RAFAŁ WĄDOŁOWSKI
ORCID: 0000-0003-0601-1213

DOI: 10.4467/20801335PBW.21.025.14302

Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne

Bieżące kierunki polskiej polityki międzynarodowej świadczą o dążeniu do zacieśniania gospodarczej i militarnej współpracy Rzeczpospolitej Polskiej ze Stanami Zjednoczonymi Ameryki. Wiedza o przyjętych w USA aktualnych regulacjach prawnych dotyczących bezpieczeństwa tajemnic publicznoprawnych może być jednym z wielu elementów wspierających kształtowanie optymalnego systemu ich ochrony w RP. Jest to szczególnie ważne w kontekście współdziałania Sił Zbrojnych RP z komponentami US Army rozlokowanymi na terytorium naszego kraju. Rzeczpospolita Polska jest związana wieloma umowami bilateralnymi z USA[1]. W 2020 r. zawarto niezwykle ważną umowę dotyczącą wzmocnionej współpracy obronnej, która konstytuuje i szczegółowo określa uwarunkowania prawne, gospodarcze i militarne pobytu Sił Zbrojnych USA na terytorium RP[2]. Strony umowy zdefiniowały rozumienie informacji niejawnych we wzajemnych stosunkach, wskazując między innymi na to, że są to informacje, które

[1] *Ustawa z dnia 20 marca 2015 r. o ratyfikacji Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie* (DzU z 2015 r. poz. 686); *Memorandum o porozumieniu między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzajemności w ramach zamówień obronnych, podpisane w Waszyngtonie dnia 27 sierpnia 2011 r. oraz w Warszawie dnia 8 września 2011 r.* (DzU z 2012 r. poz. 975); *Umowa o zabezpieczeniu społecznym między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisana w Warszawie dnia 2 kwietnia 2008 r.* (DzU z 2009 r. nr 46 poz. 374); *Protokół dodatkowy między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisany w Brukseli dnia 12 stycznia 2004 r., do Traktatu o stosunkach handlowych i gospodarczych między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, sporządzonego w Waszyngtonie dnia 21 marca 1990 r.* (DzU z 2005 r. nr 3 poz. 14).

[2] Zob. szerzej: *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzmocnionej współpracy obronnej, podpisana w Warszawie dnia 15 sierpnia 2020 r.* (DzU z 2020 r. poz. 2153).

wymagają ochrony zgodnie z prawem i regulacjami wewnętrznymi stron[3]. W kontekście ochrony tajemnic nie można pominąć umownego ustanowienia jurysdykcji umawiających się państw dotyczącej ścigania sprawców przestępstw, które potencjalnie mogą popełnić obywatele każdej ze stron na szkodę drugiego państwa[4]. W celu budowania sojuszniczej interoperacyjności warto poddać analizie amerykańskie przepisy karne i administracyjne, które regulują ochronę informacji niejawnych (*classified information*[5]). Jest to istotne z powodu deficytu aktualnych opracowań w przedmiotowym zakresie. Relewantność przedmiotowego zagadnienia wynika także z historycznych uwarunkowań, tj. kształtowania systemu ochrony tajemnic państwowych w Polsce podczas kilkudziesięcioletniego wpływu na nasz kraj wschodniego modelu zarządzania państwem. Polski system ochrony publicznoprawnych informacji był determinowany zmianami systemu politycznego, które następowały w ubiegłym stuleciu z woli narodu, a niekiedy wbrew niej. Po odzyskaniu niepodległości niebagatelne znaczenie miała recepcja do polskiego porządku prawnego kodeksu karnego feudalnej Rosji z 1903 r.[6] Rosyjskie prawodawstwo wywarło wpływ na kształtowanie polskich instytucji prawa karnego, w tym dotyczących ochrony tajemnic. Proces „sowietyzacji" przepisów karnych nasilił się w okresie socjalistycznego ustroju Polski, tj. od zakończenia II wojny światowej do 1990 r., i pomimo wprowadzenia licznych zmian i nowelizacji aktów prawnych nie można pominąć wpływu rosyjskiego prawodastwa na ukształtowanie aktualnej treści polskich przepisów prawnych.

Przyjmując powyższą argumentację za trafną, można sformułować następującą hipotezę badawczą: procedura weryfikacji osób przed udostępnieniem im informacji niejawnych oraz przesłanki odpowiedzialności karnej za ujawnienie lub wykorzystanie tajemnic publicznoprawnych w USA są krańcowo odmienne od obowiązujących w RP. W celu weryfikacji przyjętej hipotezy należy podjąć próbę sformułowania, uzasadnionych

---

[3] Tamże, art. 2 lit. j: „Wyrażenie »informacje niejawne« oznacza informacje wytworzone przez lub dla Ministerstwa Obrony Narodowej Rzeczypospolitej Polskiej lub Departament Obrony Stanów Zjednoczonych Ameryki (w Stanach Zjednoczonych jako »wojskowe informacje niejawne«), lub informacje, którymi one prawnie dysponują lub które znajdują się pod ich kontrolą, i które wymagają ochrony zgodnie z prawem i regulacjami wewnętrznymi Stron oraz postanowieniami niniejszej Umowy. Informacje niejawne mogą mieć formę ustną, wizualną, elektroniczną, formę dokumentu, lub dowolną inną formę, w tym także formę sprzętu lub technologii".

[4] Tamże, art. 14 ust. 1: „Rzeczypospolita Polska uznaje szczególne znaczenie nadzoru dyscyplinarnego władz sił zbrojnych USA nad członkami sił zbrojnych USA oraz skutki, jakie taki nadzór ma dla gotowości operacyjnej. Tym samym, Rzeczpospolita Polska, na wniosek Stanów Zjednoczonych w celu realizacji zobowiązania o wzajemnej obronie, niniejszym korzysta ze swojego suwerennego prawa i zrzeka się pierwszeństwa Rzeczypospolitej Polskiej w sprawowaniu jurysdykcji karnej".

[5] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski. Prawie wszystkie tłumaczenia w artykule pochodzą od autora (przyp. red.).

[6] *Уголовное уложение от 1903 г.* (Собрание узаконений и распоряжений правительства от 16 Апреля 1903 г. номер 88) [*Kodeks karny z 1903 r.* (Zbiór ustaw i rozporządzeń rządowych z 16 kwietnia 1903 r., numer 88)].

materiałem badawczym, odpowiedzi na następujące pytania: 1. Czy w USA weryfikacja osób przed udostępnieniem niejawnych informacji jest określona prawem, a jeżeli tak, to jaki jest zakres tych regulacji oraz charakter podmiotów wykonujących to prawo? 2. Czy w USA ujawnienie lub bezprawne wykorzystanie informacji niejawnych jest sankcjonowane, a jeżeli tak, to jakie są podstawy odpowiedzialności depozytariusza tajemnicy?

Relewantne regulacje prawne tworzące system ochrony tajemnic USA

W przeciwieństwie do konstytucyjnych regulacji w RP[7] oraz Federacji Rosyjskiej[8] Konstytucja USA[9] nie precyzuje *expressis verbis* prawa obywateli USA do informacji. Nie jest ono również wskazane wśród innych praw i swobód obywatelskich w treści późniejszych poprawek do przywołanej konstytucji. Na uwagę zasługuje pierwsza poprawka, która została przyjęta w 1791 r. Jej wprowadzenie skutkowało pojawieniem się w amerykańskim systemie prawa przepisów dotyczących między innymi wolności prasy i słowa[10].

Z uwagi na omawianą problematykę nie można pominąć również dziewiątej poprawki, zgodnie z którą wyszczególnienie w Konstytucji USA określonych praw nie wyklucza istnienia oraz nie ogranicza innych praw, które nie są w niej wskazane. Tak więc ustanowienie prawa do informacji może nastąpić w akcie niższej rangi, tj. ustawie federalnej[11].

---

[7] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.* (DzU z 1997 r. nr 78 poz. 483, ze zm.), art. 61 ust. 1: „Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa".

[8] *Конституция Российской Федерации от 12 декабря 1993 г.*, статья 29.4: „Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом" (*Konstytucja Federacji Rosyjskiej z 12 grudnia 1993 r.*, art. 29.4: „Każdy ma prawo do swobodnego poszukiwania, uzyskiwania, przekazywania, tworzenia i rozpowszechniania informacji w dowolny, zgodny z prawem, sposób. Wykaz informacji stanowiących tajemnicę państwową określa ustawa federalna").

[9] *Constitution of the United States of America*, House of Representatives, dok. No 110 – 50, 110th Congress, https://www.govinfo.gov/content/pkg/CDOC-110hdoc50/pdf/CDOC-110hdoc50.pdf [dostęp: 4 VI 2021].

[10] Pierwsza poprawka: „Żadna ustawa Kongresu nie może wprowadzić religii ani zabronić swobodnego praktykowania jej, ograniczać wolności słowa lub prasy ani prawa ludu do spokojnych zgromadzeń lub do składania naczelnym władzom petycji o naprawienie krzywd" (tłum. A. Pułło, *Konstytucja Stanów Zjednoczonych Ameryki*, Warszawa 2002).

[11] *Konstytucja Stanów Zjednoczonych Ameryki* w artykule 1 ust. 8 zawiera enumeratywne wyliczenie dziedzin, w odniesieniu do których Kongres Stanów Zjednoczonych ma prawo wydawać ustawy regulujące. Są one skodyfikowane w *United States Code* (dalej: USC) (*Kodeksie Stanów Zjednoczonych*).

Najistotniejszą regulacją uprawniającą obywateli USA do uzyskiwania informacji o funkcjonowaniu administracji rządowej jest federalna *Ustawa o wolności informacji* z 1966 r.[12] Amerykański prawodawca ustanowił w niej prawa osoby zainteresowanej uzyskaniem informacji oraz obowiązki podmiotów zobligowanych do jej udzielenia. W § 522 ust. b pkt 1–9 oraz § 522b ust. c pkt 1–10 określono przypadki wyłączające prawo do informacji, które mogą zostać zastosowane, jeżeli dany organ zdecyduje, że dane informacje spełniają kryteria ustanowione ww. przepisami.

Pierwszą przesłanką umożliwiającą odmowę udzielenia informacji jest jej zaliczenie do informacji niejawnych z uwagi na interes obrony narodowej albo polityki zagranicznej[13]. Przedmiotowa regulacja jest co do istoty zbieżna z polskimi przepisami ustawy o dostępie do informacji publicznej[14], w tym z jej art. 5. W USA istnieje też wiele odrębnych regulacji wyłączających dostęp do informacji publicznej o działalności podmiotów państwowych, czego przykładem może być § 3507 *Kodeksu Stanów Zjednoczonych*[15], w którym amerykański prawodawca między innymi zwalnia dyrektora Wywiadu Narodowego (Director of National Intelligence, DNI)[16] z obowiązku stosowania się do jakichkolwiek przepisów nakazujących ujawnienie: organizacji, funkcji, nazwisk, oficjalnych tytułów, wynagrodzeń lub liczby pracowników zatrudnionych we Wspólnocie Wywiadów (Intelligence Community, IC)[17].

Kodeks składa się z 54 tytułów podzielonych co do zasady kolejno na: rozdziały, części, sekcje, paragrafy, ustępy, punkty i litery. Ustawodawstwo federalne w USC obejmuje m.in. takie działy, jak: *Organizacja rządu i jego pracownicy* (tytuł 5), *Bezpieczeństwo wewnętrzne* (tytuł 6), *Siły zbrojne* (tytuł 10), *Przestępstwa i postępowanie karne* (tytuł 18), *Sądownictwo i procedura sądowa* (tytuł 28), *Wojna i obrona narodowa* (tytuł 50), https://uscode.house.gov/browse.xhtml [dostęp: 4 VI 2021].

[12] *Freedom of Information Act* of 1966, USC, Title 5, § 552 (*Ustawa o wolności informacji* z 1966 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 522.)

[13] Tamże, § 522 ust. b pkt 1 lit. A i lit. B: „This section does not apply to matters that are: (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order" („Niniejszy paragraf nie ma zastosowania do spraw, które są: (1)(A) specjalnie zatwierdzonymi zgodnie z kryteriami ustanowionymi w zarządzeniu wykonawczym, które mają być utrzymywane w tajemnicy w interesie obrony narodowej lub polityki zagranicznej oraz (B) są rzeczywiście właściwie sklasyfikowane zgodnie z takim zarządzeniem wykonawczym").

[14] *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej* (t.j.: DzU z 2020 r. poz. 2176).

[15] USC, Title 50, Chapter 46, § 3507 (*Kodeks Stanów Zjednoczonych,* tytuł 50, rozdział 46, § 3507), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section3507&num=0&edition=prelim [dostęp: 21 I 2021].

[16] Director of National Intelligence, urząd utworzony ustawą Kongresu USA o zapobieganiu terroryzmowi i reformie służb specjalnych z 2004 r. – *Intelligence Reform and Terrorism Prevention Act* of 2004, USC, Title 50, § 401, Public Law 108 – 458 (*Ustawa o zapobieganiu terroryzmowi i reformie służb specjalnych* z 2004 r., *Kodeks Stanów Zjednoczonych*), https://www.govinfo.gov/content/pkg/STATUTE-118/pdf/STATUTE-118-Pg3638.pdf [dostęp: 4 VI 2021].

[17] Nazwa *Intelligence Community* została użyta w *The President Executive Order 12333* of 1981, *United States Intelligence Activities* (*Zarządzeniu Wykonawczym Prezydenta 12333* z 1981 r., *Działania Wywiadowcze Stanów Zjednoczonych*), które w 2008 r. zostało znowelizowane *The President Executive Order 13470* of 2008, *United States Intelligence Activities* (*Zarządzeniem Wykonawczym 13470*

Ważnym judykatem w kontekście tych dwóch wartości, tj. prawa do informacji i prawa do odmowy jej udzielenia, jest wyrok wydany w procesie: magazyn „Hustler" versus Falwell[18]. Nie zagłębiając się w szczegóły sporu, należy odnotować, że był on spowodowany parodią reklamy napojów alkoholowych zamieszczoną w miesięczniku „Hustler", w której wykorzystano wizerunek duchownego Jerry'ego Falwella bez jego zgody. Po długotrwałym procesie sądowym w kilku instancjach Sąd Najwyższy USA w uzasadnieniu rozstrzygnięcia oparł się na pierwszej poprawce, którą zinterpretował bardzo szeroko. Podniósł między innymi, że wolność wyrażania swoich myśli nie jest wyłącznie prawem indywidualnym, a więc dobrem samym w sobie. Dodatkowo wskazał, że wolność słowa jako prawo jest podstawą wspólnego poszukiwania prawdy i siłą całego społeczeństwa[19]. Wspomniany sąd dostrzegł na tle rozpoznawanego konfliktu dotyczącego wolności prasy, że niebagatelną rolą środków masowego przekazu jest poszukiwanie prawdy, czyli zdobywanie obiektywnych informacji.

Prawo żądania udzielenia informacji jest ograniczone obowiązkiem ochrony informacji niejawnych przez ich depozytariusza. W amerykańskim piśmiennictwie prawniczym moc wiążąca imperatywu zakazu ujawniania informacji niejawnych jest szeroko

---

z 2008 r., *Działania Wywiadowcze Stanów Zjednoczonych*). Zarządzenie definiuje służby tworzące wspólnotę: „Office of the Director of National Intelligence, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs, the intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, intelligence elements of the Federal Bureau of Investigation, Office of National Security Intelligence of the Drug Enforcement Administration, Office of Intelligence and Counterintelligence of the Department of Energy, Bureau of Intelligence and Research of the Department of State, Office of Intelligence and Analysis of the Department of the Treasury, Office of Intelligence and Analysis of the Department of Homeland Security, intelligence and counterintelligence elements of the Coast Guard, and such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community" („Biuro Dyrektora Wywiadu Narodowego, Centralna Agencja Wywiadowcza, Agencja Bezpieczeństwa Narodowego, Agencja Wywiadu Obronnego, Narodowa Agencja Wywiadu Geoprzestrzennego, Krajowe Biuro Rozpoznania, inne biura w Departamencie Obrony zajmujące się gromadzeniem informacji przez krajowe i zagraniczne programy rozpoznawcze; jednostki wywiadowcze i kontrwywiadowcze Wojsk Lądowych, Marynarki Wojennej, Sił Powietrznych i Piechoty Morskiej, elementy wywiadowcze Federalnego Biura Śledczego, Biuro Wywiadu Bezpieczeństwa Narodowego Administracji ds. Walki z Narkotykami, Biuro Wywiadu i Kontrwywiadu Departamentu Energii, Biuro Wywiadu i Badań Departamentu Stanu, Biuro Wywiadu i Analiz Departamentu Skarbu, Biuro Wywiadu i Analiz Departamentu Bezpieczeństwa Wewnętrznego, elementy wywiadu i kontrwywiadu Straży Przybrzeżnej, i inne elementy dowolnego departamentu lub agencji, które mogą być wyznaczone przez prezydenta lub wyznaczone wspólnie przez dyrektora i szefa danego departamentu lub agencji jako element Wspólnoty Wywiadów"). Należy dodać, że DIA oraz FBI prowadzą także działania kontrwywiadowcze. Zob. https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf [dostęp: 4 VI 2021].

[18] Wyrok Sądu Najwyższego USA w sprawie „Hustler" v. Falwell, 485 U.S. 46, 24 II 1988 r.

[19] Tamże, s. 51: „(…) freedom to speak one's mind is not only an aspect of individual liberty – and thus a good unto itself – but also is essential to the common quest for truth and the vitality of society as a whole".

komentowana. Heidi Kitrosser negatywnie ocenia ferowanie przez sądy dotkliwych wyroków za ujawnienie informacji niejawnych. Według niej sąd powinien uzyskać stanowisko rządu w sprawie szkód, jakie wynikły z ujawnienia informacji istotnych dla bezpieczeństwa narodowego, oraz rozważyć, czy dla interesu publicznego korzyści wynikające z ujawnienia informacji przeważają nad przewidywanymi szkodami[20]. Aktem prawnym, w który kompleksowo określono zasady postępowania z informacjami niejawnymi, w tym ich klasyfikowanie, deklasyfikowanie (zmianę lub pozbawienie klauzuli) oraz procedurę udostępniania tajemnic, jest *Zarządzenie Wykonawcze Prezydenta 13526* z 2009 r.[21] Przywołany akt zawiera część wstępną, która może być uznana za uzasadnienie ograniczania przez rząd ustawowego prawa obywateli do informacji. Głównym argumentem przytoczonym przez prezydenta USA jest bezpieczeństwo narodowe postrzegane w wymiarze wewnętrznym i zewnętrznym, w tym ochrona społeczeństwa przed międzynarodowym terroryzmem. W zarządzeniu zdefiniowano podmioty uprawnione do selekcji informacji i ich klasyfikacji jako niejawne. Są to wyłącznie podmioty rządowe, a przede wszystkim administracja, która tworzy rząd pod kierunkiem prezydenta USA, oraz inne agencje i organy państwowe. Podkreślono, że agencja, która nadaje informacji klauzulę tajności, nie ma obowiązku uzasadniać swojej decyzji. Jednocześnie zastrzeżono, że główną przesłanką wyłączenia powszechnego dostępu do określonej informacji jest szkoda dla bezpieczeństwa narodowego, jaką mogłoby spowodować upublicznienie informacji objętej ochroną. Relewantnym elementem omawianej regulacji jest zobowiązanie podmiotu klasyfikującego do pozostawania w gotowości do pisemnego określenia potencjalnej szkody, która była podstawą jej utajnienia, i w konsekwencji odmowy upublicznienia (w przypadku wystąpienia z takim wnioskiem przez osobę zainteresowaną informacją). Kryterium rozstrzygającym o utajnieniu jest więc potencjalna szkoda dla interesu państwa, podobnie jak w systemie ochrony tajemnic RP.

Polski ustawodawca w art. 1 ust. 1 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[22] (dalej: ustawa o.i.n.) wskazuje kryteria, których należy użyć

---

[20] Zob. szerzej: H. Kitrosser, *Leak prosecutions and first amendment: New developments and a closer look at the feasibility of protecting leakers*, „William and Mary Law Review" 2015, nr 4, s. 1262 i nast., https://scholarship.law.wm.edu/wmlr/vol56/iss4/7 [dostęp: 4 VI 2021]. Heidi Kitrosser, profesor Uniwersytetu Minnesota, specjalizuje się w badaniu skutków oddziaływania społeczeństwa na sprawowanie władzy państwowej w USA przez korzystanie z prawa do informacji na podstawie pierwszej poprawki do *Konstytucji Stanów Zjednoczonych Ameryki*, https://www.law.umn.edu/profiles/heidi-kitrosser [dostęp: 7 VI 2021].

[21] *The President Executive Order 13526* of 2009, *Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 13526* z 2009 *r.*, *Informacje Niejawne Bezpieczeństwa Narodowego*), akt jest modyfikacją poprzedniego zarządzenia 13292 z 25 III 2003 r., które zmieniało *The President Executive Order 12958*, *Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 12958* z 17 IV 1995 r.).

[22] Tekst jednolity: DzU z 2019 r. poz. 742, art. 1 ust. 1: „Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej »informacjami niejawnymi«".

w procesie selekcji jawnych informacji w celu wyodrębnienia tylko takich, które z uwagi na konstytucyjne przesłanki ograniczenia prawa do informacji można utajnić albo wytworzyć jako niejawne. Ustanowionymi weryfikatorami są skutki, jakie mogłyby nastąpić w wyniku ujawnienia tego rodzaju informacji, czyli: 1) wystąpienie szkody dla RP, 2) spowodowanie zagrożenia wystąpienia szkody dla RP, 3) wywołanie niekorzystnego stanu interesów RP. Analizując przywołane przesłanki, należy zauważyć, że tworzą one **materialną definicję informacji niejawnych**[23], wskazują bowiem na treść, a nadanie klauzuli jest jedynie formalnym oznaczeniem chronionych informacji (komunikatem dla dysponenta wskazującym charakter informacji). W przypadku ustalenia, że ujawnienie danej informacji doprowadzi do zaistnienia chociażby jednego z wymienionych skutków, należy dokonać jej klasyfikacji i nadać odpowiednią klauzulę ochrony, a więc zastosować się do nakazu ustanowionego w art. 5 ustawy o.i.n. Jak wskazuje Trybunał Konstytucyjny w uzasadnieniu wyroku z 2009 r., *Obowiązek przyznawania właściwej klauzuli tajności istnieje i wynika z materialnoprawnych kryteriów klasyfikacji informacji oraz art. 7 Konstytucji*[24].

W procesie klauzulowania należy więc rozważyć, czy w związku z ujawnieniem danej informacji zostaną zagrożone interesy USA, a jeżeli nastąpi szkoda, to jaka, w jakiej formie i w jakim wymiarze. Przedmiotowa regulacja w części dotyczącej braku konieczności formułowania uzasadnienia decyzji klasyfikacyjnej w procesie jej podejmowania jest zbieżna z polskimi przepisami. Amerykański prawodawca uznał, że nieuprawnione ujawnienie klauzulowanych informacji nie jest przesłanką automatycznego pozbawienia ochrony lub zmiany klauzuli informacji niejawnych, podobnych lub tożsamych z ujawnionymi[25]. Przedmiotowe ujęcie tego ważnego problemu pozostaje więc w opozycji do ugruntowanego w polskiej literaturze poglądu, że upublicznione tajemnice nie podlegają karnoprawnej ochronie[26]. Jonathan Abel wskazuje, że pozostawienie upublicznionych informacji jako niejawnych wydaje się bezprzedmiotowe. Argumentuje, że przecież tajemnice USA rozpowszechnione przez Edwarda Snowdena są znane milionom użytkowników Internetu, a mimo to pozostają nadal niejawne, co wyłącza je z publicznej debaty – ze szkodą dla wolności mass mediów[27].

---

[23] Wyróżnienia w tekście pochodzą od autora (przyp. red.).

[24] Wyrok TK z 15 października 2009 r. sygn. akt K 26/08, uzasadnienie – pkt 183.

[25] *The President Executive Order 13526*…, article 1 section 1 letter c: „Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information" (*Zarządzenie Wykonawcze Prezydenta USA 13526*…, art. 1 ust. 1 lit. c*:* „Informacji niejawnych nie odtajnia się automatycznie w wyniku nieuprawnionego ujawnienia identycznych lub podobnych informacji").

[26] Zob. szerzej: M. Leciak, *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, s. 188–190; K. Lewandowski, *Przestępstwa przeciwko ochronie informacji w świetle rozdziału XXXIII Kodeksu karnego*, *orzecznictwa i doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 63; A. Marek., V. Konarska-Wrzosek, *Prawo karne*, Warszawa 2016, s. 682.

[27] Zob. szerzej: J. Abel, *Do you have to keep the Government's secrets*? *Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record*, „University of Pennsylwania Law Review" 2015, nr 4, s. 1039 i nast.

W zarządzeniu 13526 zdefiniowano pojęcie „informacja”[28] oraz wprowadzono trzy poziomy klauzul ochronnych, które są odpowiednie do szkód, jakie mogłoby spowodować nieuprawnione ujawnienie danego rodzaju informacji. Jak już zasygnalizowano, we wspomnianym zarządzeniu zobowiązano organ przyznający klauzulę do pozostawania w gotowości do zidentyfikowania lub opisania potencjalnych szkód w razie konieczności uzasadnienia podjętej decyzji klasyfikacyjnej w odniesieniu do konkretnej informacji, którą utajnił. I tak:

1) klauzulę „Top Secret” stosuje się w odniesieniu do informacji, której nieuprawnione ujawnienie (przy uwzględnieniu racjonalnych przesłanek oceny) mogłoby spowodować **wyjątkowo poważną** szkodę dla bezpieczeństwa narodowego,
2) klauzulę „Secret” stosuje się do ochrony informacji, której nieuprawnione ujawnienie mogłoby spowodować **poważną** szkodę dla bezpieczeństwa narodowego,
3) klauzula „Confidential” jest stosowana z zachowaniem warunków wskazanych w pkt 1, przy czym szkoda nie jest wartościowana.

Zgodnie z omawianym zarządzeniem 13526 przy klasyfikowaniu informacji należy kierować się ogólną zasadą nadawania informacjom bezpośrednio niższej klauzuli, jeżeli wystąpiły istotne wątpliwości co do przyznania adekwatnego poziomu ochrony[29]. Jeżeli nie można rozstrzygnąć, jakiego rodzaju szkoda wystąpiłaby po ujawnieniu informacji stanowiącej tajemnicę, np. czy byłaby ona wyjątkowo poważna, czy jedynie poważana, taką informację należy objąć niższym poziomem ochrony. Powyższa regulacja „uelastycznia” proces klasyfikacji informacji, a tym samym pozwala na uniknięcie ewentualnych zarzutów celowego zaniżenia albo zawyżenia nadanej klauzuli. Przepisy polskiej ustawy o.i.n. w tym zakresie są znacznie bardziej złożone[30], dlatego wydaje się, że recepcja tego rozwiązania na grunt krajowego prawodawstwa byłaby korzystna.

Ogólna przesłanka utajniania informacji, tj. bezpieczeństwo narodowe, w tym ochrona przed międzynarodowym terroryzmem, została doprecyzowana w części I, art. 1 ust. 4 omawianego zarządzenia, w którym enumeratywnie określono sfery podlegające ochronie. Są to:

1) wojskowe plany, systemy uzbrojenia i operacje militarne,
2) informacje od rządów obcych państw,

---

[28] *The President Executive Order 13526*…, article 6 section 1 subsec. 1 letter t: „»Information« – means any knowledge that can be communicated or dokumentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government” (*Zarządzenie Wykonawcze Prezydenta 13526*…, art. 6 ust. 1 pkt 1 lit. t: „»Informacja« – oznacza wszelką wiedzę, którą można zakomunikować albo mającą postać dokumentu materialnego, bez względu na jego fizyczną formę lub cechy, która jest własnością rządu USA lub jest wytworzona przez [rząd] lub dla tego rządu albo jest nadzorowana przez Rząd Stanów Zjednoczonych”).

[29] *The President Executive Order 13526*…, article 1 section 2 letter. c: „If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level” (*Zarządzenie Wykonawcze Prezydenta USA 13526*…, art. 1 ust. 2 lit. c: „Jeśli istnieją poważne wątpliwości co do odpowiedniego poziomu klauzuli, klasyfikuje się [ją] na niższym poziomie”).

[30] Zob. szerzej: art. 9 ustawy o.i.n.

3) stosunki z innymi państwami oraz działania USA poza granicami kraju, w tym poufne zagraniczne źródła informacji,
4) działania służb specjalnych[31], w tym operacje pod przykryciem, źródła informacji oraz metody ich działania, kryptologia,
5) zagadnienia naukowe, technologiczne i ekonomiczne związane z bezpieczeństwem narodowym,
6) rządowe programy ochrony obiektów i materiałów nuklearnych,
7) potencjał: systemów, instalacji, infrastruktury, projektów i planów, a także służb ochrony związanych z bezpieczeństwem narodowym oraz ich słabe strony,
8) rozwój, produkcja oraz stosowanie broni masowego rażenia.

Regulacje ustanowione w art. 5 ustawy o.i.n. w zakresie kryteriów stosowanych w procesie nadawania klauzuli informacjom niejawnym wykazują co do zasady zbieżność ze stosowanymi w USA. Z tego względu warto poddać analizie adekwatne przepisy polskiej ustawy, należy bowiem zauważyć, że prawodawca po skonstruowaniu ogólnej definicji informacji niejawnych w art. 1, w art. 5 ust. 1–3 określa sfery, z których informacjom można nadać klauzulę „ściśle tajne", „tajne" albo „poufne". Między ogólną (abstrakcyjną) definicją informacji niejawnych a przedmiotowym określeniem obszarów aktywności państwa, które należy chronić przez limitowanie informacji, zachodzi relacja nadrzędności i podrzędności. Dziedziny (obszary) wymienione w art. 5 zawężają możliwość szerokiego ograniczania prawa do informacji w wyniku autonomicznego stosowania art. 1 ustawy.

Za uzasadnione należy uznać wątpliwości interpretacyjne powstające w kontekście nieostrych znaczeniowo pojęć, których ustawodawca użył do konstrukcji formalnoprawnych przesłanek służących do nadawania informacjom niejawnym wymaganego poziomu ochrony. Implikuje to pytanie, czy jakakolwiek osoba ustawowo uprawniona do nadania klauzuli[32] dysponuje dostateczną wiedzą, aby uznać, że ujawnienie określonej informacji niejawnej spowoduje albo mogłoby spowodować wystąpienie wyjątkowo poważnej lub poważnej szkody dla RP. Ustawodawca w art. 5 ust. 1–3 wymienia dziedziny, w których szkoda[33] ma wystąpić, ale nie definiuje, jak należy rozumieć szkodę i jakie są kryteria jej wartościowania. Ustawowe dookreślenie szkody w art. 5 ust.1 i ust. 2 pojęciami: „zagrozi", „pogorszy", „zakłóci", „utrudni" i „osłabi" nie wyznacza jasnych ram interpretacyjnych.

Konfrontacja kryteriów weryfikacyjnych wymienionych w art. 1 oraz art. 5 ustawy o.i.n. ujawnia niekonsekwencję ustawodawcy. Zgodnie z **materialną** definicją informacji niejawnych (art. 1) do uznania informacji za niejawną dostateczną przesłankę stanowi

[31] W tekście źródłowym użyto terminu „*intelligence activities*", który jest definiowany w ust. 6 pkt 1 lit. Y *Zarządzenia Wykonawczego Prezydenta 13526* jako „działania Wspólnoty Wywiadów" (IC).

[32] Art. 6 ustawy o.i.n.: „Osobą uprawnioną do nadania klauzuli jest osoba uprawniona do podpisania dokumentu lub oznaczenia danego materiału".

[33] Kierując się zasadą zakazu homonimiczności pojęć, należy przyjąć, że szkoda wskazana w art. 1 jest tożsama ze szkodą z art. 5.

„niekorzystny wpływ na interesy RP", natomiast w definicji **materialno-formalnej** (art. 5 ust. 1 i 2) kryterium niekorzystnego wpływu na interesy RP nie występuje. Można też rozważyć przypadek przyznania jawnej informacji statusu informacji niejawnej z uwagi na niekorzystny wpływ na interesy RP, który może zaistnieć po jej ujawnieniu. Jednocześnie tego typu informacja może pozostać bez klauzuli, ponieważ jej treść nie będzie związana tematycznie z dziedzinami wymienionymi w art. 5 ust. 1–3. Ustawodawca, wskazując na interesy RP w art. 1, odwoływał się do tych obszarów aktywności państwa, które są wymienione w art. 5 ust. 1–3. Przywołane przepisy należy więc stosować łącznie, ich odrębne stosowanie prowadzi bowiem do interpretacji *ad absurdum*.

Częściowo taką sytuację potwierdza stanowisko Naczelnego Sądu Administracyjnego, który stwierdza, że (…) *informacja jest informacją niejawną, nie w następstwie jej klasyfikacji, a z uwagi na zagrożenie wynikające z jej treści lub sposobu jej uzyskania. Chroniona jest zatem jak informacja niejawna bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą*[34]. Sąd słusznie uznał, że treść informacji jest priorytetową przesłanką objęcia jej ochroną państwa, a jednocześnie pominął formalną klasyfikację (oznaczenie klauzulą) jako element przesądzający o tej ochronie.

W USA informacje, które dotyczą powyżej wymienionych zagadnień, mogą zostać zaliczone do niejawnych tylko wówczas, gdy istnieją racjonalne przesłanki pozwalające przewidywać, że ich bezprawne upublicznienie przyniesie szkodę dla bezpieczeństwa narodowego Stanów Zjednoczonych. Podobnie jak w polskim ustawodawstwie w zarządzeniu nie określono wymiaru czasowego ochrony dla danej klauzuli[35]. Sprecyzowano, że może to być dowolny okres, co do zasady nie dłuższy niż 25 lat, albo określone zdarzenie, po którego zaistnieniu należy przeprowadzić deklasyfikację lub powtórną ocenę danej informacji. Amerykański prawodawca zastrzega jednocześnie, że żadne informacje nie mogą pozostać niejawne na zawsze. Wyjątkiem od zasady ochrony do 25 lat są między innymi dane personalne osobowych źródeł informacji (niejawnych współpracowników IC). Dodatkowo prezydent USA wprowadził przepisy prewencyjne, zakazujące utrzymywania w tajemnicy informacji lub obejmowania ich klauzulą, aby ukryć naruszenie prawa przez administrację albo ograniczyć konkurencję, albo ukryć informacje kłopotliwe dla osoby fizycznej lub prawnej. Przedmiotowa regulacja nie ma odzwierciedlenia w polskich aktach normatywnych, mimo że ma aksjologiczne

[34] Wyrok Naczelnego Sądu Administracyjnego z 6 VII 2017 r., sygn. akt. I OSK 932/16.

[35] Uwzględniając aspekt historyczny, warto zaznaczyć, że w nieobowiązującej *Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* polski ustawodawca w art. 25 ust. 1 i 3 wprowadzał ochronę informacji tajnych i ściśle tajnych przez 50 lat, poufnych przez 5 lat i zastrzeżonych przez 2 lata. Obowiązująca obecnie ustawa o.i.n. nie określa długości okresów ochrony, pozostawiając to ocenie osoby, która podpisała dokument, lub osoby odpowiedzialnej za przechowywanie danego materiału, a w odniesieniu do informacji ściśle tajnych – kierownikowi jednostki organizacyjnej przy uwzględnieniu aktualności przyczyn, które spowodowały objęcie ochroną danej informacji. Wyjątkiem od powyższej zasady są informacje wskazane w art. 7 ustawy o.i.n., które dotyczą pracowników służb prowadzących czynności operacyjno-rozpoznawcze i ich współpracowników, a także informacje pochodzące z wymiany międzynarodowej, o ile taki był warunek ich udostępnienia RP – tego rodzaju informacje są objęte ochroną na zawsze.

podstawy. Należy więc postulować wprowadzenie tej instytucji do polskiego systemu ochrony informacji niejawnych. Omawiane zarządzenie wprowadza ponadto zakaz pozostawienia niejawnymi informacji, które nie są ważne ze względu na bezpieczeństwo państwa.

Przyjęcie przedmiotowych przepisów w amerykańskim systemie prawnym wskazuje, że uprawnienie publicznych organów do utajniania informacji może sprzyjać nadużyciom. Ze względu na podobieństwa zasadniczych norm systemu polskiego i amerykańskiego należy uznać, że tożsame zagrożenia występują w Polsce.

Mimo szczegółowego określenia procedury deklasyfikacji tajemnic pozostających w dyspozycji administracji rządowej i nakazu jej bieżącego prowadzenia, zarządzeniem 13526 powołano odrębny organ państwowy – Narodowe Centrum Odtajniania informacji (National Declassification Center, NDC). Głównym zadaniem tego organu jest prowadzenie szkoleń, doradztwo i działania koordynacyjne w procesie odtajniania niejawnych informacji w rządowych jednostkach organizacyjnych. Innymi istotnymi postanowieniami zawartymi w zarządzeniu są zasady dostępu do tajemnic. Wyszczególniono trzy podstawowe warunki, które przed udostępnieniem informacji muszą zostać spełnione: 1) przyznanie uprawnień do dostępu do informacji niejawnych przez kierownika agencji lub osobę przez niego wyznaczoną, 2) podpisanie przez kandydata umowy poufności (*nondisclosure agreement*)[36], 3) dostęp do informacji jest uzasadniony wykonywanymi obowiązkami lub funkcją (zgodnie z zasadą *need to know*).

Organ wydający zgodę na zapoznanie się z informacjami niejawnymi jest również zobowiązany do zorganizowania szkolenia osoby spełniającej wymienione kryteria. Poznaje ona wówczas metody właściwej ochrony informacji niejawnych oraz zostaje pouczona o grożących sankcjach karnych, administracyjnych i odpowiedzialności cywilnej za bezprawne ujawnienie tajemnicy. Warunki wymienione w pkt 1 i 3 mają odpowiedniki w polskiej ustawie o ochronie informacji niejawnych. Warto przypomnieć, że w polskim porządku prawnym dostęp do tajemnic państwowych nie jest determinowany zawarciem umowy z państwem o zachowaniu uzyskanych informacji w tajemnicy. Osoba po zakończeniu szkolenia składa jedynie oświadczenie potwierdzające znajomość przepisów o ochronie informacji niejawnych.

[36] Pisemna umowa jest zawierana pomiędzy osobą, która otrzymuje dostęp do informacji niejawnych, a Stanami Zjednoczonymi. Dokument został wprowadzony do stosowania na mocy *The President Executive Order 12958*…(*Zarządzenia Wykonawczego Prezydenta 12958*…). Osoba zainteresowana zobowiązuje się do zachowania w tajemnicy oznaczonych i nieoznaczonych informacji niejawnych, w tym przekazanych ustnie. Potwierdza, że została poinformowana o przepisach dotyczących ochrony tajemnic, oraz deklaruje ich przestrzeganie, a ponadto, że zapoznano ją z odpowiedzialnością karną jej grożącą. Dodatkowo w treści umowy oświadcza, że pouczono ją o tym, że w wyniku niewłaściwego postępowania z informacjami niejawnymi uprawniony organ może odebrać poświadczenie bezpieczeństwa, które posiada, co z kolei może być podstawą wypowiedzenia stosunku pracy. Zainteresowany zrzeka się na rzecz USA również wszelkich honorariów, należności i wynagrodzeń otrzymanych w związku z ujawnieniem informacji. Końcowy rozdział umowy zawiera wskazówki dla strony i obejmuje okres po zakończeniu udostępniania jej tajemnic, między innymi zawiera pouczenie o zagrożeniu szpiegostwem.

Ogólnokrajowy nadzór nad przetwarzaniem informacji niejawnych sprawuje w USA Urząd Nadzoru Bezpieczeństwa Informacji (Information Security Oversight Office, ISOO)[37]. W zarządzeniu ustanowiono podległość tego organu Archiwum Państwowemu USA i określono jego zadania, w tym:

1) opracowanie aktów wykonawczych w celu implementacji zarządzenia 13526,
2) nadzorowanie agencji rządowych w celu zapewnienia zgodności ich działalności z zarządzeniem i aktami wykonawczymi,
3) składanie prezydentowi USA, przynajmniej raz w roku, raportu z przebiegu implementacji zarządzenia[38].

W polskim systemie ochrony tajemnic nie ma podmiotów tożsamych z NDC i ISOO, jednak podobne zadania nadzorcze są realizowane przez ABW i SKW, zgodnie z właściwością rzeczową tych służb specjalnych. W tym miejscu warto wskazać na istotną rolę Instytutu Pamięci Narodowej, który w celu realizacji ustawowych zadań gromadzi materiały, w tym niejawne, wytworzone przed 6 maja 1990 r. Prezes IPN w każdym czasie może zażądać nieprzekazanych dotychczas dokumentów od: ministra właściwego do spraw wewnętrznych, ministra obrony narodowej, ministra sprawiedliwości, prezesa sądu powszechnego i wojskowego, prokuratora kierującego powszechną jednostką organizacyjną prokuratury, dyrektora Archiwum Akt Nowych oraz innego archiwum państwowego, szefów Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, a także innych instytucji. Na podstawie art. 27 ustawy o IPN prezes IPN jest uprawniony do uzyskania wglądu w dokumenty, jeżeli istnieje uzasadnione przypuszczenie, że te dokumenty zawierają informacje z zakresu działania Instytutu[39]. W ramach działalności archiwalnej IPN gromadzi, ewidencjonuje, przechowuje, opracowuje, zabezpiecza i udostępnia dokumenty na temat zbrodni dokonanych w latach 1917–1990 oraz dokumenty ukazujące fakty i okoliczności dotyczące losów narodu polskiego w latach 1939–1990 (informujące o poniesionych ofiarach i wyrządzonych szkodach), a także wydaje na ich podstawie uwierzytelnione odpisy, wypisy, wyciągi i reprodukcje przechowywanych dokumentów.

W USA zarządzenie prezydenckie konstytuuje przepisy sankcjonujące świadome, umyślne albo wynikające z niezamierzonych zaniedbań naruszenia zasad postępowania z informacjami niejawnymi. Przewidywanymi konsekwencjami są: upomnienie, zawieszenie w obowiązkach bez wynagrodzenia, odwołanie ze stanowiska, wygaśnięcie upoważnienia do klasyfikacji, utrata lub odmowa dostępu do informacji niejawnych i inne sankcje, przewidziane w obowiązującym prawie i aktach normatywnych danej agencji.

---

[37] Urząd został powołany na mocy *The President Executive Order 12065* of 1978, *National Security Information* (*Zarządzenia Wykonawczego Prezydenta 12065* z 1978 r., *Informacje Bezpieczeństwa Narodowego*). Jego podporządkowanie oraz zadania realizowane przez ten podmiot były wielokrotnie modyfikowane. Zob. szerzej: https://www.archives.gov/isoo/about/history [dostęp: 12 II 2021].

[38] Zob. szerzej: *The President Executive Order 13526*…, section 5 (*Zarządzenie Wykonawcze Prezydenta 13526*…, ust. 5).

[39] Zob. szerzej: *Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu* (t.j.: DzU z 2021 r. poz. 177).

Dla porównania – regulacje mające charakter retorsji nie są wprost wyartykułowane w polskiej ustawie o ochronie informacji niejawnych, ewentualne konsekwencje dyscyplinarne wynikają z prawa pracy (ustaw pragmatycznych służb), karne natomiast – z zasad ogólnych. Ponadto utrata dostępu do tajemnic (poświadczenia bezpieczeństwa) może wynikać z przeprowadzonego kontrolnego postępowania sprawdzającego.

Drugim istotnym aktem prawnym kształtującym system bezpieczeństwa informacji niejawnych w USA jest *Zarządzenie Wykonawcze Prezydenta 12968* z 1995 r., *Dostęp do informacji niejawnych*[40]. Unormowano w nim tryb i zakres postępowania (*security background investigation*) realizowanego przez agencje państwowe wobec osób, którym mają być udostępnione informacje niejawne. W ogólnych zarysach jest to postępowanie odpowiadające postępowaniu sprawdzającemu, które jest przeprowadzane na podstawie polskiej ustawy o ochronie informacji niejawnych. Amerykański prawodawca wprowadza kilkanaście zastrzeżeń natury ogólnej. I tak, dostęp do informacji niejawnych:

1) co do zasady mogą mieć obywatele USA;
2) następuje po pozytywnym zakończeniu dochodzenia bezpieczeństwa (odpowiednio: postępowania sprawdzającego ustanowionego w rozdziale 5 polskiej ustawy o.i.n., którego ogólny zarys przedstawiono po omówieniu procedury obowiązującej w USA);
3) może uzyskać osoba, której osobista oraz zawodowa przeszłość wskazuje, że jest:
   – lojalna wobec USA i ma mocny charakter (rozumie się przez to, że nie jest ona uzależniona od używek, a także że jest asertywna),
   – wiarygodna, uczciwa i rzetelna,
   – dyskretna i roztropna,
   – niepodporządkowana innemu państwu i nieuzależniona od tajnego przymusu,
   – gotowa i zdolna przestrzegać przepisów regulujących korzystanie z informacji niejawnych, postępowanie z nimi i ich ochronę.

[40] *The President Executive Order 12968* of 1995, *Access to Classified Information*. Zarządzenie zostało znowelizowane w 2008 r. przez *The President Executive Order 13467*, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 13467, Reforma procedury związanej z oceną zdolności pracowników rządowych i uprawnień do uzyskania dostępu do informacji niejawnych bezpieczeństwa narodowego*), które ostatecznie zostało znowelizowane przez *The President Executive Order 13741* of 2016, *Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters* (*Zarządzenie Wykonawcze Prezydenta 13741* z 2016 r. *zmieniające Zarządzenie Wykonawcze 13467 w celu ustanowienia kompetencji i obowiązków Krajowego Biura Postępowań Sprawdzających i spraw z tym związanych*). Zob. https://www.govinfo.gov/content/pkg/DCPD-201600648/pdf/DCPD-201600648.pdf [dostęp: 4 VI 2021].

W myśl zarządzenia wszelkie wątpliwości co do wymienionych okoliczności należy rozstrzygać na korzyść bezpieczeństwa narodowego. Podobna norma generalna została zastosowana w art. 24 ust. 4 polskiej ustawy o.i.n.

Zgodnie z zarządzeniem 12968 uzyskanie poświadczenia bezpieczeństwa (*security clearance*) nie zależy od: rasy, koloru skóry, religii, płci, narodowości, niepełnosprawności lub orientacji seksualnej. Jeśli osoba sprawdzana korzysta z poradnictwa w zakresie zdrowia psychicznego, może to uzasadniać kolejne czynności mające na celu ustalenie, jak jej stan zdrowia wpływa na predyspozycje wymienione w pkt 3.

Interesującym rozwiązaniem jest możliwość zrezygnowania z prowadzenia kolejnego dochodzenia bezpieczeństwa w przypadku upływu ważności poświadczenia bezpieczeństwa. Pominięcie procedury sprawdzeniowej może nastąpić wówczas, gdy zostaną zachowane następujące warunki:

1) osoba sprawdzana będzie u tego samego pracodawcy zajmowała stanowisko z dostępem do tego samego rodzaju informacji niejawnych, jak te, które przetwarzała w okresie ważności ostatniego poświadczenia bezpieczeństwa,
2) brakuje informacji wskazujących na to, że zainteresowana osoba już nie spełnia kryteriów określonych w zarządzeniu 12968,
3) przedłużenie ważności następuje w odniesieniu do tej kategorii informacji niejawnych, do której dana osoba uzyskała dostęp na podstawie poświadczenia bezpieczeństwa wydanego w ostatnich pięciu latach,
4) ewentualna przerwa w zatrudnieniu danej osoby nie może być dłuższa niż dwa lata, a łączny okres od wydania ostatniego poświadczenia nie może przekraczać pięciu lat.

Polskie przepisy są mniej elastyczne, gdyż nie umożliwiają odstąpienia od przeprowadzenia kolejnego postępowania sprawdzającego[41].

W myśl zarządzenia 12968, jeżeli sytuacja osobista osoby uprawnionej albo inne okoliczności mające wpływ na bezpieczeństwo przekazywanych jej informacji uległy zmianie, uprawniony organ może przeprowadzić powtórne dochodzenie bezpieczeństwa. Jest to instytucja zbliżona do kontrolnego postępowania sprawdzającego

[41] Imperatyw wystąpienia z wnioskiem o przeprowadzenie kolejnego postępowania sprawdzającego na co najmniej sześć miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa posiadanego przez pracownika wynika z dyspozycji art. 32 ust. 1 ustawy o.i.n. Ważną przesłanką faktyczną uprawniającą kierownika do skorzystania z tego trybu jest zajmowanie przez osobę, mającą być sprawdzoną, stanowiska związanego z dostępem do informacji niejawnych o określonej klauzuli oraz zbliżający się koniec ważności poświadczenia bezpieczeństwa. Błędną interpretacją tego przepisu jest przyjęcie, że można go zastosować, kierując się jedynie przesłanką upływu terminu ważności posiadanego przez pracownika poświadczenia. Określony przez ustawodawcę termin sześciu miesięcy jest terminem instrukcyjnym, nie ma charakteru prekluzyjnego, złożenie wniosku wraz z ankietą z naruszeniem terminu nie powoduje bezskuteczności tej czynności. Wniosek powinien być złożony z wyprzedzeniem sześciomiesięcznym, aby organ podczas kolejnego postępowania sprawdzającego, prowadzonego w trybie poszerzonego lub zwykłego postępowania, zdążył rozstrzygnąć o utrzymaniu dotychczasowych uprawnień lub o ich zmianie przed końcem ważności poświadczenia, które osoba sprawdzana już posiada. Takie rozwiązanie zapewnia osobie sprawdzanej ciągłość pracy i pewność zatrudnienia, a także efektywne funkcjonowanie instytucji, tj. pracodawcy.

określonego w polskiej ustawie o.i.n. Ponadto prawodawca uprawnia właściwy organ wydający poświadczenia do bieżącej oceny osób, którym udzielono dostępu do tajemnic zgodnie z zasadami określonymi przez dyrektora Wywiadu Narodowego. Zasady, o których mowa w zarządzeniu, nie są publikowane. W przypadku otrzymania odmowy lub cofnięcia prawa dostępu do tajemnic USA osoba sprawdzana jest uprawniona do zapoznania się z dokumentami, na podstawie których podjęto negatywną decyzję. W wyjątkowych przypadkach kierownik agencji może odmówić udostępnienia materiałów z uwagi na naruszenie bezpieczeństwa narodowego USA. W takiej sytuacji organem odwoławczym od tego rodzaju odmowy jest komisja składająca się z co najmniej trzech pracowników (dwóch spoza pionu bezpieczeństwa) agencji, w której podjęto decyzję negatywną. Zarządzenie nie daje możliwości zaskarżenia decyzji komisji odwoławczej – jest ona ostateczna. Procedura odwoławcza i skargowa od negatywnych rozstrzygnięć organu uprawnionego do przyznania dostępu do tajemnic w RP jest diametralnie odmienna od stosowanej w USA. O zgodności z prawem odmowy wydania poświadczenia bezpieczeństwa, po wniesieniu skargi, rozstrzygają sądy administracyjne, w pierwszej instancji wojewódzki sąd administracyjny, w drugiej – Naczelny Sąd Administracyjny.

Prawo przyznawania dostępu do informacji niejawnych USA przysługujące agencjom państwowym jest określone w aktach powołujących te podmioty. Akta te są konsultowane z organami nadzorującymi programy bezpieczeństwa informacji niejawnych. Tego rodzaju agencje są zobowiązane do współpracy z ISOO oraz NDC, a przede wszystkim z dyrektorem Wywiadu Narodowego. Przykładem instytucji o szerokim spectrum oddziaływania na bezpieczeństwo tajemnic w aspekcie osobowym jest Agencja Bezpieczeństwa i Kontrwywiadu Obronnego (Defense Counterintelligence and Security Agency, DCSA)[42]. W październiku 2019 r. DCSA przejęła prowadzenie dochodzeń bezpieczeństwa od Krajowego Biura Postępowań Sprawdzających (National Background Investigations Bureau, NBIB), które utraciło autonomię i zostało podporządkowane DCSA. NBIB przeprowadzało postępowania wobec pracowników administracji rządowej i zapewniało realizację 95 proc. sprawdzeń dla agencji rządowych. Obecnie DCSA prowadzi postępowania nie tylko wobec urzędników lub kontrahentów wykonujących zlecenia rządowe, lecz także wobec żołnierzy i pracowników US Army. NBIB posiadało również specyficzną strukturę organizacyjną, ponieważ piony merytoryczne zajmujące się bezpieczeństwem w ponad 100 agencjach zostały po 2016 r. funkcjonalnie jej podporządkowane[43]. Jako wyspecjalizowany organ NBIB prowadziło wszystkie czynności w ramach dochodzenia bezpieczeństwa i gromadziło materiały (sprawdzenia osoby w bazach danych innych podmiotów, wywiady w miejscach zamieszkania i pracy itp.).

[42] Zob. szerzej: https://www.dcsa.mil/mc/pv/mbi/gicp/ [dostęp: 4 VI 2021].

[43] Zob. szerzej: https://obamawhitehouse.archives.gov/blog/2016/01/22/modernizing-strengthening-security-effectiveness-federal-background-investigations [dostęp: 4 VI 2021].

Po zakończeniu dochodzenia bezpieczeństwa przez DCSA akta są przesyłane do agencji, w której jest zatrudniona osoba sprawdzana. Tam szef danej agencji podejmuje decyzję dotyczącą możliwości udostępnienia tej osobie informacji niejawnych i określa poziom dostępu (najwyższą klauzulę tajemnic, do jakich ma mieć dostęp sprawdzony pracownik). Sprawdzeniu podlega przeszłość danej osoby, tzn. 10 ostatnich lat, jeżeli ubiega się ona o dostęp do informacji ściśle tajnych, albo 5 lat – jeśli do informacji tajnych. Z uwagi na to, że DCSA ma komórki współdziałające w agencjach, od których przyjmuje wnioski o przeprowadzenie postępowania oraz w strukturach podległych Departamentowi Obrony USA, może uzyskać łatwy dostęp do aktualnych i poprzednich miejsc pracy, edukacji i zamieszkania sprawdzanych osób, a także do innych – nawet zagranicznych – źródeł informacji oraz wszelkich krajowych baz danych. Dodatkowo agencja udostępniająca informacje niejawne może wystąpić do DCSA o objęcie danego pracownika programem ciągłego nadzoru (*Rap Back*). W ramach tego programu pracownik jest rejestrowany w bazach danych FBI i jeżeli złamie prawo albo zainteresuje się nim FBI, to dyrektor agencji zostaje poinformowany o potencjalnym zagrożeniu bezpieczeństwa informacji niejawnych przekazywanych temu pracownikowi.

Osoba sprawdzana, podobnie jak w Polsce, jest zobowiązana do wypełnienia kwestionariusza bezpieczeństwa[44]. Podanie w nim nieprawdziwych informacji może skutkować negatywnym rozstrzygnięciem postępowania. Dodatkowo osoba sprawdzana jest zobligowana do umożliwienia pobrania wzorów linii papilarnych. Karta daktyloskopijna lub odwzorowanie elektroniczne są przechowywane w bazach danych FBI oraz w bazach DCSA.

Zgodnie z zarządzeniem 12968 osoby mające dostęp do informacji niejawnych są zobowiązane do:

1) ochrony informacji niejawnych pozostających w ich dyspozycji przed nieuprawnionym ujawnieniem,
2) zgłaszania wszystkich kontaktów z osobami, włącznie z obcokrajowcami, które dążyły w jakikolwiek sposób do nieuprawnionego uzyskania dostępu do informacji niejawnych,
3) informowania urzędników odpowiedzialnych za bezpieczeństwo tajemnic o wszelkich naruszeniach przepisów bezpieczeństwa,
4) przestrzegania wszelkich innych wymogów bezpieczeństwa określonych w zarządzeniu i dyrektywach wykonawczych,
5) zgłaszania wątpliwości co do potrzeby dalszego dostępu do tajemnic przez innych pracowników z uwagi na zachowanie interesu bezpieczeństwa narodowego.

[44] *Questionnaire for National Security Positions*. Formularz nr 86 zatwierdzony przez United States Office of Management and Budget, OMB (nr autoryzacji: 3206 0005), https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf [dostęp: 4 VI 2021]. Dokument zawiera między innymi pouczenie o odpowiedzialności karnej z § 1001 za podanie fałszywych danych, tj. o czyn zagrożony karą pozbawienia wolności do lat 5 (USC, Title 18, Part I, Chapter 47 – *Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 47).

Przedmiotowe dyspozycje prawodawca zabezpieczył sankcjami, które mogą zostać zastosowane, w przypadku gdy pracownik agencji umyślnie przyznaje uprawnienia lub udostępnia informacje niejawne innej osobie, z naruszeniem zarządzenia albo aktów wykonawczych. Konsekwencjami powyższych naruszeń są: upomnienie, zawieszenie w obowiązkach bez wynagrodzenia, odwołanie ze stanowiska, a także inne środki przewidziane w prawie powszechnym i aktach normatywnych danej agencji.

Na podstawie *Kodeksu Stanów Zjednoczonych* organem powołanym do dokonywania interpretacji przepisów omawianego zarządzenia jest Asystent Prokuratora Generalnego USA ds. Bezpieczeństwa Narodowego[45].

W polskim porządku prawnym postępowanie służące weryfikacji osób, którym mają być udostępnione informacje niejawne, ustanowiono w rozdziale 5 ustawy o.i.n. zatytułowanym *Bezpieczeństwo osobowe*.

W okresie międzywojennym oraz w socjalistycznej Polsce organami upoważnionymi do udzielania dostępu do informacji stanowiących tajemnicę państwową byli kierownicy jednostek organizacyjnych w odniesieniu do podległych pracowników. Służby specjalne wyłącznie opiniowały daną osobę na wniosek kierowników jednostek, z tym zastrzeżeniem, że negatywna opinia zobowiązywała wnioskodawcę do odmowy nadania uprawnień. Warto dodać, że upoważnienia wydawane przez kierowników jednostek nie były decyzjami administracyjnymi i w związku z tym nie były wiążące dla innych podmiotów, a ponadto nie podlegały kontroli instancyjnej lub sądowej. Zmiana miejsca zatrudnienia powodowała konieczność powtórnego sprawdzenia danej osoby i wydania nowego upoważnienia albo odmowy, w zależności od opinii służb bezpieczeństwa państwa. Wprowadzenie ustawą o ochronie informacji niejawnych demokratycznych i określonych jawnymi przepisami procedur spowodowało przyznanie uprawnionym służbom i pełnomocnikom do spraw ochrony informacji niejawnych prawa do wydawania poświadczeń bezpieczeństwa, których termin ważności jest uzależniony od poziomu klauzuli informacji dostępnych na ich podstawie[46]. Negatywne rozstrzygnięcia są podejmowane w postaci decyzji administracyjnych z zachowaniem wszelkich konsekwencji prawnych, tj. możliwości wniesienia odwołania do organu II stopnia i ewentualnie skargi do sądów administracyjnych.

---

[45] Zob. szerzej: *Code of Federal Regulations*, Title 18, Chapter I, Part 17, Subpart A, Section 17.13 (*Kodeks przepisów federalnych*, tytuł 18, rozdział I, część 17, podczęść A, sekcja 17.13). Przepisy wydawane przez administrację federalną, tzn. rządową (*Federal Regulations issued by federal administrative agencies*), są skodyfikowane w akcie o nazwie *Code of Federal Regulations* (CFR). Kodeks składa się zazwyczaj z 50 tytułów (zależnie od roku wydania) w znacznej części pokrywających się z zakresem regulowanym przez ustawy federalne skodyfikowane w USC. Jedyną różnicą jest to, że CFR obejmuje wyłącznie przepisy wydawane przez władzę wykonawczą i jest publikowany w edycji rocznej. Zob. https://www.govinfo.gov/app/collection/cfr [dostęp: 4 VI 2021].

[46] Termin ważności poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji ściśle tajnych wynosi 5 lat, tajnych 7 lat i poufnych 10 lat.

Dostęp do informacji poufnych następuje po pozytywnie zakończonym zwykłym postępowaniu sprawdzającym. Do prowadzenia tego rodzaju postępowań ustawodawca upoważnił pełnomocników jednostek organizacyjnych ds. ochrony informacji niejawnych. Z kolei poszerzone postępowania sprawdzające stanowią podstawę do rozstrzygania o dostępie do informacji tajnych i ściśle tajnych. Podmiotami uprawnionymi do ich realizacji są służby państwowe, przede wszystkim ABW i SKW, a dodatkowo podmioty wyszczególnione enumeratywnie w ustawie[47].

Kontrolne postępowania sprawdzające w odniesieniu do prawomocnie zakończonych zwykłych postępowań sprawdzających są prowadzone przez pełnomocników ochrony właściwych ze względu na miejsce zatrudnienia osoby sprawdzanej. W przypadkach uzasadnionych względami bezpieczeństwa państwa mogą być również prowadzone przez ABW albo SKW (art. 33 ust. 3 ustawy o.i.n.). Kontrolne postępowania w odniesieniu do poszerzonych postępowań sprawdzających są realizowane wyłącznie przez ABW albo SKW (wg właściwości rzeczowej), a także przez służby wymienione w art. 23 ust. 5 w stosunku do postępowań przeprowadzonych przez te służby. Postępowania sprawdzające, na podstawie których strona uzyskuje dostęp do informacji niejawnych organizacji międzynarodowych, mogą prowadzić tylko ABW lub SKW w trybie poszerzonego lub tzw. skróconego postępowania sprawdzającego[48]. Mianem „kolejne postępowanie sprawdzające" ustawodawca określa postępowanie prowadzone wobec osoby już posiadającej poświadczenie, którego termin ważności dobiega końca. W celu zapewnienia ciągłości uprawnień prawodawca wydłużył okres jego prowadzenia z trzech do sześciu miesięcy i nakazał złożyć do właściwego organu ankietę i wniosek z wyprzedzeniem sześciu miesięcy. Kolejne postępowanie jest prowadzone w trybie zwykłego lub poszerzonego postępowania sprawdzającego w zależności od stanowiska, jakie zajmuje dana osoba w dniu złożenia wniosku.

Zgodnie z art. 21 ustawy o.i.n. dostęp do informacji niejawnych o klauzuli „poufne", „tajne" albo „ściśle tajne" może nastąpić po uzyskaniu przez określoną osobę odpowiedniego poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony

[47] W art. 23 ust 5 ustawy o.i.n prawodawca uprawnia: Agencję Wywiadu, Centralne Biuro Antykorupcyjne, Służbę Ochrony Państwa, Policję, Służbę Więzienną, Służbę Wywiadu Wojskowego, Straż Graniczną i Żandarmerię Wojskową do prowadzenia poszerzonych postępowań sprawdzających wobec osób zatrudnionych w tych organach i ubiegających się o zatrudnienie, a także wobec osób realizujących zlecenia na ich rzecz.

[48] Podstawą prawną do przeprowadzenia skróconego postępowania sprawdzającego jest art. 32 ust. 4 ustawy o.i.n. Określenie „skrócone postępowanie sprawdzające" pochodzi z terminologii resortowej, ponieważ w tym trybie nie dokonuje się weryfikacji danych zawartych w ankiecie bezpieczeństwa osobowego z tego powodu, że osoba sprawdzana nie ma obowiązku jej składania. Organem prowadzącym postępowanie jest wyłącznie ABW albo SKW, ponieważ tylko te organy są uprawnione do wydawania poświadczeń bezpieczeństwa organizacji międzynarodowych. Aby skorzystać z tego trybu, osoba sprawdzana musi mieć ważne poświadczenie bezpieczeństwa do tajemnic RP, które było wydane przez ABW, SKW, Agencję Wywiadu lub Służbę Wywiadu Wojskowego, na których podstawie jest dopuszczalne ograniczenie czynności sprawdzających i wydanie poświadczenia organizacji międzynarodowej z terminem ważności takim samym, jaki określono w poświadczeniu krajowym.

informacji niejawnych[49]. Wydanie poświadczenia jest możliwe wyłącznie po przeprowadzeniu wobec określonej osoby postępowania sprawdzającego zakończonego pozytywnym wynikiem. Od tej generalnej zasady istnieją odstępstwa. Ustawa w art. 34 ust. 5, 6 oraz 9 upoważnia osoby piastujące określone stanowiska państwowe do wyrażania zgody na jednokrotny lub tymczasowy dostęp do tajemnicy osobom, które nie mają poświadczenia bezpieczeństwa. Ponadto prawodawca w art. 34 ust. 10–13 wymienił podmioty, które są zwolnione od obowiązku posiadania poświadczenia lub ten obowiązek jest ograniczony do określonych typów poświadczeń.

W kontekście bezpieczeństwa państwa oraz konstytucyjnych praw obywatelskich warto odpowiedzieć na pytanie, czym jest postępowanie sprawdzające i według jakiej procedury jest ono prowadzone w demokratycznym państwie. Na podstawie kompetencji organów prowadzących, a także praw i obowiązków osoby sprawdzanej, można stwierdzić, że wspomniane postępowanie jest ciągiem czynności urzędowych podejmowanych przez uprawniony podmiot w celu ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy[50]. Podejmowane czynności są uregulowane w ustawie, a także – w określonej części – są administracyjnym prawem procesowym[51]. Ustawodawca w art. 24 ust. 6 ustawy o.i.n. określa, że postępowanie sprawdzające powinno być zakończone przed upływem trzech miesięcy od otrzymania przez organ dokumentów nakazanych ustawą, tj. wniosku wraz z ankietą bezpieczeństwa osobowego (ABO) lub tylko ankiety w przypadku postępowań zwykłych. Z uwagi na celowy charakter postępowania oraz instrukcyjny termin prowadzenia jego tok winien mieć charakter ciągły, tzn. postępowanie powinno być prowadzone bez przerwy – od wszczęcia do rozstrzygnięcia decyzją administracyjną. Ze względu na precyzyjne określenie przebiegu postępowania w ustawie szczególnej jest ono postępowaniem autonomicznym, z pewnym zakresem stosowania elementów postępowania jurysdykcyjnego określonego Kodeksem

[49] Kierując się wyłącznie treścią art. 21, można błędnie sądzić, że osoba, która spełniła ustanowione w nim warunki, ma dostęp do każdej tajemnicy o określonej klauzuli, a także że jest to uprawnienie obejmujące wszystkie informacje chronione daną klauzulą. Należy jednak wskazać, że ustawodawca w art. 4 ustawy o.i.n. ustanowił normę generalną w zakresie dostępu osób do informacji niejawnych ograniczającą pozornie uniwersalny charakter tego uprawnienia. Wprowadził zasadę wiedzy niezbędnej, która polega na udostępnianiu osobie uprawnionej tylko takich informacji, które są jej niezbędne do wykonywania pracy (służby) na zajmowanym stanowisku albo realizacji czynności zleconych (zasada była już stosowana w okresie II RP).

[50] W art. 2 pkt 2 ustawy o.i.n. zawarto definicję legalną: „(…) rękojmią zachowania tajemnicy jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego".

[51] Zgodnie z art. 3 ustawy o.i.n.: „Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nieuregulowanym w ustawie, mają zastosowanie przepisy: art. 6–8, art. 12, art. 14–16, art. 24 § 1 pkt 1–6 i § 2–4, art. 26 § 1, art. 28, art. 29, art. 30 § 1–3, art. 35 § 1, art. 39, art. 41–47, art. 50, art. 55, art. 57–60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 65, art. 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 103, art. 104, art. 105 § 2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125 § 1, art. 156–158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego".

postępowania administracyjnego[52] oraz ustawą Prawo o postępowaniu przed sądami administracyjnymi[53] (dalej: ustawa p.p.s.a.) (w części rozpatrywania skarg na negatywne rozstrzygnięcia organów II stopnia). Można zatem stwierdzić, że postępowanie sprawdzające jest postępowaniem szczególnym w odniesieniu do ogólnego postępowania administracyjnego określonego w kpa. Trafną, chociaż lapidarną, definicję postępowania jurysdykcyjnego sformułował Adam Bochentyn, stwierdzając, że jest to postępowanie administracyjne rozumiane jako proces stosowania norm prawnych przez wydawanie decyzji administracyjnych[54].

Należy zaznaczyć, że tylko niektórzy kierownicy jednostek organizacyjnych są uprawnieni do wnioskowania lub zlecania przeprowadzenia postępowania sprawdzającego wobec podległych im pracowników. Ustawodawca w art. 1 ust. 2 wymienił podmioty władzy publicznej zobowiązane do stosowania jej przepisów oraz przykładowo je wyliczył. Pomimo zastosowania terminu „w szczególności", który wskazuje na otwarty charakter danego wykazu, w rzeczywistości przyjęty sposób określenia podmiotów związanych przepisami ustawy czyni ten katalog „zewnętrznie" zamkniętym. Decydują o tym przyjęte kryteria selekcji podmiotów, ustawę bowiem mogą stosować wyłącznie organy władzy publicznej oraz podmioty wskazane *expressis verbis* w jej treści. Postępowanie sprawdzające mogą również przeprowadzać jednostki niepubliczne spełniające szczególny warunek, zawarty w art. 1 ust. 2 pkt 6 ustawy o.i.n., lub takie instytucje, którym ustawodawca narzucił obowiązek stosowania tej ustawy, odsyłając do niej w innych aktach normatywnych[55]. Kierownicy jednostek, które nie kwalifikują się do wyżej wymienionych zbiorów, nie mają ani obowiązku, ani legitymacji do występowania o przeprowadzenie wobec pracowników postępowań sprawdzających (np. przedsiębiorcy niespełniający przesłanek określonych w art. 1 ust. 2 pkt 6 ustawy o.i.n.)[56].

Głównymi organami prowadzącymi poszerzone postępowania sprawdzające przed wydaniem poświadczenia bezpieczeństwa upoważniającego do dostępu do

---

[52] *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (t.j.: DzU z 2021 r. poz. 735).

[53] *Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi* (t.j.: DzU z 2019 r. poz. 2325, ze zm.).

[54] A. Bochentyn, *Dopuszczalność dowodu z opinii biegłego na okoliczność treści prawa krajowego i europejskiego w jurysdykcyjnym postępowaniu administracyjnym*, w: *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, t. 2, J. Sługocki (red.), Wrocław 2014, s. 359.

[55] Stosowanie odesłań do ustawy o.i.n. wynika z zakazu powtarzania tych samych regulacji w różnych aktach prawnych. Zob. § 4 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (DzU z 2016 r. poz. 283). Bezpośrednie odesłanie zastosowano w 22 innych ustawach i 12 rozporządzeniach, a pośrednie w blisko 100 ustawach i kilkudziesięciu rozporządzeniach. Zob. szerzej: D. Chromicka, *Struktura regulacji ochrony informacji niejawnych*, w: *Jawność i jej ograniczenia*, t. 4: *Struktura tajemnic*, A. Gruszczyńska (red.), Warszawa 2016, s. 237 i nast.

[56] Por. J. Borowicz, *Przetwarzanie informacji niejawnych w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne" 2011, nr 7, s. 24.

informacji o klauzuli „tajne" i „ściśle tajne" są ABW i SKW. Ustawodawca kontynuuje przyjęty w poprzednich ustawach (z 1982 r. i 1999 r. dotyczących ochrony informacji) podział kompetencji rzeczowej między podmioty cywilne i wojskowe. W art. 10 ustawy o.i.n. uszczegóławia się, że SKW realizuje zadania w odniesieniu do jednostek organizacyjnych Ministerstwa Obrony Narodowej i instytucji podległych, a także żołnierzy służby czynnej wyznaczonych na stanowiska poza wyżej wymienionymi strukturami. Wobec pozostałych osób i jednostek, do których ustawa ma zastosowanie, właściwym organem jest ABW. Zgodnie z art. 23 ust. 5 wymienieni w tym przepisie pełnomocnicy szefów służb ds. ochrony informacji niejawnych są uprawnieni do prowadzenia poszerzonych postępowań sprawdzających, według trybu określonego dla ABW i SKW. Pełnomocnicy wszczynają dane postępowanie na polecenie ich bezpośrednich przełożonych, tj. szefów wskazanych służb lub kierowników strukturalnych jednostek organizacyjnych tych podmiotów. Warto zauważyć, że w związku z konstrukcją art. 5 § 2 pkt 3 i art. 1 pkt 2 kpa pełnomocników ochrony należy zaliczyć do organów administracji publicznej, ponieważ są uprawnieni do załatwiania spraw indywidualnych w drodze decyzji administracyjnej. W literaturze przedmiotu tego rodzaju podmioty są także określane jako „funkcjonalne organy administracji publicznej"[57].

Podmiot, który zakończył postępowanie sprawdzające z wynikiem pozytywnym, na podstawie art. 29 ustawy o.i.n. jest zobowiązany przekazać osobie sprawdzonej poświadczenie bezpieczeństwa. Doręczenie stronie decyzji o odmowie wydania poświadczenia bezpieczeństwa nakazuje się w art. 30 ust. 5. Natomiast w przypadku przeprowadzenia kontrolnego postępowania sprawdzającego, ze względu na ujawnienie nowych informacji, że osoba mająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy, art. 33 ust. 8 ustawy o.i.n. stanowi podstawę doręczenia decyzji o cofnięciu poświadczenia bezpieczeństwa, która kończy to postępowanie.

Odwołanie do organu II stopnia może wnieść wyłącznie osoba, wobec której organ I stopnia zakończył postępowanie sprawdzające decyzją o cofnięciu poświadczenia bezpieczeństwa albo odmową jego wydania lub decyzją o umorzeniu postępowania sprawdzającego, a także decyzją o umorzeniu kontrolnego postępowania sprawdzającego. Jeżeli strona wnosi odwołanie na decyzję wydaną w I instancji przez ABW lub SKW, a także przez podmioty wymienione w art. 23 ust 5, kieruje je do Prezesa Rady Ministrów RP w terminie 14 dni od dnia jej otrzymania za pośrednictwem organu, który wydał zaskarżaną decyzję. Odwołanie nie wymaga uzasadnienia. Organ I stopnia jest zobowiązany przesłać odwołanie wraz z aktami postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym je otrzymał. Organ II stopnia powinien rozpatrzyć odwołanie nie później niż w ciągu trzech miesięcy. Wniesienie odwołania nie wstrzymuje wykonania decyzji.

[57] Zob. szerzej: W. Chróścielewski, J. Tarno, *Postępowanie administracyjne i postępowanie przed sądami administracyjnymi*, Warszawa 2018, s. 85 i nast.

Wnoszący odwołanie jest uprawniony, na podstawie art. 36 ust. 3 ustawy, do żądania zlecenia przez Prezesa Rady Ministrów przeprowadzenia dodatkowych czynności przez organ I stopnia w celu uzupełnienia dowodów i materiałów w poszerzonym postępowaniu sprawdzającym lub kontrolnym postępowaniu sprawdzającym. Przedmiotem wystąpienia mogą być specjalistyczne badania, o których mowa w art. 26 ust. 6 ustawy o.i.n. Przyznanie stronie inicjatywy dowodowej w postaci prawa do żądania zlecenia przez organ II stopnia przeprowadzenia dowodu jest odstępstwem od ogólnych zasad postępowania administracyjnego. Postępowanie dowodowe powinno bowiem nastąpić przed podjęciem ostatecznego rozstrzygnięcia o istocie sprawy, a więc w ramach postępowania prowadzonego przez organ I stopnia. Pozbawienie strony inicjatywy dowodowej w postępowaniu pierwszoinstancyjnym i przyznanie jej na etapie rozpatrzenia odwołania przez Prezesa RM jest rozwiązaniem, które trudno racjonalnie uzasadnić. Postulowana zmiana przepisów to odpowiednia recepcja tej regulacji do art. 26 ustawy o.i.n., który uszczegóławia zakres poszerzonego postępowania sprawdzającego. Uprawnienie strony do żądania przeprowadzenia określonych czynności w toku postępowania sprawdzającego przed jego rozstrzygnięciem upodmiotowiłoby osobę sprawdzaną, która na tym etapie jest raczej „biernym przedmiotem" rozpoznania przez organ.

Na decyzję organu II stopnia, jeżeli nie rozstrzyga on odwołania według żądania strony, osobie sprawdzanej przysługuje skarga do właściwego miejscowo wojewódzkiego sądu administracyjnego. Do postępowania przed sądem administracyjnym stosuje się odpowiednio przepisy ustawy p.p.s.a. z pewnymi ograniczeniami wynikającymi z art. 38 ustawy o.i.n. Ustawodawca w przywołanym przepisie ustala przebieg procesu w szczególnym trybie, ze względu na to, że skarga rozpoznawana jest przez sąd na posiedzeniu niejawnym, a więc istotnie ogranicza jawność procesu. Brak udziału publiczności, w tym prasy (opinii publicznej), w procesie skutkuje wyłączeniem społecznej kontroli sposobu rozpatrywania sprawy przez sąd. Przywołany przepis poważnie utrudnia stronie skorzystanie z prawa do obrony swojego interesu prawnego przez wniesienie skargi, ponieważ stanowi, że odpis sentencji wyroku wraz z uzasadnieniem zostają doręczone przez sąd tylko właściwemu organowi odwoławczemu. Skarżącemu oraz osobie uprawnionej do obsady stanowiska jest doręczany jedynie odpis wyroku. A zatem strona nie otrzymuje uzasadnienia wyroku. Na jakiej więc podstawie osoba sprawdzana (profesjonalny pełnomocnik) może skonstruować zarzuty uzasadniające skargę kasacyjną, jeżeli wyrok jest dla niej niekorzystny?

Niniejsze zagadnienie było przedmiotem skargi do Trybunału Konstytucyjnego, który w wyroku z 23 maja 2018 r. orzekł, że: *Art. 38 ust. 3 ustawy w zakresie, w jakim przewiduje doręczenie skarżącemu odpisu wyroku sądu administracyjnego bez tej części uzasadnienia, której utajnienie nie jest konieczne dla ochrony informacji niejawnych, jest niezgodny z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 78 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej*[58]. A zatem uzasadnienie wyroku, które nie zawiera informacji niejawnych, powinno być doręczone

[58] Wyrok Trybunału Konstytucyjnego z 23 maja 2018 r., sygn. SK 8/14, OTK ZU 34/A/2018.

stronie w całości. Jeżeli natomiast uzasadnienie zawiera informacje niejawne, wówczas sąd powinien wyłączyć treści stanowiące tajemnice i po modyfikacji przekazać uzasadnienie stronie.

Jeżeli wojewódzki sąd administracyjny orzekł na niekorzyść osoby sprawdzanej, gdy istnieją uzasadnione przesłanki wskazujące na obrazę prawa materialnego w wyniku jego błędnego zastosowania lub wykładni albo na naruszenie przepisów postępowania w stopniu mającym wpływ na wynik sprawy (art. 174 ustawy p.p.s.a.), przysługuje jej skarga kasacyjna albo zażalenie do Naczelnego Sądu Administracyjnego. Należy nadmienić, że zgodnie z art. 175 i art. 194 § 4 ustawy p.p.s.a. skarga kasacyjna na wyrok oraz zażalenie na postanowienie o odrzuceniu skargi kasacyjnej co do zasady powinny być sporządzone i podpisane przez adwokata lub radcę prawnego. Postępowanie przed Naczelnym Sądem Administracyjnym, podobnie jak przed wojewódzkimi sądami administracyjnymi, toczy się według procedury określonej przepisami ustawy p.p.s.a. z ograniczeniami wprowadzonymi w art. 38 ustawy o.i.n.

Wracając do rozważań związanych ze Stanami Zjednoczonymi, należy wskazać, że system bezpieczeństwa informacji niejawnych USA jest bardzo rozbudowany pod względem regulacji normatywnych. Tworzą go ustawy o resortowym charakterze. Za najważniejsze należy uznać następujące akty prawne: *Ustawę o szpiegostwie* z 1917 r.[59], *Ustawę o energetyce atomowej* z 1954 r.[60], *Ustawę o ochronie tożsamości wywiadowczych* z 1982 r.[61] oraz *Ustawę o informacjach infrastruktury krytycznej z 2002 r.*[62], ponieważ w USA nie ma jednej spójnej ustawy regulującej ochronę informacji niejawnych. Drugą grupą normodawczą są zarządzenia wykonawcze prezydenta USA, z których dwa zostały już omówione, jednak nie są to jedyne zarządzenia o szerokim zakresie regulacji. Tak samo istotne jest zarządzenie 13587 dotyczące zwiększenia bezpieczeństwa informacji niejawnych w sieciach informatycznych i ich redystrybucji[63]. W USA obowiązują

[59] *Espionage Act* of 1917, USC, Title 18, § 792 and next (*Ustawa o szpiegostwie* z 1917 r., *Kodeks Stanów Zjednoczonych*, tytuł 18, § 792 i nast.).

[60] *Atomic Energy Act* of 1954, USC, Title 42, § 1801 and next, Public Law 703 (*Ustawa o energetyce atomowej* z 1954 r., *Kodeks Stanów Zjednoczonych*, tytuł 42, § 1801 i nast.).

[61] *Intelligence Identities Protection Act* of 1982, USC, Title 50, § 401, Public Law 97 – 200 (*Ustawa o ochronie tożsamości wywiadowczych* z 1982 r., *Kodeks Stanów Zjednoczonych*, tytuł 50, § 401.) Ustawa dotyczy ochrony danych personalnych agentów lub niejawnych współpracowników Wspólnoty Wywiadów.

[62] *Critical Infrastructure Information Act* of 2002, USC, title 6, § 2135 (*Ustawa o informacjach infrastruktury krytycznej* z 2002 r., *Kodeks Stanów Zjednoczonych*, tytuł 6, § 2135). Ustawa kształtuje krajową politykę departamentów i agencji federalnych USA w celu identyfikacji infrastruktury krytycznej i najważniejszych zasobów w Stanach Zjednoczonych oraz ochrony ich przed atakami terrorystycznymi, a także zasady analizy i ochrony informacji dotyczących tej infrastruktury.

[63] *The President Executive Order 13587* of 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing nad Safeguarding of Classified Information* (*Zarządzenie Wykonawcze Prezydenta 13587* z 2011 r., *Reformy strukturalne w celu poprawy bezpieczeństwa niejawnych sieci internetowych oraz odpowiedzialnego udostępniania i zabezpieczenia informacji niejawnych*).

ponadto regulacje określające postępowanie z tajemnicami o branżowym charakterze. Przykładem mogą być niektóre przepisy *Kodeksu przepisów federalnych* USA dotyczące funkcjonowania banków[64].

Na podstawie umowy zawartej pomiędzy rządem RP a rządem USA dotyczącej środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej[65] strony zobowiązały się do wzajemnej ochrony informacji niejawnych wymienianych w ramach wojskowej współpracy między Ministerstwem Obrony Narodowej RP a Departamentem Obrony USA. Państwa określiły wzajemne przyporządkowanie stosowanych klauzul w celu zapewnienia adekwatnej ochrony wymienianym informacjom. W poniższym zestawieniu zaprezentowano klauzule stosowane przez oba państwa.

Klauzula stosowana w RP	**Klauzula stosowana w USA**
Ściśle tajne	Top secret
Tajne	Secret
Poufne	Confidential
Zastrzeżone	brak amerykańskiego odpowiednika, traktowane jak Confidential

Ważnym postanowieniem zarządzenia 13526 jest upoważnienie podmiotów, które nie mają uprawnień do zaliczania posiadanych informacji do tajemnic i nadawania im klauzul, do występowania w tej sprawie do właściwych merytorycznie (ze względu na charakter informacji) agencji państwowych. Taka regulacja nie ma odpowiednika w polskich przepisach prawnych.

Oprócz podmiotów rządowych również inne podmioty, które nie są uprawnione do stosowania przepisów właściwych w sprawie klasyfikowania i klauzulowania informacji, mogą wytworzyć informacje, które powinny podlegać ochronie ze względu np. na bezpieczeństwo państwa, a zatem powinny być utajnione. Dlatego zarządzenie 13526 zobowiązuje podmioty rządowe do podjęcia decyzji o klasyfikowaniu przekazanych im

[64] Zob. szerzej: *Code of Federal Regulations*, Title 12, Chapter X, Part 1070, Subpart B. Wymieniony akt w ust. 19 reguluje, jakie podmioty są właściwe w sprawach udzielania odpowiedzi na wnioski dotyczące przekazania informacji niejawnych. Z przywołanego paragrafu wynika, że podmiotem uprawnionym do dysponowania informacją jest wyłącznie ten organ, który nadał jej klauzulę, czyli tylko wytwórca jest właściwy do deklasyfikacji dokumentu. W przywołanym akcie uregulowano również inne aspekty związane z zabezpieczeniem tajemnic w administracji rządowej, między innymi fizyczne zabezpieczenie informacji niejawnych i ich przechowywanie, kontrolowanie przesyłanie do innych podmiotów i warunki, w jakich tego dokonywano.

[65] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej podpisana w Warszawie dnia 8 marca 2007 r.* (DzU z 2007 r. nr 224 poz. 1658). W odniesieniu do sfery cywilnej strony nie zawarły tego rodzaju umowy, dokumenty pochodzące ze wzajemnej wymiany są chronione w wyniku nadania im polskich klauzul na podstawie art. 5 ust. 5 oraz art. 7 ust. 1 pkt 3 ustawy o.i.n.

informacji w terminie 30 dni[66]. Jest to szczególnie ważne w przypadku zamkniętego katalogu podmiotów uprawnionych do klauzulowania informacji na podstawie przepisów prawa, co występuje również w Polsce. Dlatego należy postulować wprowadzenie podobnej instytucji do systemu prawnego RP.

Przepisy federalne kształtujące odpowiedzialność karną za przestępstwa przeciwko tajemnicom USA

Federalne przepisy prawa karnego materialnego USA zostały skodyfikowane w przywołanym wcześniej *Kodeksie Stanów Zjednoczonych*, tytuł 18 – *Crimes nad criminal procedure*, część I – *Crimes*. Ze względu na poruszaną tematykę istotną jednostką redakcyjną rozdziału 37 pt. *Szpiegostwo i cenzura* (*Espionage and censorship*) jest § 798[67]. W tym przepisie amerykański prawodawca penalizuje czyn ujawnienia informacji niejawnych (*disclosure of classified information*). Przed przystąpieniem do omówienia przepisów karnych warto zaznaczyć, że ustalenie zaistnienia przestępstwa w amerykańskim prawie karnym polega na potwierdzeniu wystąpienia jego sześciu

[66] *The President Executive Order 13526*…, Part I, article 1 section 3 letter e (*Zarządzenie Wykonawcze Prezydenta 13526*…, część 1, art.1 ust. 3 lit. e).

[67] USC, Title 18, Part I, Chapter 37, § 798: „(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information – (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes- Shall be fined under this title or imprisoned not more than ten years, or both" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(a) Kto świadomie i celowo komunikuje, dostarcza, przekazuje lub w inny sposób udostępnia osobie nieupoważnionej, lub publikuje, lub wykorzystuje w jakikolwiek sposób z naruszeniem bezpieczeństwa lub interesu Stanów Zjednoczonych, lub na rzecz jakiegokolwiek rządu obcego państwa ze szkodą dla Stanów Zjednoczonych jakiekolwiek informacje niejawne: (1) dotyczące charakteru, przygotowania lub stosowania jakiegokolwiek kodu, szyfru lub systemu kryptograficznego Stanów Zjednoczonych lub jakiegokolwiek rządu obcego państwa; lub (2) dotyczące projektu, konstrukcji, użytkowania, konserwacji lub naprawy jakichkolwiek urządzeń, przyrządów lub sprzętów, stosowanych lub przygotowanych lub planowanych do zastosowania przez Stany Zjednoczone lub jakikolwiek rząd obcego państwa do celów kryptograficznych lub rozpoznania komunikacyjnego; lub (3) dotyczące działalności Stanów Zjednoczonych lub jakiegokolwiek rządu obcego państwa z zakresu rozpoznania komunikacyjnego; lub (4) uzyskane przez procesy rozpoznania komunikacyjnego na podstawie wiadomości przekazywanych przez jakikolwiek rząd obcego państwa, wiedząc, że zostały one uzyskane w wyniku takich procesów; podlega karze grzywny zgodnie z niniejszym tytułem lub pozbawienia wolności na okres do dziesięciu lat, lub obu tym karom jednocześnie").

znamion. Podstawowym determinantem odpowiedzialności jest istnienie generalnej normy zakazu karnego, czyli prawa, którego złamanie w wyniku działania lub zaniechania jest zagrożone reakcją państwa w formie kary. W USA prawo nie zawsze jest prawem stanowionym w formie ustaw, ponieważ pod uwagę mogą być brane precedensy orzecznictwa sądowego. Kolejną przesłanką jest wina powiązana z umyślnością albo nieumyślnością oraz z zabronionym zachowaniem, co najkrócej można ująć zasadą koincydencji lub jej braku (podobnie jak w polskim kodeksie karnym – art. 1 § 3). Jak trafnie zauważa Roman Tokarczyk, rezultatem bezprawnego działania lub zaniechania musi być „zło samo w sobie" (łac. *malum in se*) w sensie krzywdy albo innej szkody wynikającej z naruszenia wartości chronionych przez prawo. Ostatnim znamieniem jest związek przyczynowo-skutkowy (*casual link*) nie tylko między winą a skutkiem, lecz także między zabronionym zachowaniem a złem[68].

Konstrukcja przywołanego § 798 USC pod względem redakcyjnym odbiega nieco od modelu przyjętego w technice legislacyjnej RP. W ustępie (a) amerykański ustawodawca ustanowił normę sankcjonowaną i sankcjonującą, natomiast w kolejnym – (b)[69] – zdefiniował siedem nieostrych pojęć użytych do zbudowania normy

[68] Zob. szerzej: R. Tokarczyk, *Prawo amerykańskie*, Warszawa 2011, s. 230 i nast.

[69] USC, Title 18, Part I, Chapter 37, § 798: „(b) As used in subsection (a) of this section – The term 'classified information' means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution; The terms 'code', 'cipher', and 'cryptographic system' include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications; The term 'foreign government' includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States; The term 'communication intelligence' means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients; The term 'unauthorized person' means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(b) Zgodnie z użyciem w ust. a) niniejszego paragrafu – termin »informacje niejawne« oznacza informacje, które w momencie naruszenia niniejszego paragrafu są ze względu na bezpieczeństwo narodowe konkretnie oznaczone przez dowolną agencję rządową Stanów Zjednoczonych do ograniczonego lub zastrzeżonego rozpowszechniania lub rozprowadzania; terminy »kod«, »szyfr« i »system kryptograficzny« obejmują swoim znaczeniem, oprócz swoich zwyczajowych znaczeń, wszelkie metody tajnego zapisu oraz wszelkie mechaniczne lub elektryczne urządzenia lub metody stosowane w celu maskowania lub ukrywania treści, doniosłości lub znaczenia wiadomości; termin »rząd obcego państwa« obejmuje swoim znaczeniem każdą osobę lub osoby działającą(-e) lub twierdzącą(-e), że działa(-ją) na rzecz lub w imieniu jakiegokolwiek odłamu, partii, departamentu, agencji, biura lub sił wojskowych obcego państwa lub na terytorium takiego państwa, lub na rzecz lub w imieniu jakiegokolwiek rządu lub jakiejkolwiek osoby lub osób, która/które twierdzi(-ą), że działa(-ją)

sankcjonowanej, co ułatwia jej interpretację oraz znacznie ogranicza blankietowość. Mimo zdefiniowania określonych pojęć, w ocenie autora niniejszego artykułu ich zrozumienie jest możliwe na podstawie szerszej wiedzy z danej problematyki. Ustęp (c)[70] omawianego paragrafu zawiera kontratyp, który polega na uwolnieniu od odpowiedzialności karnej osoby wyjawiającej legalnie posiadane informacje niejawne komisjom powołanym w Kongresie USA (Senat i Izba Reprezentantów). Przywołany przepis koresponduje z innymi ustawami i aktami prawnymi wydanymi przez prezydenta USA, np. *Ustawą o ochronie sygnalistów z 1989 r.*[71] Prawodawca ustanowił także podstawy bezpośredniego informowania Kongresu USA o przestępczym działaniu administracji rządowej, nawet jeśli przekazywane przez urzędników informacje są objęte tajemnicą. Wspomniane akty zapewniają ochronę „sygnalistów" przed negatywnymi konsekwencjami wynikającymi ze złożonego zawiadomienia o nieprawidłowościach ze strony ich służbowych przełożonych. Końcowa jednostka redakcyjna, tj. ustęp (d), dotyczy możliwości zastosowania środka karnego (w wyroku skazującym) w postaci orzeczenia przepadku mienia należącego do skazanego, z określeniem warunków jego konfiskaty na rzecz państwa[72]. W odniesieniu do wymiaru zagrożenia karą za popełnienie przedmiotowego

jako rząd na terytorium obcego państwa bez względu na to, czy taki rząd jest uznawany przez Stany Zjednoczone; termin »rozpoznanie komunikacyjne« oznacza wszystkie procedury i metody wykorzystywane do przechwytywania wiadomości i uzyskiwania informacji z takich wiadomości przez osoby inne niż zamierzeni odbiorcy; termin »osoba nieupoważniona« oznacza każdą osobę lub agencję, która nie jest upoważniona do otrzymywania kategorii informacji określonych w ust. (a) niniejszego paragrafu przez prezydenta lub przez szefa departamentu lub agencji rządu Stanów Zjednoczonych wyznaczonego przez prezydenta do podejmowania działań z zakresu rozpoznania komunikacyjnego na rzecz Stanów Zjednoczonych").

[70] Tamże, § 798: „(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof" („(c) Żadne z postanowień niniejszego paragrafu nie zabrania dostarczania informacji na zgodne z prawem żądanie jakiejkolwiek prawidłowo utworzonej komisji Senatu lub Izby Reprezentantów Stanów Zjednoczonych Ameryki lub wspólnej komisji obu tych izb").

[71] Zob. szerzej: *Whistleblower Protection Act* of 1989, USC, Title 5, § 1201 (*Ustawa o ochronie sygnalistów* z 1989 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 1201), https://uscode.house.gov/statutes/pl/101/12.pdf [dostęp: 4 VI 2021]; *Whistleblower Protection Enhancement Act* of 2012, USC, Title 5, § 7211 *(Ustawa o wzmocnieniu ochrony sygnalistów* z 2012 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 7211; https://www.govinfo.gov/content/pkg/BILLS-112s743enr/pdf/BILLS-112s743enr.pdf [dostęp: 4 VI 2021]; *Presidential Policy Directive/PPD-19, Protecting Whistleblowers with Access to Classified Information* October 10, 2012 (*Dyrektywa Polityczna Prezydenta/PPD-19*, *Ochrona sygnalistów z dostępem do informacji niejawnych* z 10 października 2012 r.), https://fas.org/irp/offdocs/ppd/ppd-19.pdf [dostęp: 4 VI 2021].

[72] USC, Title 18, Part I, Chapter 37, § 798: „(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law – (A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and (B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(d)(1) Skazany za naruszenie niniejszego paragrafu traci na rzecz Stanów Zjednoczonych, niezależnie od przepisów prawa stanowego – (A) wszelki majątek

przestępstwa amerykański ustawodawca w ust. (a) ustanowił karę grzywny albo karę pozbawienia wolności na okres do 10 lat, z tym że wymienione kary mogą być stosowane łącznie. Analizując zagrożenie karami przewidzianymi w art. 265 polskiej ustawy karnej, można zauważyć, że zaskakująco niskie jest zagrożenie najsurowszą karą, tj. bezwzględnym pozbawienia wolności. Jeżeli bowiem wziąć pod uwagę, że przestępczy czyn jednego człowieka może sprowadzić na państwo np. wyjątkowo poważną szkodę w dziedzinie obronności (może zagrozić niepodległości albo integralności terytorialnej) lub w bezpieczeństwie wewnętrznym, to zastosowanie chociażby górnego wymiaru kary pozbawienia wolności, tj. 5 lat (§ 1) lub 8 lat (§ 2), wydaje się zbyt łagodne.

Nasuwają się wątpliwości co do adekwatność kary do szkody wyrządzonej przestępstwem. Słusznie Ryszard Dębski sygnalizuje, że (…) *należy baczyć, aby pomiędzy zakresem normy sankcjonowanej a sankcją kryminalną, określoną w normie sankcjonującej została zachowana pewna relacja proporcji*[73]. Oznacza to, że wymiar i rodzaj kary powinny być dostosowane do społecznej szkodliwości czynu z uwzględnieniem określających ją kwantyfikatorów, szczególnie rozmiarów wyrządzonej lub grożącej szkody oraz wagi naruszonych obowiązków. Podobny pogląd na temat sprawiedliwościowej funkcji kary prezentuje Wojciech Zalewski: *Za proporcjonalizmem w karaniu przemawia wiele argumentów teoretycznych i praktycznych. Istotą kary była i jest odpłata. Jeśli dalej reakcję na przestępstwo opierać się będzie na karze, musi być to kara sprawiedliwa*[74]. Przedmiotowe rozważania są adekwatne w odniesieniu do dysproporcji zagrożenia karą wynikającą z § 1924 USC, tj. do 5 lat pozbawienia wolności łącznie z karą grzywny lub bez (§ 1924 omówiono poniżej) i zagrożenia karą przewidzianego w art. 266 kk, tj. do 3 lat pozbawienia wolności, w przypadku gdy sprawcą jest funkcjonariusz, i 2 lat wobec pozostałych sprawców.

Amerykański ustawodawca przez użycie w § 798 USC pojęcia „ktokolwiek" (*whoever*) określił podmiot przestępstwa jako powszechny. Strona podmiotowa polega na świadomym (*knowingly*) i umyślnym (*willfully*) działaniu w zamiarze bezpośrednim, polegającym na ujawnieniu lub wykorzystaniu tajemnicy[75]. Ogólnym dobrem chronionym przez § 798 USC jest interes USA, który jest konkretyzowany ochroną tajemnic o wskazanym w przepisie charakterze. Są to między innymi niejawne informacje dotyczące budowy, rozwoju i działania urządzeń kryptograficznych oraz funkcjonowania wywiadu teleinformatycznego i informacji uzyskanych w wyniku tej działalności.

---

stanowiący jakiekolwiek wpływy uzyskane przez tego skazanego bezpośrednio lub pośrednio w wyniku takiego naruszenia lub majątek uzyskany z takich wpływów; i (B) jakikolwiek składnik majątku takiego skazanego, który wykorzystano lub przeznaczono do wykorzystania, w jakikolwiek sposób lub w jakiejkolwiek części, w celu dokonania lub ułatwienia dokonania takiego naruszenia").

[73] R. Dębski, *O przepisach blankietowych w prawie karnym. Uwagi wprowadzające*, „Acta Universitatis Lodziensis. Folia Iuridica" 1991, nr 47, s. 27.

[74] W. Zalewski, *Przestępca „niepoprawny" – jako problem polityki kryminalnej*, Gdańsk 2010, s. 387.

[75] Zob. szerzej: A.M. Taber, *Information control: making secrets and keeping them safe*, „Arizona Law Review" 2015, nr 2, s. 599 i nast.

Naruszenie tajności tego rodzaju informacji (przedmiocie wykonawczym czynu) ma nastąpić przez aktywne lub bierne zachowanie się sprawcy, tj. przekazanie, dostarczanie albo przesłanie informacji niejawnej nieupoważnionej osobie, a także uczynienie takiej informacji dostępnej dla nieupoważnionej osoby w inny sposób. Strona przedmiotowa tego przestępstwa może również polegać na upublicznieniu albo wykorzystaniu niejawnej informacji w sposób szkodliwy dla bezpieczeństwa USA lub przysporzeniu korzyści obcemu rządowi, z jednoczesną szkodą dla USA.

Znamiona czasownikowe użyte do konstrukcji przepisu § 798 USC („przekazuje", „upublicznia", „wykorzystuje" itd.) w istocie skutkują ujawnieniem tajemnicy, a zatem są one tożsame ze znamieniem przestępstwa polegającego na ujawnieniu chronionych informacji, o którym mowa w art. 265 § 1 polskiego kodeksu karnego. W § 798 USC termin „wykorzystanie" ma jednak inny charakter niż w polskim kodeksie, jest ono kryminalizowane wyłącznie w przypadku, gdy jest szkodliwe dla USA[76]. Tak więc przysporzenie korzyści dysponentowi tajemnicy w wyniku wykorzystania informacji niejawnych (bez naruszenia interesu państwa) nie jest karalne. Umieszczenie w omawianym przepisie, w pkt 1–4, katalogu rodzajów informacji niejawnych poważnie zawęża zakres penalizacji i możliwość karnego ścigania sprawcy ujawnienia tajemnic, jeżeli nie są one związane rzeczowo ze wskazanymi w tym przepisie zagadnieniami (materialnie – nie są tajemnicami). Ze względu na niemal kazuistyczny charakter § 798 USC, a przede wszystkim na jego część definicyjną, nie jest przepisem niezupełnym, w przeciwieństwie do adekwatnych regulacji polskich. Na uwagę zasługuje przedmiot wykonawczy czynu zabronionego, amerykański ustawodawca bowiem nie wartościuje odpowiedzialności karnej w zależności od klauzuli ujawnionych informacji, stosuje natomiast termin ogólny – „informacje niejawne" (polski kodeks karny w art. 265 uzależnia wymiar kary od klauzuli ujawnionej informacji).

Szczególnym przepisem prawa karnego materialnego w odniesieniu do § 798 USC jest czyn zabroniony polegający na bezprawnym usuwaniu lub zatrzymaniu niejawnych dokumentów albo materiałów (*unauthorized removal and retention of classified documents or material*), który został stypizowany w § 1924 USC[77].

---

[76] J.K. Elsea, *The Protection of Classified Information: The legal Framework*, Washington 2017, s. 14.

[77] USC, Title 18, Part 1, Chapter 93 – *Public officers and employees*, § 1924: „(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than five years, or both" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część 1, rozdział 93 – *Funkcjonariusze i pracownicy publiczni*, § 1924: „(a) Kto, będąc funkcjonariuszem, pracownikiem, wykonawcą lub konsultantem Stanów Zjednoczonych, i z mocy swojego urzędu, zatrudnienia, stanowiska lub umowy, mając dostęp do dokumentów lub materiałów zawierających informacje niejawne Stanów Zjednoczonych, świadomie wynosi takie dokumenty lub materiały bez upoważnienia z zamiarem zatrzymania takich dokumentów lub materiałów w niedozwolonym miejscu, podlega karze grzywny na mocy niniejszego tytułu lub pozbawienia wolności na okres do pięciu lat lub obu tym karom jednocześnie").

Podmiot tego przestępstwa jest określony rodzajowo, indywidualnie. Amerykański prawodawca ogranicza penalizację wyłącznie do osób związanych z rządem USA stosunkiem służby, pracy albo umową, w tym kooperacją handlową, które są podstawą legalnego dostępu do informacji niejawnych USA. Przez użycie pojęcia „świadomie" (*knowingly*) w opisie czynu ustawodawca wskazuje na umyślność sprawstwa. Dobrem chronionym przez omawiany przepis jest bezpieczeństwo informacji niejawnych USA. Przedmiot ochrony przejawia się przede wszystkim w dostępie do tajemnic osób uprawnionych oraz zabezpieczeniu tych tajemnic przed dostępem osób nieupoważnionych w trakcie przechowywania w warunkach sprzecznych z prawem.

Definicję pojęcia „informacje niejawne Stanów Zjednoczonych" zawarto w ustępie (c) omawianego paragrafu[78]. Prawodawca odwołuje się w niej do aktów wydanych przez władzę wykonawczą, które w interesie bezpieczeństwa narodowego USA były podstawą zakwalifikowania danych informacji jako niejawnych i wprowadziły zakaz ich ujawniania. Tak więc w części odnoszącej się do przedmiotu wykonawczego jest to przepis blankietowy, ponieważ w celu zdekodowania normy zakazu należy użyć definicji zawartych w innych aktach. Ten przepis odnosi się jedynie do informacji niejawnych mających formę dokumentów albo materiałów, wyłączone zatem z zakresu jego regulacji są informacje nieposiadające nośnika, tj. przekazywane ustnie albo gestami, co jest wynikiem warunkowania odpowiedzialności karnej nieautoryzowanym miejscem przechowywania tajemnic.

Strona przedmiotowa przestępstwa jest określona czynnością polegającą na bezprawnym usuwaniu informacji niejawnych albo na ich przechowywaniu w miejscu, które nie jest – zgodnie z prawem – do tego przeznaczone, np. w urządzeniu nieposiadającym certyfikatu bezpieczeństwa wydanego przez uprawniony organ państwowy. Inaczej mówiąc, polega na naruszeniu zasad regulujących fizyczne zabezpieczenia nośników tajemnicy. Zgodnie z ustępem (b) § 798 USC, podobnie jak w ustępie (c), ujawnienie informacji niejawnych wobec przedstawicieli Kongresu USA nie jest penalizowane.

Odrębnym aktem normującym wykorzystanie informacji niejawnych jest *Ustawa o postępowaniu z informacjami niejawnymi* z 1980 r.[79], w której został uregulowany

[78] Tamże, § 1924: „(c) In this section, the term 'classified information of the United States' means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security" (tamże, § 1924: „(c) W niniejszym paragrafie termin »informacje niejawne Stanów Zjednoczonych« oznacza informacje pochodzące od rządu Stanów Zjednoczonych, będące jego własnością lub przez niego posiadane, dotyczące obrony narodowej lub stosunków zagranicznych Stanów Zjednoczonych, które zostały określone zgodnie z prawem lub rozporządzeniem wykonawczym jako wymagające ochrony przed nieuprawnionym ujawnieniem w interesie bezpieczeństwa narodowego").

[79] Zob. szerzej: *Classified Information Procedures Act* of 1980, USC, Title 18, Appendix III (*Ustawa o postępowaniu z informacjami niejawnymi* z 1980 r., *Kodeks Stanów Zjednoczonych*, tytuł 18, załącznik III), https://uscode.house.gov/browse/prelim@title18/title18a/node16&edition=prelim [dostęp: 4 VI 2021].

sposób postępowania z informacjami niejawnymi znajdującymi się w materiałach postępowań karnych. W paragrafie pierwszym informacje niejawne zostały zdefiniowane jako wszelkie informacje albo materiały, które zostały zakwalifikowane przez rząd USA do kategorii „niejawne". Podstawą tej kwalifikacji są: zarządzenia wykonawcze (w literaturze występują często jako dekrety prezydenta USA), ustawy federalne oraz wewnętrzne akty normatywne administracji rządowej. Zgodnie z ustawą zaliczenia informacji do tajemnic dokonuje się w celu wymuszenia ich ochrony przed nieuprawnionym ujawnieniem w związku z bezpieczeństwem narodowym albo danymi zastrzeżonymi na mocy rozdziału 11 *Ustawy o energetyce atomowej* z 1954 r.

Na marginesie niniejszych rozważań warto dodać, że ważną inicjatywą zmieniającą przepisy prawa materialnego jest projekt nowelizacji federalnych przepisów karnych. Zmiana ma polegać na zwolnieniu oskarżyciela publicznego z obowiązku dowodzenia przed sądem zamiaru wyrządzenia szkody interesom USA przez oskarżonego urzędnika, który utracił informację niejawną w wyniku rażącego zaniedbania albo celowego bezprawnego jej przechowywania[80].

Podsumowanie

Wielopłaszczyznowość struktury systemu ochrony informacji niejawnych w Stanach Zjednoczonych, wielość aktów i brak unifikacji pojęć, jak chociażby zaprezentowane definicje „*classified information*" w rozumieniu § 798 oraz § 1924 USC, powodują zawiłość regulacji prawnych. Powyższe może stwarzać niepewność co do przesłanek złamania norm zakazów karnych albo administracyjnych, skutkujące odpowiedzialnością karną albo administracyjną dla ich adresatów. Odmienność modelu systemu prawnego USA i RP może wywołać u polskich odbiorców błędne przekonanie o wadliwej strukturze regulacji prawnych USA. Warto jednak zaznaczyć, że problematyka ochrony informacji niejawnych naszego partnera jest określona prawem stanowionym, jednak praktyka stosowania tych przepisów i kultura prawna kształtuje się w USA również przez stosowanie prawa precedensowego. Skuteczne wykorzystanie gwarancji procesowych przysługujących potencjalnemu sprawcy przestępstwa w dużej mierze jest determinowane łatwością dostępu do usług profesjonalnych prawników wykonujących zawód bez spełniania uciążliwych wymogów formalnych i korporacyjnych, z którymi mamy do czynienia w Polsce.

Ważnym postulatem *de lege ferenda* jest wprowadzenie do polskiego prawa karnego – przy uwzględnieniu adekwatnych regulacji prawnych USA – kontratypu, który uwalniałby od odpowiedzialności karnej depozytariuszy tajemnic przekazujących

[80] Zob. szerzej: projekt ustawy *Classified Information Protection Act* of 2016 nr H.R. 6034 –14th, złożony do Kongresu USA 14 IX 2016 r., skierowany do Podkomisji ds. Przestępczości, Terroryzmu, Bezpieczeństwa Wewnętrznego i Dochodzeń 27 IX 2016 r. (nowelizacja pozostała w fazie projektu), https://www.congress.gov/bill/114th-congress/house-bill/6034/text [dostęp: 4 VI 2021].

organom ścigania informacje niejawne bez uzyskiwania zgody organów określonych prawem, w celu ścigania sprawców przestępstw.

Konkludując, zarówno polski, jak i amerykański system ochrony tajemnic publicznoprawnych jest unormowany aktami prawa administracyjnego oraz jest oparty na karnoprawnej ochronie informacji niejawnych. Przyjęty w obu krajach sposób weryfikacji osób przed udostępnieniem im informacji niejawnych wykazuje duże podobieństwa. Co do zasady sprawdzenia są wykonywane w obu krajach przez służby specjalne na podstawie wniosku zainteresowanej instytucji oraz osoby mającej zostać sprawdzoną. Ze względu na niejawny sposób dokonywania czynności, w tym sprawdzeń danej osoby, trudno odnieść się do ich zakresu. Wyraźne podobieństwa regulacji polskich i amerykańskich zachodzą w przypadku przepisów ustanawiających uniwersalne kryteria klasyfikacji informacji i obejmowanie ich ochroną państwa. W RP zrezygnowano z konstruowania wykazów informacji, którym należy nadać określoną klauzulę wraz z rozpoczęciem obowiązywania ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Istotną różnicą jest charakter wydawanego poświadczenia bezpieczeństwa oraz decyzji o odmowie jego wydania. W Polsce jest to szczególnego rodzaju decyzja administracyjna, od której przysługują środki zaskarżenia do sądów administracyjnych, w USA natomiast negatywne rozstrzygnięcie postępowania co do jego istoty nie ma takiego przymiotu. Brak unifikacji aktów normatywnych kształtujących system ochrony informacji niejawnych w USA oraz ich duża liczba nie pozwala na przeprowadzenie rzetelnych porównań z aktami polskimi w formie zwięzłego artykułu. Powyższe pozwala zidentyfikować pewne różnice w sposobie zapewnienia bezpieczeństwa informacjom niejawnym w RP i USA, a ponieważ nie są one krańcowo różne, przyjęta na wstępie hipoteza robocza nie została potwierdzona.

Bibliografia

Abel J., *Do you have to keep the Government's secrets? Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record*, „University of Pennsylwania Law Review" 2015, nr 4, s. 1037–1098.

Bochentyn A., *Dopuszczalność dowodu z opinii biegłego na okoliczność treści prawa krajowego i europejskiego w jurysdykcyjnym postępowaniu administracyjnym*, w: *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, t. 2, J. Sługocki (red.), Wrocław 2014, Presscom, s. 359–375.

Borowicz J., *Przetwarzanie informacji niejawnych w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne" 2011, nr 7, s. 23–33.

Chromicka D., *Struktura regulacji ochrony informacji niejawnych*, w: *Jawność i jej ograniczenia*, t. 4: *Struktura tajemnic*, A. Gryszczyńska (red.), Warszawa 2016, C.H. Beck, s. 233–255.

Dębski R., *O przepisach blankietowych w prawie karnym. Uwagi wprowadzające*, „Acta Universitatis Lodziensis. Folia Iuridica" 1991, nr 47, s. 17–45.

Elsea J.K., *The Protection of Classified Information*: *The Legal Framework*, Washington 2017, Library of Congress, Congressional Research Service.

Kitrosser H., *Leak prosecutions and first amendment: New developments and a closer look at the feasibility of protecting leakers*, „William and Mary Law Review" 2015, nr 4, s. 1221–1277.

Leciak M., *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, TNOiK – Towarzystwo Naukowe Organizacji i Kierowania „Dom Organizatora".

Lewandowski K., *Przestępstwa przeciwko ochronie informacji w świetle rozdziału XXXIII Kodeksu karnego, orzecznictwa doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 61–76.

Marek A., Konarska-Wrzosek V., *Prawo karne*, Warszawa 2016, C.H. Beck.

Jawność i jej ograniczenia, t. 11: *Standardy europejskie*, C. Mik (red.), rozdz. 8: *Analiza pojmowania i działania zasady jawności oraz jej ograniczeń z perspektywy prawa Stanów Zjednoczonych Ameryki*, Warszawa 2016, C.H. Beck, s. 251–280.

Pułło A., *Konstytucja Stanów Zjednoczonych Ameryki*, Warszawa 2002, Wydawnictwo Sejmowe.

Taber A.M., *Information control: making secrets nad keeping them safe*, „Arizona Law Review" 2015, nr 2, s. 581–607.

Zalewski W., *Przestępca „niepoprawny" – jako problem polityki kryminalnej*, Gdańsk 2010, ARCHE.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzmocnionej współpracy obronnej, podpisana w Warszawie dnia 15 sierpnia 2020 r. (DzU z 2020 r. poz. 2153).

Memorandum o porozumieniu między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzajemności w ramach zamówień obronnych, podpisane w Waszyngtonie dnia 27 sierpnia 2011 r. oraz w Warszawie dnia 8 września 2011 r. (DzU z 2012 r. poz. 975).

Umowa o zabezpieczeniu społecznym między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisana w Warszawie dnia 2 kwietnia 2008 r. (DzU z 2009 r. nr 46 poz. 374).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej z dnia 8 marca 2007 r. (DzU z 2007 r. nr 224 poz. 1658).

Protokół dodatkowy między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisany w Brukseli dnia 12 stycznia 2004 r., do Traktatu o stosunkach handlowych i gospodarczych między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, sporządzonego w Waszyngtonie dnia 21 marca 1990 r. (DzU z 2005 r. nr 3 poz. 14).

Ustawa z dnia 20 marca 2015 r. o ratyfikacji Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie (DzU z 2015 r. poz. 686).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j.: DzU z 2019 r. poz. 742).

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j.: DzU z 2019 r. poz. 2325, ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j.: DzU z 2020 r. poz. 2176).

Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (t.j.: DzU z 2021 r. poz. 177).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j.: DzU z 2021 r. poz. 735).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (DzU z 2016 r. poz. 283).

Amerykańskie akty prawne

Constitution of the United States of America, House of Representatives, doc. No 110 – 50, 110th Congress.

Classified Information Protection Act of 2016, nr H.R. 6034 –14th, projekt ustawy.

Whistleblower Protection Enhancement Act of 2012, *United States Code*, Title 5, § 7211.

Intelligence Reform and Terrorism Prevention Act of 2004, *United States Code*, Title 50, § 401.

Critical Infrastructure Information Act of 2002, *United States Code*, Title 6, § 2135.

Whistleblower Protection Act of 1989, *United States Code*, Title 5, § 1201.

Intelligence Identities Protection Act of 1982, *United States Code*, Title 50, § 401.

Classified Information Procedures Act of 1980, *United States Code*, Title 18, Appendix III.

Freedom of Information Act of 1966, *United States Code*, Title 5, § 552.

Atomic Energy Act of 1954, *United States Code*, Title 42, § 1801.

Espionage Act of 1917, *United States Code*, Title 18, § 792.

Code of Federal Regulations, Title 18, Chapter I, Part 17, Subpart A, Section 17.13.

Code of Federal Regulations, Title 12, Chapter X, Part 1070, Subpart B, Section 1070, 1301.

United States Code, Title 18, Part I, Chapter 37, § 798.

United States Code, Title 18, Part 1, Chapter 93.

United States Code, Title 18, Part I, § 1924.

Zarządzenia wykonawcze prezydenta USA

The President Executive Order 13741 of 2016, *Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters*.

Presidential Policy Directive/PPD-19, *Protecting Whistleblowers with Access to Classified Information*, October 10, 2012.

The President Executive Order 13587 of 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing nad Safeguarding of Classified Information*.

The President Executive Order 13526 of 2009, *Classified National Security Information*.

The President Executive Order 13470 of 2008, *United States Intelligence Activities*.

The President Executive Order 13467 of 2008, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*.

The President Executive Order 12968 of 1995, *Access to Classified Information*.

The President Executive Order 12958 of 1995, *Classified National Security Information*.

The President Executive Order 12333 of 1981, *United States Intelligence Activities*.

The President Executive Order 12065 of 1978, *National Security Information*.

Rosyjskie akty prawne

Конституция Российской Федерации от 12 декабря 1993 г., принятая всенародным голосованием 12 декабря 1993 года, вступила в силу в день её официального опубликования в газете „Российская газета" от 25.12.1993 № 237.

Уголовное уложение от 1903 г., Собрание узаконений и распоряжений правительства от 16 Апреля 1903 г. номер 88.

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z 23 V 2018 r., sygn. SK 8/14.

Wyrok Trybunału Konstytucyjnego z 15 X 2009 r., sygn. akt K 26/08.

Wyrok Naczelnego Sądu Administracyjnego z 6 VII 2017 r., sygn. akt. I OSK 932/16.

Wyrok Sądu Najwyższego USA w sprawie Hustler Magazine v. Falwell, 485 U.S. 46, 02.24.1988.

Abstrakt

W artykule omówiono regulacje administracyjne związane z organizacją systemu ochrony informacji niejawnych, a także przedstawiono przepisy karne dotyczące ujawniania informacji niejawnych obowiązujące w USA wraz z ich interpretacją. Omówiono również przepisy administracyjne regulujące procedurę realizacji postępowań sprawdzających wobec urzędników administracji publicznej w celu wydania poświadczenia bezpieczeństwa umożliwiającego dostęp do informacji niejawnych. Ponadto wskazano przesłanki klasyfikacji informacji i obejmowania ich ochroną adekwatnej klauzuli niejawności. Na podstawie analizy przepisów USA między innymi sformułowano wniosek, że polskie ustawodawstwo nie obejmuje kontratypu, który uwalniałby od odpowiedzialności karnej depozytariuszy tajemnic przekazujących informacje niejawne (bez uzyskiwania zgody określonych prawem organów) w celu ścigania sprawców przestępstw. Powyższe może być podstawą legislacyjnego postulatu *de lege ferenda*, przy uwzględnieniu adekwatnych regulacji prawnych USA.

Należy zaznaczyć, że artykuł nie wyczerpuje poruszanego tematu, a jedynie wskazuje wybrane zagadnienia ochrony informacji niejawnych USA. Może to zostać wykorzystane do przeprowadzenia w przyszłości pogłębionych badań komparatystycznych dotyczących przedmiotowego zagadnienia.

Słowa kluczowe: kodeks karny, ujawnienie tajemnicy, informacje niejawne, postępowanie sprawdzające, poświadczenie bezpieczeństwa, kontrwywiad.

Protection of classified information in the USA. Selected penal and administrative regulations

Abstract

The article discusses the administrative regulations regarding the classified information protection system in the USA. Moreover, it presents the effective penal code provisions directed against the disclosure of classified information in the USA and their interpretations. What is more, the paper presents the administrative provisions regulating the procedure for carrying out security background investigation of public administration officials in order to issue a security clearance which grants them access to classified information. Further, the reasons for the classification of information and its protection with an adequate classification clause are explained. On the basis of the analysis of US regulations, a conclusion is drawn that Polish legislation does not include a justification for depositaries of secrets who disclose classified information (without obtaining the affirmation from the authorities specified by law) to prosecute the perpetrators of crimes. This could be the basis to formulate postulates *de lege ferenda*. It should be noted that the article does not exhaust the topic, but only indicates selected issues of the protection system of classified information in the USA. Initiated study can be used to carry out in-depth comparative research in this field in the future.

Keywords: penal code, disclosure, classified information, verifying screening, security background investigation, security clearance, counterintelligence.