Cybersecurity and Law

2025 Nr 1(13)

DOI: 10.35467/cal/214602

Information security of the Republic of Poland in the context of criminal liability of intelligence activities

Bezpieczeństwo informacyjne RP a odpowiedzialność karna za działalność wywiadowczą

Maciej STEPCZUK
ORCID: 0009-0006-7620-4992
E-mail: maciej.step1223@wp.pl

Abstract

The article aims to provide an overview of the functioning of the Polish information security system and its vulnerability to intelligence threats from foreign secret services. The author identified and discussed what state information security is in the context of protecting strategic information resources from unauthorised disclosure. Furthermore, another objective of the work was to indicate the scope of criminal liability for the unlawful disclosure of information through participation in intelligence activities. The work analyses the basic acts of Polish law regulating information security issues and describes the system of state institutions responsible for safeguarding information security. The thesis also uses the methods of exegesis of legal texts and induction and deduction.

The considerations presented show that maintaining an appropriate level of information security in the Republic of Poland is very important in the context of growing intelligence threats from foreign countries. It should be noted here that under the current Criminal Code, the disclosure of information to foreign intelligence services may result in increasingly severe penalties for certain behaviours identified as participation in or activity on behalf of foreign intelligence. An analysis of the Polish information security system and the offence defined in Article 130 of the Criminal Code has shown that the scale of sanctions for unlawful conduct related to the information security system and exhausting the provisions of the aforementioned legal norm is multidimensional from the point of view of the Republic of Poland's information security and is treated seriously by the Polish legal system.

Keywords

Espionage, intelligence activity, information security, foreign intelligence service

Streszczenie

Artykuł ma na celu przybliżenie funkcjonowania systemu bezpieczeństwa informacyjnego RP i jego podatności na zagrożenia wywiadowcze ze strony obcych służb specjalnych. Autor wskazał i omówił czym jest bezpieczeństwo informacyjne państwa w kontekście ochrony strategicznych zasobów informacyjnych przed ich nieuprawnionym ujawnieniem. Ponadto kolejnym celem pracy było wskazanie zakresu odpowiedzialności karnej za sprzeczne z prawem ujawnianie informacji poprzez udział w działalności wywiadowczej. W pracy dokonano analizy podstawowych aktów prawa polskiego regulujących problematykę bezpieczeństwa informacyjnego oraz opisu systemu instytucji państwa stojących na straży bezpieczeństwa informacji. W pracy ponadto wykorzystano metody: egzegezy tekstów prawnych oraz indukcyjną i dedukcyjną.

Przeprowadzone rozważania wykazały, że zachowanie właściwego poziomu bezpieczeństwa informacyjnego RP jest bardzo ważne w kontekście rosnących zagrożeń wywiadowczych państw obcych. W tym miejscu należy zauważyć, że na gruncie obowiązującego Kodeksu karnego ujawnianie informacji obcym służbom wywiadowczym może wiązać się z coraz surowszą penalizacją określonych zachowań identyfikowanych jako branie udziału lub działalność na rzecz obcego wywiadu. Analiza systemu bezpieczeństwa informacyjnego RP i przestępstwa stypizowanego w art. 130 Kodeksu karnego wykazała, że skala sankcjonowania zachowań sprzecznych z prawem powiązanych z systemem bezpieczeństwa informacji i wyczerpujących dyspozycję przytoczonej normy prawnej z punku widzenia bezpieczeństwa informacyjnego RP jest wielowymiarowa i traktowana poważnie przez polski porządek prawny.

Słowa kluczowe

Szpiegostwo, działalność wywiadowcza, bezpieczeństwo informacyjne, wywiad

Uwagi ogólne

Bezpieczeństwo informacyjne RP jest nieodmiennie związane z funkcjonującym w ramach państwa systemem bezpieczeństwa, który jest kształtowany i dostosowywany do bieżącej sytuacji geopolitycznej. Polska jest demokratycznym państwem prawnym strzegącym niepodległości i nienaruszalności swojego terytorium oraz bezpieczeństwa obywateli[1]. Ustanowione konstytucyjne normy ustrojowe funkcjonowania państwa wskazują, że jednym z podstawowych zadań, przed jakimi staje RP, jest zapewnienie właściwego poziomu ochrony dla jego obywateli. Tak sformułowane zadanie

[1] Ustawa z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskie (Dz. U. z 2009 r. Nr 114, poz. 946).

zmusza konstytucyjne organy władzy ustawodawczej i wykonawczej do tworzenia systemu bezpieczeństwa państwa lub – odnosząc się do innej semantyki – systemu bezpieczeństwa narodowego, który zapewnia ochronę wszystkich sfer życia obywateli. W tym kontekście system bezpieczeństwa państwa należy traktować jako zdolność społeczeństwa oraz organów państwa do identyfikowania rzeczywistego stanu państwa, zagrożeń lub ich braku, mogących godzić w stabilność wewnętrzną i suwerenność państwa[2]. System bezpieczeństwa informacyjnego RP jest częścią systemu bezpieczeństwa państwa, który ulega zmianom w zależności od związanej z państwem sytuacji politycznej, militarnej i ekonomicznej, a więc tych, które mają bezpośredni wpływ na funkcjonowanie Polski w systemie geopolitycznym regionu Europy Środkowo-Wschodniej.

Bezpieczeństwo informacyjne RP w systemie bezpieczeństwa państwa

Począwszy od zakończenia zimnej wojny wraz u upadkiem Związku Socjalistycznych Republik Radzieckich (ZSRR), przez przyjęcie Polski w 1999 r. do Sojuszu Północnoatlantyckiego (NATO), a kończąc na członkostwie Rzeczypospolitej Polskiej w Unii Europejskiej, sytuacja związana z kształtowaniem krajowego systemu bezpieczeństwa ulegała cyklicznym zmianom. Po 2010 r. zmiany warunkujące bezpieczeństwo Polski stały się jeszcze bardziej widoczne, zważywszy na kryzys migracyjny w UE, w tym późniejszy kryzys migracyjny na granicy polsko-białoruskiej, aneksję Krymu przez Federację Rosyjską w 2014 r. oraz wybuch wojny ukraińsko-rosyjskiej w 2022 r.

Bez wątpienia czynniki te spowodowały zmianę krajowego systemu bezpieczeństwa związanego z aktywnością militarną Federacji Rosyjskiej oraz odrodzeniem się jej polityki mocarstwowej w odniesieniu do Gruzji, Ukrainy oraz dawnych państw ZSRR, w tym Polski i państw nadbałtyckich. Uwidocznione zmiany w polityce obronnej państw Europy Środkowo-Wschodniej spowodowały również konieczność jej rewizji w sektorze obronnym Polski, w tym w podzbiorze systemu bezpieczeństwa państwa jakim jest system bezpieczeństwa informacyjnego RP.

Obowiązujące w Polsce ustawodawstwo nie zawiera definicji legalnej bezpieczeństwa informacyjnego, pozostawiając interpretację tego pojęcia doktrynie, orzecznictwu oraz przedstawicielom nauk prawnych i nauk o bezpieczeństwie. W tym celu należy w pierwszej kolejności odnieść się do tego, czym jest informacja. W literaturze przedmiotu informacja jest rozumiana w kilku zasadniczych wymiarach, jako: produkt, mierzalna wielkość, potencjał, niewyczerpalny zbiór wyrażony za pośrednictwem określonych nośników

[2] A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29, s. 447-448.

materialnych i podlegający nieustannej rewizji[3]. Tak powstała wielkość w następczym procesie jest oceniana przez odbiorców pod kątem źródła pochodzenia, przekazywanej treści oraz przydatności do następczego wykorzystania[4]. Pojedyncza informacja lub ich suma stanowi podstawę do podejmowania określonych decyzji w procesie funkcjonowania państwa, począwszy od spraw ekonomicznych, a skończywszy na obronności. Natomiast zbiór informacji gromadzonych w danej dziedzinie tworzy cały system informacyjny państwa wykorzystywany w bieżącej pracy przez organy władzy wykonawczej. Uzyskiwanie, gromadzenie, analizowanie i ewentualne przekazywanie informacji przez instytucje państwowe jest szczególne istotne dla realizacji jego interesów we wszelkich sferach i działach administracji państwowej. Stąd należy uznać, że bezpieczeństwo informacyjne, jako zbiór poszczególnych informacji zawiera w swoim zakresie znaczeniowym wszystkie formy werbalne i niewerbalne wymiany i gromadzenia informacji[5].

Pojęcie bezpieczeństwa informacyjnego zostało określone w projekcie Doktryny Bezpieczeństwa Informacyjnego RP opublikowanym 24 lipca 2015 r. przez Biuro Bezpieczeństwa Narodowego[6]. Wskazano w nim, że bezpieczeństwo informacyjne państwa to wielosektorowy obszar bezpieczeństwa odnoszący się do całej sfery informacyjnej państwa (uwzględniając cyberprzestrzeń). Jego celem jest zapewnienie bezpieczeństwa funkcjonowania państwa w przestrzeni informacyjnej przez opieranie się na rodzimej, narodowej infosferze oraz skuteczną realizację zadań narodowych w zewnętrznej infosferze. Stan ten powinien zostać ukształtowany poprzez zapewnienie odpowiedniego zabezpieczenia pozostających w dyspozycji zasobów informacyjnych oraz opiekę przed nieuprawnionymi przejawami dezinformacji i propagandy. Według doktryny celem strategicznym bezpieczeństwa informacyjnego RP powinno być zapewnienie niezagrożonego funkcjonowania RP w domenie informacyjnej włączając w to bezpieczeństwo instytucji państwowych, obywatelskich oraz sektora przedsiębiorstw państwowych i prywatnych.

Określone ramy prawne funkcjonowania w systemie bezpieczeństwa informacyjnego RP przez instytucje państwowe, osoby fizyczne, spółki prawa handlowego oraz inne podmioty prawa zostały określone w szeregu aktów prawnych, najczęściej rangi ustawowej. Jednakże, w tym zakresie nie można pominąć postanowień Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., która jako ustawa zasadnicza zawiera fragmenty dotyczące bezpieczeństwa informacji odnoszące się zasadniczo do gromadzenia informacji

[3] M. Witczak, Biały wywiad w zarządzaniu bezpieczeństwem informacji, „Przegląd Bezpieczeństwa Wewnętrznego” 2024, nr 30, s. 215.
[4] K. Liderman, A. Malik, Polityka informacyjna a bezpieczeństwo informacyjne, „Studia Bezpieczeństwa Narodowego” 2013, nr 4, s. 399-400.
[5] Ibidem, s. 403.
[6] Doktryna Bezpieczeństwa Informacyjnego RP – projekt, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

na temat obywateli oraz praw do ich gromadzenia i udostępniania (art. 51). Niemniej jednak, najszerszy walor prawny dotyczący bezpieczeństwa informacyjnego RP zawierają akty prawne rangi ustawowej. Do tego katalogu można zaliczyć m. in. ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych[7], ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[8] oraz ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej[9]. W odniesieniu natomiast do postępowania z informacjami niejawnymi, czyli najbardziej newralgicznymi informacjami z punktu bezpieczeństwa państwa przetwarzanymi przez uprawnione go tego podmioty, szczególne normy prawne w tym zakresie ustawodawca zawarł w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[10]. Dyspozycje norm prawnych przytoczonego aktu prawnego wskazują zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, tj. klasyfikowania, organizowania, przetwarzania, prowadzenia postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego, organizacji kontroli stanu zabezpieczeń oraz ochrony informacji niejawnych w systemach teleinformatycznych[11].

Tak umocowany w przepisach powszechnie obowiązujących system bezpieczeństwa informacyjnego RP podlega również szeregu zagrożeń wynikających z funkcjonowania Rzeczpospolitej Polskiej w określonej infosferze, do której chcą mieć również dostęp państwa obce oraz inne podmioty prawa, które rywalizują z Polską w wielu dziedzinach funkcjonowania państwa w środowisku wewnętrznym (krajowym), a w szczególności w otoczeniu międzynarodowym (zewnętrznym). W związku z trwającą rywalizacją gospodarczą, polityczną oraz w szczególności militarną, każde z państw obcych dąży do stałego uzyskiwania informacji wchodzących w zakres dziedzin objętych systemem bezpieczeństwa informacyjnego RP. Na straży ochrony zasobu informacyjnego RP stoją instytucje państwa powołane do pełnienia zadań związanych z identyfikowaniem nieuprawnionego dostępu do zasobów informacyjnych wszystkich instytucji państwowych uzyskujących i przetwarzających informacje w zakresie swojego działania.

Do głównej instytucji chroniącej zasób informacyjny RP należy centralny urząd administracji rządowej zaliczany do kategorii służb specjalnych, tj. Agencja

[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[8] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. j.t. z 2025 r. poz. 24).
[9] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. j.t. z 2022 r. poz. 902).
[10] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. j.t. z 2025 r. poz. 1209).
[11] M. Nowikowska, Ochrona informacji niejawnych w systemie bezpieczeństwa państwa po wejściu Rzeczypospolitej Polskiej do NATO, [w:] K. Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik, Bezpieczeństwo narodowe Rzeczypospolitej Polskiej – 25 lat członkostwa w NATO, Warszawa 2024, s. 205.

Bezpieczeństwa Wewnętrznego (ABW) powołana ustawą z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[12]. W zakresie jej ustawowych kompetencji szczególnych dotyczących bezpieczeństwa informacyjnego RP leży rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa i bezprawnego ujawniania lub wykorzystywania informacji niejawnych (art. 5 ust. 1 pkt 2). Do tej kategorii należy również zaliczyć 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 (art. 5 ust. 1 pkt 3). Dodatkowo, z uwagi na szybki postęp technologiczny i związany z tym rozwój sieci teleinformatycznych służących do przesyłania zasobu informacyjnego RP, krajowa władza bezpieczeństwa skupia się również na rozpoznawaniu, zapobieganiu i wykrywaniu zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej (art. 5 ust. 1 pkt 2a).

W odniesieniu do ochrony bezpieczeństwa informacyjnego RP w domenie szeroko pojętej obronności analogiczną funkcję jak ABW wypełnia na gruncie ustawowym Służba Kontrwywiadu Wojskowego (SKW) powołana ustawą z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[13]. Jest ona właściwa do ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej (art. 1). Zapewnienie prawidłowego poziomu bezpieczeństwa informacyjnego RP przez SKW odbywa się poprzez m. in. rozpoznawanie, zapobieganie oraz wykrywanie popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i Służby Wywiadu Wojskowego oraz pracowników Sił Zbrojnych RP i innych jednostek organizacyjnych MON przestępstwa udziału w działalności obcego wywiadu stypizowanego w art. 130 Kodeksu karnego (k.k.). Znamienne jest również rozpoznawanie przez SKW przestępstw przeciwko ochronie informacji niejawnych, które mogą zagrażać katalogowi podmiotów wskazanych w art. 5 ustawy o SKW oraz SWW, a które dotyczą m. in. nieuprawnione ujawnienia lub wykorzystania informacji niejawnych, wykorzystywania informacji zapoznanych w związku z pełnioną funkcją, uzyskiwania nieuprawnionego dostępu do sieci telekomunikacyjnych oraz niszczenia, usuwania i zmieniania danych informatycznych (art. 265-269c k.k.).

[12] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. j.t. z 2025 r. poz. 1366).
[13] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. j.t. z 2025 r. poz. 179).

Oprócz umieszczonego w kompetencjach ustawowych służb specjalnych systemu ochrony bezpieczeństwa informacji RP, w polskim systemie prawnym funkcjonuje określony w Kodeksie karnym system sankcyjny związany z nieuprawnionym uzyskiwaniem, wykorzystywaniem i udostępnianiem informacji jawnych i niejawnych dotyczących wszystkich sfer funkcjonowania państwa, a wchodzących w skład zasobu systemu bezpieczeństwa informacyjnego. Funkcjonujący w Polsce system prawa karnego spełnia dzięki temu określone funkcje ochronne, prewencyjne, wychowawcze oraz dotyczące zaspokajania społecznego poczucia sprawiedliwości[14]. Jedną z najważniejszych funkcji sankcji prawno-karnych jest prewencja, zarówno ta generalna, jak również indywidualna, której podstawowym zadaniem jest poprzez właściwy system ścigania sprawców przestępstw oraz wymierzania kary, zapobieganie kolejnym zdarzeniom przestępczym chociażby w zakresie nieuprawnionego pozyskiwania i wykorzystywania informacji istotnych z punktu bezpieczeństwa państwa. Orzekanie przez sądy powszechne wymiernych do stopnia zawinienia kar za udział w działalności obcego wywiadu winno spełniać zakładane cele zapobiegawcze i wychowawcze w stosunku do oskarżonych, lecz również powinny kształtować właściwe postawy społeczne w zakresie świadomości prawnej, niezmiernie istotne w przypadku skazania za przestępstwa przeciwko Rzeczypospolitej Polskiej[15].

Obowiązujące w polskim prawie karnym materialnym sankcje nie zawsze stanowią okoliczność, która zapobiega popełnieniu przestępstw przez ewentualnych sprawców. Przesłanka ta w kontekście bezpieczeństwa informacyjnego nabiera szczególnego znaczenia, jeżeli odniesiemy ją do możliwości nieuprawnionego ujawniania zasobu informacyjnego RP poprzez spełnianie dyspozycji art. 130 k.k., tj. udziału w działalności obcego wywiadu. Oprócz opisanego systemu prewencyjnego wskazanego w polskim prawie karnym materialnym, czynności ustawowe zapobiegające przed nieuprawnionym uzyskiwaniem dostępu do informacji (również tych niejawnych), wykonują przytoczone wcześniej ABW i SKW. Podejmowane przez kontrwywiadowcze służby specjalne czynności analityczno-informacyjne, z zakresu ochrony informacji oraz w szczególności czynności operacyjno-rozpoznawcze, zmierzają do identyfikacji sprawców przestępstw udziału w działalności obcego wywiadu[16]. z uwagi na niejawny charakter rozpoznawania tego rodzaju działalności, funkcja wykrywcza sprawców ww. przestępstwa jest trudna do oceny na kanwie niniejszego artykułu. Jednakże wydaje się, że jeżeli chodzi o możliwości wykrywcze służb specjalnych szeregu informacji dostarcza publikacja Agencji

[14] A. Grześkowiak, Funkcja karząca prawa karnego na tle polskiego prawa karnego, [w:] J. Kulesza, A. Liszowska (red.), Prodignitate legis et maiestate iustitiae. Księga jubileuszowa z okazji 70. rocznicy urodzin Profesora Witolda Kuleszy, Łódź 2020, s. 345-376.

[15] M. Jaśkowiec, Branie udziału w działalności obcego wywiadu. Wybrane prawnokarne aspekty szpiegostwa, „Kwartalnik kadry Kierowniczej Policji" 2022, nr 2, s. 45.

[16] A. Żebrowski, Bezpieczeństwo służb specjalnych. Wybrane aspekty, [w:] F. Bylok, A. Kwiatek, M. Skiba (red.), Wybrane aspekty bezpieczeństwa pozamilitarnego. Zagrożenia-wyzwania-koncepcje, Częstochowa 2022, s. 208.

Bezpieczeństwa Wewnętrznego dotycząca środków pracy wywiadowczej i kontrwywiadowczej wykorzystywanych na przestrzeni lat przez służby specjalne dążące do uzyskiwania informacji dotyczących interesujących je zagadnień[17]. Dodatkowych, o wiele bardziej szczegółowych metod pracy wywiadowczej organów państwa PRL dostarcza również Instrukcja pracy operacyjnej aparatu bezpieczeństwa (1945-1989), która w sposób wyczerpujący traktuje m. in. O pozyskaniu i pracy z siecią agenturalną, zasadach prowadzenia rozpracowania agenturalnego oraz podstawowych środkach i formach pracy operacyjnej organów bezpieczeństwa publicznego PRL, w tym Służby Bezpieczeństwa[18]. Prowadzone przez służby specjalne oraz organy ścigania czynności mają dostarczyć na tyle wiarygodny materiał poszlakowy i dowody, który umożliwi wszczęcie postępowania przygotowawczego w sprawie lub w odniesieniu do konkretnej osoby lub osób, a następnie wniesienie do sądu aktu oskarżenia zmierzającego na podstawie całokształtu zgromadzonego materiału dowodowego do skazania z art. 130 k.k., tj. udziału w działalności na rzecz obcego wywiadu.

Odpowiedzialność karna za działalność wywiadowczą

Udział w działalności obcego wywiadu stanowi przestępstwo określone w art. 130 rozdziale XVII Kodeksu karnego i jest traktowane przez ustawodawcę jako przestępstwo przeciwko Rzeczypospolitej Polskiej. Kodeks karny w obecnym brzmieniu nie zawiera funkcjonującej w obiegu społecznym definicji szpiegostwa, posługując się sformułowaniem działalności na rzecz obcego wywiadu. Wydaje się zatem, że ustawodawca pozostawił doktrynie i orzecznictwu kwestie ujmowania określonych stanów faktycznych i kwalifikowania ich jako spełniających dyspozycje udziału w działalności obcego wywiadu[19]. Brak ukształtowanej definicji legalnej szpiegostwa może wynikać z dużego skomplikowania i fluktuacji stanów faktycznych, które mogą być kwalifikowane do wypełniania normy z art. 130 k.k.[20].

Na gruncie obecnie obowiązującego Kodeksu karnego ustawodawca nie zdecydował się na użycie pojęcia „szpiegostwo", wskazując jednocześnie na „działalność obcego wywiadu". Norma art. 130 § 1 k.k. wskazuje, że kto bierze udział w działalności obcego wywiadu albo działa na jego rzecz, przeciwko Rzeczypospolitej Polskiej podlega karze pozbawienia wolności na czas nie krótszy od lat 5. z analizy jej treści wynika, że jest to przestępstwo powszechne, formalne, skierowane przeciwko Rzeczypospolitej Polskiej (zagrożenie

[17] Agencja Bezpieczeństwa Wewnętrznego, Środki pracy wywiadowczej i kontrwywiadowczej, Emów 2017.
[18] Zob. szerzej: T. Ruzikowski, Instrukcja pracy operacyjnej aparatu bezpieczeństwa (1945-1989), „Materiały pomocnicze Biura Edukacji Publicznej IPN", Warszawa 2004, t. I.
[19] S. Hoc, Szpiegostwo w znowelizowanym kodeksie karnym, „Nowa Kodyfikacja Prawa Karnego", Wrocław 2023, t. LXVII, s. 133.
[20] W. Juchacz, Przestępstwo szpiegostwa na szkodę RP, „Studia z zakresu nauk prawnoustrojowych" Miscellanea 2019, nr 9, s. 110.

bezpieczeństwa i obronności w wymiarze wewnętrznym i zewnętrznym)[21]. Przestępstwo to może zostać popełnione umyślnie przez działanie, jak i zaniechanie. Jednocześnie, jak zauważył Sąd Apelacyjny w Warszawie w wyroku z 24 listopada 2017 r.[22], do udowodnienia współpracy na rzecz obcego wywiadu nie jest wymagane formalne potwierdzenie statusu oficera obcego wywiadu, jego zaszeregowania w ramach instytucji wywiadowczej, wykształcenia, stopnia wojskowego. Dodatkowo, samą działalność obcego wywiadu należy traktować rozszerzająco, jako zmierzającą do uzyskiwania i gromadzenia informacji dotyczących RP, w tym również możliwości zakłócenia prawidłowej działalności państwa i jego struktur, poprzez szerzenie zamętu i dezinformację[23]. z kolei według M. Mozgawy, przez obcy wywiad należy również rozumieć każde służby specjalne poza polskimi, doświadczone w zdobywaniu informacji dla spożytkowania do własnych celów politycznych, wojskowych lub gospodarczych[24]. Działalność na rzecz obcego wywiadu może przybierać każdą formę współpracy i zachowania sprawcy przestępstwa, który nie pozostaje formalnie w strukturach obcego wywiadu[25]. Natomiast branie udziału w działalności obcego wywiadu polega na każdej formie współpracy z tego rodzaju służbą specjalną, włączając w to przynależność do jej struktur, lecz nie jest to warunek *sine qua non*[26].

W § 2 przytoczonego przepisu ustawodawca wprowadził typ kwalifikowany, polegający na udzieleniu obcemu wywiadowi wiadomości, której przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej zagrożonego karą nie krótszą od lat 8 albo karą dożywotniego pozbawienia wolności. Wiadomością może być w tym wypadku każda informacja, która może być wykorzystana przez obcy wywiad[27]. Natomiast możliwość wyrządzenia szkody nie stanowi znamienia skutku i jest jedynie cechą przekazywanej wiadomości[28].

Odnosząc się do art. 130 § 3 k.k. ustawodawca objął sankcją karną czynność sprawczą wskazując, że kto zgłasza gotowość działania na rzecz obcego wywiadu przeciwko RP albo w celu udzielenia obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę RP, gromadzi je lub przechowuje lub wchodzi do systemu informatycznego w celu ich uzyskania podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Zachowanie to należy traktować jako jednostronne i niewymagające akceptacji ze strony obcego wywiadu, lecz musi ono dotrzeć do jego wiadomości[29]. Gromadzeniem wiadomości jest każde zbieranie informacji, które mogą zainteresować obcy

[21] Ibidem, s. 112.
[22] Wyrok Sądu Apelacyjnego w Warszawie z dnia 24 listopada 2017 r., II AKa 269/17, Lex/el.
[23] J. Kulesza, Kodeks karny. Komentarz, Warszawa 2025, Lex/el.
[24] M. Mozgawa, Kodeks karny. Komentarz aktualizowany, Warszawa 2025, Lex/el.
[25] G. Ocieczek, Wybrane zagadnienia związane z przestępstwem szpiegostwa, „Consillum Iuridicum 3 (11), 2024, s. 75.
[26] M. Mozgawa, op.cit., Lex/el.
[27] Ibidem.
[28] J. Kulesza, op.cit., Lex/el.
[29] G. Ocieczek, Wybrane zagadnienia związane z przestępstwem szpiegostwa, „Consillum Iuridicum" 2024, nr 3(11), s. 79.

wywiad i ich następcze przechowywanie na dowolnym nośniku informacji. Należy jedynie nadmienić, że wejście do systemu informatycznego może polegać zarówno na legalnym, jak również nielegalnym uzyskaniu dostępu do tego systemu i skopiowaniu znajdujących się w systemie danych[30].

Wskazane w art. 130 § 4 k.k. kierowanie i organizowanie działalności obcego wywiadu zostało przez ustawę karną objęte sankcją kary pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności. Sformułowanie organizowania obcego wywiadu odnosi się do wszystkich czynności podjętych przed formalną inicjacją działalności wywiadowczej mającą na celu organizację i stworzenie sieci agenturalnej, skoordynowanie czynności oraz opracowanie bezpiecznego kanału przesyłania informacji[31]. Natomiast kierowanie działalnością obcego wywiadu to w świetle literatury przedmiotu pełnienie w strukturze siatki obcego wywiadu funkcji, która urzeczywistnia możliwość kreowania i decydowania o przebiegu czynności wywiadowczych[32]. Wypełnienie znamion czynu zabronionego następuje poprzez wykonanie pojedynczego znamienia czasownikowego opisanego w § 4, a spełnienie obu nie powoduje popełnienia obu przestępstw[33].

W art. 130 § 5 k.k. ustawodawca wprowadził typ kwalifikowany przestępstwa określonego w § 1, definiując je jako przestępstwo indywidualne dotyczące funkcjonariuszy publicznych oraz osób pełniących dyspozycyjnie terytorialną służbę wojskową, które jest zagrożone karą pozbawienia wolności na czas nie krótszy od lat 8 albo karze dożywotniego pozbawienia wolności. Opisując szczegółowo znamiona czynu zabronionego polegającego na braniu udziału w działalności na rzecz obcego wywiadu lub działalności na jego rzecz, należy przybliżyć jedynie jakie grono osób fizycznych posiada status prawny funkcjonariusza publicznego. Osoby te są enumeratywnie wyliczone w art. 115 § 13 k.k. i zalicza się do nich m. in. posłów, sędziów, ławników, osoby zajmujące kierownicze stanowiska państwowe, żołnierzy oraz pracowników organów kontroli skarbowej. Natomiast status osoby pełniącej dyspozycyjnie terytorialną służbę wojskową został określony w art. 170 ustawy o obronie ojczyzny, który stanowi, że terytorialną służbę wojskową mogą pełnić, na ich wniosek, osoby posiadające uregulowany stosunek do służby wojskowej, a także inne osoby niepodlegające obowiązkowi odbycia zasadniczej służby wojskowej.

Ustawodawca w art. 130 § 6 k.k. traktuje o braniu udziału w działalności obcego wywiadu nieskierowanej przeciwko RP, prowadzonej na jej terytorium bez zgody właściwego organu udzielonej na podstawie odrębnych przepisów. Osoba taka podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Zgody na prowadzenie wskazanej działalności udzielają szefowie służb specjalnych. W art. 8a ustawy o ABW oraz AW Szefowie tych służb, każdy w zakresie swojej właściwości, mogą wydać zgodę na udział w działalności obcego wywiadu

[30] M. Mozgawa, op.cit., Lex/el.
[31] W. Juchacz, op.cit., s. 116.
[32] Ibidem, s. 116.
[33] M. Mozgawa, op.cit., Lex/el.

prowadzonej na terytorium RP przez organ lub służbę innego państwa, jeżeli nie narusza to interesu RP w zakresie określonym w art. 112a k.k. Natomiast, Szefowie SKW oraz SWW zgodnie z art. 9a ustawy o SKW oraz SWW mogą również wyrazić taką zgodę, jeżeli nie naruszy to obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP lub jednostek organizacyjnych MON. z drugiej strony istotne pozostaje, że odpowiedzialności karnej za wskazane przestępstwo nie podlega osoba, której związki z obcym wywiadem nieskierowane przeciwko RP ograniczają się do działalności wykonywanej w innych krajach poza RP[34]. Znamiennym jest również okoliczność, że odpowiedzialności karnej wskazanej w tym paragrafie nie podlega osoba, która bierze udział w działalności obcego wywiadu lub działa na jego rzecz po uzyskaniu od szefów służb zgody, która została wydana wadliwie z naruszeniem odrębnych przepisów prawa[35].

Obowiązujący kodeks karny w art. 130 § 7 sankcjonuje również dokonywanie dywersji, sabotażu lub dopuszczenia się przestępstwa o charakterze terrorystycznym w ramach brania udziału w działalności obcego wywiadu lub działalności na jego rzecz. Na gruncie obowiązujących przepisów trudno jest doszukać się definicji legalnych dywersji i sabotażu. Zatem w tym zakresie należy się posiłkować wykładnią językową. Dywersja w tym znaczeniu jest postrzegana jako sabotażowe lub propagandowe czynności prowadzone na obcym terytorium, w celu dezorganizacji działań militarnych państwa, a także działalność zmierzającą do zakłócenia jego dziedzin życia[36]. Przez sabotaż należy rozumieć walkę lub protest z wrogim państwem zmierzającym do uchylania się od pracy, jej nieprawidłowym realizowaniu lub uszkadzaniu istniejącej infrastruktury, w celu zmiany lub przeszkodzenia w realizacji zamierzonych przez państwo lub podmiot planów[37]. Natomiast przestępstwem o charakterze terrorystycznym zgodnie z definicją normatywną wskazaną w art. 115 § 20 k.k. jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności oraz wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej. Pozostającym w bezpośrednim związku z opisanym przestępstwem jest § 8, który obejmuje sankcją karną przygotowanie do popełnienia przestępstwa dywersji, sabotażu lub przestępstwa o charakterze terrorystycznym. Zgodnie z art. 16 § 1 k.k. przygotowanie zachodzi wówczas, gdy sprawca w celu popełnienia czynu zabronionego podejmuje czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do jego dokonania, w szczególności w tymże

[34] S. Hoc, op.cit., s. 135.
[35] J. Kulesza, op.cit., Lex/el.
[36] M. Mozgawa, op.cit., Lex/el.
[37] Ibidem.

celu wchodzi w porozumienie z inną osobą, uzyskuje lub przysposabia środki, zbiera informacje lub sporządza plan działania.

Ostatnim ze wskazanych w art. 130 k.k. typem rodzajowym przestępstwa jest określona w § 9 dezinformacja. Ustawodawca przyjął, że kto bierze udział w działalności obcego wywiadu albo działając na jego rzecz prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP albo skłonienie organu władzy publicznej RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, do podjęcia lub zaniechania określonych czynności podlega karze pozbawienia wolności na czas nie krótszy od lat 8. Poważnym zakłóceniem w ustroju lub gospodarce RP jest takie postępowanie, które doprowadzi do utrudnienia lub uniemożliwienia normalnego funkcjonowania funkcjonujących instytucji państwa[38]. Natomiast przez państwo sojusznicze należy rozumieć państwo, z którym RP zawarła umowę międzynarodową, która została zawarta dla wywołania wskazanego w niej celu[39].

Należy również podkreślić, że ustawodawca zastosował klauzulę niekaralności w odniesieniu do osób, które usiłują dokonać przestępstw określonych w art. 130 § 1, 2, 5, 7 i 9 k.k. i dobrowolnie poniechają dalszej działalności i ujawnią wobec organu powołanego do ścigania przestępstw wszystkie istotne okoliczności popełnionego czynu. Znajduje tutaj zastosowanie instytucja czynnego żalu wobec każdego, kto odstąpi od usiłowania prowadzenia takiej działalności pod warunkiem obligatoryjnym ujawnienia tych okoliczności organom ścigania. Dodatkowo, polska ustawa karna wskazuje w art. 131 § 2 k.k., że nie podlega karze za przestępstwo określone w art. 130 § 3, 6 i 8 k.k. kto dobrowolnie poniechał dalszej działalności i podjął istotne starania zmierzające do zapobieżenia popełnieniu zamierzonego czynu zabronionego oraz ujawnił wobec organów ścigania wszystkie istotne okoliczności popełnionego czynu. Niemniej istotne pozostaje, że we wszystkich kategoriach przestępstwa brania w działalności obcego wywiadu lub działalności na jego rzecz określonych w art. 130 § 1-9 k.k. sąd może również orzec przepadek przedmiotów nawet wówczas, gdy nie stanowią własności sprawy dopuszczającego się popełnienia przestępstwa.

Podsumowanie

Przeprowadzone rozważania pozwalają stwierdzić, że bezpieczeństwo informacyjne Rzeczypospolitej Polskiej obejmuje ochronę informacji istotnych dla funkcjonowania państwa, jego obywateli, administracji publicznej i sektora obronnego. Kluczowym celem prowadzonej polityki ochrony posiadanych

[38] J. Majewski, Kodeks karny. Komentarz, Warszawa 2024, Lex/el.
[39] Ibidem.

zasobów informacyjnych przez RP jest zapobieganie utracie, ujawnieniu lub wykorzystaniu danych w sposób zagrażający interesom narodowym. Obejmuje to zarówno bezpieczeństwo systemów teleinformatycznych, jak i ochronę tajemnic państwowych, służbowych oraz danych osobowych.

Ochrona wszystkich rodzajów zasobów informacyjnych pozostających w dyspozycji RP oraz prowadzone w tym zakresie przez poszczególne instytucje państwowe działania prewencyjne, zaradcze oraz wykrywcze mają zapobiegać oraz identyfikować bezprawne, nieuprawnione działania podejmowane przez zainteresowane podmioty lub państwa, w celu realizacji ich interesów gospodarczych, militarnych i politycznych. Opracowany artykuł wskazał, że w tym zakresie szczególnego waloru nabiera zagrożenie ujawnienia zasobów informacyjnych poprzez branie udziału oraz działalność na rzecz obcego wywiadu.

W artykule ponadto wykazano, że na straży ochrony systemu informacji stoją uprawnione do tego i powołane w drodze ustawy służby specjalne, tj. Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego. Jednym z ich kluczowych zadań jest rozpoznawanie, identyfikowanie oraz wykrywanie działalności wywiadowczej skierowanej przeciwko żywotnym interesom informacyjnym RP. W dobie cyfryzacji szczególnego znaczenia nabiera cyberbezpieczeństwo, stanowiące kluczowy element ochrony informacyjnej państwa. Stąd, w dobie bardzo szybkiego rozwoju technik informatycznych, teleinformatycznych oraz cyfrowych działalność wywiadowcza na rzecz obcego wywiadu może być również prowadzona wyłącznie z wykorzystaniem tego typu technik przesyłu informacji. Artykuł wskazał, że działalność wywiadowcza prowadzona na szkodę RP stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa informacyjnego. Ten stan rzeczy dostrzegł również polski system prawny, który przewiduje w tym zakresie szczególne sankcje karne klasyfikując działalność wywiadowczą jako przestępstwo przeciwko Rzeczypospolitej Polskiej. Ustawodawca przewiduje surową odpowiedzialność karną za szpiegostwo i współpracę z obcymi służbami wywiadowczymi, uregulowaną w art. 130 kodeksu karnego. Przeprowadzona interpretacja zawartych w tym artykule norm prawnych jednoznacznie wykazała szereg działań i zachowań, które wyczerpują dyspozycje norm prawnych ujawniających poszczególne czyny zakwalifikowane jako działalność wywiadowczą. Ujawniona analiza pokazała również, że w czasie rosnących zagrożeń militarnych w regonie Europy Środkowo-Wschodniej oraz rozpoznawania szerokiego spectrum zagrożeń hybrydowych oraz uczestnictwa w walce informacyjnej odpowiedź ustawodawcy na uczestnictwo w działalności wywiadowczej wiąże się z surowymi sankcjami karnymi, włącznie z karą dożywotniego pozbawienia wolności.

Bibliografia

Agencja Bezpieczeństwa Wewnętrznego, Środki pracy wywiadowczej i kontrwywiadowczej, Emów 2017.

Doktryna Bezpieczeństwa Informacyjnego RP – projekt, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

Grześkowiak A., Funkcja karząca prawa karnego na tle polskiego prawa karnego, [w:] J. Kulesza, A. Liszowska (red.), Prodignitate legis et maiestate iustitiae. Księga jubileuszowa z okazji 70. rocznicy urodzin Profesora Witolda Kuleszy, Łódź 2020.

Hoc S., Szpiegostwo w znowelizowanym kodeksie karnym, „Nowa Kodyfikacja Prawa Karnego", Wrocław 2023, t. LXVII.

Jaśkowiec M., Branie udziału w działalności obcego wywiadu. Wybrane prawnokarne aspekty szpiegostwa, „Kwartalnik kadry Kierowniczej Policji" 2022, nr 2.

Juchacz W., Przestępstwo szpiegostwa na szkodę RP, „Studia z zakresu nauk prawnoustrojowych", Miscellanea 2019, nr 9.

Kulesza J., Kodeks karny. Komentarz, Warszawa 2025, Lex/el.

Liderman K., Malik A., Polityka informacyjna a bezpieczeństwo informacyjne, „Studia Bezpieczeństwa Narodowego" 2013, nr 4.

Majewski J., Kodeks karny. Komentarz, Warszawa 2024, Lex/el.

Mozgawa M., Kodeks karny. Komentarz aktualizowany, Warszawa 2025, Lex/el.

Nowikowska M., Ochrona informacji niejawnych w systemie bezpieczeństwa państwa po wejściu Rzeczypospolitej Polskiej do NATO, [w:] K. Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik, Bezpieczeństwo narodowe Rzeczypospolitej Polskiej – 25 lat członkostwa w NATO, Warszawa 2024.

Ocieczek G., Wybrane zagadnienia związane z przestępstwem szpiegostwa, „Consillum Iuridicum" 2024, nr 3 (11).

Ruzikowski T., Instrukcja pracy operacyjnej aparatu bezpieczeństwa (1945-1989), „Materiały pomocnicze Biura Edukacji Publicznej IPN", Warszawa 2004, t. I.

Witczak M., Biały wywiad w zarządzaniu bezpieczeństwem informacji, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, nr 30.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 24 listopada 2017 r., II AKa 269/17, Lex.

Żebrowski A., Bezpieczeństwo informacyjne Polski a walka informacyjna, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.

Żebrowski A., Bezpieczeństwo służb specjalnych. Wybrane aspekty, [w:] F. Bylok, A. Kwiatek, M. Skiba (red.), Wybrane aspekty bezpieczeństwa pozamilitarnego. Zagrożenia-wyzwania-koncepcje, Częstochowa 2022.