowania przez organ wnioskowanych informacji jako niejawne, wyklucza możliwość dostępu do nich. Jednocześnie podkreślano, że *niejawność tej metody nie może ograniczać się wyłącznie do niejawności materiałów pozyskanych w toku kontroli czy w wyniku kontroli. Skoro bowiem tajemnicą objęte jest samo zarządzenie kontroli operacyjnej, to tajemnica ta rozciąga się również na jej zakończenie. W przeciwnym razie ta ostatnia czynność pośrednio ujawniałaby niejawny fakt, jakim jest jej zarządzenie (...)*⁵⁶. Mogłoby to utrudniać realizację zadań Agencji polegających na zwalczaniu przestępstw godzących w bezpieczeństwo i porządek konstytucyjny państwa.

Ciekawa linia orzecznicza ukształtowała się również na gruncie spraw, w których Szef ABW, uznając wnioskowane informacje publiczne za informacje niejawne, odmawiał ich udostępnienia, nie nadając im stosownej klauzuli tajności. Zakres kontroli sądu administracyjnego w takich sytuacjach jest paradoksalnie szerszy. Oceniając możliwość ograniczenia prawa obywatela do informacji, sąd musi bowiem zbadać element materialny pod kątem przesłanek, o których mowa w art. 1 ust. 1 u. inf. niejaw. W tym przypadku niejawny charakter

⁵⁵ Wyrok WSA w Warszawie z dnia 15 XI 2016, II SA/Wa 840/16, rozstrzygnął kwestię dostępu do informacji publicznej obywatela w zakresie informacji, czy był poddany inwigilacji lub objęty kontrolą operacyjną; podobne stanowisko WSA w Warszawie zajął w wyroku z dnia 14 II 2014 r., który zapadł również na kanwie wniosku osoby fizycznej, w którym zwracała się ona o udostępnienie informacji w zakresie liczby wniosków skierowanych wobec niego w trybie art. 27 ustawy o ABW oraz AW, liczby postanowień sądowych wydanych w przedmiocie zarządzenia kontroli operacyjnej, dat ich wydania oraz okresów, kiedy kontrola była prowadzona, liczby przypadków niecierpiących zwłoki, w których szef ABW zarządził kontrolę operacyjną w trybie art. 27 ust. 3 ustawy o ABW oraz AW, oraz liczby przypadków protokolarnego komisijnego zniszczenia materiałów zgromadzonych w trakcie kontroli operacyjnej oraz przekazania kopii ich protokołów.

⁵⁶ Wyrok NSA z dnia 23 I 2019 r., I OSK 579/17 Centralna Baza Orzeczeń Sądów Administracyjnych.

informacji wynika z jej cech materialnych, a nie z tego, czy została poddana procedurze określonej w art. 5 u. inf. niejaw. W konsekwencji sąd administracyjny jest władny, a w kontekście zasady udostępniania informacji publicznej wręcz musi ocenić, czy ów element materialny, uzasadniający uznanie określonej informacji za informację niejawną w rozumieniu art. 1 ust. 1 u. inf. niejaw., występuje. Z drugiej strony, na organie odmawiającym dostępu do informacji z powołaniem się na art. 1 ust. 1 u. inf. niejaw. spoczywa obowiązek wykazania, iż dokonana kwalifikacja nie jest dowolna, tak by możliwym było dokonanie jej weryfikacji w trakcie kontroli sądowej.

Uprawnienie sądu do badania dopuszczalności odmowy dostępu w przypadku powoływania się przez organ na art. 5 u. inf. publ., pomimo braku klauzuli, jest szczególnie istotne zwłaszcza w sytuacji, gdy według wnioskodawcy nie jest ona informacją chronioną, o której mowa w art. 1 ust. 1 u. inf. niejaw.

Mamy wówczas do czynienia z konfliktem dwóch wartości. Pierwszą z nich jest ochrona interesów Rzeczypospolitej i jej obywateli, w tym ochrona porządku i bezpieczeństwa publicznego, a więc również interesu służb, które ten porządek chronią i którym trzeba zapewnić takie warunki działania, aby mogły wykonywać zadania powierzone im ustawą. Często przy argumentacji wskazującej na konieczność takiej ochrony wskazuje się na walkę z terroryzmem i przestępczością zorganizowaną. Z drugiej jednak strony ochronie podlega również konstytucyjne prawo dostępu do informacji publicznej. Poza tym działania organów państwa winny być transparentne w zakresie, w jakim nie szkodzi to jego interesom. Społeczna kontrola działalności tych organów zapobiega nadużywaniu przez nie posiadanych uprawnień, chroni państwo prawa przed wszechwładzą służb specjalnych i służy ochronie konstytucyjnych praw obywateli⁵⁷.

W takich sytuacjach sądy, stosując przepisy ustawy o ochronie informacji niejawnych, odwołują się do wykładni celowościowej w celu ustalenia, jaka była intencja ustawodawcy przy tworzeniu określonych przepisów oraz czy ujawnienie żądanych we wniosku informacji rzeczywiście zagraża interesom państwa, porządkowi prawnemu, bezpieczeństwu funkcjonariuszy, czy też bezpieczeństwu prowadzonych przez nich operacji.

Jednocześnie w orzecznictwie⁵⁸ podkreśla się, że:

ze względu na specyfikę odmowy udostępnienia informacji publicznej z uwagi na ochronę informacji niejawnych organ nie musi wskazywać w uzasadnieniu decyzji konkretnych zagrożeń związanych z ewentualnym udostępnieniem wnioskowanych informacji, a może poprzestać jedynie na wskazaniu zagrożeń sprecyzowanych, lecz hipotetycznych.

⁵⁷ I. Kamińska, *Zasady dostępu do informacji publicznej oraz stosunek ustawy o dostępie do informacji publicznej do innych ustaw*, „Kwartalnik Prawa Publicznego” 2012, nr 3, s. 201–208.

⁵⁸ Wyrok NSA z dnia 8 III 2017 r., I OSK 1312/15, Centralna Baza Orzeczeń Sądów Administracyjnych.

Podanie konkretnych zagrożeń w takim przypadku, tudzież obejmowanie informacji klauzulą, a nawet odwoływanie się do przepisów określających podstawę nadania klauzuli mogłoby bowiem w istocie prowadzić do uzyskania wprost, bądź też umożliwiłoby adresatowi decyzji wywnioskowanie przez niego wiedzy na temat informacji, objętych odmową ze względu na ich niejawność. Godziłoby to wprost w istotę i sens regulacji art. 5 ust. 1 u. inf. publ.⁵⁹.

Niemniej jednak sądy zaznaczają, że takie podejście nie zwalnia organu od wskazania w sposób adekwatny do przedmiotu wniosku przesłanek materialnego uznania informacji publicznej za niejawną, przy uzasadnianiu odmowy jej udostępnienia⁶⁰.

Podsumowanie

Dostęp do informacji publicznej jest prawem niezwykle istotnym z punktu widzenia demokratycznego państwa prawnego oraz społeczeństwa obywatelskiego. Jego znaczenie jest nie do przecenienia, zwłaszcza w tych sferach, w których władza publiczna w sposób dotkliwy ingeruje w życie prywatne obywateli, jak to nierzadko ma miejsce w przypadku działalności służb specjalnych, opierającej się na metodach niejawnej inwigilacji. Z tego względu niezwykle istotnym jest, by działalność ta nie była wyłączona całkowicie spod kontroli społecznej.

Niemniej jednak, nie może ująć uwadze, iż udostępnienie informacji publicznej nie może prowadzić do ograniczenia możliwości skutecznego działania służby, ryzyko takie natomiast pojawia się w przypadku zapytań dotyczących informacji odnoszących się do posiadanych (bądź nie) możliwości technologicznych tudzież stosowanych przez służby metod operacyjnych. Powszechna wiedza w tym zakresie bez wątpienia może trudnić ABW realizację przypisanych jej ustawowych zadań, co w kontekście rosnącego na świecie i w Polsce zagrożenia terrorystycznego, jak również panującej sytuacji geopolitycznej, potencjalnie zagrozić może bezpieczeństwu państwa i jego obywateli.

W tym kontekście niezwykle istotne jest rozważne ważenie przez sądy administracyjne, sprawujące kontrolę nad rozstrzygnięciami wydawanymi przez organy w trybie ustawy o dostępie do informacji publicznej, konstytucyjnych dóbr, jakimi są z jednej strony prawo do prywatności, z drugiej zaś prawo do

⁵⁹ Podobne stanowisko zajął NSA w wyroku z dnia 18 VII 2018 r., I OSK 2248/16, stwierdzając że *ze względu na specyfikę odmowy udostępnienia informacji publicznej z uwagi na ochronę informacji niejawnych organ nie musi szczegółowo uzasadniać i wskazywać konkretnych zagrożeń związanych z ich ewentualnym udostępnieniem, ewentualna negatywna odpowiedź na sformułowane we wniosku pytania mogłaby bowiem prowadzić do udostępnienia informacji niejawnej. Nie jest tymczasem pożądane z punktu widzenia bezpieczeństwa i obronności państwa, aby publiczną stała się informacja o ewentualnych brakach w wyposażeniu służb specjalnych w konkretne systemy służące działalności operacyjnej.*

⁶⁰ Wyrok NSA z dnia 27 IX 2019, I OSK 2687/17, Centralna Baza Orzeczeń Sądów Administracyjnych.

życia w bezpiecznym państwie. Analizując orzecznictwo, można dojść do wniosku, że sądy administracyjne dostrzegają wagę zwłaszcza tej drugiej wartości i o ile stanowisko organu odmawiające dostępu do informacji jest dostatecznie uargumentowane i tym samym nie nosi cech dowolności, właśnie za nią się opowiadają. Kierunek ten należy ocenić jako zasługujący na aprobatę.

Piotr Burczaniuk
Michał Ordyniak

Rozdział 12.

Wyzwania regulacyjne ustaw kompetencyjnych służb specjalnych z perspektywy zachodzących zmian w systemie prawa oraz kształtowania nowej siatki zagrożeń dla bezpieczeństwa państwa

Wprowadzenie. Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu — rys historyczny

Celem niniejszego rozdziału jest analiza oraz próba podjęcia szerszego dyskursu obejmującego konieczność zmian w przepisach ustawowych służb specjalnych.

Punktem wyjścia do niniejszych rozważań powinna stać się analiza aktualnego stanu prawnego, ze szczególnym zwróceniem uwagi na aspekty historyczne, warunkujące stosowne zmiany.

Przepisami rangi ustawowej określającymi ramy funkcjonowania służb specjalnych we współczesnej Polsce są chronologicznie, w odniesieniu do:

- 1) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu — *ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (przepisy pragmatyczne oraz ustrojowe);
- 2) Centralnego Biura Antykorupcyjnego — *ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (przepisy pragmatyczne oraz ustrojowe);
- 3) Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego — *ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (przepisy ustrojowe) oraz *ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego* (przepisy pragmatyczne).

W pierwszej kolejności wskazać należy, iż najstarsza z wymienionych ustaw, tj. ustawa o ABW oraz AW, została oparta na schemacie konstrukcyjnym przyjętym przez ustawę regulującą poprzednika prawnego wskazanych służb, tj. *Urząd Ochrony Państwa*, i *ustawę z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa*.

W tym miejscu dodatkowo zwrócić należy uwagę na dwa aspekty. Po pierwsze, iż ustawa o UOP sama powieliła schemat konstrukcyjny — uwzględniając oczywiście aspekt ideologicznego zakotwiczenia w systemie socjalistycznym i brak realizacji standardu wynikającego z zasady demokratycznego państwa prawnego — dla części ustrojowej w *ustawie z dnia 14 lipca 1983 r. o urządzeniu Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów* oraz, dla części pragmatycznej, w *ustawie z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej Polskiej Rzeczypospolitej Ludowej*. Po drugie, ustawa o UOP do roku 2003, kiedy to przyjęto *ustawę z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych*, stanowiła jedyny akt rangi ustawowej, regulujący funkcjonowanie służb specjalnych w Polsce, wyznaczając wskazany wzorzec dla innych opracowywanych w tym zakresie ustaw. Dodać należy, iż podobną rolę odegrała kilka lat później ustawa o ABW oraz AW, która została niemal wiernie powielona w czytanych łącznie ustawie o SKW oraz SWW i ustawie o służbie w SKW oraz SWW, nie tylko w zakresie użytego schematu konstrukcyjnego, ale również przyjętych rozwiązań merytorycznych, których zresztą znaczna część została przyjęta również w regulacjach dotyczących CBA przepisami ustawy o CBA. Rozważania powyższe prowadzą do refleksji nad swoistą ciągłością zarówno stosowanego schematu konstrukcyjnego ustaw regulujących funkcjonowanie służb specjalnych, jak i powielania w nich tożsamych rozwiązań merytorycznych.

Biorąc za punkt wyjścia analizę ustawy o ABW oraz AW, wskazać należy — posiłkując się uzasadnieniem do jej projektu z 2002 r. — że wprowadzona nią reforma:

(...) jest najdalej idącą zmianą od 1990 roku, kiedy to powstał Urząd Ochrony Państwa i Wojskowe Służby Informacyjne. Jest również logiczną kontynuacją decyzji, które w 1996 r. przyniosły wyprowadzenie UOP ze struktur Ministerstwa Spraw Wewnętrznych i podporządkowanie jego szefa bezpośrednio Prezesowi Rady Ministrów. Podstawowym elementem obecnej reformy (jak można było przeczytać w uzasadnieniu — wł.) jest oddzielenie struktur wywiadu od struktur odpowiedzialnych za wewnętrzne bezpieczeństwo państwa, skoncentrowanie zadań wywiadowczych i kontrwywiadowczych w dwóch odrębnych, wyspecjalizowanych centralnych organach administracji rządowej. Nowe agencje mają być jedynymi w Rzeczypospolitej Polskiej instytucjami właściwymi w zakresie swych zadań. Uzyskują precyzyjnie określone uprawnienia oraz formalne możliwości działania w ramach administracji rządowej¹.

Co istotne, z perspektywy przedmiotu niniejszego rozdziału, w uzasadnieniu do projektu ustawy o ABW oraz AW podkreślano, iż *we wszystkich sprawnie zorganizowanych państwach, które skutecznie chronią swoje bezpieczeństwo, służby specjalne to najbardziej dynamiczne pod względem*

¹ Uzasadnienie do druku nr 276 Sejmu RP IV kadencji, [online]: <http://orka.sejm.gov.pl/proc4.nsf/opisy/276.htm>, [dostęp: 20 VI 2021].

funkcjonalno-organizacyjnym struktury, które szybko, a niekiedy z wyprzedzeniem, muszą dostosowywać się do zmieniających się zagrożeń. Nie inaczej było w Polsce w ciągu ostatnich 11 lat². Porównując główne zadania likwidowanego Urzędu Ochrony Państwa oraz stawiane przed dwoma nowymi agencjami, kształtowały się one następująco:

Urząd Ochrony Państwa	Agencja Bezpieczeństwa Wewnętrznego ³	Agencja Wywiadu ⁴
rozpoznawanie i przeciwdziałanie zagrożeniom godzącym w bezpieczeństwo, obronność, niezależność, całość i międzynarodową pozycję państwa (art. 1 ust. 2 pkt 1)	rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa (art. 5 ust. 1 pkt 1)	rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej (art. 6 ust. 1 pkt 2)
zapobieganie i wykrywanie przestępstw: szpiegostwa i terroryzmu oraz innych przestępstw godzących w bezpieczeństwo państwa oraz ściganie ich sprawców (art. 1 ust. 2 pkt 2) godzących w podstawy ekonomiczne państwa i ściganie ich sprawców (art. 1 ust. 2 pkt 3) o charakterze lub zasięgu międzynarodowym, w tym nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi, psychotropowymi lub materiałami jądrowymi i promieniotwórczymi oraz ściganie ich sprawców (art. 1 ust. 2 pkt 4)	rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa, godzących w podstawy ekonomiczne państwa, korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z 21 sierpnia 1997 r. o ograniczenia prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. nr 106, poz. 679 z późn. zm.), jeśli może to godzić w bezpieczeństwo wewnętrzne państwa, w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, nielegalnego wytwarzania, posiadania i obrotu bronią,	

² Tamże.

³ Opracowano zgodnie z pierwotnym tekstem ustawy w obowiązującym od 29 VI 2002 r.

⁴ Opracowano zgodnie z pierwotnym tekstem ustawy w obowiązującym od 29 VI 2002 r.

Urząd Ochrony Państwa	Agencja Bezpieczeństwa Wewnętrznego ³	Agencja Wywiadu ⁴
	amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym - oraz ściganie ich sprawców (art. 5 ust. 1 pkt 2)	
rozpoznawanie i przeciwdziałanie naruszeniom tajemnicy państwowej (art. 1 ust. 2 pkt 5)	realizowanie w granicach swojej właściwości, zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych (art. 5 ust. 1 pkt 3)	
	uzyskiwanie, analizowanie, przetwarzanie i przekazywanie informacji mogących mieć znaczenie dla bezpieczeństwa wewnętrznego Rzeczypospolitej Polskiej i jej porządku konstytucyjnego (art. 5 ust. 1 pkt 4)	uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz potencjału ekonomicznego i obronnego (art. 6 ust. 1 pkt 1)
	podejmowanie innych działań określonych w odrębnych ustawach i umowach (art. 5 ust. 1 pkt 5)	podejmowanie innych działań określonych w odrębnych ustawach i umowach (art. 6 ust. 1 pkt 9)
przygotowywanie dla najwyższych organów władzy i administracji państwowej informacji i analiz istotnych dla bezpieczeństwa państwa (art. 1 ust. 2 pkt 6)	przekazywanie Prezydentowi Rzeczypospolitej Polskiej i Prezesowi Rady Ministrów informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, a jeśli uzyskane informacje dotyczą spraw objętych zakresem działania właściwego ministra, Szef Agencji przekazuje je temu ministrowi, chyba że Prezes Rady Ministrów zdecyduje inaczej (art. 18 ust. 1 i 2)	przekazywanie Prezydentowi Rzeczypospolitej Polskiej i Prezesowi Rady Ministrów informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej, a jeśli uzyskane informacje dotyczą spraw objętych zakresem działania właściwego ministra, Szef Agencji przekazuje je temu ministrowi, chyba że Prezes Rady Ministrów zdecyduje inaczej (art. 18 ust. 1 i 2)

Urząd Ochrony Państwa	Agencja Bezpieczeństwa Wewnętrznego ³	Agencja Wywiadu ⁴
kryptograficzna ochrona wiadomości stanowiących tajemnicę państwową i służbową, przekazywanych przez techniczne środki łączności na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych (art. 1 ust. 2 pkt 7)		
		rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej, (art. 6 ust. 1 pkt 5)
		rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia (art. 6 ust. 1 pkt 6)
		rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa, oraz podejmowanie działań mających na celu eliminowanie tych zagrożeń (art. 6 ust. 1 pkt 7)
		ochrona zagranicznych przedstawicielstw Rzeczypospolitej Polskiej i ich pracowników przed działaniami obcych służb

Urząd Ochrony Państwa	Agencja Bezpieczeństwa Wewnętrznego ³	Agencja Wywiadu ⁴
		specjalnych i innymi działaniami mogącymi przynieść szkodę interesom Rzeczypospolitej Polskiej (art. 6 ust. 1 pkt 3)
		zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej (art. 6 ust. 1 pkt 4)
		prowadzenie wywiadu elektronicznego (art. 6 ust. 1 pkt 8)

Z powyższego zestawienia wynika, że większość zadań likwidowanego Urzędu Ochrony Państwa zostało praktycznie przejętych przez Agencję Bezpieczeństwa Wewnętrznego, natomiast zadania Agencji Wywiadu zostały zdefiniowane praktycznie od nowa. Niemniej jednak z powyższej tabeli wynika również, że większość zadań AW zostało uregulowanych, podobnie jak ABW, jednakże z uwzględnieniem specyfiki działalności poza granicami kraju oraz wydarzeń, jakie mają miejsce poza granicami RP.

Analiza zmian w ustawie ABW oraz AW

Przechodząc do analizy ustawy o ABW oraz AW z perspektywy formułowanych wobec niej postulatów legislacyjnych wskazać należy, iż w okresie blisko 20 lat jej obowiązywania była ona przedmiotem 62 zmian ogólnych, przy czym tylko trzy nowelizacje dotyczyły wyłącznie przedmiotowo jej treści, i były to:

- 1) *ustawa z dnia 25 listopada 2004 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. poz. 2647);
- 2) *ustawa z dnia 20 grudnia 2007 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2008 r. poz. 59);
- 3) *ustawa z dnia 23 października 2008 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. poz. 1428).

Pozostałe nowelizacje miały w większości charakter porządkowy i były wynikiem wprowadzania zmian w innych przepisach, w szczególności dotyczących systemu służb mundurowych. Spośród wskazanych aktów nowelizujących bez wątpienia do najważniejszych należy zaliczyć te, w wyniku których nastąpiła modyfikacja uprawnień ABW oraz AW, tj.:

- 1) *ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. 2006, poz. 708) oraz wskazaną powyżej *ustawę z dnia 20 grudnia 2007 r. o zmianie ustawy o ABW oraz AW* (Dz.U. 2008, poz. 59), która dokonała zmiany właściwości ABW w zakresie ścigania sprawców przestępstw korupcji, w związku z przejściem większości tych przestępstw przez CBA;

- 2) *ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. poz. 1228), która dokonała zmiany terminologii właściwości ABW określonej w art. 5 ust. 1 pkt 2 lit. a i pkt 3 w zakresie dostosowania siatki pojęciowej do nowej ustawy o ochronie informacji niejawnych;
- 3) *ustawę z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej* (Dz.U. poz. 1371), na podstawie której Szef ABW zyskał nowe zadanie polegające na wykonywaniu zadań punktu kontaktowego do wymiany danych, o których mowa w art. 16 ust. 3 decyzji Rady 2008/615/WSiS w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.Urz. UE L 210 z 06.08.2008, s. 1);
- 4) *ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. 2019, poz. 796 z późn. zm.). Zmiany wprowadzone tą ustawą ocenić należy jako najszersze i najbardziej istotne z punktu widzenia realizowanych zadań, jak również uprawnień funkcjonariuszy. Po pierwsze, ustawa ta wprowadziła zmianę w zadaniach ABW, dodając obowiązek w zakresie rozpoznawania, zapobiegania i wykrywania zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 *ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. 2019, poz. 1398). Ponadto wskazana ustawa po raz pierwszy uporządkowała i doprecyzowała systemowo zadania organów państwa w sytuacji wystąpienia zdarzenia o charakterze terrorystycznym lub wystąpienia takiego zdarzenia. Zakres zadań i uprawnień został uzależniony od fazy zagrożenia, tj. „przed” i „po”, przyznając Szefowi ABW funkcję koordynacyjną w tej pierwszej fazie, w wyniku czego stał się on organem odpowiedzialnym za koordynację czynności analityczno-informacyjnych podejmowanych przez służby specjalne oraz wymianę informacji przekazywanych przez pozostałe służby odpowiedzialne za bezpieczeństwo państwa, a także koordynację czynności operacyjno-rozpoznawczych, czy też prowadzenie wykazu osób mogących mieć związek ze zdarzeniami o charakterze terrorystycznym. Co szczególnie istotne, omawiane zmiany — tak silnie zwiększające kompetencje i uprawnienia ABW — zostały wprowadzone do aktu prawnego innego niż ustawa o ABW oraz AW, czyniąc z ustawy o działaniach antyterrorystycznych swoistą „małą ustawę o ABW”, co strategicznie musi być uwzględniane przy projektowaniu zmian w systemie służb specjalnych lub samej ABW;
- 5) *ustawę z dnia 23 marca 2017 r. o zmianie ustawy — Kodeks karny oraz niektórych innych ustaw* (Dz.U. poz. 768). Na podstawie tej ustawy ABW została zobowiązana do ujawniania mienia zagrożonego przypadkiem w związku z przestępstwami pozostającymi w zakresie jej właściwości. Ponadto dodano

zadanie polegające na ściganiu sprawców przestępstw przeciwko wymiarowi sprawiedliwości, określonych w art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 *ustawy z dnia 6 czerwca 1997 r. — Kodeks karny* (Dz.U. 2019, poz. 1950 i 2128), jeżeli pozostają one w związku z przestępstwami, o których mowa w art. 5 ust. 1 pkt 2 lit. a–e. Warto zauważyć, że to nowe zadanie zostało uregulowane w sposób precyzyjny, zgodnie z aktualnymi wymogami dotyczącymi precyzji aktu prawnego, który to sposób pozwolił na precyzyjne określenie nowego zadania służby.

Wskazać w tym miejscu należy, że wprowadzony do ustawy o ABW oraz AW całokształt opisanych powyżej zmian spowodował powiększenie jej struktury o około 65 proc. treści, co wynika ze zmiany liczby ustępów w niej zawartych (pierwotny tekst ustawy o ABW oraz AW zawierał ich 432, zaś w obowiązującym w czerwcu 2021 r. tekście jest ich już 717). Statystyka ta nie uwidacznia oczywiście zmiany przepisów, którym zostało nadane nowe brzmienie.

Na tym tle warto dodać, iż właściwość Agencji Wywiadu była zmieniana tylko jeden raz, kiedy to ustawa o działaniach antyterrorystycznych dodała do jej zakresu obowiązek rozpoznawania, przeciwdziałania i zapobiegania zdarzeniom o charakterze terrorystycznym wymierzonym przeciwko obywatelom lub mieniu Rzeczypospolitej Polskiej poza granicami państwa, z wyłączeniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko personelowi lub mieniu Sił Zbrojnych Rzeczypospolitej Polskiej.

Podobnie rzecz się ma z zadaniami realizowanymi przez wojskowe służby specjalne. W ciągu 15 lat obowiązywania ustawy o SKW oraz SWW właściwość SKW była nowelizowana czterokrotnie, zaś SWW tylko raz.

Jednocześnie zauważyć należy, iż ustawa o ABW oraz AW była przedmiotem orzecznictwa Trybunału Konstytucyjnego, który zajmował się nią ośmiokrotnie, w tym:

1. analizując przepisy ustrojowe:

- 1) w sprawie o sygn. akt K 45/02⁵, gdzie w wyroku z 20 kwietnia 2004 r. stwierdzono niezgodność z Konstytucją RP art. 14 ust. 1, art. 23 ust. 1 pkt 1 i 6, art. 41 ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 2, art. 30, art. 31 oraz art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w zw. z art. 31 ust. 3, a także art. 92 ust. 1 i art. 103 ust. 1 Konstytucji RP;
- 2) w sprawie o sygn. akt K 10/11⁶ (dotyczącej środków przymusu bezpośredniego), gdzie w wyroku z 17 maja 2012 r. stwierdzono niezgodność z Konstytucją RP m.in. art. 25 ust. 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 92 ust. 1 oraz art. 41 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP;

⁵ Dz.U. 2004, poz. 1159.

⁶ Dz.U. 2012, poz. 627.

- 3) w sprawie o sygn. akt K 23/11⁷ (dotyczącej kontroli operacyjnej), gdzie w wyroku z 30 lipca 2014 r. stwierdzono niezgodność zakresową z Konstytucją RP m.in. art. 27 i art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując jako wzorzec kontroli art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP;
 - 4) w sprawie o sygn. akt K 17/14⁸ (dotyczącej kontroli osobistej), gdzie w wyroku z 14 grudnia 2017 r. stwierdzono niezgodność z Konstytucją RP m.in. art. 23 ust. 1 pkt 5 i ust. 7 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 41 ust. 1 i art. 47 w związku z art. 31 ust. 3 oraz art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP.
2. analizując przepisy pragmatyczne:
- 1) w sprawie o sygn. akt K 45/02, gdzie w wyroku z 20 kwietnia 2004 r. stwierdzono niezgodność z Konstytucją RP art. 230 ust. 1 i 7 (zwolnienie za służby) ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 7, art. 32, art. 60 Konstytucji RP;
 - 2) w sprawie o sygn. akt P 30/05⁹, gdzie w wyroku z 29 czerwca 2006 r. stwierdzono niezgodność z Konstytucją RP art. 93 (uprawnienia rodzicielskie) ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 32 i art. 33 Konstytucji RP;
 - 3) w sprawie o sygn. akt K 31/08¹⁰, gdzie w wyroku z 9 lipca 2009 r. uznano za niekonstytucyjne również dwa rozporządzenia w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy ABW oraz AW;
 - 4) w sprawie o sygn. akt SK 48/13¹¹, gdzie w wyroku z 15 kwietnia 2014 r. stwierdzono niezgodność z Konstytucją RP art. 128 ust. 1 pkt 2 (ekwiwalent pieniężny za niewykorzystany urlop) ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 66 ust. 2 Konstytucji RP;
 - 5) w sprawie o sygn. akt K 18/14¹², gdzie w wyroku z 24 listopada 2015 r. stwierdzono niezgodność z Konstytucją RP m.in. art. 52 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przyjmując za wzorzec kontroli art. 66 w zw. z art. 92 ust. 1 Konstytucji RP.

W kontekście przytoczonego orzecznictwa polskiego sądu konstytucyjnego uwagę zwraca treść uzasadnienia historycznie pierwszego z tych orzeczeń

⁷ Dz.U. 2014, poz. 1055.

⁸ Dz.U. 2017, poz. 2405.

⁹ Dz.U. 2006, poz. 852.

¹⁰ Dz.U. 2009, nr 114, poz. 957.

¹¹ Dz.U. 2014, poz. 544.

¹² Dz.U. 2015, poz. 2023.

w sprawie o sygn. akt K 45/02, w którym Trybunał przedstawił interesujące wnioski dotyczące przeprowadzonej wówczas reformy, szczególnie w kontekście prawno-ustrojowej pozycji służb specjalnych, jak również ich działania i tworzenia. Trybunał Konstytucyjny wskazał wówczas, że:

(...) po pierwsze, w świetle postanowień art. 5 i art. 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U. nr 74, poz. 676 ze zm.) zadania tych organów odpowiadają zadaniom Urzędu Ochrony Państwa określonym w art. 1 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz.U. z 1999 r. nr 5, poz. 526 ze zm.). Wniosek taki potwierdzają również przepisy rozdziału 11 ustawy o ABW i AW, na mocy, których wprowadzono zmiany w obowiązujących ustawach. (...) Zniesienie Urzędu Ochrony Państwa i utworzenie w jego miejsce dwóch Agencji miało charakter zmiany organizacyjnej, a nie strukturalnych reform w funkcjonowaniu służb specjalnych. Analiza statutów nowych Agencji (zarządzenia Prezesa Rady Ministrów z 26 czerwca 2002 r. nadające statut ABW — M.P. nr 26, poz. 432 oraz AW — M.P. nr 26, poz. 433) prowadzi do wniosku, że w miejsce dawnych jednostek organizacyjnych UOP powołano podobne jednostki w nowych Agencjach (por. statut UOP — *rozporządzenie Prezesa Rady Ministrów z dnia 6 grudnia 1996 r.*, Dz.U. nr 145, poz. 675). Brak jest zatem prawnomaterialnych przesłanek dokonania kadrowej rekonstrukcji korpusu funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. (...) W ocenie Trybunału Konstytucyjnego, ustawodawca kształtując w art. 230 ust. 1 pkt 2 zasady doboru funkcjonariuszy, pozostawił Szefom Agencji nadmierny zakres swobody i uznaniowości, przez to, że odwołał się do kryteriów nieadekwatnych w sytuacji, gdy wprowadzone zmiany w funkcjonowaniu służb specjalnych miały w istocie charakter organizacyjny, a nie strukturalny.

Podsumowując powyższe rozważania, wskazać należy, biorąc pod uwagę porównanie zadań ABW i AW oraz UOP, a także treść cytowanego powyżej uzasadnienia wyroku Trybunału Konstytucyjnego, iż przepisy regulujące obecnie działanie Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu są *de facto* regulacjami, których perspektywa historyczna wyznaczona została blisko 30-letnim okresem. Jest to o tyle istotne, gdyż w zacytowanym na wstępie fragmencie uzasadnienia projektu ustawy o ABW oraz AW ustawodawca wskazał, że *służby specjalne to najbardziej dynamiczne pod względem funkcjonalno-organizacyjnym struktury, które szybko, a niekiedy z wyprzedzeniem, muszą dostosowywać się do zmieniających się zagrożeń*. W świetle powyższego automatycznie nasuwa się zatem pytanie, czy regulacje dotyczące największej służby specjalnej, posiadające najbardziej rozbudowany katalog najistotniejszych zadań dotyczących bezpieczeństwa państwa oraz przepisy odnoszące się do innych służb, są adekwatne do aktualnej sytuacji geopolitycznej i kierunku przeobrażeń zaistniałych w systemie prawa, w tym wynikających z orzecznictwa sądu konstytucyjnego?

Prace nad reformą cywilnych służb specjalnych

Pierwszą znaczącą próbą kompleksowej zmiany ustawy o ABW oraz AW były projekty ustaw z 2012 r., regulujące oddzielne funkcjonowanie każdej z tych służb, zawarte w drukach sejmowych nr 2294 — Agencja Wywiadu¹³ i 2295 — Agencja Bezpieczeństwa Wewnętrznego¹⁴. Były to projekty rządowe, które zostały opracowane pod przewodnictwem ówczesnego ministra spraw wewnętrznych, następnie po procesie uzgodnień i zatwierdzeniu ich przez Radę Ministrów zostały wniesione do rozpatrzenia przez Sejm i Senat RP.

Z uzasadnienia wskazanego projektu ustawy o Agencji Bezpieczeństwa Wewnętrznego wynika, że powodem projektowanych zmian była:

analiza działania organów administracji rządowej przeprowadzona w efekcie wydarzeń związanych z tzw. sprawą „Amber Gold” z 2012 r., która była punktem wyjścia do dyskusji na temat zmian w systemie cywilnych służb specjalnych. Okazało się wówczas, że kompetencje Agencji Bezpieczeństwa Wewnętrznego (...) i Policji nie są precyzyjnie określone i w znacznej mierze pokrywają się, przez co nie można było wskazać służby jednoznacznie odpowiedzialnej za rozpoznanie i podjęcie działań wobec zagrożenia, które się wówczas pojawiło. (...) Zakres kompetencji trzech służb zajmujących się zwalczaniem najpoważniejszej przestępczości gospodarczej — Policji, Agencji Bezpieczeństwa Wewnętrznego oraz Centralnego Biura Antykorupcyjnego — powinien zostać na tyle precyzyjnie określony, aby odpowiedzialność tych służb za ściganie poszczególnych rodzajów przestępstw nie budziła wątpliwości¹⁵.

Dodatkowo:

ABW ma stać się służbą wyspecjalizowaną w przeciwdziałaniu zagrożeniom terrorystycznym, w kontrwywiadzie i w ochronie informacji niejawnych. Ponadto ABW będzie odpowiedzialna za ściganie najpoważniejszych przestępstw przeciwko interesom ekonomicznym państwa, to znaczy zagrażających Skarbowi Państwa powstaniem uszczerbku w wysokości co najmniej 16 mln złotych (taka wielkość została zdefiniowana w Kodeksie karnym skarbowym jako znamię przestępstw skierowanych przeciwko istotnym interesom finansowym państwa polskiego). Wzmocniony zostanie pion informacyjny ABW nastawiony na wczesne rozpoznawanie zagrożeń. Policja, a w szczególności wzmocnione Centralne Biuro Śledcze (CBS), przejmie od ABW realizację zadań związanych ze zwalczaniem poważnych przestępstw kryminalnych, w tym handlu narkotykami i działalności zorganizowanych grup przestępczych, a także tych przestępstw gospodarczych, które nie znajdują się w nowo zakreślonym

¹³ Uzasadnienie do druku nr 276 Sejmu RP IV kadencji, [online]: <https://www.sejm.gov.pl/sejm7.nsf/druk.xsp?nr=2294>.

¹⁴ Uzasadnienie do druku nr 276 Sejmu RP IV kadencji, [online]: <https://www.sejm.gov.pl/sejm7.nsf/druk.xsp?nr=2295>.

¹⁵ Tamże.

obszarze zainteresowań ABW. ABW prowadzi obecnie ok. 200 śledztw, po zmianach w kompetencji służby pozostanie mniej niż połowa, a przekazanie pozostałych uwolni siły i środki, które można przeznaczyć na wzmocnienie najważniejszych kierunków działania służby. Centralne Biuro Antykorupcyjne będzie wiodącą służbą odpowiedzialną za ściganie najpoważniejszych, zagrażających państwu przestępstw korupcyjnych i przejmie od ABW zadania ścigania tych przestępstw, których głównym znamieniem jest korupcja¹⁶.

Zawarte w tym projekcie propozycje zakładały wprowadzenie zmian w obrębie całej ustawy. Planowano wówczas zdefiniować na nowo zakres zadań ABW przez jego uszczegółowienie, doprecyzowanie i przekazanie niektórych z nich innym służbom, aby wyeliminować dotychczasowe wątpliwości interpretacyjne. W związku z planowanym wzmocnieniem pionu informacyjnego miał być położony szczególny nacisk na przeciwdziałanie zagrożeniom skierowanym przeciwko bezpieczeństwu wewnętrznemu RP oraz jej porządkowi konstytucyjnemu. Ograniczony miał zostać zakres właściwości dotyczącej prowadzenia postępowań przygotowawczych przez wskazanie precyzyjnego, zamkniętego katalogu. Doprecyzowano także kwestie przekazywania informacji najważniejszym organom państwa. Zmiany miały objąć też uprawnienia funkcjonariuszy ABW przez ich doprecyzowanie, zgodnie z zasadą poszanowania konstytucyjnych praw obywatelskich dotyczących precyzyjnego określenia granic sfery praw i wolności człowieka i obywatela. Bardzo dużo zmian zostało wprowadzonych również do części dotyczącej służby w ABW, wynikających zarówno z orzecznictwa sądów administracyjnych, jak i konieczności dostosowania niektórych przepisów do aktualnych standardów tworzenia prawa, polegających na przeniesieniu niektórych regulacji z aktów wykonawczych do ustawy, np. załatwianie spraw osobowych funkcjonariuszy, oddelegowanie do pełnienia służby poza ABW, kwestie związane z prowadzeniem postępowań dyscyplinarnych.

Zarówno projekt dotyczący Agencji Bezpieczeństwa Wewnętrznego, jak i projekt zawarty w druku 2294, dotyczący Agencji Wywiadu, po przekazaniu ich do prac parlamentarnych zostały skierowane do pierwszego czytania na posiedzeniu Sejmu, przy czym dalsze prace nie były kontynuowane.

W tym miejscu wspomnieć należy o pojawiających się w 2017 r. informacjach dotyczących prac nad projektem reformy służb specjalnych, nakierowanym w szczególności na zmiany organizacyjne w kontrwywiadowczej i wywiadowczej, cywilnej służbie specjalnej, które miały być zrealizowane w postaci opracowywanego wówczas rządowego projektu ustawy o Agencji Bezpieczeństwa Narodowego¹⁷. Jak wskazywano w *rzędzie ma powstać stanowisko superministra do spraw bezpieczeństwa. Będzie on zwierzchnikiem Agencji Bezpieczeństwa Narodowego*,

¹⁶ Tamże.

¹⁷ *Media: Zmiany w służbach specjalnych?*, <https://www.infosecurity24.pl/media-zmiany-w-sluzbach-specjalnych>, [dostęp: 20 VI 2021].

która powstanie z połączenia obecnej ABW z Agencją Wywiadu¹⁸. ABN miała być jednocześnie wywiadem, kontrwywiadem, formacją zwalczającą terroryzm, superpolicją oraz służbą zbierającą wszelkie informacje ważne dla bezpieczeństwa państwa, nawet jeśli nie będą one wskazywać na naruszenia prawa¹⁹. Zwierzchnikiem nowej służby miałyby pozostać minister koordynator, przy czym planowane było utworzenie odrębnego resortu, który byłby zwierzchnikiem całej administracji w kwestiach bezpieczeństwa państwa. Wskazany minister bezpieczeństwa narodowego oprócz nadzoru, kontroli i koordynacji nad ABN miał też wykonywać analogiczne uprawnienia wobec CBA, a w stosunku do wojskowych służb specjalnych — kontrolować je i koordynować. Jeśli chodzi o służby wojskowe, to nadzór nad nimi miałyby w dalszym ciągu sprawować minister obrony narodowej, jednakże minister bezpieczeństwa narodowego miał moc żądać od szefów służb wojskowych informacji (także niejawnych) oraz wydawać im wytyczne, jedynie informując o tym szefa resortu obrony. Dodatkowo, projekt miał zakładać likwidację Kolegium ds. Służb Specjalnych, powołanie Kolegium Szefów Służb Specjalnych, z ministrem bezpieczeństwa narodowego na czele i szefami służb (ABN, CBA, SKW i SWW), jako członkami, przy czym minister bezpieczeństwa narodowego mógłby zaprosić na wybrane posiedzenia utworzonego kolegium przedstawicieli rządu i prezydenta. Wśród nowych uprawnień funkcjonariusze ABN mieliby prawo stosowania kontroli operacyjnej zarówno wobec sprawców przestępstw, jak i zagrożeń (obecnie możliwość taką ABW posiada tylko w sytuacji ścigania sprawców przestępstw — przyp. autorzy). Ponadto, funkcjonariusze nowej służby mieli mieć przyznany pełny, niejawni dostęp do informacji na temat osób, których dane są zgromadzone w rejestrach publicznych i ewidencjach wszystkich instytucji. Zgodnie z projektem, w razie wprowadzenia stanu wojennego ABN miałyby zostać automatycznie przekształcona w jednostkę wojskową.

Z informacji objętych rządowym procesem legislacyjnym wynika, iż wobec projektu ustawy o Agencji Bezpieczeństwa Narodowego nie podjęto formalnych czynności określonych przez Regulamin Prac Rady Ministrów jako proces legislacyjny.

Wskazanie obszarów co do których zasadna jest dyskusja dotycząca potrzeby zmiany przepisów regulujących funkcjonowanie polskich służb specjalnych

Przedstawiony tylko na przykładzie Agencji Bezpieczeństwa Wewnętrznego okres obowiązywania przepisów regulujących jej funkcjonowanie, wywodzących się *de facto* z ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa, liczba wprowadzonych dotychczas zmian oraz fakt, że najistotniejsze

¹⁸ A. Stankiewicz, *Superminister od bezpieczeństwa*, <https://wiadomosci.onet.pl/tylko-w-onecie/superminister-od-bezpieczenstwa/v7k36cl>, [dostęp: 20 VI 2021].

¹⁹ Tamże.

z nich zostały wprowadzone po raz ostatni w 2016 r., wskazuje na jak najbardziej uzasadnioną potrzebę analizy obszarów wymagających zmian.

Zagrożenia dla bezpieczeństwa państwa, które były aktualne 30 lat temu miały zupełnie inny charakter, były związane z ówczesną sytuacją RP, przechodzącej transformację ustrojowo-gospodarczą. Inny był też poziom technologiczny i inne metody działania sprawców przestępstw, sprowadzając *modus operandi* głównie do działalności kryminalnej. Bardzo duże zmiany w sytuacji ogólnoświatowej sprawiły, że pojawiły się nowe rodzaje zagrożeń, nieznane na początku lat 90. XX w., których zwalczanie powinno, jak się wydaje, znaleźć się we właściwości oraz rozpoznaniu służb specjalnych. Zagrożenia te mogą wynikać z bezpośredniego oddziaływania na Polskę, ale także na kraje sojusznicze czy też pozostawać w związku z sytuacją zagrożeń występujących w państwach nam najbliższych. Ponadto uwaga powinna być także skupiona na przemianach politycznych i społeczno-gospodarczych zachodzących w różnych regionach świata, w szczególności w organizacjach, których członkiem jest RP. Z tego powodu warto w dyskusji nad ewentualnymi zmianami normatywnymi służb specjalnych zastanowić się, czy wymiernym efektem nie byłyby zmiany organizacyjne.

W dalszej części tego punktu przedstawione zostaną wybrane zagadnienia, które jak się wydaje, pozostają lub powinny pozostawać we właściwości służb specjalnych lub dotyczą specyfiki funkcjonowania tych służb, które aktualnie pozostają poza zakresem regulacyjnym, lub nad którymi zasadne jest rozpoczęcie dyskusji o kierunku i zakresie zmian normatywnych.

Nowe rodzaje zagrożeń

Nową formą zagrożenia, które nie znalazło dotychczas odzwierciedlenia w przepisach regulujących funkcjonowanie służb specjalnych, pozostaje problematyka tzw. działań hybrydowych. Zagrożenie to charakteryzuje się połączeniem cech zbrojnej napaści przez formację bądź grupę ludzi nieposiadających oficjalnego związku z jakimkolwiek państwem z działaniami destabilizującymi wewnętrzną sytuację danego państwa.

Obserwowane do tej pory podobne działania poprzedzały klasyczne konflikty zbrojne i były z reguły przedmiotem analiz i strategii wojskowych. Sytuacja diametralnie zmieniła się w 2014 r. — od wydarzeń, które rozegrały się we wschodniej części Ukrainy. Charakteryzowały się one ingerencją obcego państwa oraz dezorganizacją tamtych regionów. Zostały poprzedzone długofalowym przygotowaniem, polegającym na silnym uzależnieniu gospodarczym, społecznym, surowcowym, czy też kulturowym, od Rosji. Podobne działania są obserwowane np. w Mołdawii, w dwóch regionach, które nie uznają zwierzchnictwa władzy państwowej, tj. Naddniestrza i Gaugauzji, czy też Gruzji, której dwa regiony są faktycznie kontrolowane przez Rosję.

Przeciwdziałanie wojnie hybrydowej, ale też i innym formom wrogich działań, powinno obejmować ochronę nie tylko obronności, ale w coraz większym stopniu sektorów istotnych z punktu widzenia prawidłowego funkcjonowania

państwa, takich jak: bezpieczeństwo łączności, energetyka, systemy finansowe, zaopatrzenie w wodę i żywność, ochrona zdrowia, a także działalność administracji publicznej, ochrona nowych technologii, przemysł, sprawy ekonomiczne i kulturowe. Z pewnością dyskusja dotycząca regulacji uprawniających do zwalczania tej formy działalności powinna objąć, oprócz zadań służb odpowiedzialnych za bezpieczeństwo państwa, także aspekty polityki karnej, a w szczególności norm prawa karnego, które pomimo kilkuletniego trwania stanu zagrożenia na Ukrainie, do tej pory nie doczekały się istotnej debaty m.in. dotyczącej wyzwań regulacyjnych stojących przed przestępstwem szpiegostwa, gdzie wprowadzenie zmian świadczyłoby o reakcji polskiego prawodawcy na ten nowy typ zagrożeń²⁰.

Dodać w tym miejscu należy, że w obliczu nowych form zagrożeń, takich jakie wystąpiły we wschodniej części Ukrainy, w kwietniu 2017 r. RP oraz niektóre państwa Unii Europejskiej i NATO podpisały porozumienie o utworzeniu w Helsinkach centrum do walki z zagrożeniami hybrydowymi, wśród których wymieniono ataki cybernetyczne, propagandę czy dezinformację. Decyzja ta jest zgodna z wytycznymi Komisji Europejskiej dotyczącymi zacieśniania współpracy państw UE oraz NATO, a także wypracowania wspólnej koncepcji walki z tymi zagrożeniami. Aby działania podejmowane na arenie międzynarodowej przyniosły odpowiedni skutek, niezbędne jest również podjęcie zmagania legislacyjnych przez poszczególne kraje członkowskie. Poznanie nowych form działalności powinno przełożyć się więc na stworzenie nowoczesnych regulacji, będących skuteczną odpowiedzią na nowe formy zagrożeń, których do tej pory nie opracowano.

Innym przykładem zagrożeń, nieznanymi w okresie tworzenia UOP czy też uchwalenia ustawy o ABW oraz AW, wpływających obecnie negatywnie na bezpieczeństwo w całej Unii Europejskiej, jest niekontrolowany i masowy kryzys migracyjny i powiązane z nim zagrożenia wynikające z radykalizmu islamskiego, których skutkiem mogą być ataki terrorystyczne. Wskazane zagrożenia są tym bardziej realne z uwagi na sygnalizowane problemy związane z właściwą identyfikacją poszczególnych migrantów. Fakt ten dowodzi również, że zmiany powinny objąć nie tylko służby specjalne, ale również zadania i uprawnienia innych organów, a także procedury i narzędzia odnoszące się do legalizacji pobytu cudzoziemców na terytorium naszego kraju. Przepisy te stanowią łańcuch naczyń połączonych, których każdy element jest istotny dla zapewnienia bezpieczeństwa kraju. Migracje ludności powinny być bowiem elementem oceny bezpieczeństwa zarówno w ujęciu międzynarodowym, jak i krajowym, a dopiero łączna analiza tych elementów powinna stanowić podstawę do formułowania miarodajnych ocen poziomu bezpieczeństwa państwa.

Kolejnym aspektem dotyczącym ataków terrorystycznych, który należy uwzględnić w dyskusji, jest zmiana celu działań organizacji terrorystycznych.

²⁰ Por. P. Burczaniuk, *Przestępstwo szpiegostwa — rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państwa*, w: *Uprawnienie służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, Warszawa 2017, s. 103–107.

Aktualnie tego rodzaju zagrożenia, oprócz pozbawienia życia jak największej liczby ludności, są wymierzone w inne obiekty, niezbędne do funkcjonowania państwa, takie jak elementy infrastruktury krytycznej, o której mowa w art. 3 pkt 2 *ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*. Dlatego też dyskusja na temat ewentualnych zmian prawnych powinna uwzględniać kontekst odpowiedniego zabezpieczenia całokształtu elementów infrastruktury krytycznej, ale także zwracać szczególną uwagę na środki łączności służące do zarządzania tymi elementami i ich prawidłowego funkcjonowania. Z uwagi na znaczny rozwój technologii teleinformatycznych i wykorzystywanie Internetu do funkcjonowania wymienionych elementów infrastruktury krytycznej kluczowym obecnie elementem polityki bezpieczeństwa państwa powinno być stworzenie takich przepisów, które będą umożliwiały szybkie i skuteczne podjęcie odpowiednich działań, zmierzających do przeciwdziałania wszelkiego rodzaju zagrożeniom skierowanym na tę infrastrukturę.

Elementem analiz ukierunkowanych na ocenę zasadności dyskusji w zakresie zmian regulacji dotyczących polskich służb specjalnych powinna być również problematyka tzw. ochrony (osłony) kontrwywiadowczej. Ochrona ta, nie mając swojej definicji legalnej, jest przedmiotem dyskusji wielu publicystów stawiających tezy o konieczności jej prowadzenia, przy jednoczesnym dość mglistym określeniu jej zakresu i sposobu prowadzenia. Wskazany rodzaj działalności jest komentowany i analizowany w obszarze nauk o bezpieczeństwie oraz w literaturze ekonomicznej, gdzie obejmuje perspektywę podmiotów prowadzących działalność gospodarczą i problem ochrony najważniejszych informacji, stanowiących tajemnicę przedsiębiorstwa. Podejmowane w tym zakresie działania związane są z analizą zagrożeń, wykrywaniem ich i neutralizacją, pochodzących z dwóch obszarów związanych z działalnością przedsiębiorstwa, takich jak:

- 1) otoczenie zewnętrzne (konkurencja, wywiad gospodarczy prowadzony przez inne podmioty gospodarcze lub przez inne państwa);
- 2) otoczenie wewnętrzne, do których zalicza się nieprawidłowości pojawiające się wewnątrz danego podmiotu.

W dyskursie nad tym zagadnieniem pojawiają się postulaty odpowiedzialności służb specjalnych za realizację osłony kontrwywiadowczej w odniesieniu do najważniejszych osób w państwie oraz osób kierujących kluczowymi instytucjami państwa. W związku z powyższym potrzebna jest dyskusja w zakresie potrzeb, organizacji i zakresu tego rodzaju działań.

Przeciwdziałanie zagrożeniom wynikającym z nowych form technologii

Jakkolwiek aspekty te były przedmiotem analiz i szerokich dyskusji w 2016 r., przy okazji przygotowywania projektu oraz uchwalania ustawy o działaniach antyterrorystycznych, to należy podkreślić z całą mocą, iż technologie telekomunikacyjne zaliczają się do jednych z najszybciej rozwijających się dziedzin badań, nauki i biznesu, które zyskują coraz większe znaczenie w funkcjonowaniu zarówno organizmów państwowych, jak i społeczeństw. Z tego względu

badania nad ich bezpieczeństwem, a co za tym idzie odpowiednie uprawnienia służb w tym zakresie, powinny być stałym elementem analiz potrzeb legislacyjnych służb i organów odpowiedzialnych za bezpieczeństwo państwa.

Oprócz opisywanych wcześniej zagrożeń dla bezpieczeństwa systemów łączności, innym przykładem nowoczesnych technologii, który powinien być poddany analizie pod kątem niezbędnych zmian są bezzałogowe statki powietrzne (UAV). Dyskusja w tym zakresie powinna dotyczyć nie tylko możliwości wykorzystania ich do realizacji zadań przez służby specjalne, ale także kwestii zwalczania ewentualnych zagrożeń realizowanych przy ich pomocy. Aktualnie żadna z ustaw dotyczących działania służb specjalnych ani też *ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego* (Dz.U. 2019, poz. 2418), czy też *ustawa z dnia 3 lipca 2002 r. — Prawo lotnicze* (Dz.U. 2020, poz. 1970 z późn. zm.), nie zawiera odpowiednich regulacji określających uprawnienia służb specjalnych do przejmowania kontroli nad tego typu obiektami w sytuacji zagrożenia bezpieczeństwa. Oczywiście jest, że w sytuacji wystąpienia fizycznego zagrożenia przeprowadzenia ataku terrorystycznego z wykorzystaniem UAV każda ze służb odpowiedzialnych za bezpieczeństwo będzie mogła unieszkodliwić UAV, np. przez jego zestrzelenie, działając w stanie wyższej konieczności, o którym mowa w art. 26 *ustawy z dnia 6 czerwca 1997 r. Kodeks karny*. Jak się wydaje, jest to jednak rozwiązanie ostateczne, a służby powinny mieć możliwość wyboru wariantu unieszkodliwienia takiego urządzenia, np. przez przejęcie nad nim kontroli, przy czym opracowanie wachlarza możliwości powinno być poprzedzone odpowiednią dyskusją.

Służba i pragmatyka służbowa funkcjonariuszy służb specjalnych

Istotnym elementem, o którym należy również wspomnieć, są kwestie dotyczące służby funkcjonariuszy służb specjalnych, czyli pragmatyki służbowej, a więc kształtu przepisów ustrojowych.

Na podstawie analizy przepisów dotyczących Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego stwierdzić można, że przepisy dotyczące funkcjonariuszy ostatniej z wymienionych formacji zawierają istotne różnice w odniesieniu do funkcjonariuszy pozostałych służb. Zauważyć bowiem należy, że ustawa o CBA nie przewiduje np. możliwości nadania funkcjonariuszom CBA stopni służbowych. Inne istotne różnice odnoszą się do świadczeń pieniężnych związanych ze służbą, takich jak np. prawo do lokalu mieszkalnego, prawo do ekwiwalentu pieniężnego za brak lokalu mieszkalnego, prawo do zwrotu kosztów dojazdu, pomoc finansowa na uzyskanie lokalu mieszkalnego, zachowanie prawa do lokalu mieszkalnego po zwolnieniu ze służby. Przepisy regulujące działalność CBA kształtują system przyznawania uposażeń funkcjonariuszom, który opiera się na dodatkach stałych oraz o charakterze premiovym, uzależnionych w znacznej mierze od wyników w służbie osiągniętych przez funkcjonariuszy. Z kolei zarówno system uposażeń,

jak i innych świadczeń pieniężnych przysługujących funkcjonariuszom pozostałych służb, jest uregulowany w sposób podobny, ukształtowany analogicznie do regulacji zawartych w ustawie o Urzędzie Ochrony Państwa. Wobec powyższego dyskusja nad reformą służb specjalnych powinna objąć również tę sferę przepisów. Niewątpliwie niektóre z tych świadczeń, ukształtowane w innych realiach społeczno-gospodarczych państwa, nie przystają do aktualnej sytuacji w kraju, w szczególności na rynku pracy.

Zasadne zatem jest rozważenie takiego sposobu uregulowania pragmatyki służbowej, aby przyjęte rozwiązania we wszystkich służbach specjalnych były jak najbardziej zbliżone do siebie. W szczególności dotyczy to kwestii wysokości uposażenia funkcjonariuszy służb specjalnych. Różnice w wysokości uposażenia, a także w możliwości uzyskania określonych świadczeń finansowych, niejednokrotnie powodowały sytuacje „przechodzenia” funkcjonariuszy jednej służby do innej, co w przypadku najbardziej doświadczonych i wyszkolonych funkcjonariuszy należy uznać za zjawisko bardzo negatywne z uwagi na powstające braki kadrowe, mogące przełożyć się na trudności lub ograniczenie możliwości realizacji poszczególnych zadań przez daną służbę. Innym aspektem, na który należy zwrócić uwagę w tym kontekście, jest konieczność ponownego szkolenia i wydatkowania na ten cel kolejnych środków finansowych z budżetu państwa przez funkcjonariuszy, którzy wcześniej zostali wyszkoleni do realizacji innych zadań. Przykładem uregulowania zagadnienia pragmatyki służbowej funkcjonariuszy wszystkich służb specjalnych mogłoby być np. opracowanie projektu jednej wspólnej ustawy dla wszystkich służb specjalnych albo, jak wspomniano wyżej, wprowadzenie analogicznych, spójnych ze sobą zmian w poszczególnych ustawach pragmatycznych. Jest to jeden z wariantów, który mógłby być wzięty pod uwagę w sytuacji dyskusji nad zmianami lub w przypadku tworzenia nowych przepisów dotyczących służb specjalnych.

Podsumowanie

Przedstawione powyżej rozważania i zaprezentowane zagadnienia uzasadniają pogląd co do konieczności prowadzenia stałej dyskusji nad zmianami w prawie w odniesieniu do służb specjalnych. Świadczy o tym zarówno fakt, że obecne regulacje często mają swoje zakorzenienie w przepisach tworzonych z perspektywy odmiennej sytuacji geopolitycznej, a w konsekwencji pozostawiają poza sferą regulacyjną część nowo pojawiających się zagrożeń dla bezpieczeństwa państwa. Ponadto obowiązujące przepisy muszą być poddawane zmianom dostosowującym je do zachodzących przeobrażeń systemu prawnego, wyznaczanych częstokroć orzecznictwem zarówno Trybunału Konstytucyjnego, jak i Sądu Najwyższego.

W tym kontekście najważniejszym zagadnieniem jest ocena potrzeby dostosowania przepisów ustrojowych poszczególnych służb do aktualnej sytuacji polityczno-gospodarczej w Polsce i na świecie oraz przeanalizowanie potrzeb regulacyjnych w zakresie sposobu realizacji tych zadań przez pryzmat interesów

społeczeństwa obywatelskiego. W dalszej kolejności należy zastanowić się nad zmianami dotyczącymi regulacji pragmatycznych w zakresie ich uaktualnienia oraz uspołnieniem przebiegu służby funkcjonariuszy różnych służb specjalnych.

Warto, by nowo wprowadzane rozwiązania charakteryzowały się precyzją, nie pozwalając na wątpliwości co do zakresu uprawnień przysługujących poszczególnym służbom, a zwłaszcza by stwarzały dogodne warunki podejmowania konkretnych decyzji przez funkcjonariuszy realizujących te zadania.

Bibliografia

Wykaz aktów prawnych

- Decyzja Nr 5/MON Ministra Obrony Narodowej z dnia 29 stycznia 2018 r. w sprawie opracowywania, uzgadniania, wydawania i ogłaszania aktów normatywnych oraz innych dokumentów w resorcie obrony narodowej (Dz.Urz. MON 2018, poz. 5 z późn. zm.).
- Dekret z dnia 7 grudnia 1954 r. o naczelnych organach administracji państwowej w zakresie spraw wewnętrznych i bezpieczeństwa publicznego (Dz.U. 1954, nr 54, poz. 269, z późn. zm.).
- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady (UE) z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. UE-sp.13-29.514).
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE L 119 z 4.05.2016 r., s. 89.
- Konstytucja Polskiej Rzeczypospolitej Ludowej z dnia 22 lipca 1952 r. (Dz.U. 1952, nr 33, poz. 232).
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997, nr 78, poz. 483 z późn. zm.).
- Memorandum o Porozumieniu między Ministrem Obrony Narodowej Rzeczypospolitej Polskiej, Ministrem Obrony Republiki Słowackiej, Ministerstwem Obrony Republiki Chorwacji, Ministerstwem Obrony Republiki Czeskiej, Federalnym Ministerstwem Obrony Republiki Federalnej Niemiec, Ministerstwem Obrony Węgier, Ministerstwem Obrony Republiki Włoskiej, Ministerstwem Obrony Republiki Litewskiej, Ministerstwem Obrony Narodowej Rumunii, Ministerstwem Obrony Republiki Słowenii dotyczącym utworzenia, administracji i działania Centrum Ekspertyz Kontrwywiadu NATO, podpisanym w Norfolk dnia 29 września 2015 r. (M.P. z 2016 r. poz. 590).
- Porozumienie w sprawie zapewnienia przez Komendę Główną Policji udziału Agencji Bezpieczeństwa Wewnętrznego we współpracy prowadzonej w ramach Międzynarodowej Organizacji Policji Kryminalnych Interpol i Europejskiego Urzędu Policji — Europol, niepublikowany.
- Projekt Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Druk nr 276, Warszawa, 22 lutego 2002 r., dostępne w Internecie: [https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/\\$file/276.pdf](https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/276/$file/276.pdf), [dostęp: 20 V 2021].

- Projekt ustawy o Centralnym Biurze Antykorupcyjnym wraz z projektami aktów wykonawczych, druk sejmowy nr 275, dostępne w Internecie: [https://orka.sejm.gov.pl/Druki5ka.nsf/0/C7181EB8C7824F41C125710A0045AD56/\\$file/275](https://orka.sejm.gov.pl/Druki5ka.nsf/0/C7181EB8C7824F41C125710A0045AD56/$file/275), [dostęp: 9 VI 2021].
- Rozporządzenie Ministra Rolnictwa i Reform Rolnych z dnia 1 marca 1945 r. w sprawie wykonania dekretu Polskiego Komitetu Wyzwolenia Narodowego z dnia 6 września 1944 r. o przeprowadzeniu reformy rolnej (Dz.U., nr 10, poz. 51 z późn. zm.).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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); Dz.Urz. UE L 119 z 4.05.2016 r., s. 1.
- Rozporządzenie Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie szczególnego zakresu działania Ministra-członka Rady Ministrów — Koordynatora Służb Specjalnych, Zbigniewa Wassermanna (Dz.U. 2006, nr 141, poz. 998).
- Rozporządzenie Prezesa Rady Ministrów z dnia 21 września 2007 r. w sprawie szczególnego zakresu działania Ministra-członka Rady Ministrów — Koordynatora Służb Specjalnych, Zbigniewa Wassermanna, Dz.U. 2007, nr 178, poz. 1255.
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 lutego 2013 r. w sprawie szczególnego zakresu działania Bartłomieja Sienkiewicza — Ministra Spraw Wewnętrznych — w zakresie koordynacji służb specjalnych, Dz.U. 2013, poz. 22.
- Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2014 r. w sprawie szczególnego zakresu działania Ministra — członka Rady Ministrów Jacka Cichockiego w zakresie koordynacji służb specjalnych, Dz.U. 2014, poz. 1276.
- Rozporządzenie Prezesa Rady Ministrów z dnia 13 grudnia 2017 r. w sprawie szczególnego zakresu działania Ministra — członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych, Dz.U. 2017, poz. 2332.
- Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczególnego zakresu działania Ministra — członka Rady Ministrów Mariusza Kamińskiego — Koordynatora Służb Specjalnych, Dz.U. 2019, poz. 2273.
- Uchwała nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. 2016, poz. 1006).
- Umowa podpisana w Warszawie dnia 11 lipca 2001 r. między Rządem RP a Rządem Rumunii o współpracy w zwalczaniu przestępczości zorganizowanej, terroryzmu i innych rodzajów przestępstw (Dz.U. 2004, nr 154, poz. 1625).
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o współpracy w zakresie zwalczania przestępczości zorganizowanej oraz innej przestępczości, podpisana w Warszawie dnia 26 czerwca 2003 r. (Dz.U. 2004, nr 216, poz. 2195; 2008, nr 12, poz. 71).
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o współpracy w zwalczaniu przestępczości zorganizowanej, podpisana w Warszawie dnia 28 lipca 2003 r. (Dz.U. 2004, nr 216, poz. 2197).
- Umowa między RP a Republiką Słowacką o współpracy w zwalczaniu przestępczości oraz o współdziałaniu na terenach przygranicznych, podpisana w Warszawie dnia 23 marca 2004 r., podpisana w Warszawie dnia 23 marca 2004 r., Dz.U. 2007, nr 85, poz. 568; 2011, nr 249, poz. 1497).
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Albanii o wzajemnej ochronie informacji niejawnych, podpisana w Tiranie dnia 21 września 2004 r., Dz.U. 2005, nr 247, poz. 2093.

- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Włoskiej w sprawie wzajemnej ochrony informacji niejawnych z dnia 11 lutego 2005 r. (Dz.U. 2007, nr 30, poz. 196), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o wzajemnej ochronie informacji niejawnych z dnia 18 sierpnia 2006 r. (Dz.U. 2007, nr 140, poz. 985).
- Umowa między Rzeczpospolitą Polską a Republiką Portugalską o wzajemnej ochronie informacji niejawnych z dnia 2 sierpnia 2007 r. (Dz.U. 2009, nr 154, poz. 1228), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Francuskiej o wzajemnej ochronie informacji niejawnych z dnia 28 maja 2008 r. (Dz.U. 2009, poz. 394).
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych z dnia 9 września 2010 r. (Dz.U. 2012 r.), Lex.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federalnym Republiki Austrii o wzajemnej ochronie informacji niejawnych z dnia 4 grudnia 2013 r. (Dz.U. 2014, poz. 1746), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Czarnogóry o wzajemnej ochronie informacji niejawnych z dnia 18 listopada 2014 roku (Dz.U. 2016, poz. 246), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o wzajemnej ochronie informacji niejawnych z dnia 11 czerwca 2015 roku (Dz.U. 2016, poz. 795), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Gabinetem Ministrów Ukrainy o wzajemnej ochronie informacji niejawnych z dnia 27 sierpnia 2015 roku (Dz.U. 2017, poz. 81), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Finlandii o wzajemnej ochronie informacji niejawnych z dnia 25 maja 2017 r. (Dz.U. 2008, poz. 780), Legalis.
- Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych z dnia 31 maja 2019 roku (Dz.U. 2020), Lex.
- Ustawa z dnia 31 grudnia 1944 r. o powołaniu Rządu Tymczasowego Rzeczypospolitej Polskiej (Dz.U. 1944.19.99).
- Ustawa z dnia 13 listopada 1956 r. o zmianie organizacji naczelnych organów administracji publicznej w zakresie bezpieczeństwa publicznego (Dz.U. 1956, nr 54, poz. 241).
- Ustawa z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów (Dz.U. 1983, nr 38, poz. 172, z późn. zm.).
- Ustawa z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej Polskiej Rzeczypospolitej Ludowej (Dz.U. 1985, nr 38, poz. 181).
- Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. 2020, poz. 360 z późn. zm.).
- Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz.U. 1990, nr 30, poz. 180).
- Ustawa Konstytucyjna z dnia 17 października 1992 o wzajemnych stosunkach między władzą ustawodawczą i wykonawczą Rzeczypospolitej Polskiej oraz o samorządzie terytorialnym (Dz.U. 1992, nr 84, poz. 426).
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2020, poz. 1444 z późn. zm.).

- Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (tekst jednolity: Dz.U. 2016, poz. 543).
- Ustawa z 14 kwietnia 2000 r. o umowach międzynarodowych (Dz.U. 2020, poz. 127, z późn. zm.).
- Ustawa z 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz.U. 2019, poz. 1461, z późn. zm.).
- Ustawa z dnia 6 lipca 2001 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, ustawy o odszkodowaniach przysługujących w razie wypadków i chorób pozostających w związku ze służbą w Milicji Obywatelskiej, ustawy o zaopatrzeniu inwalidów wojennych i wojskowych oraz ich rodzin, ustawy o uposażeniu żołnierzy, ustawy o Policji, ustawy o Urzędzie Ochrony Państwa, ustawy o Państwowej Straży Pożarnej, ustawy o kontroli skarbowej, ustawy o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin, ustawy o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Urzędu Ochrony Państwa, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej i Służby Więziennej oraz ich rodzin, ustawy o zakwaterowaniu Sił Zbrojnych Rzeczypospolitej Polskiej, ustawy o Służbie Więziennej oraz ustawy o Inspekcji Celnej (Dz.U. 2001, nr 81, poz. 877).
- Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. 2020, poz. 431 z późn. zm.).
- Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2020, poz. 27 z późn. zm.).
- Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych (Dz.U. 2003, nr 139, poz. 1326; nr 179, poz. 1750; 2004, nr 19, poz. 177; nr 171, poz. 1800; nr 273, poz. 2703).
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2021, poz. 576).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2021, poz. 670).
- Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. 2019, poz. 1921 z późn. zm.).
- Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2019, poz. 687 z późn. zm.).
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019, poz. 742).
- Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz.U. 2021, poz. 575).
- Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz.U. 2020, poz. 725).
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019, poz. 125).
- Ustawa z dnia 11 września 2019 r. — Prawo zamówień publicznych (Dz.U. 2019, poz. 2019 z późn. zm.).
- Zarządzenie Nr 6/13 Szefa Centralnego Biura Antykorupcyjnego z dnia 4 kwietnia 2013 r. w sprawie metod i form wykonywania w Centralnym Biurze Antykorupcyjnym zadań w zakresie legislacji, wydawania pełnomocnictw i upoważnień oraz koordynacji pomocy prawnej (Dz.Urz. CBA 2013, poz. 6, z późn. zm.).
- Zarządzenie Nr 38 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 14 października 2015 r. w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego (Dz.Urz. ABW 2015, poz. 24).
- Zarządzenie Nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. 2018, poz. 927).
- Zarządzenie Nr 11 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 5 lutego 2019 r. w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego (Dz.Urz. ABW 2021, poz. 4).

Zarządzenie Nr 7/21 Szefa Centralnego Biura Antykorupcyjnego z dnia 30 kwietnia 2021 r. w sprawie zasad procedowania projektów aktów prawnych oraz wydawania pełnomocnictw i upoważnień (Dz.Urz. CBA 2021, poz. 7).

Wykaz orzecznictwa

- Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 24 maja 1993 r., sygn. akt III SA 2017/92, OSNSA 1993/4/113 (Lex nr 10 400).
- Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 15 stycznia 1997 r., sygn. akt III SA 534/96, „Monitor Podatkowy” 1997/12/374 (Lex 31 185).
- Wyrok Trybunału Konstytucyjnego z dnia 1 grudnia 1998 r., sygn. K 21/98, OTK 1998, nr 7, poz. 116.
- Wyrok Trybunału Konstytucyjnego z dnia 28 czerwca 2000 r., sygn. K 25/99, OTK 2000, nr 5, poz. 141.
- Wyrok Trybunału Konstytucyjnego z dnia 20 kwietnia 2004 r., sygn. K 45/02, OTK-A 2004/4/30 (Dz.U. 2004, nr 109, poz. 1159).
- Wyrok Trybunału Konstytucyjnego z dnia 19 października 2010 r., sygn. K 35/09, OTK-A 2010, nr 8, poz. 77.
- Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11 (Dz.U. 2014, poz. 1055).
- Wyrok Trybunału Konstytucyjnego z dnia 14 grudnia 2017 r., sygn. K 17/14, OTK-A 2018/4 (Dz.U. 2017, poz. 2405).

Wykaz literatury

- Aleksandrowicz R., *Pojęcie czynu o charakterze terrorystycznym „de lege lata” i „de lege ferenda” (wybrane zagadnienia)*, „Problemy praworządności” 1988, nr 10.
- Balcerowicz P. (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008.
- Balicki R., Bartoszewicz M., Complak K., Ławniczak A., Masternak-Kubiak M., Haczowska M., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2014.
- Barcikowski A., *Bezpieczeństwo wewnętrzne różne perspektywy analityczne i doktrynalne*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, t. 11/14.
- Biuro Bezpieczeństwa Narodowego, *National Security Bureau*, „(MINI)SŁOWNIK BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa”, dostępne w Internecie: (MINI)SŁOWNIK BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa - Biuro Bezpieczeństwa Narodowego [dostęp: 20 V 2021].
- Bobrow D.B., Haliżak E., Zięba R. (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997.
- Bodziony K., *Rola służb specjalnych w systemie instytucji odpowiedzialnych za bezpieczeństwo ekonomiczne państwa*, „Przegląd Bezpieczeństwa Wewnętrznego” 2012, t. 7 (4).
- Boratyńska K., Chojniak Ł., Jasiński W., *Postępowanie karne. Studia Prawnicze*, wyd. 3, Warszawa 2018.
- Borowik G., *Zwalczanie zmów cenowych jako zagrożenia ekonomicznych interesów RP — próba oceny skuteczności unormowań prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, t. 9.
- Bożek M., *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej” 2015, t. 1.

- Bożek M., *Instytucjonalny system bezpieczeństwa państwa w świetle Konstytucji RP na tle członkostwa Polski w Unii Europejskiej*, w: *Europa — kontynent ryzyka? Społeczne, polityczne i normatywne uwarunkowania bezpieczeństwa w Europie*, red. M. Bożek, M. Troszyński, Warszawa 2007.
- Bożek M., *Pozycja prawna Agencji Bezpieczeństwa Wewnętrznego (struktura, zadania, zakres uprawnień)*, Emów 2003.
- Bożek M., *Uprawnienia operacyjne służb specjalnych jako środki umożliwiające ingerencję w wolności i prawa jednostki (zarys problemu)*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, t. 17 (9).
- Bożek M., *Współczesny model polskich służb specjalnych. Służby informacyjne czy policyjne?*, „Zeszyty Naukowe AON” 2005, nr 1.
- Bożek M., *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, „Studia Iuridica Lublinensia” 2015, t. 24.
- Bożek M., Czupryn M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych*, Lex a Wolters Kluwers business, Warszawa 2014.
- Bożek M., Czupryn M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2014.
- Bożek M., Karpiuk M., Kostrubiec J., Walczuk K., *Zasady ustroju politycznego państwa*, Poznań 2012.
- Bożek M., Troszyński M. (red.), *Europa — kontynent ryzyka? Społeczne, polityczne i normatywne uwarunkowania bezpieczeństwa w Europie*, Warszawa 2007.
- Bógdań-Brzezińska A., Gawrycki M.F., *Cyberterrorizm jako nowe zagrożenia dla bezpieczeństwa międzynarodowego w dobie globalizacji*, w: *Terroryzm w świecie współczesnym*, red. E. Haliżak, Warszawa 2004.
- Burczaniuk P., *Przestępstwo szpiegostwa — rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw*, red. P. Burczaniuk, Warszawa 2017.
- Burczaniuk P., *System nadzoru i kontroli nad służbami specjalnymi w Polsce — stan obecny na tle analizy prawno-porównawczej wybranych państw. Postulaty de lege ferenda*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, Warszawa 2017.
- Burczaniuk P., Kamiński M., Nowiński M., Wiczerza M., *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach*, Agencja Bezpieczeństwa Wewnętrznego, Emów 2017.
- Chrabkowski M., *Wykorzystywanie materiałów kontroli operacyjnej w postępowaniu przygotowawczym*, Szczytno 2009.
- Czczot Z., Tomaszewski T., *Kryminalistyka ogólna*, Toruń 1996.
- Dana A., *Prawo o czynnościach operacyjno-rozpoznawczych*, „Prokuratura i Prawo” 2021, nr 3, Legalis.
- Document C-M(2002)49–REV1 *Security Within the North Atlantic Treaty Organisation (NATO)*, niepublikowany.
- Filar M., *Terroryzm — problemy definicyjne oraz regulacje prawne w polskim prawie karnym w świetle prawa międzynarodowego i porównawczego* w: *Terroryzm. Materiały z sesji naukowej*, red. V. Kwiatkowska-Darul, Toruń 2002.
- Florczak-Wątor M., *Komentarz do art. 7 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziewicz, WKP, Warszawa 2019.

- Freytag von Loringhoven A., *Nowa era działalności wywiadowczej NATO*, w: „Prze-
gląd NATO” 2019, dostępne w Internecie: [https://www.nato.int/docu/review/pl/artic-
les/2019/10/29/nowa-era-dzialalnosci-wywiawczej-nato/index.html](https://www.nato.int/docu/review/pl/articles/2019/10/29/nowa-era-dzialalnosci-wywiawczej-nato/index.html) [dostęp: 30 V, 9 VI
2021].
- Garlicki A., *Konstytucja Rzeczypospolitej Polskiej. Komentarz III*, Wydawnictwo
Sejmowe, Warszawa 2003.
- Giezek J. (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014.
- Górka M., *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględ-
nieniem wybranych aspektów polityki bezpieczeństwa III RP*, ŚSP, nr 2 (17).
- Gruza E., *Czynności operacyjno-rozpoznawcze*, w: E. Gruza, M. Goc, J. Moszczyński,
Kryminalistyka — czyli rzecz o metodach śledczych, Wydawnictwo Akademickie
i Profesjonalne, Warszawa 2008.
- Grzegorzczak T., Tylman J., *Polskie postępowanie karne*, Warszawa 2011.
- Grzegorzczak T., Tylman J., *Polskie postępowanie karne*, Warszawa 2014.
- Grzelak A., *Komentarz do art. 72 i komentarz do art. 73*, w: *Traktat o funkcjonowaniu
Unii Europejskiej. Komentarz*, t. 1, red. A. Wróbel, N. Półtorak, D. Miąsik, Warszawa
2012.
- Guzik-Makaruk E., Filipkowski W., *Kryminalizacja finansowania terroryzmu na tle
prawnoporównawczym*, „Studia prawnoustrojowe” 2009, nr 10.
- Haliżak E. (red.), *Terroryzm w świecie współczesnym*, Warszawa 2004.
- Haliżak E., *Ekonomiczne wymiary bezpieczeństwa narodowego i międzynarodo-
wego*, w: *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*,
red. D.B. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997.
- Hanausek T., *Kryminalistyka a praca operacyjna*, „Problemy Kryminalistyki” 1982, nr 183.
- Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 1996.
- Hanausek T., *Kryminalistyka*, *Zarys wykładu*, Kraków 2005, w: *Ustawa o Agencji
Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Komentarz*, oprac. B. Opaliń-
ski, M. Rogalski, P. Szustakiewicz, Kraków 2005, Legalis.
- Hanausek T., *Zarys taktyki kryminalistycznej*, Warszawa 1994.
- Herbut R., *Ekstremizm*, w: *Słownik politologii*, Wrocław 2003.
- Herbut R., *Słownik politologii*, Wrocław 2003.
- Hoc S., *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Wydawnictwo Uniwersytetu
Opolskiego, Opole 2002.
- Hoc S., Szustakiewicz P., *Komentarz do art. 2 ustawy o Centralnym Biurze Antykorupcyj-
nym*, w: *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, LEX/el., 2012.
- Hoc S., Szustakiewicz P., *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*,
Lex/el. 2012.
- Hoc S., Szustakiewicz P., *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*,
teza 2 do art. 13, Lex, 2012.
- Holmes Kim R., *What is National Security? The Heritage Foundation*, dostępne
w Internecie: [www.heritage.org/sites/default/files/201910/2015_IndexOfUSMilitary-
Strength_What%20Is%20National%20Security.pdf](http://www.heritage.org/sites/default/files/201910/2015_IndexOfUSMilitary-
Strength_What%20Is%20National%20Security.pdf), [dostęp: 31 V 2021].
- Hołyst B., *Kryminalistyka*, Warszawa 2016.
- Jakubowska M., *Agencja Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa
państwa*, w: *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość —
teraźniejszość — przyszłość. Materiały i studia*, Warszawa–Szczecin 2012.
- Joint answer given by High Representative/Vice-President Ashton on behalf of the Commis-
sion Written questions: E-006018/12, E-006020/12*, dostępne w Internecie: <https://>

- www.europarl.europa.eu/doceo/document/E-7-2012-006018-ASW_CS.html?redirect [dostęp: 30 V 2021].
- Kaczmarczyk B., *Bezpieczeństwo i zagrożenia w praktyce*, SA PSP, Kraków, 2014.
- Kardas P., *Komentarz do art. 130 Kodeksu karnego*, LEX/el.,
- Karpiuk M., *Zasady ustroju politycznego państwa w Rzeczypospolitej Polskiej* w: M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012.
- Karpiuk M., Kostrubiec J., Walczuk K., *Zasady ustroju politycznego państwa*, Poznań 2012.
- Kitler W., *Organizacja bezpieczeństwa narodowego RP w kontekście ochrony ładu wewnętrznego państwa*, „Zeszyty Naukowe AON” 2013, t. 4 (93).
- Koebcke S., *Przyczynek do rozważań o teorii pracy operacyjnej*, „Problemy Kryminalistyki” 1981, nr 50.
- Kolaszyński M., *Status ustrojowy polskich służb specjalnych po 1989 r.*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2016.
- Konieczny J., *Czynności operacyjno-rozpoznawcze*, w: *Kryminalistyka*, red. J. Widacki, Wydawnictwo C.H. Beck, Warszawa 2008.
- Kowalczyk K., Wróblewski W. (red.), *Terroryzm: globalne wyzwanie*, Wydawnictwo Adam Marszałek, Toruń 2006.
- Koziej S., *Obronność Rzeczypospolitej Polskiej w latach 1989–2009*, Warszawa 2010.
- Kuciński J., *Nauka o państwie*, Wyższa Szkoła Zarządzania i Prawa, Warszawa 2012.
- Kuć T., *Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, t. 16/17.
- Kurzępa B., *Podstęp w toku czynności karnoprosesowych i operacyjnych*, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora”, Toruń 2003.
- Larecki J., *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Książka i Wiedza, Warszawa 2007.
- Lipka M., Krwawicz J., *O rozpracowaniach operacyjnych*, Warszawa 1963.
- Łabuz P., Safjański T., W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz*, Warszawa 2019.
- Marczuk K.P., *Bezpieczeństwo wewnętrzne w perspektywie kosmopolityzmu*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, t. 11/14.
- Matusiak K.B. (red.), *Innowacje i transfer technologii. Słownik pojęć*, Warszawa 2011.
- Mąka J., *Wyzwania stojące przed służbami specjalnymi — 20 lat temu i obecnie*, „Przegląd Bezpieczeństwa Wewnętrznego” 2011, wydanie specjalne.
- Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej — skimming*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, t. 10.
- Nowiński M., *Pojęcie bezpieczeństwa narodowe w prawie europejskim i międzynarodowym w kontekście uprawnień służb specjalnych*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, 2017.
- Opaliński B., Rogalski M., Szustakiewicz P. (oprac.), *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Komentarz*, Kraków 2005, Legalis.
- Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017 („Krótkie Komentarze Becka”).
- Osmaczyk J.E., *Encyklopedia spraw międzynarodowych i ONZ*, Warszawa 1974.

- Ożóg-Wróbel K., *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych”, t. 22, 2012, nr 4.
- Paprzycki L., Rau Z. (red.), *Praktyczne elementy przestępczości zorganizowanej i terroryzmu*, Oficyna a Wolters Kluwer business, Warszawa 2009.
- Polok M., *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2006.
- Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2011 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2012.
- Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2012 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013.
- Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2013 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2014.
- Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2015.
- Rydlewski G., *Służby specjalne w systemie bezpieczeństwa wewnętrznego* [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, str. 228.
- Sarnecki P. (red.), *Konstytucjonalizacja zasad i instytucji ustrojowych*, wyd. 1, Warszawa 1997.
- Schaff L., *O niektórych problemach dotyczących zakresu postępowania przygotowawczego*, NP 1957, nr 12.
- Skoneczny Ł., *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej* „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1.
- Skorupka J. (red.), *Kodeks postępowania karnego. Komentarz, art. 312*, Legalis.
- Skorupka J. (red.), *Kodeks postępowania karnego. Komentarz*, wyd. 4, Warszawa 2019.
- Skrzydło W., *Komentarz do art. 7 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX 2013.
- Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX 2013.
- Sławik K., *Kryminalistyka, przegląd zagadnień*, Warszawa 2002.
- Smolak M., *Formy zwalczania procederu prania brudnych pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, t. 9.
- Sprengel B., *Ustrój organów administracji bezpieczeństwa i porządku publicznego*, Włocławek 2004.
- Stankiewicz A., *Superminister od bezpieczeństwa*, <https://wiadomosci.onet.pl/tylko-w-onecie/superminister-od-bezpieczenstwa/v7k36cl> [dostęp: 20 VI 2021].
- Stankowska I., *Komentarz do ustawy o ochronie informacji niejawnych*, wyd. 1, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2011.
- Stefański R.A. (red.), *Kodeks karny. Komentarz*, wyd. 3, Warszawa 2017.
- Stefański R.A. (red.), *Kodeks karny. Komentarz*, wyd. 5, Warszawa 2020 („Komentarze Kodeksowe”).
- Stężycki M., Siuda M., Dudzik P., *Proliferacja towarów i technologii podwójnego zastosowania. Rola ABW w zakresie przeciwdziałania tego typu zagrożeniom* „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1.
- Sulowski S., Brzeziński M. (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009.
- Sulowski S., *W poszukiwaniu definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństw Wewnętrznych” 2009, t. 1 (9).
- Szymczak M. (red.), *Słownik języka polskiego, t. 2–3*, Wydawnictwo Naukowe PWN, Warszawa 1999.

- Taracha A., *Czynności operacyjno-rozpoznawcze a ochrona praw jednostki*, „Problemy Praworządności”. 1988, nr 8–9.
- Taracha A., *Czynności operacyjno-rozpoznawcze aspekty kryminalistyczne i prawno-dowodowe*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006.
- Treaty series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations 2010*, s. 351, <https://treaties.un.org/doc/Publication/UNTS/Volume%202673/v2673.pdf>, [dostęp 29 V 2021].
- Tuleja P., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2019.
- Tuleja P., Czarny P., Florczak-Wątor M., Naleziński B., Radziejewicz P. (red.), *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, WKP, Warszawa 2019.
- Tzu Sun, *Sztuka wojny*, Przedświt, Warszawa 1994.
- Uniszewski Z., *Przeszukanie. Problematyka kryminalistyczna*, Wydawnictwo Neriton, Warszawa 2000.
- Ura E., *Prawne zagadnienia bezpieczeństwa państwa*, Krajowa Agencja Wydawnicza, Rzeszów 1988.
- Widacki J. (red.), *Kryminalistyka*, Warszawa 1999.
- Widacki J. (red.), *Kryminalistyka*, Wydawnictwo C.H. Beck, Warszawa 2008.
- Widacki J., *Prehistoria UOP*, „Przegląd Bezpieczeństwa Wewnętrznego” 2010, wydanie specjalne.
- Widacki J., *Przedmowa*, w: M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2006.
- Wierczyński G., *Redagowanie i ogłaszanie aktów normatywnych. Komentarz*, Warszawa 2016.
- Wiśniewski B., *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2013.
- Wiśniewski B., Zalewski S., Podleś D., Kozłowska K., *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004.
- Wojciechowski S. *Terroryzm. Analiza pojęcia*. „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1.
- Wojtaszczyk K., *Istota i dylematy bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, t. 1.
- Wojtaszczyk K. (red.), *Polskie służby specjalne. Słownik*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2011.
- Wróbel A., Półtorak N., Miąsik D. (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, Warszawa 2012.
- Wygoda J., *Pojęcie czynności operacyjno-rozpoznawczych w ustawodawstwie polskim — propozycja wykładni. Teza nr 2*, „Wojskowy Przegląd Prawniczy” 2017, nr 1, 1.5, LEX.
- Zalewski S., *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009.
- Zalewski S., *Ewolucja modelu polskich służb specjalnych 1990–2002*, Warszawa 2002.
- Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002.
- Zalewski S., *Służby specjalne w państwie demokratycznym*, Akademia Obrony Narodowej — Wydział Wydawniczy, Warszawa 2005.
- Zdrowski B., *Istota bezpieczeństwa państwa*, „Annales Universitatis Pedagogicae Cracoviensis, Studia de Securitate” 2019, t. 9 (3), dostępne w Internecie: DOI 10.24917/26578549.9.3.4 [dostęp: 20 V 2021].

Zespół w polityce, Agencja Wywiadu przewodniczy w 2016 roku Cywilnemu Komitetowi Wywiadowczemu NATO, 5 stycznia 2016 r., <https://wpolityce.pl/polityka/277139-agencja-wywiadu-w-2016-roku-przewodniczy-cywilnemu-komitetowi-wywiadowczemu-nato>, [dostęp 30 V 2021].

Zięba R., *Bezpieczeństwo a terroryzm — aspekty teoretyczne*, w: *Terroryzm: globalne wyzwanie*, red. K. Kowalczyk, W. Wróblewski, Wydawnictwo Adam Marszałek, Toruń 2006, s. 29.

Zimny M., *Terroryzm samobójczy*, Warszawa 2006.

Żebrowski A., *Czynności operacyjno-rozpoznawcze. Regulacje prawne*, Kraków 2000.

Wykaz autorów

Redaktor naukowy

Piotr Burczaniuk — doktor nauk prawnych, adiunkt w Katedrze Teorii i Filozofii Prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; radca prawny, członek Okręgowej Izby Radców Prawnych w Lublinie; ukończył aplikację legislacyjną, legislator, członek Polskiego Towarzystwa Legislacji.

Autorzy

Tomasz Batory — absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.

Roman Brzozowski — absolwent prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, radca prawny, członek Okręgowej Izby Radców Prawnych we Wrocławiu.

Magdalena Gołaszewska — absolwentka prawa na Wydziale Prawa Uniwersytetu w Białymstoku, radca prawny, członek Okręgowej Izby Radców Prawnych w Białymstoku.

Michał Kamiński — absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, radca prawny, członek Okręgowej Izby Radców Prawnych w Warszawie.

Renata Klejc — absolwentka prawa na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego, radca prawny, członek Okręgowej Izby Radców Prawnych w Warszawie.

Marcin Nowiński — absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu, legislator.

Michał Ordyniak — absolwent prawa na Wydziale Prawa Uniwersytetu w Białymstoku, ukończył aplikację legislacyjną, legislator, członek Polskiego Towarzystwa Legislacji.

Gracjan Poterała — absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, ukończył aplikację legislacyjną, legislator.

Bianka Skowronek — absolwentka prawa na Wyższej Szkole Handlu i Prawa im. Ryszarda Łazarskiego w Warszawie, radca prawny, członek Okręgowej Izby Radców Prawnych w Warszawie.

Mateusz Wiczerza — absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, ukończył aplikację dyplomatyczno-konsularną, radca prawny, członek Okręgowej Izby Radców Prawnych w Lublinie.