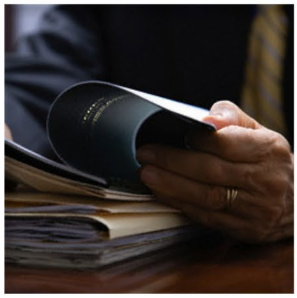
Raporty
Opinie
Sprawozdania



Służby specjalne, policyjne i skarbowe a prawa człowieka – standardy konstytucyjne i międzynarodowe oraz kierunki niezbędnych zmian legislacyjnych

Barbara Grabowska-Moroz
adw. Artur Pietryka

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA

Warszawa, maj 2016

Spis treści

1. Wstęp ... 3
1.1. Zakres podmiotowy opracowania ... 4
1.2. Aktualny model kontroli działalności służb specjalnych w Polsce ... 4
2. Ewolucja regulacji służb specjalnych, policyjnych i skarbowych ... 6
2.1. Okres 1989 – 1994 r. ... 6
2.2. Okres 1995 r. – 2005 r. ... 6
2.3. Okres 2005 r. – 2015 r. ... 9
2.4. Zmiany wprowadzone w 2016 r. ... 14
2.5. Projekt ustawy o działaniach antyterrorystycznych ... 17
2.6. Projekty zmian legislacyjnych, które nie zostały uchwalone ... 18
2.6.1. Projekty rządowe ... 18
2.6.2. Projekty poselskie ... 19
2.6.3. Projekty senackie ... 20
2.7. Podsumowanie ... 21
3. Niejawne pozyskiwanie informacji o obywatelach – standard konstytucyjny ustanowiony przez Trybunał Konstytucyjny i jego realizacja w obowiązujących przepisach ... 22
4. Standardy prawa międzynarodowego odnoszące się kompetencji służb specjalnych i policyjnych ... 29
4.1. Rada Europy ... 29
4.2. Unia Europejska ... 38
4.3. Organizacja Narodów Zjednoczonych ... 40
4.4. Międzynarodowe standardy dotyczące transparentności działania służb ... 41
5. Konkluzje ... 44

Załączniki ... 46
Załącznik nr 1. Wybrane sprawy prowadzone przez HFPC przed sądami administracyjnymi. ... 46
Załącznik nr 2. Rezolucje Parlamentu Europejskiego w sprawie masowej inwigilacji. ... 47
Załącznik nr 3. Zestawienie dobrych praktyk dotyczących kontroli nad służbami wywiadowczymi (w języku angielskim). ... 49

1. Wstęp

Bezpieczeństwo i prawa człowieka są zazwyczaj prezentowane w różnych wymiarach – zwykle jako wartości przeciwstawne. Jednak coraz częściej – zarówno w literaturze, jak i w orzecznictwie sądów – podkreśla się wzajemne ich uwarunkowanie. Trudno bowiem mówić o prawach człowieka bez zapewnienia bezpieczeństwa publicznego, z drugiej zaś strony możliwość korzystania z praw i wolności staje się warunkiem poczucia bezpieczeństwa. Dodatkowo, obie te wartości mają bezpośredni wpływ na procesy polityczne i demokratyczne w państwie.

Zagadnieniem, które jak w soczewce skupia te trzy zagadnienia – bezpieczeństwo, prawa człowieka i demokrację – jest działalność służb odpowiedzialnych za bezpieczeństwo i porządek publiczny. W systemie polskiego prawa funkcjonują różne rodzaje służb realizujące to zadanie – specjalne, policyjne, skarbowe. Zakres posiadanych przez nie kompetencji bezpośrednio wpływa na poziom ochrony praw i wolności, które to z kolei mają wpływ na skuteczność istniejących mechanizmów demokratycznych, takich jak m.in. kontrola nad władzą wykonawczą.

Pomimo częstej obecności tematyki dotyczącej służb (w szczególności służb specjalnych) w debacie publicznej, jak również podejmowanych regularnie inicjatyw legislacyjnych w tym zakresie, stan prawa polskiego odbiega istotnie od wytycznych, które w kontekście międzynarodowych standardów praw człowieka, powinny zostać zaimplementowane do prawa krajowego dla prawidłowego zabezpieczenia zarówno statusu jednostki, jak również zasady demokratycznego państwa prawa.

Celem niniejszego opracowania jest zarysowanie kształtu i kierunku dotychczasowych zmian legislacyjnych dotyczących służb specjalnych w dwóch powiązanych ze sobą aspektach – wpływu na prawa i wolności oraz mechanizmów kontroli nad służbami. Posłuży to ukazaniu, w jakim kierunku powinny zmierzać dalsze zmiany prawa regulujące działalność służb, tak aby uwzględniały wytyczne dotyczące zapewnienia odpowiedniego poziomu ochrony praw człowieka. Wytyczne te wynikają przede wszystkim z intensywnego rozwoju standardów na poziomie prawa międzynarodowego – zarówno o charakterze *soft law*, jak i *hard law* – oraz orzecznictwa sądów, które starają się wyważyć nowe zagrożenia dla bezpieczeństwa publicznego z obowiązkiem respektowania praw i wolności.

Niniejsze opracowanie zostało przygotowane w ramach „Monitoringu procesu legislacyjnego w obszarze wymiaru sprawiedliwości" funkcjonującego od 2010 r. w Helsińskiej Fundacji Praw Człowieka[1]. Jednym ze stałych elementów działalności Monitoringu, są zmiany w służbach stojących na straży bezpieczeństwa i porządku publicznego[2]. Kompetencje przyznane służbom z jednej strony warunkują realizację powierzonych im zadań, z drugiej – istotnie wkraczają w prawa i wolności prawnie chronione, takie jak prywatność, wolność osobista czy wolność słowa. Co więcej, zagadnienie uprawnień służb

1 Obecnie „Monitoring procesu legislacyjnego w obszarze wymiaru sprawiedliwości" jest realizowany przez Helsińską Fundację Praw Człowieka dzięki dotacji otrzymanej z programu „Obywatele dla Demokracji" finansowanego z Funduszy EOG.

2 Por. Opinia Helsińskiej Fundacji Praw Człowieka do projektów – ustawy o Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu oraz Komisji ds. Kontroli Służb Specjalnych (dostępna na stronie: http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2013/12/ABW_AW_KKSSopinia.pdf); Analiza sądowej kontrola wniosków o zarządzenie kontroli operacyjnej (dostępna na stronie: http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2013/06/amicus_curiae_TK_K_23_11.pdf); Uwagi HFPC do projektu założeń reformy przepisów regulujących dostęp sądów, organów ścigania i służb specjalnych do danych telekomunikacyjnych przechowywanych przez operatorów (dostępne na stronie: http://www.obserwatorium.org/images/retencja_MSW.pdf).

odpowiedzialnych w Polsce za zapewnienie porządku i bezpieczeństwa stało się przedmiotem zainteresowania Zgromadzenia Parlamentarnego Rady Europy, które zleciło Komisji Weneckiej opracowanie odpowiedniej analizy[3].

1.1. Zakres podmiotowy opracowania

W art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[4] ustawodawca wprowadził definicję podmiotową służb specjalnych. Zgodnie z tym przepisem służbami specjalnymi są: Agencja Bezpieczeństwa Wewnętrznego (ABW), Agencja Wywiadu (AW), Służba Kontrwywiadu Wojskowego (SKW), Służba Wywiadu Wojskowego (SWW) oraz Centralne Biuro Antykorupcyjne (CBA). Brak jest natomiast w obowiązujących przepisach definicji przedmiotowej służb oraz definicji takich określeń jak: służba policyjna, czy służba skarbowa. Dlatego też na potrzeby niniejszego opracowania autorzy za służby policyjne uznali Policję, Żandarmerię Wojskową oraz Straż Graniczną, zaś za skarbowe – wywiad skarbowy i Służbę Celną. To zastrzeżenie ma charakter jedynie umowny i porządkujący, albowiem mimo ustawowego przyporządkowania CBA do służb specjalnych, z uwagi na jego główny przedmiot swojej działalności, tj. ściganie przestępczości, jest ono raczej służbą policyjną niż służbą specjalną[5]. Wspólnym mianownikiem wszystkich tych służb jest możliwość prowadzenia przez nie działań niejawnych, tzw. czynności operacyjno-rozpoznawczych. Kompetencja do ich stosowania jest jedną z najbardziej inwazyjnych z punktu widzenia praw człowieka. Dlatego też użycie pojęcia „służby specjalne" w niniejszym dokumencie odnosi się również do służb policyjnych i skarbowych w zakresie, w jakim prowadzą one w ramach realizowanych ustawowych zadań czynności operacyjno-rozpoznawcze.

1.2. Aktualny model kontroli działalności służb specjalnych w Polsce

Z uwagi na fakt, że służby stanowią część administracji rządowej, podstawowy szczebel kontroli i nadzoru nad nimi koncentruje się na poziomie Rady Ministrów, w szczególności w Kolegium do spraw Służb Specjalnych lub w osobie ministra koordynatora służb specjalnych. W Sejmie podmiotem prowadzącym bieżącą kontrolę jest sejmowa Komisja do Spraw Służb Specjalnych, funkcjonująca od 1995 r.[6] Ponadto Sejm i Senat są adresatami przedkładanych przez Prokuratora Generalnego i Ministra Spraw Wewnętrznych informacji statystycznych o stosowaniu niektórych form czynności operacyjno – rozpoznawczych[7].

---

3 Por.: *Amendment to the Act on Police and other legal acts regulating surveillance by the law enforcement agencies and security services. Comments of the Helsinki Foundation for Human Rights*, dokument dostępny na stronie: http://www.hfhr.pl/wp-content/uploads/2016/05/HFHR_hand_out_Venice_Commission_Act_on_Police_FNL.pdf.

4 Dz. U. z 2015 r. poz. 1929 t.j. dalej: ustawa o ABW oraz AW.

5 Por.: P. Radziewicz, *Opinia prawna w sprawie zgodności z Konstytucją niektórych przepisów projektu ustawy o Centralnym Burze Antykorupcyjnym – druk nr 275*, Zeszyty Prawnicze Biura Studiów i Ekspertyz Kancelarii Sejmu, nr 2/2006, s. 81-82:„CBA jest formacją o cechach policji administracyjnej, która ma możliwość używania środków przymusu bezpośredniego (we wskazanych przez przepisy warunkach), i której podstawowym celem jest wykrywanie i przeciwdziałanie określonym rodzajom przestępstw (podobnie jak Policja lub Agencja Bezpieczeństwa Wewnętrznego)".

6 Na podstawie art. 141a Regulaminu Sejmu Komisja ds. Służb Specjalnych powinna uchwalić regulamin, w oparciu o który będzie procedować.

7 Art. 11 ustawy z dnia 28 stycznia 2016 r. - Prawo o prokuraturze (Dz. U. Poz. 177); art. 19 ust. 22 ustawy z 6 kwietnia 1990 r. o Policji (Dz. U. 2015, poz. 355 t.j., ze zm.).

Nieco inaczej wygląda natomiast kwestia zaangażowania sądów w działalność służb. Po pierwsze, sądy uczestniczą w procesie stosowania niektórych czynności operacyjno – rozpoznawczych (wyrażają zgodę pierwotną lub następczą na stosowanie kontroli operacyjnej). Dalej, w ramach rozpoznawanych spraw karnych rozstrzygają w oparciu o zgromadzone przez służby materiały operacyjne (np. z kontroli operacyjnej, czy też zakupu kontrolowanego lub przesyłki niejawnie nadzorowanej). Ponadto, orzekają w sprawach dotyczących ewentualnych nadużyć ze strony służb (o przestępstwa funkcjonariuszy, lub ochronę dóbr osobistych osób poddanych stosowaniu czynności operacyjno – rozpoznawczych). Wreszcie - w przypadku sądów administracyjnych - decydują o tym, czego obywatele w ramach dostępu do informacji publicznej mogą dowiedzieć się na temat działalności służb.

Kolejnym ośrodkiem, którego funkcjonowanie wiąże się z działalnością służb, jest prokuratura. Prokuratorzy współuczestniczą obok sądów w zarządzaniu np. kontroli operacyjnej i mogą m.in. nie wyrazić zgody na wniosek o jej zarządzenie. Prokuratorzy wyrażają również zgodę na stosowanie określonych technik np. zakupu kontrolowanego i przesyłki niejawnie nadzorowanej. Wreszcie decydują o wykorzystaniu procesowym materiałów zgromadzonych dzięki stosowaniu czynności operacyjno – rozpoznawczych, natomiast w ramach postępowań przygotowawczych mogą zlecać dokonanie określonych niezbędnych czynności. Obecny model kontroli nad działalnością służb ma zatem charakter rozproszony. W strukturze każdej z władz można znaleźć bowiem jej instrumenty.

2. Ewolucja regulacji służb specjalnych, policyjnych i skarbowych

Uregulowanie służb zajmujących się ochroną bezpieczeństwa i porządku publicznego było jednym z pierwszych i podstawowych elementów transformacji ustrojowej po 1989 r. W procesie kształtowania się ich struktur mówić można o pewnych fazach, w których dokonywane były zmiany przepisów, inspirowane bieżącymi potrzebami, wydarzeniami, a także kształtującym się orzecznictwem sądowym.

2.1. Okres 1989 – 1994 r.

W pierwszym 5-letnim okresie transformacji ustrojowej ukształtowana została struktura z dwoma pionami służb specjalnych: cywilnym w postaci UOP oraz wojskowym z WSI, dwoma pionami służb policyjnych – cywilnym z Policją i Strażą Graniczną oraz wojskowym z Żandarmerią Wojskową, a także zaczątkiem pionu służb skarbowych. Zapoczątkowało go uchwalenie aktów prawnych regulujących działalność Policji i Urzędu Ochrony Państwa, które następnie były punktem wyjścia dla kolejnych regulacji działalności służb, w tym wojskowych.

Warto jedynie zasygnalizować, że w rzeczonym okresie Trybunał Konstytucyjny zajmował się dwiema istotnymi z perspektywy niniejszego opracowania sprawami. Orzeczeniem z 19 czerwca 1992 r. TK uznał za niezgodne z Konstytucją RP i niektórymi ustawami uchwały Sejmu Rzeczypospolitej Polskiej z dnia 28 maja 1992 r. zobowiązującej Ministra Spraw Wewnętrznych do podania pełnej informacji na temat urzędników państwowych od szczebla wojewody wzwyż, posłów, senatorów, prokuratorów, adwokatów, radnych gmin i członków zarządów gmin będących współpracownikami UB i SB w latach 1945 – 1990 (tzw. lista Macierewicza)[8]. Postanowieniem z 15 czerwca 1993 r. TK umorzył zaś postępowanie w sprawie konstytucyjności instrukcji nr 0015/92 dyrektora Biura Analiz i Informacji Urzędu Ochrony Państwa z dnia 26 października 1992 r. o pracy pism analiz i informacji UOP, ponieważ w toku postępowania w sprawie została ona uchylona[9].

2.2. Okres 1995 r. – 2005 r.

W kolejnym okresie od 1995 r. do 2005 r. doszło do zmian w zakresie nadzoru i kontroli nad służbami, ich uprawnień oraz struktur. W zakresie tych pierwszych wskazać należy na uchwalenie ustaw: 1) podporządkowującej Szefa UOP bezpośrednio Prezesowi Rady Ministrów oraz tworzącej przy Radzie Ministrów Kolegium do Spraw Służb Specjalnych jako organu opiniodawczo–doradczego w sprawach programowania, nadzoru i koordynowania działań UOP i WSI oraz podejmowanych dla ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej oraz ŻW[10], 2) wprowadzającej prokuratorsko-sądową kontrolę nad zarządzaniem kontroli operacyjnej stosowanej przez uprawnione organy Straży Granicznej i Policji,

8 Sygn. U 6/92.

9 Sygn. U 3/93.

10 Ustawa z 8 sierpnia 1996 r. o zmianie niektórych ustaw normujących funkcjonowanie gospodarki i administracji publicznej (Dz. U. z 1996 r. Nr 106, poz. 496).

zamiast kontroli prokuratorsko–ministerialnej[11], 3) znoszącej UOP i tworzącej w jego miejsce ABW oraz AW. W zakresie zmian dotyczących uprawnień służb zwrócić należy uwagę na uchwalenie: 1) ustawy wprowadzającej możliwość stosowania przez Policję, Straż Graniczną i Urząd Ochrony Państwa instytucji tzw. zakupu kontrolowanego oraz przesyłki niejawnie nadzorowanej[12], 2) ustawy przyznającej kontroli skarbowej uprawnienia do stosowania przez kontrolę skarbową czynności operacyjno – rozpoznawczych umożliwiających uzyskiwanie informacji oraz utrwalanie śladów i dowodów[13], 3) ustaw poszerzających katalogi przestępstw, w ramach ścigania których można było stosować kontrolę operacyjną, zakup kontrolowany, przesyłkę niejawnie nadzorowaną[14], 4) ustawy nadającej ŻW uprawnienia „policji dla wojskowych", z powieleniem rozwiązań ustawy o Policji, w tym m.in. w zakresie stosowania czynności operacyjno – rozpoznawczych[15].

Okres ten niewątpliwie stał pod znakiem wzmacniania kompetencji służb, w kierunku czynienia ich formacjami o charakterze policyjnym. Objawiało się to przyznawaniem nowych uprawnień i poszerzaniem możliwości ich działania. Znamienne jest przy tym, że już w tym okresie pojawiła się tendencja do powierzenia tych samych zadań różnym służbom, co widoczne jest zwłaszcza w zakresie zwalczania przestępczości o charakterze korupcyjnym. Z drugiej strony, w okresie tym doszło do fundamentalnej zmiany w zakresie kontroli nad ich działalnością. Ustawodawca stworzył tu bowiem instrumenty kontroli nad ich pracą na poziomie Rady Ministrów, a także odszedł od ministerialno-prokuratorskiej kontroli nad stosowaniem najbardziej inwazyjnej formy inwigilacji, jaką jest kontrola operacyjna.

Odnotować należy, że w tym okresie Trybunał Konstytucyjny wydał dwa istotne orzeczenia w sprawach dotyczących uprawnień służb specjalnych. Ponadto Trybunał Konstytucyjny wydał postanowienie sygnalizacyjne (sygn. S 2/06) dotyczące obowiązku tzw. notyfikacji.

W wyroku z 20 kwietnia 2002 r. (sygn. K 45/02), Trybunał Konstytucyjny uznał art. 23 ust. 1 pkt 6 ustawy o ABW oraz AW za niekonstytucyjny. Przepis ten uprawniał funkcjonariuszy ABW do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń i dźwięku towarzyszącego tym zdarzeniom w miejscach publicznych. Problem polegał na tym, iż ustawodawca nie przewidział w ustawie o ABW oraz AW żadnych mechanizmów pozwalających na skontrolowanie zasadności takich czynności, a także nie określał sposobu wykorzystania uzyskanych w ich wyniku informacji. W toku prac nad zmianami ustawy o ABW oraz AW, mających na celu wykonanie ww. wyroku wyłonił się problem wprowadzenia obowiązku informowania jednostek o prowadzonych wobec nich obserwacjach, dokonywanych w ramach czynności operacyjno-rozpoznawczych. Przedstawiony przez Radę Ministrów projekt przewidywał, iż na sposób przeprowadzenia czynności miało przysługiwać zażalenie wnoszone w terminie 7 dni od dnia jej

11 Ustawa z 11 kwietnia 2001 r. o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw (Dz. U. z 2001 r. Nr 45, poz. 498) oraz ustawa 27 lipca 2001 r. o zmianie ustawy o Policji, ustawy o działalności ubezpieczeniowej, ustawy - Prawo bankowe, ustawy o samorządzie powiatowym oraz ustawy - Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz. U. z 2001 r. Nr 100, poz. 1084).

12 Ustawa z 21 lipca 1995 r. o zmianie ustawy o urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa, o Straży Granicznej oraz niektórych innych ustaw (Dz. U. z 1995 r. Nr 104, poz. 515).

13 Ustawa z 7 listopada 1996 r. o zmianie ustawy o kontroli skarbowej i niektórych innych ustaw (Dz. U. z 1996 r. Nr 152, poz. 720).

14 Ustawa z 27 lipca 2001 r. o zmianie ustawy o Policji, ustawy o działalności ubezpieczeniowej, ustawy - Prawo bankowe, ustawy o samorządzie powiatowym oraz ustawy - Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz. U. z 2001 r. Nr 100, poz. 1084).

15 Ustawa z 24 sierpnia 2001 r. o Żandarmerii Wojskowej oraz wojskowych organach porządkowych (Dz. U. z 2001 r. Nr 123, poz. 1353) (dalej: ustawa o ŻW).

wykonania do właściwego miejscowo prokuratora[16]. Według A. Tarachy[17] *de facto* oznaczało to obowiązek po stronie ABW poinformowania jednostki o prowadzonej obserwacji. Natomiast według uczestniczących w posiedzeniach komisji przedstawicieli ABW przepis miał mieć zastosowanie tylko wtedy, gdy osoba inwigilowana dowiedziała się sama o prowadzeniu wobec niej obserwacji[18].

Ostatecznie art. 23 ust. 7 ustawy o ABW oraz AW otrzymał brzmienie:

„Na sposób przeprowadzenia czynności, o których mowa w ust. 1
1) pkt 1, 2, 5, 7 i 8, w terminie 7 dni od dnia dokonania czynności,
2) pkt 6, w terminie 7 dni od dnia gdy podmiot dowiedział się o dokonanych wobec niego czynnościach – przysługuje zażalenie do prokuratora właściwego ze względu na miejsce przeprowadzenia czynności. Do zażalenia stosuje się przepisy Kodeksu postępowania karnego w zakresie dotyczącym postępowania odwoławczego"[19].

Zatem nowelizacja nie nałożyła na funkcjonariuszy ABW formalnego obowiązku poinformowania jednostki o prowadzonej obserwacji i czynność tę poddała jedynie kontroli prokuratorskiej.

Z kolei w wyroku z 12 grudnia 2005 r. (sygn. K 32/04) Trybunał Konstytucyjny stwierdził niezgodność z Konstytucją m.in. art. 19 ust. 4 oraz art. 19 ust. 18 ustawy o Policji. Pierwszy z nich przewidywał, iż sąd okręgowy mógł wyrazić zgodę na zachowanie materiałów zebranych w toku kontroli operacyjnej prowadzonej w przypadkach „niecierpiących zwłoki", przeprowadzonej bez zgody sądu. Drugi, umożliwiał prowadzenie kontroli operacyjnej za wyrażoną na piśmie zgodą nadawcy lub odbiorcy przekazu informacji, lecz bez zgody sądu. Trybunał Konstytucyjny w wyroku zwrócił uwagę na szereg problematycznych kwestii związanych w ogóle z zagadnieniem stosowania czynności operacyjno – rozpoznawczych i wykorzystywaniem na potrzeby procesu karnego materiałów dzięki nim pozyskanych. TK poruszył m.in. kwestię informowania osoby, wobec której prowadzona jest kontrola operacyjna, o fakcie podjęcia tej czynności. Trybunał Konstytucyjny stwierdził konstytucyjność art. 19 ust. 16 ustawy o Policji w zakresie, w jakim nie wykluczał on po zakończeniu kontroli operacyjnej powiadomienia o tej kontroli podejrzanego i jego obrońcy.

Jednocześnie Trybunał skierował do Sejmu postanowienie sygnalizacyjne, w którym wskazał na „potrzebę podjęcia inicjatywy ustawodawczej w przedmiocie zagwarantowania w ustawie o Policji konstytucyjnych praw osób poddanych kontroli operacyjnej". Odnosząc się w postanowieniu do wyroku z 12 grudnia 2005 r. Trybunał podkreślił, że „uznając konstytucyjność art. 19 ust. 16 ustawy o Policji, stwierdził, że przepis ten bynajmniej nie wyklucza (jak to sformułowano we wniosku) możliwości informowania osoby poddanej kontroli operacyjnej o przeprowadzeniu tej kontroli. Natomiast wyłącza (i to ograniczenie Trybunał uznał za mieszczące się w granicach regulacyjnej swobody ustawodawcy) konieczność podania takiej informacji w czasie trwania czynności operacyjnych".

16 Druk sejmowy nr 3427, Sejm IV kadencji.

17 A. Taracha, *Czynności operacyjno - rozpoznawcze. Aspekty kryminalistyczne*, Lublin 2006.

18 Por.: stenogram posiedzenia sejmowej Komisji Sprawiedliwości i Praw Człowieka z dnia 23 listopada 2004 r. http://orka.sejm.gov.pl/Biuletyn.nsf/wgskrnr/KSS-141.

19 Ustawa z dnia 25 listopada 2004 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz. U. Nr 267, poz. 2647).

„Czym innym jest jednak brak przeszkody w zaskarżonym przepisie [art. 19 ust. 16 – przyp. aut.] *do udostępnienia materiałów, na żądane zainteresowanego, co w ocenie Trybunału zapewnia już obecny stan prawny, a czym innym pozytywny obowiązek informowania osoby poddanej działaniom operacyjnym przez policję z jej własnej inicjatywy, o prowadzeniu kontroli operacyjnej, o czym była mowa we wniosku Rzecznika Praw Obywatelskich. Zmierzał on bowiem w rzeczywistości do zakwestionowania braku wyrażenia w zaskarżonym przepisie ustawy pozytywnego obowiązku informowania przez policję o bezskutecznej, zakończonej kontroli operacyjnej wobec osoby poddanej takiej kontroli, jeśli w stosunku do tej osoby nie są prowadzone dalsze czynności procesowe. W związku z tym należy zauważyć, że istnienie takiego obowiązku policji* ***byłoby zapewne wskazane i odpowiadałoby potrzebie efektywnej instrumentalizacji proceduralnej konstytucyjnego prawa określonego w art. 51 ust. 4 Konstytucji****. Podobny problem w innych państwach europejskich doprowadził do podwyższenia standardu gwarancji proceduralnych (na tle sprawy Klass i inni wprowadzono w niemieckim ustawodawstwie, pozytywny obowiązek informacji o prowadzonej, zakończonej kontroli operacyjnej).”*

Postanowienie TK z 25 stycznia 2006 r. S 2/06 (fragment)

2.3. Okres 2006 r. – 2015 r.

Kolejne lata przyniosły dalsze zmiany w zakresie struktur służb, nadzoru i kontroli nad nimi, a także ich uprawnień. Przykładem zmian w zakresie struktur służb było powołanie ustawami z 9 czerwca 2006 r.[20] Centralnego Biura Antykorupcyjnego jako służby specjalnej ukierunkowanej na zwalczanie korupcji, a także zastąpienie Wojskowych Służb Informacyjnych dwoma służbami: Służbą Kontrwywiadu Wojskowego oraz Służbą Wywiadu Wojskowego.

W zakresie uprawnień służb wskazać należy przede wszystkim na fundamentalną zmianę – uchwalenie nowelizacji Prawa telekomunikacyjnego[21], implementującą do polskiego porządku prawnego przepisy tzw. dyrektywy retencyjnej[22]. Nowelizacja wprowadziła przede wszystkim obowiązek przedsiębiorców telekomunikacyjnych przechowywania przez okres 24 miesięczny tzw. danych telekomunikacyjnych[23] i udostępniania ich na potrzeby służb, w związku m.in. z realizacją ich ustawowych zadań. Tym samym ustawa stworzyła niezwykle szeroką kompetencję do pozyskiwania przedmiotowych informacji, przy użyciu sieci telekomunikacyjnych. Jednocześnie nowelizacja praktycznie nie wprowadzała jakichkolwiek

20 Ustawa z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2006 r. Nr 104, poz. 708 ze zm.) (dalej: ustawa o CBA) oraz ustawa z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2006 r. Nr 104, poz. 709 ze zm.) (dalej: ustawa o SKW oraz SWW).

21 Ustawa z 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 85, poz. 716)

22 Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającą dyrektywę 2002/58/WE (Dz.U. UE z 13 kwietnia 2006 r. L 105, s. 54).

23 Prawo telekomunikacyjne rozróżnia trzy rodzaje danych, regulowanych odpowiednio w art. 159 ust. 1 art. 179 ust. 9 oraz w art. 180c.

mechanizmów ochrony przed nadużyciami ze strony służb w tym zakresie. Dopiero ustawa z 16 listopada 2012 r.[24] doprowadziła do skrócenia okresu przechowywania tych danych do 12 miesięcy.

Ponadto w omawianym okresie spotkać można przykłady podejmowania inicjatyw poszerzających katalogi przestępstw, w ramach ścigania których możliwe było stosowanie kontroli operacyjnej przez poszczególne służby. Jednym z przykładów jest tu nowelizacja ustawy o CBA, która miała wykonać wyrok TK z 22 czerwca 2009 r. (sygn. K 54/07). Trybunał Konstytucyjny stwierdził niekonstytucyjność przepisów ustawy o CBA w zakresie definicji korupcji (art. 1 ust. 3), braku instrumentów kontroli nad przetwarzaniem danych osobowych, w tym wrażliwych (art. 22 ust. 4-7), a także braku przepisów dotyczących wykorzystywania i przechowywania danych zgromadzonych w ramach oględzin (art. 40). Przy okazji tego wyroku, po raz kolejny w zdaniu odrębnym prof. E. Łętowskiej, zaakcentowana została kwestia wprowadzenia obowiązku informowania jednostki o prowadzonej kontroli operacyjnej.

> *„[G]warancja (sugerowana w wyroku o sygn. K 32/04 i aprobowana np. w niemieckim systemie prawnym) sprzyja samodyscyplinie funkcjonariuszy służb stosujących techniki niejawne i zbieranie danych. Brakuje gwarancji rzeczywiście efektywnego niszczenia zbędnie uzyskanych danych. Nie wystarczy zapisać, że coś trzeba komisyjnie zniszczyć. Należy jeszcze zapewnić w efektywny sposób możliwość sprawdzenia – choćby wyrywkowo – czy tak się naprawdę robi. Brakuje (co można byłoby w tych warunkach kwalifikować jako legislacyjne pominięcie) choćby próby rozwiązania problemu danych uzyskanych refleksowo – np. przy podsłuchach (gdy podsłuch założono komu innemu, a wykorzystuje się go wobec rozmówców formalnie podsłuchiwanego). Nie są kompensowane żadnymi innymi gwarancjami. Kompetencja jest nazbyt szeroka – brak elementu kontroli nad tym co Policja zbiera i przekazuje".*
>
> Fragment zdania odrębnego prof. E. Łętowskiej do wyroku z 22 czerwca 2009 r. (sygn. K 54/07)

Ustawa z 5 sierpnia 2010 r.[25] za wskazaniami TK doprowadziła do zmiany definicji „korupcji". Jednakże już niekoniecznie za dające się pogodzić z wyrokiem TK uznać można inne wprowadzone nią zmiany. Przykładowo, z wyroku w żaden sposób nie wynikała właśnie konieczność poszerzenia katalogu przestępstw, których ściganie możliwe jest przy użyciu kontroli operacyjnej. Ponadto wiele wątpliwości wzbudzała kwestia powierzenia prawidłowości przetwarzania tzw. danych wrażliwych przez CBA, nie sądowi, ale nowo powoływanemu pełnomocnikowi do spraw przetwarzania danych.

Jeśli chodzi o zmiany w zakresie nadzoru i kontroli wskazać należy na ustawę z 4 lutego 2011 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw[26]. Doprecyzowała ona obowiązek

24 Ustawa z 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. poz. 1445)

25 Ustawa z 5 sierpnia 2010 r. o zmianie ustawy o Centralnym Biurze Antykorupcyjnym oraz ustawy o sporcie (Dz. U. Nr 151 poz. 1014).

26 Ustawa z 4 lutego 2011 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. Nr 53, poz. 273).

niszczenia materiałów z kontroli operacyjnej[27]. Nałożyła ponadto obowiązek sprawozdawczy po stronie Prokuratora Generalnego oraz Ministra Spraw Wewnętrznych odpowiednio o liczbie osób, wobec których stosowana była w danym roku kontrola operacyjna[28], a także o liczbie stosowanych przez Policję kontroli operacyjnej[29]. Nowelizacja wprowadziła też obowiązek przedkładania sądowi okręgowemu materiałów operacyjnych „uzasadniających" zarządzenie kontroli operacyjnej.

Ponadto nowelizacja uregulowała mechanizm tzw. **następczej zgody sądu** na wykorzystywanie zgromadzonych w ramach kontroli operacyjnej materiałów dotyczących innych przestępstw i osób niż wskazane we wniosku o zarządzenie kontroli operacyjnej. Kluczowym orzeczeniem w tym zakresie było postanowienie Sądu Najwyższego z 26 kwietnia 2007 r. (syn. I KZP 6/07). Sąd Najwyższy wskazał, że przez uzyskane w ramach kontroli operacyjnej dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego należy rozumieć wyłącznie dowody popełnienia przestępstw wymienionych w katalogu z art. 19 ust. 1 ustawy o Policji. Zatem Policja nie mogła wykorzystać materiałów dotyczących przestępstw innych niże te, które może ścigać przy użyciu kontroli operacyjnej. Po drugie Sąd Najwyższy wskazał, iż uzyskane w czasie kontroli operacyjnej dowody popełnienia przestępstw – określonych w art. 19 ust. 1 ustawy o Policji - przez osobę inną niż objęta postanowieniem wydanym na podstawie art. 19 ust. 2 tej ustawy albo popełnionych wprawdzie przez osobę nim objętą, ale dotyczące przestępstw innych niż wskazane w tym postanowieniu, mogą być wykorzystane w postępowaniu przed sądem. Sąd Najwyższy w tym szeroko komentowanym orzeczeniu[30] wyszedł z założenia, iż w przypadku niejasności przepisów, konieczne jest restrykcyjne wykładanie obecnych przepisów, albowiem ze stosowaniem czynności operacyjno – rozpoznawczych wiąże się przeważnie głęboka ingerencja w konstytucyjne prawa i wolności. Ten kierunek – restrykcyjnej wykładni przepisów dotyczących stosowania czynności operacyjno – rozpoznawczych – utrwalił się, a nawet był rozwijany w orzecznictwie[31], by doprowadzić do zmian z dniem 11 czerwca 2011 r. przepisów poprzez prawne usankcjonowanie obowiązku uzyskiwania tzw. zgody następczej.

27 Warto zauważyć, że po wejściu w życie tych przepisów TK umorzył z przyczyn formalnych postępowanie ze skargi konstytucyjnej Krzysztofa P. dotyczące konstytucyjności art. 19 ustawy o Policji w zakresie, w jakim przepis ten umożliwiał gromadzenie i dołączanie do akt postępowania karnego materiałów kontroli operacyjnej dokumentujących kontakty oskarżonego z obrońcą, jak również nie zawierały obowiązku zniszczenia takich materiałów oraz nie przewidywały procedury umożliwiającej skuteczne żądanie ich zniszczeni (sygn. SK 7/10).

28 Zgodnie z art. 11 § 1 Prawa o prokuraturze, Prokurator Generalny przedstawia Sejmowi i Senatowi jawną roczną informację o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej, ze wskazaniem liczby osób, co do których: 1) sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną, 2) sąd odmówił zarządzenia kontroli i utrwalania rozmów lub kontroli operacyjnej, 3) wniosek o kontrolę operacyjną nie uzyskał zgody prokuratora – z wyszczególnieniem liczby osób w wymienionych kategoriach, co do których o kontrolę operacyjną wnioskował właściwy organ.

29 Zgodnie z art. 19 ust. 22 ustawy o Policji, Minister właściwy do spraw wewnętrznych przedstawia corocznie Sejmowi i Senatowi informację o stosowaniu przez Policję kontroli operacyjnej, a także dane o z informacji dotyczących umów ubezpieczenia, a w szczególności z przetwarzanych przez zakłady ubezpieczeń danych podmiotów, w tym osób, które zawarły umowę ubezpieczenia, a także przetwarzanych przez banki informacji stanowiących tajemnicę bankową.

30 S. Hoc, Glosa do postanowienia SN z 26 kwietnia 2007 r., I KZP 6/07, Ius Novum 2-3/2007, s. 142-149, J. Skorupka, Glosa do postanowienia SN z 26 kwietnia 2007 r., I KZP 6/07, PiP 2/2008, R. Signerski, Glosa do postanowienia SN z dnia 26 kwietnia 2007 r., I KZP 6/07, Lex/el. 2007, D. Szumiło-Kulczycka, Glosa do postanowienia SN z dnia 26 kwietnia 2007 r., I KZP 6/07, Palestra 2008/9-10/303.

31 Por. mi.n uchwałę SN z 23 marca 2011 r. I KZP 32/10.

„Jeśli bowiem w orzecznictwie Trybunału kładziony jest nacisk na konieczność wskazania, wobec jakich przestępstw kontrola ta może być stosowana i na konieczność poddania jej kontroli sądowej, ***to nie można przyjąć interpretacji przepisu art. 19 ust. 15, zgodnie z którą możliwe jest wykorzystanie także materiałów nie dotyczących przestępstw enumeratywnie wskazanych w katalogu*** *i w przypadku których – właśnie ze względu na to, że w katalogu tym się nie znajdują – sąd nie mógłby wydać ani uprzedniej, ani następczej zgody na zarządzenie kontroli operacyjnej. Trybunał wskazał także na niezbędność wykazania konieczności ingerencji (wkroczenia) władz w sferę prywatności i to co do konkretnego – opisanego co do zakresu i sposobu – ograniczenia wprowadzonego w ustawie zwykłej. Uznanie zatem, że można wykorzystać wszelkie dowody zebrane w trakcie kontroli operacyjnej, o ile tylko pozwalają one na wszczęcie jakiegokolwiek postępowania karnego,* ***oznaczałoby, iż w tym wypadku ustawodawca nie wskazał zakresu tej ingerencji****, przyjmując że jest ona możliwa w przypadku każdego przestępstwa.*
(…)
Skoro tak, to jest możliwe wykorzystanie dowodów zebranych w toku kontroli operacyjnej wobec „katalogowego" przestępstwa innej osoby niż objęta postanowieniem sądu oraz wobec osoby tym postępowaniem wprawdzie objętej, ale co do innego przestępstwa „katalogowego" niż wymienione w tym postanowieniu. ***Jednak nie bezwarunkowo****, bowiem nie tylko przynależność jakiegoś przestępstwa do zbioru określonego w katalogu z art. 19 ust. 1 ustawy o Policji umożliwia uznanie przeprowadzonej kontroli operacyjnej za legalną.* ***Warunkiem jest uzyskanie następczej zgody sądu****. Jest ona w tym przypadku konieczna, bowiem cel kontroli operacyjnej określony w art. 19 ust. 1 oraz zasada subsydiarności jej stosowania, wyznaczają dopuszczalny zakres tej kontroli i jednocześnie wskazują, że warunkiem legalności działań podejmowanych w jej ramach jest zgoda sądu wyrażona przed ich przeprowadzeniem lub wyjątkowo, w warunkach określonych w ust. 3, po zarządzeniu kontroli operacyjnej. Pod tymi warunkami zbieranie informacji podczas kontroli, odnoszące się do innej osoby niż objęta postanowieniem sądu oraz do innych przestępstw tej samej osoby, nie będzie wykraczało poza granice legalności tej kontroli, o której zawsze stanowi postanowienie sądu."*

Postanowienie Sądu Najwyższego z dnia 26 kwietnia 2007 r. (sygn. I KZP 6/07)

W omawianym okresie przyjęła się praktyka powierzania przez Prezesa Rady Ministrów nadzoru i koordynacji działań służb specjalnych członkom Rady Ministrów w oparciu o rozporządzenie[32]. Rozwiązanie takie zostało zaskarżone do Trybunału Konstytucyjnego. Argumentacja skarżących wskazywała przede

32 Rozporządzenia Prezesa Rady Ministrów z 24 listopada 2011 r. w sprawie szczegółowego zakresu działania Jacka Cichockiego Członka Rady Ministrów – w zakresie koordynacji służb specjalnych (Dz. U. z 2011 r. Nr 254, poz. 1524), Rozporządzenie Prezesa Rady Ministrów z 28 lutego 2013 r. w sprawie szczegółowego zakresu działania Bartłomieja Sienkiewicza – Ministra Spraw Wewnętrznych w zakresie koordynacji służb specjalnych (Dz. U. poz. 272).

wszystkim na brak podstawy ustawowej do zastosowania takiej konstrukcji prawnej[33]. Ostatecznie postępowanie zostało umorzone ze względu na utratę mocy obowiązującej zaskarżonego rozporządzenia[34]. Również na mocy obecnie obowiązujących przepisów[35] kompetencje nadzorcze premiera zostały przekazane innemu członkowi Rady Ministrów.

Bez wątpienia jednym z najważniejszych judykatów mających bezpośredni wpływ na kształt regulacji służb policyjnych i specjalnych jest wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r. Sprawa zainicjowana przez Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego doprowadziła do uznania przez Trybunał za niekonstytucyjny szereg przepisów dotyczących braku niezależnej kontroli nad pozyskiwaniem przez służby danych telekomunikacyjnych oraz braku odpowiedniej ochrony tajemnic zawodowych w trakcie prowadzenia kontroli operacyjnej. Jednak ogłoszenie wyroku Trybunału poprzedziła kilkuletnia dyskusja na temat ewentualnego kształtu orzeczenia oraz możliwego kształtu ustawy o czynnościach operacyjno-rozpoznawczych jako skutku orzeczenia. Co więcej, utrata mocy obowiązującej przepisów uznanych za niekonstytucyjne została odroczona na 18 miesięcy. Pomimo tak długiego czasu żaden z ośrodków monitorujących kompetencje służb odpowiedzialnych za bezpieczeństwo publiczne (Kolegium ds. służb specjalnych, Ministerstwo Spraw Wewnętrznych, Rada Bezpieczeństwa Narodowego, sejmowa Komisja ds. służb specjalnych) nie wypracował założeń przyszłych zmian w prawie, które mogłyby przyjąć postać reformy dotychczasowego modelu nadzoru nad służbami i realizowanymi przez nie zadaniami. Szczegółowa analiza wypracowanego standardu konstytucyjnego zostanie przedstawiona w dalszej części opracowania.

33 Przedmiotowe rozporządzenie powierzające koordynację nad służbami, zostało zaskarżonego do TK przez grupę posłów. Wnioskodawcy zarzucili tu niekonstytucyjność polegającą na: 1) przekazaniu bez delegacji ustawowej uprawnienia Prezesa Rady Ministrów w zakresie nadzoru i koordynacji nad służbami specjalnymi MSW i podporządkowaniu mu nie podlegających jego nadzorowi na mocy odrębnych ustaw, centralnych organów administracji rządowej (Szefów ABW, AW, SKW, SWW, CBA), 2) przekazaniu MSW, członkowi Kolegium do Spraw Służb Specjalnych, uprawnień i kompetencji Przewodniczącego tego ciała, 3) przekazaniu MSW koordynacji i nadzoru nad działaniami służb zewnętrznych – AW i SKW, 4) powierzeniu MSW, a nie Ministrowi Koordynatorowi Służb Specjalnych uprawnienia do żądania od Szefów: ABW, AW, SKW, SWW, CBA informacji związanych z planowaniem i wykonywaniem powierzonych zadań, 5) powierzeniu MSW, a nie Ministrowi Koordynatorowi Służb Specjalnych uprawnienia do zapewnienia współdziałania służb specjalnych w celu realizacji ich ustawowych zadań z wykroczeniem poza ustawową delegację w zakresie przekazywania tych kompetencji, 6) powierzeniu MSW bez delegacji ustawowej kompetencji Prezesa Rady Ministrów do wyrażania zgody na współdziałanie ABW, AW, CBA z właściwymi organami i służbami innych państw, 7) upoważnieniu bez delegacji ustawowej MSW do zapoznawania się z informacjami mogącymi mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP, a zgromadzonymi przez ABW, AW, SKW, SWW i upoważnieniu go do decydowania, który członek Rady Ministrów ma się z nimi zapoznać, 8) upoważnieniu bez delegacji ustawowej MSW do zapoznawania się z informacjami pełnomocnika do spraw kontroli przetwarzania przez CBA danych osobowych, 9) upoważnieniu MSW bez delegacji ustawowej do zapoznawania się z informacjami z CBA, 10) upoważnieniu MSW bez delegacji ustawowej do zapoznawania się i opiniowania rocznych sprawozdań pełnomocnika do spraw przetwarzania przez CBA danych osobowych, 11) powierzenia bez delegacji ustawowej MSW kompetencji do wyrażania zgody na współdziałania SKW i SWW z właściwymi organami i służbami innych państw, 12) upoważnienia bez delegacji ustawowej MSW do zapoznawania się i analizy oświadczeń o stanie majątkowym Szefa CBA i jego zastępców, 13) upoważnienia bez delegacji ustawowej MSW do dokonywania uzgodnień, o których mowa w art. 36 ust. 3 ustawy o CBA, 14) przekazanie bez delegacji ustawowej MSW uprawnienia do dokonywania czynności wynikających ze stosunku służbowego wobec Szefów: ABW, AW, CBA, 15) powierzenia obsługi MSW w zakresie w rozporządzeniu wskazanym, Kancelarii Prezesa Rady Ministrów. TK ostatecznie umorzył postępowanie w sprawie z uwagi na uchylenie przedmiotowego rozporządzenia.

34 Postanowieniem o umorzeniu z dnia 20 marca 2013 r. (sygn. U 3/12).

35 Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych (Dz. U. Poz. 1921).

2.4. Zmiany wprowadzone w 2016 r.

Odrębnego omówienia wymagają zmiany uchwalone i wprowadzone w życie w I kwartale 2016 r. Przede wszystkim uchwalono **ustawę z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw**[36] mającą na celu wykonanie wyroku TK z 30 lipca 2014 r. (sygn. K 23/11). Próby wykonania wyroku podjęto jeszcze w trakcie VII kadencji Sejmu[37], jednak nie zostały one ukończone przed końcem kadencji.

Ostatecznie ustawa ta dookreśliła[38] oraz rozbudowała[39], w przypadku niektórych służb, katalogi przestępstw, w ramach ścigania, wykrywania, zapobiegania, możliwe jest stosowanie kontroli operacyjnej. Ponadto w ustawie nastąpiła zmiana zakresu przedmiotowego środków możliwych do stosowania w ramach kontroli operacyjnej.

Formy kontroli operacyjnej (na gruncie m.in. ustawy o Policji) do 6 lutego 2016 r.	Zakres kontroli operacyjnej zaproponowany z senackim projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (lipiec 2016 r.)	Zakres kontroli operacyjnej na podstawie ustawy z 15 stycznia 2016 r. (obowiązuje od 7 lutego 2016 r.)
1. kontrolowanie treści korespondencji; 2. kontrolowanie zawartości przesyłek; 3. stosowanie środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.	1. podsłuch rozmów prowadzonych przy użyciu środków technicznych; 2. podsłuch i podgląd pomieszczeń i osób poza miejscami publicznymi; 3. kontrola treści korespondencji 4. nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu; 5. kontrola zawartości przesyłek.	1. uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; 2. uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; 3. uzyskiwanie i utrwalanie treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; 4. uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; 5. uzyskiwaniu dostępu i kontroli zawartości przesyłek.

36 Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

37 Senacki projekt ustawy o o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967, druk sejmowy nr 3765) Por. Opinie HFPC do projektu ustawy: na etapie prac w Senacie - http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/07/druk967opiniaK2311.pdf oraz po skierowaniu ustawy do Sejmu – http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/09/opinia-26-08-15-KSW-Sejm-3765.pdf.

38 W przypadku ustawy o ABW oraz AW w art. 27 ust. 1 ustawodawca zakreślił katalog przestępstw godzących w podstawy ekonomiczne państwa, jednak nie zmienił jednak art. 5 ustawy dotyczącego zadań ABW, a tym samym – pośrednio – podstaw pozyskiwania danych telekomunikacyjnych czy internetowych.

39 W przypadku CBA, podstawy stosowania kontroli operacyjnej zostały poszerzone o ściganie przestępstw z art. 305 k.k. (utrudnianie przetargu publicznego).

W ustawie wprowadzono regulację pozyskiwania tzw. danych internetowych na zasadach analogicznych do pozyskiwania danych telekomunikacyjnych i pocztowych[40]. Wreszcie wprowadzony został obowiązek przekazania sądom okręgowym statystycznej informacji o przypadkach przekazania niektórych danych telekomunikacyjnych, internetowych oraz pocztowych i fakultatywnej kontroli sądowej nad pozyskiwaniem tych danych[41]. Zdaniem projektodawców procedura ta stanowi formę kontroli sądowej nad pozyskiwaniem danych telekomunikacyjnych czy internetowych przez służby, a tym samym wypełnia obowiązek wynikający z wyroku Trybunału z 30 lipca 2014 r. Podstawowe zastrzeżenia formułowane wobec takiego rozwiązania dotyczą tego, na ile takie rozwiązanie stanowi zapewnienie skutecznej kontroli nad czynnością operacyjną służb, jaką jest pozyskiwanie danych telekomunikacyjnych. Fakultatywny charakter kontroli w połączeniu z zagregowanym i statystycznym charakterem przedstawianych sprawozdań[42] może uniemożliwiać dostrzeżenie przez sąd ewentualnych naruszeń prawa. Ponadto, zgodnie z art. 20ca ust. 4 ustawy o Policji przewiduje, że sąd informuje organ Policji o wyniku kontroli. Ustawa nie przyznaje sądom kompetencji np. do nakazania zniszczenia danych uzyskanych niezgodnie z prawem[43].

Istotne znaczenie z punktu widzenia czynności operacyjno-rozpoznawczych prowadzonych przez służby ma uchwalona 28 stycznia 2016 r. ustawa - **Prawo o prokuraturze**. Oprócz wspomnianego obowiązku informowania o ilości przypadków, w których zastosowano kontrolę operacyjną, ustawa przewiduje, że prokurator (również Prokurator Generalny oraz Krajowy) sprawuje kontrolę nad czynnościami operacyjno-rozpoznawczymi w oparciu o rozporządzenie Ministra Sprawiedliwości[44]. Ponadto, Prokurator Generalny może zwrócić się o przeprowadzenie czynności operacyjno-rozpoznawczych podejmowanych przez właściwe uprawnione organy, „jeżeli pozostawałyby one w bezpośrednim związku z toczącym się postępowaniem przygotowawczym". Ustawa przyznała Prokuratorowi Generalnemu możliwość zapoznania się z materiałami z czynności operacyjno-rozpoznawczych, a także w szczególnie uzasadnionych przypadkach możliwość znoszenia lub zmiany klauzuli tajności na potrzeby prowadzonego postępowania karnego, po zasięgnięciu opinii tego organu i poinformowaniu o takim zamiarze Prezesa Rady Ministrów. W uzasadnieniu tej zmiany wskazuje się, iż stanowi ona reakcję na problemy w zakresie

40 Ustawa ta wprowadziła pojęcie tzw. danych internetowych – poprzez odesłanie do przepisów art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844) i wprowadziła możliwość ich pozyskiwania na zasadach analogicznych do danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, ze zm.), a także danych pocztowych, o których mowa w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830).

41 Zgodnie z art. 20ca ustawy o Policji kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.

42 W świetle art. 20ca ustawy o Policji, organ Policji przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, w okresach półrocznych, sprawozdanie obejmujące: 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych; 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

43 Por.: opinia HFPC dotycząca poselskiego projektu ustawy o zmianie ustawy o Policji (druk sejmowy nr 154) – http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/12/HFPC_opinia_ustawa_o_policji.pdf; opinia Fundacji „Panoptykon" - https://panoptykon.org/wiadomosc/sluzby-wciaz-poza-kontrola-zmarnowana-szansa-na-dobra-zmiane.

44 Na podstawie art. 36 § 4 Prawa o prokuraturze, Minister Sprawiedliwości określi w drodze rozporządzenia, sposób realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi określonymi w art. 57 § 2, mając w szczególności na uwadze zapewnienie merytorycznej i efektywnej kontroli podstaw faktycznych wnioskowanych czynności, zapewnienie legalności i prawidłowości inicjowania i przeprowadzania tych czynności oraz konieczność poszanowania podstawowych praw i wolności obywatelskich. Rozporządzenie nadal nie zostało opublikowane.

ochrony informacji niejawnych pomiędzy prokuraturą a innymi organami władzy publicznej[45]. Tak istotne poszerzenie kompetencji Prokuratora Generalnego nie zostało obwarowane żadnymi gwarancjami niezależności Prokuratora Generalnego (tj. Ministra Sprawiedliwości). Co więcej, Prokurator Generalny, będzie mógł przedstawić informacje dotyczące konkretnych spraw również „innym osobom" (tj. nie pełniącym funkcji w ramach organów władzy publicznej), jeżeli informacje takie mogą być istotne dla bezpieczeństwa państwa. Nad taką kompetencją ustawa nie przewiduje żadnej kontroli[46].

Istotne zmiany w zakresie czynności operacyjno-rozpoznawczych wprowadziła również kolejna nowelizacja procedury karnej. Ustawa z 11 marca 2016 r. **o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw[47]** zmieniła regułę dowodową określoną w art. 168a k.p.k.

Art. 168a k.p.k. od 1 lipca 2015 r.	Art. 168a k.p.k. od 15 kwietnia 2016 r.
„Niedopuszczalne jest przeprowadzenie i wykorzystanie dowodu uzyskanego do celów postępowania karnego za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego."	*„Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności."*

Projekt zmian w procedurze karnej pojawił się pół roku po wejściu w życie poprzedniej obszernej nowelizacji kodeksu postępowania karnego. Pierwotnie projektodawca[48] zakładał całkowite usunięcie art. 168a wprowadzonego ustawą z września 2013 r.[49] argumentując, że przepis ten prowadzi w automatyczny sposób do usuwania z procesu karnego istotnych dowodów. Nie wskazano przy tym na żadne orzecznictwo sądowe, które w tak krótkim czasie nie miało nawet szansy zostać wypracowane. Ostatecznie zdecydowano się na zmianę brzmienia art. 168a k.p.k., który całkowicie odwraca jego pierwotne znaczenie i cel. Nowe brzmienie art. 168a k.p.k. zakazuje uznania przez sąd dowodu za niedopuszczalny na tej podstawie, że został uzyskany nielegalnie. Nie będzie tym samym możliwe uznanie dowodu za niedopuszczalne z powodu uzyskania go np. przy jednoczesnym przekroczeniu uprawnień przez funkcjonariusza publicznego. W tym sensie, przepis prowadzi do konstatacji, że nawet dowody nielegalne będą musiały zostać przez sąd uznane za dopuszczalne, a tym samym wzięte pod uwagę przy rozstrzyganiu zawisłej sprawy[50]. To z kolei może skutkować uznaniem całego postępowania za naruszającego zasady rzetelności, m.in. na gruncie art. 6 Europejskiej Konwencji Praw Człowieka[51].

45 Por. uzasadnienie rządowego projektu ustawy – Prawo o prokuraturze (druk sejmowy nr 162, Sejm VIII kadencji) dostępne pod adresem: http://orka.sejm.gov.pl/Druki8ka.nsf/0/8318081684D46B25C1257F2B002F31CC/%24File/162.pdf.

46 Twórcy projektu ustawy – Prawo o prokuraturze wychodzą z założenia, że wystarczająca dla sprawnego działania prokuratury jest kontrola parlamentarna.

47 Ustawa z 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 437).

48 Druk sejmowy nr 207.

49 Ustawa z dnia 27 września 2013 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. Poz. 1247, ze zm.)

50 Wystąpienie HFPC do Marszałka Sejmu z 26 lutego 2016 r. dostępne na stronie: http://www.hfhr.pl/wp-content/uploads/2016/02/HFPC_wystapienie_Marszalek_Sejmu_260202016.pdf.

51 Por. Wniosek Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego z 6 maja 2016 r. (sygn. K 27/16).

Ponadto ustawa ta dodała art. 168b k.p.k. Przepis ten stanowi, że *„jeżeli w wyniku kontroli operacyjnej zarządzonej na wniosek uprawnionego organu na podstawie przepisów szczególnych uzyskano dowód popełnienia przez osobę, wobec której kontrola operacyjna była stosowana, innego przestępstwa ściganego z urzędu lub przestępstwa skarbowego niż przestępstwo objęte zarządzeniem kontroli operacyjnej lub przestępstwa ściganego z urzędu lub przestępstwa skarbowego popełnionego przez inną osobę niż objętą zarządzeniem kontroli operacyjnej,* ***prokurator podejmuje decyzję*** *w przedmiocie wykorzystania tego dowodu w postępowaniu karnym."* Zmiana ta oznacza rezygnację z obowiązku uzyskiwania zgody następczej sądu na wykorzystanie materiałów z kontroli operacyjnej[52]. Jest to zatem wyraźne odejście od linii orzeczniczej zapoczątkowanej postanowieniem SN z 26 kwietnia 2007 r. I KZP 6/07. Jest to niepokojące przede wszystkim z uwagi na fakt, że standard wyrażony w tym orzeczeniu został oparty o prokonstytucyjną wykładnię przepisów ustawy o Policji. Istnieje tym samym duże prawdopodobieństwo, że wprowadzona zmiana pozostawiająca decyzję prokuratorowi nie wyposażonego w niezawisłość (oraz z poważnym ograniczeniem gwarancji niezależności) narusza konstytucyjny standard ochrony jednostki przed inwazyjnymi (potencjalnie nielegalnymi w świetle art. 168a k.p.k.) działaniami państwa.

Twórcy poprawki rządowej wprowadzającej tę zmianę, wskazują, że zainicjowanie kontroli i utrwalania rozmów, o której mowa w k.p.k., oraz kontroli operacyjnej ma miejsce w ściśle określonych wypadkach i wymaga zarządzenia sądu, gdyż stanowi ingerencję w gwarantowane konstytucyjnie prawo do prywatności. W związku z tym wskazują, że nie ma potrzeby limitować dostępu do środków dowodowych dla organów ścigania. Jako dodatkowe argumenty wskazują, iż niewątpliwie przyczyni się to do zwiększenia skuteczności ścigania przestępczości, wzmocnienia zasady swobodnej oceny dowodów. Podkreślają także, że zgoda następcza nie jest powszechnie znana w innych państwa UE, a raczej należy do wyjątków.

2.5. Projekt ustawy o działaniach antyterrorystycznych

W trakcie prac legislacyjnych nad ustawą z 15 stycznia 2016 r. nie przeprowadzono konsultacji społecznych. Jak zapewniał przedstawiciel Rządu w styczniu 2016 r., konsultacje takie miały zostać przeprowadzone w ramach planowanych prac nad tzw. ustawą antyterrorystyczną. Niestety Rządowi nie udało się dotrzymać złożonej obietnicy. Bezpośrednio po ataku terrorystycznym, który miał miejsce w marcu 2016 r. w Brukseli, Rząd ogłosił, że ustawa terrorystyczna zostanie pospiesznie uchwalona. Po miesiącu tajnych prac legislacyjnych w ramach Rady Ministrów, w maju 2016 r. został skierowany do Sejmu projektu ustawy o działaniach antyterrorystycznych[53].

Projekt przewiduje m.in. możliwość prowadzenia kontroli operacyjnej wobec cudzoziemców bez zgody sądu przez 3 miesiące. Projekt przyznaje również kompetencję Ministrowi Spraw Wewnętrznych do określenia katalogu zdarzeń o charakterze terrorystycznym[54]. Ustawa poszerza uprawnienia Szefa ABW (m.in. w zakresie dostępu do danych osobowych czy też uprawnień w zakresie zwalczania tzw. cyberprzestępczości), nie tworząc żadnego mechanizmu niezależnej kontroli nad sposobem wykonywania tych kompetencji.

52 Art. 4-6, 12-13, 17-18 ustawy z 11 marca 2016 r. uchylały odpowiednie przepisy regulujące procedurę tzw. zgody następczej.

53 Rządowy projekt ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw (druk sejmowy nr 516).

54 W świetle projektu rozporządzenia dołączonego do ustawy wydarzeniem takim będzie m.in. wizyty w polskich zakładach penitencjarnych islamskich duchownych bądź przedstawicieli organizacji zrzeszających osoby tego wyznania czy informacje na temat planów utworzenia w naszym kraju uczelni islamskich.

Prace nad ustawą antyterrorystyczną stanowią kolejny przykład na to, w jaki sposób prowadzone są prace legislacyjne w zakresie regulacji uprawnień służb policyjnych i specjalnych. Zdiagnozowane wcześniej braki w zakresie zapewnienia odpowiedniej kontroli nad całością niejawnej działalności służb zostały całkowicie zignorowane z uwagi na blankietowe zagrożenie dla bezpieczeństwa. Korzystanie z uprawnień najbardziej ingerujących w prawa i wolności zostało pozostawione decyzji egzekutywy.

2.6. Projekty zmian legislacyjnych, które nie zostały uchwalone

W ostatnich 20 latach podjęto kilka inicjatyw mających na celu dokonanie zmian w zakresie kompetencji służb, jak i mechanizmów kontroli nad nimi. Podstawowe znaczenie mają podejmowane kilkukrotnie próby opracowania ustawy o czynnościach operacyjno-rozpoznawczych, które jednak nigdy nie zostały zakończone uchwaleniem takiej regulacji. Na skutek tego, co pewien czas, przy różnych okazjach pojawiały się pomysły cząstkowych zmian obowiązujących przepisów w zakresie działalności służb[55].

2.6.1. Projekty rządowe

W omawianym okresie zwrócić należy uwagę na kilka rządowych projektów zmian legislacyjnych, dotyczących problematyki funkcjonowania służb, które nie doczekały się uchwalenia.

W pierwszej kolejności wskazać należy na projekt ustawy o zmianie ustawy o Policji[56]. Zakładał on przede wszystkim rozszerzenie katalogu przestępstw, w ramach ścigania których można byłoby stosować kontrolę operacyjną, zakup kontrolowany i przesyłkę niejawnie nadzorowaną. Ponadto przewidywał zmianę zakresu środków stosowanych w ramach kontroli operacyjnej o: *„stosowanie środków elektronicznych umożliwiających niejawne i zdalne uzyskanie dostępu do zapisu na informatycznym nośniku danych, treści przekazów nadawanych i odbieranych oraz ich utrwalanie"*. Wreszcie projektował uniezależnienie CBŚ w zakresie stosowania czynności operacyjno – rozpoznawczych od Komendanta Głównego Policji. Ostatecznie projekt ten nie trafił pod obrady Sejmu, jednakże częściowo propozycje w nim zawarte w późniejszym czasie zostały wykorzystane w ramach prac nad innymi propozycjami legislacyjnymi[57].

Warto też zwrócić uwagę na rządowe projekty ustaw: o Agencji Bezpieczeństwa Wewnętrznego (druk sejmowy nr 2295) oraz o Agencji Wywiadu (druk sejmowy nr 2294)[58]. Zakładały one rozdzielenie regulacji dotyczącej ABW oraz AW, przy czym propozycje w ok. 90 % powielały rozwiązania już obowiązujące w ustawie o ABW oraz AW. Ponadto projekt ustawy o ABW przewidywał zastąpienie Kolegium do Spraw Służb Specjalnych przez ograniczony osobowo Komitet Rady Ministrów ds. Bezpieczeństwa Państwa,

55 Por.: J. Kudła, *Wybrana problematyka czynności operacyjnych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno – rozpoznawczych*, Z. Rau, Czynności operacyjno – rozpoznawcze w polskim systemie prawa – działania w kierunku uniwersalnej ustawy (w:) Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu Nowoczesne technologie i praca operacyjna red. L. Paprzycki, Z. Rau, Warszawa 2009.

56 Projekt w brzmieniu z dnia 26 sierpnia 2009 r. Dostępny pod adresem: http://www.hfhrpol.waw.pl/precedens/images/stories/file/ustawa_Policja.pdf.

57 Dla przykładu tak stało się z pomysłem wyraźnego rozdzielenia możliwości stosowania przez CBŚ kontroli operacyjnej.

58 Opinia Helsińskiej Fundacji Praw Człowieka dotycząca projektów ustawy o ABW, o AW oraz Komisji Kontroli Służb Specjalnych dostępna pod adresem: http://bip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2013/22523,Projekt-ustawy-z-dnia-2013-r-o-Komisji-Kontroli-Sluzb-Specjalnych.html.

powoływany w drodze zarządzenia Prezesa Rady Ministrów i rezygnacja ze stanowiska Ministra – Koordynatora do Spraw Służb Specjalnych. Jednakże w przypadku obu projektów prace nad nimi nie doszły nawet do II czytania w Sejmie.

Wreszcie zwrócić należy uwagę na rządowy **projekt ustawy o Komisji Kontroli Służb Specjalnych**. Przewidywał on powołanie Komisji Kontroli Służb Specjalnych[59], właściwej w sprawach: 1) kontroli zgodności działania ABW, AW, CBA, SKW i SWW z Konstytucją RP i ustawami, w szczególności w kwestii praw i wolności obywatelskich, a także innymi przepisami prawa w zakresie wykonywania czynności operacyjno – rozpoznawczych i przetwarzania danych osobowych obywateli RP, uzyskiwania i przetwarzania danych telekomunikacyjnych i pocztowych, 2) kontroli prawidłowości realizacji postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, 3) odwołań od decyzji o odmowie lub cofnięciu poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego albo od decyzji o umorzeniu postępowania sprawdzającego, 4) skarg na działanie służb specjalnych, 5) oceny aktów prawa wewnętrznego służb specjalnych. Projekt nie został jednak skierowany do Sejmu.

Przykład ww. projektów rządowych i niepowodzeń w pracach nad nimi dowodzi tego, że niepowodzenia prac nad tymi projektami należy upatrywać w zmianach koncepcji w Radzie Ministrów w zakresie tego, jak powinny działać służby.

2.6.2. Projekty poselskie

Wśród poselskich projektów dotyczących podstaw działalności służb wskazać trzeba na tożsame projekty **ustawy o czynnościach operacyjno – rozpoznawczych** (druk sejmowy nr 1570, Sejm V kadencji i druk sejmowy nr 353, Sejm VI kadencji). Projekt ten realizował koncepcję uchwalenia jednej ustawy o działalności operacyjnej, albowiem przenosił on materię czynności operacyjno – rozpoznawczych prowadzonych przez różne służby do jednej ustawy. Projekt proponował wprowadzenie pojęcia czynności operacyjno – rozpoznawczych, a zatem wychodził naprzeciw postulatom doktryny w tym zakresie. Czynności operacyjno-rozpoznawcze proponowano zdefiniować jako zespół przedsięwzięć, jawnych i niejawnych prowadzonych wyłącznie w celu: 1) rozpoznania, zapobiegania i wykrywania przestępstw; 2) odnajdywania osób ukrywających się przed organami ścigania lub wymiarem sprawiedliwości oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginięcie jest wynikiem przestępstwa, a także odnajdywanie rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem; 3) ustalenia tożsamości osób i zwłok, w przypadku uzasadnionego podejrzenia przestępczego działania. W projekcie proponowano także dookreślenie form i metod prowadzenia tych czynności[60]. Ponadto projekt regulował zasady prowadzenia i dokumentowania czynności operacyjno – rozpoznawczych[61]. Mimo szerokich dyskusji środowiskowych prace nad żadnym z projektów nie wyszły poza prace komisyjne[62].

59 W jej skład miało wejść 6 członków powoływanych przez Sejm, posiadających co najmniej 10-letnie doświadczenie w zakresie wymiaru sprawiedliwości, kontroli państwowej lub ochrony praw człowieka, powoływanych na 6 letnią kadencję, przy czym co 2 lata następować miała rotacja w jej składzie.

60 Por. art. 2 ust. 2 i 3 projektu.

61 Por. Rozdział II i III projektu.

62 Pierwsze czytanie miało miejsce w dniu 30 marca 2007 r. Prace nad projektem zakończyły się na etapie komisyjnym wraz ze skróceniem kadencji Sejmu. Pierwsze czytanie odbyło się 27 maja 2008 r. Prace zakończyły się na etapie komisyjnym.

2.6.3. Projekty senackie

Senat jako odpowiedzialny z mocy art. 85a i następnych Regulaminu Senatu za wykonywanie orzeczeń Trybunału Konstytucyjnego podjął kilka inicjatyw zmierzających do wprowadzenia zmian w przepisach dotyczących uprawnień służb policyjnych, specjalnych i skarbowych. Szerszego zasygnalizowania wymagają co najmniej trzy z nich.

W 2009 r. Komisja Ustawodawcza skierowała do Marszałka Senatu projekt ustawy o zmianie ustawy o Policji (druk senacki nr 730, Senat VII kadencji)[63], który stanowił próbę wykonania postanowienia sygnalizacyjnego TK z 25 stycznia 2006 r. (sygn. S 2/06), wydanego w następstwie wyroku TK z 12 grudnia 2005 r. (sygn. K 32/04). Ww. projekt senacki przewidywał wprowadzenie w ustawie o Policji przepisu art. 19 ust. 16a, który wykonywałby postanowienie sygnalizacyjne S 2/06.

> *„Organ Policji, który wnioskował o zarządzenie kontroli operacyjnej, po jej zakończeniu w przypadku nieuzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego, informuje osobę, wobec której kontrola była stosowana o jej przeprowadzeniu. Informacja wskazuje cel, zakres oraz wyniki przeprowadzonej kontroli operacyjnej."*
>
> Art. 19 ust. 16a ustawy o Policji w brzmieniu zaproponowanym w projekcie ustawy o zmianie ustawy o Policji (druk senacki nr 730, Senat VII kadencji)

Jednakże pod wpływem krytyki szczególnie ze strony Policji, w dniu 11 maja 2010 r. Komisja Ustawodawcza Senatu RP na posiedzeniu wycofała projekt spod rozpatrzenia.

Kolejnym projektem senackim, był projekt ustawy o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk sejmowy nr 636, Sejm VII kadencji). Projekt ten w dniu 9 lipca 2012 r. został zarejestrowany jako druk sejmowy nr 636 i skierowany na I czytanie do Komisji Spraw Wewnętrznych, z której już nie wyszedł. Stanowił on próbę wykonania postanowienia sygnalizacyjnego TK z dnia 15 października 2010 r. (sygn. S 4/10), wydanego w następstwie postanowienia o umorzeniu postępowania z dnia 4 października 2010 r. (sygn. P 79/08). W tej sprawie TK umorzył postępowanie w sprawie konstytucyjności przepisów art. 5 ust. 1 pkt 2 lit. b w związku z art. 27 ust. 1, art. 27 ust. 15, a także art. 27 ust. 11a ustawy

63 Projekt dostępny pod adresem: http://ww2.senat.pl/k7/dok/dr/700/730.pdf.

o ABW oraz AW[64]. TK umorzył postępowanie z przyczyn formalnych i jednocześnie wystosował postanowienie sygnalizacyjne. Trybunał wskazał, że z zaskarżonych przepisów nie wynika, w związku z jakim typem przestępstwa, określonego przez ustawę karną, sąd zarządza kontrolę operacyjną, gdy powołuje się na zadania ABW – w zakresie rozpoznawania, zapobiegania i wykrywania „przestępstw godzących w podstawy ekonomiczne państwa".

Wreszcie wspomnieć należy o senackim projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 3765, Sejm VII kadencji). Stanowił on próbę wykonania wyroku TK z dnia 30 lipca 2014 r. (sygn. K 23/11). W wersji, która trafiła do Sejmu przewidywał m.in.: 1) doprecyzowanie katalogu środków stosowanych w ramach kontroli operacyjnej i wyraźne ich odróżnienie od obserwacji w pomieszczeniach, jak i pozyskiwania danych telekomunikacyjnych, 2) wprowadzenie mechanizmu weryfikacji, czy zgromadzone w ramach kontroli operacyjnej dane zawierają tajemnice zawodowe, prawnie chronione, 3) wprowadzenie obowiązku sprawozdawczego o przypadkach pozyskiwania danych telekomunikacyjnych. Projekt trafił do Sejmu w dniu 29 lipca 2015 r., a 5 sierpnia 2015 r. odbyło się I czytanie. Prace nad projektem zakończyły się wraz z końcem prac Sejmu VII kadencji.

2.7. Podsumowanie

W świetle powyższych kierunków zmian, trudno uznać, że zmiany legislacyjne w zakresie służb wprowadzane w okresie ostatnich 20 latach realizowały klarowną koncepcją dotyczącą służb policyjnych i specjalnych. Z analizy ww. projektów wynika, że ustawodawca próbował dążyć do poszerzania kompetencji służb (np. nowelizacja z 15 stycznia 2016 r.), być może nie zawsze skutecznie (np. rządowy projekt ustawy o Policji z 2009 r.). W zakresie kontroli nad działalnością służb mówić należy o pewnym utrzymywaniu istniejącego stanu, w którym to na sądy i prokuratury przerzucona została odpowiedzialność za kontrolę służb. Jednocześnie też skutecznie udawało się wstrzymywać prace nad projektami zwiększającymi kontrolę nad służbami. Przykładem są tu próby umożliwienia jednostkom udziału w sądowo-prokuratorskich procedurach zarządzania czynności operacyjno-rozpoznawczych. Stąd też niepowodzenie senackiego projektu nr 730. Niestety, pomimo braku zmian podwyższających poziom kontroli nad służbami, ustawodawca w dalszym ciągu poszerza uprawnienia służb (np. projekt ustawy antyterrorystycznej).

64 Pierwszy z tych przepisów przewidywał, że do zadań ABW należy rozpoznawanie, zapobieganie i wykrywanie przestępstw „godzących w podstawy ekonomiczne państwa", przy czym na podstawie art. 27 ust. 1 ustawy o ABW realizacja tego zadania była możliwa przy użyciu kontroli operacyjnej. Problem polegał jednak na tym, że ten katalog przestępstw był nieprecyzyjny. Drugi z przepisów został zaskarżony w zakresie, w jakim nie formułował taksatywnego i konkretnego katalogu przestępstw, jakich dotyczy obowiązek przekazania materiałów uzyskanych w toku czynności operacyjnych oraz regulował obowiązek przekazania materiałów uzyskanych w toku czynności operacyjnych niezależnie od: 1) zakresu kompetencji przyznanych Agencji Bezpieczeństwa Wewnętrznego w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, 2) przestrzegania rygorów warunkujących stosowanie środków techniki operacyjnej co umożliwia wykorzystanie materiałów niejawnych dotyczących przestępstw innych niż wskazane w postanowieniu wydanym na podstawie art. 27 ust. 1 ustawy, bądź przestępstw popełnionych przez inne osoby niż wskazane w postanowieniu wydanym na podstawie art. 27 ust. 1 ustawy oraz dotyczących niedookreślonego katalogu przestępstw. Trzeci z przepisów został zaskarżony w zakresie, w jakim nie przewidywał kontroli instancyjnej postanowień sądu w przedmiocie zarządzenia kontroli operacyjnej wydanych na podstawie art. 27 ust. 1 o ABW oraz AW i możliwości zaskarżenia postanowień sądu przez strony postępowania karnego.

3. Niejawne pozyskiwanie informacji o obywatelach – standard konstytucyjny ustanowiony przez Trybunał Konstytucyjny i jego realizacja w obowiązujących przepisach

W wyroku z 30 lipca 2014 r. (sygn. K 23/11) Trybunał Konstytucyjny określił minimalne wymagania, dotyczące przepisów regulujących niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach. Doniosłość tego orzeczenia każe zaprezentować poniżej te wymogi, z jednoczesnym odniesieniem się do aktualnego poziomu ich realizacji w ramach obowiązującego ustawodawstwa. Standard konstytucyjny został zrekonstruowany przez Trybunał Konstytucyjny w oparciu o dotychczasowe orzecznictwo Trybunału, jak również o bogate orzecznictwo Europejskiego Trybunału Praw Człowieka. Podstawowy mankament ustawy z 15 stycznia 2016 r. wykonującej ten wyrok polegał na założeniu, że wykonanie wyroku może ograniczyć się do zmiany przepisów wskazanych w sentencji wyroku, z jednoczesnym pominięciem wytycznych wynikających z uzasadnienia.

1. Gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, dopuszczalne jest wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy.

W dużej mierze standard ten jest realizowany w praktyce, przy czym zauważyć należy, że w projekcie ustawy o działaniach antyterrorystycznych, proponuje się obniżenie jego poziomu ochrony. Przykładem tego jest propozycja zawarta w projekcie ustawy antyterrorystycznej przyznającej władzy wykonawczej kompetencje do prowadzenia (w formie aktów podustawowych oraz aktów prawa wewnętrznego) różnego rodzaju wykazów (np. zdarzeń terrorystycznych, osób związanych ze zdarzeniami o charakterze terrorystycznych), które miałyby bezpośredni wpływ na prawa i wolności. Co więcej, w drodze analogicznych aktów prawnych określany miałby być zakres informacji gromadzonych w takich wykazach oraz sposob pozyskiwania informacji z tych wykazów[65].

2. Konieczne jest precyzyjne określenie w ustawie organów państwa upoważnionych do gromadzenia oraz przetwarzania danych o jednostce, w tym do stosowania czynności operacyjno-rozpoznawczych.

Wydaje się, że standard ten jest realizowany – zarówno w prawie, jak i w praktyce jego stosowania, przy czym problematyczny w tym kontekście może być przede wszystkim brak definicji czynności operacyjno-rozpoznawczych w polskim ustawodawstwie.

3. W ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi są: wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im. Ustawa powinna wskazywać rodzaje takich przestępstw.

Wymóg ten jedynie połowicznie został zrealizowany w drodze uchwalenia ustawy z 15 stycznia 2016 r. Ustawa ta z jednej strony wprowadziła w ustawie o ABW oraz AW oraz ustawie o ŻW bardziej precyzyjny katalog przestępstw, których ściganie jest zadaniem odpowiednio ABW oraz ŻW. Jednakże w dalszym ciągu,

65 Art. 6 ust. 4 przewiduje, że Szef ABW określi, w drodze zarządzenia, z uwzględnieniem wymogów dotyczących ochrony informacji niejawnych: 1) zakres informacji gromadzonych w wykazie osób „niebezpiecznych", o którym mowa w art. 6 ust. 1 ustawy; 2) sposób prowadzenia wykazu; 3) tryb uzyskiwania informacji z wykazu przez podmioty uprawnione.

podstawa sięgania przez Policję po np. dane telekomunikacyjne czy internetowe jest zarysowana bardzo szeroko i obejmuje: zapobieganie lub wykrywanie przestępstw, ratowanie życia lub zdrowia ludzkiego, wsparcie działań poszukiwawczych. Ponadto nowelizacja k.p.k. z 11 marca 2016 r. znosząc instytucję zgody następczej, wprowadza możliwość wykorzystywania informacji zdobytej w drodze podsłuchu w postępowaniu karnym o każdym w zasadzie przestępstwie ściganym z urzędu[66].

W przypadku pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych, podejmowanie tego typu działań możliwe jest natomiast w celu szeroko rozumianej realizacji „ustawowych zadań", np. w przypadku służb specjalnych[67].

4. Ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze

W polskim ustawodawstwie przyjęło się regulować tę kwestię w sposób nieograniczony. Nie ma zatem żadnych generalnych wyłączeń dotyczących ograniczenia możliwości stosowania kontroli operacyjnej wobec dziennikarzy czy obrońców. Wskazuje się przy tym na argument dotyczący równości wobec prawa oraz okoliczność, że przedstawiciele zawodów zaufania publicznego również mogą być podejrzani o popełnienie przestępstw. Ustawa z 15 stycznia 2016 r. wykonując wyrok Trybunału wprowadziła specjalną procedurę dotyczącą informacji zgromadzonych w trakcie prowadzenia kontroli operacyjnej, które mogą stanowić jedną z tajemnic prawnie chronionych[68]. Procedura przewiduje obowiązek niszczenia zgromadzonych informacji, które stanowią tajemnicę spowiedzi oraz tajemnicą obrończą. W przypadku pozostałych tajemnic (adwokacka, dziennikarska) szef służby musi przekazać zgromadzone materiały prokuratorowi, który nie może podjąć żadnych decyzji w przedmiocie tych informacji, a który został zobligowany do ich przekazania sądowi wraz z wnioskiem o dopuszczenie do wykorzystania w postępowaniu karnym. Podstawową przesłanką, którą sąd bierze pod uwagę jest fakt, iż wykorzystanie materiału jest „niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu". Kształt tej procedury zdaje się wskazywać, że jej głównym celem jest przede wszystkim umożliwienie wykorzystania zgromadzonych informacji w ramach postępowania karnego.

Tymczasem, wyrok Trybunału uznał obowiązujące dotychczas przepisy za niekonstytucyjne „w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne". Trybunał ustanawiając standard konstytucyjny bazował zatem na kodeksowej procedurze zwolnienia z tajemnicy przewidzianej w art. 180 k.p.k. Natomiast ustawodawca literalnie odczytując sentencję wyroku wprowadził do przepisów regulujących pracę operacyjną procedurę analogiczną do rozwiązań kodeksowych, nie dostrzegając wszystkich wyzwań

66 Art. 168b k.p.k.: *Jeżeli w wyniku kontroli operacyjnej zarządzonej na wniosek uprawnionego organu na podstawie przepisów szczególnych uzyskano dowód popełnienia przez osobę, wobec której kontrola operacyjna była stosowana,* ***innego przestępstwa ściganego z urzędu*** *lub przestępstwa skarbowego niż przestępstwo objęte zarządzeniem kontroli operacyjnej lub* ***przestępstwa ściganego z urzędu*** *lub przestępstwa skarbowego popełnionego przez inną osobę niż objętą zarządzeniem kontroli operacyjnej, prokurator podejmuje decyzję w przedmiocie wykorzystania tego dowodu w postępowaniu karnym.*

67 Por. art. 18 ust. 1 ustawy o CBA, art. 28 ust. 1 ustawy o ABW oraz AW.

68 Por. art. 19 ust. 15f – 15j ustawy o Policji.

z tym związanych[69]. Żadnej natomiast procedury chroniącej np. tajemnicę dziennikarską nie przewidziano w zakresie pozyskiwania przez służby danych telekomunikacyjnych czy internetowych.

Innymi słowy, czynności operacyjno – rozpoznawcze mogą być stosowane wobec każdej jednostki, czy też osoby prawnej. Wynika to również z tego, że nie ma w obowiązujących przepisach cezury czasowej, ograniczającej możliwość ich stosowania już po wszczęciu postępowania karnego[70]. Brak jest w tym zakresie np. obowiązku skorzystania po wydaniu postanowienia o wszczęciu postępowania karnego, z analogicznych do czynności operacyjno-rozpoznawczych, instytucji procesowych. Powoduje to także istotne zaniżenie poziomu ochrony praw jednostki, która nie może korzystać z przysługujących jej praw procesowych.

5. Pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków

W tym zakresie mówić należy o podwyższeniu standardów gwarancyjnych w przypadku kontroli operacyjnej, w stosunku do regulacji ocenianych przez TK w wyroku z 30 lipca 2014 r. Co jednak istotne, wydaje się, że oprócz uszczegółowienia rodzajów środków wykorzystywanych do prowadzenia kontroli operacyjnej, jednocześnie ustawodawca rozszerzył ten katalog[71].

Inaczej sytuacja przedstawia się w przypadku uprawnienia do pozyskiwania tzw. danych internetowych, które to pojęcie jest nieostre[72]. Tym samym wymóg precyzyjnego określenia rodzaju pozyskiwanych informacji nie został spełniony. Nie zmienia tego wyłączenie zawarte w art. 20c ust. 1 ustawy o Policji, zgodnie z którym Policja może pozyskiwać dane internetowe nie stanowiące treści komunikatu. Przede wszystkim, wynika to z faktu braku bieżącej kontroli nad pozyskiwaniem tych danych (kontrola sądowa ma charakter następczy, fakultatywny i jest oparta na sprawozdaniu przedstawionym przez same służby). Co więcej, ze względów technicznych dane posiadane przez operatora usług internetowych mogą być przechowywane w taki sposób, że nie będzie możliwe odseparowanie treści komunikatu od tzw. metadanych.

6. Czynności operacyjno-rozpoznawcze winny być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób.

Standard ten realizowany jest jedynie w przypadku zakupu kontrolowanego oraz przesyłki niejawnie nadzorowanej. Iluzorycznie chroniony jest w przypadku kontroli operacyjnej, albowiem obecne przepisy dopuszczają bardzo szeroką możliwość wykorzystywania procesowego materiałów z kontroli operacyjnej, uzyskanych przez przypadek (z uwagi na dodany art. 168b k.p.k.).

W toku prac nad ustawą z 15 stycznia 2016 r. podnoszony był postulat zastrzeżenia subsydiarnego cha-

69 D. Głowacka, A. Ploszka, M. Sczaniecki, Wiem i powiem. Ochrona sygnalistów i dziennikarskich źródeł informacji. Praktyczny przewodnik, Helsińska Fundacja Praw Człowieka 2016, s. 82-85.

70 Art. 57 § 3 Prawa o prokuraturze przewiduje, że Prokurator Generalny może zwrócić się o przeprowadzenie czynności operacyjno-rozpoznawczych podejmowanych przez właściwe uprawnione organy, jeżeli pozostawałyby one w bezpośrednim związku z toczącym się postępowaniem przygotowawczym. Prokurator Generalny może zapoznać się z materiałami zgromadzonymi w toku takich czynności.

71 Por. art. 19 ust. 6 pkt 4 ustawy o Policji.

72 Por. art. 18 ust 1-5 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002, Nr 144, poz. 1204).

rakteru pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych, jednakże nie spotkał się on z aprobatą ze strony Rady Ministrów i posłów. Tym samym korzystanie z tych danych nie wymaga wcześniejszego wykorzystania innych mniej ingerujących środków.

7. W ustawie należy określić maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek, który nie może przekraczać ram koniecznych w demokratycznym państwie prawa.

Ustawa z 15 stycznia 2016 r. zakreśliła maksymalny okres prowadzenia kontroli operacyjnej przez Policję[73] i CBA[74]. Ograniczenia takiego nie wprowadzono na gruncie ustaw regulujących działalność ABW i SKW, wskazując na charakter realizowanych przez nich działań kontrwywiadowczych. Rozwiązanie takie zostało zakwestionowane przez Rzecznika Praw Obywatelskich we wniosku z 18 lutego 2016 r.[75]

8. Niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji

Zgoda sądu wymagana jest w przypadku procedury zarządzania kontroli operacyjnej, tj. najbardziej ingerującej w prawa i wolności spośród – nieuregulowanych na poziomie ustawy – czynności operacyjno-rozpoznawczych. Do 15 kwietnia 2016 r. zgoda taka była wymagana również w wypadkach pozyskania dowodów o innym tzw. przestępstwie katalogowym (tj. pozwalającym na prowadzenie kontroli operacyjnej) lub popełnionym przez inną osobę.

Warto jednak wskazać, że postanowienie sądu o zarządzeniu kontroli operacyjnej wymaga sporządzenia uzasadnienia jedynie w wypadku odmowy/zarządzenia/przedłużenia kontroli operacyjnej[76]. Tym samym wydanie zgody na kontrolę operacyjną nie wymaga żadnego uzasadnienia. Praca nad wnioskami o zarządzenie kontroli operacyjnej jest prowadzona w systemie tygodniowych dyżurów w kancelarii tajnej, które nie są wliczane do statystyki obciążenia pracą sędziego. Co więcej, sędzia nie ma w tym sprawach do pomocy asystenta sędziego. Istotne znaczenie ma również to, że służby są zobligowane do przedstawienia materiałów uzasadniających prowadzenie kontroli operacyjnej, a nie całości zgromadzonego materiału istotnego dla sprawy[77].

W przypadku innych czynności, takich jak zakup kontrolowany i przesyłka niejawnie nadzorowana, niezbędne jest uzyskanie zgody właściwego prokuratora, którego nie sposób uznać za organ niezależny. Natomiast w przypadku danych telekomunikacyjnych, pocztowych i internetowych, nie jest konieczne uzyskanie uprzedniej zgody niezależnego organu.

---

73 Art. 19 ust. 9 ustawy o Policji.

74 Art. 17 ust. 9 ustawy o CBA.

75 sygn. K 9/16.

76 Załącznik nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 10 czerwca 2011 r. w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów (rozporządzenie uznano za uchylone na podstawie ustawy z 15 stycznia 2016 r., jednak jak dotychczas nie uchwalono nowych przepisów).

77 Rzecznik Praw Obywatelskich skierował do Trybunału Konstytucyjnego wniosek o uznanie m.in. art. 19 ust. 1a ustawy o Policji za niezgodny z Konstytucją w zakresie, w jakim w/w przepisy ograniczają przekazanie właściwemu sądowi materiałów wyłącznie do uzasadniających potrzebę zarządzenia kontroli operacyjnej (sygn. K 41/15).

Wątpliwe z perspektywy niniejszego wymogu jest proponowane w projekcie ustawy o działaniach antyterrorystycznych wprowadzenie możliwości prowadzenia kontroli operacyjnej wobec „osoby niebędącej obywatelem Rzeczypospolitej Polskiej" bez zgody sądu przez pierwsze 3 miesiące prowadzenia takich czynności.

9. Konieczne jest precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych

Obowiązujące przepisy jedynie połowicznie realizują przedmiotowe zalecenie. Problematyczne jest, że niszczenie materiałów np. z kontroli operacyjnej, nie jest obwarowane żadnym konkretnym terminem. Przepisy posługują się w tym zakresie stwierdzeniem, iż np. komisyjne, protokolarne zniszczenie ma nastąpić niezwłocznie. Przepisy ustaw nie ustanawiają jednak mechanizmów kontrolujących proces niszczenia.

Na tym polu pojawia się również problem stosowania przepisów przejściowych z ustawy z 15 stycznia 2016 r. Zgodnie z art. 13, art. 15 oraz art. 16 tej ustawy, do stanów prawnych i faktycznych sprzed 7 lutego 2016 r. (dnia wejścia w życie tej nowelizacji) możliwe jest stosowanie przepisów dotychczasowych, które TK w wyroku z 30 lipca 2014 r. uznał za niekonstytucyjne[78].

10. Niezbędne jest zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów

Spełnienie niniejszego standardu niewątpliwie napotyka na przeszkody. Przede wszystkim, po wyroku TK w sprawie K 54/07, tylko w CBA wprowadzono pełnomocnika do spraw przetwarzania danych osobowych, w tym wrażliwych. Wyrok ten, mimo, że analogiczne regulacje dotyczące zbierania danych znajdują się w przepisach regulujących pracę innych służb, nie wywarł skutku w stosunku do tych regulacji. Nie została zastosowana tu rozszerzona skuteczność tego orzeczenia. Nie zostały w tym zakresie wprowadzone procedury kontroli prawidłowości przetwarzania tych danych, pomimo, że właściwość Generalnego Inspektora Ochrony Danych Osobowych jest z mocy ustawy w tym zakresie wyłączona.

Wydaje się, że zagrożeniem dla zagwarantowania bezpieczeństwa zgromadzonych danych jest rozwiązanie zawarte w art. 12 Prawa o prokuraturze umożliwiające przedstawienie przez Prokuratora Generalnego „innym osobom" (innym niż organy władzy publicznej) informacji dotyczących konkretnych spraw.

11. Unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo.

Wymóg ten na gruncie obecnie obowiązujących przepisów nie jest w ogóle respektowany. Obowiązujące przepisy nie nakładają na służby pozytywnego obowiązku poinformowania jednostki o prowadzeniu czynności operacyjno-rozpoznawczych, z wyjątkiem pozyskania danych objętych tajemnicą bankową. Nie dają też, w sytuacji powzięcia o tym informacji, możliwości zakwestionowania legalności takiego działania przez złożenie zażalenia. Jedynym instrumentem ochrony prawnej w takiej sytuacji pozostaje powództwo

78 Rozwiązanie takie skarży RPO we wniosku z 18 lutego 2016 r. (sygn. K 9/16).

o ochronę dóbr osobistych, przy założeniu, że powód dysponuje informacjami uprawdopodobniającymi np. nielegalne pozyskiwanie danych[79].

12. Zagwarantowanie transparentności stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej, przejawiające się w publicznej jawności i dostępności zagregowanych danych statystycznych, nadających się do porównania, o ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych

Wymóg ten nie jest w pełni realizowany w polskim ustawodawstwie. Aktualnie ustawowo zobligowanymi do przekazywania Sejmowi i Senatowi informacji o stosowaniu kontroli operacyjnej są Prokurator Generalny oraz Minister Spraw Wewnętrznych. Zakres tych informacji jest jednak dość ograniczony przepisami ustaw, odpowiednio o Policji oraz Prawa o prokuraturze. W przypadku danych telekomunikacyjnych, pocztowych oraz internetowych takiego obowiązku brakuje w obowiązujących przepisach.

Nie czyni też zadość temu obowiązkowi przekazywanie Sądowi Okręgowemu w Warszawie zagregowanej informacji, o której mowa chociażby w art. 20c ustawy o Policji. Tego typu informacje będą bowiem przekazane zgodnie z przepisami z zachowaniem rygorów właściwych ochronie informacji niejawnych.

13. Nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne

Przepisy w sposób ambiwalentny podchodzą do tej kwestii. Wszystkie ww. opisane służby specjalne, policyjne czy skarbowe, wykazują daleko posunięte podobieństwa pod względem kompetencji, których realizacja wiąże się z naruszaniem praw i wolności konstytucyjnych. Jednak co istotne, Agencja Wywiadu posiada kompetencję do prowadzenia „wywiadu elektronicznego", który nie został w najmniejszym stopniu uregulowany na gruncie ustawy o ABW oraz AW[80].

14. Zróżnicowanie poziomu ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się możne także nastąpić z uwagi na to, czy niejawne pozyskiwanie informacji dotyczy obywateli, czy osób niemających polskiego obywatelstwa

W polskim ustawodawstwie brak jest zróżnicowania dla tej sytuacji. Pod pretekstem realizacji tego wymogu w ustawie o działaniach antyterrorystycznych proponuje się wprowadzenie możliwości stosowania środków właściwych kontroli operacyjnej w stosunku do osób niebędących obywatelami, bez kontroli sądu – jedynie w oparciu o decyzję Szefa ABW informującego równolegle Prokuratora Generalnego (tj. Ministra Sprawiedliwości). Projektodawcy argumentują dopuszczalność takiego rozwiązania z uwagi na fakt skierowania do Sejmu w 2014 r. rządowego projektu ustawy o Agencji Bezpieczeństwa Wewnętrznego[81]. Prace nad projektem zakończyły się na etapie prac w komisji. Projekt zakładał możliwość prowadzenia kontroli operacyjnej wobec cudzoziemców w oparciu jedynie o zgodę Szefa ABW.

79 Por. wyrok Sądu Okręgowego w Warszawie z 26 kwietnia 2012 r., sygn. akt II C 626/11; uzasadnienie wyroku dostępne jest na stronie: http://www.obserwatorium.org/images/wyrok_SO_B_Wroblewski.pdf.

80 Art. 6 ust. 1 pkt 8 ustawy o ABW oraz AW.

81 Druk sejmowy nr 2295, Sejm VII kadencji.

Trybunał w wyroku z 30 lipca 2014 r. wskazując na generalną dopuszczalność różnicowania poziomu ochrony prywatności ze względu na obywatelstwo, odrzucił jednak interpretację, która pozwalałaby na gromadzenie o cudzoziemcach „informacji niekoniecznych w demokratycznym państwie". Trybunał zakreślił przy tym wyraźną granicę takiego zróżnicowania: „nie może [ona] prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich". Dlatego Trybunał przyjął „jako założenie wyjściowe – jednakowy standard ingerencji w konstytucyjne wolności oraz prawa, bez względu na to, czy ich podmiot ma obywatelstwo polskie". Trybunał wskazał dalej, że „każdy znajdujący się pod władzą Rzeczypospolitej (…) niezależnie od statusu obywatelskiego – może zatem zasadnie oczekiwać ochrony przed nieuzasadnioną ingerencją w przysługujące mu wolności i prawa" oraz stwierdził, że standardem konstytucyjnym nałożonym na ustawodawcę jest „konieczność ustanowienia takich samych standardów dotyczących pozyskiwania, gromadzenia czy przechowywania danych zgromadzonych przez władze publiczne w toku czynności operacyjno-rozpoznawczych w stosunku do wszystkich podmiotów, które znajdują się pod władzą Rzeczypospolitej Polskiej".

Od tak zakreślonych zasad ogólnych dopuszczalne są jednak wyjątki, które muszą spełniać wymogi zasady proporcjonalności określone w art. 31 ust. 3 Konstytucji. Trybunał odrzucił tym samym tezę, jakoby art. 37 ust. 2 stanowił *lex specialis* wyłączający zastosowanie art. 31 ust. 3 Konstytucji. Odmienne stanowisko skutkowałoby tym, że „cudzoziemcy nie mieliby faktycznie żadnych gwarantowanych konstytucyjnie praw". Ograniczenie praw nie może naruszać ani przekreślać ich istoty[82].

82 Konsekwencją obowiązywania art. 37 ust. 2 Konstytucji jest natomiast możliwość dokonania bardziej elastycznej interpretacji poszczególnych przesłanek składających się na zasadę proporcjonalności, uzasadniającej większy poziom ingerencji w wolności i prawa cudzoziemców niż obywateli.

4. Standardy prawa międzynarodowego odnoszące się kompetencji służb specjalnych i policyjnych.

Struktura, organizacja i kompetencje służb specjalnych nie są regulowane na poziomie prawa międzynarodowego. Wynika to m.in. z założenia, że kwestie związane z zapewnieniem porządku i bezpieczeństwa publicznego stanowią istotę suwerenności państwowej. Jednak jednym z osiągnięć cywilizacyjnych XX wieku jest samoograniczanie się państw poprzez podjęcie szeregu zobowiązań w zakresie ochrony praw i wolności człowieka. W ten sposób prawo międzynarodowe – zarówno na poziomie globalnym (np. w ramach ONZ) jak i regionalnym (np. w ramach Rady Europy) – wpływa na funkcjonowanie służb specjalnych i policyjnych w ramach suwerennych państw.

Międzynarodowe regulacje dotyczące praw człowieka przyjmują co do zasady formę umów międzynarodowych podpisywanych i ratyfikowanych przez państwa. Jednak oprócz norm prawnych – zwykle dość ogólnych – organizacje i instytucje międzynarodowe wypracowały również na przestrzeni ostatnich lat szereg rekomendacji adresowanych do państw, mających jednak formę norm *soft law*, a zatem niebędących źródłami praw czy obowiązków.

4.1. Rada Europy

Polska stała się członkiem Rady Europy w 1991 r. Założenia, na których oparta jest Rada Europy – poszanowanie praw człowieka, praworządności i demokracji – spowodowały, że w latach 90-tych organy i ciała eksperckie Rady Europy podejmowały zagadnienie kontroli nad służbami policyjnymi czy specjalnych w świetle zmian ustroju, do jakiego doszło na przełomie lat 80-tych i 90-tych w Europie Środkowo-Wschodniej. Tym samym głównym zagadnieniem analizowanym wówczas była kwestia **tzw. rozliczeń z przeszłością**, tj. pociągnięcia do odpowiedzialności za zbrodnie popełnione przez reżimy totalitarne (np. przez komunistyczne służby bezpieczeństwa) przy zagwarantowaniu podstawowych zasad obowiązujących w państwach demokratycznych. Jednak w ostatnich latach coraz większy nacisk kładzie się na wpływ tzw. wojny z terroryzmem na prawa i wolności jednostki, w szczególności prawo do prywatności oraz wolność osobistą.

Centralny akt prawa Rady Europy – Europejska Konwencja Praw Człowieka (dalej: EKPC) – reguluje kompetencje i pozycje krajowych organów odpowiedzialnych za zapewnienie bezpieczeństwa, w zakresie w jakim ich działalność ma wpływ na prawa i wolności, w szczególności wolność osobistą, prawo do prywatności, prawo do życia, swobodę informacji. Stąd też przedmiotem skarg kierowanych do Europejskiego Trybunału Praw Człowieka (dalej: ETPC) były stany faktyczne, w których do ograniczenia tych praw dochodziło również na skutek działalności służb policyjnych czy specjalnych. Organy państwa zbierające w sposób niejawny informacje o jednostkach zostały w ten sposób objęte kontrolą ze strony organu międzynarodowego. Z orzecznictwa Trybunału wynika, że kontroli takiej poddany został cały system funkcjonowania organów władzy publicznej, które mają wpływ na to, w jaki sposób służby bezpieczeństwa realizują swoje kompetencje, np. poprzez wkroczenie w sferę prawnie chronioną (np. wolność czy prywatność).

Jednak kwestia systemu kontroli nad służbami jest jedynie pośrednio analizowana przez Trybunał, przy okazji oceny proporcjonalności wkroczenia w prawo gwarantowane przez Konwencję. Istnienie odpowiednich zabezpieczeń przed nadużyciami uprawnień ze strony organów władzy publicznej jest istotnym czynnikiem dla oceny, czy dane wkroczenie w prawo lub wolność chronione przez Konwencję, nie jest

nadmierne. Ostatecznie jednak, kontrola prowadzona przez Trybunał – w oparciu o indywidualną skargę – nie jest w stanie zapewnić odpowiedzialności w większym stopniu niż np. krajowy organ ekspercki zajmujący się kontrolą nad służbami[83]. Jednak pomimo tych faktycznych ograniczeń, istotne znaczenie ma fakt, że kwestie bezpieczeństwa (stanowiące uzasadnienie ograniczeń praw i wolności) nie pozostają w orzecznictwie Trybunału poza kontrolą pod kątem zgodności działań z Konwencją.

Przedmiotem pierwszego orzeczenia ETPC w przedmiocie niejawnego pozyskiwania informacji o osobach, było niemieckie ustawodawstwo antyterrorystyczne wprowadzone w 1968 r.[84] W 1970 r. zostało ono poddane kontroli pod kątem zgodności z Ustawą Zasadniczą Niemiec. Federalny Trybunał Konstytucyjny (FTK) orzekł wówczas, że nowe prawo narusza konstytucję poprzez brak obowiązku poinformowania osoby o tym, że była poddana inwigilacji, jeśli taka informacja nie stanowiłaby zagrożenia dla prowadzonego postępowania[85]. Na skutek wyroku FTK odpowiednie służby zostały zobligowane do informowania osoby poddanej inwigilacji o tym fakcie, pod warunkiem że nie stanowiło to zagrożenia dla bezpieczeństwa czy skuteczności prowadzonych działań. Decyzję w przedmiocie notyfikacji podejmował właściwy minister po uzyskaniu zgody tzw. Komisji G10. Ponadto, minister sprawozdawał się regularnie Komisji, co w praktyce oznaczało potrzebę uzyskania jej zgody w każdym przypadku skorzystania ze środków przewidzianych w ustawie.

W sprawie *Klass przeciwko Niemcom*[86] Europejski Trybunał Praw Człowieka wskazał, że wkroczenie przez organy władzy publicznej w tajemnicę korespondencji przez organy państwa wymaga zapewnienia przez prawo **adekwatnych i skutecznych gwarancji przeciwko nadużyciu uprawnień**. Czynniki które powinny zostać wzięte pod uwagę przy konstruowaniu takich gwarancji obejmują: rodzaj, zakres i czas trwania środków inwigilacji, podstawy wymagane do zastosowania takich środków, organy uprawnione do zarządzenia ich stosowania, jak również do nadzoru nad ich stosowaniem, rodzaj środków ochrony prawnej przewidziany na gruncie prawa krajowego. Ponadto, elementem oceny zgodności z Konwencją, jest istnienie w prawie krajowym procedury, która zapewnia adekwatną gwarancję przed nadużyciami. Jako domniemany (i optymalny) standard kontroli nad czynnościami inwigilacji wskazano na kontrolę sądową[87]. Pomimo braku uprzedniej kontroli sądowej w prawie niemieckim, Trybunał uznał, że istniejące zabezpieczenia (tj. kontrola ze strony komisji parlamentarnej oraz Komisji G10) stanowią wystarczającą gwarancję. Sprawa była również analizowana pod kątem zgodności z art. 13 Konwencji. Zdaniem Trybunału brak wymogu notyfikacji tj. obowiązku informowania osoby poddanej inwigilacji o fakcie jej prowadzenia, nie naruszył Konwencji również w tym względzie. Warto jednak podkreślić, że Trybunał wziął pod uwagę orzeczenie FTK z 1970 r., system kontroli realizowanej przez Komisję G10, jak również dostępność skargi konstytucyjnej na gruncie prawa niemieckiego.

---

83 *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) and updated by the Venice Commission at its 102nd Plenary Session* (Venice, 20-21 March 2015) CDL-AD(2015)010-e, § 126. Wynika to przede wszystkim z subsydiarnego charakteru kontroli prowadzonej przez Trybunał.

84 Przewidywało ono możliwość wkraczania w tajemnicę korespondencji czy komunikacji telefonicznej w przypadku potwierdzonego podejrzenia możliwości popełnienia przestępstw przeciwko bezpieczeństwu państwa czy porządkowi demokratycznemu. Decyzję w tej sprawie podejmował szef uprawnionej służby zajmującej się ochroną bezpieczeństwa. Kontrolę nad prowadzoną inwigilacją prowadził urzędnik posiadający jednak kompetencję do pełnienia funkcji sędziowskiej. Odpowiadał on również za niszczenie danych nie mających znaczenia z punktu widzenia celu prowadzonej inwigilacji.

85 Wyrok z 15 grudnia 1970 r.

86 Wyrok z 6 września 1978 r., skarga nr 5029/71. skarżącymi było pięciu prawników, w tym jeden sędzia.

87 § 56.

W ostatnim czasie Europejski Trybunał Praw Człowieka wydał dwa bardzo istotne orzeczenia dotyczące zgodności z Konwencją niejawnej inwigilacji uregulowanej w ustawodawstwie rosyjskim[88] oraz węgierskim[89]. W pierwszej ze spraw (*Zakharov przeciwko Rosji*) Trybunał postanowił ujednolicić swoje orzecznictwo w kwestii przyznania statusu „ofiary" naruszenia prawa prywatności, do którego miało dojść na skutek tajnej inwigilacji. **Ustalenia poczynione w tym zakresie przez Trybunał mogą mieć kluczowe znaczenie dla Polski przy ewentualnej ocenie zgodności prawa polskiego ze standardem strasburskim.** W świetle wyroku w sprawie *Zakharov*, nadanie statusu „ofiary", który wynikałby z samego faktu obowiązywania prawa pozwalającego na tajną inwigilację, jest możliwe w wypadku spełnienia dwóch warunków. Po pierwsze, zakres dopuszczalnej prawem tajnej inwigilacji powoduje, że skarżący może zostać nią objęty ponieważ należy do grupy „*targeted*" lub ponieważ prawo obejmuje wszystkich użytkowników tworząc system umożliwiający przechwycenie każdej rozmowy/komunikacji. Drugim czynnikiem branym przez Trybunał pod uwagę jest kwestia dostępności i skuteczności środków ochrony praw na poziomie prawa krajowego, które umożliwią przeprowadzenie weryfikacji przeprowadzonej inwigilacji. Trybunał wskazał przy tym na zależność, że w przypadku braku takiego środka, istnieje większa potrzeba przeprowadzenia kontroli obowiązujących regulacji przez Trybunał. W takim wypadku skarżący nie musi przedstawiać dowodu na istnienie ryzyka, że był inwigilowany. Z kolei istnienie w prawie krajowym skutecznych środków ochrony, czyniłoby trudniejszym sformułowanie zarzutu o naruszeniach przepisów czy przekroczeniach uprawnień. W przypadku istnienia takich środków, skarżący musi wykazać przed Trybunałem, że z uwagi na jego status jest on potencjalnie zagrożony stosowaniem wobec niego środków inwigilacji.

Trybunał uznał przede wszystkim, że brak w rosyjskim prawie odpowiedniego środka ochrony praw (*remedy*) skutkuje możliwością uznania skarżącego za „ofiarę" naruszenia praw w rozumieniu Konwencji, a tym samym merytorycznego rozpoznania sprawy. Z kolei poszczególne elementy analizowane przez Trybunał (dostępność prawa, zakres regulacji, gwarancje proceduralne, czas trwania inwigilacji, procedury chroniące przed nadużyciami) doprowadziły do konkluzji, że prawo rosyjskie nie stwarza wystarczających gwarancji chroniących przed nadużyciami.

Prowadzona w ten sposób przez ETPC kontrola abstrakcyjna pozwala na ocenę krajowego systemu niejawnego pozyskiwania informacji w całości, przy uwzględnieniu gwarancji, które powinny być wbudowane w ten system[90]. W przypadku sprawy *Zakharov*, nawet istniejąca na gruncie prawa rosyjskiego kontrola sądowa nie okazała się wystarczającym zabezpieczeniem oraz nie była w stanie naprawić negatywnych konsekwencji, które wiążą się z szerokim zakresem przesłanek umożliwiających stosowanie inwigilacji.

W drugiej ze spraw (*Szabo i Vissy przeciwko Węgrom*), skarżący byli pracownikami węgierskiej organizacji pozarządowej, zaś przedmiotem skargi były rozwiązania wprowadzone do prawa węgierskiego na mocy ustawy z 2010 r.[91] Podobnie jak w przypadku sprawy Zakharov, Trybunał musiał rozstrzygnąć kwestię związaną ze statusem ofiary naruszenia praw. Trybunał uznał, że mimo iż „związek ze społeczeństwem obywatelskim" nie stanowi przesłanki zastosowania środków na podstawie ustawy z 2010 r., to jednak przesłanki tej ustawy zostały zakreślone na tyle szeroko, że mogą właściwie obejmować każdą osobę. Trybunał zwrócił

88 Wyrok w sprawie *Zakharov v. Rosja*, wyrok z 4 grudnia 2015 r., skarga nr 47143/06.

89 Wyrok w sprawie *Szabo and Vissy v. Węgry*, wyrok z 12 stycznia 2016 r., skarga nr 37138/14.

90 L. Woods, *Zakharov v Russia: Mass Surveillance and the the European Court of Human Rights*, EU Law Analysis 16 grudnia 2015 r.

91 Utworzono specjalną służbę TEK (*Terrorelhárítási Központ*) ds. zwalczania terroryzmu. Ustawa przyznawało tej służbie kompetencje do prowadzenia działań niejawnych (np. przeszukania pomieszczeń czy korespondencji), zaś ich stosowanie tylko w niektórych wypadkach wymagało zgody sądu.

uwagę, że przed skierowaniem sprawy do Strasburga skarżący skierowali skargę do Trybunału Konstytucyjnego, który jednak nie podzielił ich argumentów.

W sprawie *Szabo i Vissy* Trybunał zauważył, że w porównaniu ze sprawą *Klass*, mamy do czynienia z dalej idącym rozwojem technologii, stąd możliwe są bardziej dotkliwe naruszenia Konwencji. Jednym z elementów przeprowadzonego przez Trybunał testu proporcjonalności była ocena, na ile rozwój metod prowadzonej inwigilacji wiązał się z jednoczesnym rozwojem uprawnień jednostki poddanej inwigilacji. Przejawem braków w tym zakresie był m.in. fakt, że prawo nie nakazywało, aby wniosek o zainicjowanie inwigilacji musiał zostać poparty szczegółowymi materiałami uzasadniającymi jej prowadzenie. Co więcej, w pewnym zakresie prawo węgierskie nie wymagało uprzedniej zgody sądu na ich prowadzenie – było to zależne od decyzji właściwego ministra. Trybunał nie podzielił argumentu rządu, zgodnie z którym minister jest lepiej „umocowany" (niż sąd) do tego, żeby podejmować decyzję w przedmiocie inwigilacji. Trybunał wskazał nawet na ustalenia poczynione w sprawie *Klass*, zgodnie z którymi zasada praworządności (*rule of law*) wymaga, aby wkroczenie przez władzę wykonawczą w prawa jednostki było poddane skutecznej niezależnej kontroli, docelowo – sądowej. Jest to szczególnie aktualne w wypadkach, w których łatwo o nadużycia uprawnień (np. ze względu na tajność prowadzonych działań).

Standardem, według którego Trybunał analizuje sprawy związane z inwigilacją, jest *„strict necessity test"*, rozumiany w dwóch aspektach – w znaczeniu ogólnym, gdy wkroczenie jest niezbędne dla zabezpieczenia instytucji demokratycznych oraz – w znaczeniu szczegółowym – gdy pozwala na uzyskanie istotnych informacji w konkretnych sprawach. Prawo węgierskie nie stworzyło skutecznych mechanizmów kontroli prowadzonej inwigilacji w taki sposób, aby zabezpieczyć prawa osób, które zostały jej poddane. Za skuteczny środek ochrony praw nie uznano możliwości zgłoszenia swojej sprawy do węgierskiego Ombudsmana[92].

Obowiązek notyfikacji na gruncie orzecznictwa ETPC

W sprawie *Klass* Trybunał, wskazał, że na gruncie prawa niemieckiego, w sytuacji, w której jednostka uważa, że prawdopodobnie jest poddana inwigilacji, ma możliwość skierowania skargi konstytucyjnej do FTK, jak również możliwość złożenia skargi do Komisji G10. Podstawowym zarzutem formułowanym wówczas przez skarżących był brak w prawie niemieckim obowiązku notyfikacji o byciu inwigilowanym. Trybunał ocenił, że sam brak takiej procedury nie stanowi samoistnej przesłanki naruszenia Konwencji. Trybunał wziął jednak pod uwagę wcześniejszy wyrok FTK, który częściowo przynajmniej wprowadzał taki obowiązek. Od jego realizacji zależy możliwość skorzystania z innych środków ochrony praw, np. przed sądami krajowymi.

Standard zawarty w wyroku *Klass* został następnie potwierdzony w decyzji ETPC z 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*[93]. Zmiany w prawie niemieckim wprowadzone w 1994 r.

92 Przed Trybunałem zawisły dwie sprawy dotyczące tzw. masowej inwigilacji odnoszące się do informacji ujawnionych przez Edwarda Snowdena. HFPC przedstawiła w tych sprawach opinie *amicus curiae*. Opinia HFPC w sprawie *Big Brother Watch i inni przeciwko Wielkiej Brytanii* dostępna jest na stronie: http://www.hfhr.pl/wp-content/uploads/2016/02/Amicus_Big_Brother_Watch_i_inni_pko_Wielkiej_Brytanii.pdf; Opinia HFPC w sprawie *Bureau of Investigative Journalism przeciwko Wielkiej Brytanii* dostępna jest na stronie: http://www.hfhr.pl/wp-content/uploads/2016/02/Amicus_Bureau_of_Investigative_Journalism_pko_Wielkiej_Brytanii.pdf.

93 Decyzja z dnia 29 czerwca 2006 r., skarga nr 54943/00.

poszerzały kompetencje służb niemieckich w zakresie tzw. inwigilacji strategicznej (*strategic monitoring*). Zmiany te były przedmiotem m.in. orzeczenia Federalnego Trybunału Konstytucyjnego z 1999 r., który uznał część rozwiązań za niekonstytucyjne[94]. Prawo niemieckie zostało po raz kolejny zmienione w 2001 r. Jednym z elementów, który zaważył na tym, że ETPC wydał decyzję o niedopuszczalności skargi, był fakt, że skarżący na gruncie prawa niemieckiego dysponowali skutecznym mechanizmem notyfikowania osób zainteresowanych, których dane były gromadzone, pod warunkiem, że taka notyfikacja zagrażała celom prowadzonej inwigilacji (np. zapewnieniu bezpieczeństwa).

Standard wypracowany na gruncie spraw „niemieckich" był punktem odniesienia dla oceny spraw dotyczących prawa bułgarskiego. W 2007 r. w sprawie *The Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii*[95] Trybunał orzekł, że prawo bułgarskie nie zawiera gwarancji chroniących przed nadużyciami ze strony służb. Trybunał wskazał m.in. na brak w prawie bułgarskim obowiązku notyfikacji, jak również na brak niezależnej kontroli nad prowadzeniem inwigilacji ze strony służb. Porównał przy tym rozwiązania bułgarskie z niemieckimi. Dostrzeżone braki skutkowały orzeczeniem o naruszeniu zarówno art. 8, jak również art. 13.

Inne rozwiązanie, które ma na celu zabezpieczenie przed nadużyciami ze strony służb, zostało przez Trybunał przeanalizowane na gruncie sprawy *Kennedy v. UK*[96]. Na gruncie prawa brytyjskiego funkcjonuje *Investigatory Powers Tribunal* (IPT) posiadający kompetencje do rozpatrywania indywidualnych skarg dotyczących m.in. nielegalnych podsłuchów. Pomimo, iż prawo brytyjskie nie przewiduje obowiązku notyfikacji, mechanizm oparty o możliwość złożenia skargi do IPT został przez Trybunał uznany za wystarczającą gwarancję przeciwko nadużyciom.

W sprawie *Szabo i Vissy przeciwko Węgrom*, Trybunał podkreślił, że prawo krajowe nie przewiduje ani obowiązku notyfikacji, ani żadnego narzędzia służącego ochronie praw jednostki w wypadku niejawnego pozyskiwania informacji na jej temat, w tym w przypadku wkroczenia w tajemnicę korespondencji. Trybunał wskazał przy tym na standard z wyroków *Weber i Saravia przeciwko Niemcom* oraz w sprawie *Zakharov*, zgodnie z którym w wypadkach, w których notyfikacja nie naraża na szwank prowadzonego przez służby działania, informacja powinna zostać przekazana osobie zainteresowanej.

Powyższe wskazuje, że w świetle orzecznictwa ETPC, obowiązek notyfikacji – mimo, iż nie jest jednolitym i bezwzględnym wymogiem kierowanym pod adresem prawa krajowego – pełni co najmniej dwie funkcje – zabezpieczenia przed nadużyciami służb oraz służy ochronie praw jednostki[97].

94 Wyrok z 14 lipca 1999 r.

95 Wyrok z dnia 28 czerwca 2007 r., skarga nr 62540/00.

96 Wyrok z 18 maja 2010 r., skarga nr 26839/05.

97 P. De Hert, The Rights of Notification after Surveillance is over: Ready for Recognition?, Digital Enlightment Yearbook 2012, s. 37.

Rekomendacja R (87) 15 Komitetu Ministrów Rady Europy o Ochronie Danych Osobowych wykorzystywanych w sektorze policji z 17 września 1987 roku

„1.1. Każde Państwo Członkowskie powinno dysponować niezależnym i zewnętrznym w stosunku do Policji organem nadzorczym, upoważnionym do czuwania nad przestrzeganiem Zasad zawartych w niniejszej Rekomendacji.
(…)
2.2. Tam, gdzie dane dotyczące osoby były gromadzone i przechowywane bez jej wiedzy, powinna ona - jeśli dane takie nie zostały usunięte - zostać poinformowana w miarę możliwości o tym, iż informacje o niej są przetwarzane w zbiorze. Należy tego dokonać, gdy tylko przestanie istnieć ryzyko, iż przedmiot działań Policji poniesie jakąkolwiek szkodę wynikającą z ujawnienia osobie, której dane dotyczą faktu istnienia tych informacji.
(…)
31. W ramach krajowych ustaw o ochronie danych główną rolę odgrywają organy ochrony danych oraz rzecznicy. Wszędzie tam, gdzie władze takie istnieją należy im powierzyć zadania określone w niniejszej Rekomendacji. Niepożądanym byłoby utworzenie odrębnego, konkurującego organu dla celów niniejszej Rekomendacji. Jednakże każdy nowo utworzony organ winien być faktycznie niezależny od kontroli Policji. Jest to podstawowa właściwość biorąc pod uwagę, iż niniejsza Rekomendacja zakłada możliwość przekazania kompetencji podejmowania decyzji, w tym także ocenę ograniczeń nałożonych na działania Policji odnośnie danych osobowych, temu właśnie organowi.
(…)
32. Struktura ustrojowa niektórych Państw Członkowskich może nakładać obowiązek utworzenia kilkunastu niezależnych organów władzy nadzorczej w sytuacji, gdy organy ochrony danych lub rzecznicy ochrony danych osobowych jeszcze nie istnieją. Ciało takie nie musi koniecznie być ciałem kolegialnym. Umożliwiałoby to osobie fizycznej spełnianie roli „gwarantującego poszanowanie Zasad zawartych w niniejszej Rekomendacji". Jednakże biorąc pod uwagę, jak ważna jest to rola, pożądanym byłoby, aby organ nadzorczy, bez względu na formę, posiadał wystarczające środki do efektywnego działania".

Oprócz zagadnień związanych z ochroną prywatności, której pełna analiza przekracza granice niniejszego opracowania, orzecznictwo ETPC obejmuje zagadnienia, w których działalność służb specjalnych i policyjnych ma wpływ na ograniczenie (czasem nawet naruszenie) prawa do życia, zakazu tortur[98] czy prawa do rzetelnego procesu.

W przypadku zakazu tortur, ściganie ewentualnych naruszenia w tym zakresie popełnione przez służby Państwa-Strony Konwencji napotyka szereg utrudnień wynikających przede wszystkim z charakteru funkcjonowania służb specjalnych. Europejski Trybunał Praw Człowieka w wyrokach *Al Nashiri przeciwko Polsce* oraz *Abu Zubaydah przeciwko Polsce* przeprowadził dość wnikliwą analizę systemu kontroli nad służbami funkcjonującego na gruncie prawa polskiego. Mimo, że sama skarga, jak również wyrok Trybunału, nie odnosił się bezpośrednio do prawidłowości obowiązujących regulacji w tym zakresie, Trybunał wyraził poważne wątpliwości, czy funkcjonujący w Polsce kształt demokratycznej kontroli nad służbami, w odpowiedni sposób zabezpiecza przez ewentualnymi naruszeniami praw człowieka.

98 Zarzut naruszenia art. 3 pojawiał się m.in. w sprawach dotyczących ekstradycji (Wyrok w sprawie Chahal przeciwko Wielkiej Brytanii z dnia 15 listopada 1996 r., skarga nr 22414/93).

„498. Niniejsza sprawa, oprócz podniesienia kwestii skutecznego śledztwa w sprawie rzekomego sprzecznego z art. 3 Konwencji niewłaściwego traktowania, wskazuje w tym kontekście również na ***szerszy problem demokratycznego nadzoru nad służbami wywiadowczymi*** *(...). Ochrona praw człowieka gwarantowana przez Konwencję zwłaszcza w artykułach 2 i 3, nie tylko wymaga przeprowadzenia skutecznego śledztwa w sprawie rzekomych naruszeń praw człowieka, ale również* ***zapewnienia odpowiednich zabezpieczeń*** *- zarówno w prawie jak i w praktyce - wobec służb wywiadowczych naruszających określone w Konwencji prawa, głównie podczas realizacji ich tajnych operacji.* ***Okoliczności niniejszej sprawy mogą budzić zaniepokojenie, czy w polskim porządku prawnym ten wymóg został spełniony****."*

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 24 lipca 2014 r.
w sprawie Al Nashiri przeciwko Polsce (skarga nr 28761/11) (fragment)

Sprawy tajnych więzień CIA w Europie[99] stanowią przykład jednego z najpoważniejszych wyzwań związanych z działalnością służb specjalnych, a mianowicie **współpracy wywiadowczej służb**. Występujący w tym wypadku czynnik transgraniczny może skutkować poważnym ograniczeniem „zdolności" kontrolnych odpowiednich organów każdego z państw uczestniczących w takiej współpracy. Odnotowane w tym względzie braki w zapewnieniu odpowiedzialności (tzw. „*accountability gap*") wynikają m.in. z zasad ochrony informacji niejawnych, np. *third party rule*, zgodnie z którą informacje uzyskane w ramach współpracy wywiadowczej mogą być przekazane osobie trzeciej jedynie po uzyskaniu zgody strony będącej źródłem tych informacji. Definicję „osoby trzeciej" interpretuje się przy tym rozszerzająco, przez co często obejmuje ono również krajowe organy kontrolne inne niż umieszczone w agencji lub w samym rządzie[100]. Z jednej strony zasady te przyjmują formę norm zawartych w umowach międzynarodowych regulujących ochronę informacji niejawnych, z drugiej jednak, zasady te stanowią kwintesencję niepisanych reguł takiej współpracy.

Działalność służb jest również na gruncie EKPC analizowana pod kątem zgodności z art. 6 Konwencji, w szczególności, gdy działalność służb ma bezpośredni wpływ na przyszłe postępowanie sądowe, w szczególności karne. Granica dopuszczalności zdobywania dowodów jest szczególnie aktualna w przypadku tzw. prowokacji policyjnej[101]. Z orzecznictwa Europejskiego Trybunału Praw Człowieka wynika standard, zgodnie z którym nie jest możliwym wszczynanie postępowań karnych „na postawie materiałów uzyskanych w drodze prowokacji czynnej, polegającej na nakłanianiu do popełnienia przestępstwa, w szczególności wtedy, gdy nie przedstawiono dowodów, że prowokowany już wcześniej czynił starania w celu popełnienia przestępstwa"[102]. Z punktu widzenia tak zakreślonego standardu rzetelności postępowania, niepokój budzi nowe brzmienie art. 168a k.p.k.

Kwestia nadzoru nad służbami specjalnymi była również przedmiotem dogłębnej analizy ze strony **Komisji Weneckiej** - organu eksperckiego funkcjonującego w ramach Rady Europy. Zagadnienie to było kilkukrotnie przedmiotem opinii opracowanych przez Komisję w odniesieniu do projektów ustaw czy też

99 M.in. Wyrok w sprawie *El-Masri v. Macedonia* z 13 grudnia 2012 r., skarga nr 39630/09.

100 Komisja Wenecka 2015, par. 13

101 Art. 19a ustawy o Policji; art. 19 ustawy o CBA.

102 P. Kładoczny, A. Pietryka, *Prowokacja policyjna a wyłączenie odpowiedzialności prowokowanego w świetle orzecznictwa strasburskiego – postulaty pod adresem polskiej regulacji*, Przegląd Legislacyjny 2/2013, s. 17.

zmian prawa uchwalonych w niektórych państwach Rady Europy[103]. Jednak oprócz opinii odnoszących się do indywidualnych rozwiązań prawnych, Komisja Wenecka opracowała również – na zlecenia organów Rady Europy – badania ogólne, mające na celu wyartykułowanie standardów, jakie regulacje działalności służb w państwach Rady Europy powinny spełniać.

Pierwsze z takich opracowań zostało opublikowane w 1998 r. na zlecenie Zgromadzenia Parlamentarnego Rady Europy[104]. Wśród minimalnych standardów odnoszących się do statusu służb specjalnych, Komisja wskazała m.in. na konieczność zagwarantowania odpowiedzialności za działania służb oraz obowiązek uregulowania podstaw ich działalności w prawie powszechnym uchwalonym przez parlament. Wskazano również, że kontrola nad służbami nie może mieć jedynie wewnętrznego charakteru.

W 2007 r. opracowane zostało kolejne studium zrealizowane na wniosek Komitetu Ministrów Rady Europy[105]. Wówczas szczególny nacisk został położony na wyzwania związane z potrzebą zapewnienia skutecznej kontroli nad służbami przy jednoczesnej konieczności zagwarantowania skuteczności działań prowadzonych przez służby, w szczególności w kontekście wojny z terroryzmem. Zaktualizowana wersja raportu opublikowana w 2015 r.[106] stanowi obecnie jedną z najbardziej kompleksowych analiz mających za przedmiot demokratyczną kontrolę nad służbami specjalnymi.

Komisja Wenecka wyszła z założenia, że służby muszą ponosić odpowiedzialność za swoją działalność, przy wyraźnym zaznaczeniu, że podstawową trudnością w zapewnieniu tej odpowiedzialności jest niejawny charakter działań realizowanych przez te służby. Oprócz kontroli sprawowanej przez poszczególne rodzaje władzy publicznej (parlament, rząd i sądy), Komisja Wenecka szczególny nacisk kładzie na potrzebę istnienia skutecznego mechanizmu skargowego, który wzmacnia odpowiedzialność służb. Z kolei w ramach rozpatrywania skarg istotne jest zapewnienie rzetelności, z drugiej zaś strony – zapewnienie ochrony uzasadnionym interesom publicznym (np. bezpieczeństwa). Ponadto mechanizm ten powinien obejmować możliwość sądowego dochodzenia odszkodowania za krzywdy wyrządzone przez służby.

Zaktualizowany raport Komisji Weneckiej z 2015 r. koncentruje się przede wszystkim na wyzwaniach związanych z masową inwigilacją[107]. Jego głównym przedmiotem jest tzw. *signals intelligence* (SIGINT), który – najogólniej rzecz ujmując – przejawia się w monitorowaniu telekomunikacji. Znacząco różni się od tradycyjnej inwigilacji, tzw. „*targeted surveillance*" zapoczątkowanej przez podejrzenie co do konkretnej osoby lub osób. Działania podejmowane w ramach SIGINT mają charakter proaktywny, przez co systemy nadzoru nad *signals intelligence* są słabsze niż względem tradycyjnych form inwigilacji. Jednym z argumentów, który ma uzasadnić taką słabszą kontrolę, jest założenie, że w mniejszym stopniu narusza prywatność (poprzez fakt, że monitoruje komunikację, nie zaś jej treść). Inny argument wskazuje, że SIGINT nakierowany jest na kontakty zewnętrzne, nie zaś na komunikację obywateli danego państwa. To z kolei rodzi szereg problemów następczych, w szczególności przy próbie określenia, której

103 Por.: *Opinion on the Federal Law on the Federal Security Services (FSB) of the Russian Federation* (CDL-AD(2012)015).

104 *Venice Commission, Internal Security Services in Europe, Report adopted at the 34th Plenary meeting* (Venice, 7 March 1998), CDL-INF(1998)006.

105 *Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session* (Venice, 1-2 June 2007), CDL-AD(2007)016-e.

106 *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) and updated by the Venice Commission at its 102nd Plenary Session* (Venice, 20-21 March 2015) CDL-AD(2015)010-e.

107 *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session* (Venice, 20-21 March 2015) DL-AD(2015)006-e.

jurysdykcji podlega działalność agencji prowadzącej taką działalność na terytorium innego państwa. Poza tym trzeba mieć na uwadze szybki rozwój technologii pozwalający na coraz szersze gromadzenie danych przez służby, jak również na fakt, że tak szybki rozwój technologii nie pozwala na równie szybką reakcję legislatora krajowego pozwalającą na uregulowanie takiej działalności. W kontekście SIGINT zwraca się uwagę m.in. na negatywne skutki, jakie masowa inwigilacja może mieć na wolność słowa i możliwy „efekt mrożący" (*chilling effect*) wywołany przez fakt prowadzenia takiej działalności[108]. Zaś w przypadku działań nakierowanych na zapewnienie „dobrobytu ekonomicznego państwa" (*„economic well-being of the nation"*) SIGINT może przybrać formy szpiegostwa gospodarczego[109].

Również na zlecenie **Komisarza Praw Człowieka Rady Europy** w 2015 r. opublikowana została analiza na temat demokratycznego nadzoru nad służbami[110]. Główny nacisk położono na potrzebę stworzenia przynajmniej jednego w pełni niezależnego organu zajmującego się kontrolą wszystkich aspektów działalności służb. Kontrola ta powinna obejmować również wszystkie aspekty niejawnego gromadzenia informacji o jednostce. Dlatego organ ten musi również posiadać uprawnienia do kontrolowania współpracy ze służbami innych państw. Uprzednia zgoda niezależnego organu (tu np. sądu) powinna dotyczyć najbardziej inwazyjnych elementów działalności służb. W świetle analizy Komisji Praw Człowieka, należy rozważyć wprowadzenie w systemach krajowych *„security-cleared public interest advocates"* w przypadku postępowań sądowych (np. sądowoadministracyjnych), w których dowodem są informacje niejawne[111]. Wśród rekomendacji, wskazano na potrzebę stworzenia skutecznego systemu rozpatrywania skarg, który będzie spełniał standardy rzetelnego postępowania (np. przez także niezależny organ kontrolny). W analizie sformułowano postulat, zgodnie z którym zewnętrzny organ kontrolny powinien mieć kompetencje do przerwania nielegalnie lub niepotrzebnie prowadzonej inwigilacji. Ponadto, musi istnieć wzmocniona relacja między ciałem kontrolnym a parlamentem, będącym źródłem legitymacji. Zewnętrznemu organowi kontrolnemu należy zagwarantować pełny dostęp do potrzebnych informacji oraz kompetencję/narzędzia do ich weryfikacji. Natomiast po stronie służb musi istnieć obowiązek współpracy z tym organem kontrolnym. Co więcej, dostęp organu kontrolnego do danych nie powinien być objęty *„third party rule"*. Dobrą praktyką powinno być również proaktywne udostępnianie informacji organowi kontrolnemu przez służby.

W analizie podkreślono znaczenie eksperckiego charakteru takiego organu przy jednoczesnym zapewnieniu odpowiednich warunków kadrowych i finansowych oraz gwarancji ochrony informacji. Ponadto, organ kontrolny powinien przedstawiać regularne raporty ze swojej działalności, zaś prowadzona przez niego kontrola powinna podlegać regularnej ewaluacji.

Na poziomie Rady Europy również **Zgromadzenie Parlamentarne** analizowało różne aspekty funkcjonowania służb, w szczególności zagadnienie masowej inwigilacji, dostępu do informacji publicznej oraz

108 *Joint statement: United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights – Joint Declaration on Surveillance Programs and their Imact on Freedom of Expression* (2013) – http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1. R. Ackland, *Mass surveillance makes us subjects of the state. That's chilling*, Guardian 26 maj 2015 r., http://www.theguardian.com/commentisfree/2015/may/26/mass-surveillance-makes-us-subjects-of-the-state-thats-chilling.

109 *Update of the 2007 Report…*, ·§ 77.

110 *Democratic and effective oversight of national security services. Issue paper published by the Council of Europe Commissioner for Human Rights*, CommDH/IssuePaper(2015)2. Analiza została przygotowana przez A. Willis'a, niezależnego współpracownika.

111 Por.: opinia Naczelnej Rady Adwockiej do ustawy o zmianie ustawy o Policji – http://www.adwokatura.pl/z-zycia-nra/opinia-nra-do-projektu-nowelizacji-ustawy-o-policji/.

ochrony sygnalistów. W rezolucji z kwietnia 2015 r. w sprawie masowej inwigilacji Zgromadzenie Parlamentarne wezwało Państwa Rady Europy do uzgodnienia i opracowania wielostronnego „kodeksu wywiadowczego" ("*intelligence codex*"), w którym ustalone zostałyby zasady współpracy służącej zwalczaniu terroryzmowi oraz przestępczości zorganizowanej. Takie uzgodnienie powinno obejmować również zasady prowadzenia inwigilacji oraz wymiany informacji zgromadzonych w legalny sposób[112].

4.2. Unia Europejska

Prawo Unii Europejskiej nie reguluje zasad funkcjonowania służb odpowiedzialnych za porządek publiczny w poszczególnych państwach. Jednak do kompetencji dzielonych należy przestrzeń wolności, bezpieczeństwa i sprawiedliwości, która obejmuje m.in. współpracę wymiarów sprawiedliwości w sprawach karnych oraz współpracę policyjną. Ponadto, w ramach Unii Europejskiej dochodzi do wymiany informacji między poszczególnymi służbami państw członkowskich, zarówno w formie zinstytucjonalizowanej (poprzez Europol), jak również w sposób mniej formalny (*Berne Club*). Ewentualne wzmocnienie współpracy wywiadowczej między Państwami Członkowskimi pozostaje szeroko dyskutowanym zagadnieniem, jednak z uwagi na wrażliwy przedmiot tej współpracy, nie należy się spodziewać, aby przybrał formę nowych rozwiązań instytucjonalnych.

Instytucją, która na bieżąco prowadzi dyskusję na temat różnych aspektów działań służb, jest **Parlament Europejski**, w szczególności **Komitet LIBE**. Przedmiotem zainteresowania LIBE były zarówno zagadnienie tajnych więzień CIA w Europie oraz masowej inwigilacji prowadzonej przez administrację USA oraz państwa europejskie. Działania podejmowane przez Parlament, których efekty mają najczęściej formę rezolucji, mają przede wszystkich charakter działań o charakterze politycznym.

Parlament Europejski niemal natychmiast po upublicznieniu materiałów ujawnionych przez E. Snowdena podjął prace mające na celu wyjaśnienie sytuacji związanej z masową inwigilacją obywateli UE. W rezolucji z 2014 r. wezwano Państwa Członkowskie m.in. do zapewnienia organom kontrolującym służby dostępu do wszystkich niezbędnych informacji, również tych dotyczących współpracy wywiadowczej z innymi państwami. W rezolucji wskazano, że modele kontroli nad służbami ukształtowane w latach 90-tych okazują się nieaktualne wobec współczesnych wyzwań wynikających z rozwoju technologii oraz jej wpływu na prawa i wolności.

Unia Europejska jest istotnym podmiotem w zakresie statusu służb odpowiadających za bezpieczeństwo również ze względu na **orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej** w Luksemburgu. Możliwość orzekania TSUE w odniesieniu do zagadnień związanych z funkcjonowaniem służb wynika z zakresu prawa Unii Europejskiej (obejmuje m.in. ochronę danych osobowych), jak również z uwagi na fakt, iż Karta Praw Podstawowych – mająca stanowić odzwierciedlenie standardów strasburskich - jest prawem pierwotnym Unii. Przykładowo w 2006 r. Unia Europejska zdecydowała się na stworzenie wspólnej unijnej regulacji dotyczącej tzw. retencji danych telekomunikacyjnych. Jej ocena pod kątem zgodności z Kartą Praw Podstawowych doprowadziła do unieważnienia dyrektywy.

112 Rezolucja 2045 (2015). Por. raport „Mass surveillance" , PACE Committee on Legal Affairs and Human Rights, Doc. 13734, 18 marca 2015 r.

*„27 Całokształt tych danych **może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób**, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają.*

(…)

*37 Należy stwierdzić, że – jak w pkt 77 i 80 swojej opinii zauważył rzecznik generalny – dyrektywa 2006/24 stanowi szczególnie daleko posuniętą ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty. Ponadto okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych jest dokonywane **bez poinformowania** o tym abonenta lub zarejestrowanego użytkownika, może – zgodnie z pkt 52 i 72 tej opinii – **wywołać u osób, których danych są zatrzymywane czy też wykorzystywane, poczucie, iż ich życie prywatne podlega stałemu nadzorowi**.*

(…)

*56 Co się tyczy kwestii, czy ingerencja, którą zakłada dyrektywa 2006/24, jest ograniczona do tego, co ściśle niezbędne, należy zauważyć, że zgodnie z art. 3 w związku z art. 5 ust. 1 dyrektywa ta zobowiązuje do zatrzymywania wszystkich danych o ruchu związanych z telefonią stacjonarną i mobilną, dostępem do Internetu, pocztą elektroniczną oraz telefonią internetową. Obowiązek ten dotyczy zatem wszystkich środków komunikacji elektronicznej, którymi posługiwanie się jest bardzo rozpowszechnione i ma coraz większe znaczenie w życiu codziennym każdego. Ponadto, zgodnie z art. 3 powyższej dyrektywy, obejmuje ona swoim zakresem stosowania wszystkich abonentów i zarejestrowanych użytkowników. **Ingeruje więc w prawa podstawowe prawie wszystkich mieszkańców Unii Europejskiej**.*

(…)

*59 Z drugiej strony, mając jednocześnie na celu przyczynienie się do walki z poważną przestępczością, dyrektywa ta **nie wymaga istnienia żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego**; w szczególności dyrektywa nie ogranicza się do zatrzymywania danych związanych albo z określonym czasem, określonym obszarem geograficznym lub określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, albo osobami, których zatrzymane dane z innych powodów mogłyby przyczynić się do zapobiegania poważnym przestępstwom oraz ich wykrywania lub ścigania.*

(…)

61 Ponadto dyrektywa nie określa żadnych materialnych i proceduralnych przesłanek, w przypadku zaistnienia których właściwe organy krajowe będą mogły uzyskać dostęp do danych i następnie je wykorzystać.

(…)

62 W szczególności dyrektywa 2006/24 nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby ograniczyć liczbę osób uprawnionych do uzyskiwania dostępu i późniejszego wykorzystywania zatrzymanych danych do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu. Przede wszystkim to uzyskanie przez właściwe organy krajowe dostępu do danych nie podlega uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które pilnowałyby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu, oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. Co więcej, dyrektywa nie nakazuje państwom członkowskim w sposób wyraźny ustanowienia takich mechanizmów.

(…)

66 Ponadto w odniesieniu do reguł związanych z bezpieczeństwem i ochroną danych zatrzymywanych przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności,

należy zauważyć, że dyrektywa 2006/24 nie ustanawia gwarancji takich jak te określone w art. 8 karty, pozwalających na zapewnienie skutecznej ochrony tych danych przed ryzykiem nadużyć oraz przed jakimkolwiek dostępem do nich i wykorzystywaniem w sposób niedozwolony. (...)"

Wyrok Trybunału Sprawiedliwości UE z 8 kwietnia 2014 r., C-293/12 i C-594/12

Z kolei Agencja Praw Podstawowych (*Fundamental Rights Agency*, dalej: FRA) w raporcie **„Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union - Mapping Member States' legal frameworks"**[113] opublikowanym w 2015 r. na zlecenie Parlamentu Europejskiego wskazała, że większość Państw Członkowskich reguluje zasady stosowania tzw. *targeted surveillance*, natomiast jedynie pięć państw reguluje *„signals intelligence"*[114]. Mimo, że większość państw członkowskich przewiduje kontrolę parlamentarną nad służbami, organy te nie mają zapewnionego bezwzględnego dostępu do wszystkich informacji gromadzonych przez służby. W 15 Państwach Członkowskich utworzono specjalne organy eksperckie zajmujące się kontrolą działalności służb. Ich kompetencje różnią się w zależności od państwa, ale co do zasady obejmują m.in. rozpatrywanie skarg na działania służb lub też prawo żądania informacji od służb w celu przeprowadzenia kontroli. W przypadku organów eksperckich, oprócz wiedzy prawniczej istotne znaczenie mają również kompetencje „techniczne". W raporcie FRA analizie poddano również organy ochrony danych osobowych w poszczególnych państwach członkowskich – wzmocnienie ich pozycji jest kluczowe dla zapewnienia środków ochrony praw jednostki (*remedies*). Odnotowano przy tym, że fragmentaryzacja i różnorodność różnych form kontroli skutkuje osłabieniem skuteczności środków ochrony praw. Również obowiązek notyfikacji jest różnorodnie uregulowany. W 8 państwach członkowskich, w tym w Polsce, prawo nie przewiduje w ogóle takiego obowiązku, a co za tym idzie nie przyznaje też prawa dostępu do zgromadzonych informacji dotyczących jednostki, w 20 państwach prawo przewiduje taki obowiązek, jest on jednak zróżnicowany, m.in. pod względem ram czasowych. Jedynie w przypadku dwóch państw obowiązek informowania odnosi się do działań prowadzonych w ramach *signals intelligence*. W zakresie ochrony sądowej, dotychczasowe badania FRA wskazywały na brak specjalizacji sędziów w zakresie ochrony danych osobowych. Pomimo jednolitych standardów wynikających z prawa Rady Europy czy ONZ, wśród państw członkowskich występuje duże zróżnicowanie w zakresie sposobu prowadzenia inwigilacji oraz jej kontrolowania.

4.3. Organizacja Narodów Zjednoczonych

Podobnie jak w przypadku systemu prawnego Rady Europy, również na poziomie uniwersalnym, tj. Organizacji Narodów Zjednoczonych, zagadnienia funkcjonowania służb są regulowane przez prawo międzynarodowe w zakresie, w jakim działania służb mają wpływ na prawa i wolności jednostki. Międzynarodowy Pakt Praw Obywatelski i Politycznych zobowiązuje Państwa do zapewnienia osobom poddanym ich jurysdykcji m.in. prawo do wolności osobistej i bezpieczeństwa (art. 9), prawo do sprawiedliwego rozpatrzenia sprawy przez niezawisły i bezstronny sąd (art. 14) czy prawo do ochrony życia prywatnego (art. 17).

113 Raport dostępny jest na stronie: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf.

114 Są to: Niemcy, Holandia, Francja, Szwecja, Wielka Brytania.

Na poziomie ONZ kwestia zarówno skutecznych działań służb wywiadowczych, jak również zagadnień związanych z kontrolą ich funkcjonowania, były w ostatnich latach analizowane jako element debaty nad międzynarodową wojną z terroryzmem. W 2005 r. Komisja Praw Człowieka ONZ powołała specjalnego sprawozdawcę ds. zwalczania terroryzmu oraz ochrony praw człowieka. Gromadzone przez niego informacje przyniosły szereg istotnych opracowań odnoszących się do zasad kontroli i nadzoru nad służbami wywiadowczymi w ramach działań antyterrorystycznych[115]. Mimo, że opracowane przez specjalnych sprawozdawców analizy i raporty mają charakter niewiążących rekomendacji, stanowią istotny punkt odniesienia dla prowadzenia debaty o potrzebie reformy służb w poszczególnych państwach. Zbiór „dobrych praktyk" opracowany przez specjalnego sprawozdawcę w 2010 r. podkreśla, iż dla zapewnienia, że służby działają zgodnie z prawem konieczna jest kontrola nad ich działalnością, realizowana przez różne podmioty władzy publicznej, w tym przez wyspecjalizowane organy kontrolne oraz fakt, że przynajmniej jeden z tych podmiotów jest w pełni niezależny od służb oraz władzy wykonawczej[116].

W grudniu 2013 r. Zgromadzenie Ogólne ONZ podjęło rezolucję ***„The right to privacy in the digital age"***[117]. W rezolucji tej wezwano państwa do stworzenia na poziomie krajowym niezależnych mechanizmów kontrolujących, ale również służących zapewnieniu odpowiedzialności państw za prowadzoną inwigilację i gromadzenie danych osobowych. Powołany w 2015 r. Specjalny Sprawozdawca ONZ ds. prawa do prywatności, opublikował w 2016 r. raport, w którym wskazał na główne wyzwania związane z ochroną prywatności. Zarysował przy tym 10-elementowy plan działania adresowany do poszczególnych państw. Odnosi się on nie tylko do potrzeby zagwarantowania odpowiednich procedur prawnych chroniących prywatność, ale również potrzeby podnoszenia świadomości oraz odpowiednich zabezpieczeń technologicznych[118].

4.4. Międzynarodowe standardy dotyczące transparentności działania służb

Zagwarantowanie możliwie najszerszej kontroli nad działalnością służb specjalnych wymaga również istnienia skutecznej kontroli społecznej w tym zakresie. Podstawowe narzędzie do realizacji tego celu, jakim jest dostęp do informacji publicznej, często napotyka ograniczenie w postaci blankietowej potrzeby ochrony bezpieczeństwa publicznego.

Dostęp do relewantnych informacji dotyczących bezpieczeństwa jest kluczowy, m.in. dla możliwości przeprowadzenia rzetelnej kontroli przez uprawnione organy działań służb. Jest to również niezbędne dla prawidłowego procesu decyzyjnego dotyczącego zapewnienia bezpieczeństwa na przyszłość[119]. Zgromadzenie Parlamentarne Rady Europy w rezolucji z 2013 r. wskazało, że sposobem chroniącym

115 M.in. raport z 2009 r. (A/HRC/10/3) analizował szereg zagadnień związanych z funkcjonowaniem służb: stosowanie „specjalnych technik śledczych", współpracę wywiadowczą służb i ich odpowiednią regulację na poziomie prawa krajowego czy zapewnienie transparentności działań służb.

116 „Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight" dostępny na stronie: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf. Fragment wytycznych (w języku angielskim) stanowi załącznik nr 3 do niniejszego dokumentu.

117 Rezolucja z 18 grudnia 2013 r., A/RES/68/167.

118 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64, 8 March 2016.

119 Por. National security and access to information, Parliamentary Assembly of Council of Europe, Committee on Legal Affairs and Human Rights, Doc. 13293, 3 września 2013 r.

przed nadużyciami związanymi ze zbyt szerokim utajnianiem informacji przez uprawnione do tego organy, powinien być mechanizm pozwalający na ujawnienie danej informacji z uwagi na istotny interes publiczny (np. fakt, że dana informacji stanowi dowód na poważne naruszenia praw człowieka)[120].

Na podobnym stanowisku stoją autorzy Zasad z Tshwane (*Tshwane Principles*)[121], dokumentu opracowanego przez 22 organizacje i ośrodki akademickie w porozumieniu z ponad 500 ekspertami z ponad 70 krajów[122]. Autorzy zasad wyszli z założenia, że „uzasadnione interesy bezpieczeństwa narodowego najlepiej chronione są wówczas, gdy opinia publiczna jest dobrze poinformowana o działaniach państwa, w tym podejmowanych w celu ochrony bezpieczeństwa narodowego".

Podobnie jak Zgromadzenie Parlamentarne Rady Europy, również Zasady z Tshwane wskazują na istnienie informacji, których upublicznienia może wymagać ważny interes publiczny. Zgodnie z Zasadą 10.: „Niektóre kategorie informacji (…) są szczególnie istotne dla interesu publicznego, ze względu na ich znaczenie dla procesu demokratycznej kontroli i rządów prawa. W związku z tym istnieją istotne przesłanki – a w niektórych przypadkach nadrzędny imperatyw – przemawiające za koniecznością proaktywnego ujawnienia takich informacji opinii publicznej." Wśród takich informacji są m.in.: te dotyczące naruszeń międzynarodowych praw człowieka i prawa humanitarnego, decyzji o użyciu siły zbrojnej bądź nabyciu broni masowego rażenia, odpowiedzialności za naruszenia konstytucji i ustaw oraz innych przypadków nadużycia władzy.

W przypadku, w którym – wbrew powyższym zasadom – zbyt duża ilość informacji jest utajniona, może dojść do sytuacji określanej w literaturze jako *overclassification*, którego rezultatem z kolei mogą się okazać tzw. przecieki – tzn. ujawnienia (ze względu na interes publiczny) informacji utajnionych świadczących np. na poważne naruszenia praw człowieka. W świetle Zasad z Tshwane przypadki tzw. „chronionego ujawnienia" szkodliwego postępowania powinny wiązać się z zapewnieniem ochrony dla osób podających takie informacje do publicznej wiadomości – tzw. sygnalistów (*whistleblowers*)[123]. Ochrona ta powinna przejawiać się w istnieniu odpowiednich procedur umożliwiających zgłoszenie występujących nieprawidłowości, zaś po stronie organów przyjmujących takie zgłoszenie występuje obowiązek ochrony tożsamości funkcjonariuszy, którzy zgłosili nieprawidłowości[124].

120 Rezolucja Zgromadzenia Parlamentarnego 1954 (2013), 2 października 2013 r., pkt 9.5.

121 Polskie tłumaczenie dokumentu zostało opracowane przez Helsińską Fundację Praw Człowieka m.in. we współpracy z Open Society Justice Initiative w ramach „Monitoringu procesu legislacyjnego w obszarze wymiaru sprawiedliwości". Tłumaczenie dostępne jest pod adresem: http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/03/Globalne-zasady-internet-popr.pdf (dostęp w dniu 13 maja 2016 r.).

122 Dokument został opublikowany w 2013 r. Prace nad nim zostały prowadzone w trakcie 14 spotkań zorganizowanych na całym świecie przy wsparciu Open Society Justice Initiative. W powstaniu dokumentu uczestniczyli m.in.: Frank La Rue, Specjalny Sprawozdawca ONZ ds. Prawa do Wolności Opinii i Wypowiedzi, Ben Emmerson, Specjalny Sprawozdawca ds. Promocji oraz Ochrony Praw Człowieka Podczas Zwalczania Terroryzmu, Pansy Tlakula, Specjalna Sprawozdawczyni Afrykańskiej Komisji Praw Człowieka i Ludów (ACHPR) ds. Wolności Wypowiedzi i Dostępu do Informacji, Catalina Botero, Specjalna Sprawozdawczyni Organizacji Państw Amerykańskich ds. Wolności Wypowiedzi i Dostępu do Informacji; oraz Dunja Mijatovic, Przedstawicielka Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE) ds. Wolności Mediów.

123 Zasada 37.

124 B. Grabowska-Moroz, Czy służby specjalne podlegają kontroli obywatelskiej? Dostęp do informacji publicznej a bezpieczeństwo narodowe w świetle standardów międzynarodowych (Zasady z Tshwane) [w:] Prawa człowieka – współczesne wyzwania międzynarodowe, publikacja dostępna jest na stronie: https://pl.boell.org/sites/default/files/prawa_czlowieka_wyzwania_miedzynarodowe_hfpc_raport.pdf, s. 79.

Powyższe rekomendacje opierają się na założeniu, że istnienie takich mechanizmów ochronnych będzie zachęcało funkcjonariuszy publicznych do zgłaszania nieprawidłowości, a tym samym – w konsekwencji ich działań – na eliminowanie przypadków naruszania prawa. Z tego względu w 2014 r. Komitet Ministrów Rady Europy wezwał Państwa Rady Europy do stworzenia „normatywnych, instytucjonalnych oraz sądowych ram", które pozwolą na zapewnienie ochrony osobom dokonującym zgłoszeń o zaistniałych nieprawidłowościach[125].

125 Rekomendacje CM/Rec(2014)7 z 30 kwietnia 2014 r. (Por. rezolucję Zgromadzenia Parlamentarnego Rady Europy 2060(2015) z 23 czerwca 2015 r.)

5. Konkluzje

Niniejsza analiza z uwagi na swój ograniczony charakter nie jest w stanie objąć swym zakresem całości zagadnień związanych z funkcjonowaniem służb posiadających uprawnienia do prowadzenia czynności operacyjno-rozpoznawczych. Wydaje się jednak, że ogrom zarysowanych zagadnień wynikających m.in. z prawa międzynarodowego prowadzi do wniosku o potrzebie przeprowadzenia rzetelnej i – prawdopodobnie – długotrwałej debaty na temat kształtu służb specjalnych i policyjnych funkcjonujących w Polsce. Nieadekwatne gwarancje przed nadużywaniem uprawnień oraz niejawny charakter działań operacyjnych będzie skutkował niskim poziomem ochrony praw i wolności. Z tego względu, nawet pobieżna analiza standardów konstytucyjnych i międzynarodowych pozwala na sformułowanie szeregu wniosków i rekomendacji:

1. Model nadzoru nad służbami został ukształtowany w latach 90-tych XX w. i stanowił odpowiedź na wyzwania związane z okresem transformacji ustrojowej. Nie został on jednak zweryfikowany pod kątem nowych wyzwań wynikających z nowych zagrożeń dla bezpieczeństwa, rozwoju technologii oraz jej wpływu na ochronę prywatności.

2. Dotychczasowe zmiany w służbach specjalnych, policyjnych oraz skarbowych nie były poprzedzane debatą publiczną na temat ich modelu, zakresu kompetencji służb, sposobu nadzoru nad nimi. Przeprowadzenie takiej rzetelnej debaty jest niezbędne dla zapewnienia zaufania społecznego do działań realizowanych przez służby. Debata taka musi obejmować również współczesne wyzwania związane z zagrożeniami prawa do prywatności wynikającymi m.in. z ciągłego rozwoju technologii.

3. Przeprowadzenie rzetelnej debaty publicznej będzie miało wpływ na wzmocnienie kontroli społecznej nad służbami stanowiącymi część administracji rządowej. W tym celu należy przeprowadzić weryfikację, na ile praktyka polskiego prawa dostępu do informacji publicznej realizuje wytyczne wyrażone w „Zasadach z Tshwane". W ramach podwyższenia transparentności działań służb konieczne jest wprowadzenie przejrzystych i rzetelnych mechanizmów zbierania informacji o skali prowadzonych wobec jednostek czynności operacyjno – rozpoznawczych. W postulat wzmocnienia kontroli społecznej nad służbami wpisuje się również potrzeba zapewnienia (m.in. na poziomie regulacji ustawowej) skutecznych mechanizmów ochrony sygnalistów.

4. Prawo powinno przewidywać, że kontrola nad działalnością służb będzie kompletna, tj. będzie obejmowała całość ich funkcjonowania. Kontrola taka powinna obejmować zarówno legalność, jak i efektywność prowadzonych działań. Dlatego niezbędne jest, aby taką całościową kontrolę wykonywał organ ekspercki, jednak w pełni niezależny od służb i Rady Ministrów[126]. Zapewnienie skutecznej i niezależnej kontroli jest kluczowe dla zagwarantowania odpowiedzialności służb za błędy lub nadużycia.

5. Jako element wykonania wyroków *Al Nashiri* i *Abu Zubaydah* służby powinny przeprowadzić – pod nadzorem Kolegium ds. służb specjalnych oraz pod kontrolą parlamentarnej Komisji ds. służb specjalnych – weryfikację standardów ochrony praw człowieka w ramach prowadzonej współpracy wywiadowczej ze służbami zagranicznymi.

126 Rekomendacja R (87) 15 Komitetu Ministrów Rady Europy o Ochronie Danych Osobowych wykorzystywanych w sektorze policji z 17 września 1987 r.: *1.1. Każde Państwo Członkowskie powinno dysponować niezależnym i zewnętrznym w stosunku do Policji organem nadzorczym, upoważnionym do czuwania nad przestrzeganiem Zasad zawartych w niniejszej Rekomendacji.*

6. Konieczne jest stworzenie skutecznego mechanizmu skargowego, poprzez m.in. wykonanie postanowienia sygnalizacyjnego S 2/06, tj. rozważenie wprowadzenia obowiązku notyfikacji lub innej procedury pozwalającej jednostce na zweryfikowanie, czy była inwigilowana.

7. Wpływ na skuteczność niezależnej kontroli nad służbami mają również regulacje procesowe, dlatego należy uchylić rozwiązania wprowadzone ustawą z 11 marca 2016 r., które ograniczają sądową kontrolę dowodów zebranych podczas pracy operacyjnej i wykorzystanych w postępowaniu karnym.

8. Ponadto, należy wzmocnić kontrolę nad procedurą zarządzania kontroli operacyjnej. Należy rozważyć poszerzenie zakresu kontroli sądowej poprzez objęcie nią procedury zarządzania przesyłki niejawnie nadzorowanej, zakupu kontrolowanego, a także pozyskania danych telekomunikacyjnych w postaci wykazu połączeń i danych o lokalizacji (w szczególności w odniesieniu do osób wykonujących zawody zaufania publicznego lub w wypadkach innych niż pilne).

9. Należy rozważyć utworzenie w postępowaniu sądowoadministracyjnym tzw. specjalnego pełnomocnika realizującego dostęp do informacji niejawnych zgromadzonych przez służby w ramach realizacji ich zadań.

10. Wskazane jest również, aby ustawa z 15 stycznia 2016 r. oraz Prawo o prokuraturze zostały poddane – możliwie szybko – kontroli pod kątem ich zgodności z Konstytucją.

Załączniki

Załącznik nr 1. Wybrane sprawy prowadzone przez HFPC przed sądami administracyjnymi.

Przedmiot sprawy	Stan sprawy	Rozstrzygnięcie
Statystyki stosowania przez ABW kontroli operacyjnej	Sprawa częściowo zakończona wyrokiem NSA z 21 września 2012 r. I OSK 1393/12	NSA stwierdził brak przesłanek do odmowy udostępnienia informacji publicznej nt. statystyk stosowania przez ABW kontroli operacyjnych
Statystyki stosowania przez CBA kontroli operacyjnej	Sprawa zakończona wyrokiem WSA w W-wie z 7 lutego 2012 r. II SA/Wa 2695/11	WSA stwierdził brak przesłanek do odmowy udostępnienia informacji publicznej nt. statystyk stosowania przez CBA kontroli operacyjnych w okresie: 2006 -31 marca 2009 r.
Stosowanie systemu GPS przez Policję w ramach kontroli operacyjnej	Sprawa zakończona wyrokiem WSA w W-wie II SA/Wa 20/13 z 17 kwietnia 2013 r. po przekazaniu sprawy do ponownego rozpoznania przez NSA wyrokiem z 30 sierpnia 2012 r. I OSK 397/12	Sprawa prawomocnie zakończona. KGP został zobowiązany do udzielenia odpowiedzi. Jego zdaniem możliwe jest stosowanie w ramach kontroli operacyjnej systemu GPS.
Korzystanie przez CBA z systemu XKeyscore, a także programów umożliwiających przeszukiwanie Internetu za pomocą słów kluczowych	Wyrok WSA w W-wie z 28 marca 2014 II SA/Wa 141/14, wyrok NSA (częściowo uwzględniający skargę kasacyjną) z 18 sierpnia 2015 r. I OSK 1679/14, wyrok WSA w W-wie (oddalający skargę po ponownym rozpoznaniu sprawy) z 26 listopada 2015 r. II SA/Wa 1537/15.	Sprawa w toku
Korzystanie przez ABW z systemu XKeyscore, a także programów umożliwiających przeszukiwanie Internetu za pomocą słów kluczowych	Wyrok WSA w W-wie z 25 czerwca 2014 r. II SA/Wa 710/14	Sprawa w toku
Korzystanie przez SWW z systemu XKeyscore, a także programów umożliwiających przeszukiwanie Internetu za pomocą słów kluczowych	Wyrok WSA w W-wie (częściowo uwzględniający) 8 października 2014 r. II SA/Wa 616/14	Sprawa w toku
Korzystanie przez SKW z systemu XKeyscore, a także programów umożliwiających przeszukiwanie Internetu za pomocą słów kluczowych	Wyrok WSA w W-wie z oddalający) 11 września 2014 r. II SA/Wa 723/14	Sprawa w toku
Korzystanie przez CBA z programu Remote Control System	Wyrok z 13 lutego 2015 r. II SA/Wa 1670/14	Sprawa w toku
Przekazywanie NSA przez ABW informacji w ramach programów OAKSTAR oraz partnerstwo, w programie Buffalogreen	Wyrok WSA w W-wie z 14 stycznia 2015 r. II SA/Wa 1623/14	Sprawa w toku
Korzystanie przez CBA z programu umożliwiającego przeszukiwanie za pomocą słów kluczowych	Wyrok WSA w W-wie (częściowo oddalający) z 16 listopada 2015 r. II SA/Wa 1171/15	Sprawa w toku

Załącznik nr 2. Rezolucje Parlamentu Europejskiego w sprawie masowej inwigilacji.

Rezolucja PE z dnia 12 marca 2014 r.

„Parlament Europejski (...)

BW. mając na uwadze, że służbom wywiadowczym w społeczeństwach demokratycznych udzielono specjalnych uprawnień i **zapewniono im możliwości ochrony praw podstawowych, demokracji oraz rządów prawa**, praw obywateli i państwa przed poważnymi zagrożeniami wewnętrznymi i zewnętrznymi, **podlegają one również kontroli sądowej oraz rozliczalności demokratycznej**; mając na uwadze, że służby te dysponują szczególnymi uprawnieniami i możliwościami wyłącznie w tym zakresie; mając na uwadze, że uprawnienia te powinny być wykorzystywane **w ramach granic prawnych wyznaczonych prawami podstawowymi, demokracją i praworządnością**, zaś ich stosowanie powinno podlegać **skrupulatnej kontroli**, w przeciwnym wypadku służby tracą legitymizację oraz ryzykują podważeniem demokracji;

BX. mając na uwadze fakt, że dozwolony jest pewien stopień poufności w przypadku służb wywiadowczych z uwagi na potrzebę uniknięcia narażania prowadzonych operacji, ujawnienia trybu funkcjonowania służb lub zagrożenia życia agentów, przy czym **poufność taka nie może być nadrzędna w stosunku do zasad demokratycznej i sądowej kontroli i inspekcji ich działalności**, jak również przejrzystości lub ich wyłączać, szczególnie jeżeli chodzi o poszanowanie praw podstawowych i praworządności, które stanowią podwaliny społeczeństwa demokratycznego;

BY. mając na uwadze, że większość istniejących krajowych mechanizmów oraz organów nadzoru utworzono lub zrekonstruowano w latach 90. XX w. i **niekoniecznie przystosowano je do gwałtownego rozwoju politycznego i technologicznego, jaki można było zaobserwować w ostatnim dziesięcioleciu**, a który doprowadził do aktywniejszej międzynarodowej współpracy wywiadu, która obejmuje także wymianę danych osobowych na wielką skalę, jak również do zatarcia granicy dzielącej wywiad i działania w zakresie egzekwowania prawa;

BZ. mając na uwadze, że demokratyczny **nadzór nad działaniami wywiadowczymi** jest w dalszym ciągu prowadzony **wyłącznie na szczeblu krajowym**, pomimo rosnącej wymiany informacji między państwami członkowskimi UE oraz między państwami członkowskimi a państwami trzecimi; mając na uwadze, że istnieje coraz większa **przepaść między poziomem międzynarodowej współpracy a możliwościami nadzoru ograniczonymi do szczebla krajowego**, co skutkuje niewystarczającą i nieskuteczną kontrolą demokratyczną;

CA. mając na uwadze, że **krajowe organy nadzoru często nie mają pełnego dostępu do informacji** otrzymywanych od zagranicznej agencji wywiadu, co może prowadzić do luk, w których międzynarodowa wymiana informacji może odbywać się bez adekwatnej kontroli; mając na uwadze, że problem ten dodatkowo pogłębia tzw. zasada osoby trzeciej lub zasada kontroli organu zastrzegającego, opracowana z myślą o umożliwieniu organowi zastrzegającemu sprawowania kontroli nad dalszym rozpowszechnianiem należących do niego szczególnie chronionych danych, która to zasada jest jednak niestety często rozumiana jako mająca zastosowanie również do kontroli służb odbiorcy;

CB. mając na uwadze, że prywatne i publiczne inicjatywy reformatorskie na rzecz przejrzystości są kluczowe dla zapewnienia publicznego zaufania do działań agencji wywiadu; (…)

75. podkreśla, że chociaż nadzór nad działaniami służb wywiadowczych powinien opierać się zarówno na legitymacji demokratycznej (silnych ramach prawnych, upoważnieniu ex ante i weryfikacji ex post), jak i na odpowiednich zdolnościach technicznych i wiedzy fachowej, **większości obecnych unijnych i amerykańskich organów nadzoru zdecydowanie brakuje ich obu, zwłaszcza zdolności technicznych**;

76. podobnie jak w przypadku Echelonu, wzywa wszystkie parlamenty narodowe, które jeszcze tego nie uczyniły, **do przyznania kompetencji prawnych w zakresie prowadzenia dochodzeń w ramach znaczącego nadzoru nad działaniami wywiadowczymi sprawowanego przez parlamentarzystów lub organy eksperckie**; wzywa parlamenty narodowe do zapewnienia tego, aby takie komisje/organy nadzoru posiadały wystarczające zasoby, fachową wiedzę techniczną i środki prawne, w tym prawo do prowadzenia kontroli na miejscu, umożliwiające im sprawowanie skutecznej kontroli nad służbami wywiadowczymi;

77. wzywa do powołania grupy złożonej z posłów i ekspertów w celu zbadania, w sposób przejrzysty i we współpracy z parlamentami krajowymi, **zaleceń służących nasileniu demokratycznej kontroli, w tym kontroli parlamentarnej nad służbami wywiadowczymi, oraz bardziej intensywnej współpracy w zakresie kontroli w UE**, w szczególności w jej

wymiarze transgranicznym; uważa, że grupa ta powinna rozważyć możliwość ustanowienia **minimalnych europejskich norm lub wytycznych w zakresie nadzoru** (ex ante i ex post) nad służbami wywiadowczymi w oparciu o obowiązujące sprawdzone wzorce postępowania i zalecenia organów międzynarodowych (ONZ, Rady Europy), w tym kwestię uznawania organów nadzorczych za osobę trzecią na podstawie „zasady osoby trzeciej" lub „zasady kontroli organu zastrzegającego", dotyczące sprawowania nadzoru nad wywiadem z państw obcych i pociągania go do odpowiedzialności, kryteria zwiększonej przejrzystości oparte na podstawie ogólnej zasady dostępu do informacji i tak zwanych „zasad z Tshwane" , a także zasady dotyczące ograniczenia czasu trwania i zakresu nadzoru, dbając o to, by były one proporcjonalne i ograniczone do celu nadzoru;

(…)

79. wzywa państwa członkowskie do wykorzystania najlepszych praktyk, aby **poprawić dostęp ich organów nadzoru do informacji na temat działań wywiadowczych** (w tym informacji niejawnych i informacji pochodzących od innych służb) oraz ustanowienia uprawnień w zakresie przeprowadzania wizyt na miejscu, solidnego zbioru uprawnień w zakresie przesłuchań, odpowiednich zasobów i fachowej wiedzy technicznej, zdecydowanej niezależności od ich rządu oraz obowiązku sprawozdawczego wobec ich parlamentów;

80. wzywa państwa członkowskie do **rozwoju współpracy między organami nadzoru, zwłaszcza w ramach europejskiej sieci ds. monitorowania krajowych służb wywiadowczych (ENNIR)**".

Rezolucja PE z dnia 29 października 2015 r.

„Parlament Europejski (…)

20. w pełnym poszanowaniu faktu, że parlamenty narodowe mają pełne uprawnienia do nadzorowania krajowych służb wywiadowczych, wzywa wszystkie parlamenty narodowe, które jeszcze tego nie uczyniły, **do ustanowienia prawdziwego nadzoru nad działalnością wywiadowczą i do oceny tej działalności oraz do zadbania o to, by takie komisje/organy nadzorujące posiadały dostateczne zasoby, fachową wiedzę techniczną i środki prawne oraz dostęp do wszystkich odnośnych dokumentów, aby móc skutecznie i w niezależny sposób nadzorować służby wywiadowcze oraz wymianę informacji z innymi służbami wywiadowczymi**; ponownie wyraża swoje zobowiązanie do ścisłej współpracy z parlamentami narodowymi na rzecz zadbania o wprowadzenie skutecznych mechanizmów nadzoru, w tym poprzez dzielenie się najlepszymi praktykami i stosowanie wspólnych norm;

(…)

22. uważa, że należy wspierać i w większym stopniu **wykorzystywać istniejące narzędzia współpracy między organami nadzoru**, np. europejską sieć ds. monitorowania krajowych służb wywiadowczych (ENNIR), ewentualnie poprzez wykorzystywanie potencjału platformy IPEX do wymiany informacji między parlamentami narodowymi zgodnie z jej zakresem i możliwościami technicznymi;

(…)

24. podkreśla, że aby Unia Europejska i jej państwa członkowskie mogły zagwarantować pewność prawa, potrzebna jest **wspólna definicja „bezpieczeństwa narodowego"**; zauważa, że brak jednoznacznej definicji umożliwia arbitralność oraz naruszanie praw podstawowych i zasad praworządności przez kręgi wykonawcze i wywiadowcze w UE;

25. zachęca Komisję i państwa członkowskie do wprowadzenia do ustawodawstwa umożliwiającego gromadzenie danych osobowych lub inwigilację obywateli europejskich przepisów dotyczących wygaśnięcia i przedłużenia; podkreśla, że takie przepisy są istotnymi gwarancjami służącymi zadbaniu o to, by instrument naruszający prywatność był regularnie analizowany pod względem jego niezbędności i proporcjonalności w społeczeństwie demokratycznym".

Załącznik nr 3. Zestawienie dobrych praktyk dotyczących kontroli nad służbami wywiadowczymi (w języku angielskim).

Good practices on legal and institutional frameworks for intelligence services and their oversight (fragment)

Practice 5. **Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law**. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

Practice 6. **Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law**. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

Practice 7. **Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates**. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

(…)

Practice 9. **Any individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution**. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services **are independent of the intelligence services and the political executive**. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

(…)
Practice 14. **States are internationally responsible for the activities of their intelligence services and their agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is**. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services.

(…)

Practice 17. **Members of intelligence services are legally obliged to refuse superior orders that would violate national law or international human rights law**. Appropriate protection is provided to members of intelligence services who refuse orders in such situations.

(…)

Practice 25. **An independent institution exists to oversee the use of personal data by intelligence services**. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

Practice 26. Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence

service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information.

Practice 27. Intelligence services are not permitted to use powers of arrest and detention if they do not have a mandate to perform law enforcement functions. They are not given powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities.
(…)
Practice 30. Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on **national law that outlines clear parameters for intelligence exchange**, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

Practice 33. Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

Practice 34. **Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.**

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA

Helsińska Fundacja Praw Człowieka
ul. Zgoda 11,
00-018 Warszawa
tel.: (+48) 22 828 10 08
(+48) 22 828 69 96
(+48) 22 556 44 40
fax: (+48)22 556 44 50
www.hfhr.pl

MONITORING PROCESU LEGISLACYJNEGO W OBSZARZE WYMIARU SPRAWIEDLIWOŚCI

Program „Monitoring procesu legislacyjnego w obszarze wymiaru sprawiedliwości" realizowany jest przez Helsińską Fundację Praw Człowieka dzięki dotacji otrzymanej z programu „Obywatele dla Demokracji" finansowanego z Funduszy EOG.
http://programy.hfhr.pl/monitoringprocesulegislacyjnego/