

Emilian Kaufman

Realizacja zadań i uprawnień polskich służb specjalnych w aspekcie ochrony praw człowieka¹

Zamachy terrorystyczne, jakie dotyczą społeczeństwa praktycznie na całym świecie na przestrzeni ostatnich kilkunastu lat, bez względu na poziom demokracji państwa i przestrzegania prawa, stawiają przed sprawującymi władzę nowe zadania dotyczące zapewnienia obywatelom należytego poziomu bezpieczeństwa, zarówno w wymiarze wewnętrznym, jak i międzynarodowym. Działalność służb specjalnych² jest nieodłącznie powiązana z zagwarantowaniem bezpieczeństwa państwa, które jest podstawą prawidłowego funkcjonowania demokracji. Stanem bezpieczeństwa określa się możliwość ochrony wartości immanentnych dla przetrwania państwa, takich jak: terytorialna integralność, biologiczne przeżycie ludności czy suwerenność. Istotna jest też rola, jaką służby specjalne odgrywają w pozyskiwaniu informacji o możliwych zagrożeniach. W związku ze zmianami zagrożeń będzie się również zmieniał charakter oraz zakres wiadomości stanowiących przedmiot zainteresowania służb. Bezpieczeństwo państwa zależy w dużym

¹ Fragment pracy magisterskiej pt. *Ochrona praw człowieka przy realizacji uprawnień służb specjalnych*, która została wyróżniona w konkursie Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2015/2016). Autor jest absolwentem Katolickiego Uniwersytetu Lubelskiego, Wydziału Prawa. Redakcja dokonała w tekście niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

² Służby specjalne to „(...) ogólna nazwa dla cywilnych i wojskowych służb organizujących i prowadzących działania wywiadowcze i kontrwywiadowcze”, zob. *Słownik terminów z zakresu bezpieczeństwa narodowego*, W. Łepkowski (red.), Warszawa 2002, s. 116. Także: <http://pl.scribd.com/doc/98030285/S%C5%81OWNIK-TERMINOW-Z-ZAKRESU-BEZPIECZE%C5%83STWA-NARODOWEGO-AON#scribd> [dostęp: 28 III 2016]. Inna definicja: „(...) służby usytuowane w strukturze aparatu państwowego, samodzielne organizacyjnie lub wchodzące w skład innej jednostki państwowej, instytucje uprawnione do prowadzenia działań o charakterze tajnym z wykorzystaniem metod operacyjnych, naruszających prawa i wolności osobiste”, zob. J. Larecki, *Wielki leksykon służb specjalnych świata*, Warszawa 2007, s. 621. Patrz również R. Grochowski, *Rola służb specjalnych w demokratycznym państwie prawa*, „Środkowoeuropejskie Studia Polityczne” 2013, nr 4, s. 195; http://ssp.amu.edu.pl/?page_id=310 [dostęp: 24 III 2016]; http://ssp.amu.edu.pl/wp-content/uploads/2014/03/SSP_2013_4_195-208.pdf [dostęp: 28 III 2016]. Określenie służby specjalne zostało przywołane w art. 11 ustawy o ABW: „(...) działalności ABW, AW, Służby Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, zwanych dalej »służbami specjalnymi«, jak również w art. 40 ust.1 tejże ustawy, tj.: „Szef ABW koordynuje podejmowane przez służby specjalne czynności operacyjno-rozpoznawcze”. Te służby zostały również wymienione w art. 13a ordynacji podatkowej, zob. *Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa* (Dz.U. z 2015 r. poz. 613, ze zm.). Za Z. Grzegorowskim: „Każda z tych służb w Polsce została wyodrębniona zarówno instytucjonalnie, jak i prawnie”, Z. Grzegorowski, *Instytucja „służby specjalne” a rzeczywistość funkcjonowania państwa polskiego. Wybrane zagadnienia*, „Studia Gdańskie. Wizje i rzeczywistość” 2010, t. 8, s. 47.

stopniu od skuteczności pozyskiwania informacji ważnych z punktu widzenia interesów państwa. Rola służb specjalnych powinna być postrzegana przez pryzmat funkcji im przypisywanych. W czasie pokoju służby realizują funkcje: a) informacyjną – polegającą m.in. na rozpoznawaniu zagrożeń i przeciwdziałaniu im; b) procesową – obejmującą m.in. rozpoznawanie, wykrywanie i ściganie sprawców przestępstw; c) ochronno-kontrolną – realizowaną jako ochrona informacji niejawnych. Wsparcie sił zbrojnych państwa lub sojuszu militarnego to zadania, na których koncentrują się służby specjalne w przypadku konfliktu zbrojnego³. Polskie służby specjalne są wyposażone w wiele narzędzi służących do realizacji zadań nadanych im przez ustawy kompetencyjne. Naczelnym celem służb jest ochrona interesów Rzeczypospolitej Polskiej oraz zapewnienie bezpieczeństwa jej obywatelom. Jednocześnie, co oczywiste, przez działania służb są zagrożone prawa człowieka. Każde uprawnienie wykorzystane w sposób sprzeczny z ustawą bądź wewnętrznymi rozporządzeniami jest poważnym zagrożeniem praw i wolności człowieka. Podczas podejmowania walki z najgroźniejszymi rodzajami przestępczości, włącznie z terroryzmem, służby specjalne stosują ofensywne działania operacyjno-rozpoznawcze, które mogą prowadzić do wystąpienia negatywnych implikacji będących zagrożeniem dla jednostki przez zbyt daleką ingerencję w sferę jej praw i wolności. Celem organów nadzorczych jest dopilnowanie, aby służby działały w ramach i na podstawie prawa. Zasadne jest przedstawienie uprawnień charakterystycznych dla służb specjalnych wraz ze wskazaniem na zakres ingerencji w prawa człowieka.

Czynności operacyjno-rozpoznawcze jako priorytetowa forma działań służb specjalnych

Czynności operacyjno-rozpoznawcze⁴ są w praktyce stosowane zarówno przez

³ M. Bożek, i in., *Służby specjalne w strukturze władz publicznych*, Warszawa 2014, s. 62–63.

⁴ Nie istnieje definicja legalna czynności operacyjno-rozpoznawczych. Stanowią one zespół „(...) jawnych i niejawnych przedsięwzięć” prowadzonych przez służby państwowe na podstawie upoważnień zawartych w ustawach „(...) wyłącznie w celu rozpoznania, zapobiegania i wykrywania przestępstw; odnajdywania osób ukrywających się oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginięcie jest wynikiem przestępstwa, a także odnajdywanie rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem; ustalenia tożsamości osób i zwłok, w przypadku uzasadnionego podejrzenia przestępczego działania”, zob. art. 1 ust. 3, art. 2 ust. 1 pkt 1, 2, 3 *Projekt ustawy o czynnościach operacyjno-rozpoznawczych*, druk sejmowy nr 353. Natomiast zgodnie z art. 2 ust. 2 pkt 1 i 2 tego *Projektu*: „Czynności operacyjne w szczególności polegają na uzyskiwaniu, gromadzeniu, przetwarzaniu i sprawdzaniu w sposób jawny i niejawny informacji o przestępstwach; uzyskiwaniu dokumentacji, próbek i materiałów porównawczych w celu ujawnienia lub zabezpieczenia dowodów przestępstwa”. Wacław Marciniak definiuje pracę operacyjną „(...) jako ogół czynności operacyjno-rozpoznawczych wykonywanych przez Policję w celu rozpoznania, zapobiegania, wykrywania przestępstw i wykroczeń. Składa się na nią zespół jawnych i niejawnych metod, form, środków i przedsięwzięć taktyczno-technicznych, opartych na przepisach prawa i wiedzy kryminalistycznej”, patrz J. Kudła, *Wybrana problematyka czynności operacyjnych na tle uwag de large ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych*, Prokuratura Okręgowa w Zielonej Górze, <http://www.zielona-gora.po.gov.pl/index.php?id=26> [dostęp: 17 V 2016]; także: W. Marciniak, *Praca operacyjna Policji*, Szczytno 2001. Według „(...) T. Hanauska czynności

policję, jak i inne służby, w tym służby specjalne. Należą one do codziennych środków walki z przestępczością oraz stanowią najskuteczniejszą metodę pozyskiwania informacji. Czynności, o których mowa, nie mają ustawowej definicji, w związku z czym w niniejszej pracy przywołano kilka ich określeń. Działalność służb specjalnych jest nierozdzielnie związana ze zdobywaniem informacji w sposób niejawnym⁵. Czynności operacyjno-rozpoznawcze muszą być prowadzone z poszanowaniem godności oraz respektowaniem praw i wolności człowieka⁶. Niejednokrotnie te czynności są jedynym sposobem na pozyskanie wiarygodnych informacji, ustalenie źródeł dowodowych, sprawców przestępstw, miejsc przechowywania oraz zabezpieczenie dowodów rzeczowych⁷. W projekcie ustawy o czynnościach operacyjno-rozpoznawczych zawarto następujące metody ich prowadzenia: wywiad, penetracja terenu, zasadzka, eksperyment, analiza operacyjna, obserwacja osób, miejsc i środków transportu, pułapka, współpraca z osobami fizycznymi niebędącymi funkcjonariuszami polegająca na przekazywaniu informacji i dokumentów świadczących o planowaniu przestępstwa, wykonywaniu zadań i zleconych czynności w celu rozpoznania, zapobiegania i wykrywania przestępstw, kontrola korespondencji (kontrola operacyjna⁸), środki techniczne – podsłuch rozmów telefonicznych, podsłuch i podgląd pomieszczeń oraz osób, podsłuch techniczny środków łączności przewodowej i radiowej, nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu, nadzór elektroniczny środków łączności przewodowej i radiowej, zakup kontrolowany⁹, przesyłka

operacyjno-rozpoznawcze stanowią odrębny system poufnych bądź tajnych działań, uprawnionych do tego ustawowo organów, prowadzonych poza procesem karnym, lecz zazwyczaj służących aktualnym lub przyszłym celom tego procesu i wykonywanych dla zapobiegania i zwalczania przestępczości oraz innych negatywnych zjawisk społecznych”, za: M. Bożek i in. *Służby specjalne...*, s. 110.

⁵ M. Bożek i in., *Służby specjalne...*, s. 109.

⁶ Art. 4 ust. 1 *Projekt ustawy o czynnościach...*

⁷ A. Szumski, *Rola czynności operacyjno-rozpoznawczych w uzyskiwaniu dowodów w procesie karnym*, „Nowa kodyfikacja prawa karnego” 2010, t. 26, s. 195–198.

⁸ Za kontrolę operacyjną należy rozumieć czynności operacyjno-rozpoznawcze prowadzone niejawnie polegające na „(...) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; uzyskiwaniu dostępu i kontroli zawartości przesyłek” – art. 27 ust. 6 ustawy o ABW oraz AW, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW oraz SWW.

⁹ Zakupem kontrolowanym określa się „(...) czynności operacyjno-rozpoznawcze zmierzające do sprawdzenia uzyskanych wcześniej wiarygodnych informacji o przestępstwie oraz wykrycia sprawców i uzyskania dowodów mogą polegać na dokonaniu w sposób niejawnym nabycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi, albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także przyjęcie lub wręczenie korzyści majątkowej” – art. 29 ust. 1 ustawy o ABW oraz AW, art. 19 ust. 1 ustawy o CBA, art. 33 ust. 1 ustawy o SKW oraz SWW.

niejawnie nadzorowana¹⁰, obiekty specjalne¹¹, kombinacja operacyjna¹², gra operacyjna¹³ oraz operacja specjalna¹⁴.

Ze względu na wzrost znaczenia ujęcia prawnoprocesowego czynności operacyjno-rozpoznawczych, w tym na możliwość uzyskania dowodów przestępstwa, te czynności pełnią bardzo istotną funkcję¹⁵. Powszechny jest pogląd, że głównym narzędziem realizacji ustawowych zadań służb specjalnych są ich uprawnienia operacyjne. Zasadność tej tezy potwierdza działalność służb specjalnych, która może być rozpatrywana w dwóch ujęciach, tj. w roli informacyjnej i wykrywczej, jaką odgrywają one w zakresie bezpieczeństwa państwa, oraz w utajonym charakterze ich funkcjonowania. Te dwie cechy wpływają w zdecydowany sposób na wykorzystywanie przez służby specjalne posiadanych uprawnień ustawowych w zakresie realizowania czynności operacyjno-rozpoznawczych. Uprawnienia operacyjne w najwyższym stopniu są właściwe do niejawnego (tajnego) pozyskiwania informacji o zagrożeniach i ewentualnych przestępstwach oraz ich weryfikacji. W ustawach kompetencyjnych używa się terminu *czynności operacyjno-rozpoznawcze*. Na pierwszym miejscu wymienia się właśnie te czynności, a dopiero później czynności dochodzeniowo-śledcze, analityczno-informatyczne bądź kontrolne. Tajność czynności operacyjno-rozpoznawczych w ustawach kompetencyjnych jest zaakcentowana m.in. pod określeniami: „niejawnie”, „niejawnego charakteru podejmowanych czynności”, „w sposób niejawnym” oraz „niejawny cha-

¹⁰ Pod pojęciem *przesyłka niejawnie nadzorowana* rozumie się „(...) czynności operacyjno-rozpoznawcze zmierzające do udokumentowania przestępstw”, wskazanych w ustawach kompetencyjnych „(...) albo ustalenia tożsamości osób uczestniczących w tych przestępstwach lub przejęcia przedmiotów przestępstwa”, polegające na niejawnym nadzorowaniu „(...) wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia dla życia lub zdrowia ludzkiego” – zob. art. 30 ust. 1 ustawy o ABW oraz AW, art. 34 ust. 1 ustawy z o SKW oraz SWW.

¹¹ Za *obiekty specjalne* uznaje się „(...) rzeczowe środki pracy operacyjnej w postaci zespołu nieruchomości, lokali mieszkalnych i użytkowych oraz pojazdów pozostających w dyspozycji służb państwowych, których faktyczne przeznaczenie jest zakamuflowane” – art. 2 ust. 3 pkt 13 *Projekt ustawy o czynnościach...*

¹² *Kombinacja operacyjna* to „(...) zaplanowane i przygotowane przedsięwzięcie, realizowane przy użyciu pozostałych metod pracy operacyjnej”, m.in. wywiadu, penetracji terenu, zasadzki, eksperymentu, analizy operacyjnej, obserwacji, współpracy z osobami fizycznymi, „(...) wykorzystujące błędne przeświadczenie osób, przeciwko którym jest skierowane, co do faktycznego znaczenia zaangażowanych zdarzeń oraz osób w nich występujących, służące osiągnięciu celów pracy operacyjnej” – art. 2 ust. 3 pkt 14 *Projekt ustawy o czynnościach...*

¹³ *Gra operacyjna* to „(...) najbardziej złożona metoda pracy operacyjnej, stanowiąca rodzaj kombinacji operacyjnej charakteryzująca się długofalowością i szczególnym skomplikowaniem podejmowanych działań” – art. 2 ust. 3 pkt 15 *Projekt ustawy o czynnościach...*

¹⁴ *Operację specjalną* stanowi „(...) szczególny rodzaj kombinacji operacyjnej charakteryzujący się stosowaniem działań maskujących, w szczególności w postaci zespołu czynności określonych” w kombinacji operacyjnej, grze operacyjnej oraz z wykorzystaniem obiektów specjalnych – zob. art. 2 ust. 3 pkt 16 *Projekt ustawy o czynnościach...*

¹⁵ M. Bożek i in., *Służby specjalne...*, s. 109.

rakter czynności”¹⁶. Czynności operacyjno-rozpoznawcze mogą być wykonywane nie tylko pod kątem uzyskiwania informacji o potencjalnych zagrożeniach, lecz także w celu zwalczania przestępstw. W ustawach kompetencyjnych wyraźnie wskazano, że służby specjalne podejmują (...) *czynności operacyjno-rozpoznawcze w celu zapobiegania popełnianiu przestępstw, ich rozpoznawania i wykrywania*, a także w celu (...) *uzyskiwania i przetwarzania informacji istotnych z zakresu zwalczania zagrożeń ukierunkowanych na określone wartości*, jak np. porządek konstytucyjny, bezpieczeństwo państwa, zagrożenie międzynarodowym terroryzmem czy też interesy ekonomiczne państwa. Jak widać, uprawnienia służb specjalnych do przeprowadzania czynności operacyjno-rozpoznawczych w znacznej mierze są narzędziem uniwersalnym, a ich funkcjonariusze mogą je realizować zarówno w celu zwalczania przestępczości, jak i w związku z prowadzonymi typowymi działaniami profilaktyczno-kontrywywiadowczymi, a nie wykrywczymi. Oczywiście uzyskiwanie informacji co do zdarzeń zakłócających normalne funkcjonowanie państwa może być realizowane nie tylko przez stosowanie czynności operacyjno-rozpoznawczych, lecz także czynności procesowych (dochodzeniowo-śledczych). Jednak służby specjalne, tj. tylko ABW i CBA, mogą prowadzić czynności procesowe wyłącznie w ramach prowadzonego postępowania przygotowawczego. Z reguły czynności operacyjno-rozpoznawcze są prowadzone przed wszczęciem postępowania przygotowawczego, które to niejednokrotnie jest możliwe dzięki zdobyciu informacji podczas realizowanej pracy operacyjnej. Czynności, o których mowa, mogą być też prowadzone równoległe do toczącego się postępowania przygotowawczego, a nawet po jego zakończeniu. Skuteczne działanie służb specjalnych, znaczenie sprawy i jej charakter determinują, z jakich uprawnień będą korzystały służby i na jakim etapie realizowanych czynności je zastosują¹⁷.

Pozaprocessowy charakter czynności operacyjno-rozpoznawczych polega na tym, że są one podejmowane i realizowane poza procesem karnym, w trybie innym niż wynikający z kodeksu postępowania karnego¹⁸, chociaż rezultat tych czynności może być wykorzystany w przyszłości w procesie karnym. Rezultaty czynności operacyjno-rozpoznawczych nie sprowadzają się jedynie do pozyskiwania informacji, lecz także do ich gromadzenia, analizy, sprawdzania bądź przetwarzania. W sferze operacyjnego, zgodnego z prawem, zainteresowania służb mogą znaleźć się zarówno osoby, jak i miejsca, przedmioty lub zagrożenia¹⁹.

Tylko niektóre z czynności operacyjno-rozpoznawczych realizowane przez służby specjalne znajdują swoje bezpośrednie umocowanie w ustawach. Funkcjonariusze tych służb podejmują także działania, które nie mają bezpośredniego oparcia

¹⁶ Zob. art. 27 ust. 6 i 8, art. 29 ust. 1 i 5 ustawy o ABW oraz AW.

¹⁷ M. Bożek, *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej” 2015, nr 1, s. 18–22.

¹⁸ *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (Dz.U. z 1997 r. nr 89 poz. 555, ze zm.).

¹⁹ Z. Niemczyk, *Czynności operacyjno-rozpoznawcze i możliwość wykorzystania ich rezultatów w postępowaniu karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury” 2013, z. 3, s. 6.

w normach ustaw, a ich realizacja przybiera postać „sposobów, metod i form” kodyfikowanych nie w ustawach kompetencyjnych, ale w zarządzeniach wydawanych przez szefów służb specjalnych²⁰. Szefowie służb (...) *każdy w zakresie swojej właściwości, w drodze zarządzeń, określają sposoby, metody i formy wykonywania zadań (...) w zakresie nieobjętym innymi przepisami*²¹. Zarządzenia przez nich wydawane na podstawie powyższej normy, w celu określenia „sposobów, metod i form” realizacji zadań, w żaden sposób nie mogą przeistaczać rozwiązań ustawowych przyjętych w tym zakresie. Te zarządzenia nie podlegają publikacji – są dokumentami niejawnymi. Tego rodzaju rozwiązania mogą wywoływać w demokratycznym państwie prawnym wątpliwości i kontrowersje. W państwie prawnym bowiem ostatecznością jest ingerowanie w wolności i prawa jednostki, a w razie konieczności działania państwa realizowane w tym zakresie muszą mieć ustawowe umocowanie (chodzi tutaj o konieczne rozwiązania konstytucyjne).

W Konstytucji RP czynności operacyjno-rozpoznawcze nie są jednoznacznie wymienione jako dozwolone ograniczenie praw i wolności jednostki²². Trybunał Konstytucyjny w wyroku z 12 grudnia 2005 r., sygn. akt K 32/04²³, zważył między innymi:

Wniosek Rzecznika Praw Obywatelskich kwestionuje kilka przepisów ustawy (...) oraz zarządzenie (...) w kwestii pozyskiwania, w trybie czynności operacyjnych (...) informacji i przechowywania tych informacji. Są to przepisy dotyczące różnych aspektów i sposobów wkraczania władzy wykonawczej w prywatność jednostki, w zakresie jej konstytucyjnie unormowanych wolności komunikowania się i ochrony związanej ze sferą prywatną (...) realizującą swe kompetencje poprzez czynności operacyjno-rozpoznawcze. Czynności te są z natury rzeczy niejawne (także wobec zainteresowanego), prowadzone w warunkach dających policji szeroki margines uznaniowości, przy ograniczonych gwarancjach dla praw osoby poddanej tym czynnościom, a także okrojonej kontroli zewnętrznej, w tym sądowej. Ten sposób działania (...) jest we współczesnym państwie nieodzowny. Przejrzystość czynności operacyjnych powodowałaby ich nieskuteczność. Współczesne państwo, zobowiązane do zapewniania bezpieczeństwa (co także jest powinnością konstytucyjną), staje przed trudnym zadaniem, ze względu na zagrożenia terroryzmem, przestępczością (w tym także zorganizowaną). Techniczne udogodnienia, wpływające na szybkość komunikowania się i przemieszczania, w równym stopniu mogą być wykorzystywane w celu ochrony bezpieczeństwa państwa, jak i przez przestępców. Działalność operacyjna (...) regulowana w ustawodawstwie zwykłym, realizowana w warunkach nie-

²⁰ M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 25.

²¹ Art. 19 ust. 3 ustawy o ABW oraz AW, art. 10 ust. 3 ustawy o CBA, art. 20 ust. 3 ustawy o SKW oraz SWW.

²² M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 25–26.

²³ *Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. sygn. akt 23/11*, „Orzecznictwo Trybunału Konstytucyjnego. Zbiór Urzędowy” 2005, nr 11A, poz. 132 (dalej: OTK ZU); Dz.U. nr 250 poz. 2116.

jawności, pozostaje w naturalnym, nieusuwalnym konflikcie z niektórymi prawami zasadniczymi jednostki. W szczególności dotyczy to prawa jednostki do prywatności, konstytucyjnej wolności komunikowania się i związanej z tym ochrony tajemnicy komunikowania się, ochrony autonomii informacyjnej (którą w Polsce określają art. 49 i 51 Konstytucji), a także z konstytucyjną gwarancją sądowej ochrony praw jednostki. Konflikt ten występuje powszechnie, jest znany we wszystkich demokratycznych państwach prawnych, a także na tle praktyki organów międzynarodowych, gdzie – na tle art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (...) wypracowano uniwersalne standardy, służące ocenie proporcjonalności między ingerencją władzy a prawami jednostki w rozważanej sferze (...). W państwach demokratycznych, nawet tych, które wprowadzają ograniczenia konstytucyjnych wolności jednostki, ze względu na potrzeby walki z przestępczością i terroryzmem, ustawodawstwo powszechne, regulujące czynności operacyjno-wykrywcze, ma zakotwiczenie konstytucyjne.

Odnosnie do prowadzenia przez organy władzy publicznej czynności operacyjno-rozpoznawczych wielokrotnie wypowiadał się Trybunał Konstytucyjny. Między innymi w wyroku z 30 lipca 2014 r., sygn. akt K 23/11²⁴, podniósł, że

(...) Europejski Trybunał Praw Człowieka nie zanegował dopuszczalności niejawnego pozyskiwania informacji o osobach przez władze publiczne. Wskazywał wręcz na ich niezbędność, jako narzędzia umożliwiającego efektywne zagwarantowanie bezpieczeństwa oraz ochronę instytucji demokratycznego państwa przed wyrafinowanymi formami zagrożeń, zwłaszcza szpiegostwem czy terroryzmem (zob. m.in. wyrok ETPCz z 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*, pkt 48 uzasadnienia)²⁵.

W uzasadnieniu zważył również m.in.:

W dotychczasowym orzecznictwie Trybunał Konstytucyjny kilkakrotnie wypowiadał się w sprawie konstytucyjności przepisów regulujących czynności operacyjno-rozpoznawcze prowadzące do ingerencji w sferę prywatności jednostki i tajemnicę komunikowania się (...). Trybunał Konstytucyjny nie podważył dopuszczalności ich stosowania w demokratycznym państwie prawa. Przeciwnie, wyraźnie podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o obywatelach w toku kontroli operacyjnej ukierunkowanej na zapobieganie przestępstwom, ich wykrywanie oraz zwalczanie, jest nieodzowne. Jawność tych czynności powodowałaby bowiem ich nieskuteczność, a to z kolei rzutowało by na poziom bezpieczeństwa państwa i jego obywateli (...). Ocena ta wynikała z dostrzeżenia specyfiki działalności

²⁴ Wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r. w sprawie sygn. akt K 23/11.

²⁵ Orzeczenie ETPCz z dnia 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*, skarga nr 5029/71.

przestępczej i coraz trudniejszych warunków zapewniania bezpieczeństwa spowodowanych zagrożeniem terroryzmem, zorganizowaną przestępczością, czy wykorzystaniem przez przestępców nowych technologii w celu komunikowania się między sobą i popełniania rozmaitych przestępstw specjalistycznych.

Trybunał Konstytucyjny w wyroku z 13 grudnia 2001 r. sygn. akt K 19/99²⁶ podniósł:

Jedną z ważnych funkcji demokratycznego państwa prawa jest skuteczne zwalczanie tych negatywnych zjawisk, które w skrajnym nasileniu mogą godzić w samo istnienie tego państwa. Dlatego ustawodawca ma – zdaniem Trybunału – nie tylko prawo, ale także obowiązek zwalczania tych negatywnych zjawisk poprzez nadawanie takich uprawnień organom (...) które to uprawnienia, pozostając w zgodzie z zasadami konstytucji, będą miały bezpośredni wpływ na zwiększenie sprawności działań (...) zwłaszcza w zakresie wykrywania i zwalczania (...) przestępczości.

Czynności operacyjno-rozpoznawcze są tą domeną działania służb specjalnych, podczas realizacji których dochodzi do ingerencji w prawa i wolności człowieka. Choć ustawodawca zabezpiecza prawa każdego człowieka, to jednak skuteczna walka z terroryzmem, w tym również w cyberprzestrzeni, z przestępczością zorganizowaną (przeważnie o zasięgu światowym), jak: handel ludźmi, nielegalny handel bronią, przemyt narkotyków, pranie brudnych pieniędzy pochodzących z działalności przestępczej, przestępcza działalność w cyberprzestrzeni, przestępstwa korupcyjne, gospodarcze zagrażające stabilności finansowej państwa – musi odbić się na ograniczaniu praw i wolności obywatela.

Kontrola operacyjna

Kontrola operacyjna jako jedna z ofensywnych metod pracy operacyjnej²⁷ jest realizowana przez stosowanie czynności operacyjno-rozpoznawczych służb specjalnych. Jest ona prowadzona w sposób niejawny i polega na uzyskiwaniu i utrwalaniu treści rozmów przy użyciu środków technicznych, w tym sieci telekomunikacyjnych; uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób znajdujących się w pomieszczeniach, środkach transportu lub w miejscach innych niż miejsca publiczne; uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych telekomunikacyjnych, urządzeniach końcowych, systemach informatycznych i teleinformatycznych; uzyskiwaniu dostępu do za-

²⁶ *Wyrok TK z dnia 13 grudnia 2001 r. sygn. akt K 19/99*, (OTK ZU 2001, nr 2, poz. 30; Dz.U. z 2001 r. nr 14 poz. 143).

²⁷ M. Chrabkowski, *Wykorzystanie metod pracy operacyjnej w czynnościach sprawdzających (uwagi do artykułu K. Chalubek)*, „Prokuratura i Prawo” 2013, nr 7–8, s. 195.

wartości przesyłek oraz ich kontroli²⁸. Agencja Bezpieczeństwa Wewnętrznego i Centralne Biuro Antykorupcyjne mogą prowadzić kontrolę operacyjną przy wykonywaniu czynności operacyjno-rozpoznawczych dokonywanych przez te służby w celu rozpoznawania przestępstw, zapobiegania im oraz ich wykrywania, a także uzyskiwania i utrwalania dowodów przestępstw i ścigania ich sprawców – gdy inne środki okazały się bezskuteczne albo będą nieprzydatne. W przypadku ABW kontrola operacyjna²⁹ dotyczy przestępstw, o których mowa w art. 5 ust. 1 pkt 2 lit. a, c, d, e, oraz w rozdziałach XXXV–XXXVII kodeksu karnego i rozdziałach 6 oraz 7 Kodeksu karnego skarbowego, jeżeli godzą w podstawy ekonomiczne państwa. Ustawodawca jednoznacznie określił katalog przestępstw, wobec których CBA może stosować kontrolę operacyjną³⁰. Są one wymienione w art. 228–231, art. 250a, art. 258, art. 286, art. 296–297, art. 299, art. 305, art. 310 § 1, 2 i 4 kk oraz przestępstw skarbowych, o których mowa w art. 2 ust. 1 pkt 1 lit. d kks, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę, określonego na podstawie przepisów *Ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę* (t.j.: Dz.U. z 2017 r. poz. 847 – przyp. red.). Natomiast w przypadku SKW kontrola operacyjna może być prowadzona przy wykonywaniu czynności operacyjno-rozpoznawczych w celu realizacji zadań określonych w art. 5 ust. 1 pkt 1, 5, 7 i 8 oraz ust. 2 ustawy o SKW oraz SWW, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne³¹. Świadczy to o tym, że SKW jest upoważniona do korzystania ze stosowania kontroli operacyjnej nie tylko w celu (...) *rozpoznawania, zapobiegania oraz wykrywania (...) przestępstw*, ale również, gdy realizuje czynności skupiające się na uzyskiwaniu informacji w zakresie prowadzenia kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony (...) *kryptograficznej i kryptoanalizy; ochrony (...) bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa; ochrony (...) bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez SZ RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez SZ RP i inne jednostki organizacyjne MON*³². Nie jest konieczne, aby informacje w tych obszarach wskazywały na okoliczności związane z działaniami przestępczymi. Służba Kontrwywiadu Wojskowego jest służbą o charakterze kontrwywiadowczym, której działania są skierowane na przeciwdziałanie zagrożeniom niekoniecznie związanym ze zjawiskiem przestępczości³³. Kontrolę operacyjną w przypadku ABW i CBA może, w drodze postanowienia, zarządzić Sąd Okręgo-

²⁸ Art. 27 ust. 6 ustawy o ABW oraz AW, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW oraz SWW.

²⁹ Art. 27 ust. 1 pkt 1 i 2 ustawy o ABW oraz AW.

³⁰ Art. 17 ust. 1 pkt 1 i 2 ustawy o CBA.

³¹ Art. 31 ust. 1 ustawy o SKW oraz SWW.

³² Art. 5 ust. 1 pkt 1, 5, 7 i 8 ustawy o SKW oraz SWW.

³³ M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 31.

wy w Warszawie, na pisemny wniosek szefa tej służby złożony po uzyskaniu pisemnej zgody prokuratora generalnego³⁴. Zgodnie z art. 31 ust. 1 i 2 ustawy o SKW oraz SWW Wojskowy Sąd Okręgowy w Warszawie może, w drodze postanowienia, zarządzić kontrolę operacyjną na pisemny wniosek szefa SKW, złożony po uzyskaniu pisemnej zgody prokuratora generalnego. Wniosek, o którym mowa, przedstawia się wraz z materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej³⁵. Powinien on zawierać przede wszystkim numer sprawy i jej kryptonim, jeżeli został jej nadany; opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej; okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków; dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie stosowana kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania, a także cel, czas i rodzaj prowadzonej kontroli operacyjnej³⁶. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, szef ABW, CBA lub SKW może zarządzić, po uzyskaniu pisemnej zgody prokuratora generalnego, kontrolę operacyjną, zwracając się jednocześnie do sądu, według właściwości jak wyżej, z wnioskiem o wydanie postanowienia w tej sprawie. Sąd wydaje postanowienie w przedmiocie wniosku w terminie pięciu dni. W przypadku nieudzielenia przez sąd zgody, szef ABW, CBA lub SKW wstrzymuje kontrolę operacyjną oraz poleca niezwłoczne, protokolarne, komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania³⁷. Kontrolę operacyjną zarządza się na okres nie dłuższy niż trzy miesiące. Jeżeli nie ustały przyczyny zarządzenia tej kontroli, sąd może, na pisemny wniosek szefa ABW, CBA lub SKW złożony po uzyskaniu pisemnej zgody prokuratora generalnego, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej na okres nie dłuższy niż kolejne trzy miesiące³⁸. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawiają się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, na pisemny wniosek szefa ABW, CBA lub SKW złożony po uzyskaniu pisemnej zgody prokuratora generalnego, może wydać – również po upływie okresów, o których mowa wyżej – kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy³⁹. Do wniosków, w przypadkach niecierpiących zwłoki lub kolejnego przedłużenia

³⁴ Art. 27 ust. 1 i 2 ustawy o ABW oraz AW, art. 17 ust. 1 i 2 ustawy o CBA.

³⁵ Art. 27 ust. 1a ustawy o ABW oraz AW, art. 17 ust. 1a ustawy o CBA, art. 31 ust. 1a ustawy o SKW oraz SWW.

³⁶ Art. 27 ust. 7 ustawy o ABW oraz AW, art. 17 ust. 7 ustawy o CBA, art. 31 ust. 5 ustawy o SKW oraz SWW.

³⁷ Art. 27 ust. 3 ustawy o ABW oraz AW, art. 17 ust. 3 ustawy o CBA, art. 31 ust. 3 ustawy o SKW oraz SWW.

³⁸ Art. 27 ust. 8 ustawy o ABW oraz AW, art. 17 ust. 8 ustawy o CBA, art. 31 ust. 6 ustawy o SKW oraz SWW.

³⁹ Art. 27 ust. 9 ustawy o ABW oraz AW, art. 17 ust. 9 ustawy o CBA, art. 31 ust. 7 ustawy o SKW oraz SWW.

kontroli operacyjnej, o których mowa w art. 27 ust. 3, 8 i 9 ustawy o ABW oraz AW, art. 17 ust. 3, 8 i 9 ustawy o CBA, art. 31 ust. 3, 6 i 7 ustawy o SKW oraz SWW, stosuje się odpowiednio również przepisy dotyczące ich zawartości – art. 27 ust. 1a i 7 ustawy o ABW oraz AW, art. 17 ust. 1a i 7 ustawy o CBA oraz art. 31 ust. 1a i 5 ustawy o SKW oraz SWW. Natomiast sąd przed wydaniem postanowienia w sprawie zapoznaje się z materiałami uzasadniającymi wnioszek, szczególnie zgromadzonymi podczas stosowania kontroli operacyjnej zarządzanej w tej sprawie⁴⁰. Na postanowienie sądu w przedmiocie wydania postanowienia o zarządzeniu kontroli operacyjnej, o którym mowa w art. 27 ust. 1, 3, 8 i 9 ustawy o ABW oraz AW, zażalenie przysługuje szefowi ABW; na podstawie art. 17 ust. 1, 3, 8 i 9 ustawy o CBA – zażalenie przysługuje szefowi CBA; na podstawie art. 31 ust. 1, 3, 6 i 7 ustawy o SKW oraz SWW – zażalenie przysługuje szefowi SKW, natomiast prokuratorowi generalnemu przysługuje zażalenie na postanowienia, o których mowa w art. 27 ust. 3 i ustawy o ABW oraz AW, art. 17 ust. 3 i ustawy o CBA oraz art. 31 ust. 3 i ustawy o SKW oraz SWW. Do zażalenia stosuje się odpowiednio przepisy *Ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego*⁴¹ (t.j.: Dz.U. z 2017 r. poz. 1904 – przyp. red.).

Zakończenie kontroli operacyjnej powinno nastąpić niezwłocznie po ustaniu przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona⁴². Szef ABW, CBA lub SKW informuje prokuratora generalnego o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie – również o przebiegu tej kontroli, przedstawiając zebrane w jej toku materiały⁴³. W przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego szef ABW, CBA lub SKW przekazuje prokuratorowi generalnemu wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej⁴⁴.

Służby specjalne są uprawnione do stosowania kontroli operacyjnej również przy dokonywaniu zakupu kontrolowanego i kontrolowanego wręczenia lub przyjęcia korzyści majątkowej, a także – w przypadku ABW i SKW – przy realizacji przesyłki niejawnie nadzorowanej⁴⁵.

W ustawie antyterrorystycznej⁴⁶ szefowi ABW ustawodawca nadał szczególne

⁴⁰ Art. 27 ust. 10 ustawy o ABW oraz AW, art. 17 ust. 10 ustawy o CBA, art. 31 ust. 8 ustawy o SKW oraz SWW.

⁴¹ Art. 27 ust. 11a ustawy o ABW oraz AW, art. 17 ust. 17 ustawy o CBA, art. 31 ust. 10 ustawy o SKW oraz SWW.

⁴² Art. 27 ust. 13 ustawy o ABW oraz AW, art. 17 ust. 13 ustawy o CBA, art. 31 ust. 12 ustawy o SKW oraz SWW.

⁴³ Art. 27 ust. 14 ustawy o ABW oraz AW, art. 17 ust. 14 ustawy o CBA, art. 31 ust. 13 ustawy o SKW oraz SWW.

⁴⁴ Art. 27 ust. 15 ustawy o ABW oraz AW, art. 17 ust. 15 ustawy o CBA, art. 31 ust. 14 ustawy o SKW oraz SWW.

⁴⁵ Art. 31 ustawy o ABW oraz AW, art. 20 ustawy o CBA, art. 36 ustawy o SKW oraz SWW.

⁴⁶ *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. poz. 904, ze zm. – przyp. red.). Tekst ustawy został przekazany do senatu zgodnie z art. 52 regulaminu sejmu. Ustawę uchwalono 10 czerwca 2016 r. na posiedzeniu sejmu nr 20. Senat przyjął ustawę bez poprawek 13 czerwca 2016 r. W dniu 14 czerwca 2016 r. ustawę przekazano Prezydentowi RP, który podpisał

uprawnienia w zakresie kontroli operacyjnej. Zgodnie z art. 9 ust. 1 przywołanej ustawy, w celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym szef ABW może zarządzić niejawnie prowadzenie czynności wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, na okres nie dłuższy niż trzy miesiące. Czynności te polegają na:

- uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych,
- uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne,
- uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej,
- uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych,
- uzyskiwaniu dostępu i kontroli zawartości przesyłek.

Kontrola operacyjna jest tą metodą pracy operacyjno-rozpoznawczej, która w sposób szczególny głęboko ingeruje w prywatność osoby, niejednokrotnie dotykając, a nawet naruszając sferę życia intymnego. Stosowanie różnego rodzaju współczesnych technik w zakresie kontroli operacyjnej naraża szeroką grupę, niejednokrotnie niewinnych osób, na wnikanie w ich prywatność i wolność, szczególnie gdy te czynności są prowadzone w miejscach, do których dostęp jest praktycznie nieograniczony. Takim przykładem może być stosowanie kontroli operacyjnej w gabinecie lekarskim.

Uzyskiwanie danych telekomunikacyjnych, pocztowych lub internetowych

Służby specjalne mogą uzyskiwać dane niestanowiące treści odpowiednio: przekazu telekomunikacyjnego⁴⁷, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w art. 180c (np. dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego inicjującego połączenie, do którego jest kierowane połączenie; określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego)⁴⁸, niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1

ją 22 czerwca 2016 r.

⁴⁷ Za przekaz telekomunikacyjny rozumie się „(...) treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych” – art. 2 pkt 27a *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (Dz.U. z 2017 r. poz. 1907 – przyp. red.).

⁴⁸ Zgodnie z art. 180c.:

„1. Obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie;

2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego.

ustawy o ABW oraz AW, art. 2 ustawy o CBA oraz art. 5 ustawy o SKW oraz SWW, i art. 180d *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (dalej: ustawa p.t.), dotyczącym obowiązków przedsiębiorcy telekomunikacyjnego⁴⁹, zwane „dany-

2. Minister właściwy do spraw łączności w porozumieniu z ministrem właściwym do spraw wewnętrznych, mając na uwadze rodzaj wykonywanej działalności telekomunikacyjnej przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych, dane określone w ust. 1, koszty pozyskania i utrzymania danych oraz potrzebę unikania wielokrotnego zatrzymywania i przechowywania tych samych danych, określi w drodze rozporządzenia: 1) szczegółowy wykaz danych, o których mowa w ust. 1; 2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych”.

W art. 180a zawarto, że:

„1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:

1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;

2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także Służbie Celnej, sądowni i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych;

3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159–175a, art. 175c i art. 180e (...)”

⁴⁹ Zgodnie z art. 180d: „Przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także Służbie Celnej, sądowni i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3–5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych”.

Zgodnie z art. 159:

„1. Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej „tajemnicą telekomunikacyjną”, obejmuje:

1) dane dotyczące użytkownika; (...)

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; (...)

5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń (...)”

W art. 161. zawarto, że:

„1. Z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem”, dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.

2. Dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną:

1) nazwisk i imion;

mi telekomunikacyjnymi”); art. 82 ust. *Ustawy z 23 listopada 2012 r. – Prawo pocztowe* (t.j.: Dz.U. z 2017 r. poz. 1481 – przyp. red.), zwane „danymi pocztowymi”⁵⁰; art. 18 ust. 1–5 *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (t.j.: Dz.U. z 2017 r. poz. 1219), zwane „danymi internetowymi”⁵¹, które mogą prze-

-
- 2) imion rodziców;
 - 3) miejsca i daty urodzenia;
 - 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania;
 - 5) numeru ewidencyjnego PESEL – w przypadku obywatela Rzeczypospolitej Polskiej;
 - 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu;
 - 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

3. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych”.

Według art. 179. ust. 9. „Przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy”.

⁵⁰ W art. 82. ust. 1. zawarto m.in. że: ”Operator pocztowy, począwszy od dnia rozpoczęcia działalności pocztowej, jest obowiązany do nieodpłatnego zapewnienia, w ramach wykonywanej przez siebie działalności pocztowej, technicznych i organizacyjnych możliwości wykonywania przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy, zwane dalej „uprawnionymi podmiotami”, oraz prokuraturę i sądy, ich zadań określonych odrębnymi przepisami, wymagających: 1) uzyskania danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług (...)”

⁵¹ Według art. 18: „1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:

- 1) nazwisko i imiona usługobiorcy;
- 2) numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość;
- 3) adres zameldowania na pobyt stały;
- 4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3;
- 5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
- 6) adresy elektroniczne usługobiorcy.

2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.

3. Usługodawca wyróżnia i oznacza te spośród danych, o których mowa w ust. 2, jako dane, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną zgodnie z art. 22 ust. 1.

4. Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów określonych w art. 19 ust. 2 pkt 2, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną.

5. Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):

- 1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa

tworząc bez wiedzy i zgody osoby, której dotyczy⁵². Powyższe dane przedsiębiorca telekomunikacyjny⁵³, operator pocztowy⁵⁴ lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie odpowiednio funkcjonariuszom ABW, CBA lub SKW⁵⁵. Szef właściwej służby prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierających informacje identyfikujące jednostkę organizacyjną i funkcjonariusza służby specjalnej uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr jest prowadzony w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych⁵⁶.

Również w celu realizacji zadań, o których mowa odpowiednio w art. 5 ust. 1 ustawy o ABW oraz AW, art. 2 ustawy o CBA, a także art. 5 ustawy o SKW oraz SWW służby mogą uzyskiwać i przetwarzać bez wiedzy i zgody osoby, której dotyczą, dane z wykazu, o którym mowa w art. 179 ust. 9 ustawy p.t.; dane, o których mowa w art. 161 ustawy p.t.; w przypadku użytkownika, który nie jest osobą fizyczną, numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i firmę organizacyjną tego użytkownika; w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci udostępnione użytkownikowi. Do udostępniania i przetwarzania powyższych danych stosuje się odpowiednio art. 28 ust. 2–7 ustawy o ABW oraz AW, art. 18 ust. 2–7 ustawy o CBA, art. 32 ust. 2–9 ustawy o SKW oraz SWW⁵⁷.

W przypadku uzyskiwania danych telekomunikacyjnych, pocztowych lub internetowych obywatel ma do czynienia z inwigilacją w pełnym tego słowa znaczeniu.

w ust. 1;

2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;

3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;

4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną⁷⁷.

⁵² Art. 28 ust. 1 ustawy ABW oraz AW, art. 18 ust. 1 ustawy o CBA, art. 32 ust. 1 ustawy o SKW oraz SWW.

⁵³ Przedsiębiorca telekomunikacyjny to przedsiębiorca „(...) lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, który wykonuje działalność gospodarczą polegającą na dostarczaniu sieci telekomunikacyjnych, świadczeniu usług towarzyszących lub świadczeniu usług telekomunikacyjnych, przy czym przedsiębiorca telekomunikacyjny, uprawniony do: a) świadczenia usług telekomunikacyjnych, zwany jest „dostawcą usług”, b) dostarczania publicznych sieci telekomunikacyjnych lub świadczenia usług towarzyszących, zwany jest „operatorem” – art. 2 pkt 27 ustawy Prawo telekomunikacyjne.

⁵⁴ Operator pocztowy to przedsiębiorca uprawniony do wykonywania działalności pocztowej, na podstawie wpisu do rejestru operatorów pocztowych – art. 3 pkt 12 *Ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe*.

⁵⁵ Art. 28 ust. 2 ustawy o ABW oraz AW, art. 18 ust. 2 ustawy o CBA, art. 32 ust. 2 ustawy o SKW oraz SWW.

⁵⁶ Art. 28 ust. 5 ustawy o ABW oraz AW, art. 18 ust. 5 ustawy o CBA, art. 32 ust. 7 ustawy o SKW oraz SWW.

⁵⁷ Art. 28b ust. 2 ustawy o ABW oraz AW, art. 18b ust. 2 ustawy o CBA, art. 32b ust. 2 ustawy o SKW oraz SWW.

Uzyskiwane są jego numery telefonów, e-maile, dostęp do forów, komunikatorów, śledzone są połączenia, miejsca ich realizacji, godziny itp. Obecnie wydaje się, że nie ma takiej możliwości komunikowania się bądź nawiązywania łączności, aby nie pozostawić śladu nawet próby takiego działania.

Zakup kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści majątkowej

Instytucja zakupu kontrolowanego jako jedna z metod pracy operacyjnej stosowana przez służby specjalne została zdefiniowana w ustawach kompetencyjnych. Wyróżnia się dwie odmiany: zakup kontrolowany (*sensu stricto*) oraz kontrolowane przyjęcie lub wręczenie korzyści majątkowej (tzw. kontrolowana łapówka). Obie te kategorie są określane również jako *transakcje pozorne*⁵⁸. Funkcjonariusze CBA mogą realizować czynności zakupu kontrolowanego polegające m.in. na złożeniu propozycji nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, a także złożeniu propozycji przyjęcia lub wręczenia korzyści majątkowej⁵⁹. Czynności związane z realizacją przez funkcjonariuszy służb specjalnych zakupu kontrolowanego lub kontrolowanej łapówki nie mogą polegać na kierowaniu działaniami wyczerpującymi znamiona czynu zabronionego pod groźbą kary⁶⁰. W art. 33 ust. 1 ustawy o SKW oraz SWW jest mowa o (...) *uzyskaniu wiarygodnych informacji o popełnieniu przestępstwa, oraz dodatkowo o zbyciu, a nie tylko nabyciu lub przejęciu przedmiotów*. Zakup kontrolowany zarządza, na czas określony, szef ABW, CBA lub SKW – po uzyskaniu pisemnej zgody prokuratora generalnego, którego na bieżąco informuje się o przebiegu tych czynności i ich wyniku⁶¹. Prokurator generalny przed wydaniem pisemnej zgody zapoznaje się z materiałami uzasadniającymi potrzebę przeprowadzenia zakupu kontrolowanego⁶². W przypadku potwierdzenia informacji o przestępstwie wskazanych w ustawach kompetencyjnych szef ABW, CBA lub SKW przekazuje prokuratorowi generalnemu wszystkie materiały zgromadzone w wyniku wykonywanych czynności⁶³.

W przypadku tego rodzaju działań operacyjnych jesteśmy narażeni na niezgodne z prawem zachowania ze strony służb specjalnych podczas stosowania niedozwolonej formy prowokacji, jaką jest namawianie wprost przez funkcjonariusza pod przykryciem do dokonania przestępstwa, a nawet kierowania takim działaniem. Niezmiernie ważne jest, aby służby, stosując tę metodę pracy operacyjnej, zachowały wszelkie zasady praworządności i kodeksu etyki. Muszą też pamiętać, że bez operacyjnych podstaw do

⁵⁸ M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 37–38.

⁵⁹ Art. 19 ust. 3 ustawy o CBA.

⁶⁰ Art. 29 ust. 3 ustawy o ABW oraz AW, art. 19 ust. 4 ustawy o CBA, art. 33 ust. 3 ustawy o SKW oraz SWW.

⁶¹ Art. 29 ust. 2 ustawy o ABW oraz AW, art. 19 ust. 2 ustawy o CBA, art. 33 ust. 2 ustawy o SKW oraz SWW.

⁶² Art. 29 ust. 2a ustawy o ABW oraz AW, art. 19 ust. 2a ustawy o CBA, art. 33 ust. 2a ustawy o SKW oraz SWW.

⁶³ Art. 29 ust. 4 ustawy o ABW oraz AW, art. 19 ust. 5 ustawy o CBA, art. 33 ust. 4 ustawy o SKW oraz SWW.

stosowania tej metody pracy, jakimi są „wiarygodne informacje o przestępstwie”, nie mogą tych „dział” wytaczać przeciwko jednostce.

Przesyłka niejawnie nadzorowana

Wykorzystanie przesyłki niejawnie nadzorowanej jest kolejnym uprawnieniem operacyjnym przyznanym służbom specjalnym w celu zwalczania przestępstw. Ustawa o CBA nie przyznaje tej służbie takiego uprawnienia⁶⁴. Przesyłka niejawnie nadzorowana może być wykorzystana w sprawach o przestępstwa, o których mowa w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW, a także w art. 5 ust. 1 pkt 1 ustawy o SKW oraz SWW w ramach czynności operacyjno-rozpoznawczych zmierzających do udokumentowania tych przestępstw albo ustalenia tożsamości osób uczestniczących w tych przestępstwach lub przyjęcia przedmiotów przestępstwa. Te czynności polegają na niejawnym nadzorowaniu wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia życia lub zdrowia ludzkiego. Zarządzenie wykorzystania przesyłki niejawnie nadzorowanej jeszcze przed wszczęciem postępowania karnego może wydać szef ABW lub szef SKW. Szef właściwej służby specjalnej ma obowiązek niezwłocznego zawiadomienia prokuratora generalnego o wydaniu zarządzenia, przebiegu i wynikach czynności. Prokurator generalny może nakazać zaniechanie tych czynności. W związku z realizacją działań, o których mowa, urzędy, instytucje i podmioty prowadzące działalność pocztową i transportową, organy celne oraz organy Straży Granicznej są (...) *obowiązane dopuścić do dalszego przewozu przesyłki zawierające przedmioty przestępstwa w stanie nienaruszonym lub po ich usunięciu albo zastąpieniu lub w części*. W przypadku potwierdzenia informacji o przestępstwie szef danej służby specjalnej przekazuje prokuratorowi generalnemu wszystkie materiały zgromadzone w wyniku wykonywania czynności⁶⁵.

Służby specjalne uprawnione do stosowania przesyłki niejawnie nadzorowanej, w sposób niejawny czasowo wyłączać przesyłki lub inne przedmioty z obrotu albo z procesu ich wytwarzania. Przysługuje również tym służbom prawo otwierania przesyłek w celu sprawdzenia i oceny ich zawartości, usunięcia przedmiotów przestępstwa albo zamiany na inne przedmioty w całości lub w części, ich oznakowania, a także w celu ujawnienia i zabezpieczenia ewentualnych śladów kryminalistycznych. Funkcjonariusze służb specjalnych mogą również zamykać przesyłki i inne przedmioty po otwarciu oraz włączyć je do dalszego obrotu lub procesu wytwarzania⁶⁶. Sprawdzenia i oceny zawartości przesyłek oraz innych rzeczy dokonuje się

⁶⁴ M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 41.

⁶⁵ Art. 30 ustawy o ABW oraz AW, art. 34 ustawy o SKW oraz SWW.

⁶⁶ M. Bożek, *Charakterystyka ustawowych uprawnień...*, s. 41. Zob. § 2 ust. 2 pkt 1–2 *Rozporządzenia Prezesa Rady Ministrów z dnia 7 października 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Agencję Bezpieczeństwa Wewnętrznego niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa* (Dz.U. z 2014 r. poz. 1772).

metodą organoleptyczną lub – w razie potrzeby – pobiera próbki do badań właściwości fizykochemicznych lub innych cech identyfikacyjnych, istotnych z uwagi na okoliczności przeprowadzenia czynności, a także w celu upewnienia się, że prowadzenie czynności nie stworzy zagrożenia życia i zdrowia ludzkiego. Wykorzystując przesyłkę niejawnie nadzorowaną, funkcjonariusze w celu ochrony niejawności form i metod ich przeprowadzania mogą posługiwać się dokumentami uniemożliwiającymi ich identyfikację lub identyfikację osoby udzielającej im pomocy, a także środków, którymi się posługują⁶⁷.

Również ta forma działalności służb specjalnych, należąca do ofensywnych metod pracy operacyjnej, naraża obywateli na ingerencje w prawo do prywatności, narusza ich wolność korespondencji, intymność informacji, np. o miejscu pobytu, kontaktach. Również osoby niemające nic wspólnego z przestępczością mogą być narażone na ingerencję służb np. w przypadku skierowania przesyłki z narkotykami przez handlarza na adres sąsiada.

Uzyskiwanie i gromadzenie informacji

Wyróżnikiem działalności służb specjalnych jest uzyskiwanie oraz ochrona informacji mających kluczowe znaczenie dla zagwarantowania zarówno wewnętrznego, jak i zewnętrznego bezpieczeństwa państwa⁶⁸. W ustawach kompetencyjnych służby specjalne, każda w zakresie swojej właściwości, zostały upoważnione do uzyskiwania, gromadzenia, sprawdzania i przetwarzania informacji, w tym także o charakterze niejawnym⁶⁹.

Zgodnie z normami zawartymi w art. 34 ust. 1 ustawy o ABW oraz AW i art. 38 ust. 1 ustawy o SKW oraz SWW te służby – w zakresie swojej właściwości – mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 27 i 28 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (t.j.: Dz.U. z 2016 r. poz. 922 – przyp. red.), m.in. ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Mogą również korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je, w rozumieniu ustawy o ochronie danych

⁶⁷ Paragraf 2 ust. 4, § 7 ust. 2 rozporządzenie PRM w sprawie sposobu przeprowadzania i dokumentowania przez Agencję Bezpieczeństwa Wewnętrznego niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa.

⁶⁸ K. Haftarczyk, *Służby specjalne jako element bezpieczeństwa narodowego*, „Zeszyty naukowe SOWL” 2011, nr 3, s. 197.

⁶⁹ Art. 33 ustawy o ABW oraz AW, art. 22 ustawy o CBA, art. 37 ust. 4 ustawy o SKW oraz SWW.

osobowych, bez wiedzy i zgody osoby której one dotyczą⁷⁰. Centralne Biuro Antykorupcyjne – w granicach zadań wskazanych w art. 2 ust. 1 ustawy o CBA – może przetwarzać dane osobowe, w tym dane wskazane w art. 27 ust. 1 ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której te dane dotyczą⁷¹. Przetwarzanie danych osobowych⁷² przez CBA trwa przez okres, w którym są one niezbędne do realizacji jego ustawowych zadań. Nie rzadziej niż co pięć lat ta służba dokonuje weryfikacji potrzeby dalszego przetwarzania tych danych, usuwając dane zbędne⁷³. W przypadku CBA dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową partyjną lub związkową oraz dane o stanie zdrowia, nałogach lub życiu seksualnym osób podejrzanych o popełnienie przestępstw, które nie zostały skazane za te przestępstwa, podlegają komisijnemu i protokolarnemu zniszczeniu niezwłocznie po uprawomocnieniu się stosownego orzeczenia – art. 22a ust. 10 ustawy o CBA. Ustawodawca zezwala na tworzenie zbioru danych osobowych szefowi CBA – art. 22a ust. 11 ustawy o CBA. Zdaniem T. Miłkowskiego: *Prawo do informacji nie może być jednak zbyt kazuistyczne i powinno uwzględniać różne poziomy dostępu w zależności od tego, czy powodem ich zbierania jest ochrona porządku konstytucyjnego, ściganie sprawców przestępstwa lub (...) wykroczenia, czy też realizacja obowiązków administracyjnych*⁷⁴.

W przypadku gromadzenia danych osobowych przez służby specjalne obywatel może być narażony na nielegalne rozpowszechnienie, przekazanie – „wyciek” – swoich danych (mogą to być nawet dane wrażliwe), a co za tym idzie – na naruszenie prywatności i prawa nieinformowania o osobie.

Dokumenty legalizacyjne

Niejednokrotnie czynności realizowane przez służby specjalne wymagają zachowania ich w tajemnicy. Przykładem jest prowadzenie działań pod przykryciem, gdzie nieodzownym elementem pracy operacyjnej jest posługiwanie się dokumentami legalizacyjnymi⁷⁵. Te dokumenty zawierają nieprawdziwe dane osób, które się nimi

⁷⁰ Art. 34 ust. 1 ustawy o ABW oraz AW, art. 38 ust. 4 ustawy o SKW oraz SWW.

⁷¹ Art. 22a ust. 1 ustawy o CBA.

⁷² Zgodnie z art. 7 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest to „(...) jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych”.

⁷³ Art. 22a ust. 8 ustawy o CBA.

⁷⁴ T. Miłkowski, *Czy ABW powinna korzystać ze „specjalnego” prawa do informacji?*, „Przeгляд Bezpieczeństwa Wewnętrznego” 2014, nr 10, s. 211.

⁷⁵ Tego typu działania „(...) wykonują funkcjonariusze pod przykryciem, będący kadrowymi funkcjonariuszami danej służby, przeszkolonymi do wykonywania zadań opartych na stosowanej legendzie określane również mianem przykrywkowców lub operatorów”, zob. R. Lizak, *Dokumenty legalizacyjne w służbach specjalnych*, „Prokuratura i Prawo” 2013, nr 2, s. 142–143. Natomiast legenda „(...) to fikcyjne lub częściowo fikcyjne wytłumaczenie jakiegoś faktu czy zjawiska opracowane w celu ukrycia przed osobami trzecimi prawdziwej wersji wydarzeń lub rzeczywistych

posługują, nadając tym osobom fałszywą tożsamość. Ta forma realizacji czynności operacyjno-rozpoznawczych, szczególnie tych ofensywnych, jest konieczna i jednocześnie najbardziej efektywna⁷⁶.

Służby specjalne w związku z wykonywaniem swoich zadań zapewniają ochronę środków, form i metod realizacji zadań, ochronę zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy tych służb. Funkcjonariusze służb specjalnych podczas wykonywania czynności operacyjno-rozpoznawczych mogą posługiwać się dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi posługuje się przy wykonywaniu zadań. Takimi dokumentami mogą posługiwać się osoby udzielające służbom specjalnym pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych. Służba Wywiadu Wojskowego, na potrzeby uprawnionych organów, służb i instytucji państwowych, sporządza i wydaje dokumenty wojskowe oraz dokumenty SKW i SWW uniemożliwiające ustalenie danych identyfikujących żołnierzy, funkcjonariuszy albo pracowników tych organów, służb i instytucji, a także osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych. Prowadzi również rejestr tych dokumentów. Sporządzanie i wydanie dokumentów na potrzeby organów, służb i instytucji innych niż SWW następuje na ich wniosek. Uprawnione organy, służby i instytucje państwowe, na pisemny wniosek szefa SKW lub SWW, wydają dokumenty i znaki identyfikujące osobom posługującym się nimi jako funkcjonariusze lub pracownicy tych organów, służb lub instytucji państwowych⁷⁷. Zgodnie z art. 35 ust. 4 ustawy o ABW oraz AW, z zastrzeżeniem ust. 5, (...) *na wniosek upoważnionych organów, służb i instytucji państwowych, ABW sporządza i wydaje dokumenty uniemożliwiające ustalenie danych identyfikujących funkcjonariuszy i pracowników tych organów, służb lub instytucji oraz osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych, a także prowadzi centralny rejestr tych dokumentów*. Art. 35 ust. 5 stanowi, że dokumenty i znaki identyfikujące osoby posługujące się nimi jako funkcjonariuszy lub pracowników organów, służb lub instytucji państwowych, o których mowa w ust. 4, wydają odpowiednio te organy, służby lub instytucje. W ustawach kompetencyjnych zawarto zapis, że nie popełnia przestępstwa ten, kto poleca sporządzenie lub kieruje sporządzeniem dokumentów legalizacyjnych, sporządza taki dokument, udziela pomocy w sporządzeniu takich dokumentów, a także funkcjonariusz służb specjalnych lub osoba udzielająca pomocy posługująca się takimi dokumentami przy wykonywaniu czynności operacyjno-rozpoznawczych⁷⁸.

intencji”, zob. V.V. Severski, M. Plebanek, *Kontrwywiadowcze zadania polskich służb specjalnych po 1990 roku*, <http://vincentvseverski.tumblr.com/post/70107542416/micha%C5%82-plebanek-kontrwywiadowcze-zadania-polskich> [dostęp: 8 IV 2016].

⁷⁶ R. Lizak, *Dokumenty legalizacyjne w służbach...*, s. 142–143.

⁷⁷ Art. 35 ust. 1–3 ustawy o ABW oraz AW, art. 24 ust. 1–3 ustawy o CBA, art. 39 ust. 1–5 ustawy o SKW oraz SWW.

⁷⁸ Art. 35 ust. 6 ustawy o ABW oraz AW, art. 24 ust. 4 ustawy o CBA, art. 39 ust. 6 ustawy o SKW oraz SWW.

Tutaj może dochodzić do nadużyć, np. w sytuacji „prywatnego wykorzystania” dokumentów legalizacyjnych, co jest działaniem przestępczym. Innym zagrożeniem jest wytworzenie do celów operacyjnych dokumentu mającego uwiarygodnić określony stan, np. posiadania i wykorzystywania dokumentu w celu namówienia lub zachęcenia figuranta w sposób niedozwolony do popełnienia przestępstwa.

Korzystanie służb specjalnych z pomocy osób niebędących ich funkcjonariuszami

Jednym z najważniejszych, a także najstarszym uprawnieniem funkcjonariuszy służb specjalnych jest możliwość korzystania z pomocy osób niebędących ich funkcjonariuszami – tajnych współpracowników (agentów), osób godnych zaufania czy informatorów. Jest to jedna z najskuteczniejszych metod stosowanych w pracy operacyjnej, która służy rozpoznawaniu, przeciwdziałaniu i zwalczaniu zagrożeń, jakie zgodnie z zakresem zadań przypisano służbom specjalnym w ustawach kompetencyjnych⁷⁹.

Krajowe służby specjalne przy wykonywaniu swoich ustawowych zadań mogą korzystać, z pewnymi wyjątkami, z pomocy osób niebędących ich funkcjonariuszami. Z reguły zabronione jest ujawnianie danych o osobie udzielającej służbom pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych. Taka osoba nie może ujawniać tego, że udziela pomocy ani okoliczności związanych z jej udzieleniem. Wspomnianej osobie może być przyznane wynagrodzenie wypłacane z funduszu operacyjnego. W przypadku utraty życia lub zdrowia, szkody w mieniu, w czasie korzystania lub w związku z korzystaniem z pomocy tej osoby przez służby specjalne, tym osobom lub ich spadkobiercom przysługuje odszkodowanie⁸⁰. Ujawnienie danych o takiej osobie może nastąpić np. w przypadku żądania prokuratora albo sądu, zgłoszonego w celu ścigania karnego za czyn zabroniony stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych⁸¹.

W przypadku korzystania z pomocy osób niebędących funkcjonariuszami służb cały system działań operacyjno-rozpoznawczych służb specjalnych może być narażony przez prywatny interes „źródła”, np. przez wprowadzenie w błąd, wskazywanie fałszywych dowodów czy dekonspirację. W związku z tym osoby poddane działaniom operacyjnym mogą stać się niewinnym celem służb specjalnych. W razie zaistnienia tak hipotetycznej sytuacji może dojść do najcięższych naruszeń praw i wolności człowieka. Służby bezwzględnie muszą mieć świadomość motywacji działań takiej osoby.

⁷⁹ M. Bożek i in., *Służby specjalne...*, s. 133.

⁸⁰ Art. 36 ust. 1, 2a–4 ustawy o ABW oraz AW, art. 25 ust. 1, 3, 4 ustawy o CBA, art. 40 ust. 1, 3–6 ustawy o SKW oraz SWW.

⁸¹ Art. 36 ust. 2, art. 39 ust. 4 ustawy o ABW oraz AW, art. 25 ust. 2, art. 28 ustawy o CBA, art. 40 ust. 2, art. 43 ust. 4 ustawy o SKW oraz SWW.

Zakończenie

Służby specjalne dysponują instrumentami służącymi realizacji zadań państwa w zakresie zapewnienia mu bezpieczeństwa. Z tego względu podczas realizacji swoich zadań muszą być w sposób szczególny zobowiązane do ochrony praw i wolności człowieka i obywatela, co wiąże się z poddaniem ich precyzyjnemu nadzorowi oraz kontroli sądowo-prokuratorskiej. Celowe wydaje się podjęcie procesu legislacyjnego zmierzającego do przygotowania jednolitej ustawy o czynnościach operacyjno-rozpoznawczych, która obejmowałaby wszystkie rodzaje służb upoważnionych do realizacji tego typu zadań. W ustawie o działaniach antyterrorystycznych szef ABW uzyskał szczególne uprawnienia w zakresie zarządzania kontroli operacyjnej. Z uwagi na to, że ta metoda pracy operacyjnej głęboko ingeruje w sferę praw i wolności człowieka, te działania powinny być poddane nadzorowi i kontroli niezawisłego sądu. Przyznanie służbom tak szerokich uprawnień w zwalczaniu terroryzmu i najcięższych form przestępczości, w tym przestępczości zorganizowanej, jest nieodzownie związane z ingerencją państwa w sferę praw i wolności człowieka i obywatela. Dotyczy to również osób utrzymujących kontakt z figurantem poddawanych czynnościom operacyjnym. Stąd też ustawodawca musi stosować takie ograniczenia w działalności tych służb, aby zminimalizować ich ingerencję w wyżej wymienione prawa i wolności.

Służby specjalne, realizując ofensywne metody pracy operacyjnej, szczegółowo ingerują w wolność i tajemnicę komunikowania się, prawo do poszanowania życia prywatnego i rodzinnego, nienaruszalność mieszkania, prawo do nieujawniania informacji o sobie oraz w prawo do rzetelnego procesu sądowego. Również przy innych czynnościach operacyjno-rozpoznawczych dochodzi do naruszenia prawa do poszanowania życia prywatnego i rodzinnego, prawa do nieujawniania informacji o sobie oraz nienaruszalności mieszkania. Dotyczy to m.in. takich uprawnień w pracy operacyjno-rozpoznawczej służb, jak uzyskiwanie danych telekomunikacyjnych, pocztowych lub internetowych, gromadzenie danych osobowych, wykorzystanie dokumentów legalizacyjnych czy korzystanie przez służby z pomocy osób niebędących ich funkcjonariuszami. Do ingerencji w prawo do życia, wolności, poszanowania życia prywatnego i rodzinnego czy swojego mieszkania dochodzi najczęściej przy realizacji takich zadań służb specjalnych, jak: legitymowanie osób, wydawanie poleceń określonego zachowania się, zatrzymanie osób, dokonywanie kontroli osobistej, przeszukanie osób i pomieszczeń, obserwowanie i rejestrowanie obrazu zdarzeń z miejsc publicznych.

Należy zatem stwierdzić, że służby specjalne podczas realizacji zadań naruszają prawa i wolności człowieka przede wszystkim w sferze prawa do poszanowania życia prywatnego i rodzinnego, prawa do rzetelnego procesu sądowego, prawa do wolności oraz prawa do życia. Prowadzenie skutecznej walki z przestępczością zorganizowaną, przeciwdziałanie terroryzmowi czy realizacja zadań kontrwywiadowczych i wywiadowczych wymusza na służbach odpowiedzialnych za bezpieczeństwo państwa stosowanie ofensywnej i wzmożonej działalności operacyjno-rozpoznawczej. Skuteczne przeciwdziałanie zagrożeniom, inicjuje wyposażenie tych organów w adekwatne in-

strumenty służące zwalczaniu tego rodzaju przestępczości. Należy również zwrócić uwagę na kontratypy, jakie zostały zawarte w ustawach kompetencyjnych w związku z realizacją przez funkcjonariuszy czynności operacyjno-rozpoznawczych. Usprawiedliwione działanie funkcjonariusza publicznego, a także nadanie mu uprawnień do niejednokrotnie głębokiej ingerencji w prawa i wolności człowieka i obywatela, musi mieć jednoznaczną normatywną rangę ustawową.

Dla przypadków czynności operacyjno-rozpoznawczych, których realizację cechuje równoznaczność wypełnienia znamion czynu zabronionego, ustanowiono kontratypy operacyjne. Do takich czynności operacyjno-rozpoznawczych należą m.in. zakup kontrolowany, przyjęcie lub wręczenie korzyści majątkowej, posługiwanie się dokumentami maskującymi prawdziwe dane osobowe⁸² funkcjonariusza (również pomocnictwo w sporządzaniu dokumentów i wytworzenie takich dokumentów) stosowane w tzw. działaniach pod przykryciem⁸³. Te unormowania są zawarte w art. 32 ustawy o ABW oraz AW:

Nie popełnia przestępstwa, kto, będąc do tego uprawnionym, wykonuje czynności określone w art. 29 ust. 1, jeżeli zostały zachowane warunki określone w art. 29 ust. 3, a także kto wykonuje czynności określone w art. 30 ust. 1.

oraz w art. 35 ust. 6:

Nie popełnia przestępstwa: 1) kto poleca sporządzenie lub kieruje sporządzeniem dokumentów, o których mowa w ust. 2 i 3; 2) kto sporządza dokumenty, o których mowa w ust. 2 i 3; 3) kto udziela pomocy w sporządzeniu dokumentów, o których mowa w ust. 2 i 3; 4) funkcjonariusz Agencji lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2 i 3.

W podobny sposób zostały zawarte te unormowania w ustawie o CBA, tj. w art. 21 oraz art. 24 ust. 4, a także w ustawie o SKW oraz SWW – art. 35 i art. 39 ust. 6.

Praca operacyjna realizowana przez służby specjalne niejednokrotnie przybiera różny zakres, polega także na korzystaniu z rozmaitych środków. Bezspornie rozwój przestępczości, w tym wykorzystywanie przez sprawców najnowocześniejszych osiągnięć techniki, musi wywoływać w konsekwencji właściwe reakcje służb odpowiedzialnych za jej zwalczanie. Z tego też powodu czynności operacyjno-rozpoznawcze mogą przybierać bardzo skomplikowaną formę działań, zarówno pod kątem prawnym, jak i logistycznym czy też technicznym⁸⁴.

⁸² D a n e o s o b o w e t o „(...) wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej” – zob. art. 6 ust. 1 ustawy o ochronie danych osobowych.

⁸³ F. Prusak, *Kontratyp czynności operacyjno-rozpoznawczych*, „Zeszyty Prawnicze” 2013, nr 1, s. 22–26.

⁸⁴ Z. Niemczyk, *Czynności operacyjno-rozpoznawcze...*, s. 7–8.

Mateusz Rakowski

„Nowe wojny” – wybrane aspekty asymetrycznych konfliktów w cyberprzestrzeni¹

Technologiczny postęp, który obserwujemy od czasów II wojny światowej, przyczynił się między innymi do rozwoju radiotelekomunikacji. Jednym z głównych wydarzeń było stworzenie rozległej sieci ARPANET², która została zaprezentowana przez Donalda Daviesa³ 5 sierpnia 1968 r.⁴ Dała ona początek erze Internetu, tworząc tym samym nową przestrzeń cybernetyczną. Pomimo prowadzenia prac już od końca lat 70. XX w., za początek Internetu w Polsce uznaje się 17 sierpnia 1991 r., kiedy po raz pierwszy nawiązano łączność przez protokół TCP/IP⁵ z Centrum Komputerowym Uniwersytetu w Kopenhadze⁶. Nowa sieć gwałtownie rozszerzała się, obejmując swym zasięgiem cały glob. Szacuje się, że współcześnie 46,1 proc. światowej populacji korzysta z Internetu⁷, włączając w to pojedynczych użytkowników, podmioty sektora prywatnego oraz instytucje państwowe.

1. Cyberprzestrzeń jako przestrzeń nieograniczona i ekspansywna oraz jej podstawowe elementy

Analizę problemu cyberwojen należy poprzedzić próbą zdefiniowania cyberprzestrzeni. *Polska Polityka Ochrony Cyberprzestrzeni* z 2013 r. opisuje tę sferę jako: (...) *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinfor-*

¹ Fragment pracy licencjackiej pt. „*Nowe wojny*” - *wybrane aspekty asymetrycznych konfliktów w cyberprzestrzeni*, która została wyróżniona w konkursie Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2015/2016). Autor jest absolwentem Akademii im. Jana Długosza w Częstochowie, Wydział Filozoficzno-Historyczny. Redakcja dokonała w tekście niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

² *Advanced Research Projects Agency Network* (Sieć Agencji Zaawansowanych Projektów Badawczych) – stworzona przez Advanced Research Projects Agency, ARPA (obecnie: Defense Advanced Research Projects Agency, DARPA) pierwsza rozległa sieć, będąca przodkiem współczesnej sieci World Wide Web. Na jej podstawie stworzono wykorzystywany dziś protokół TCP/IP.

³ Donald Davies (7 czerwca 1924 r. – 28 maja 2000 r.) – walijski naukowiec, od 1947 r. związany z National Physical Laboratory (Wielka Brytania), twórca konceptu komutacji pakietów, stanowiących podstawę działania Internetu w formie, która jest obecnie wykorzystywana, <http://www.npl.co.uk/people/donald-davies> [dostęp: 10 XII 2015].

⁴ <http://news.bbc.co.uk/2/hi/technology/7541123.stm> [dostęp: 10 XII 2015].

⁵ TCP/IP (*Transmission Control Protocol/Internet Protocol*) – warstwowy model struktury protokołów komunikacyjnych, na których jest oparty dzisiejszy Internet. Został stworzony w latach 70. XX w. przez DARPA. Obecnie TCP/IP ma skomplikowaną strukturę, gdyż w rzeczywistości stanowi całą rodzinę protokołów komunikacyjnych, funkcjonujących w odrębnych warstwach modelu, <http://www.garykessler.net/library/tcpip.html> [dostęp: 10 XII 2015].

⁶ <http://www.nask.pl/run/n/Historia> [dostęp: 20 I 2016].

⁷ <http://internetworldstats.com/stats.htm> [dostęp: 10 XII 2015].