WSTĘP

Problematyka dotycząca zagrożeń bezpieczeństwa narodowego leży w kręgu zainteresowań służb specjalnych, zarówno polskich, jak i zagranicznych. Obecnie obowiązujące uregulowania prawne w tym zakresie zostały wykreowane przed laty, często w okresie zimnej wojny, na podstawie ówczesnej siatki zagrożeń, w wielu wymiarach stanowiących reakcję na dwubiegunowy podział świata. Pojawienie się nowych rodzajów zagrożeń o charakterze hybrydowym, łączących w sobie działania destabilizacyjne, konwencjonalne, nieregularne, cybernetyczne czy też dezinformacyjne, oraz zagrożeń asymetrycznych, takich jak terroryzm, wreszcie postępująca informatyzacja praktycznie wszystkich dziedzin życia oraz rozwój nowych technologii i miniaturyzacja technologii, stanowią asumpt do podjęcia dyskusji na temat gruntownej redefinicji zadań i narzędzi organów odpowiadających za bezpieczeństwo państwa, w tym służb specjalnych, a zwłaszcza ich organizacji. Znalezienie właściwego remedium na współczesne zagrożenia – przy jednoczesnym zagwarantowaniu konstytucyjnych wolności i praw człowieka i obywatela – jest kwestią niezwykle istotną nie tylko z punktu widzenia organów władzy wszystkich państw na świecie, lecz także społeczeństwa obywatelskiego.

Niniejsza publikacja jest kontynuacją dyskusji zapoczątkowanej w opracowaniu pt. *Analiza rozwiązań prawnych w zakresie funkcjonowania służb specjalnych w wybranych państwach* wydanym w maju 2017 r. przez Agencję Bezpieczeństwa Wewnętrznego w ramach serii wydawniczej Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego. Opracowanie zatytułowane *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* jest poświęcona największym wyzwaniom, przed jakimi stoją obecnie służby specjalne całego świata, w tym polskie.

Służby specjalne wszystkich państw stoją w chwili obecnej przed koniecznością takiego określenia ich uprawnień, aby z jednej strony skutecznie rozpoznawać wszelkie zagrożenia bezpieczeństwa narodowego, zapobiegać i przeciwdziałać im oraz je zwalczać, a z drugiej – aby działania służb nie naruszały praw i wolności obywatelskich. Ma temu służyć m.in. właściwe zdefiniowanie pojęcia bezpieczeństwo narodowe oraz jego zakresu, które jest przedmiotem wielu rozważań oraz dyskusji naukowych. Właściwa interpretacja bezpieczeństwa narodowego jest zasadnicza dla funkcjonowania służb specjalnych na całym świecie, a także dla określenia granic ingerencji organów państwa w wolności i swobody obywatelskie. Szczególnie istotne jest znaczenie wyżej wymienionego pojęcia w prawie europejskim, gdyż stosowanie różnego rodzaju instrumentów prawnych (w kontekście korzystania przez służby z ich kompetencji wywiadowczych i kontrwywiadowczych) podlega wielu rygorom prawnym wynikającym z rozmaitych aktów prawa Unii Europejskiej, ale przede wszystkim ograniczeniom, których źródłem są podstawowe wolności i prawa obywatelskie.

Niniejsze opracowanie zawiera analizę istniejących rozwiązań prawnych w zakresie prawa europejskiego, podejmuje również próbę wskazania ich prawidłowej inter-

pretacji na podstawie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej oraz uwzględnia kontekst bieżących prac legislacyjnych na forum Unii Europejskiej, odnoszących się do bezpieczeństwa narodowego. Ponadto w publikacji podjęto próbę usystematyzowania problemu kontroli i nadzoru nad służbami specjalnymi w Rzeczpospolitej Polskiej, które są przejawem gwarancji przyznanych obywatelom na mocy Konstytucji RP. Jednocześnie ten aspekt został uzupełniony o analizę prawno-porównawczą modeli nadzoru i kontroli nad służbami występujących w wybranych porządkach prawnych państw tożsamych kulturowo.

Sprawą bezsporną dla organów władzy wszystkich państw jest przyznanie służbom takich instrumentów, a także taki podział między nie zadań, aby w sposób efektywny mogły przeciwdziałać wielu zagrożeniom bezpieczeństwa narodowego i społeczeństwa. Przykładem realizacji powyższego w Rzeczpospolitej Polskiej jest niewątpliwie *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, która przyznała polskim służbom różnego rodzaju kompetencje, w tym nowe uprawnienia operacyjno-rozpoznawcze w zakresie zapobiegania zdarzeniom o charakterze terrorystycznym. Z uwagi na to, że wspomniana ustawa jest jednym z najważniejszych aktów prawnych regulujących tak istotne zagadnienie, jakim niewątpliwie jest ochrona przed zamachami terrorystycznymi, zdecydowano o przedstawieniu w niniejszej publikacji etiologii prac nad nią. Przy opracowywaniu tekstu wyżej wymienionej ustawy istotne znaczenie miało właściwe wyważenie adekwatności środków i narzędzi przyznanych służbom, które będą skuteczne w zapobieganiu aktom o charakterze terrorystycznym i jednocześnie nie będą naruszały istoty konstytucyjnych wolności i praw człowieka i obywatela, co, jak się wydaje, udało się osiągnąć. Zasygnalizowano jednocześnie ważne elementy powyższego aktu prawnego, zwłaszcza przez wskazanie pojawiających się poglądów doktryny i sądownictwa w kontekście interesującego nas zagadnienia.

Jednym z najważniejszych czynników negatywnie wpływających na bezpieczeństwo narodowe jest – oprócz ataków terrorystycznych – działalność wywiadowcza obcych służb. Z uwagi na mnogość działań, które wpisują się w taką działalność, a które często mogą się łączyć z zamiarem zdestabilizowania sytuacji wewnętrznej kraju, wydaje się, że sprawą niezwykle istotną dla polskiej racji stanu, bezpieczeństwa narodowego oraz ochrony konstytucyjnych wolności i praw człowieka i obywatela winno być właściwe przedefiniowanie pojęć p r z e s t ę p s t w o s z p i e g o s t w a i samego pojęcia w y w i a d. Niniejsza publikacja ma na celu wywołanie dyskusji dotyczącej koniecznych zmian regulacyjnych obejmujących ten czyn zabroniony, ukierunkowanych z jednej strony na rozwiązanie praktycznych problemów pojawiających się na tym gruncie w praktyce funkcjonowania służb w Polsce, a z drugiej – na aktualizację tej normy prawnej w celu jej dostosowania do zmieniającej się siatki zagrożeń bezpieczeństwa Rzeczpospolitej Polskiej, oscylujących wokół zagrożeń o charakterze hybrydowym i asymetrycznym.

Opisując zagrożenia bezpieczeństwa narodowego, nie należy zapominać także o sieciach teleinformatycznych, które mogą stać się celem ataku zarówno dla terrorystów, jak i obcych służb specjalnych. Właściwe zorganizowanie porządku instytucjonalnego w zakresie cyberobrony zaprząta obecnie uwagę rządów w wielu krajach, ale odpowiedzi na pytanie, jak powinien wyglądać model właściwy, bywają różne. Publikacja, którą trzymają Państwo w ręku, zawiera również charakterystykę modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia funkcjonowania wybranych służb specjalnych na świecie. To zagadnienie jest o tyle istotne, że potencjalne ataki w cyberprzestrzeni mogą godzić w sektory strate-

giczne z punktu widzenia bezpieczeństwa narodowego (jak np. w energetykę, system finansowy czy obronny), ale także – z uwagi na powszechny dostęp do Internetu – w zwykłych użytkowników tej sieci. Nie należy zapominać o tym, że informacje, które są niejednokrotnie przechowywane przez użytkowników na twardych dyskach komputerowych, oraz przesyłane przez nich dane, często zawierają dane osobowe lub inne dane wrażliwe. Kradzież danych osobowych i innych tego typu informacji stanowi niewątpliwie poważne zagrożenie obywateli, ich wolności i praw odnoszących się m.in. do prawa do prywatności, ochrony wizerunku czy tajemnicy korespondencji.

W publikacji zdecydowano się przedstawić także charakterystykę rozwiązań legislacyjnych i najważniejszych problemów związanych z – budzącą spory natury prawnej i etycznej w większości państw Unii Europejskiej i NATO – praktyką wykorzystywania przez służby specjalne instrumentów pozwalających na pozyskiwanie danych za pośrednictwem systemów i sieci informatycznych. Dane dotyczące prowadzenia tego typu działań na masową skalę przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA) zostały ujawnione w 2013 r. przez byłego analityka tej Agencji, Edwarda Snowdena. Wywołało to duże kontrowersje nie tylko w Stanach Zjednoczonych, lecz także w państwach europejskich i było katalizatorem trwającej do dziś debaty publicznej nad rolą służb specjalnych i granicami ich kompetencji w systemie demokratycznym, zwłaszcza w kontekście przestrzegania praw i wolności człowieka i obywatela.

Istotnym zagadnieniem wchodzącym w zakres bezpieczeństwa narodowego jest także problem ochrony informacji niejawnych. Obecnie obowiązująca *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* zawiera rozwiązania, które sprawiają, że system ochrony tego typu informacji w Rzeczpospolitej Polskiej nie działa w pełni efektywnie. W związku z powyższym w niniejszej publikacji podjęto próbę sformułowania propozycji zmian legislacyjnych, które wzmocnią skuteczność działania systemu ochrony informacji niejawnych przez uwzględnienie wieloletniego doświadczenia nabytego przez organy sprawujące nadzór nad tym systemem oraz inne właściwe podmioty. Jednocześnie zdecydowano się na wskazanie rozwiązań, których celem miałoby być dostosowanie przepisów wyżej wymienionej ustawy do planowanych zmian w całym systemie bezpieczeństwa państwa.

Należy podkreślić, że przyznanie odpowiedniego zakresu uprawnień i instrumentów (odpowiedzialności) służbom specjalnym jest zagadnieniem niezwykle złożonym. Nie należy zapominać, iż kompetencje przysługujące służbom często stoją w pozornej sprzeczności z zagwarantowanymi konstytucyjnie wolnościami i prawami obywatelskimi. Zadaniem organów władzy jest pogodzenie obu tych wartości, co stanowi poważne wyzwanie ustawodawcze. Jednym z podstawowych praw człowieka i obywatela jest prawo do ochrony danych osobowych. Ochrona tego typu danych jest stosunkowo nową gałęzią ochrony praw jednostki, która jednak w ostatnim czasie, na skutek przemian społecznych i gospodarczych wywołanych powszechną w skali globalnej informatyzacją, zyskuje w szybkim tempie na znaczeniu. W chwili obecnej trwa wielka reforma systemu danych osobowych w Unii Europejskiej zwiększająca m.in. uprawnienia podmiotu danych. Takie ukształtowanie ustawodawstwa unijnego będzie oddziaływało na prawa i obowiązki służb specjalnych, dla których niejawne przetwarzanie informacji o osobach jest nieodzownym elementem działalności służącej ochronie innych fundamentalnych wartości, wśród których poczesne miejsce zajmuje prawo obywateli do życia.

Z gwarancją ochrony danych osobowych nierozerwalnie łączy się problem retencji danych. W ostatnim czasie stał się on niezwykle istotny dla działalności europejskich

organów ścigania i służb specjalnych z uwagi na wyrok Trybunału Sprawiedliwości Unii Europejskiej z 21 grudnia 2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB/Post-ochtelestyrelsen i C-698/15 Secretary of State for the Home Departament/Tom Watson i inni, znany powszechnie jako „wyrok w sprawie Tele2". Najważniejszą tezą tego wyroku jest stwierdzenie przez TSUE, że państwa członkowskie nie mogą nakładać na dostawców usług komunikacji elektronicznej ogólnego obowiązku retencji danych.

W publikacji przedstawiono także analizę międzynarodowych i krajowych podstaw prawnych reagowania na zdarzenia CBRN. Została ona sporządzona w celu weryfikacji stopnia zgodności polskich przepisów prawnych z przepisami prawa międzynarodowego oraz identyfikacji obszarów, w których system prawa polskiego w zakresie reagowania na zdarzenia CBRN winien zostać zmodyfikowany.

Szef
Agencji Bezpieczeństwa Wewnętrznego
prof. dr hab. Piotr Pogonowski