Do druku nr 3765

SZEF KANCELARII SENATU

Ewa Polkowska
SK- 0401-15/15

Warszawa, dnia 29 lipca 2015 r.

SEKRETARIAT SZEFA KS
L.dz. .....
Data wpływu 29. 07. 2015

Szanowny Pan
Lech Czapla
Szef Kancelarii Sejmu

Szanowny Panie Ministrze,

W związku z przesłaniem do Sejmu, podjętej przez Senat na 79. posiedzeniu uchwały z dnia 24 lipca 2015 r. w sprawie wniesienia do Sejmu projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (wraz z projektem tej ustawy), pragnę przekazać Panu Ministrowi stanowiska podmiotów zewnętrznych przesłane do Senatu w toku postępowania zmierzającego do wypracowania przedmiotowego projektu ustawy.

Stanowiska w sprawie projektu ustawy przedstawiły następujące podmioty:

1) Minister Administracji i Cyfryzacji,
2) Krajowa Rada Sądownictwa,
3) Szef Agencji Bezpieczeństwa Wewnętrznego,
4) Prezes Urzędu Komunikacji Elektronicznej,
5) Generalny Inspektor Ochrony Danych Osobowych,
6) Szef Biura Ochrony Rządu,
7) Szef Centralnego Biura Antykorupcyjnego,
8) Prokuratoria Generalna Skarbu Państwa,
9) Sąd Najwyższy,
10) Fundacja Panoptykon,
11) Prokurator Generalny,
12) Minister Sprawiedliwości,
13) Minister Finansów,
14) Helsińska Fundacja Praw Człowieka,
15) Komendant Główny Straży Granicznej,
16) Naczelna Rada Adwokacka,
17) Minister Obrony Narodowej.

z wyrazami szacunku

ul. Wiejska 6, 00-902 Warszawa, tel. 22 694-94-10, fax 22 694-92-24, e-mail secretary.general@senat.gov.pl

Warszawa, dnia 10 lipca 2015 r.

RZECZPOSPOLITA POLSKA
MINISTER
ADMINISTRACJI I CYFRYZACJI

DP-WL.0210.788.2015

Dot.: BPS/KU-034/967/22/15

Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

Szanowny Panie Przewodniczący,

w odpowiedzi na pismo z dnia 26 czerwca 2015 r., w którym przekazano prośbę o zaopiniowanie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967), niniejszym przedstawiam co następuje.

Projekt ustawy ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), w którym Trybunał orzekał o konstytucyjności przepisów zawierających regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych w ustawach: o Policji, Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Centralnym Biurze Antykorupcyjnym, Straży Granicznej, kontroli skarbowej, Żandarmerii Wojskowej i wojskowych organach porządkowych, a także Służbie Celnej. W projekcie przewiduje się również zmianę ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.), zwanej dalej „Pt", poprzez uchylenie art. 180g. Przedmiotowa zmiana wprowadzona została w związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej w sprawach połączonych C-293/12 oraz C-594/12, który przesądził o nieważności *dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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 zmieniająca dyrektywę 2002/58/WE*, zwanej dalej „dyrektywą retencyjną". Uregulowania z art. 180g Pt, wynikające bezpośrednio z dyrektywy retencyjnej, przewidują obowiązek przekazywania do Prezesa UKE informacji o:

- łącznej liczbie przypadków, w których uprawnionym podmiotom, służbie celnej, sądowi i prokuratorowi były udostępnione dane retencyjne;

- czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty wymienione w poprzednim punkcie wniosku lub ustnego żądania o ich udostępnienie;
- łącznej liczbie przypadków, w których wniosek lub ustne żądanie, o których mowa w poprzednim punkcie, nie mogły być zrealizowane

oraz przekazywania przez Prezesa UKE powyższych informacji uzyskanych od przedsiębiorców telekomunikacyjnych do Komisji Europejskiej.

W związku z uznaniem dyrektywy retencyjnej za nieważną i brakiem innych podstaw w prawodawstwie UE do utrzymania powyższych obowiązków, art. 180g Pt powinien zostać uchylony. W zakresie powyżej wskazanej zmiany uwag zatem nie zgłaszam.

Wątpliwości interpretacyjne budzi natomiast brzmienie art. 1 pkt 1 lit. h projektu ustawy (dotyczącego zmienianego art. 19 ust. 21 pkt 5 ustawy o Policji). Wyjaśnienia wymaga, czy przedmiotem upoważnienia jest określenie wzorów dokumentów wchodzących w zakres rejestrów, czy wzorów rejestrów. Jeżeli zamierzeniem projektodawcy było stworzenie upoważnienia do określenia wzorów rejestrów to należy pamiętać, iż elementem określenia sposobu prowadzenia rejestrów (vide ust. 21 pkt 4) może być wymóg ich prowadzenia w postaci elektronicznej. Zasadnym jest nadto wskazanie, iż zgodnie z art. 14 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114), organy administracji rządowej zobowiązane są do zapewnienia działania rejestrów publicznych, używając systemów teleinformatycznych. Należy wskazać, iż z uwagi na różnicę w nośnikach danych, nie jest możliwym określenie na dokumencie papierowym wzoru rejestru prowadzonego w postaci elektronicznej. W odniesieniu do rejestru elektronicznego możliwe jest określenie zakresu przetwarzanych danych, który może być określony na podstawie art. 19 ust. 21 pkt 4 ustawy o Policji. Analogiczną uwagę zgłaszam do art. 2 pkt 1 lit. h, art. 3 pkt 3 lit. h, art. 6 pkt 3 lit. h, art. 7 pkt 2 lit. g, art. 9 pkt 1 lit. g, art. 10 pkt 1 lit. g senackiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.

Z poważaniem,

z up. Marek Wójcik,
Podsekretarz Stanu w Ministerstwie Administracji i Cyfryzacji
/-podpisano bezpiecznym podpisem elektronicznym
weryfikowanym przy pomocy ważnego kwalifikowanego
certyfikatu/

KU 214/15

PRZEWODNICZĄCY
KRAJOWEJ RADY SĄDOWNICTWA

Warszawa, 8 lipca 2015 r.

Nr WO-020-93/15

Dot.: BPS/KU-034/967/2/15

Pan Senator Piotr ZIENTARSKI
Przewodniczący
Komisji Ustawodawczej Senatu RP

Szanowny Pan Przewodniczący

W załączeniu, uprzejmie przesyłam odpis opinii Krajowej Rady Sądownictwa z dnia 7 lipca 2015 r. *w przedmiocie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw* (druk senacki nr 967).

Z poważaniem

Wiceprzewodniczący
Krajowej Rady Sądownictwa

płk Piotr Raczkowski
sędzia Wojskowego Sądu Okręgowego

OPINIA

KRAJOWEJ RADY SĄDOWNICTWA

z dnia 7 lipca 2015 r.

w przedmiocie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw

Krajowa Rada Sądownictwa, po zapoznaniu się z treścią projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw co do zasady opiniuje go pozytywnie, z tym jednakże zastrzeżeniem, że w zależności od liczby spraw, które będą wpływały do sądów, a będą dotyczyły spraw związanych z kontrolą pozyskiwania danych telekomunikacyjnych i pocztowych sądy, a w szczególności Sąd Okręgowy w Warszawie, mogą zostać obciążone dodatkowo dużą liczbą spraw do rozpoznania, co może wiązać się z obciążeniem budżetu w zakresie zapewnienia obsady sędziowskiej i urzędniczej w sytuacji potrzeby utworzenia wydziału kontroli danych telekomunikacyjnych i pocztowych. Krajowa Rada Sądownictwa sygnalizuje ponadto, że w przedmiocie proponowanej zmiany, projektodawca nie przedstawił wielkości i źródła pokrycia ewentualnych kosztów związanych z utworzeniem takiego wydziału w strukturze organizacyjnej danego sądu.

Wiceprzewodniczący
Krajowej Rady Sądownictwa

płk Piotr Raczkowski
sędzia Wojskowego Sądu Okręgowego

KU 224/15

RZECZPOSPOLITA POLSKA

Warszawa, 15 07. 2015 r.

Szef
Agencji Bezpieczeństwa Wewnętrznego

gen. bryg. Dariusz Łuczak

P - 1121/B-22002/2015

Pan Senator Piotr ZIENTARSKI

PRZEWODNICZĄCY KOMISJI
USTAWODAWCZEJ
SENATU
RZECZYPOSPOLITEJ POLSKIEJ

Odpowiadając na pismo Pana Przewodniczącego nr BPS/KU-034/967/14/15 z dnia 26 czerwca 2015 r., przy którym został przesłany projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967) uprzejmie informuję, iż Agencja Bezpieczeństwa Wewnętrznego zgłasza następujące uwagi do przedmiotowego projektu ustawy, w zakresie nowelizacji ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej na potrzeby pisma „ustawą o ABW oraz AW":

1) ***art. 7 pkt 1 – dot. art. 5 ust. 1 pkt 2 lit. a*** – ABW proponuje dodanie do katalogu przestępstw wymienionych w tym przepisie również art. 141 i art. 142 Kodeksu karnego. Przepisy te dotyczą odpowiednio przestępstwa:
   a) służby w obcym wojsku lub w obcej organizacji wojskowej, popełnionego przez obywatela polskiego nie posiadającego zgody właściwego organu albo pełnienia najemnej służby wojskowej zakazanej przez prawo międzynarodowe,
   b) prowadzenia zaciągu obywateli polskich lub przebywających na terytorium RP cudzoziemców do służby wojskowej w obcym wojsku lub obcej organizacji wojskowej albo prowadzenia zaciągu do zakazanej przez prawo międzynarodowe wojskowej służby najemnej, albo opłacania takiej służby najemnej, jej organizowania (...).

   Powyższa propozycja wynika z faktu, iż ABW prowadziła i prowadzi postępowania przygotowawcze w tego rodzaju sprawach. Propozycja ABW jest tym bardziej zasadna, iż coraz częściej występują przypadki prowadzenia zaciągu do służby najemnej w obcym wojsku lub w obcej organizacji wojskowej, a zwłaszcza do organizacji militarnych o charakterze terrorystycznym.

2) ***art. 7 pkt 1 – dot. art. 5 ust. 1 pkt 2 lit. b*** – ABW proponuje wykreślenie z katalogu przestępstw wymienionych w tym przepisie art. 224a Kodeksu karnego, penalizującego fałszywe zawiadomienie o nieistniejącym zdarzeniu, zagrażającym życiu lub zdrowiu wielu osób lub mieniu w znacznych rozmiarach, wywołującym czynność właściwej instytucji użyteczności publicznej lub organu ochrony bezpieczeństwa, porządku publicznego lub zdrowia, mającą na celu uchylenie tego zagrożenia.
Wskazane przestępstwo, jakkolwiek mogące negatywnie oddziaływać na odczucie bezpieczeństwa obywateli oraz zmuszające organy władzy publicznej do podjęcia określonych czynności, nie spełnia jednak przesłanek określonych dla przestępstwa o charakterze terrorystycznym. Organy władzy publicznej muszą wówczas podjąć czynności zmierzające wyłącznie do uchylenia nieistniejącego zagrożenia.

3) ***art. 7 pkt 2 – dot. art. 27 ust. 6*** – zdaniem ABW zaproponowana przez Senat RP definicja kontroli operacyjnej jest niepełna i w znaczący sposób utrudni realizację przez ABW ustawowych zadań.

Nadto ABW zwraca uwagę na to, że zaproponowana w senackim projekcie ustawy definicja kontroli operacyjnej pomija możliwość stosowania przez ABW podglądu: transmisji internetowej, wiadomości e-mail, danych zawartych w systemie informatycznym oraz pomija możliwość stosowania przez ABW kontroli zawartości przesyłek.

Ponadto analizując propozycje zawarte w art. 27 ust. 6 pkt 1 i 2 senackiego projektu ustawy, ABW uprzejmie informuje, iż kontrola operacyjna polegająca na podsłuchu rozmów telefonicznych w praktyce realizowana może być równocześnie z podglądem informacji wysyłanych i otrzymywanych z objętego kontrolą operacyjną telefonu. Powyższe wiąże się z rozwojem technologicznym aparatów telefonicznych (smartfony, iphony, itp.), które obecnie pozwalają na wykonywanie wielu – poza rozmowami – czynności np. wysyłanie/odbieranie wiadomości sms, e-mail, przeglądanie zawartości internetu, prowadzenie rozmów z wykorzystaniem komunikatorów.

W odniesieniu do propozycji zawartej w art. 27 ust. 6 pkt 4 senackiego projektu ustawy, ABW uprzejmie wyjaśnia, iż nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu pozwala jedynie na zbieranie informacji o przybliżonym położeniu w danym czasie osoby lub rzeczy. Zastosowanie wymienionych środków technicznych nie pozwala natomiast pozyskiwać, gromadzić, utrwalać informacji będących w posiadaniu określonej osoby, przekazywanych w toku wymiany korespondencji, bezpośrednich rozmów telefonicznych, czy też informacji przekazywanych za pośrednictwem sieci telekomunikacyjnych. W związku z powyższym możliwość uzyskiwania informacji w ramach nadzoru elektronicznego osób, miejsc i przedmiotów oraz środków transportu nie powinno być uznane za kontrolę operacyjną i tym samym nie powinno podlegać rygorom przewidzianym w art. 27 ustawy o ABW oraz AW (konieczności uzyskiwania uprzedniej zgody Prokuratora Generalnego oraz Sądu Okręgowego w Warszawie).

W związku z powyższym ABW proponuje przyjąć w art. 27 ust. 6 definicję kontroli operacyjnej w następującym brzmieniu:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
1) kontrolowaniu treści korespondencji;
2) kontrolowaniu zawartości przesyłek;
3) wykorzystaniu środków technicznych pozwalających na uzyskanie i utrwalenie informacji w postaci:
a) obrazu lub dźwięku,
b) danych zawartych w systemie informatycznym,
c) treści przekazywanych za pomocą sieci telekomunikacyjnych.”.

Przedstawiając powyższą propozycję ABW pragnie zauważyć, iż doprecyzowanie środków technicznych, którymi ABW może posługiwać się w ramach prowadzenia kontroli operacyjnej zmierzającej do uzyskania i utrwalenia informacji, czyni zadość wyrokowi Trybunału Konstytucyjnego, który w uzasadnieniu określił, iż ustawodawca powinien zdefiniować, jak należy rozumieć termin „środek techniczny".

Ponadto ABW nadmienia, iż powyższa propozycja brzmienia art. 27 ust. 6 jest zbieżna z propozycją definicji kontroli operacyjnej przedstawioną przez Zespół ds. zmian legislacyjnych wynikających z wyroku Trybunału Konstytucyjnego K 23/11 z dnia 30 lipca 2014 r., który powstał na podstawie decyzji Przewodniczącego Kolegium do Spraw Służb Specjalnych z dnia 8 października 2014 r. – Pani Ewy Kopacz – Prezesa Rady Ministrów, pod przewodnictwem Przewodniczącego Zespołu – Podsekretarza Stanu w Ministerstwie Spraw Wewnętrznych Pana Grzegorza Karpińskiego.

W konsekwencji zmiany brzmienia definicji kontroli operacyjnej z art. 27 ust. 6 ABW proponuje nadanie ust. 6a i 6b następującego brzmienia:

„6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6 pkt 3, polegające na:

1) realizacji czynności, o których mowa w art. 23 ust. 1 pkt 6;
2) uzyskiwaniu danych, o których mowa w art. 28 ust. 1;
3) uzyskiwaniu danych ze zbiorów danych, o których mowa w art. 34.

6b. Informacje, o których mowa w ust. 6, mogą być pozyskiwane za pomocą:

1) kontroli manualnej lub technicznej przesyłek i korespondencji;
2) środków technicznych służących do odbioru i rejestracji obrazu lub dźwięku;
3) środków technicznych zapewniających dostęp do danych zawartych w systemach informatycznych lub przekazywanych w systemach telekomunikacyjnych.".

Przedstawiona przez ABW propozycja brzmienia ust. 6a ma na celu utworzenie zamkniętego katalogu czynności, które nie będą stanowić kontroli operacyjnej.

Podobnie rzecz się ma z przedstawioną przez ABW propozycją brzmienia ust. 6b mającą na celu utworzenie również zamkniętego katalogu metod, którymi ABW będzie mogła posługiwać się przy uzyskiwaniu informacji w ramach kontroli operacyjnej.

Zdaniem ABW propozycja brzmienia ust. 6a i 6b w pełniejszym zakresie czyni zadość wyrokowi Trybunału Konstytucyjnego i wyeliminuje wątpliwości interpretacyjne, co do zakresu realizacji przez ABW jej ustawowych zadań.

ABW - jako służba specjalna - realizuje zadania o charakterze kontrwywiadowczym i powyższe propozycje, w tym definicja kontroli operacyjnej, najpełniej i najbardziej precyzyjnie powinny określać możliwości stosowania przez ABW tej kontroli.

4) ***art. 7 pkt 2 lit. f - dot. art. 27 ust. 16b – 16f oraz ust. 18*** – w opinii ABW nowelizacja ustawy o ABW oraz AW w wymienionym zakresie jest zbędna, z uwagi na fakt, iż przytoczone przepisy są przepisami natury technicznej i nie powinny stanowić materii ustawowej. W obowiązującym stanie prawnym sprawy z tego zakresu są uregulowane na poziomie rozporządzenia Prezesa Rady Ministrów z dnia 30 lipca 2013 r. w sprawie sposobu dokumentowania prowadzonej przez Agencję Bezpieczeństwa Wewnętrznego kontroli operacyjnej (...) – (Dz. U. poz. 1048). Ponadto przy jakiejkolwiek zmianie np.: w zakresie nazewnictwa stosowanych przez ABW rejestrów, czy też zmianie sposobu prowadzenia rejestrów z rejestru papierowego na rejestr elektroniczny będzie należało przeprowadzić długotrwałą procedurę legislacyjną związaną ze zmianą ustawy. Nowelizacja rozporządzenia jest znacznie szybszym i prostszym zabiegiem legislacyjnym i ma znacznie ograniczony zakres uzgodnień z zainteresowanymi podmiotami. W związku z powyższym ABW proponuje, aby w/w przepisów nie zamieszczać w ustawie o ABW

oraz AW, a w dodatku nowelizacja w tym obszarze wykracza poza zakres zmian wynikających z orzeczenia Trybunału Konstytucyjnego.

5) ***art. 7 pkt 3 – dot. art. 28 ust. 1*** – zdaniem ABW:

a) pkt 2 powinien otrzymać następujące brzmienie:

„2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe;".

Zaproponowane w senackim projekcie nowelizacji ustawy odesłanie do art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe, w opinii ABW, nie jest prawidłowe. Art. 2 ustawy – Prawo pocztowe określa jedynie, co stanowi, i co nie stanowi, usługi pocztowej. Natomiast art. 82 ust. 1 pkt 1 ustawy – Prawo pocztowe, do którego proponuje odesłać ABW, wskazuje wprost uprawnione podmioty, w tym ABW, do uzyskiwania od operatorów pocztowych: danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację podmiotów korzystających z tych usług.

Ponadto ABW informuje, iż analogiczne rozwiązanie (odesłanie do art. 82 ust. 1 pkt 1 ustawy – Prawo pocztowe) przewidywał projekt nowelizacji ustawy o ABW oraz AW przygotowany przez Zespół Ministra Grzegorza Karpińskiego, jak i rządowy projekt ustawy o ABW (druk sejmowy nr 2295 – art. 33 ust. 1 pkt 2).

b) po pkt 2 ABW proponuje dodać nowy pkt 3 w brzmieniu:

„3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną".

Uprawnienie ABW do pozyskiwania danych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, ma istotne znaczenie w odniesieniu do realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1, 2 lub 5 ustawy o ABW oraz AW. Chodzi bowiem o możliwość uzyskania przez ABW danych m.in. o użytkownikach np. Internetu lub danych o numerach IP. Dane te mają charakter równorzędny z danymi określonymi w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne.

SZEF
Agencji Bezpieczeństwa Wewnętrznego
gen. bryg. Dariusz ŁUCZAK

Warszawa, dnia 6 lipca 2015 r.

PREZES
URZĘDU KOMUNIKACJI ELEKTRONICZNEJ

Magdalena Gaj

DP-0330-7/14 (5)

Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

W związku z otrzymanym projektem ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, mającym na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), pozwolę sobie zgłosić następujące uwagi do przedmiotowego projektu.

1. Niektóre z proponowanych rozwiązań normatywnych należy doprecyzować poprzez zastąpienie ich określeniami precyzyjnie wskazującymi zarówno zakres, jak i znaczenie poszczególnych norm projektu. W kilku jednostkach redakcyjnych projekru użyto określenia „polska ustawa karna" (strony 1, 9, 20) oraz określenia „ustawa karna polska" (strona 29). Wydaje się, że użyte sformułowania nie spełniają zasady określoności prawa. Nie jest bowiem jasne, jakiej ustawy dotyczyć będzie przedmiotowy przepis. Odesłanie w zaproponowanej formule można bowiem interpretować jako odesłanie do wszystkich przepisów o charakterze karnym zawartych w polskich ustawach albo do przepisów ustawy z dnia 2 sierpnia 1997 r. - Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.).

2. W propozycji brzmienia przepisów dotyczących kontroli operacyjnej w art. 19 ust. 6 pkt 4 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 i 529) użyto niejasnego pojęcia „nadzór elektroniczny". Pragnę zaznaczyć, iż w kontekście braku definicji tego pojęcia oraz jego niejasnego znaczenia zakres projektowanego przepisu może budzić wątpliwości interpretacyjne. Biorąc pod uwagę, iż przedmiotowy przepis wyznacza zakres czynności podejmowanych w ramach kontroli operacyjnej, która prowadzona jest niejawnie i w znaczący sposób ingeruje w prawa obywateli, należy podkreślić, że powinien być on sformułowany w możliwie najbardziej precyzyjnym stopniu. Analogiczna uwaga dotyczy przepisów zawartych na stronach 9, 20, 30, 35, 42 i 48 projektu.

3. W propozycji zmiany brzmienia art. 19 ust. 6 ustawy o Policji - w stosunku do obecnie obowiązującego art. 19 ust. 6 pkt 2 ustawy o Policji - zaproponowano skreślenie „kontrolowania zawartości przesyłek" z katalogu czynności prowadzonych w ramach kontroli operacyjnej. Natomiast w dodawanym ust. 20a w pkt 1 ustawy o Policji zaproponowano, aby dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej stanowiły nośniki, na których utrwalona została m. in. zawartość przesyłek. Proponowana konstrukcja może zatem budzić wątpliwości, ponieważ jeżeli kontrola zawartości przesyłek nie należy do czynności podejmowanych w ramach kontroli operacyjnej to trudno mówić o sporządzaniu dokumentacji z takich czynności podczas stosowania kontroli operacyjnej. Analogiczna uwaga dotyczy proponowanych zmian przepisów zawartych na stronach 20 i 21, 30 i 32, 35 i 37, 42 i 43 oraz 48 i 50 projektu.

4. Na stronie 4 projektu ustawy w art. 20c ust. 1 ustawy o Policji zaproponowano, aby Policja mogła mieć udostępniane dane telekomunikacyjne i pocztowe „w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw". Projektowany przepis dotyczy czynności w znaczący sposób ingerujących w prawa obywateli, a zatem powinien on być sformułowany w możliwie najbardziej precyzyjnym stopniu. Uwagę tę powinno się również odnieść do analogicznych przepisów proponowanych w innych ustawach.

   Projektowane przepisy stanowiące podstawę udostępniania danych telekomunikacyjnych i pocztowych mogą budzić również szereg innych wątpliwości. Tytułem przykładu pragnę wskazać, iż w art. 28 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm) zaproponowano przesłankę pozyskiwania przez Agencję Bezpieczeństwa Wewnętrznego danych telekomunikacyjnych w sposób umożliwiający bardzo szeroką jej interpretację („w celu rozpoznawania zagrożeń").

   Pragnę również wskazać, iż należy mieć na uwadze, iż precyzyjne, niebudzące wątpliwości określenie przypadków, w których dane telekomunikacyjne i pocztowe mogą być udostępniane, konieczne jest również z uwagi na obowiązek zapewnienia zgodności projektowanych przepisów z prawem europejskim. W szczególności, w odniesieniu do danych telekomunikacyjnych, należy uwzględnić przepisy art. 5, art. 6, art. 8 ust. 1 – 4, art. 9 i art. 15 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.07.2002, str. 37).

5. W odniesieniu do projektowanych art. 20c ust. 2 i 3 oraz 20cb ust. 3 ustawy o Policji (strona 5 i 7) należy odnotować, że przepisy te używają pojęć „podmiot prowadzący działalność telekomunikacyjną" oraz „operator świadczący usługi pocztowe", podczas gdy w obecnie obowiązującym art. 19 ust. 12 tej ustawy jest mowa o „podmiotach wykonujących działalność telekomunikacyjną" oraz o „podmiotach świadczących usługi pocztowe" (przepis ten nie jest nowelizowany w projekcie). W związku z tym proponuję ujednolicić terminologię używaną w ustawie o Policji w przedmiotowym zakresie. Niniejszą uwagę należy również odnieść odpowiednio do przepisów innych zmienianych ustaw.

6. Na stronie 6 projektu w art. 20c w ust. 8 ustawy o Policji określono, że Komendant Główny Policji lub osoba przez niego upoważniona powołuje komisję, która ma niszczyć dane oraz materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, które nie zawierają informacji mających znaczenie dla postępowania karnego lub nie są niezbędne dla realizacji ustawowych zadań. Z czynności komisji sporządza się protokół. W związku z tym, że w innych przepisach

projektu (art. 20ca ust. 3 oraz art. 20cb ust. 5 i 6 ustawy o Policji) dotyczących niszczenia materiałów lub danych nie została określona procedura powoływania komisji ani odesłanie do wskazanej komisji, powstaje pytanie, czy ta sama komisja będzie niszczyć materiały, o których mowa w przywołanych jednostkach redakcyjnych projektu.

7. W projektowanej zmianie art. 20da ustawy o Policji w ust. 1 w części wspólnej należy rozważyć odesłanie do odpowiedniego stosowania także art. 20c ust. 7 i 8 ustawy o Policji. Wydaje się bowiem, że także w przypadku przetwarzania danych udostępnionych w celu poszukiwania osób zaginionych należy ograniczyć okres tego przetwarzania oraz zastosować mechanizm weryfikacji dotyczącej potrzeby dalszego przetwarzania tych danych.

8. Projektowane art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (strona 38), art. 32 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.) (strona 45) oraz art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym (strona 51), dają odpowiednim służbom możliwość uzyskiwania danych telekomunikacyjnych i pocztowych, jednakże w przeciwieństwie do analogicznych przepisów proponowanych w innych ustawach, nie odnoszą się do możliwości przetwarzania tych danych (por. np. część wspólna w projektowanym art. 20c ust. 1 ustawy o Policji). W związku z tym proponuję rozważenie wprowadzenia odpowiednich zmian w tym zakresie.

9. Projektowany art. 18b ust. 6 ustawy o Centralnym Biurze Antykorupcyjnym (strona 53) przewiduje obowiązek zniszczenia danych telekomunikacyjnych niezawierających informacji mających znaczenie dla prowadzonego postępowania. Przepis ten nie odnosi się jednak do danych pocztowych, w związku z czym wymaga uzupełnienia.

10. W ramach uwag o charakterze redakcyjnym pragnę zauważyć, że na stronie:

    a) 13, 45, 51 – odpowiednio w: art. 10b ust. 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.), art. 32 ust. 5 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz art. 18 ust. 3 ustawy o Centralnym Biurze Antykorupcyjnym po wyrazach „usługi pocztowe" należy dodać wyraz „lub",

    b) 56 – w projektowanym art. 75 dc ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.) wyrazy „w zakresie art. 180c oraz art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne" należy zastąpić wyrazem „telekomunikacyjnych" – stosownie do skrótu wprowadzonego w projektowanym art. 75d ust. 1 tej ustawy.

Z poważaniem

Do wiadomości:
Pan Marek Wójcik
Podsekretarz Stanu
w Ministerstwie Administracji i Cyfryzacji

Urząd Komunikacji Elektronicznej
Warszawa, ul. Kasprzaka 18/20, tel. (22) 53 49 272 , fax (22) 53 49 130

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia 15 lipca 2015 r.

DOLiS – 033 – 284/15/BG /62915/15

Pan
Piotr Zientarski
Przewodniczący Komisji Ustawodawczej

Senat Rzeczypospolitej Polskiej
ul. Wiejska 6
00 – 902 Warszawa

Szanowny Panie Przewodniczący,

w odpowiedzi na pismo z dnia 26 czerwca 2015 r. – znak: BPS/KU-034/967/25/15 – uprzejmie informuję, że do **projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)**, Generalny Inspektor Ochrony Danych Osobowych zgłasza następujące uwagi.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) za niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji uznał przepisy art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej, **w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy Prawo telekomunikacyjne**.

W opiniowanym projekcie ustawy zaproponowano, aby podmiotem wyznaczonym do kontroli nad uzyskiwaniem danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku – w odniesieniu do Policji, Straży

ul. Stawki 2
00-193 Warszawa
tel. 860 70 81
fax. 860 70 90

Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Zdaniem Generalnego Inspektora **zaproponowana przez senatorów forma kontroli jest niewystarczająca** – przepisy nie nakładają bowiem na Policję i służby innych nowych obowiązków poza przekazywaniem sądom raz na 6 miesięcy sprawozdań obejmujących liczbę i rodzaj pozyskanych danych telekomunikacyjnych lub pocztowych, podstawę prawną ich pozyskania, rodzaje przestępstw, w związku z którymi wystąpiono o dane.

W ramach kontroli sąd **może** zapoznać się z materiałami uzasadniającymi udostępnianie danych, a w przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych, podlegają one zniszczeniu (s. 8, 15, 19, 28, 41, 47, 53, 56 projektu). Uprzednia kontrola miałaby mieć miejsce jedynie wtedy, gdy z materiałów sprawy wynikałoby, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego. Jednak co do zasady, **proponowany w projekcie model w rzeczywistości przewiduje jedynie fakultatywną kontrolę następczą** (zachodzi zatem podstawowa obawa, że w praktyce sądy nie będą z tego uprawnienia korzystać), co nie może zostać uznane za należyte wykonanie wyroku Trybunału Konstytucyjnego.

Przypomnieć należy, iż Trybunał uznał za konieczne wprowadzenie proceduralnego wymogu, którym jest **kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa**. Status ustrojowy i zakres ustawowych kompetencji takiego organu ma gwarantować efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa. Konieczne jest, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to uznać należy za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej (jak wskazane zostało w cz. III, pkt 2 i 3 uzasadnienia wyroku – np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05).

Trybunał nie przesądził jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Zdaniem Trybunału, nie jest wobec tego wykluczone – w

odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Jak wskazano w wyroku, „regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. **Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach.** W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb".

Skoro pozyskiwanie danych telekomunikacyjnych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, **brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć.** Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji.

Z całą pewnością nie można uznać za wystarczający modelu kontroli zaproponowanego przez projektodawcę, który nie przewiduje jako zasady **każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych.** Nadal nie istnieje zatem gwarancja odpowiedniego poziomu ochrony prywatności i tajemnicy komunikowania się osób, których dane są pozyskiwane przez Policję i służby. Nie przesądzając jakie konkretnie organy miałyby zajmować się taką kontrolą, Generalny Inspektor stoi na stanowisku, iż projektowane przepisy powinny szczegółowo określać mechanizmy kontroli. Wskazać również należy, iż **kontrola następcza powinna być traktowana jako wyjątek i stosowana jedynie w sprawach niecierpiących zwłoki.** W każdym jednak przypadku niezależny organ powinien ocenić czy pozyskanie danych telekomunikacyjnych jest w konkretnej sytuacji rzeczywiście niezbędne i należycie uzasadnione oraz czy cel, w którym dane są udostępniane nie mógłby zostać zrealizowany przy użyciu innych, mniej ingerujących w prywatność jednostki środków.

Zapowiedzi uregulowania w przepisach zewnętrznej kontroli przez niezależny autonomiczny organ, znalazły się już w opracowanym w 2011 r. *Raporcie dotyczącym retencji danych telekomunikacyjnych. Propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych.* Przedmiotowy raport podkreślał ograniczone możliwości takiej

kontroli wobec służb specjalnych realizujących swoje kompetencje w zakresie wykonywania czynności operacyjno - rozpoznawczych i jako remedium proponował model niezależnego, powoływanego przez parlament, organu kontrolnego, którego celem byłaby **kontrola przestrzegania przez służby specjalne Konstytucji Rzeczypospolitej Polskiej oraz innych przepisów prawa, szczególnie w zakresie praw i wolności obywatelskich**. W dokumencie tym dość kompleksowo odniesiono się do przedmiotowej instytucji, omawiając tak istotne z punktu widzenia jego działania zagadnienia, jak powoływanie i skład, zadania, kompetencje oraz wyniki pracy organu kontrolnego.

Ponadto należy przypomnieć, że w informacji o wynikach kontroli *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, Najwyższa Izba Kontroli wskazała, iż „sięganie po dane retencyjne stanowi istotną ingerencję w prawa i wolności obywatelskie, w szczególności prawo do prywatności. (...) W obecnym stanie prawnym nie istnieje żaden podmiot, który mógłby sprawować rzeczywistą kontrolę nad wykorzystaniem tego środka przez uprawnione organy, służby i formacje. **Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej. W 24 państwach taką kontrolę sprawuje sąd lub prokuratura albo niezależny organ administracyjny**".

Również przedstawiony w styczniu 2012 r. projekt unijnej dyrektywy o przetwarzaniu danych osobowych w policji i w wymiarze sprawiedliwości w sprawach karnych wyraźnie wskazuje na konieczność istnienia niezależnego organu, który sprawowałby zewnętrzną kontrolę nad danymi retencyjnymi wykorzystywanymi przez służby.

Z uwagi na powyższe, Generalny Inspektor wskazuje, iż projektowane przepisy przewidywać powinny **każdorazową, obowiązkową kontrolę przez niezależny organ adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych.**

Odnosząc się do innych zmian wprowadzonych przez projekt, za niedostateczną realizację wyroku Trybunału Konstytucyjnego należy uznać przepisy ograniczające czas przeprowadzania kontroli operacyjnej przez Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu (s. 36 projektu), Służbę Kontrwywiadu Wojskowego (s. 42 projektu) oraz Centralne Biuro Antykorupcyjne (s. 49 projektu). Zgodnie ze stanowiskiem Trybunału, „ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. (...) Ustawodawca musi mieć także na uwadze, że **w demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów**". Tymczasem, w przypadku wyżej wymienionych służb, dopuszczalne byłoby wydawanie kolejnych

postanowień o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (bez ograniczenia, że może być to tylko jedno postanowienie). W praktyce, proponowane rozwiązanie stwarzałoby zatem możliwość bezterminowego prowadzenia czynności operacyjno-rozpoznawczych, co stoi w sprzeczności ze standardami konstytucyjnymi i intencją Trybunału.

Projekt przewiduje ponadto prowadzenie rejestrów postanowień, zgód, wniosków i zarządzeń dot. kontroli operacyjnej (s. 3, 11, 21, 31, 37, 43, 49 projektu). Założenie, iż sposób prowadzenia tych rejestrów oraz wzory dokumentów wchodzących w ich zakres miałyby określać rozporządzenia, nie może zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych. Należy w tym miejscu zwrócić uwagę na stanowisko Trybunału Konstytucyjnego, wyrażone w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007), „zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej". Wymóg umieszczenia bezpośrednio w ustawie wszystkich zasadniczych elementów regulacji prawnej musi być stosowany ze szczególnym rygoryzmem, gdy regulacja ta dotyczy korzystania przez obywateli z ich praw i wolności (wyrok Trybunału Konstytucyjnego z dnia 25 maja 1998 r., sygnatura U 19/97). Podobnie orzekł Trybunał w wyroku z dnia 18 grudnia 2014 r. (sygnatura K 33/13), dotyczącym tworzenia rejestrów danych medycznych na podstawie rozporządzenia przez ministra zdrowia. W związku z powyższym, **przepisy rangi ustawowej powinny regulować zasadnicze kwestie dotyczące prowadzenia rejestru**, w szczególności zaś: kto jest administratorem danych osobowych, katalog danych znajdujących się w rejestrze, okres przechowywania tych danych, zasady udostępniania informacji z rejestru, krąg podmiotów mających dostęp do danych.

Kolejną kwestią, która budzi zastrzeżenia Generalnego Inspektora jest określenie w projekcie, że dane telekomunikacyjne i pocztowe są przetwarzane przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym nie rzadziej niż co 5 lat dokonuje się weryfikacji potrzeby ich dalszego przetwarzania (s. 6, 13, 17, 26, 39, 46, 51, 55 projektu). Tego rodzaju **sformułowanie jest zbyt szerokie, stwarza ryzyko swobodnej oceny i w praktyce może doprowadzić do nieuzasadnionego, bezterminowego przechowywania danych**, co stoi w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego. Okres przetwarzania danych telekomunikacyjnych i pocztowych powinien być określony w sposób precyzyjny, tak, aby wyeliminować ryzyko nadużyć (istniejące obecnie wobec faktu, iż nie przewidziano zewnętrznej kontroli niezbędności dalszego przetwarzania danych

do realizacji ustawowych zadań) a ewentualna weryfikacja potrzeby ich dalszego przetwarzania powinna odbywać się częściej niż raz na 5 lat.

Podsumowując, w opinii Generalnego Inspektora Ochrony Danych Osobowych, zaproponowana nowelizacja ustawy o Policji i innych ustaw nie stwarza wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowi pełnej realizacji wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

Z poważaniem

GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

BIURO OCHRONY RZĄDU

Tel. (+48 22) 606 50 00
Tel. (+48 22) 606 51 01
Tel. (+48 22) 602 51 36
Fax (+48 22) 843 26 02

ul. Podchorążych 38, 00-463 Warszawa, www.bor.gov.pl, e-mail: kancelaria@bor.pl

Warszawa, dnia ..... 2015 r.

Egz. Nr ...

GSZ.[illegible]/2015

Pan
Piotr Zientarski

Przewodniczący
Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

W odpowiedzi na pismo z dnia 26 czerwca 2015 r. nr BPS/KU034/967/19/15 dotyczącego projektu ustawy o zmianie ustawy o Policji i innych ustaw, uprzejmie przedstawiam następujące stanowisko.

Druk senacki nr 967 obejmujący nowelizację ustawy o Policji i innych ustaw ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11). W przedmiotowym orzeczeniu Trybunał Konstytucyjny zbadał konstytucyjność przepisów ustaw zawierających regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych, zawartych w ustawach: o Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego.

Pragnę zaznaczyć, iż w ustawie z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (Dz. U. z 1014 r, poz. 170 ze zm.) nie zostały umieszczone normy prawne obejmujące powyższe regulacje. Mocą art. 12 ustawy, BOR realizuje jedynie uprawnienia profilaktyczne i administracyjno - porządkowe.

Z tych względów niemożliwym jest ustosunkowanie się formacji do przedłożonych w rzeczonym projekcie norm prawnych.

Szef
Biura Ochrony Rządu

gen. bryg. Krzysztof Klimek

Wykonano w 2 egz.:
Egz. Nr 1 – adresat
Egz. Nr 2 – ad acta
Wykonał: K. Kowalewska

RZECZPOSPOLITA POLSKA

SZEF CENTRALNEGO
BIURA ANTYKORUPCYJNEGO

Paweł Wojtunik

P-402/15/W

Warszawa, 15 lipca 2015 r.

Przewodniczący
Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

Pan Piotr Zientarski

Szanowny Panie Przewodniczący!

Odpowiadając na pismo z 26 ub.m., sygn. BPS/KU-034/967/18/15, przedstawiam opinię Centralnego Biura Antykorupcyjnego odnośnie do projektu *ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw* (druk nr 967). Uwagi dotyczą proponowanych zmian w ustawie o CBA, jednak przez analogię odnieść je można także do ustaw regulujących funkcjonowanie innych służb.

Art. 17 ust. 5

Przede wszystkim należy zauważyć, że wykonanie wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. akt K 23/11, nie wymaga zmiany tego przepisu. Art. 17 ustawy o CBA (podobnie jak analogiczne przepisy innych ustaw) został uznany za niezgodny z Konstytucją wyłącznie w zakresie, w jakim nie przewidywał „gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne".

Niemniej jednak, odnosząc się do zawartej w projekcie definicji kontroli operacyjnej, należy wskazać, że w pkt 1 i 2 użyty w niej został termin „podsłuch", będący dotychczas raczej określeniem potocznym. Brak jego legalnej definicji niesie ze sobą ryzyko niewłaściwej, zawężającej interpretacji, ograniczającej podsłuch do możliwości niejawnego zapoznania się z informacją za pomocą zmysłu słuchu, nie uwzględniającej natomiast elementu utrwalenia dźwięku. Rozważyć zatem należy zastąpienie terminu „podsłuch" bardziej precyzyjnym określeniem „uzyskiwanie i utrwalanie dźwięku, w szczególności treści rozmów". Gdyby natomiast termin „podsłuch" miał w projekcie pozostać, należałoby w proponowanym art. 17 ust. 5b wskazać, że chodzi o użycie środków technicznych niezbędnych do uzyskiwania i utrwalania informacji.

Zawarta w projekcie definicja kontroli operacyjnej wymaga uzupełnienia o kontrolę zawartości przesyłek. Należy bowiem zwrócić uwagę, że termin „korespondencja" odnosi się

jedynie do wymiany informacji. Co za tym idzie, kontrola korespondencji oznaczać będzie kontrolę przesyłanych (w postaci papierowej bądź elektronicznej) informacji. Istotą kontroli zawartości przesyłek jest sprawdzenie, jakie przedmioty czy też substancje są w nich przesyłane.

Krytycznie ocenić należy włączenie do pojęcia „kontrola operacyjna" elektronicznego nadzoru osób, miejsc i przedmiotów oraz środków transportu. Należy zwrócić uwagę, że przywołane w pkt III.2.4 uzasadnienia wyroku TK orzecznictwo Europejskiego Trybunału Praw Człowieka wskazuje, że monitorowanie aktywności jednostek w przestrzeni publicznie dostępnej za pomocą urządzeń lokalizacyjnych (np. GPS) nie wymaga stosowania tak wysokich standardów odnoszących się do jakości regulacji, jak np. stosowanie podsłuchów czy pozyskiwanie treści korespondencji.

Podsumowując powyższe uwagi należy stwierdzić, że w ocenie CBA ingerencja w obecne brzmienie art. 17 ust. 5 nie jest niezbędna. Gdyby jednak przyjąć, iż istnieje potrzeba znowelizowania tego przepisu, to powinien on otrzymać następujące brzmienie:

Art. 17. 5. Kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji lub zawartości przesyłek poprzez:
   a) ich otwarcie lub
   b) wykorzystanie środków technicznych służących sprawdzeniu treści korespondencji lub zawartości przesyłek bez ich otwierania;
2) uzyskiwaniu i utrwalaniu, poprzez wykorzystanie środków technicznych, treści przekazywanych przy pomocy środków łączności przewodowej lub bezprzewodowej, w szczególności treści rozmów telefonicznych lub korespondencji elektronicznej;
3) uzyskiwaniu i utrwalaniu obrazu lub dźwięku, w szczególności treści rozmów, w miejscach nie będących miejscami publicznymi przy pomocy środków technicznych służących uzyskiwaniu i utrwalaniu obrazu lub dźwięku;
4) uzyskiwaniu i utrwalaniu danych zawartych w systemach lub urządzeniach teleinformatycznych przy pomocy środków technicznych służących uzyskaniu dostępu i utrwaleniu tych danych.

Art. 17 ust. 5a

Celem tego przepisu - z uwagi na szeroki charakter definicji kontroli operacyjnej - jest wskazanie, jakie czynności z tej definicji są wyłączone. W ocenie CBA winien on uwzględniać przede wszystkim dokumentowanie przez funkcjonariusza lub osobę udzielającą mu pomocy wykonywanych czynności operacyjno-rozpoznawczych poprzez rejestrację obrazu lub dźwięku. Należy podkreślić, że dokumentowane w ten sposób są czynności, w których funkcjonariusz lub osoba udzielająca mu pomocy bierze osobisty udział, a zatem zna treść rozmów czy przebieg wydarzeń, trudno jest zatem mówić o naruszeniu np. prawa do prywatności czy tajemnicy komunikowania się. Podkreślenia wymaga również to, że zasadniczym celem takiego dokumentowania jest umożliwienie wykazania funkcjonariuszowi (lub osobie udzielającej mu pomocy), iż czynności operacyjno-rozpoznawcze zostały przeprowadzone w sposób prawidłowy, a w szczególności zgodny z prawem. Należy wreszcie wskazać, że o ile zapisy utrwalone w wyniku stosowania kontroli operacyjnej mają samoistną wartość dowodową, o tyle zapisy będące efektem dokumentowania czynności operacyjno-rozpoznawczych - gdyby miały być w wyjątkowych okolicznościach wykorzystane w procesie karnym - będą miały charakter wtórny wobec dowodu pierwotnego, jakim są zeznania świadka.

Proponowany przepis powinien również jednoznacznie wskazywać, iż nie są kontrolą operacyjną:

- obserwowanie i rejestrowanie, przy użyciu środków technicznych, obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych podejmowanych na podstawie ustawy (art. 14 ust. 1 pkt 6).
- uzyskiwanie danych telekomunikacyjnych na podstawie art. 18.

Art. 17 ust. 5a powinien zatem otrzymać brzmienie:

Art. 17. 5a. Nie jest kontrolą operacyjną:

1) dokumentowanie przez funkcjonariusza lub osobę udzielającą mu pomocy wykonywanych czynności operacyjno-rozpoznawczych poprzez rejestrację obrazu lub dźwięku, z wyłączeniem czynności, o których mowa w art. 17 ust. 5 pkt 3 i art. 20;

2) realizacja czynności, o których mowa w art. 14 ust. 1 pkt 6;

3) uzyskiwanie danych telekomunikacyjnych na podstawie art. 18.

Art. 17 ust. 5b

Przyjęcie definicji kontroli operacyjnej zaproponowanej w uwagach do art. 17 ust. 5 czyni ten przepis zbędnym (z zastrzeżeniem wskazanym przy uwagach odnośnie do terminu „podsłuch").

Art. 17 ust. 15f-i

W ocenie CBA zaproponowany w ust. 15f tryb postępowania z materiałami, w odniesieniu do których zachodzi przypuszczenie, że mogą zawierać informacje, o których mowa w art. 178 k.p.k., nie tylko nie znajduje podstaw w uzasadnieniu wyroku TK, ale wręcz jest z nim sprzeczny.

W pkt III.11 uzasadnienia Trybunał dokonał analizy zagadnień związanych z ochroną tajemnicy zawodowej, obejmując tym określeniem także kwestie związane z informacjami, o których mowa w art. 178 k.p.k. Trybunał stwierdził, że „nie jest wykluczone umożliwienie służbom policyjnym i służbom ochrony państwa pozyskanie informacji o charakterze poufnym, przekazywanym podmiotom wykonującym zawody zaufania publicznego". Polemizując z postulatem ogólnego wyłączenia „spod kontroli operacyjnej podmiotów zobowiązanych w ustawie do zachowania tajemnicy zawodowej", wskazał, że „nie da się zazwyczaj abstrakcyjnie określić relacji między dobrem, którego ochronie mają służyć zakazy dowodowe (i tajemnica zawodowa), a dobrem wymiaru sprawiedliwości, bezpieczeństwem państwa i porządkiem publicznym w kategoriach „wyższe – niższe" czy „ważniejsze – mniej ważne" (zob. wyrok TK z 13 grudnia 2011 r., sygn. K 33/08, cz. III, pkt 6.4 uzasadnienia). **Takie wartościowanie można przeprowadzić *ad casum*, z uwzględnieniem okoliczności konkretnej sprawy** [podkr. CBA]".

Konkludując tę część swych rozważań Trybunał wskazał m.in. na konieczność „ustanowienia mechanizmu prewencyjnej **sądowej** [podkr. CBA] kontroli i selekcji materiałów, co do których zachodzi prawdopodobieństwo, że stanowią tajemnicę zawodową".

W tym kontekście trudno uznać za trafną propozycję, by Szef CBA dokonywał oceny materiałów pod kątem zbadania, czy zawierają informacje, o których mowa w art. 178 k.p.k. Oceny takiej - zarówno w opinii TK, jak i CBA - winien dokonywać sąd.

CBA za co najmniej wątpliwe - w świetle uzasadnienia wyroku TK - uważa pośrednictwo Prokuratora Generalnego w procedurze opisanej w proponowanych ust. 15f-15i. W pkt III.11.8.1 Trybunał wyraźnie wskazał, że należy dążyć do zapobieżenia, a przynajmniej zminimalizowania ryzyka wykorzystania informacji wymagających ochrony. Stwierdził, że „Mankamentem konstytucyjnym art. 19 ustawy o Policji jest niezagwarantowanie w ustawie, że w sytuacji uzasadnionego podejrzenia, że zgromadzone materiały zawierają informacje objęte tajemnicę zawodową i z tego powodu wymagają szczególnej ochrony, nastąpi dodatkowa weryfikacja tych materiałów przez sąd i ewentualne zwolnienie z tajemnicy zawodowej, zanim zostaną przekazane funkcjonariuszom służb **bądź prokuratorowi** [podkr. CBA]".

Wydaje się zatem uzasadnione, by – w przypadku uzyskania w toku kontroli operacyjnej informacji stanowiących tajemnice zawodowe – Szef CBA kierował stosowne fragmenty materiałów z kontroli bezpośrednio do sądu. Pozwoli to na wyeliminowanie ogniwa pośredniego w procedurze i ograniczenie do minimum kręgu osób, mających dostęp do informacji wymagających ochrony.

Podsumowując powyższe uwagi, CBA proponuje, by przepisom tym należy nadać brzmienie (przy czym ust. 15i stanie się zbędny):

Art. 17. 15f. W przypadku gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 15, mogą zawierać informacje, o których mowa w art. 178 Kodeksu postępowania karnego, lub stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA przekazuje fragmenty materiałów mogące zawierać te informacje sądowi, o którym mowa w ust. 2, wraz z wnioskiem o stwierdzenie dopuszczalności ich wykorzystania w postępowaniu karnym.

15g. W terminie 14 dni od dnia złożenia wniosku sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje, o których mowa w art. 178 Kodeksu postępowania karnego, lub stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, albo zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

15h. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów mogących zawierać informacje, o których mowa w art. 178 Kodeksu postępowania karnego, lub stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego. Szef CBA niezwłocznie informuje sąd, o którym mowa w ust. 2.

Art. 17 ust. 16d pkt 1

Przewidziane w tym przepisie niszczenie dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej byłoby działaniem nieracjonalnym. Dokumentacja ta (w szczególności nośniki i ich kopie, o których mowa w proponowanym ust. 16c pkt 1 i 2) winny być przekazywane - wraz z samymi materiałami - Prokuratorowi Generalnemu. Zniszczeniu podlegać powinna jedynie ta część dokumentacji, która nie została przekazana PG.

Za przyjęciem takiego rozwiązania przemawiają z jednej strony względy prawne (nośniki, na których utrwalone zostały np. treści rozmów, mogą być dowodami w procesie karnym), jak i praktyczne (dokumenty, o których mowa w proponowanym ust. 16c pkt 3, mogą być przydatne w toku ewentualnych czynności procesowych).

Art. 17 ust. 16d pkt 1 winien zatem otrzymać brzmienie:

Art. 17. 16d. (...)

1) ust. 15 - niezwłocznie po przekazaniu prokuratorowi materiałów, które dokumentuje, w części, w jakiej nie została przekazana prokuratorowi; (...).

Art. 18 ust. 1

Zaproponowana w projekcie zmiana tego przepisu wykracza poza sentencję wyroku Trybunału. Art. 18 ustawy o CBA został uznany za niezgodny z Konstytucją wyłącznie w zakresie, w jakim nie przewiduje zniszczenia danych niemających znaczenia dla prowadzonego postępowania, zaś ust. 1 pkt 1 tego przepisu dodatkowo przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. W pozostałym zakresie Trybunał postępowanie umorzył. W tym stanie rzeczy propozycja zmiany art. 18 ust. 1 ustawy o CBA jest zbędna i należy z niej zrezygnować.

Ponadto nowoprojektowane brzmienie tego przepisu nie uwzględnia danych identyfikujących usługobiorców w rozumieniu przepisów o świadczeniu usług drogą elektroniczną. Do usług tych zalicza się między innymi udostępnianie kont poczty elektronicznej, serwisów społecznościowych czy też komunikatorów internetowych. Przepis art. 18 ust. 9 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422) nakłada na usługodawców obowiązek przekazywania danych identyfikujących usługobiorców organom państwowym na potrzeby prowadzonych przez nie postępowań. Jest to przepis wzorowany na rozwiązaniach przyjętych w art. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243). Należy uznać, że brak odniesienia do przepisów o świadczeniu usług drogą elektroniczną w przepisach kompetencyjnych służb (np. art. 18 ustawy o CBA, art. 20c i 20d ustawy o Policji czy art. 28 ustawy o ABW) stanowi lukę w prawie, którą przy okazji tej nowelizacji należy usunąć. Umożliwi to jednoznaczne rozstrzygnięcie sporów interpretacyjnych pomiędzy usługodawcami a uprawnionymi służbami odnośnie do znaczenia art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną.

W związku z tym ewentualna nowelizacja przepisu art. 18 ust. 1 powinna uwzględniać dodanie pkt 3 w brzmieniu:

3) identyfikujące usługobiorców w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422).

Art. 18 ust. 2 pkt 4

W przepisie tym należy przewidzieć – analogicznie do rozwiązania zawartego w pkt 1 – możliwość udzielenia przez Szefa CBA upoważnienia do odebrania danych, udostępnianych przez podmiot prowadzący działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, funkcjonariuszowi Biura. Propozycja wynika zarówno z praktyki funkcjonowania CBA, jak i podmiotów prowadzących działalność telekomunikacyjną, które rygorystycznie interpretują przepisy dotyczące danych retencyjnych i kontroli operacyjnej. Trudno też sobie wyobrazić, aby każdorazowo Szef osobiście odbierał dane od przedsiębiorców. Z obecnie obowiązujących przepisów prawa oraz z praktyki ich stosowania wynika, że zasadne jest, aby dane te odbierał upoważniony przez Szefa CBA funkcjonariusz.

Co za tym idzie, przepis ten powinien otrzymać brzmienie:

Art. 18. 2. (...)

4) Szefowi CBA lub osobie przez niego upoważnionej w przypadku postanowienia Sądu Okręgowego w Warszawie wyrażającego zgodę na pozyskanie danych w przypadkach, o których mowa w art. 18b ust. 1 lub 3.

Art. 18 ust. 3

Przepisowi należy nadać brzmienie:

Art. 18. 3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub pocztowych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, lub przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem.

Zaproponowana zmiana ma charakter redakcyjny.

Art. 18a

Przepisowi należy nadać brzmienie:

Art. 18a. 1. W przypadku gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 5, mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA przekazuje fragmenty materiałów mogące zawierać te informacje sądowi, o którym mowa w art. 17 ust. 2, wraz z wnioskiem o stwierdzenie dopuszczalności ich wykorzystania w postępowaniu karnym.

2. W terminie 14 dni od dnia złożenia wniosku sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, albo zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

3. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA niezwłocznie informuje sąd, o którym mowa w ust. 2.

Uzasadnienie powyższej propozycji jest analogiczne do przedstawionego w odniesieniu do art. 17 ust. 15f-i.

Art. 18c ust. 2

W opinii CBA okres sprawozdawczy powinien wynosić 12 miesięcy.

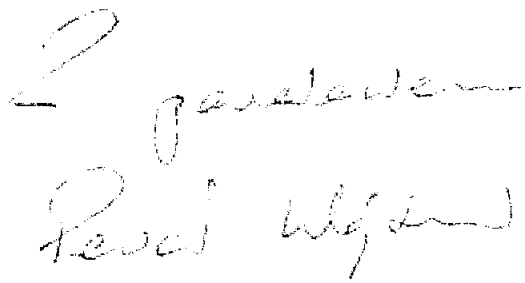
Ponadto zgłaszam uwagi do niektórych z przepisów przejściowych projektu.

Art. 12 ust. 1 projektu

Przepis ten jest zbędny, gdyż zgodnie z zasadą bezpośredniego stosowania prawa przy braku przepisów przejściowych, do wszelkich stosunków prawnych i zdarzeń, niezależnie od tego czy rozpoczęły się przed, czy też po wejściu w życie nowych przepisów, stosuje się nowe normy prawne.

Art. 14 ust. 1 projektu

Centralne Biuro Antykorupcyjne kategorycznie sprzeciwia się temu przepisowi. Należy mieć na uwadze, że pod rządami aktualnie obowiązujących przepisów trwają czynności operacyjno-rozpoznawcze i procesowe z wykorzystaniem materiałów z kontroli operacyjnej. Stanowią one materiał dowodowy mający istotne znaczenie dla ustalenia prawdy materialnej. Konsekwencją zniszczenia materiałów uzyskanych w toku kontroli operacyjnej pod rządami aktualnie obowiązujących przepisów byłoby zakończenie trwających spraw operacyjnych, postępowań przygotowawczych i sądowych. Trybunał Konstytucyjny w pkt II sentencji orzekł, że uchylone przepisy utratą swoją moc dopiero po upływie 18 miesięcy od dnia ogłoszenia wyroku w Dzienniku Ustaw, a więc z dniem 7 lutego 2016 r. Do tego momentu pozostają przepisami obowiązującym i wszelkie działania podjęte na ich podstawie są legalne. Dlatego też nieuzasadnione jest wprowadzenie przepisu nakazującego zniszczenie wszelkich materiałów uzyskanych w toku kontroli operacyjnych zarządzonych na podstawie obecnie obowiązujących przepisów. Podkreślić przy tym należy, że projektodawca nie przedstawił w uzasadnieniu projektu *ratio legis* tego przepisu.



PROKURATORIA GENERALNA SKARBU PAŃSTWA
Główny Urząd Prokuratorii Generalnej Skarbu Państwa

ul. Hoża 76/78 , 00-682 Warszawa
tel.: (+48) 022 392-31-17, fax: (+48) 022 392-31-20
www.prokuratoria.gov.pl
e-mail: kancelaria@prokuratoria.gov.pl

KR-51-351/15/KBU
DOPL/ [illegible]/15

Warszawa, 2015.07.16

Pan
Piotr ZIENTARSKI
Przewodniczący Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

W odpowiedzi na pismo z dnia 26.06.2015 r., znak: BPS/KU-034/967/24/15, dotyczące zaopiniowania **projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)**, w załączeniu uprzejmie przekazuję opinię Prokuratorii Generalnej Skarbu Państwa do przedłożonego projektu.

Otrzymują:

1) adresat – 1 egz.,
2) a/a – 1 egz.

KR-51-351/15/KBU

Opinia do projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)

W związku z otrzymaniem do zaopiniowania *projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)*, zauważa się, co następuje:

1. Trybunał Konstytucyjny w pkt III.5.3 uzasadnienia wyroku z dnia 30 lipca 2014 r., sygn. K 23/11 na podstawie dokonanej analizy swoich wcześniejszych orzeczeń jak również orzecznictwa Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej wskazał minimalne wymagania, które łącznie muszą spełniać przepisy ograniczające konstytucyjne wolności i prawa. Jednym z tych wymagań jest zagwarantowanie transparentności stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej przez publiczną jawność i dostępność zagregowanych danych statystycznych, nadających się do porównania, dotyczących ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych. Tym samym w przepisach zmienianych ustaw dotyczących rejestrów postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej (art. 1 pkt 1 lit. f, art. 2 pkt 1 lit. f, art. 3 pkt 3 lit. c, art. 6 pkt 3 lit. f, art. 7 pkt 2 lit. f, art. 9 pkt 1 lit. f i art. 10 pkt 1 lit. e projektu) należałoby uwzględnić publiczną jawność zagregowanych danych statystycznych dotyczących ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych. Zwrócić należy uwagę, iż projektowany art. 175b dodawany do *ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133 i 509)* przewiduje coroczne przedstawianie Sejmowi i Senatowi przez Ministra Sprawiedliwości zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych i pocztowych, z podziałem na liczbę i rodzaj udostępnianych danych oraz wyników przeprowadzonych kontroli. Przepis ten nie uwzględnia jednak przekazywania danych dotyczących liczby czynności operacyjno-rozpoznawczych stosowanych przez poszczególne organy władzy publicznej.

2. W art. 6 pkt 3 lit. h projektu proponuje się zmienić brzmienie projektowanego ust. 20 w art. 31 zmienianej *ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, z późn. zm.)* zawierającego upoważnienie do wydania aktu wykonawczego, przez dodanie jako materii mającej być uregulowaną w tym akcie sposobu prowadzenia rejestrów, o których mowa w ust. 17a w tym artykule.

3. W art. 31 ust. 16 pkt 4 i 5 zmienianej *ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.)* (art. 9 pkt 1 lit. g projektu) należałoby zastosować prawidłowe odesłanie do ust. 15b zamiast do nieistniejącego ust. 16b.

4. W przepisach *ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.)* (art. 11 projektowanej ustawy) należałoby uregulować kwestię prowadzenia rejestrów postanowień, zarządzeń i wniosków dotyczących kontroli operacyjnej.

K. Bucz[illegible]
[illegible].12.2015

Warszawa, dnia 15 lipca 2015 r.

PIERWSZY PREZES
SĄDU NAJWYŻSZEGO
RZECZYPOSPOLITEJ POLSKIEJ

BSA II-021-300/15

Pan
Piotr ZIENTARSKI
Przewodniczący Komisji Ustawodawczej
Senat Rzeczypospolitej Polskiej

W odpowiedzi na pismo z dnia 26 czerwca 2015 r., BPS/KU-034/967/3/15 uprzejmie informuję, że Sąd Najwyższy nie zgłasza uwag do ***projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.***

Z poważaniem

w/z

prof. dr hab. Tadeusz ERECIŃSKI
Prezes Sądu Najwyższego

FUNDACJA
PANOPTYKON

Warszawa, 17 lipca 2015 r.

Szanowny Pan Senator
Piotr Zientarski
Przewodniczący Komisji Ustawodawczej

Szanowny Panie,

Fundacja Panoptykon przedstawia swoje stanowisko dotyczące projektu zmiany ustawy o Policji oraz niektórych innych ustaw (druk senacki 967). Jednocześnie zgłaszamy zainteresowanie udziałem w pracach legislacyjnych nad projektem, które będą prowadzone w Komisji Ustawodawczej.

W imieniu Fundacji Panoptykon,

Szymielewicz

Katarzyna Szymielewicz
Prezeska

Fundacja Panoptykon | ul. Orzechowska 4 lok. 4 | 02-068 Warszawa
e: fundacja@panoptykon.org | t: +48 660 074 026 | w: panoptykon.org

FUNDACJA
PANOPTYKON

Warszawa, 17 czerwca 2015 r.

STANOWISKO FUNDACJI PANOPTYKON[1]

w sprawie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki 967)

Projekt zmiany ustawy o Policji oraz niektórych innych ustaw – jak wynika z jego uzasadnienia – ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. o sygn. K 23/11 (dalej: **wyrok TK**). Ze względu na skomplikowaną sytuację prawną, a także zbliżający się termin wejścia w życie wyroku Trybunału Konstytucyjnego, podjęcie przez Senat inicjatywy legislacyjnej jest niezwykle cenne. Jednak, w ocenie Fundacji Panoptykon, proponowane rozwiązania w sposób fragmentaryczny i niepełny wdrażają wyrok TK, a także pomijają wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 (dalej: **wyrok TSUE**). Rodzi to daleko idące wątpliwości co do zgodności projektu z Konstytucją RP i prawem UE.

Na wstępie przypominamy, że dane telekomunikacyjne stanowią integralny element tajemnicy komunikowania się. Potwierdził to m.in. Europejski Trybunał Praw Człowieka w wyrokach Malone przeciwko Wielkiej Brytanii (skarga nr 8691/79) i Copland przeciwko Wielkiej Brytanii (skarga nr 62617/00). W pierwszym z tych wyroków ETPC wskazał, że „pozyskiwanie danych zawartych w tzw. bilingach nie może wprawdzie być utożsamiane z podsłuchem rozmów telefonicznych, jednakże ujawnienie policji tego rodzaju danych bez zgody abonenta powinno być traktowane jako równoważne ingerencji w prawo zagwarantowane w art. 8 ust. 1 Konwencji (prawo do prywatności)". Stanowisko to potwierdziły w swoich wyrokach zarówno TK, jak i TSUE. W związku z tym, jak wskazał TSUE „ochrona życia prywatnego w każdym wypadku wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, **co jest absolutnie konieczne**".

TSUE, stwierdzając niezgodność z Kartą praw podstawowych tzw. dyrektywy retencyjnej[2], zwrócił uwagę na następujące problemy:

- konieczność zapewnienia, by uprawnione organy miały dostęp do danych wyłącznie w sprawie przestępstw, „które z uwagi na zakres i wagę ingerencji w prawa podstawowe

[1] Stanowisko przygotowane przez Wojciecha Klickiego.
[2] 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 zmieniającej dyrektywę 2002/58/WE

ustanowione w art. 7 i 8 karty, można uznać za **wystarczająco poważne**, by taką ingerencję uzasadnić";

- uzyskanie dostępu do danych powinno podlegać **uprzedniej kontroli sądu lub niezależnego organu administracyjnego**, które pilnowałyby, aby udostępnienie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne;
- dane telekomunikacyjne powinny być w należyty sposób chronione (zwłaszcza dotyczy to obowiązku przechowywania danych na terenie UE);

Stwierdzenie niezgodności dyrektywy retencyjnej z Kartą praw podstawowych z wymienionych wyżej powodów powinny być wzięte pod uwagę przy pracach legislacyjnych w państwach członkowskich. Jak wskazał bowiem dr Maciej Taborowski w analizie skutków wyroku TSUE[3], „na mocy art. 4 ust. 3 TUE (zasada lojalności) **wyrok prejudycjalny stwierdzający nieważność aktu prawa UE wiąże** instytucje UE oraz **wszystkie organy państw członkowskich** (nie tylko sądy krajowe), **w tym organy legislacyjne**". Zwracamy przy tym uwagę, że nieuwzględnienie wytycznych płynących z wyroku TSUE może być podstawą do podjęcia działań przez Komisję Europejską, która – jako strażniczka traktatów UE – zobowiązana jest do weryfikacji zgodności przepisów krajowych z prawem UE[4].

Przed przejściem do omówienia szczegółowych propozycji zawartych w projekcie, zwracamy uwagę, że opinia dotyczy **wyłącznie** przepisów związanych z dostępem Policji i innych uprawnionych podmiotów do danych telekomunikacyjnych. W opinii nie odnosimy się do elementów projektu związanych z kontrolą operacyjną, co w żadnym razie nie powinno być traktowane jako ich akceptacja.

1. Kontrola nad sięganiem przez uprawnione podmioty po dane telekomunikacyjne

W wyroku K 23/11 Trybunał Konstytucyjny wskazał, że przepisy uprawniające do sięgania po dane telekomunikacyjne naruszają Konstytucję **„przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych"**.

Opiniowany projekt zakłada dwa modele kontroli nad sięganiem po dane telekomunikacyjne. Pierwszy model, kontroli uprzedniej, ma dotyczyć jedynie danych telekomunikacyjnych „dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego". W tym modelu niezbędne będzie uzyskanie zgody sądu na pozyskanie danych i ich wykorzystanie w postępowaniu karnym. Projektodawca przewidział także możliwość uzyskania następczej zgody sądu w przypadkach niecierpiących zwłoki, a także konieczność uzyskania zgody sądu na wykorzystanie w postępowaniu karnym materiałów potencjalnie naruszających tajemnicę zawodową w sytuacji, w której dopiero po ich pobraniu okazało się, że dotyczą one wskazanych kategorii osób.

Drugi model, w praktyce odnoszący się do przeważającej większości przypadków pobrania danych, sprowadza się do kontroli następczej, sprawowanej przez sąd. Zgodnie z projektem podmioty uprawnione do pobierania danych mają przekazywać, raz na 6 miesięcy, sprawozdania obejmujące liczbę i rodzaj pozyskanych danych: podstawę prawną pozyskania

---

[3] Analiza dostępna pod adresem: http://www.hfhr.pl/wp-content/uploads/2014/04/skutki_wyroku_TSUE_MTaborowski-3.pdf

[4] Do Komisji Europejskiej w tej sprawie zwróciła się koalicja organizacji pozarządowych European Digital Rights, której Fundacja Panoptykon jest członkiem, zwróciła się. Wystąpienie dostępne pod adresem: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702.pdf

danych, rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane oraz liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane. W ramach prowadzonej kontroli sąd okręgowy **może** zapoznać się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych, podlegają one zniszczeniu.

Na wstępie należy przywołać stanowisko Trybunału Konstytucyjnego odnośnie kontroli nad sięganiem po dane telekomunikacyjne. TK *„nie przesądza, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału, nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in.* ***specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne*** *dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem* ***kontroli uprzedniej*** *w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych* ***osób wykonujących zawody zaufania publicznego*** *lub* ***jeśli nie ma konieczności pilnego działania służb".***

TK sformułował więc dwie wytyczne dotyczące kształtu kontroli nad sięganiem po dane. Po pierwsze, sposób kontroli może być uzależniony od charakteru danych telekomunikacyjnych oraz od charakteru działalności uprawnionego podmiotu. Po drugie, kontrola uprzednia nad sięganiem po dane powinna dotyczyć osób wykonujących zawody zaufania publicznego oraz sytuacji, w których nie ma konieczności pilnego działania. Trybunał w Luksemburgu wskazał zaś wprost, że uzyskanie dostępu do danych powinno podlegać **uprzedniej kontroli sądu lub niezależnego organu administracyjnego.**

W naszej ocenie mechanizmu kontroli nad sięganiem po dane przewidziany w projekcie nie uwzględnia wszystkich wytycznych płynących z wyroków TK i TSUE i **nie zrealizuje zakładanego celu z następujących względów:**

- kontrola następcza prowadzona przez sąd na podstawie składanych co 6 miesięcy sprawozdań ma mieć charakter fakultatywny: obawiamy się, że doprowadzi to do niepodejmowania przez sąd realnych czynności kontrolnych[5];
- czynności kontrolne podejmowane przez sąd będą miały charakter wyjątkowy i incydentalny, tymczasem zasadą powinno być kontrolowanie dostępu do danych telekomunikacyjnych w każdej sprawie, a brak takiej kontroli– wyjątkiem;

[5] W tym kontekście zwracamy uwagę na stanowisko Krajowej Rady Sądownictwa wobec projektu. KRS w swoim stanowisku wskazała, że przyznanie sądom dodatkowych uprawnień będzie się wiązać z dodatkowym obciążeniem budżetu sądów, tymczasem projektodawca nie przedstawił wielkości i źródeł ich pokrycia.

- kontrola prowadzona po 6 miesiącach od pobrania danych telekomunikacyjnych będzie mniej efektywna, a jednocześnie bardziej czasochłonna od kontroli prowadzonej przed lub bezpośrednio po pobraniu danych;
- projektodawca nie przewidział jakichkolwiek negatywnych konsekwencji dla funkcjonariuszy sięgających po dane telekomunikacyjne w przypadku stwierdzenia braku podstaw do pozyskania danych.

W naszej ocenie kontrola nad sięganiem po dane telekomunikacyjne powinna być wzorowana na tej dotyczącej kontroli operacyjnej. Jak wskazał w zdaniu odrębnym do wyroku TK sędzia Wojciech Hermeliński „celowe powinno być osiągnięcie porównywalnego standardu ochrony prawa do prywatności i wolności komunikowania się jak przy kontroli operacyjnej. Przy obecnym poziomie rozwoju technologii inwazyjność tych dwóch sposobów pozyskiwania informacji o obywatelach jest zbliżona (choć dane telekomunikacyjne – w przeciwieństwie do informacji uzyskiwanych w toku kontroli operacyjnej – nie dostarczają informacji o treści komunikatów, to w zamian za to można na ich podstawie ustalić np. fakt przebywania danej osoby w określonym miejscu lub grono osób, z którymi się ona kontaktuje)".

Stoimy na stanowisku – które znajduje oparcie w wyroku TK – że tryb uzyskania dostępu do danych telekomunikacyjnych powinien być uzależniony od ich charakteru – np. z rozróżnieniem danych abonenckich od pozostałych kategorii danych telekomunikacyjnych. Dostęp dodanych abonenckich , które w mniejszym stopniu ingerują w prywatność jednostki, nie musi być uzależniony od każdorazowej zgody organu zewnętrznego. Taka zgoda powinna być natomiast konieczna do uzyskania dostępu do takich danych, jak wykaz połączeń czy geolokalizacja. Przy czym zasadą powinno być uzyskanie zgody przed sięgnięciem po dane, natomiast możliwość uzyskiwania zgody następczej w przypadkach niecierpiących zwłoki powinna zostać dopuszczona jako wyjątek.

Zwracamy uwagę, że wbrew stanowisku projektodawcy, możliwe jest sprawne funkcjonowanie systemu kontroli uprzedniej nad pozyskiwaniem danych telekomunikacyjnych. W Danii i Finlandii dostęp do danych telekomunikacyjnych możliwy jest po uprzednim uzyskaniu zgody sądu. Krajowe przepisy umożliwiają – jedynie w wyjątkowych sytuacjach – uzyskanie tej zgody w trybie następczym.

2. Pozostałe problemy związane z dostępem do danych telekomunikacyjnych

a. Zasada subsydiarności

Zgodnie z uzasadnieniem projektu „zastosowanie zasady subsydiarności przed wystąpieniem po dane telekomunikacyjne w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudnić skuteczne ściganie ich sprawców". Projektodawcy wskazują przy tym na przestępstwa internetowe, w których nie ma innych czynności, które można wykonać przed pobraniem danych telekomunikacyjnych albo wykazać ich nieskuteczność.

Brak zasady subsydiarności zobowiązującej uprawnione podmioty do wykorzystywania danych telekomunikacyjnych był poruszony przez Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego, inicjującym postępowanie o sygn. K 23/11. Należy w tym miejscu przypomnieć, że TK – uznając niekonstytucyjność braku kontroli nad sięganiem po dane – nie rozstrzygnął, czy pozostałe zarzuty sformułowane przez Rzecznik Praw Obywatelskich i Prokuratora Generalnego zasługują na uwzględnienie. Zwracamy uwagę, że zdaniem Prokuratora Generalnego „brak wymogu subsydiarności sięgania po dane telekomunikacyjne

świadczy o nieproporcjonalnej ingerencji, niespełniającej warunku konieczności"; w postępowaniu przed TK to stanowisko podzielił także Marszałek Sejmu.

W naszej ocenie ustawodawca powinien wprowadzić zasadę subsydiarności. Argumenty przywołane przeciwko wprowadzeniu tej zasady w uzasadnieniu projektu są niewłaściwe i nie odnoszą się do istoty zasady subsydiarności. Jeśli w konkretnej sprawie nie istnieją inne czynności, które można wykonać przed pobraniem danych telekomunikacyjnych albo wykazać ich nieskuteczność, zasada subsydiarności nie stoi na przeszkodzie wykorzystaniu danych.

Jak wskazał w zdaniu odrębnym do wyroku TK sędzia Wojciech Hermeliński „wskazany **brak subsydiarności** zaskarżonych przepisów **otwiera możliwość wykorzystywania danych telekomunikacyjnych** nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy **gdy jest to po prostu najprostsze i najwygodniejsze** (...) Istnieje ryzyko, że sprawdzenie bilingów z rozmów telefonicznych czy odczytów z GPS zamontowanego w telefonie czy samochodzie będzie wkrótce pierwszą czynnością podejmowaną we wszystkich sprawach na przykład w celu wytypowania wstępnego kręgu osób zamieszanych w dane przestępstwo, nawet wtedy gdy – bez szkody dla wyniku postępowania – można ten sam cel osiągnąć tradycyjnymi metodami śledczymi, bez ingerencji w prywatność dużej liczby obywateli".

b. Informowanie

Projektodawca nie przewidział procedury informowania osób, których dane zostały pobrane, o tym fakcie. Stoi to w sprzeczności z wytycznymi sformułowanymi w uzasadnieniu wyroku TK, zgodnie z którym: *„ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie".*

Naszym zdaniem należy rozważyć wprowadzenie mechanizmu informowania o pobraniu danych telekomunikacyjnych, analogicznego do rozwiązań przewidzianych w Kodeksie postępowania karnego. Wprowadzenie tego mechanizmu jest niezbędnym elementem wdrożenia wyroku TK, który jednoznacznie stwierdził, że zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Zdaniem TK „obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności".

Niewątpliwie od zasady informowania powinny zostać wprowadzone wyjątki, uwzględniające sytuacje, w których dane zostały pozyskane przypadkowo i nie podlegają dalszej analizie bądź pozyskano je w ramach działań wywiadowczych, których cel byłby zniweczony przez informowanie osób objętych zainteresowaniem służb. Takie – uzasadnione – wyjątki nie mogą jednak podważać potrzeby wprowadzenia zasady informowania o pobraniu danych telekomunikacyjnych.

Na marginesie zwracamy uwagę, że na brak obowiązku powiadamiania osób, których dotyczyły działania służb, o fakcie pobrania danych telekomunikacyjnych skrytykował również Federalny Sąd Konstytucyjny Niemiec, który wyrokiem z 2 marca 2010 r. (sygn. 1 BvR 256/08) unieważnił

krajowe przepisy wdrażające dyrektywę retencyjną. Jednym z powodów takiej decyzji był brak konieczności powiadamiania podmiotu poddanego inwigilacji o pozyskaniu dotyczących go danych.

c. Długość przechowywania danych

W swoim wyroku TK zwrócił uwagę, że 12-miesięczny okres zatrzymywania danych telekomunikacyjnych jest „stosunkowo długi". Analizując statystyki wskazujące na średni czas przechowywania danych telekomunikacyjnych przed ich pobraniem przez uprawnione podmioty, TK wskazał, że „może budzić wątpliwości, czy zatrzymywanie danych o ruchu i lokalizacji na czas dłuższy niż 6 miesięcy spełnia konstytucyjny wymóg przydatności, wynikający z zasady proporcjonalności".

Na problem czasu przechowywania danych zwrócił uwagę TSUE, który niezgodności dyrektywy retencyjnej z Kartą praw podstawowych dopatrzył się m.in. w braku zróżnicowania między okresem przechowywania różnych kategorii danych telekomunikacyjnych w zależności od ewentualnej użyteczności danych w stosunku do zakładanego celu, a także stopnia ich ingerencji w prywatność jednostki.

W naszej ocenie ustawodawca – chcąc w pełni zrealizować wyrok TK, a jednocześnie zapewnić wysoki stopień ochrony praw jednostki, powinien w przekonujący sposób wykazać konieczność 12-miesięcznej retencji danych, a także rozważyć zróżnicowanie okresu ich przechowywania od ich charakteru i przydatności.

d. Obowiązki sprawozdawcze – sądy i Minister Sprawiedliwości

Zdaniem TK, brak jednolitych standardów sprawozdawczości stanowi istotny konstytucyjny mankament obowiązujących unormowań. Istniejące przepisy nie wprowadzają bowiem spójnej metodologii liczenia realizowanych zapytań o dane telekomunikacyjne, a zarówno operatorzy telekomunikacyjni, jak i poszczególne uprawnione podmioty stosują w tym zakresie różne standardy.

Fundacja Panoptykon co roku publikuje informacje dotyczące skali sięgania po dane telekomunikacyjne. Zgodnie z danymi przekazanymi Urzędowi Komunikacji Elektronicznej przez operatorów telekomunikacyjnych w 2013 r. otrzymali oni 1,75 mln zapytań. Natomiast zgodnie z przekazanymi Fundacji przez część uprawnionych podmiotów (policję, Straż Graniczną, Centralne Biuro Antykorupcyjne, Agencję Bezpieczeństwa Wewnętrznego, Żandarmerię Wojskową, kontrolę skarbową i służbę celną[6]), tylko te podmioty skierowały do operatorów telekomunikacyjnych 2,18 mln zapytań. Ta rozbieżność potwierdza brak jednolitych standardów i przejrzystości w ocenie rzeczywistej skali ingerencji policji i innych służb w prywatność użytkowników telefonów komórkowych i Internetu.

Pozytywnie oceniamy projektowane przeniesienie obowiązku sprawozdawczego dotyczącego częstotliwości sięgania po dane telekomunikacyjne z operatorów telekomunikacyjnych na organy państwowe. W naszej ocenie daje to szanse na zwiększenie spójności i przejrzystości generowanych statystyk.

Naszym zdaniem ponownego rozważenia wymaga jednak zakres informacji, jakie mają być przekazywane przez sądy ministrowi, a następnie przez ministra – Sejmowi. W szczególności

---

[6] Informacje te nie obejmują pytań skierowanych do operatorów telekomunikacyjnych przez sądy, prokuratorów i Służbę Kontrwywiadu Wojskowego.

sądzimy, że obowiązkiem sprawozdawczym powinien zostać objęty także rodzaj przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne. Skoro projekt zakłada przedkładanie przez uprawnione organy prezesom sądów okręgowych danych tego rodzaju, nie ma przeszkód, by sądy przedstawiały je Ministrowi Sprawiedliwości, a ten – Sejmowi. Jednocześnie postulujemy rozważenie przeniesienia uprawnienia do wydania rozporządzenia, o którym mowa w art. 180c ust. 2 Prawa telekomunikacyjnego z ministra właściwego do spraw łączności na Ministra Sprawiedliwości, który w ten sposób uzyskałby pełną kontrolę nad sprawozdawczością dotyczącą sięgania po dane telekomunikacyjne.

e. Przestępstwa, w związku z którymi możliwe jest sięganie po dane telekomunikacyjne

Projekt doprecyzowuje, w jakich sytuacjach policja i inne uprawnione podmioty będą mogły wykorzystywać dane telekomunikacyjne. W przypadku policji mają to być **przestępstwa ścigane z oskarżenia publicznego**, a także działania w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, w przypadku Straży Granicznej: przestępstwa i **wykroczenia**, o których mowa w art. 1 ust. 2 pkt 4 ustawy o Straży Granicznej, w przypadku kontroli skarbowej: przestępstwa skarbowe, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę, w przypadku Żandarmerii Wojskowej: przestępstwa, w tym przestępstwa skarbowych popełnione przez żołnierzy, a także działania w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, w przypadku Agencji Bezpieczeństw Wewnętrznego, Służby Kontrwywiadu Wojskowego i Centralnego Biura Antykorupcyjnego: rozpoznawanie, zapobieganie, zwalczanie i wykrywanie albo utrwalanie dowodów przestępstw w celu realizacji ustawowych zadań.

Pozytywnie oceniamy kierunek proponowanych zmian, który uwzględnia zasadę, zgodnie z którą ingerencja w prawo do prywatności związana z pozyskiwaniem danych telekomunikacyjnych powinna być dopuszczalna tylko w związku z poważnymi przestępstwami. Projekt nie realizuje jednak tego celu w sposób konsekwentny, dopuszczając m.in. wykorzystywanie przez Straż Graniczną danych telekomunikacyjnych w sprawach wykroczeń.

Naszym zdaniem pożądane byłoby ograniczenie możliwości sięgania po dane telekomunikacyjne do tych samych przypadków, w których prawo przewiduje możliwość prowadzenia kontroli operacyjnej, przy jednoczesnym dopuszczeniu wyjątków od tej zasady. Takim wyjątkiem mogłoby być wykrywanie wykroczeń, o których mowa w art. 66 Kodeksu wykroczeń (fałszywe alarmy bombowe), przestępstwo uporczywego nękania (tzw. stalking), a także przestępstwa popełnione za pośrednictwem środków komunikacji elektronicznej w sytuacji, gdy dane telekomunikacyjne są niezbędne do przeprowadzenia czynności w śledztwie.

f. Przechowywanie danych telekomunikacyjnych poza terenem Unii Europejskiej

Na konieczność szczególnej ochrony danych telekomunikacyjnych przechowywanych przez operatorów telekomunikacyjnych zwróciły uwagę zarówno TK, jak i TSUE. W ocenie Trybunału w Luksemburgu brak zapewnienia, by dane były przechowywane na terenie UE, oznacza, iż dyrektywa nie gwarantuje „kontroli poszanowania wymogów ochrony i bezpieczeństwa". Obecnie – jak wskazał podczas rozprawy przed TK przedstawiciel Urzędu Komunikacji Elektronicznej – przedsiębiorcy zastrzegają informacje dotyczące umiejscowienia serwerów lub

dotyczące własnej sieci, jako tajemnicę przedsiębiorstwa. Organ ten nie zna więc miejsca ich przechowywania".

W naszej ocenie niezbędne jest wprowadzenie takich regulacji, które wymuszą na operatorach telekomunikacyjnych przechowywanie danych na terenie Unii Europejskiej ze względu na obowiązujące tu standardy ochrony danych osobowych.

3. Podsumowanie

W ocenie Fundacji Panoptykon projekt nie odpowiada na kluczowe problemy związane z pozyskiwaniem przez policję i inne uprawnione podmioty danych telekomunikacyjnych. Jego przyjęcie byłoby jedynie **fasadowym** wdrożeniem wyroku Trybunału Konstytucyjnego. W szczególności, kształt proponowanego mechanizmu kontroli nad sięganiem po dane telekomunikacyjne nie realizuje standardów niezbędnych w demokratycznym państwie prawa.

Jednocześnie projekt nie realizuje innych, ważnych wytycznych wynikających z wyroku Trybunału Sprawiedliwości Unii Europejskiej, w szczególności wprowadzenia zasady subsydiarności, informowania osób, których dane zostały pobrane oraz ograniczenia celu, w jakim dane mogą zostać pobrane.

Z powyższych względów, w naszej ocenie, opiniowany projekt jest niezgodny zarówno z Konstytucją RP, jak i prawem UE. Jego przyjęcie w tym kształcie doprowadzi zatem do ponownego uchylenia odpowiednich przepisów przez Trybunał Konstytucyjny lub podjęcia odpowiednich kroków przez Komisję Europejską. Do tego czasu będzie jednak dochodziło do systematycznego naruszenia prawa do prywatności osób, których dane telekomunikacyjne będą pobierane przez policję i inne uprawnione podmioty.

W naszej ocenie niezbędna jest:

- Gruntowna rewizja przewidzianego modelu kontroli nad wykorzystywaniem danych telekomunikacyjnych w taki sposób, by konieczność uzyskania zgody sądu bądź innego niezależnego organu było zasadą, a nie wyjątkiem;
- wprowadzenie zasady subsydiarności, która zapewni, że uprawnione podmioty będą sięgać po dane wyłącznie w sytuacjach, w których inne środki okażą się niewystarczające lub nieprzydatne;
- wprowadzenie mechanizmu informowania osób, których dane zostały pobrane, o tym fakcie;
- konsekwentne ograniczenie sytuacji, w których możliwe jest sięganie po dane telekomunikacyjne, do spraw dotyczących poważnych przestępstw.

RZECZPOSPOLITA POLSKA
PROKURATOR GENERALNY

Warszawa, dnia 17.07. 2015 r.

PG VII G 025-224/15

Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej Senatu RP

Szanowny Panie Przewodniczący

W nawiązaniu do pisma z dnia 26 czerwca 2015 r., nr BPS/KU-034/967/4/15, dotyczącego ***projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)***, przekazanego Prokuratorowi Generalnemu do wyrażenia opinii w trybie art. 3 ust. 1 pkt 9 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r. Nr 270, poz. 1599, z późn. zm.), uprzejmie przedstawiam następujące stanowisko.

I. Zmiany proponowane w projekcie ustawy są konsekwencją wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, zatem w tej części stanowiska ocenie poddano poprawność projektowanych regulacji w aspekcie zachowania standardów konstytucyjnych, czy realizują one wskazany wyrok Trybunału Konstytucyjnego.

W orzeczeniu tym Trybunał orzekł o niezgodności z Konstytucją RP szeregu unormowań ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawy o Służbie Kontrwywiadu Wojskowego i o Służbie Wywiadu Wojskowego, ustawy o Centralnym Biurze Antykorupcyjnym, jak również o Służbie Celnej, dotyczących między innymi

prowadzenia przez te służby kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej oraz niszczenia zbędnych lub objętych zakazami dowodowymi danych pozyskanych przez te służby (vide: OTK ZU Nr 7/A/2014, poz. 80, s. 1179 - 1181).

Umarzając w części omawiane postępowanie, zainicjowane połączonymi wnioskami Prokuratora Generalnego oraz Rzecznika Praw Obywatelskich, Trybunał Konstytucyjny powołał się na własne orzecznictwo, zgodnie z którym, jeśli Trybunał stwierdza niekonstytucyjność kwestionowanej regulacji chociażby z jednym ze wskazanych wzorców kontroli, postępowanie w zakresie badania zgodności tej regulacji z pozostałymi wzorcami kontroli może zostać umorzone na podstawie art. 39 ust. 1 pkt 1 ustawy o TK ze względu na zbędność wyrokowania. Mając to na uwadze, Trybunał postanowił umorzyć na tej podstawie badanie zgodności niektórych przepisów, co do których orzekł o niekonstytucyjności przynajmmniej z jednym ze wskazanych wzorców kontroli. Takie rozstrzygnięcie, uwarunkowane ekonomią postępowania, nie może być jednak odczytane jako aprobata zakwestionowanych przepisów ingerujących w konstytucyjne prawo do ochrony prywatności, autonomię informacyjną i ochronę tajemnicy komunikowania się z punktu widzenia wzorców, wobec których postępowanie zostało umorzone na podstawie art. 39 ust. 1 pkt 1 ustawy o TK. Ustawodawca zobowiązany jest - konstruując nowe unormowania w zakresie kontroli operacyjnej oraz udostępniania i przetwarzania danych telekomunikacyjnych - uwzględnić standard konstytucyjny dotyczący czynności operacyjno-rozpoznawczych, przedstawiony w powołanym wyroku (por. op. cit., s. 1277 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny podkreślił również, że mając na uwadze cele omawianego postępowania, a także ekonomię procesową, Trybunał, uwzględniając argumentację zawartą we wszystkich wnioskach Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego dotyczących gromadzenia i przetwarzania danych telekomunikacyjnych, postanowił najpierw poddać kontroli art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW z punktu widzenia ich zgodności z art. 49

w związku z art. 31 ust. 3 Konstytucji, a także art. 75d ust. 1 ustawy o S.C. - z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji. Stwierdzenie niekonstytucyjności tych przepisów w całości uczyniłoby bowiem zbędnym rozpoznawanie szczegółowych zarzutów Prokuratora Generalnego, ujmujących je w związku z konkretnymi przepisami innych ustaw (por. op. cit., s. 1255).

Jednocześnie Trybunał Konstytucyjny stanął na stanowisku, że oceniając konstytucyjność przepisów kompetencyjnych, które upoważniają organy władzy publicznej do wykorzystywania danych telekomunikacyjnych w pracy operacyjno-rozpoznawczej, Trybunał nie może ignorować otoczenia normatywnego, w jakim zaskarżone przepisy funkcjonują oraz sposobu ich stosowania przez właściwe organy. Nie może również pominąć znaczenia wyroku Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. o sygn. C - 293/12, który orzekł o nieważności dyrektywy 2006/24/WE (vide: ibidem).

Trybunał Konstytucyjny przyjął, że wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. w sprawie sygn. C - 293/12 ma charakter ostateczny. Wiąże nie tylko instytucje i organy UE, ale również wszystkie organy państw członkowskich, w tym sądy i organy stosujące przepisy regulujące dostęp do danych telekomunikacyjnych. W związku z tym, że TSUE nie ograniczył w wyroku jego skutków w czasie, należałoby przyjąć, iż w zakresie nieważności dyrektywy w sprawie zatrzymywania danych wyrok wywiera skutek ex tunc (por. op. cit., s. 1220).

Zgodnie ze wspomnianym wyrokiem z dnia 8 kwietnia 2014 r., sygn. C 293/12, jednym z powodów stwierdzenia nieważności dyrektywy retencyjnej Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 15 marca 2006 r. nr 2006/24/WE był fakt, że dyrektywa ta nie tylko nie wyznaczała ogólnych granic zakresu jej stosowania, ale także nie przewidywała żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw, które, z uwagi na zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i art. 8 Karty Praw Podstawowych Unii Europejskiej, można uznać za wystarczająco poważne, by taką ingerencję uzasadnić. Przeciwnie, dyrektywa 2006/24/WE

ograniczała się do ogólnego odesłania, w art. 1 ust. 1, do pojęcia „poważnych przestępstw" określonych w ustawodawstwie każdego państwa członkowskiego.

Z kolei sam Trybunał Konstytucyjny stanął na stanowisku, że w ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi to przesłankami są wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im, ustawa powinna wskazywać rodzaje takich przestępstw (por. wyrok z dnia 30 lipca 2014 r., op. cit., s. 1230 oraz powołane tam orzecznictwo Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka).

Trybunał Konstytucyjny podkreślił, że to ustawa ma precyzować przedmiotowe przesłanki zarządzenia czynności operacyjno-rozpoznawczych. Aby zachować standard konstytucyjny, nie wystarcza odwołanie się do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest wobec tego zdefiniować zamknięty i możliwie wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki (vide: ibidem, s. 1225).

Analiza proponowanych w projekcie ustawy unormowań, określających dopuszczalny zakres pozyskiwania danych telekomunikacyjnych przez poszczególne służby mundurowe oraz specjalne uprawnia do wysnucia wniosku, że projektodawca w sposób zróżnicowany i niekonsekwentny uregulował uprawnienia tychże służb, nierzadko ignorując wymogi stawiane w wyrokach: Trybunału Konstytucyjnego - z dnia z 30 lipca 2014 r., sygn. K 23/11 oraz Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r., sygn. C - 293/12/WE.

Przykładowo, proponowana regulacja art. 20c ust. 1 pkt 1 ustawy o Policji, o czym w dalszej części opinii, stanowi, że w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalania dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych, Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy - Prawo telekomunikacyjne. Z kolei, zgodnie z proponowaną regulacją art. 30 ust. 1 pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych „[w] celu rozpoznawania, zapobiegania, zwalczania, wykrywania przestępstw, w tym przestępstw skarbowych albo uzyskania i utrwalenia dowodów popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1,

3, 5 i 6 albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych i ratowniczych Żandarmeria Wojskowa, może mieć udostępniane dane, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne".

Ewentualne przyjęcie obu wskazanych wyżej propozycji regulacji, w kontekście omawianych wyroków Trybunału Konstytucyjnego (z dnia 30 lipca 2014 r.) oraz Trybunału Sprawiedliwości Unii Europejskiej (z dnia 8 kwietnia 2014 r.) należy uznać za niedopuszczalne. Pogląd, że wszystkie stypizowane przez ustawodawcę przestępstwa (w tym skarbowe), czy chociażby tylko wszystkie przestępstwa ścigane z oskarżenia publicznego są przestępstwami „poważnymi", należałoby uznać za pogląd całkowicie niezasadny. Natomiast działania ratownicze lub poszukiwawcze (*per se*) nie mogą zostać zakwalifikowane jako wykrywanie lub zwalczanie przestępstw, choć w określonych warunkach mogą uzasadniać wkroczenie w prawa i wolności obywatelskie.

Podobnie wadliwie zredagowano proponowany art. 10b ust. 1 pkt 1 ustawy o Straży Granicznej (art. 2 pkt 2 projektu), stanowiący, że w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalania dowodów przestępstw określonych w art. 1 ust. 2 pkt 4 oraz ust. 2a Straż Graniczna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy - Prawo telekomunikacyjne. Art. 1 omawianej ustawy (nienowelizowany) w ust. 2 pkt 4 oraz w ust. 2a wymienia, przy różnym stopniu uszczegółowienia, czyny zabronione pod groźbą kary, do ścigania których jest właściwa Straż Graniczna. Przykładowo, w przepisie tym wskazano również przestępstwa wymienione w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, w tym określone w art. 95 § 1 Kodeksu karnego skarbowego (nieprzechowywanie dokumentów mających znaczenie dla kontroli celnej), które, trudno zakwalifikować do kategorii „przestępstw poważnych". Tym samym, proponowana regulacja nie zasługuje na ocenę pozytywną.

Kolejnym problemem, wymagającym podniesienia w kontekście wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, jest określenie rodzaju środka technicznego, za pomocą którego mają być pozyskiwane w toku kontroli operacyjnej informacje i dowody dotyczące jednostki. W omawianym wyroku Trybunał orzekł, że art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży

Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym, rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną wskaże określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z powołanymi w sprawie wzorcami kontroli konstytucyjnej (wyrok K 23/11, op. cit., s. 1180).

Jednocześnie Trybunał Konstytucyjny stwierdził, że ustawodawca nie sprecyzował elementów, jakie ma zawierać postanowienie sądu o zarządzeniu kontroli operacyjnej, w przeciwieństwie do wymagań odnoszących się do wniosku pochodzącego od szefa właściwej służby. Trybunał Konstytucyjny w toku rozpoznawania niniejszej sprawy ustalił, że w orzecznictwie sądowym istnieje rozbieżna praktyka dotycząca wskazywania w postanowieniu o zarządzeniu kontroli operacyjnej rodzaju środka technicznego, o którym mowa w art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA oraz art. 31 ust. 4 pkt 3 ustawy o SKW. Co do zasady, sądy nie wskazują w postanowieniu środka technicznego, ograniczając się jedynie do zdefiniowania, że chodzi o środek techniczny (por. ibidem, s. 1252).

Trybunał Konstytucyjny stwierdził ponadto, że pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków (vide: ibidem, s. 1230). Wydaje się więc, że skoro Trybunał Konstytucyjny posłużył się w wyroku konstrukcją tak zwanego orzeczenia interpretacyjnego, a postanowienia sądu nie można skorygować w drugiej instancji na skutek środka odwoławczego (ani prokuratora, ani osoby zainteresowanej), to ustawodawca winien w sposób pozytywny określić, jakie elementy, w omawianym zakresie, powinno zawierać postanowienie sądu o zarządzeniu kontroli operacyjnej. W szczególności, ustawodawca powinien przyjąć regulację określającą obowiązek wskazania przez właściwy organ zarządzający kontrolę operacyjną

określonego w prawie rodzaju środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowanego w konkretnej sprawie.

Jak już sygnalizowano, Trybunał Konstytucyjny zastrzegł w wyroku z dnia 30 lipca 2014 r., sygn. K 23/11, iż ustawodawca zobowiązany jest - konstruując nowe unormowania w zakresie kontroli operacyjnej oraz udostępniania i przetwarzania danych telekomunikacyjnych - uwzględnić standard konstytucyjny dotyczący czynności operacyjno-rozpoznawczych, przedstawiony w tymże wyroku (por. op. cit., s. 1277). Takiego wymogu nie spełnia opiniowany projekt ustawy, pozostawiając w obrocie prawnym regulacje ewidentnie sprzeczne z ustalonym przez Trybunał Konstytucyjny standardem.

Zgodnie z analizowanym wyrokiem Trybunału Konstytucyjnego w sprawie K 23/11, niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych. Przede wszystkim powinien istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby te czynności na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie. Obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności (por. op. cit., s. 1229 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny zaliczył tym samym do standardu konstytucyjnego 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 (vide: ibidem, s. 1230). Trybunał zastrzegł równocześnie, że ma świadomość, iż w pewnych sytuacjach może być również uzasadnione odstąpienie od wspomnianego

obowiązku informacyjnego. Kwestie te musi rozstrzygnąć jednak sam ustawodawca (por. ibidem, s. 1229).

Mimo takiego stanowiska Trybunału Konstytucyjnego, ustawodawca nie poczynił żadnych modyfikacji w zakresie obowiązujących unormowań, ustanawiających regułę w postaci zakazu udostępniania materiałów zgromadzonych podczas trwania kontroli operacyjnej osobie, wobec której kontrola operacyjna była stosowana (art. 19 ust. 16 ustawy o Policji, art. 9e ust. 17 ustawy o Straży Granicznej, art. 36c ust. 13 ustawy o kontroli skarbowej, jak również art. 31 ust. 17 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Nie wprowadzono również żadnych stosownych uregulowań do art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, jak również art. 17 ustawy o Centralnym Biurze Antykorupcyjnym.

W tym miejscu wypada odnotować, że jedynie pozytywny wynik kontroli operacyjnej, polegający na uzyskaniu spodziewanych dowodów i prowadzący w rezultacie do wniesienia oskarżenia, może pośrednio, w trybie art. 321 Kodeksu postępowania karnego, doprowadzić do ujawnienia faktu prowadzenia takiej kontroli. Negatywny wynik kontroli operacyjnej (kiedy nie uzyska się w jej toku dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego) w praktyce wyklucza realizację wskazanego przez Trybunał obowiązku informacyjnego. Warto również zaznaczyć, że negatywny wynik kontroli operacyjnej może wynikać z wadliwej prognozy, dotyczącej pozyskania materiałów pozwalających na zapobieżenie, wykrycie, ustalenie sprawców, a także uzyskanie i utrwalenie dowodów przestępstw, poczynionej przez służbę składającą wniosek o zarządzenie takiej kontroli, albo błędnej decyzji sądu w zakresie potrzeby podjęcia kontroli operacyjnej. W opisanej sytuacji, obowiązujące rozwiązanie prawne uniemożliwia podjęcie skutecznych czynności kontrolnych wobec wadliwie działającej służby.

Zdaniem Trybunału Konstytucyjnego istotne znaczenie, z punktu widzenia konstytucyjnych standardów dopuszczalności czynności operacyjno-rozpoznawczych, ma zapewnienie osobie zainteresowanej poddania sądowej ocenie legalności

zastosowania wobec niej działań operacyjnych (por. wyrok z dnia 30 lipca 2014 r., op. cit., s. 1230). Trybunał stanął na stanowisku, że ustawodawca, konstruując nowe unormowania w zakresie kontroli operacyjnej oraz udostępniania i przetwarzania danych telekomunikacyjnych, obowiązany jest uwzględnić standard konstytucyjny zapewniający osobie zainteresowanej poddanie sądowej ocenie legalności zastosowana wobec niej działań operacyjnych. Trybunał nie wskazał przy tym możliwości odstępstw od przedstawionej zasady.

Projektodawca w omawianym zakresie nie uwzględnił orzeczenia Trybunału Konstytucyjnego, pozostawiając bez zmian obowiązujące regulacje art. 19 ust. 20 i art. 20 ust. 8 ustawy o Policji, art. 9e ust. 19 oraz art. 10c ust. 7 ustawy o Straży Granicznej, art. 36c ust. 4 ustawy o kontroli skarbowej, art. 31 ust. 19 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 11a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, jak również art. 17 ust. 17 oraz 23 ust. 7 ustawy o Centralnym Biurze Antykorupcyjnym, które to przepisy przyznają środek odwoławczy od postanowienia sądu w przedmiocie kontroli operacyjnej oraz w przedmiocie zgody na udostępnienie informacji i danych wskazanego podmiotu jedynie organowi służby, który o takie postanowienie sądu występował, przy pominięciu przyznania takiego uprawnienia osobie zainteresowanej oraz prokuratorowi.

Projektodawca w opiniowanym projekcie ustawy zaproponował natomiast poszerzenie uprawnień służb poprzez przyznanie im podobnych uprawnień w zakresie możliwości wnoszenia zażalenia na postanowienie sądu w przedmiocie zgody na pozyskanie danych dotyczących osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, poprzez zamieszczenie w projekcie nowych regulacji art. 20cb ust. 4 ustawy o Policji, art. 10bb ust. 4 ustawy o Straży Granicznej, art. 36bc ust. 4 ustawy o kontroli skarbowej, art. 30c ust. 4 ustawy o Żandarmerii Wojskowej i wojskowych służbach porządkowych, art. 28 ust. 2 pkt 4 i art. 28b ust. 4 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32b ust. 4 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18b ust. 4 ustawy o Centralnym Biurze Antykorupcyjnym, jak również art. 75db ust. 4 ustawy o Służbie Celnej. Projektodawca przyznając, wbrew

stanowisku Trybunału Konstytucyjnego, powyższe uprawnienie organom służb, takiego uprawnienia nie przyznał osobom zainteresowanym, jak również możliwości wnoszenia zażalenia nie przyznano prokuratorowi.

W związku z takim zabiegiem legislacyjnym polegającym na pozostawieniu w obrocie prawnym wymienionych wyżej regulacji i wprowadzenie do obrotu prawnego unormowań analogicznych, nie tylko nie prowadzi do dostosowania systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, ale będzie kolidowało również z art. 2 i art. 45 ust. 1 w związku z art. 78 Konstytucji oraz z art. 6 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności.

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, prawo do sądu obejmuje cztery podstawowe elementy: prawo dostępu do sądu, prawo do odpowiedniego ukształtowania procedury sądowej zgodnie z wymogami sprawiedliwości i jawności, prawo do uzyskania wiążącego rozstrzygnięcia sprawy przez sąd oraz prawo do odpowiedniego ukształtowania ustroju i pozycji organów rozpoznających sprawy. Trybunał Konstytucyjny wielokrotnie wyjaśniał znaczenie konstytucyjnych standardów sprawiedliwego postępowania sądowego. Sprawiedliwość proceduralna należy do istoty konstytucyjnego prawa do sądu, albowiem prawo do sądu bez zachowania standardu rzetelności postępowania byłoby prawem fasadowym (vide - wyroki: z dnia 21 lipca 2009 r., sygn. K 7/09, OTK ZU Nr 7/A/2009, poz. 113, s. 1186 - 1187 oraz powołane tam orzecznictwo, jak również z dnia 14 stycznia 2014 r., sygn. SK 25/11, OTK ZU Nr 1 /A/2014, poz. 1, s. 13 oraz powołane tam orzecznictwo).

Z kolei zakres podmiotowy prawa do sądu został wyznaczony przez konstytucyjne pojęcie „sprawy". Trybunał Konstytucyjny ustalając znaczenie tego terminu wielokrotnie wyrażał pogląd, że urzeczywistnienie konstytucyjnych gwarancji prawa do sądu obejmuje wszystkie sytuacje, bez względu na szczegółowe regulacje proceduralne, w których pojawia się konieczność rozstrzygnięcia o prawach danego podmiotu (w relacji do innych równorzędnych podmiotów lub w relacji do władzy publicznej), a jednocześnie natura danych stosunków prawnych wyklucza arbitralność rozstrzygnięcia o sytuacji prawnej podmiotu przez drugą stronę tego stosunku (por. wyroki: z dnia 18 maja 2004 r, sygn. SK 28/03, OTK ZU Nr 5/A/2004, poz. 45, s. 629

i z dnia 11 czerwca 2002 r., sygn. SK 5/02, OTK ZU Nr 4/A/2002, poz. 41, s. 554 oraz powołane tam orzecznictwo).

Ustawodawca kształtując uprawnienia stron postępowania, musi wziąć pod uwagę także ogólne cele postępowania oraz inne wartości, takie jak sprawność postępowania, wyważywszy kolidujące interesy. Trybunał Konstytucyjny zwracał w związku z tym uwagę na granice swobody regulacyjnej przy stanowieniu ustaw normujących postępowania sądowe. Swoboda ustawodawcy kształtowania odpowiednich procedur nie oznacza dopuszczalności wprowadzania rozwiązań arbitralnych, które ponad miarę, a więc bez wystąpienia istotnych racji, ograniczają prawa procesowe strony, których realizacja stanowi przesłankę prawidłowego i sprawiedliwego rozstrzygnięcia sprawy. Jeżeli ograniczenie uprawnień procesowych strony jest zbędne, z punktu widzenia zamierzonych przez ustawodawcę celów, takich jak zapewnienie większej efektywności postępowania i jego szybkości, a jednocześnie wypacza pozycję stron, uniemożliwia właściwe zrównoważenie ich pozycji procesowej, a tym samym łamie podstawowy postulat sprawiedliwości proceduralnej, czy wreszcie prowadzi do arbitralnego rozstrzygnięcia sprawy - to w tego rodzaju wypadkach dochodziłoby do naruszenia gwarancji konstytucyjnych związanych z prawem do sądu (vide - wyrok z dnia 21 lipca 2009 r., sygn. K 7/09, op. cit., s 1187 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny przypominał także funkcje społeczne sprawiedliwej procedury sądowej. Procedura taka ma szczególne znaczenie dla kształtowania zaufania obywateli do wymiaru sprawiedliwości i poczucia poszanowania ich praw. Nierzetelne procedury sądowe, nawet jeśli nie muszą prowadzić wprost do faktycznego zawieszenia obowiązywania konstytucyjnego prawa do sądu, a pośrednio do unicestwienia innych praw i wolności konstytucyjnych, których ochronę gwarantuje prawo do sądu (np. godność osobista, życie, wolność, prawo własności), to jednak przez naruszenie zaufania, jakie winna wytwarzać rzetelna procedura sądowa, budzą zastrzeżenia (por. ibidem, s. 1187 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny stanął również na stanowisku, że sprawiedliwa procedura sądowa powinna zapewniać stronom uprawnienia procesowe stosowne do przedmiotu prowadzonego postępowania. W każdym wypadku ustawodawca powinien

zapewnić jednostce prawo do wysłuchania. Jednostka musi uzyskać w szczególności możliwość przedstawienia swoich racji oraz zgłaszania wniosków dowodowych. Istotny element sprawiedliwej procedury sądowej stanowi prawo strony do osobistego udziału w czynnościach procesowych (vide - wyrok z dnia 19 września 2007 r., sygn. SK 4/06, OTK ZU Nr 8/A/2007, poz. 98, s. 1224 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny zaakcentował także pogląd, że konieczność ochrony w demokratycznym państwie takich wartości jak: bezpieczeństwo państwa, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, wolności i praw innych osób nie może uzasadniać zamknięcia drogi sądowej w odniesieniu do praw objętych zakresem zastosowania art. 77 ust. 2 Konstytucji, może natomiast, co najwyżej, uzasadniać pewne ograniczenia ochrony sądowej, przejawiające się w odmiennym ukształtowaniu zasad postępowania sądowego w stosunku do ogólnych reguł proceduralnych (por. wyrok z dnia 10 maja 2000 r., sygn. K. 21/99, OTK ZU Nr 4/2000, poz. 109, s. 558).

Nadto wypadałoby odnotować, iż w literaturze przedmiotu przyjmuje się, że art. 78 Konstytucji RP wyraża generalną zasadę aksjologiczną: drugoinstancyjna kontrola orzeczeń i decyzji jest istotnym elementem ochrony praw jednostki bo, stwarzając możliwość weryfikacji pierwszego rozstrzygnięcia, przeciwdziała arbitralności i ułatwia unikanie pomyłek i krzywd. W tym sensie stanowi ona komponent demokratycznego państwa prawnego. Tak rozumiany art. 78 Konstytucji wykazuje bliskie związki logiczne z tymi przepisami konstytucyjnymi, które - z jednej strony - formułują prawo do sądu (art. 45 ust. 1 i art. 77 ust. 2), a - z drugiej strony - ustanawiają nakaz dwuinstancyjnego postępowania sądowego (art. 176 ust. 1). Niemniej art. 78 Konstytucji nie może być traktowany jako kolejne - po art. 77 ust. 2 - przypomnienie, że każdemu przysługuje prawo do sądu, czy jako element ogólnego prawa do sądu. Jest to raczej wskazanie szczególnej gwarancji „sprawiedliwości proceduralnej", odnoszącej się do wszystkich typów postępowań, więc wykraczającej poza zakres postępowań toczących się przed sądami. W odniesieniu do postępowań sądowych prawo do zaskarżania pierwszoinstanyjnych orzeczeń traktowane jest jako środek wzmacniający prawo do sądu i urealniający jego prawidłowe urzeczywistnienie. Oczywiście prawo zaskarżania pierwszoinstancyjnych rozstrzygnięć rzutuje w sposób

zasadniczy na sposób realizacji prawa do sądu (por. Leszek Garlicki, [w:] Konstytucja Rzeczypospolitej Polskiej, Komentarz, V Tom, Wydawnictwo Sejmowe, Warszawa 2007, tezy do art. 78, s. 2 oraz powołane tam poglądy doktryny).

Zakres podmiotowy art. 78 Konstytucji odniesiony do stron, powiązano więc z podmiotami uczestniczącymi w postępowaniu, które doprowadziło do wydania orzeczenia lub decyzji. Pojęciu strony należy natomiast przypisywać autonomiczne znaczenie: nie musi ono pokrywać się ze sposobem jego rozumienia w przepisach poszczególnych procedur. Za „stronę" należy więc uznać każdego uczestnika postępowania, w którym wydano orzeczenie lub decyzję, tzn. każdego, kto formalnie został dopuszczony do udziału w tym postępowaniu, jako dotyczącym jego praw, obowiązków czy sytuacji prawnej. Każdej, tak rozumianej, stronie postępowania art. 78 Konstytucji gwarantuje prawo zaskarżania poszczególnych, podejmowanych w tym postępowaniu rozstrzygnięć. Zarazem prawo to może przysługiwać tylko stronie, więc (poza sytuacjami szczególnymi) nie może rozciągać się na podmioty, które nie mają interesu prawnego w sprawie i, które nie uczestniczyły w pierwszoinstancyjnej procedurze. Prawo to powinno przysługiwać wszystkim „stronom" postępowania na równych zasadach, wynika to zarówno z ogólnych konsekwencji zasady równości, jak i z zasady „równości broni" (por. Leszek Garlicki, op. cit., s. 4 oraz powołane tam poglądy doktryny).

W doktrynie podnosi się, że „[p]rawo do zaskarżenia odnosi się do rozstrzygnięć o wszelkim charakterze: zarówno kończących postępowanie (orzekających o istocie sprawy), jak i najróżniejszych rozstrzygnięć wpadkowych. (...) Prawo do zaskarżenia odnosi się do rozstrzygnięć wydawanych we wszelkiego typu postępowaniach, chyba że zostanie ono wyłączone szczególnym przepisem konstytucyjnym" (vide - ibidem, s. 5 - 6).

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, do koniecznych uprawnień stron w sprawiedliwej procedurze sądowej należą m.in. odpowiednie środki zaskarżenia. Trybunał przypominał przy tym, że przy określaniu uprawnień przysługujących stronom niezbędne jest takie ukształtowanie środków proceduralnych, aby umożliwić właściwe zrównowazenie pozycji procesowej każdej ze stron (vide -

wyrok z dnia 21 lipca 2009 r., sygn. K 7/09, op. cit., s 1187 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny niejednokrotnie prezentował stanowisko, że obowiązywanie zasady dwuinstancyjnego postępowania nie musi ograniczać się do głównego nurtu postępowania sądowego. Zasada ta ma zastosowanie także wobec kwestii rozstrzyganych incydentalnie, wpadkowo, poza nurtem postępowania „głównego", jeżeli dotyczą praw lub obowiązków danego podmiotu (por. wyroki: z dnia 22 października 2013 r., sygn. SK 14/13, OTK ZU Nr 7/A/2013, poz. 100, s. 1403 oraz powołane tam orzecznictwo, jak również z dnia 12 kwietnia 2012 r., sygn. SK 21/11, OTK ZU Nr 4/A/2012, poz. 38, s. 376 oraz powołane tam orzecznictwo).

Szczególnie istotne znaczenie ma konstatacja Trybunału Konstytucyjnego, który stwierdził że, określając podmiot prawa do zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji, prawodawca konstytucyjny posłużył się terminem „każda ze stron". Przez stronę, w rozumieniu art. 78 Konstytucji, należy rozumieć każdy podmiot, którego praw lub obowiązków dotyczy rozstrzygnięcie wydane w pierwszej instancji, nawet jeżeli prawo nie przewiduje udziału tego podmiotu w postępowaniu prowadzącym do wydania tego rozstrzygnięcia (vide - wyrok z dnia 19 września 2007 r., sygn. SK 4/06, op. cit., s. 1225 oraz powołane tam orzecznictwo, jak również wyrok z dnia 14 marca 2006 r., sygn. SK 4/05, OTK ZU Nr 3/A/2006, poz. 29, s. 292).

Trybunał Konstytucyjny podkreślał niejednokrotnie, że celem reguły instancyjności jest zapobieganie pomyłkom i arbitralności w pierwszej instancji. Brak możliwości zaskarżenia do sądu wyższej instancji ogranicza zainteresowanym prawo do sądu, co jest sprzeczne z zasadą demokratycznego państwa prawnego (por. wyrok z dnia 12 czerwca 2002 r., sygn. P 13/01, OTK ZU Nr 4/A/2002, poz. 42, s. 569 oraz powołane tam orzecznictwo, jak również z dnia 25 lipca 2013 r., sygn. SK 61/12, OTK ZU Nr 6/A/2013, poz. 84, s. 1165 oraz powołane tam orzecznictwo).

Postanowienia sądu w przedmiocie kontroli operacyjnej niewątpliwie stanowią rozstrzygnięcia o wolnościach i prawach osoby poddawanej takiej kontroli. Tym samym, wyczerpują one konstytucyjne pojęcie „sprawy" w rozumieniu przytoczonego wyżej orzecznictwa Trybunału Konstytucyjnego, co przesądza, że ustawodawca jest obowiązany unormować wspomnianą kwestię, respektując konstytucyjne gwarancje

prawa do sądu. Prawo do sądu bez zachowania standardu rzetelności postępowania byłoby jedynie prawem fasadowym. Przytoczone orzecznictwo Trybunału Konstytucyjnego przesądza, że nawet jeśli podmiot, o którego prawach lub obowiązkach rozstrzyga sąd w pierwszej instancji, nie bierze udziału w postępowaniu prowadzącym do wydania tego rozstrzygnięcia (jak ma to miejsce w przypadku postanowień w przedmiocie kontroli operacyjnej), to i tak podmiotowi temu przysługuje prawo do zaskarżenia takiego orzeczenia.

Obowiązujące procedury wydawania przez sąd postanowień w przedmiocie kontroli operacyjnej, w ramach czynności operacyjno-rozpoznawczych, nie przewidują żadnego udziału zainteresowanego, którego ta kontrola dotyczy. Innymi słowy, procedury te nie gwarantują zainteresowanemu ani prawa do wysłuchania, wskazywanego przez Trybunał Konstytucyjny jako podstawowy standard sprawiedliwej procedury, ani realizacji wymienionych w orzecznictwie Trybunału, jako koniecznych do zagwarantowania, uprawnień strony do zgłaszania wniosków dowodowych oraz osobistego udziału w czynnościach procesowych. Nierespektowanie przez ustawodawcę wymienionych wyżej standardów ukształtowania procedury sądowej usprawiedliwia się niejawnym charakterem czynności operacyjno-rozpoznawczych i koniecznością podejmowania takich czynności w tajemnicy przed zainteresowanym. Jednakże w takiej sytuacji szczególnego znaczenia nabiera konieczność rygorystycznego przestrzegania pozostałych standardów sprawiedliwości proceduralnej, w tym prawidłowego ukształtowania postępowania odwoławczego w sprawach, w których zapadły postanowienia sądu w przedmiocie kontroli operacyjnej. Analiza tak obowiązujących, jak i projektowanych przepisów zawartych w ustawach instytucjonalnych poszczególnych służb mundurowych oraz służb specjalnych uprawnia do wniosku, że konstytucyjna zasada, iż każda ze stron ma prawo do zaskarżania orzeczeń i decyzji wydanych w pierwszej instancji (art. 78 ustawy zasadniczej), w zakresie czynności operacyjno- rozpoznawczych stała się w polskim systemie prawnym wyjątkiem ograniczonym do tak zwanych podsłuchów procesowych oraz, w pewnym zakresie, podsłuchów realizowanych przez SKW (art. 31 ust. 10 ustawy o SKW). Regułą jest natomiast, że w przypadku podsłuchów realizowanych podczas kontroli operacyjnej przez Policję, Straż Graniczną, wywiad skarbowy, Żandarmerię

Wojskową, ABW, jak również CBA, zażalenie na postanowienie sądu w tym zakresie przysługuje jedynie organom służb, przy jednoczesnym pozbawieniu tego prawa osoby, wobec której podsłuch jest stosowany (prawa odroczonego w czasie).

Konsekwencją tej niezgodnej z Konstytucją RP zasady są zawarte w senackim projekcie ustawy propozycje kolejnych, wymienionych przypadków przyznania środka odwoławczego wyłącznie organom służb, przy pominięciu osoby zainteresowanej. Niejako na marginesie należałoby w tym miejscu odnotować, że ustawodawca pozbawił tego prawa (i zamierza to uczynić w projektowanych regulacjach) również prokuratora, co jednak wymagałoby przedstawienia odrębnych wywodów, wykraczających poza ramy niniejszej oceny projektu ustawy.

Przechodząc do oceny kwestionowanych regulacji w kontekście art. 6 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności, należy odnotować poglądy doktryny, iż próba najbardziej ogólnego określenia zakresu pojęciowego prawa do rzetelnego postępowania, wynikającego z powołanego art. 6 ust. 1 Konwencji, sprowadza się do wymienienia dwóch podstawowych elementów standardu, to jest prawa do kontradyktoryjnego postępowania i zasady równości broni (por. Piotr Hofmański i Andrzej Wróbel, Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, Komentarz do artykułów 1 - 18, Tom I, pod redakcją Leszka Garlickiego, Wydawnictwo C.H. Beck, Warszawa 2010, s. 329 oraz powołane tam orzecznictwo Europejskiego Trybunału Praw Człowieka). W literaturze przedmiotu, jak również w orzecznictwie definiuje się, że „równość broni" oznacza, iż każda strona procesu musi mieć zapewnioną taką samą możliwość prezentowania swojej sprawy (także dowodów) w warunkach, które nie stawiają jej w sytuacji gorszej niż ta, w której znajduje się oponent (por. Piotr Hofmański i Andrzej Wróbel, op. cit., s. 335 oraz powołane tam orzecznictwo Europejskiego Trybunału Praw Człowieka, jak również Krystyna Kowalik - Bańczyk, Zasada równości broni, [w:] Prawo do obrony w unijnych postępowaniach antymonopolowych w kierunku unifikacji standardów proceduralnych w Unii Europejskiej)

Przedstawiciele nauki podkreślają również, że biorąc pod uwagę zakres stosowania art. 6 ust. 1 Konwencji, wymóg rzetelności postępowania należy odnieść do wszystkich jego stadiów, także do postępowania poprzedzającego wniesienie

oskarżenia do sądu, jak i do postępowań odwoławczych (por. Piotr Hofmański i Andrzej Wróbel, op. cit., s. 332 oraz powołane tam orzecznictwo ETPCz).

Zgodnie z orzecznictwem ETPCz, podstawowym aspektem prawa do rzetelnego procesu jest kontradyktoryjność postępowania karnego, włącznie z elementami postępowania związanymi z procedurą karną, oraz równość broni pomiędzy oskarżeniem a obroną (por. wyroki: z dnia 16 lutego 2000 r., Rowe i Davis v. Wielka Brytania, sygn. 28901).

Europejski Trybunał Praw Człowieka podkreślał również wielokrotnie, że pojęcie „rzetelnego procesu", gwarantowanego przez art. 6 ust. 1 Konwencji, obejmuje poszanowanie zasady równości broni. Zasada ta, która stanowi jeden z elementów szerszego pojęcia rzetelnego procesu w rozumieniu art. 6 ust. 1, wymaga zachowania sprawiedliwej równowagi pomiędzy stronami: każdemu winna zostać dana rozsądna możliwość przedstawienia swojej sprawy w warunkach, które nie stawiają tej osoby w mniej korzystnej sytuacji niż strony przeciwnej. Należy jednocześnie wskazać, iż to do organów władzy krajowej należy zapewnienie w danym przypadku poszanowania warunków „rzetelnego procesu" (por. wyroki: z dnia 12 kwietnia 2012 r., Legerdere v. Francja, sygn. 18851/07, z dnia 15 stycznia 2008 r., Luboch v. Polska, sygn. 37469/05, z dnia 5 lipca 2005 r., Lomaseita Oy i inni v. Finlandia, sygn. 45029/98 oraz z dnia 16 lutego 2000 r., Jasper v. Wielka Brytania).

Trybunał przypomniał również, że na podstawie zasady równości broni, jako jednego z elementów szerszej koncepcji słusznego procesu, każdej ze stron należy zapewnić rozsądną sposobność przedstawienia jej sprawy na warunkach, które nie umieszczają jej w położeniu niekorzystnym vis-a-vis jej przeciwnika (por. wyrok z dnia 22 lutego 1996 r., BULUT v. Austria, Orzecznictwo Strasburskie, Zbiór orzeczeń Europejskiego Trybunału Praw Człowieka 1990 — 1997, Tom I, Toruń 1998, s. 290, z dnia 23 października 1996 r., Ankeler v. Szwajcaria, Orzecznictwo Strasburkie, Zbiór orzeczeń..., op. cit., s. 303 oraz z dnia 27 października 1993 r., Dombo Beheer B.V. v. Holandia, Orzecznictwo Strasburskie, Zbiór orzeczeń..., op. cit. s. 225).

ETPCz niejednokrotnie prezentował również stanowisko, że nawet jeżeli podstawowym celem art. 6 Konwencji, w odniesieniu do spraw karnych, jest zapewnienie sprawiedliwego procesu przed „sądem" właściwym do rozstrzygnięcia

w przedmiocie „każdego oskarżenia", nie wynika stąd, iż artykuł ten nie ma zastosowania do postępowania poprzedzającego postępowanie sądowe. Art. 6 znajduje więc zastosowanie zanim sprawa jest wniesiona do sądu, jeżeli i tak dalece, jak rzetelność postępowania sądowego może zostać poważnie naruszona przez uprzedni brak zgodności z wymogami tego artykułu (por. wyroki: z dnia 6 czerwca 2000 r., Magee v. Wielka Brytania, sygn. 45029/98 oraz z dnia 23 czerwca 1981 r, le Comte, Van Leuven i De Meyere v. Belgia, sygn. 6878/75.

W kontekście przytoczonego orzecznictwa Europejskiego Trybunału Praw Człowieka, nie ulega wątpliwości, że Trybunał przykłada wielką wagę do zasady równości broni, jako fundamentalnego warunku rzetelnego procesu. Co więcej, zasada ta musi być respektowana również w toku realizacji procedur poprzedzających postępowanie sądowe, jak i w postępowaniu odwoławczym. Z omawianego orzecznictwa ETPCz wynika wprost, iż rzetelny proces wymaga zachowania sprawiedliwej równowagi między stronami oraz, że żadnej ze stron nie wolno postawić w sytuacji mniej korzystnej niż sytuacja strony przeciwnej.

Analiza aktualnie obowiązujących, jak i proponowanych w projekcie unormowań dotyczących środków odwoławczych od postanowień sądu w przedmiocie czynności operacyjno-rozpoznawczych prowadzi do wniosku, że polski ustawodawca, przyjmując te unormowania i proponując unormowania nowe, nie respektuje zasady równości broni. Służby mundurowe oraz specjalne zostały postawione przez ustawodawcę w sytuacji prawnej wyraźnie uprzywilejowanej w stosunku do osób, wobec których stosowane są podsłuchy oraz, wobec których zbierane są dane i informacje, nawet po zakończeniu owych czynności.

Jak już sygnalizowano, osobie, wobec której podejmowane są omawiane czynności operacyjno-rozpoznawcze, z samej natury niejawnych procedur nie gwarantuje się ani prawa do wysłuchania, ani prawa do zgłaszania wniosków dowodowych, ani prawa do osobistego udziału w czynnościach przed wydaniem przez sąd stosownego postanowienia w przedmiocie kontroli operacyjnej lub w przedmiocie pozyskiwania i wykorzystywania danych i informacji, ale nie ma uzasadnienia dla utrzymywania takiego stanu rzeczy już po zakończeniu owych czynności, i to nawet w czasie, gdy ujawnienie faktu ich prowadzenia nie może już w żaden sposób zagrozić

realizacji nadrzędnych celów procesu lub innym wartościom chronionym konstytucyjnie.

Poniżej przedstawiam bardziej szczegółowe odniesienie się do projektowanych zmian, proponowanych w poszczególnych ustawach kompetencyjnych, wskazując na najbardziej istotne wątpliwości, jak również poddaję pod rozwagę następujące uwagi.

II. Uregulowania proponowane w art. 1 projektu - obejmujące zmiany w ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 roku, poz. 355)

Art. 1 pkt 1 lit b projektu - zmieniający art. 19 ust. 6 ustawy o Policji

Przepis jest eklektyczny, razi niekonsekwencją i pozostaje w sprzeczności z normami gwarantowanymi konstytucyjnie. Jego treść wskazuje się, że kontrola operacyjna prowadzona jest niejawnie i polega na „podsłuchu rozmów prowadzonych przy użyciu środków technicznych", ale podkreślić należy, iż nie każdy przekaz informacji (np. treść wiadomości sms, mms) jest „rozmową" podlegającą kontroli operacyjnej. Pewna zatem część przekazów pozostawałaby poza dopuszczalną możliwością kontroli, wypaczając jej ustalenia.

Projektowany przepis, z uwagi na interpretację przez Trybunał Konstytucyjny pojęcia „korespondencji" ma bardzo szeroki zakres, albowiem zdaniem Trybunału, wyrażenie „kontrola treści korespondencji" nie zawęża się jedynie do tradycyjnej formy wymiany informacji, lecz obejmuje każdy sposób przekazywania informacji pomiędzy jednostkami, bez względu na formę (tradycyjna poczta, e-mail, SMS, MMS itp.).

W projektowanym art. 19 ust. 6 pkt 1 wymieniono jedynie podsłuch rozmów prowadzonych przy użyciu środków technicznych. Wątpliwości budzi to, czy w przypadku przepisu, wskazującego enumeratywnie na czym polega kontrola operacyjna i braku możliwości stosowania wykładni rozszerzającej, możliwe będzie objęcie kontrolą operacyjną także sms i mms. W punkcie pierwszym przepisu wskazuje się, że kontrola operacyjna polega na podsłuchu rozmów prowadzonych przy użyciu

„środków technicznych". Nasuwa się więc pytanie czy pozostałe formy kontroli operacyjnej polegające na:

- podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi,
- nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu nie będą prowadzone przy użyciu środków technicznych. Charakter czynności wskazanych w ust. 6 pkt 2 i 4 jednoznacznie wskazują, że mają one być wykonywane przy użyciu takich środków. Przepis wymaga więc przeredagowania w taki sposób, by odpowiadał rzeczywistemu charakterowi dozwolonych czynności operacyjnych.

W przepisie brak jest dookreślenia rodzajów użytych środków technicznych, co stanowiło dla Trybunału Konstytucyjnego wyznacznik poszanowania konstytucyjnej zasady legalizmu, zgodnie z którą wszystkie organy władzy publicznej mają działać na podstawie i w granicach prawa (art. 7 Konstytucji RP). Nie chodzi oczywiście o to, by w akcie rangi ustawowej specyfikować rodzaje możliwych do użycia środków technicznych, gdyż miałoby to negatywny wpływ na efektywność czynności operacyjnych. Nie byłoby też wskazane ze względu na dokonujący się postęp techniczny i związane z nim poszerzanie możliwości kontroli operacyjnej. Chodzi natomiast o to, by wnioskując o zastosowanie środka technicznego, a w szczególności podejmując decyzję o jego zastosowaniu odnosić się do konkretnego, zindywidualizowanego rodzaju użytego środka technicznego. W związku z tym, przepisy zmienianych ustaw w zakresie odnoszącym się do użycia środków technicznych winny wskazywać, że chodzi o „określone", względnie „wskazane" we wniosku środki techniczne.

Zasadnym byłoby więc doprecyzowanie przepisu (chyba, że sms i mms mogłyby zostać uznane za korespondencję, wymienioną art. 19 ust. 6 w pkt 3 ustawy, ale brak regulacji w tym zakresie mógłby powodować odmienne interpretacje i odmienną praktykę.

Ponadto przepis, który określa na czym polega kontrola operacyjna, należałoby również uzupełnić poprzez wskazanie, że uprawniony organ może nie tylko stosować podsłuch rozmów, ale również rejestrować ich treść, poprzez dodanie wyrazów: „i utrwalanie ich treści". Uzupełnienie przepisu o proponowaną treść konieczne jest również z tego powodu, iż w literaturze nie są odosobnione poglądy nakazujące

prowadzenie kontroli operacyjnej „na bieżąco", bez utrwalania treści rozmów, co ma umożliwić natychmiastowe reagowanie na zaistniałe zdarzenia, a przede wszystkim zapobiegać utrwalaniu treści osobistych, intymnych i nie mających znaczenia dla sprawy. Ostatnim i być może najistotniejszym argumentem uzasadniającym uzupełnienie proponowanego przepisu o wskazane „i utrwalanie ich treści" są kwestie dotyczące różnych interpretacji dotyczącej instytucji zgody następczej i terminów wystąpienia o zgodę następczą.

Podobne zmiany należałoby wprowadzić odpowiednio do:

1) art.2 pkt 1 „b" projektu ustawy, zmieniającego art. 9e ustawy o Straży Granicznej;

2) art. 3 pkt 3 lit. b projektu ustaw, zmieniającego art.36c ustawy z dnia 28 września 1991 roku o kontroli skarbowej;

3) art. 6 pkt 3 lit. b projektu ustawy zmieniającego art. 31 ust.7 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych;

4) art. 7 pkt 2 lit. a projektu ustawy, zmieniającego art.27 ust.6 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;

5) art. 9 pkt 1 lit. b projektu ustawy zmieniającego art. 31 ust.4 ustawy o Służbie Kontrwywiadu Wojskowego oraz o Służbie Wywiadu Wojskowego;

6) art. 10 pkt 1 lit. a projektu ustawy, zmieniającego art. 17 ust. 5 ustawy o Centralnym Biurze Antykorupcyjnym.

W związku z tą uwagą pozwolę sobie w tym miejscu poddać pod rozwagę zasadność dokonania we wszystkich ustawach kompetencyjnych ujednolicenia i doprecyzowania przepisów odnoszących się do terminów kierowania wniosków o wyrażenie zgody następczej, poprzez wskazanie, że organ „policyjny" nie później niż w terminie 2 miesięcy od zakończenia kontroli przekazuje materiały prokuratorowi, który nie później niż miesiąc od dnia ich otrzymania skieruje wniosek do sądu. Aktualne brzmienie tego przepisu budzi bowiem wątpliwości, czy wprowadzony w niej dwumiesięczny termin dotyczy przekazania materiałów kontroli operacyjnej prokuratorowi, czy też jest terminem, w którym to prokurator musi już skierować wniosek do sądu.

Art. 1 pkt 1 lit. c – dodawany art. 19 ust. 6a i 6b ustawy o Policji

Zastosowana w projekcie konstrukcja prawna przewiduje stosowanie wszelkich środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i zakłada równocześnie, że tą drogą może być pozyskany każdy dowód i każda informacja o osobie.

Trybunał Konstytucyjny w przywołanym na wstępie wyroku uznał za spełniające gwarancje konstytucyjne przyjęcie praktyki, w myśl której, organ zarządzający kontrolę operacyjną jest obowiązany do zindywidualizowania w każdej sprawie środka technicznego, jaki ma być stosowany. Z punktu widzenia wymagań konstytucyjnych dopuszczalne jest zastosowanie tylko takiego środka, który przewidziany został przez prawo i może być stosowany przez organ wnoszący o zarządzenie kontroli operacyjnej. Obowiązujące prawo musi precyzować dopuszczalne dla każdej ze służb „sposoby stosowania kontroli operacyjnej", spośród których organ składający wniosek o taką kontrolę ma dopiero wskazać rekomendowany w danej sprawie sposób kontroli.

Trybunał Konstytucyjny zwrócił uwagę, że ustrojowa pozycja sądów, jako organów niezależnych od władzy wykonawczej oraz postawionych na straży konstytucyjnych wolności i praw podmiotowych (art. 10, art. 77 ust. 2 Konstytucji) predestynuje je do przeprowadzania kompleksowej oceny wniosków o zarządzenie kontroli operacyjnej, a w konsekwencji także do precyzyjnego wyznaczania jej zakresu oraz sposobów pozyskiwania informacji. Z tego powodu, zarówno wniosek jak i postanowienie sądu musi wskazywać „konkretny" rodzaj środka technicznego, za pomocą którego mają być pozyskiwanie informacje i dowody dotyczące jednostki.

Art. 1 pkt 1 lit. d projektu, w którym nadaje się nowe brzmienie art. 19 ust. 9 ustawy o Policji.

W projektowanym przepisie przewidziano jednokrotną możliwość wydania postanowienia o przedłużeniu kontroli operacyjnej na czas oznaczony, jednak nie

dłuższy niż 12 miesięcy, po upływie okresów, o których mowa w ust. 8 (tj. 6 miesiącach).

Pozytywny aspekt proponowanej zmiany polega na ograniczeniu prawa do przedłużenia kontroli operacyjnej do „jednokrotnego" wydania postanowienia w tym przedmiocie przez sąd okręgowy. Należy jednak zwrócić uwagę, że w zestawieniu z czasem trwania kontroli i utrwalania rozmów telefonicznych określonym w art. 238 § 1 k.p.k., które mogą być wprowadzone najwyżej na okres 3 miesięcy, z możliwością przedłużenia, w szczególnie uzasadnionym wypadku, na okres najwyżej dalszych 3 miesięcy - przewidziany w art. 19 ust. 9 ustawy o Policji okres wykonywania kontroli operacyjnej jest niewspółmiernie długi, może bowiem łącznie wynosić aż 18 miesięcy. Wynika to z możliwości przedłużenia pierwotnego okresu kontroli operacyjnej na mocy postanowienia sądu o dalsze 3 miesiące i możliwości kolejnego, jednokrotnego przedłużenia tej kontroli na mocy postanowienia sądu na okres nieprzekraczający 12 miesięcy. Wskazany dysonans wynikający ze zróżnicowania długości terminów prowadzenia kontroli potęguje okoliczność, że kontrola operacyjna, prowadzona jest pod zdecydowanie mniejszym nadzorem sądu niż podsłuch procesowy.

Ponadto wydaje się, że konstrukcja „jednorazowego" wydawania takiego postanowienia może rodzić w praktyce wątpliwości ze stosowaniem tego przepisu i jego wykładnią. Z jednej strony - w przypadku przedłużenia kontroli operacyjnej np. o 3 miesiące norma wskazana w tym przepisie może spowodować „utratę" pozostałego okresu, z drugiej strony - jednorazowe przedłużenie na zbyt długi okres mieszczący się w 12 miesiącach (włącznie) prowadzić może do sytuacji, gdy kontrola taka będzie prowadzona do końca tego okresu pomimo ustania ku temu przesłanek.

Powyższa uwaga dotyczy również projektowanych zmian analogicznych przepisów w pozostałych ustawach kompetencyjnych (poza ustawą o ABW i AW oraz ustawą o SKW i SWW, w odniesieniu do których nie przewidziano w ogóle maksymalnego terminu prowadzenia kontroli operacyjnej, co również budzi wątpliwości, z uwagi na możliwość permanentnego „kontrolowania" danej osoby. Wydaje się więc zasadne precyzyjne uregulowanie, w jakich sytuacjach kontrola operacyjna może być prowadzona bez ograniczenia terminu.

Analogiczna uwaga odnosi się do tożsamej treści art. 9e ust. 10 ustawy o Straży Granicznej, a także art. 36c ust. 7 ustawy o kontroli skarbowej oraz art. 31 ust. 10 ustawy o Żandarmerii Wojskowej, które zawierają wskazany maksymalny okres 18 miesięcy stosowania kontroli operacyjnej.

Przejawem niekonsekwencji projektodawcy jest okoliczność, że w początkowym okresie limituje okres stosowania kontroli operacyjnej wprowadzając okresy 3 miesięczne, a następnie w sposób nieproporcjonalny zezwala na wydłużenie okresu kontroli czterokrotnie w stosunku do podstawowego okresu stosowania kontroli, wynoszącego 3 miesiące.

Art. 1 pkt 1 lit. e projektu – w którym w art. 19 dodaje się ust. 15f- 15i ustawy o Policji

Podstawowy zarzut do proponowanego przepisu dotyczy braku określenia terminu, w którym Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazuje prokuratorowi materiały mogące zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. Wskazany brak manifestuje się w sposób szczególny w zestawieniu z proponowanym w projekcie dalszym trybem procedowania z takimi materiałami. Mianowicie w art. 19 ust. 15g wskazuje się, że „prokurator niezwłocznie po otrzymaniu materiałów, kieruje je do sądu".

Projekt w art. 19 ust. 15h obliguje również sąd do wydania zarządzenia w przedmiocie zniszczenia materiałów w terminie 14 dni od dnia złożenia wniosku przez prokuratora. W konsekwencji w myśl projektu tylko organy Policji nie są limitowane terminem przekazania materiałów zawierających tajemnice, o których mowa w art. 180 § 2 k.p.k.

Projektowane art. 19 ust. 15f — 15i ustawy o Policji nie rozwiązują kwestii dotyczących możliwości wykorzystania materiałów uzyskanych w wyniku kontroli operacyjnej, zawierających okoliczności związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 1 k.p.k. Zasadnym byłoby więc wprowadzenie uregulowań w tym zakresie, celem wyeliminowania wątpliwości mogących występować w praktyce.

Ponadto w projektowanym ust. 15f nie uwzględniono zakazu dowodowego wynikającego z art. 178a kpk (dotyczącego mediatora), który to przepis wszedł w życie w dniu 1 lipca 2015 r., w związku z tym należałoby przepis ten odpowiednio uzupełnić.

Również w przypadku projektowanego ust. 15h nie wskazano jednoznacznie, jakie są przesłanki podejmowania przez sąd decyzji w przedmiocie stwierdzenia dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. oraz, czy na przewidziane w nim rozstrzygnięcie dotyczące zarządzenia zniszczenia materiałów przysługuje zażalenie (przy czym zasadnym byłoby przyznanie prokuratorowi prawa do wniesienia takiego zażalenia, z uwagi na to, iż wykonanie takiego rozstrzygnięcia będzie prowadziło do nieodwracalnej utraty takich materiałów - w celu wyeliminowania wątpliwości w tym zakresie należałoby dodać klauzulę dotyczącą odpowiedniego stosowania uregulowań art. 180 § 2 -5 k.p.k.

Przepis art. 19 ust. 15f pkt 2 w zakresie, w jakim dotyczy przekazania wymienionych materiałów przez Policję należałoby więc uzupełnić o zwrot „niezwłocznie".

Na marginesie należy zauważyć zbędną dychotomię określenia terminów, w jakich poszczególne organy podejmują działania „14 dni" i „niezwłocznie", co z uwagi na ugruntowane orzecznictwo prowadzi, mimo odmienności użytych określeń do tożsamego skutku w określeniu zakładanego w projekcie terminu.

Powyższe uwagi dotyczą również projektowanych zmian analogicznych przepisów w pozostałych ustawach kompetencyjnych.

Analogiczne braki w zakresie wymogu „niezwłoczności" działania organów uprawnionych do stosowania kontroli operacyjnej zawierają przepisy:

- art. 36d ust. lf pkt 2 ustawy o kontroli skarbowej,
- art. 30b ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- art. 27 ust. 15h pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2010 r. Nr 29, poz. 154 ze zm.),
- art. 75da ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej,

- art. 18a ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym.

Art. 1 pkt 2, w którym proponuje się nowe brzmienie art. 20c ustawy o Policji

Zgodnie z projektem Policja „może mieć udostępniane dane" telekomunikacyjne, jak również może je przetwarzać w celu nie tylko - jak dotychczas - zapobiegania lub wykrywania przestępstw, ale także ich rozpoznawania i zwalczania, albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, (art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej oraz art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej).

Wydaje się, że projektodawca nadal bardzo ekstensywnie zamierza określać zakres udostępnienia Policji danych telekomunikacyjnych. W tym kontekście należy więc mieć na uwadze, że ingerencja w konstytucyjne prawo do ochrony prywatności (art. 47 Konstytucji RP) i tajemnicę komunikowania się (art. 49 Konstytucji RP) może mieć miejsce nie tylko w wypadku zapoznawania się organów władzy publicznej z samą treścią komunikatów przekazywanych między jednostkami, ale również w sytuacji pozyskania przez władze informacji towarzyszących temu procesowi. Oznacza to, że udostępnienie Policji danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, stanowi ingerencję w prawo do ochrony prywatności i ochrony tajemnicy komunikowania się. Mimo, że tego rodzaju ingerencję można uzasadnić, z uwagi na potrzebę zapewnienia efektywnego zwalczania przestępczości, to jednak dopuszczalność tego środka uzależniona jest od spełnienia wymagań wynikających z zasady proporcjonalności (art. 31 ust. 3 Konstytucji). Przede wszystkim należy zwrócić uwagę na niedostateczne gwarancje proceduralne, związane z brakiem efektywnej zewnętrznej kontroli udostępniania danych telekomunikacyjnych.

Przepisy ustawowe, upoważniające Policję do pozyskiwania danych telekomunikacyjnych powinny więc zawierać mechanizm niezależnej kontroli, skoro pozyskiwanie tych danych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, o których informacje są przez Policję gromadzone, a zarazem przy

ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Wskazana regulacja może przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka.

Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji.

Art. 1 pkt 3 projektu, w którym proponuje się dodanie art. 20ca - 20cc ustawy o Policji

Projektowane przepisy nie określają przesłanek decyzji podejmowanych przez sąd w przedmiocie stwierdzenia dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. oraz nie wskazują, czy na przewidziane w przepisie rozstrzygnięcie dotyczące zarządzenia zniszczenia materiałów przysługuje zażalenie - odnosi się również do projektowanego art. 20ca ust. 3 (oraz projektowanych zmian analogicznych przepisów w pozostałych ustawach kompetencyjnych).

Zobowiązanie organu Policji (art. 20cc ust. 2) do przedstawiania zbiorczych, uogólnionych informacji o liczbie kontroli danych telekomunikacyjnych lub pocztowych, podstawach prawnych ich uzyskania jak i rodzaju przestępstw, w związku z zaistnieniem których wystąpiono o wskazane dane - nie stanowi rzeczywistej kontroli zasadności występowania o wskazane dane.

Nadto, należy zauważyć, że proponowana w projekcie kontrola ma charakter następczy, dotyczy bowiem udostępnionych danych telekomunikacyjnych i ma być związana ze sporządzanym przez organy Policji sprawozdaniem. Nie przewiduje się natomiast kontroli na etapie przystępowania przez organy Policji, Żandarmerii Wojskowej, wywiadu skarbowego, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego i Centralnego Biura Antykorupcyjnego do pozyskiwania danych telekomunikacyjnych i pocztowych. W szczególności projekt nie przewiduje zgody sądu lub prokuratora na uzyskanie

dostępu do wskazanych danych oraz danych identyfikujących podmiot korzystający z usług pocztowych, o których mowa w art. 20c ust. 1 pkt 2 projektu. Uprawnienia sądu ograniczone zostały w projekcie do kontroli uprzednio zgromadzonych danych telekomunikacyjnych:

III. Uregulowania proponowane w art. 2 projektu obejmujące zmiany ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 roku, poz. 1402)

Art. 2 pkt 1 projektu

W projektowanym art. 9e ust. 1 pkt 4 ustawy o Straży Granicznej zastrzeżenia budzi wybiórcze wskazanie - spośród przestępstw przeciwko mieniu - wyłącznie tych spenalizowanych w art. 278 § 1 kk i art. 291 § 1 kk, co pozwoli na stosowanie kontroli operacyjnej wobec sprawcy kradzieży i każdego pasera - jeżeli przestępstwa te będą pozostawać w związku z przemieszczaniem przedmiotów przestępstwa przez granicę państwową, ale już nie kradzieży z włamaniem (art. 279 § 1 kk) czy rozboju (art. 280 kk).

Art. 2 pkt 2 projektu

Straż Graniczna, zgodnie z projektem ma uzyskać uprawnienie dostępu do danych telekomunikacyjnych także w celu rozpoznawania, zwalczania i utrwalenia dowodów przestępstw. Należy więc zauważyć, że projekt poszerza w art. 10b ust. 1 ustawy o Straży Granicznej zakres dostępu do danych telekomunikacyjnych w przypadku podejmowania czynności związanych z „rozpoznawaniem" przestępstw skarbowych w odniesieniu, do których wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę.

W odróżnieniu jednak od regulacji zawartej w art. 20c projektu ustawy o Policji, art. 1 ust. 2 pkt 4 ustawy o Straży Granicznej definiuje rodzaje przestępstw, których rozpoznawanie oraz wykrywanie i którym zapobieganie, a także ściganie ich sprawców należy do właściwości Straży Granicznej.

Projekt ustawy dotyczący tej służby powiela procedurę kontrolną sądu okręgowego zawartą w art. 20cc projektu, dotyczącą organów Policji - co aktualizuje podniesione wyżej zastrzeżenia dotyczące przyjęcia formy kontroli następczej oraz braku zindywidualizowanej procedury kontroli legalności i zasadności dostępu do danych telekomunikacyjnych.

Zastrzeżenia należy podnieść również do treści art. 10b ust. 5 oraz art. 10ba ust. 1 ustawy o Straży Granicznej, które nie przewidują w stosunku do funkcjonariuszy Straży Granicznej obowiązku „niezwłocznego" przekazania prokuratorowi materiałów mających znaczenie dla postępowania karnego oraz materiałów zawierających dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję. Podobnie jak w przypadku ustawy o Policji niewytłumaczalne jest, z jakich powodów w projekcie zakreśla się termin do procedowania ze wskazanymi materiałami prokuratorowi (art. 10ba ust. 2) i sądowi (art. 10ba ust. 3), a w stosunku do organu Straży Granicznej nie przewiduje się w projekcie takiego wymogu.

Należy wskazać, że proponowane zmiany w ustawie o Straży Granicznej nie gwarantują realnej ochrony życia prywatnego obywateli oraz wolności i ochrony tajemnicy komunikowania się.

IV. Uregulowania zawarte w art. 3 projektu – obejmujące zmiany ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. 2011 r. Nr 41, poz. 214 ze zm.).

Zgodnie z projektem wywiad skarbowy ma uzyskać uprawnienie dostępu do danych telekomunikacyjnych także w celu rozpoznawania, zwalczania i utrwalenia dowodów przestępstw skarbowych.

Jako pozytywną zmianę należy odnotować propozycję ograniczenia katalogu sytuacji uprawniających wywiad skarbowy do pozyskiwania danych telekomunikacyjnych do przypadków dotyczących przestępstw skarbowych, w odniesieniu, do których wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę, określonego na podstawie odrębnych przepisów (art. 36b ust. 1 ustawy o kontroli skarbowej).

Dotychczasowy brak jakichkolwiek ograniczeń w tym zakresie, nawet obejmujących przestępstwa skarbowe o relatywnie niskim ładunku społecznej szkodliwości, nasuwał uzasadnione zastrzeżenia.

V. W zakresie regulacji zawartych w art. 6 projektu, dotyczących nowelizacji ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 i 628 oraz z 2014 r. poz. 1055) pod rozwagę poddaję następujące kwestie:

- *w art 6 pkt 2 projektu ustawy, w którym dodaje się min. art. 30b ust. 1* - w brzmieniu projektowanego przepisu odwołano się do nieistniejącej w tym przepisie jednostki redakcyjnej „art. 30b ust. 5";

- *art. 6 pkt 3 lit a projektu, w którym nadaje się nowe brzmienie art. 31 ust. 1 w pkt 4* w katalogu wymienionych przestępstw należałoby wskazać również art. 263 § 1 i 2 k.k. (nielegalne posiadanie, wyrabianie i handel bronią), które to przestępstwo aktualnie stanowi podstawę stosowania przez Żandarmerię Wojskową kontroli operacyjnej i określone jest w aktualnym brzmieniu nowelizowanej ustawy w art. 31 ust. 1 pkt 12;

- *art. 6 pkt 3 lit a - zmieniający art. 31 ust. 1 ustawy* - w projektowanym art. 31 ust. 1 poszerzono katalog przestępstw, w odniesieniu do których można stosować kontrolę operacyjną np. art. 286 § 1 kk, art. 299 § 1 - 6, art. 305, art. 310 § 1, 2, i 4, nie wskazując w uzasadnieniu argumentów dla takiej regulacji;

- *art 6 pkt 3 lit. e* – wątpliwości budzi odrębna procedura uzyskiwania zgody sądu na wykorzystanie w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. Podnoszone wątpliwości (sformułowane przez Naczelną Prokuraturę Wojskową) dotyczą sposobu uzyskiwania zgody sądu. Wątpliwości nie budzi samo występowanie prokuratora do sądu z wnioskiem o wyrażenie zgody na wykorzystanie w postępowaniu karnym omawianych materiałów,

jeżeli nie będzie wymagana tzw. „zgoda następcza" sądu, określona w art. 31 ust. 16c ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, jednakże w przypadku konieczności wystąpienia do sądu z wnioskiem wskazanym w art. 31 ust. 16c ustawy Żandarmerii Wojskowej i wojskowych organach porządkowych (w terminie 2 miesięcy od zakończenia kontroli), dodatkowe wcześniejsze (niezwłoczne) przekazywanie materiałów i sporządzanie wniosku do sądu, wydaje się zbędne. Powodować to będzie konieczność dodatkowego selekcjonowania materiałów, sporządzania wniosków i przekazywania ich do sądu. Wydaje się, że wyłączenie i podzielenie materiałów może utrudniać sądowi podjęcie decyzji, bowiem sąd zostanie pozbawiony możliwości kompleksowego zapoznania się z całością materiałów, z uwagi na odrębnie wysłany wniosek w oparciu o regulacją proponowaną w art. 6 pkt 3 lit. e projektu - dodawane w art. 31 ust. 16f-16i.

VI. Uwagi przedstawione wyżej odnoszą się również do analogicznych procedur proponowanych **w art. 9 projektu – w zakresie ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.**

Zasadnym wydaje się jest rozważenie rozszerzenia katalogu przestępstw, do których rozpoznawania, zapobiegania i zwalczania uprawniona jest ta służba.

Służba Kontrwywiadu Wojskowego, jako służba specjalna, właściwa jest, zgodnie z treścią art. 1 wskazanej ustawy w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej, także w sprawach ochrony przed zagrożeniami ekonomicznymi, którą realizuje Zarząd Ochrony Ekonomicznych Interesów Sił Zbrojnych SKW.

Aby zadania postawione przed tą służbą mogły być realizowane w sposób pełny i właściwy realizowane, niezbędne wydaje się uzupełnienie katalogu przestępstw wskazanych w art. 5 ust. 1 lit. d ustawy określonych w art. 228-230 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, poprzez wskazanie również przestępstw z art. 231 § 2 k.k. i art. 305 k.k., jeżeli mogą one zagrażać bezpieczeństwu, zdolności bojowej SZ

RP lub innych jednostek organizacyjnych MON. Pozwoli to na skuteczniejsze i efektywniejsze realizowanie czynności operacyjno-rozpoznawczych, wymienionych w art. 31 ustawy. Wobec obowiązku realizacji stawianych przed wymienioną służbą zadań związanych z monitorowaniem zamówień publicznych, brak możliwości kontroli operacyjnej łączącej się z powyższymi przestępstwami, zdecydowanie utrudnia, a często uniemożliwia właściwe zabezpieczenie, istotnych z punktu widzenia bezpieczeństwa i obronności, zamówień publicznych realizowanych przez Ministerstwo Obrony Narodowej.

VII. Uregulowania proponowane w art. 7 projektu - obejmujące zmiany w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.)

W projekcie proponuje się między innymi zmianę zakresu zadań Agencji Bezpieczeństwa Wewnętrznego poszerzając zakres właściwości rzeczowej tej służby.

W wątpliwość należy podać wprowadzenie w projekcie kompetencji tej służby do ścigania przestępstwa z art. 266 § 2 k.k, polegającego na ujawnieniu osobie nieuprawnionej informacji niejawnej o klauzuli „zastrzeżone" lub „poufne", zagrożonego przez ustawę karną karą pozbawienia wolności do lat 3. Założeniem ustawowym winno być powierzanie wyodrębnionej służbie postępowań o zdecydowanie większej wadze. Określając w art. 5 ust. 1, pkt 2 lit. a katalog przestępstw, których rozpoznawanie, zapobieganie im, wykrywanie oraz ustalanie i ściganie ich sprawców pozostaje we właściwości Agencji Bezpieczeństwa Wewnętrznego ustawodawca nadal posługuje się niedookreślonym pojęciem: „jeżeli ich popełnienie zagraża bezpieczeństwu państwa". Pojęcie: „przestępstwo zagrażające bezpieczeństwu państwa" nie nawiązuje ani do potocznych, ani do ustawowych nazw poszczególnych typów przestępstw, nie wykazuje również związku z systematyką przestępstw przyjętą w Kodeksie karnym.

Podobne sformułowanie „przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej" - występuje jedynie w art. 112 pkt 1 k.k. przy określeniu podstaw do stosowania Kodeksu karnego. Przepis ten

wymaga jednak dopełnienia przepisami, w których określone są znamiona poszczególnych czynów zabronionych, gdyż art. 112 pkt 1 k.k. samodzielnie nie konstytuuje typu przestępstwa.

VIII. Pozwalam sobie zwrócić również uwagę na błąd zawarty w treści art. 18a ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym (**art. 10 pkt 3 projektu ustawy**) nakazujący wystąpić do Sądu Okręgowego w Warszawie z wnioskiem o wykorzystanie w postępowaniu karnym materiałów zawierających dane dotyczące osoby wykonującej zawód lub funkcje, o których mowa w art. 180 § 2 k.p.k. nie Prokuratorowi Generalnemu, lecz prokuratorowi wojskowemu. W związku z tym wyrazy „prokurator wojskowy" należy zastąpić wyrazami „Prokurator Generalny", gdyż to właśnie Prokurator Generalny ma podejmować określone w tym przepisie czynności.

IX. W odniesieniu do zawartego w **art. 13 ust. 2 projektu przepisu intertemporalnego**, który stanowi, że „po zakończeniu kontroli operacyjnej, o której mowa w art. 12 ust. 2, wskutek upływu terminu może zostać jednokrotnie zarządzona kontrola operacyjna na podstawie art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji, art. 9e ust. 10 ustawy z dnia 12 października 1990 r. o Straży Granicznej, art. 36c ust. 7 ustawy z dnia 28 września 1991 r. o kontroli skarbowej i art. 31 ust. 10 ustawy z dnia z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, w brzmieniu nadanym niniejszą ustawą.". Wskazany przepis budzi wątpliwości bowiem zezwala na powtórzenie przeprowadzenia kontroli operacyjnej, mimo, że kontrola operacyjna została już raz przeprowadzona na podstawie dotychczas obowiązujących przepisów.

Reasumując powyższe, wyrażam pogląd, że analiza rozwiązań proponowanych *w senackim projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki 967)* nasuwa uwagi i wątpliwości, które uniemożliwiają pozytywne zaopiniowanie tego projektu, który wbrew deklaracji zawartej w uzasadnieniu, nie realizuje w pełni celu w postaci dostosowania systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K. 23/11, a zawarte w nim regulacje

nierzadko kolidują z pozostałym, wskazanym w niniejszej opinii, orzecznictwem Trybunału Konstytucyjnego, Europejskiego Trybunału Praw Człowieka, jak również Trybunału Sprawiedliwości Unii Europejskiej. Wydaje się, że w projektowanych przepisach brak jest efektywnej regulacji gwarancyjnej, mogącej chronić jednostkę przed ewentualną, potencjalną dowolnością lub arbitralnością decyzji podejmowanych przez służby w zakresie wkraczania w konstytucyjne i konwencyjne prawa i wolności jednostki, co w kontekście orzecznictwa Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka należy uznać za niedopuszczalne.

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
Marek Jamrogowicz

MINISTER
SPRAWIEDLIWOŚCI

DL III 023-46/15/6

Warszawa, dnia 17 lipca 2015 r.

Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej
Senatu RP

Szanowny Panie Przewodniczący

W odpowiedzi na pismo z dnia 26 czerwca 2015r. (BPS/KU-034/967/1/15), w sprawie opinii dotyczącej senackiego projektu ustawy o zmianie ustawy – o Policji oraz niektórych innych ustaw (druk senacki nr 967), uprzejmie przestawiam następujące stanowisko.

Inicjatywa senacka wyrażająca się w w/w projekcie stanowi realizację wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014r. (sygn. akt K/23/11) dot. czynności operacyjno-rozpoznawczych i retencji danych telekomunikacyjnych, którym to Trybunał Konstytucyjny orzekł m.in., iż:

a) art. 20c ust. 1 ustawy o Policji,
b) art. 10b ust. 1 ustawy o Straży Granicznej,
c) art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej,
d) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
e) art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

f) art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

g) art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym,

h) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 oraz z 2014 r. poz. 486)

– przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243), są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

Za niekonstytucyjne, Trybunał uznał również te przepisy odpowiednich ustaw regulujących organizację poszczególnych służb, które 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, jak również tych danych, które nie mają znaczenia dla prowadzonego postępowania.

Z aprobatą należy stwierdzić, że podjęte przez Senat RP prace legislacyjne stanowią realizację w/w wyroku Trybunału Konstytucyjnego. Kierunkowo projekt ustawy przewiduje kontrolę sądów szczebla okręgowego nad udostępnianiem danych telekomunikacyjnych oraz zobowiązanie Ministra Sprawiedliwości do corocznego przedstawiania Sejmowi i Senatowi zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych.

Przy ocenie proponowanych rozwiązań, trzeba jednak zwrócić uwagę, że Trybunał Konstytucyjny nie przesądził ostatecznego kształtu rozwiązań, w szczególności zaś nie wskazał, że konieczne jest pozyskiwanie uprzedniej zgody dla pozyskania danych telekomunikacyjnych przez w/w służby, niezbędnych z perspektywy zapobiegania i wykrywania przestępstw. Co za tym idzie, jak się wydaje, dopuszczalne jest przez Trybunał uzyskanie zgody *ex post* lub też kontrola *ex post* zasadności pozyskania takich danych. Trybunał również nie przesądził

o tym, że wyłącznymi organami, które mogłyby sprawować kontrolę nad tego rodzaju działaniami w/ w służb powinny być sądy, choć *prima vista* rozwiązanie takie jawi się jako optymalne. *Trybunał Konstytucyjny nie wymaga jednocześnie – przychylając się do argumentacji wnioskodawców i pozostałych uczestników postępowania – by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to należałoby uznać za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także ETPC i TSUE (uzasadnienie wyroku).*

Nie można jednak stracić z pola widzenia, biorąc pod uwagę znaczną liczbę wystąpień o dane telekomunikacyjne (czego nie pomija nawet Trybunał Konstytucyjny w swoim wyroku), że byłoby to kolejne, znaczne rozszerzenie kognicji sądów, zwłaszcza na poziomie szczebla okręgowego i mogłoby doprowadzić do istotnej przewlekłości postępowań prowadzonych przed tymi sądami.

Należy zatem rozważyć, jaki inny organ spełniałby wymagania Trybunału Konstytucyjnego w obszarze niezależności od Rady Ministrów i jak się wydaje, rolę taką mogliby sprawować prokuratorzy, niezależni oraz niepozostający z funkcjonariuszami innych służb w relacji służbowej zwierzchności.

Wydaje się również, że tego rodzaju rozwiązanie korelowałoby z dotychczasowymi rozwiązaniami, wynikającymi np. z art. 20c ust. 6 ustawy o Policji, wskazującego, że materiały uzyskane w wyniku czynności pozyskania danych telekomunikacyjnych, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi. Rozwiązanie to wskazuje także na ścisłe związki podejmowanych przez służby działań na tym etapie, z następną fazą postępowania, jakim może być rozpoczęcie postępowania karnego. Wydaje się również, że przyjęcie tego rodzaju rozwiązania korelowałoby z kolejnym założeniem, że to Prokurator Generalny

byłby zobowiązany do przedstawiania zbiorczej informacji w sprawie pozyskiwanych danych telekomunikacyjnych. Wszak nie bez znaczenia pozostaje fakt, że już dziś Prokurator Generalny posiada stosowne obowiązki informacyjne w związku z kontrolą operacyjną, bowiem na mocy art. 10e ustawy 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 organ Policji.

W zakresie dotyczącym propozycji wprowadzenia, w przepisach regulujących organizację i zakres działań poszczególnych służb, sposobu postępowania w przypadku zarejestrowania danych stanowiących tajemnicę chronioną na podstawie art. 178 k.p.k. lub art. 180 par. 2 k.p.k. niewątpliwie pominięto, ochronę tajemnicy mediatora z art. 178a k.p.k. Należy również zastanowić się, czy w procesie podejmowania decyzji o niezwłocznym, komisyjnym i protokolarnym zniszczeniu materiałów, co do których zachodzi przypuszczenie, że zawierają one informacje, o których mowa w art. 178 i 178a k.p.k. nie powinno się uwzględniać prokuratora, który wydawał zgodę na podjęcie kontroli operacyjnej. W proponowanym brzmieniu przepisu art. 19 ust. 15f. pkt. 1 ustawy o Policji, byłaby to de facto decyzja arbitralna Komendanta Głównego Policji, Komendanta CBŚP albo komendanta wojewódzkiego Policji.

Z poważaniem
z upoważnienia
MINISTRA SPRAWIEDLIWOŚCI
dr hab. Monika Zbrojewska
PODSEKRETARZ STANU

Warszawa, dnia 17 lipca 2015 r.

RZECZPOSPOLITA POLSKA
MINISTER FINANSÓW

WS10.S0330.20.2015.10001.1

Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej
Senatu Rzeczypospolitej Polskiej

Szanowny Pani Przewodniczący,

W nawiązaniu do pisma z 26 czerwca 2015 r., nr BPS/KU-034/967/13/15, w sprawie sporządzenia opinii w przedmiocie rozwiązań zaproponowanych w projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967) uprzejmie informuję, co następuje.

Przede wszystkim pragnę zwrócić uwagę na fakt, że wprowadzona w przedmiotowym projekcie zmiana w ustawie z dnia 28 września 1991 r. o kontroli skarbowej, w odniesieniu do art. 36d ust. 1 pkt 1 (art. 3 pkt 4 lit. a projektu), poprzez jego wykreślenie i dokonanie zmian we wszystkich innych przepisach tej ustawy powiązanych z ww. artykułem, nie znajduje uzasadnienia. Celem projektowanej ustawy jest bowiem dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. sygn. akt K 23/11, który w żadnym zakresie nie odnosi się do wskazanego wyżej przepisu ustawy o kontroli skarbowej, niezwykle ważnego z punktu widzenia działań kontroli skarbowej. Działania te są ukierunkowane na zwalczenie oszustw podatkowych przynoszących ogromne straty dla budżetu państwa, zwłaszcza w zakresie wyłudzeń nienależnego zwrotu podatku VAT (karuzele podatkowe). Postępowania kontrolne, na rzecz których wywiad skarbowy prowadzi czynności, są skuteczne dzięki wskazanemu wyżej przepisowi art. 36d ust. 1 pkt 1 ustawy o kontroli skarbowej, zgodnie z którym materiały uzyskane w czasie prowadzenia czynności wywiadu skarbowego, w tym materiały zgromadzone podczas stosowania kontroli operacyjnej lub niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, które zawierają informacje mające znaczenie dla postępowania kontrolnego, są przekazywane właściwemu miejscowo organowi kontroli skarbowej, w razie potrzeby z wnioskiem o wszczęcie postępowania kontrolnego. Treść powyższego przepisu została wprowadzona do ustawy o kontroli skarbowej z dniem 1 stycznia 1998 roku. Początkowo, w świetle przepisów ustawy o kontroli skarbowej, informacje uzyskiwane przez wywiad skarbowy w drodze czynności operacyjno-rozpoznawczych mogłyby być wykorzystywane wyłącznie przez organy kontroli skarbowej dla celów postępowania kontrolnego. Wywiad skarbowy został bowiem powołany przede wszystkim na potrzeby kontroli skarbowej, której celem jest, zgodnie z art. 1 ust. 1 ustawy o kontroli skarbowej, ochrona interesów i praw majątkowych Skarbu Państwa oraz zapewnienie skuteczności wykonywania zobowiązań podatkowych i innych należności stanowiących dochód budżetu państwa lub państwowych funduszy celowych. Wywiad skarbowy, jako szczególna forma kontroli skarbowej, realizuje ustawowe zadania głównie na potrzeby prowadzonych postępowań kontrolnych. Realizacja tych postępowań opiera się na zasadach określonych w ordynacji podatkowej i kodeksie postępowania administracyjnego, dlatego materiały i informacje uzyskane w czasie

prowadzenia czynności wywiadu skarbowego, przekazywane organowi kontroli skarbowej mają istotne znaczenie dla udowodnienia popełnienia przestępstwa osobom za nie odpowiedzialnym, co często nie jest możliwe przy wykorzystaniu tylko i wyłącznie czynności administracyjnych.
Taki tryb postępowania ma niezwykle istotne znaczenie, szczególnie w sprawach dotyczących tzw. oszustw karuzelowych, oszustw związanych z wyprowadzeniem spod opodatkowania towarów i usług, unikania opodatkowania z wykorzystaniem dostaw i nabyć wewnątrzwspólnotowych oraz odpraw celnych towarów importowanych w procedurze 42xx. W takich przypadkach zgromadzony w trakcie czynności wywiadu skarbowego materiał dowodowy przekazany do postępowania kontrolnego ma podstawowe znaczenie dla udowodnienia świadomości sprawców przestępstw skarbowych i osób, które udzielają im pomocy, a przez to ich eliminacji z obrotu gospodarczego.
Wynika to z faktu, że postępowanie kontrolne oraz postępowanie w sprawie o przestępstwo skarbowe są ze sobą nierozerwalnie związane. Dotyczą tego samego czynu (mamy do czynienia z tożsamością stanu faktycznego i dowodowego) i toczą się równolegle. Ponadto od decyzji wydanej w postępowaniu kontrolnym zależy również ustalenie wysokości należności podatkowej w postępowaniu w sprawie o przestępstwo karne skarbowe.
Formuła kontroli skarbowej, typowej jeszcze kilka lat temu, opartej na administracyjnym trybie działania nie sprawdza się w dzisiejszych warunkach. W zwalczaniu zorganizowanej przestępczości gospodarczej, powodującej straty budżetu państwa na wielką skalę to metody operacyjne są najbardziej skuteczne.

Dowodem, że wykorzystanie materiałów i informacji z czynności wywiadu skarbowego przez kontrolę skarbową przynosi wymierny rezultat ekonomiczny są zamieszczone poniżej coroczne statystyki efektów działań wywiadu skarbowego i kontroli skarbowej.

I. Ilość postępowań kontrolnych

Następuje systematyczny wzrost udziału postępowań kontrolnych wszczynanych na wniosek wywiadu skarbowego (a więc z wykorzystaniem czynności wywiadu skarbowego) w stosunku do ogólnej liczby wszczynanych postępowań.
2010 r. - 9,6% postępowań kontrolnych wszczynanych na wniosek wywiadu skarbowego
2012 r. - 15,8% postępowań kontrolnych wszczynanych na wniosek wywiadu skarbowego
2014 r. - 16,3 % postępowań kontrolnych wszczynanych na wniosek wywiadu skarbowego

II. Ustalenia podatkowe

Następuje systematyczny wzrost ustaleń podatkowych z postępowań kontrolnych prowadzonych na wniosek wywiadu skarbowego:
2010 r. - ok. 1 mld zł ustaleń podatkowych z kontroli na wniosek wywiadu skarbowego tj. 47% ustaleń kontroli skarbowej ogółem.
2012 r. - 2,46 mld zł ustaleń podatkowych z kontroli na wniosek wywiadu skarbowego tj. 41% ustaleń kontroli skarbowej ogółem.
2014 r. - 5,9 mld zł ustaleń podatkowych z kontroli na wniosek wywiadu skarbowego tj. 50% ustaleń kontroli skarbowej ogółem.

III. Skuteczność kontroli – średnie ustalenia podatkowe przypadające na 1 postępowanie kontrolne przeprowadzone na wniosek wywiadu skarbowego wyniosły w 2014 r. ok. 4,4 mln zł, podczas gdy ta sama wartość na 1 postępowanie kontrolne przeprowadzone na wniosek innych komórek kontroli

skarbowej i instytucji zewnętrznych (tryb wyłącznie administracyjny) wyniosła 1,2 mln zł.

W 2010 r. proporcje te to: 1 mln (WS) do 1,2 mln zł (KS), a w 2012 r. 1,9 mln (WS) do 2,3 mln zł (WS).

Zdaniem Ministerstwa Finansów wykreślenie art. 36d ust. 1 pkt 1 z ustawy o kontroli skarbowej uniemożliwi kontroli skarbowej skuteczną realizację ustawowych zadań oraz będzie miało szkodliwy wpływ na ochronę interesów ekonomicznych Skarbu Państwa.

W związku z powyższym proponuję rezygnację z uchylenia art. 36d ust. 1 pkt 1 oraz nadania nowego brzmienia ust. 1a w tym artykule. W konsekwencji powyższego konieczne jest wprowadzenie zmian w pozostałych przepisach projektowanej ustawy dotyczących ustawy o kontroli skarbowej, po uprzednim zmodyfikowaniu zaproponowanego w projekcie ustawy nowego brzmienia art. 36b ust. 1 ustawy o kontroli skarbowej (art. 3 pkt 1 lit. a projektu) uprawniającego wywiad skarbowy do pozyskiwania danych telekomunikacyjnych i pocztowych, o przestępstwa przeciwko mieniu, w stosunku do których wywiad skarbowy posiada również, zgodnie z art. 36c ust. 1 pkt 4 ustawy o kontroli skarbowej, uprawnienia do stosowania kontroli operacyjnej. Ponadto powyższe uzasadnia fakt, że coraz częściej jak wynika z orzecznictwa sądów, podmioty uczestniczące w karuzelach VAT-owskich, których celem jest niezapłacenie podatku VAT, a następnie wyłudzenie z budżetu Państwa jego nienależnego zwrotu, nie popełniają przestępstw skarbowych ze względu na fikcyjny obrót gospodarczy, ale przestępstwa karne przeciwko mieniu, w szczególności przestępstwo określone w art. 286 kk.

Poniżej przedstawiam szczegółowe uwagi do projektowanej ustawy w części dotyczącej zmian wprowadzanych w ustawie o kontroli skarbowej:

1) **Do art. 3 pkt 1 lit. a dot. art. 36b ust. 1**

Wprowadzenie do wyliczenia w tym przepisie powinno brzmieć:

„W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw:

- skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
- przeciwko mieniu, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
- przestępstw, o których mowa w art. 2 ust. 1 pkt 14b

wywiad skarbowy, może mieć udostępniane dane:" i pozostałą treść przepisu pozostawić bez zmian.

2) **Do art. 3 pkt 2 dodającego art. 36ba-36bd**

a) w odniesieniu do art. 36ba:

- ust. 1 tego artykułu powinien brzmieć:
  „Materiały uzyskane w wyniku czynności związanych z udostępnianiem danych, o których mowa w art. 36b ust.1, które:

1) zawierają dowody pozwalające na wszczęcie albo mające znaczenie dla postępowania w sprawie o przestępstwo lub przestępstwo skarbowe, o których mowa w art. 36b ust. 1, Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu,
2) zawierają informacje mające znaczenie dla postępowania kontrolnego, są przekazywane właściwemu miejscowo organowi kontroli skarbowej, w razie potrzeby z wnioskiem o wszczęcie postępowania kontrolnego."

- ust. 2 tego artykułu powinien brzmieć: „Materiały uzyskane w wyniku czynności związanych z udostępnianiem danych, o których mowa w art. 36b ust. 1, które nie zawierają informacji mających znaczenie dla postępowania w sprawie o przestępstwo lub przestępstwo skarbowe, o których mowa w art. 36b ust. 1 lub dla postępowania kontrolnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Art. 36d ust. 4 pkt 2 stosuje się odpowiednio.";

b) w odniesieniu do art. 36bb:
   - w ust. 1 po zwrocie „zawierają dowody pozwalające na wszczęcie albo mające znaczenie dla postępowania w sprawie o przestępstwo lub przestępstwo skarbowe wymienione w art. 36b ust. 1" dodać słowa „lub zawierają informacje mające znaczenie dla postępowania kontrolnego" i pozostałą treść przepisu pozostawić bez zmian;
   - w ust. 2 w miejsce kropki wstawić zwrot „lub w postępowaniu kontrolnym" i następnie postawić kropkę;
   - z treści ust. 3 wynika jedynie, że Sąd Okręgowy zarządza komisyjne i protokolarne zniszczenie. Przepis milczy w zakresie zlecenia wykonania tego zarządzenia Generalnego Inspektora Kontroli Skarbowej, a w ust. 4 mowa jest o tym, że Generalny Inspektor Kontroli Skarbowej jest zobowiązany do niezwłocznego poinformowania Sądu o jego wykonaniu. Przepis wymaga doprecyzowania;
c) w odniesieniu do art. 36bc ust. 1 w miejsce kropki wstawić zwrot „lub w postępowaniu kontrolnym" i następnie postawić kropkę;
d) w odniesieniu do art. 36bd ust. 2 pkt 3 po zwrocie „rodzaje przestępstw" należy wstawić słowa „lub przestępstw skarbowych" i dalszą treść tego przepisu pozostawić bez zmian.

3) **Do art. 3 pkt 3 lit. b dot. art. 36c ust. 4**
Wydaje się niepotrzebne zmienianie tego przepisu, gdyż po pierwsze Trybunał Konstytucyjny nie orzekł jego niekonstytucyjności, zaś po drugie, wbrew intencjom projektodawcy, jego brzmienie budzi jednak wątpliwości interpretacyjne. Nie jest jasne jaki jest zakres pojęciowy zwrotu „kontrola treści korespondencji". Czy jest to korespondencja tradycyjna/papierowa, jak i elektroniczna i czy mieszczą się w tym pojęciu sms-y, mms-y, poczta mailowa?

4) **Do art. 3 pkt 3 lit. f dodającego w art. 36c ust. 14a-14c**
Przepis ust. 14b nakazuje zniszczenie dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej niezwłocznie po ich przekazaniu w trybie art. 36d ust. 1 pkt 2 ustawy o kontroli skarbowej. Natomiast art. 36d ust. 1 pkt 2 ww. ustawy stanowi, że materiały zgromadzone w toku czynności wywiadu skarbowego, w tym m.in. w toku kontroli operacyjnej w przypadku gdy zwierają dowody pozwalające na wszczęcie albo mają znaczenie dla

postępowania w sprawie o przestępstwo lub przestępstwo skarbowe Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu.

5) **Do art. 3 pkt 4 lit. a dot. art. 36d ust. 1 pkt 1**
Proponuje się wykreślić tę zmianę. Szczegółowe uzasadnienie dla tej uwagi znajduje się w początkowej części pisma.

6) **Do art. 3 pkt 4 lit. b dot. art. 36d ust. 1a**
Proponuje się wykreślić tę zmianę. Szczegółowe uzasadnienie dla tej uwagi znajduje się również w początkowej części niniejszego pisma.

7) **Do art. 3 pkt 4 lit. c dodającego w art. 36d ust. 1f-1h**
Proponuje się w projektowanym ust. 1g pkt 1 po zwrocie „w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe" dodać wyrazy „lub w postępowaniu kontrolnym" i pozostałą treść przepisu postawić bez zmian. Podobnie w nowo projektowanym ust. 1h po słowach „Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe" dodać zwrot „lub w postępowaniu kontrolnym" i pozostałą treść przepisu postawić bez zmian.

8) **Do art. 3 pkt 4 lit. d dot. art. 36d ust. 3**
W treści tego przepisu proponuje się dodać po słowach „niezawierające dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe" zwrot „lub niemające znaczenia dla postępowania kontrolnego", który to zwrot znajduje się w obecnym brzmieniu tego przepisu (zmienianym tylko ze względu na to, że niszczenie danych telekomunikacyjnych i pocztowych zarządzał będzie Generalny Inspektor Kontroli Skarbowej, a nie kierownik komórki organizacyjnej urzędu obsługującego ministra właściwego do spraw finansów publicznych właściwego w sprawach w sprawach wywiadu skarbowego) i pozostałą treść przepisu postawić bez zmian.

Poniżej przedstawiam uwagi dotyczące przedmiotowego projektu w zakresie zmian wprowadzanych w ustawie o Służbie Celnej.

1) **Do art. 11 pkt 1 lit. c dot. art. 75d ust. 5**
   a) Przepis w tym brzmieniu może być interpretowany podobnie, jak to uczynił RPO we wniosku o stwierdzenie niezgodności z Konstytucją ust. 5 art. 75d, tzn. w oderwaniu od ust. 1 art. 75d, wskazując, że poprzez brzmienie ust. 5 (który zakres normowania ma szerszy niż ust. 1: *Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.*) można rozszerzająco interpretować ust. 1 art. 75d, skutkiem czego, Służbie Celnej, wg RPO, mogły być udostępniane dane inne niż tylko dotyczące działań przestępczych przeciwko organizacji gier hazardowych, określone w rozdziale 9 kks. A zatem *ustawowy cel gromadzenia danych telekomunikacyjnych jest węższy niż cel ich przechowywania i ewentualnie dalszego wykorzystania.*

Wprawdzie Trybunał Konstytucyjny zwrócił uwagę, że *poprawnie dokonywana – w perspektywie konstytucyjnej – wykładnia systemowa art. 75d ust. 5 ustawy o SC nie daje podstaw do nadania mu aż tak szerokiej treści, jak czyni to wnioskodawca. Przepis regulujący przesłanki gromadzenia danych (ust. 5) zawarty jest bowiem w tej samej jednostce redakcyjnej ustawy co przepis regulujący cel ich zbierania (ust. 1). Obydwa te przepisy powinny były być zatem interpretowane łącznie. Wówczas rozumienie zakwestionowanego przepisu ograniczone będzie wyłącznie do przestępstw skarbowych i wykroczeń skarbowych określonych w rozdziale 9 k.k.s., do którego to odsyła art. 75d ust. 1 ustawy o SC. Trybunał przyjmuje jednak, że konstytucyjny organ państwa, jakim jest Rzecznik Praw Obywatelskich, dokonał analizy stosowania zaskarżonego przepisu. Trybunał przyjmuje zatem, że przepis ten jest rozumiany przez właściwe organy państwa tak, jak to wskazał Rzecznik i w konsekwencji Trybunał stwierdził, że art. 75d ust. 5 ustawy o SC w zakresie, w jakim zezwala na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 k.k.s., jest niezgodny z art. 51 ust. 4 Konstytucji.*

Mając na uwadze sposób interpretacji przepisów przez RPO i wniosek do TK o stwierdzenie niekonstytucyjności przepisu, proponuje się rozważenie zmiany ust. 5 art. 75d poprzez dodanie wyrażenia ***W przypadku gdy*** przed wyrazem ***Materiały*** oraz odpowiednie przeredagowanie przepisu.

b) Proponuje się wskazać termin, w jakim materiały te należy przekazać do prokuratora (np. niezwłocznie).

c) Proponuje się dokonać zmiany w zakresie właściwości prokuratora, któremu należy przekazać materiały, w taki sposób, jaki został wskazany w ustawie o Policji (art. 20c ust. 5), czy ustawie o Straży Granicznej (art. 10b ust. 5), tj. poprzez zastąpienie wyrażenia *ze względu na siedzibę organu przekazującego* na wyrażenie *miejscowo lub rzeczowo.*

d) Niezależnie od powyższego należy wskazać, że proponowany przepis nakazuje przekazywać wszelkie uzyskane od operatorów materiały zawierające informacje mające znaczenie dla postępowania karnego lub postępowania karnego skarbowego, prokuratorowi. Z zakresu ust. 1 art. 75d wynika, że Służba Celna gromadzi dane dla postępowania karnego skarbowego, o których mowa w rozdziale 9, z wyłączeniem art. 108 § 2, Kodeksu karnego skarbowego. Z art. 75d ust. 5 wynika, że przekazuje do prokuratora materiały z zakresu postępowania karnego i postępowania karnego skarbowego.

Cel tego przepisu jest niezrozumiały. Biorąc pod uwagę to, że urząd celny prowadzi samodzielnie postępowanie przygotowawcze w sprawach o przestępstwa skarbowe i wykroczenia skarbowe określone w art. 107-111 § 1 kodeksu karnego skarbowego, nie jest zrozumiałe przekazywanie materiałów w tym zakresie do prokuratora. W zależności więc od celu przepisu należałoby mu nadać odpowiednią treść oraz w dalszej kolejności ustalić zadania prokuratora, co do danych otrzymanych od Służby Celnej. Ponieważ, jak wyżej wskazano Służba Celna, zgodnie z art. 75d ust. 1, może gromadzić i przetwarzać dane do celów postępowania karnego skarbowego w zakresie rozdziału 9 kks, to nie ma uzasadnienia do przekazywania ich do prokuratora, ponieważ uzyskując te dane jednocześnie zostawałaby ich pozbawiona. Jeśli celem tego przepisu jest przekazywanie do prokuratora jedynie tych danych, które mają znaczenie dla

postępowania karnego, to należałoby przepis ten zawęzić, tylko do tych danych. Wówczas do prokuratora przekazywane byłyby dane mające znaczenie dla postępowania karnego. A zatem z zakresu ust. 5 należy wyłączyć te dane, które Służba Celna przetwarza zgodnie z ust. 1.

Biorąc pod uwagę systemowe podejście do projektu ustawy należy zauważyć, że dane zgromadzone przez Policję czy Straż Graniczną w zakresie postępowań karnych również są przekazywane do prokuratora. Z uwagi na to, że organy tych formacji również mogą samodzielnie prowadzić postępowania przygotowawcze, nie jest co do zasady zrozumiały sens tego przepisu.

Na marginesie należy zaznaczyć, że wątpliwości legislacyjne budzi zastąpienie dotychczasowej normy ust. 5 zupełnie inną treścią i przeniesienie dotychczasowej normy ust. 5 do ust. 10.

Mając powyższe na uwadze proponuje się następujące brzmienie całego art. 75d ust. 5:

5. W przypadku gdy, w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych, zostały uzyskane materiały, które zawierają informacje mające znaczenie dla postępowania karnego lub postępowania karnego skarbowego innego niż w sprawie przestępstw określonych w ust. 1, Szef Służby Celnej albo dyrektor izby celnej przekazuje te materiały niezwłocznie prokuratorowi właściwemu miejscowo lub rzeczowo.

2) **Do art. 11 pkt 1 lit. c (powinno być d) dot. art. 75d ust. 6**

Uwagi analogiczne do uwag zgłoszonych do proponowanego ust. 5 art. 75d w zakresie konstrukcji tego przepisu (pkt 2 lit. a niniejszego pisma).

Mając powyższe na uwadze proponuje się następujące brzmienie całego art. 75d ust. 6:

6. W przypadku gdy w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych, zostały uzyskane materiały, które nie zawierają informacji mających znaczenie dla postępowania karnego lub postępowania karnego skarbowego, materiały te podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

3) **Do art. 11 pkt 2 dot. art. 75da ust. 1**

W przepisie należy doprecyzować, jakiemu prokuratorowi należy przekazać te materiały. Proponuje się uzupełnić przepis poprzez wskazanie, że chodzi tu o **prokuratora okręgowego właściwego miejscowo**.

4) **Do art. 11 pkt 2 dot. art. 75db ust. 1**

Uwaga systemowa. W projektach ustaw o Policji (art. 20cb ust. 1) i Straży Granicznej (art. 10bb ust. 1) taki sam przepis rozpoczyna się słowami *Jeżeli z materiałów sprawy wynika, że* ... Mając na uwadze fakt, że przepisy tych ustaw i ustawy o Służbie Celnej są tożsame co do zakresu normowania w nich zawartego, zasadnym wydaje się, aby brzmiały one jednakowo.

5) **Do art. 11 pkt 2 dot. art. 75db ust. 6**

Uwaga systemowa. W przepisie występuje sformułowanie *danych osób, o których mowa*.... W takim samym przepisie projektu ustawy o Policji brak jest słowa *osób*. Wydaje się, że sformułowanie to w większym stopniu koresponduje z treścią ust. 1, do którego odwołuje się ust. 5. W związku z powyższym proponuje się usunięcie z przepisu wyrazu *osób*.

6) **Do art. 11 pkt 2 dot. art. 75db ust. 6**
Uwaga literowa. W wyrazie *znaczenia* literę *a* zastąpić literą *e - znaczenie.*

7) **Do art. 11 pkt 2 dot. art. 75db ust. 7**
a) Uwaga interpunkcyjna: po wyrazie *Celnej* proponuje się postawić przecinek;
b) Proponuje się doprecyzować, jaki sąd okręgowy należy poinformować o zniszczeniu danych. Proponuje się, aby był to sąd, o którym mowa w ust. 1.

Mając powyższe na uwadze proponuje się następujące brzmienie całego art. 75db ust. 7:

O zarządzeniu zniszczenia danych telekomunikacyjnych, o których mowa w ust. 5 pkt 1 i ust. 6, oraz o jego wykonaniu, organ Służby Celnej jest obowiązany niezwłocznie poinformować sąd okręgowy, ***o którym mowa w ust. 1.***

8) **Do art. 11 pkt 2 dot. art. 75dc ust. 1**
Uwaga legislacyjna. Po wyrazie *ustawy* należy dodać wyrazy *z dnia 16 lipca 2004 r,* a po wyrazach *Prawo telekomunikacyjne* należy dodać promulgator tej ustawy tj. (Dz. U. z 2014 r. poz. 243, 827 i 1198), z uwagi na to, że ustawa wcześniej nie tworzy skrótu dla ustawy Prawo telekomunikacyjne.

9) **Do art. 11 pkt 2 dot. art. 75dc ust. 2**
Proponuje się usunięcie tego przepisu.
Mając na uwadze znikomą ilość wystąpień Służby Celnej o dane telekomunikacyjne powyższa norma stanowi przeregulowanie. Służba Celna wystąpiła o dane telekomunikacyjne w 2014 r. w 58 przypadkach, a w I połowie 2015 r. w 46 przypadkach. Zakres informacji, o które Służba Celna może wystąpić jest bardzo wąski, dotyczy on jedynie teoretycznie 10 przepisów kodeksu karnego skarbowego, przy czym w większości wnioski dotyczyły przestępstw z art. 107 § 1 kks. W ocenie Ministerstwa Finansów w wyroku Trybunału Konstytucyjnego K23/11 z dnia 30 lipca 2014 r. nie ma stanowiska, według którego należałoby objąć szczególną kontrolą pozyskiwanie danych przez Służbę Celną. Trybunał Konstytucyjny w wyroku nie zobowiązał również prawodawcy do zróżnicowania nadzoru sądu nad pozyskiwaniem danych przez poszczególne Służby. Z uwagi na brak uzasadnienia dla zróżnicowania tej regulacji należy domniemywać, że wolą projektodawcy było zapewnienie większego nadzoru dla pozyskiwania danych przez Służbę Celną. O ile należy przyznać, że w demokratycznym państwie prawnym, tego rodzaju zabezpieczenia są wskazane, to jednak należy je stosować w równiej mierze dla każdego rodzaju pozyskiwanych danych przez pozostałe Służby. Wówczas odpowiednia ochrona i nadzór nad pozyskiwaniem danych będzie kompletny. Pozostawienie takiej regulacji jedynie w ustawie o Służbie Celnej spowoduje, że w innych przypadkach pozyskiwania danych, nadzór ten będzie niepełny.

z poważaniem,

Z upoważnienia Ministra Finansów
PODSEKRETARZ STANU
Agnieszka Królikowska

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA
HELSINKI FOUNDATION for HUMAN RIGHTS

RADA FUNDACJI

Halina Bortnowska-Dąbrowska
Jerzy Ciemniewski
Janusz Grzelak
Michał Nawrocki
Marek Antoni Nowicki
Teresa Romer
Mirosław Wyrzykowski

ZARZĄD FUNDACJI

Prezes: Danuta Przywara
Wiceprezes: Adam Bodnar
Sekretarz: Maciej Nowicki
Skarbnik: Elżbieta Czyż
Członek Zarządu: Janina A. Kłosowska

Warszawa, 20 lipca 2015 r.

1652./2015/MPL/BGM

Szanowny Pan
Senator Piotr Zientarski
Komisja Ustawodawcza
Senat RP

Opinia do projektu ustawy
o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)

Celem opiniowanego projektu jest dostosowanie polskiego ustawodawstwa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. K 23/11). Wyrok ten obejmuje swoim zakresem: po pierwsze, kwestie związane z zasadami prowadzenia kontroli operacyjnej, po drugie – zagadnienie zapewnienia odpowiedniej kontroli nad pozyskiwaniem przez uprawnione służby danych telekomunikacyjnych.

1. Cel i zakres projektu

Opiniowany projekt ma za zadanie docelowo realizować przede wszystkim sentencję i wytyczne wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. W ocenie Helsińskiej Fundacji Praw Człowieka, prawidłowe wykonanie wyroku Trybunału Konstytucyjnego w odniesieniu do drugiego zagadnienia wymaga uwzględnienia wytycznych wynikających z wyroku Trybunału Sprawiedliwości z 8 kwietnia 2014 r. w sprawie *Digital Rights Ireland*, którego przedmiotem była kwestia zgodności tzw. dyrektywy retencyjnej z Kartą Praw Podstawowych UE. Konieczność uwzględnienia wyroku Trybunału Sprawiedliwości wynika m.in. z faktu, że argumentacja Trybunału Konstytucyjnego była zbieżna ze wcześniejszymi ustaleniami Trybunału Sprawiedliwości, mimo iż nie znalazła odzwierciedlenia w samej sentencji wyroku.

Pierwotnie prace nad zmianami w systemie kontroli nad pozyskiwaniem danych telekomunikacyjnych przez służby prowadziła senacka Komisja Praw Człowieka, Praworządności i Petycji. Prace te miały na celu przede wszystkim realizację wniosków płynących z **raportu Najwyższej Izby. Kontroli** nt. udostępniania danych telekomunikacyjnych[1]. Następnie Komisja Praw Człowieka, Praworządności i Petycji podjęła

1 Informacja o wynikach kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne" (Nr ewid. 107/2013/P/12/191/KPB).

00-018 Warszawa, ul. Zgoda 11; tel.: (48 22) 556-44-40, fax: (48 22) 556-44-50; e-mail: hfhr@hfhr.org.pl, www.hfhr.org.pl
NIP: 525-12-61-255, konto: PKO BP SA I O/Centrum 58 1020 1013 0000 0502 0002 9165, swift: BPKOPLPW

również próbę dostosowania obowiązujących przepisów do wymogów płynących z wyroku Trybunału Sprawiedliwości[2]. Jednak ostatecznie prace nad tym projektem[3] zostały porzucone[4] ze względu na podjęcie prac legislacyjnych przez Komisję Ustawodawczą nad projektem będącym przedmiotem niniejszej opinii (druk senacki nr 967).

Sentencja wyroku Trybunału Konstytucyjnego zobowiązuje ustawodawcę do dostosowania obowiązującego porządku prawnego do wymogów Konstytucji w zakresie:

1. zasad prowadzenia przez uprawnione służby **kontroli operacyjnej**, które swoim zakres powinny obejmować:
   1.1. sprecyzowanie przesłanki przedmiotowej prowadzenia kontroli operacyjnej przez ABW w zakresie jej kompetencji do rozpoznawania, zapobiegania i wykrywania „przestępstw godzących w podstawy ekonomiczne państwa" (art. 5 ust. 1 pkt 2 lit. b ustawy o ABW)
   1.2. zagwarantowanie, aby właściwy organ (sąd) zarządzający kontrolę operacyjną wskazywał (w postanowieniu o zarządzeniu kontroli) „określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie";
   1.3. stworzenie gwarancji procesowej polegającej na „niezwłocznym, komisyjnym i protokolarnym zniszczeniu materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne";

oraz

2. zasad zatrzymywania i udostępniania **danych telekomunikacyjnych**, tj:
   2.1. zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne;
   2.2. wprowadzenia obowiązku niszczenia danych niemających znaczenia dla prowadzonego postępowania (art. 28 ustawy o ABW, art. 32 ustawy o SKW, art. 18 ustawy o CBA, art. 75d ust. 5 ustawy o Służbie Celnej).

2. Zmiany w zakresie zasad prowadzenia kontroli operacyjnej

2.1. Środki techniczne używane podczas kontroli operacyjnej

Trybunał Konstytucyjny orzekł, że m.in. art. 19 ust. 6 pkt 3 ustawy o Policji czy art. 27 ust. 6 pkt 3 ustawy o ABW – rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną ma obowiązek wskazać określony w prawie rodzaj środka technicznego pozyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

---

2 Posiedzenie Komisji Praw Człowieka, Praworządności i Petycji z 13 maja 2014 r. Przedmiotem posiedzenia było omówienie wpływu orzeczenia Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 roku w sprawie *Digital Rights Ireland* na zasady korzystania przez policję i inne organy publiczne z danych telekomunikacyjnych dla celów zapobiegania i zwalczania przestępczości. Program posiedzenia: http://senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2014/kpcpp/materialy/140513p1.pdf.

3 Dostępny na stronie: http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2015/kpcpp/materialy/bilingi/wniosek_nik_bilingi0312002014022109572 4.pdf.

4 Posiedzenie Komisji Praw Człowieka, Praworządności i Petycji w dniu 7 lipca 2015 r.

Obecne brzmienie przepisów poszczególnych ustaw służbowych przyznających kompetencje do prowadzenia kontroli operacyjnej oparte jest o brzmienie ustawy o Policji, która w art. 19 ust. 6 przewiduje, że kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji;
2) kontrolowaniu zawartości przesyłek;
3) stosowaniu 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.

Trybunał ocenił, że art. 19 ust. 6 pkt 3 spełnia standard precyzji przepisu zezwalającego na ingerencję w prawo do prywatności. Prokonstytucyjna wykładnia normy wynikającej z tego przepisu została oparta o obowiązek wskazania przez sąd zarządzający kontrolę operacyjną określonego w prawie rodzaju środka technicznego pozyskiwania informacji. Jak słusznie zauważył Trybunał ustawodawca nie sprecyzował elementów, jakie ma zawierać postanowienie sądu o zarządzeniu kontroli operacyjnej. Zawiera je jednak, m.in. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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[5] lub analogiczne rozporządzenie Prezesa Rady Ministrów odnoszące się do Agencji Bezpieczeństwa Wewnętrznego. Przewidują one, że sąd okręgowy zarządzający kontrolę operacyjną wskazuje w postanowieniu „rodzaj stosowanej kontroli operacyjnej"[6].

Projektodawca w uzasadnieniu projektu wskazał, że „wychodząc naprzeciw oczekiwaniom Trybunału odnośnie sprecyzowania w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania (...) ustawodawca (...) określił sposoby prowadzenia kontroli operacyjnej"[7]. **Niestety nie odpowiada temu brzmienie m.in. projektowanego art. 19 ust. 6 ustawy o Policji**:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
1) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;
2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;
3) kontroli treści korespondencji;
4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu."

W uzasadnieniu wyroku Trybunału Konstytucyjnego wskazano na potrzebę sprecyzowania „w przepisach prawa **zamkniętego rodzajowo katalogu środków i metod działania**, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach". Trybunał zaznaczył przy tym słusznie, że „nie chodzi o wskazanie parametrów technicznych, ale **rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania** za ich pomocą (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób,

5 Dz.U. 2011 nr 122 poz. 697; Rozporządzenie zostało zmienione przez Rozporządzenie Ministra Spraw Wewnętrznych z dnia 10 marca 2014 r. zmieniające rozporządzenie 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 (Dz.U. 2014 poz. 396) oraz Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 października 2014 r. zmieniające rozporządzenie 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 (Dz.U. 2014 poz. 1357).

6 „Sąd Okręgowy (...) postanawia ZARZĄDZIĆ/PRZEDŁUŻYĆ/ODMÓWIĆ ZARZĄDZENIA/PRZEDŁUŻENIA kontrolę(-li) operacyjną(-nej) polegającą(-cej) na ...**[rodzaj stosowanej kontroli operacyjnej]**".

7 s. 7 uzasadnienia.

miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej")". Trybunał uznał, że docelowo rodzaje tych środków technicznych powinny zostać uregulowane w ustawie. „Zasadne jest tym samym, by to parlament zaakceptował dopuszczalność stosowania rodzajów środków technicznych, które w szerokim zakresie ingerują w wolności i prawa człowieka".

Projektowany przepis w dalszym ciągu jest bardzo ogólny. Ponadto wydaje się, że pojęcie „rozmowy", o których mowa w pkt 1 mieszczą się w pojęciu „korespondencji", o którym mowa w pkt 3. Zwrócił na to również uwagę Trybunał Konstytucyjny na gruncie obowiązujących obecnie przepisów: Zdaniem Trybunału, wyrażenie „kontrola treści korespondencji" nie zawęża się jedynie do tradycyjnej formy wymiany informacji, lecz obejmuje każdy sposób przekazywania informacji pomiędzy jednostkami, bez względu na formę (tradycyjna poczta, e-mail, SMS, MMS itp.).

Dla porównania poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych skierowany do Sejmu VI kadencji (druk sejmowy nr 353) przewidywał nieco bardziej uszczegółowiony katalog środków technicznych (art. 2 ust. 3 pkt 10 projektu):

a) podsłuch rozmów telefonicznych,
b) podsłuch i podgląd pomieszczeń i osób,
c) podsłuch techniczny środków łączności przewodowej i radiowej,
d) nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu,
e) nadzór elektroniczny środków łączności przewodowej i radiowej[8].

Wątpliwości Fundacji co do zgodności projektowanej regulacji z wymogami wynikającymi z Konstytucji[9] wynikają m.in. z postępowań sądowych prowadzonych przez Fundację przeciwko poszczególnym służbom w sprawie wniosków o dostęp do informacji publicznej. Przykładowo, Helsińska Fundacja Praw Człowieka skierowała do Centralnego Biura Antykorupcyjnego wniosek o udostępnienie informacji na temat korzystania przez CBA z oprogramowania „Remote Control System". System ten (RCS) umożliwia monitorowanie komputerów i telefonów, pozyskiwanie danych przechowywanych na tych urządzeniach, nawet w sytuacji gdy użytkownik nie jest podłączony do Internetu oraz śledzenie korespondencji w Internecie. RCS pozwala także kopiować pliki z dysku twardego komputera, nagrywać rozmowy Skype, przechwytywać hasła wprowadzone do wyszukiwarki, włączyć kamerę internetową lub mikrofon komputera. Centralne Biuro Antykorupcyjne odmówiło udzielenia wnioskowanej informacji[10], podczas gdy Agencja Bezpieczeństwa Wewnętrznego poinformowała, że takiego oprogramowania nie stosuje[11]. Ostatnie doniesienia medialne nt. ataku na serwery firmy Hacking Team – producenta oprogramowania RCS – wskazują, że Centralne Biuro Antykorupcyjne wykupiło licencję na ten program. **W świetle brzmienia projektowanych przepisów nadal nie jest jasne czy na ich gruncie zakup takiego oprogramowania przez Policję, ABW czy CBA a następnie ich stosowanie jest dopuszczalne**

8 Art. 14 ust. 6 projektu ustawy o czynnościach operacyjno-rozpoznawczych przewidywał, że kontrola operacyjna prowadzona jest niejawnie i polega na: 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu 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, 4) tajnej lustracji pomieszczeń i środków transportu.

9 Trybunał wskazał, że „pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków".

10 Por. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 lutego 2015 r., sygn. II SA/Wa 1670/14.

11 http://www.hfhrpol.waw.pl/precedens/aktualnosci/abw-nie-stosuje-narzedzi-do-zdalnego-kontrolowania-komputerow-i-telefonow.html

na gruncie definicji kontroli operacyjnej. Nierozstrzygniętym problemem pozostaje również to czy dopuszczalne jest stosowanie takiego oprogramowania poza procedurą kontroli operacyjnej, np. w ramach kompetencji Agencji Wywiadu to prowadzenia wywiadu elektronicznego (art. 6 ust. 1 pkt 8 ustawy o ABW i AW).

2.2. Termin prowadzenia kontroli operacyjnej

Projekt przewiduje doprecyzowanie terminu prowadzenia kontroli operacyjnej na podstawie art. 19 ust. 9 ustawy o Policji. Odnosi się on do sytuacji, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa. Wówczas możliwe jest przedłużenie przez sąd prowadzenia kontroli operacyjnej nawet po upływie terminów z art. 19 ust. 8 ustawy o Policji, tj. 6 miesięcy. Projekt zakłada, że to wyjątkowe przedłużenie prowadzenia kontroli operacyjnej będzie możliwe na okres oznaczony nie dłuższy niż **12 miesięcy**, przez co łączne prowadzenie kontroli operacyjne będzie mogło trwać nawet **18 miesięcy**.

W uzasadnieniu nie wskazano jednak czemu projektodawca zaproponował aż tak długi okres. Projektodawca wydaje się porównywać ten okres z 12 miesięcznym terminem retencji danych telekomunikacyjnych. Porównanie to jednak jest zupełnie nieadekwatne. **W ocenie Fundacji powinien on być nie dłuższy niż okres prowadzenia kontroli operacyjnej przewidziany w ustępie 8, tj. 6 miesięcy**. Co więcej projektodawca nie przedstawił informacji jak obecnie wygląda praktyka w zakresie stosowania art. 19 ust. 9, w którym termin nie został w ogóle oznaczony. **Uzyskanie takich informacji wydaje się niezbędne na dalszych etapach prowadzenia prac legislacyjnych nad projektem.**

Odmienny standard zastosowano na gruncie przepisów ustawy o CBA, ABW czy SKW. Przewidują one, że w sytuacji pojawienia się nowych istotnych okoliczności dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, „sąd (...) może wydawać, również po upływie okresów, o których mowa w ust. 8, kolejne **postanowienia** o przedłużeniu kontroli operacyjnej **na następujące po sobie okresy**, z których **żaden** nie może trwać dłużej niż **12 miesięcy**". **Tym samym projektodawca nie ustanawia *de facto* i *de iure* maksymalnego okresu prowadzenia kontroli operacyjnej przez CBA, ABW i SKW**. W uzasadnieniu wskazano, że takie zróżnicowanie wynika ze specyfiki zadań realizowanych przez służby specjalne. „*Przyjęcie takiego rozwiązania w odniesieniu do służb specjalnych jest niezbędne z perspektywy bieżących zagrożeń, m.in. w kontekście przyjmowanego obecnie modus operandi sprawców takich przestępstw jak przestępstwa o charakterze terrorystycznym, sabotaż, czy szpiegostwo, wykorzystujących tzw. uśpione ogniwo.*" - wskazano w uzasadnieniu[12]. **Problem polega jednak na tym, że żadnego z tych przestępstw nie ściga Centralne Biuro Antykorupcyjne.**

Projektodawca powołuje się przy tym na stanowisko Trybunału Konstytucyjnego, który zaznaczył, że „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". Projektowana regulacja (m.in. art. 27 ust. 9 ustawy o ABW czy art. 17 ust. 9 ustawy CBA) w zestawieniu z powyższym standardem rodzi szereg wątpliwości. Po pierwsze, w świetle powyższych kryteriów nie wydaje się, aby Centralne Biuro Antykorupcyjne spełniało kryterium służby wywiadowczej ani służby zajmującej się ochroną bezpieczeństwa państwa. Po drugie, przedstawione uzasadnienie projektu opiera się na wnioskowaniu „z mniejszego na większe". W oparciu o prawdopodobną specyfikę *modus operandi* niektórych przestępstw (np. o charakterze

12 s. 8 uzasadnienia.

terrorystycznym) proponuje się stworzyć normę generalną mającą zastosowanie do wszystkich przestępstw ściganych np. przez ABW (np. niektórych przestępstw określonych w kodeksie karnym skarbowym)[13].

W ocenie Fundacji **rozwiązanie zaproponowane w art. 27 ust. 9 ustawy o ABW, art. 17 ust. 9 ustawy o CBA oraz art. 31 ust. 7 ustawy o SKW jest nieproporcjonalnym wkroczeniem w prawo do prywatności oraz tajemnicę korespondencji**. Realizacja zamierzeń projektodawcy odnosząca się do specyfiki niektórych przestępstw (zresztą niezwykle lakonicznie przedstawiona w uzasadnieniu projektu) powinna być precyzyjnie powiązana z poszczególnymi przestępstwami (np. sabotażu albo o charakterze terrorystycznym). W odniesieniu do pozostałych przestępstw, standard precyzji przepisów dotyczących czasu trwania kontroli operacyjnej powinien być zbliżony do terminów prowadzenia kontroli operacyjnej przez Policję, tj. nie powinien przekraczać 6 miesięcy (art. 19 ust. 8) przedłużony maksymalnie o kolejne 6 miesięcy (po spełnieniu przesłanej z art. 19 ust. 9).

2.3. Niszczenie materiałów kontroli operacyjnych zawierających tajemnice zawodowe

Kolejny wymóg wynikający z wyroku Trybunału Konstytucyjnego odnoszący się do zasad prowadzenia kontroli operacyjnej wiąże się z obowiązkiem zapewnienia ochrony tajemnicy zawodowej, o której mowa w art. 180 § 2 k.p.k. oraz tajemnicy obrończej i tajemnicy spowiedzi (art. 178 k.p.k.). Trybunał orzekł, że m.in. art. 19 ustawy o Policji jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji **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.**

Projekt wprowadza w poszczególnych ustawach specjalną procedurę zawartą m.in. w art. 19 ust. 15f-15i ustawy o Policji. Procedura ta odmiennie traktuje informacje, o których mowa w art. 178 k.p.k., odmiennie zaś tajemnice zawodowe z art. 180 § 2 k.p.k. **Wydaje się, że stoi to w sprzeczności ze standardem, który Trybunał zastosował jednakowo w odniesieniu do obu rodzaju informacji.**

W przypadku tajemnicy obrończej[14] i tajemnicy spowiedzi właściwy komendant Policji nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie materiałów zawierających te informacje (art. 19 ust. 15f pkt 1). Natomiast w odniesieniu do tajemnicy zawodowej, o której mowa w art. 180 § 2 k.p.k. projekt przewiduje obowiązek przekazania materiałów prokuratorowi (art. 19 ust. 15f pkt 2 ustawy o Policji), który następnie kieruje je obowiązkowo do sądu wraz z wnioskiem o 1. wyrażenie zgody na ich wykorzystanie w postępowaniu karnym albo 2. wydanie zarządzenia o niezwłocznym komisyjnym, protokolarnym zniszczeniu.

Nie jest przy tym jasne jaki jest cel przekazania tych informacji prokuratorowi, jeśli nie jest on w stanie nakazać zniszczenia tych materiałów Policji, a jedynie może wnioskować do sądu o takie zniszczenie. Projektowany przepis nie wyraża nadzorczej roli prokuratora w procedurze kontroli

13 Projekt przewiduje daleko idące uporządkowanie kompetencji ABW zawartych art. 5 ust. 1 ustawy o ABW. Rozwiązanie to stanowi kopię propozycji rządowej z 2014 r. (por. projekt ustawy o ABW, druk sejmowy nr 2295).

14 Art. 178 pkt 1 k.p.k. w brzmieniu obowiązującym od 1 lipca 2015 r. odwołuje się do „obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę".

operacyjnej. Prowadzi jedynie do poszerzenia kręgu osób, które mogą się zapoznać z informacjami zawierającymi tajemnice zawodowe znajdującymi w materiałach z kontroli operacyjnej.

Art. 19 ust. 15h ustawy o Policji przewiduje, że sąd wydaje – w terminie 14 dni – postanowienie w przedmiocie wniosków prokuratora. Przepis ten nie wskazuje jednak **jakie przesłanki sąd bierze pod uwagę** wydając postanowienie na podstawie tego przepisu. W przypadku, o którym mowa art. 180 § 2 k.p.k., sąd może wyrazić zgodę na przesłuchanie osób zobowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej ***„tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu"***. Taka przesłanka nie występuje na gruncie ust. 15h co może oznaczać dowolność po stronie sądu podejmującego decyzje w przedmiocie wniosków prokuratora.

Co więcej, w odróżnieniu z procedurą z art. 180 § 2 k.p.k. projekt przewiduje że na postanowienie sądu z art. 19 ust. 15h ustawy o Policji nie przysługuje zażalenie stronie objętej kontrolą operacyjną. Jest to zatem o wiele niższy poziom ochrony tajemnicy zawodowej (adwokackiej czy dziennikarskiej) niż ma to miejsce na etapie procesowym[15], mimo iż w uzasadnieniu projektodawca wskazał, że „nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym"[16].

W ocenie Helsińskiej Fundacji Praw Człowieka, projektowana procedura nie wykonuje standardu zawartego w orzeczeniu Trybunału Konstytucyjnego.

2.4. Wykonanie postanowienia sygnalizacyjnego S 2/06

Uzasadnienie projektu odwołuje się do wymogu płynącego z postanowienia sygnalizacyjnego Trybunału Konstytucyjnego z 25 stycznia 2006 r. (sygn. S 2/06). Trybunał wskazał na potrzebę uregulowania obowiązku informowania osób objętych kontrolą operacyjną o fakcie jej prowadzenia. Trybunał argumentował, 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)"*. Wskazał na to również Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. wskazując wśród standardów konstytucyjnych odnoszących się do prowadzonych czynności operacyjno-rozpoznawczych wymóg *„unormowania 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"*.

Projektodawca nie podziela jednak konkluzji płynących z postanowienia sygnalizacyjnego z 2006 r. oraz z wyroku z 2014 r. i wskazuje na trzy rodzaje przeszkód związanych z wykonaniem postanowienia sygnalizacyjnego:

- „wiązałoby się z naruszeniem podstawowych zasad na podstawie których funkcjonują służby i poważnie mogłoby zaważyć na skutecznym działaniu służb, ale także mogłoby zagrozić bezpieczeństwu Sił Zbrojnych RP oraz osób, które w niejawny sposób udzielają pomocy służbom"

15 Zgodnie z art. 180 § 2 zd. 3 na postanowienie sądu przysługuje zażalenie.

16 s. 5 uzasadnienia

- wiązałoby się z tym trudności z ustaleniem danych osób z uwagi na znaczną skalę używania tzw. telefonów pre-paid
- obowiązek informowania pozostawałby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia.

Wspomniany obowiązek ochrony form i metod jest obowiązkiem wynikającym z ustawy, podczas gdy obowiązek informowania jednostki o prowadzeniu wobec niej kontroli operacyjnej wynika z przywołanej interpretacji art. 51 ust. 4 Konstytucji. Należy zatem przede wszystkim zadać sobie pytanie czy ustawowy obowiązek ochrony form i metod w takim zakresie w jakim wynika z ustaw resortowych jest zgodny z Konstytucją. Odmienna argumentacja oparta o twierdzenie iż wymóg wynikający z Konstytucji jest niezgodny z unormowaniem ustawowym nie znajduje oparcia w konstytucyjnej hierarchii źródeł prawa powszechnie obowiązującego.

W ocenie Helsińskiej Fundacji Praw Człowieka wykonanie wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. wymaga implementowania postanowienia sygnalizacyjnego Trybunału z 25 stycznia 2006 r.

3. Dane telekomunikacyjne

Jak zostało wskazane na początku, wyrok Trybunału Konstytucyjnego odnoszący się zasad pozyskiwania przez służby danych telekomunikacyjnych zobowiązuje ustawodawcę do:

1. zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne;
2. wprowadzenia obowiązku niszczenia danych niemających znaczenia dla prowadzonego postępowania (art. 28 ustawy o ABW, art. 32 ustawy o SKW, art. 18 ustawy o CBA, art. 75d ust. 5 ustawy o Służbie Celnej).

Drugi z powyższych wymogów projektodawca realizuje dodając do obowiązujących przepisów nowe jednostki redakcyjne (np. art. 28 ust. 6 ustawy o ABW i AW, art. 18 ust. 6 ustawy o CBA, art. 75d ust. 6 ustawy o Służbie Celnej), które analogicznie przewidują, że „materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych, które nie zawierają informacji mających znaczenie dla postępowania karnego lub postępowania karnego skarbowego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu".

Wykonanie jednak pierwszego wymogu dotyczącego zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych wymaga od ustawodawcy szerzej zakrojonych działań. Wskazał na to m.in. przedstawiciel Prokuratora Generalnego podczas posiedzenia senackiej Komisji Ustawodawczej w dniu 8 czerwca 2015 r.[17] Z takim stanowiskiem zgodził się wówczas przedstawiciel Ministra Spraw Wewnętrznych, który wskazał zespół rządowy pracujący nad projektem wykonującym wyrok Trybunału Konstytucyjnego nie koncentruje się jedynie na sentencji wyroku, ale również bierze pod uwagę kwestie związane z dyrektywą retencyjną. Należy jednak wyraźnie podkreślić, że wbrew tym zapewnieniom, projekt nie realizuje wytycznych wynikających z wyroku Trybunału Sprawiedliwości, który sformułował pod adresem dyrektywy szereg zarzutów, które skutkowały ostatecznie uznaniem jej za nieważną:

17 Obecny na posiedzeniu przedstawiciel Prokuratora Generalnego wskazał, że przy wykonaniu tego wyroku projektodawcy będą musieli uwzględnić duże szersze tło wynikające, w szczególności, z wyroku Trybunału Sprawiedliwości. Wskazał on również, że deficyty dyrektywy retencyjnej są odzwierciedlone w polskim prawie.

- bardzo szeroki zakres dyrektywy i gromadzonych na jej podstawie danych co skutkuje brakiem wyłączeń m.in. wobec osób których komunikacja objęta jest tajemnicą zawodową;
- brak kryteriów do określenia najpoważniejszych przestępstw, które uzasadniałyby dostęp do tych danych;
- brak wymogów odnoszących się do **uprzedniej kontroli**, tym samym - brak gwarancji ochrony przed nadużyciami;
- brak zależności między okresem retencji a rodzajem przechowywanych danych oraz brak kryteriów co do czasu ich zatrzymania (duża rozbieżność między okresem minimalnym i maksymalnym);
- brak regulacji dotyczących odpowiedniego zabezpieczenia danych przez podmioty prywatne, w szczególności w odniesieniu do obowiązku zatrzymania danych na obszarze Unii, co powoduje, że nie można zagwarantować kontroli poszanowania wymogów ochrony i bezpieczeństwa.

Projekt nie uwzględnia również postulatów wynikających z raportu Najwyższej Izby Kontroli, będący punktem wyjście do prac legislacyjnych Komisji Praw Człowieka, Praworządności i Petycji. W informacji o wynikach kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne", zawarto szereg wniosków i zaleceń - skierowanych pod adresem Prezesa Rady Ministrów – mających na celu:
- doprecyzowanie **zakresu danych**, które powinny podlegać retencji;
- weryfikację **katalogu spraw**, na potrzeby których dane telekomunikacyjne mogą być przez uprawnione służby pozyskiwane;
- przeanalizowanie możliwości wprowadzenia dodatkowych **rozwiązań o charakterze gwarancyjnym**, ograniczających możliwość pozyskiwania danych retencyjnych w stosunku do osób wykonujących tzw. „zawody zaufania publicznego";
- ustanowienie **kontroli zewnętrznej** nad procesem pozyskiwania danych, obejmującej weryfikację zasadności ich pozyskiwania;
- wprowadzenie skutecznych instrumentów gwarantujących **niezwłoczne niszczenie** pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania;
- ustanowienie **mechanizmów sprawozdawczych**, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych;
- wprowadzenie przepisów gwarantujących osobom, których dane bilingowe były pobierane, **prawa do informacji o zakresie i czasie zbierania tych danych**, po zakończeniu w danej sprawie czynności – wyjątki w tym zakresie powinny określić przepisy ustawy;
- opracowanie wytycznych dotyczących technicznych i organizacyjnych **środków bezpieczeństwa** w zakresie uzyskiwania dostępu do danych, w tym procedur ich przekazywania;
- wzmocnienie, do czasu wprowadzenia zmian systemowych, **nadzoru** nad wykorzystaniem przez organy państwa uprawnień w zakresie pozyskiwania danych obywateli.

3.1. Projekt ustawy a wymogi płynące z wyroku Trybunału Sprawiedliwości w sprawie *Digital Rights Ireland*

Niestety projekt całkowicie pomija wymogi i wskazówki płynące z wyroku Trybunału Sprawiedliwości w sprawie *Digital Right Ireland*. Co prawda wyrok skutkuje przede wszystkim unieważnieniem dyrektywy retencyjnej, to jednak należy mieć na uwadze, że stanowi on element dorobku konstytucyjnego Unii Europejskiej, zaś orzecznictwo Trybunału Sprawiedliwości jest wiążące dla Państw Członkowskich.

Z całą pewnością skutkiem wyroku jest konieczność przeanalizowania regulacji krajowej pod kątem ich zgodności z art. 15 dyrektywy 2002/58 o prywatności i łączności elektronicznej[18]. Dopuszcza on możliwość wprowadzenia przez Państwa Członkowskie ograniczeń od zasad ochrony danych osobowych, m.in. danych o ruchu[19] pod warunkiem, że „takie ograniczenia stanowią środki **niezbędne, właściwe i proporcjonalne** w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (m.in. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej".

W ocenie Helsińskiej Fundacji Praw Człowieka elementem wykonania wyroku w sprawie *Digital Rights Ireland* powinno być **zweryfikowanie czy obecny system retencji danych telekomunikacyjnych na gruncie Prawa telekomunikacyjnego jest zgodny z art. 15 dyrektywy 2002/58**. Z kolei do przeprowadzenia tej weryfikacji niezbędne może się okazać skorzystanie ze wskazówek zawartych właśnie w wyroku *Digital Rights Ireland*[20]. Trybunał Sprawiedliwości ocenił bowiem, że zakres danych gromadzonych jest niezmiernie szeroki, nie przewiduje żadnych wyłączeń podmiotowych, co umożliwia zbieranie informacji dotyczących życia prywatnego wszystkich obywateli Unii Europejskiej. **Tymczasem opiniowany projekt nie zawiera żadnej analizy co do jego zgodności z prawem UE.** Na samym końcu uzasadnienia projektu wskazano jedynie, że „zakres przedmiotowy projektowanej ustawy jest zgodny z prawem UE".

Brak analizy projektu pod kątem jego zgodności z prawem Unii Europejskiej może się okazać jego najpoważniejszym mankamentem, w szczególności w świetle ostatniego wyroku z 17 lipca 2015 r. High Court of Justice w sprawie ***David Davis and others -v- Secretary of State for the Home Department***[21]. Przedmiotem sprawy była ocena (przez sąd krajowy) zgodności z prawami człowieka brytyjskiego prawa krajowego dotyczącego retencji danych telekomunikacyjnych (*Data Retention and Investigatory Powers Act 2014*) uchwalonego w lipcu 2014, tj. już po ogłoszeniu wyroku przez Trybunał Sprawiedliwości. Pomimo iż dyrektywa retencyjna nie jest aktem obowiązującym, High Court of Justice ocenił, że kwestie związane z zasadami ochrony danych osobowych (a tym samym również ograniczeń takich danych) objęte są prawem Unii Europejskiej od ponad 20 lat. Z kolei analiza wyroku *Digital Rights Ireland* doprowadziła sąd brytyjski do wniosku, że prawodawstwo ustanawiające generalny reżim retencji danych telekomunikacyjnych narusza prawa z art. 7 i 8 Karty Praw Podstawowych, chyba że towarzyszy takiemu reżimowi system, który gwarantuje adekwatne zabezpieczenia dla ochrony tych praw[22]. High Court of Justice

18 Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.; J. Raughofer, D.M. Sitgigh, *The Data Retention Directive Never Existed*, SrpitEd 1/2014, s. 126.

19 Art. 6 dyrektywy 2002/58.

20 Podobne stanowisko zostało wyrażone w opinii prawnej zamówionej przez Parlament Europejski „LIBE - Questions relating to the judgment of the Court of Justice of 8 April 2014 in Jolned Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others - Directive 2006/24/EC on data retention - Consequences of the judgment (Legal Opinion), 22 grudnia 2014 r. (dokument dostępny jest na stronie http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf); S. Peers, Are national data retention laws within the scope of the Charter? - http://eulawanalysis.blogspot.com/2014/04/are-national-data-retention-laws-within.html.

21 Sprawa [2015] EWHC 2092 (Admin), Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014. Wyrok dostępny jest na stronie:https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/.

22 § 89 uzasadnienia wyroku.

uznał *Data Retention and Investigatory Powers Act 2014* za niezgodny z prawem Unii Europejskiej ponieważ:

- nie zawiera jasnych i precyzyjnych reguł ograniczających korzystanie z danych telekomunikacyjnych jedynie do ścigania najpoważniejszych przestępstw;
- dostęp do danych telekomunikacyjnych nie zależy od wcześniejszej kontroli ze strony sądu lub niezależnego organu administracyjnego, którego decyzje mogłyby taki dostęp ograniczyć i gwarantować że sąd wykorzystywane do ścigania najpoważniejszych przestępstw[23].

Z kolei opiniowany projekt nie zawiera żadnej propozycji zróżnicowania poszczególnych rodzajów danych telekomunikacyjnych według głębokości ingerencji w prawo do prywatności i skutkującym zróżnicowaniem mechanizmów kontroli według poszczególnych rodzajów danych. Brak również w projekcie jakichkolwiek odniesień do wymogów zapewnienia bezpieczeństwa danych gromadzonych przez operatorów telekomunikacyjnych, w szczególności w odniesieniu do obowiązku zatrzymania danych na obszarze Unii Europejskiej.

Co więcej, dyrektywa retencyjna przewidywała, że dostęp do zgromadzonych danych telekomunikacyjnych będzie możliwy „celu dochodzenia, wykrywania i ścigania poważnych przestępstw" (art. 1 ust. 1). Tymczasem polskie przepisy krajowe umożliwiają obecnie sięganie po te dane w przypadku ścigania wszystkich przestępstw, które znajdują zakresie zadań danej służby. Obecne brzmienie art. 20c ustawy o Policji przewiduje, że „w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (...)". Projektowane brzmienie art. 20c ustawy o Policji praktycznie nie wprowadza żadnych zmian w tym zakresie: „W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych". Można wręcz odnieść wrażenie, że podstawa do uzyskiwania danych telekomunikacyjnych przez Policję została poszerzona. **Zaproponowanie zmian w katalogu przestępstw dających podstawę do wykorzystania danych telekomunikacyjnych wymagałoby jednak przeprowadzenia odpowiednich analiz w tym zakresie, w szczególności określenia w przypadku których przestępstw najczęściej pozyskiwane są dane telekomunikacyjne, w przypadku których przestępstw technika ta jest zbędna, oraz przede wszystkim na ile jest to narzędzie skuteczne i niezbędne to realizacji zadań poszczególnych służb.** Na gruncie przywołanego wyroku *David Davis and others -v- Secretary of State for the Home Department* sąd brytyjski orzekający w tej sprawie dysponował m.in. *Report of the Interception of Communications Commissioner*[24] przygotowanym przez urząd specjalnego komisarza ds. komunikacji oraz prawie 400-stronicowym opracowaniem "*A question of Trust. Report of the Invetigatory powers review*"[25] analizującym m.in. uprawnienia służb brytyjskich pod kątem ich zgodności z prawami człowieka, w szczególności prawem do prywatności.

23 § 114 uzasadnienia wyroku.

24 Sir Anthony May, Report of the Interception of Communications Commissioner, March 2015, dostępny na stronie: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf.

25 David Anderson, Independent Reviewer of Terrorism Legislation, "*A question of Trust. Report of the Invetigatory powers review*" https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

Błędem wydaje się ograniczenie projektowanych zmian w zakresie Prawa telekomunikacyjnego jedynie do propozycji usunięcia art. 180g Prawa telekomunikacyjnego[26]. Zdaniem projektodawcy jest to jedyny obowiązek „implementacyjny" wynikający z wyroku w sprawie *Digital Rights Ireland*. Z jednej strony projektodawca nakłada obowiązki sprawozdawcze na służby w zakresie pozyskiwania danych telekomunikacyjnych (pkt 3.4 opinii), z drugiej zaś zdejmuje się te obowiązki z operatorów telekomunikacyjnych. Takie rozwiązanie wydaje się być niezgodne z sugestiami zawartymi w raporcie NIK[27] oraz z wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r.:

> *„Trybunał Konstytucyjny zwraca także uwagę na konieczność wprowadzenia prawnego obowiązku **podawania do publicznej wiadomości zagregowanych danych statystycznych o liczbie i rodzaju stosowanych czynności operacyjno-rozpoznawczych ingerujących w konstytucyjne wolności i prawa człowieka**. Wymóg ten wynika z zasady demokratycznego państwa prawnego (art. 2 Konstytucji). Stanowi także urzeczywistnienie konstytucyjnego prawa do uzyskiwania informacji o działalności organów władzy publicznej (art. 61 ust. 1 Konstytucji). Transparentność danych statystycznych obrazujących skalę niejawnego pozyskiwania danych o jednostkach przez organy państwa powinna być w szczególności nieodzownym elementem demokratycznej kontroli nad działalnością organów państwa (zob. orzeczenie ETPC z 25 czerwca 2013 r. w sprawie Youth Initiative for Human Rights przeciwko Serbii, nr skargi 48135/06). Zdaniem Trybunału Konstytucyjnego, prawodawca i organy stosujące prawo mają szanować ten obowiązek. Prawodawca powinien także, w celu efektywnego i rzetelnego wykonywania obowiązku sprawozdawczego, **ustalić w miarę możliwości jedną, stosowaną przez wszystkie zobowiązane podmioty, metodologię sporządzania statystyk, gwarantującą jednoznaczność i porównywalność upubliczniających danych, nawet w odniesieniu do ubiegłych lat**".*

Dotychczasowe problemy na tym tle wiązały się właśnie ze stosowaniem art. 180g Prawa telekomunikacyjnego, tj. informacji rocznej przekazywanej Komisji Europejskiej przez Prezesa Urzędu Komunikacji Elektronicznej. Z uwagi na brak ujednoliconej metodologii liczenia przypadków sięgania po dane telekomunikacyjnej[28] dane te są nieporównywalne między poszczególnymi Państwami Członkowskimi, ale co więcej nie dają informacji na temat rzeczywistej praktyki pozyskiwania danych telekomunikacyjnych przez uprawnione do tego służby w Polsce. W ocenie Helsińskiej Fundacji Praw Człowieka, projekt ustawy nie powinien ograniczać się do uchylenia art. 180g, ale powinien odzwierciedlać wytyczne Trybunału Konstytucyjnego oraz Najwyższej Izby Kontroli co do stworzenia ram prawnych dla optymalnej informacji nt. częstotliwości pozyskiwania danych telekomunikacyjnych przez służby.

---

26 Przepis ten nakłada na przedsiębiorców telekomunikacyjnych obowiązek przekazywania przez Prezesowi Urzędu Komunikacji Elektronicznej określonego rodzaju informacji na potrzeby sporządzenia sprawozdania dla Komisji Europejskiej.

27 „Jak wykazała kontrola NIK, funkcjonujący obecnie system gromadzenia informacji o pozyskiwaniu danych retencyjnych, **nie zapewnia rzetelnej informacji o liczbie tego rodzaju przypadków**. Brak jest precyzyjnie określonych wskaźników pomiarowych, a ustanowione procedury nie zapobiegają wystąpieniu rażących błędów. Również zakres gromadzonych danych sprawozdawczych nie pozwala na ocenę, dla jakich celów, jak często i z jakim skutkiem retencja danych jest stosowana. W ocenie NIK, dla prawidłowej oceny funkcjonowania systemu retencji danych niezbędne jest gromadzenie danych w zakresie: liczby przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych dane retencyjne (z wyodrębnieniem sytuacji, gdy były to wyłącznie dane osobowe użytkownika); liczby osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy; łącznej liczby odmów udostępnienia danych (ze wskazaniem zasadniczych przyczyn); informacji na temat rodzaju spraw, w których środek ten wykorzystywano oraz jego skuteczności." (Raport NIK, s. 16-17).

28 Trybunał wskazał w wyroku, że „liczba zapytań o dane telekomunikacyjne na podstawie zakwestionowanych przepisów nie odzwierciedla rzeczywistej liczby abonentów, których dane telekomunikacyjne pozyskiwano. (...) Jak wynika z udzielonych wyjaśnień najwięcej zapytań (około 50%) dotyczy ustalenia danych osobowych abonenta. Wynika to z braku centralnej bazy abonentów, z której można pobrać stosowne dane, a także z dużej liczby użytkowników telefonów komórkowych korzystających z tzw. kart przedpłaconych *pre paid* (według przekazanych Trybunałowi danych, około 52% użytkowników telefonów komórkowych w Polsce korzysta z tej formy rozliczeń)".

3.2. Zasada subsydiarności wnioskowania o udostępnienie danych telekomunikacyjnych

Jak wynika z uzasadnienia wyroku Trybunału Konstytucyjnego przepisy kompetencyjnej upoważniające do niejawnego pozyskiwania informacji o jednostkach w toku czynności operacyjno-rozpoznawczych (np. danych telekomunikacyjnych) **„musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne"**. Projektodawca uznał jednak, że zasada subsydiarności w odniesieniu do danych telekomunikacyjnych nie powinna zostać wyrażona w ustawie. W uzasadnieniu projektu wskazano, że „zastosowanie zasady subsydiarności przed wystąpieniem o udostępnienie danych telekomunikacyjnych w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudniać skuteczne ściganie ich sprawców". Podając jako przykład przestępstwa popełnione przy użyciu urządzeń telekomunikacyjnych oraz przestępstw internetowych, gdzie podstawową metodą pracy operacyjnej jest najprawdopodobniej dostęp do danych telekomunikacyjnych, projektodawca wskazuje, że zasada subsydiarności nie jest możliwa do zastosowania w przypadku innych przestępstw.

W ocenie Helsińskiej Fundacji Praw Człowieka, możliwe jest zastosowanie do procesu udostępniania danych telekomunikacyjnych zasady subsydiarności analogicznej do tej zawartej w procedurze zarządzania kontroli operacyjnej ***„gdy inne środki okazały się bezskuteczne albo będą nieprzydatne"***. Wówczas ściganie np. przestępstw internetowych przy użyciu danych telekomunikacyjnych będzie dopuszczalne z uwagi fakt, że inne środki z zakresu czynności operacyjno-rozpoznawczych – mniej ingerujące w prawo do prywatności – okażą się nieprzydatne.

3.3. Kontrola nad udostępnianiem danych telekomunikacyjnych

Konkluzja Trybunału Konstytucyjnego o potrzebie zapewnienia niezależnej kontroli nad pozyskiwaniem danych telekomunikacyjnych została poprzedzona szeregiem uwag odnoszących się do obecnej regulacji pozyskiwania przez służby danych telekomunikacyjnych. Trybunał wytknął obecnej regulacji, że ***„ustawodawca nie uzależniał możliwości żądania danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie – wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji***". Trybunał zdecydował się położyć cały nacisk na kwestie proceduralne związane z zewnętrzną kontrolą nad pozyskiwaniem danych.

Brak kontroli uprzedniej, brak wymogu zgody prokuratora, brak kontroli *ex post* doprowadziło Trybunał do wniosku, że ***„pozyskiwanie danych telekomunikacyjnych (...) pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane***". Trybunał nie zdecydował się jednak na zarysowanie jak powinien wyglądać optymalny – z punktu widzenia Konstytucji – model kontroli nad dostępem służb do danych telekomunikacyjnych.

Trybunał zaznaczył, że „nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka". Stąd nie wykluczył jako zasady kontroli następczej, zaznaczając przy tym, że, ustawodawca regulując ten mechanizm powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Jako sytuacje, które – przykładowo – powinny wymagać kontroli uprzedniej ustawodawca wskazał na dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma

konieczności pilnego działania służb. O ile opiniowany projekt realizuje pierwszą z sytuacji, to całkowicie pomija sytuacje niewymagające pilnego działania służb.

W odniesieniu zaś do kwestii podmiotowych – organu, który powinien sprawować taką kontrolę – Trybunał wskazał, że nie wymaga by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. **„Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności"**.

Idea stworzenia niezależnego organu pełniącego kontrolę nad działalnością służb została również zawarta w „Raporcie dotyczących retencji danych telekomunikacyjnych" zaprezentowanym przez ministra J. Cichockiego w 2011 r.[29] Próbą realizacji tego pomysłu był projekt ustawy o Komisji Kontroli Służb Specjalnych[30] opracowany przez Ministerstwo Spraw Wewnętrznych w 2013 r.

Niestety wbrew tym zapowiedziom opiniowany projekt ustawy ogranicza planowany system kontroli nad pozyskiwaniem danych telekomunikacyjnych do:

- **uprzedniej kontroli sądowej** odnoszącej się jedynie do przypadków pozyskiwania danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego;
- **obowiązku sprawozdawczego służb**, który – w założeniu projektodawcy – ma stanowić efektywny mechanizm kontroli *ex post*.

Tym samym projekt opiera się na zupełnie odmiennych założeniach i **prezentuje o wiele niższy standard ochrony prawa do prywatności** niż projekt ustawy opracowany przez senacką Komisję Praw Człowieka, Praworządności i Petycji, która zakładała uprzednią kontrolę sądową w każdym wypadku uzyskiwania danych telekomunikacyjnych, kontrolę Generalnego Inspektora Ochrony Danych Osobowych oraz kontrolę ze strony specjalnych pełnomocników ds. ochrony danych osobowych.

Projektowany art. 20ca ustawy o Policji przewiduję procedurę – analogiczną do tej zastosowanej przy kontroli operacyjnej – weryfikacji danych dotyczących osób, o których mowa w art. 180 § 2 k.p.k. Podobnie jak w przypadku art. 19 ust. 15f ustawy o Policji materiały zawierające takie informacje są przekazywane prokuratorowi, który następnie kieruje te materiały do sądu z wnioskiem „o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym" (art. 20ca ust. 2). W takiej procedurze **udział prokuratora wydaje się automatyczny**, ponieważ może on jedynie skierować do sądu tylko jeden rodzaj wniosku (o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym), podczas gdy w przypadku materiałów z kontroli operacyjnej mógł również złożyć wniosek o zniszczenie materiałów. Nie jest zatem zrozumiałe jaka *de facto* jest rola prokuratora w niniejszej procedurze. Jeśli ostatecznie ma decydować w tym przedmiocie sąd, być może lepszym rozwiązaniem byłoby bezpośrednie kierowanie materiałów do sądu. Ponadto, podobnie jak w przypadku niszczenia materiałów z kontroli operacyjnych projekt nie zawiera przesłanek, które sąd podejmując decyzję w przedmiocie wniosku prokuratora powinien wziąć po uwagę.

Udział prokuratora został z kolei pominięty w procedurze na podstawie art. 20cb ustawy o Policji, tj. wymagających pozyskania *ab initio* danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osób, o których mowa w art. 180 § 2 k.p.k. **W kontekście postanowienia**

29 Raport, s. 8-10.

30 Projekt UD107 – dostępny na stronie Rządowego Procesu Legislacyjnego: http://legislacja.rcl.gov.pl/projekt/181401.

sygnalizacyjnego S 2/06 należy rozważyć czy w przypadku braku zgody sądu na udostępnienie danych telekomunikacyjnych nie należy poinformować o tym fakcie osoby, których dotyczą wnioskowane dane.

3.4. Obowiązek sprawozdawczy służb

Jednym z elementów systemu kontroli zaproponowanym w opiniowanym projekcie jest procedura sprawozdawczości przewidziana m.in. w art. 20cc ust. 2 ustawy o Policji. Przewiduje ona, że właściwy organ Policji[31] raz na 6 miesięcy przekazuje sądowi sprawozdanie obejmujące:

1) liczbę i rodzaj pozyskanych danych telekomunikacyjnych lub pocztowych;
2) podstawę prawną pozyskania danych telekomunikacyjnych lub pocztowych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub pocztowe;
4) liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane telekomunikacyjne lub pocztowe.

Projekt następnie zakłada, że **sąd może zapoznać** się z materiałami uzasadniającymi udostępnieniu Policji danych telekomunikacyjnych oraz z materiałami uzyskanymi w wyniku podjętych czynności. Tym samym projekt zakłada pewne zręby sądowej kontroli następczej nad pozyskiwaniem przez służby danych osobowych. Jednak, w ocenie Helsińskiej Fundacji Praw Człowieka, zaproponowany model kontroli nosić będzie cechy fasadowości tworząc jedynie fikcję skutecznej kontroli nad pozyskiwaniem danych telekomunikacyjnych. Przede wszystkim kierowane do sądów sprawozdania nie będą najprawdopodobniej zawierać informacji w sprawie poszczególnych rodzajów spraw, lecz jedynie pewnie dane zagregowane. Oznacza to, że nawet jeśli sąd podejmie wątpliwości co do prawidłowości udostępnienia danych telekomunikacyjnych, sąd nie będzie wiedział o jakie materiały powinien wystąpić do Policji.

Ponadto, aby taka kontrola była efektywna jej merytoryczne prowadzenie musi opierać się o ustawowy wymóg subsydiarnego charakteru sięgania po te dane. W przeciwnym wypadku, sąd nie będzie miał kryteriów według których miałby weryfikować prawidłowość podjętych działań, w szczególności w Policji, której projektowana podstawa do sięgania po dane telekomunikacyjne jest bardzo ogólna i obejmuje „rozpoznawanie, zapobieganie, zwalczanie, wykrywanie albo uzyskanie i utrwalenie dowodów przestępstw ściganych z oskarżenia publicznego".

Wydaje się jednak, że w świetle projektowanych zmian (art. 4 i 5 opiniowanego projektu ustawy) podstawowym celem kierowania przez służby sprawozdań do sądów ma na celu ich dalsze przekształcenie w roczne sprawozdanie kierowane do Ministra Sprawiedliwości (projektowane art. 6a Prawa o ustroju sądów wojskowych oraz art. 175b prawa o ustroju sądów powszechnych), który następnie przedstawia corocznie Sejmowi i Senatowi zagregowaną informację na temat przetwarzania danych telekomunikacyjnych i pocztowych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym. Zdaniem Helsińskiej Fundacji Praw Człowieka, przebieg rozprawy przed Trybunałem Konstytucyjnym (w szczególności problemy z uzyskaniem informacji na temat zarządzania kontroli operacyjnej przez Sąd Okręgowy w Warszawie) wskazuje na pilną **potrzebę objęcia obowiązkiem sprawozdawczości informacji na temat działalności sądów w zakresie zarządzania (lub odmowy zarządzania) kontroli operacyjnej.**

---

31 Obowiązek ten dotyczy również, m.in. Straży Granicznej (art. 10bc ustawy o Straży Granicznej), Generalnego Inspektora Kontroli Skarbowej (art. 36bc ustawy o kontroli skarbowej), Żandarmeria Wojskowa (art. 30d ustawy o Żandarmerii Wojskowej).

W ocenie Helsińskiej Fundacji Praw Człowieka równolegle do tak projektowanej kontroli sądowej rolę organu oceniającego sprawozdania powinien pełnić specjalny pełnomocnik ds. danych osobowych, funkcjonujący obecnie jedynie na gruncie ustawy o CBA (por. pkt 3.5 opinii).

3.5. Pełnomocnicy ds. ochrony danych osobowych

Opiniowany projekt całkowicie pomija rozwiązania zawarte wcześniej w projekcie Komisji Praw Człowieka, Praworządności i Petycji, który zawierał propozycję ustanowienia w poszczególnych służbach niezależnych pełnomocników ds. danych osobowych. Organ taki funkcjonuje obecnie na gruncie ustawy o CBA. Rozwiązanie to stanowi wynik wykonania wyroku Trybunału Konstytucyjnego z 23 czerwca 2009 r. (sygn. K 54/07). Trybunał orzekł wówczas o niezgodności z Konstytucją art. 22 ust. 4-7 ustawy o CBA z uwagi na brak zagwarantowania instrumentów kontroli sposobu przechowywania i weryfikacji danych wskazanych w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz sposobu usuwania danych zbędnych dla wykonywania ustawowych zadań Centralnego Biura Antykorupcyjnego. Projekt Komisji Praw Człowieka, Praworządności i Petycji przewidywał utworzenie urzędu pełnomocnika w każdej służbie prowadzącej czynności operacyjno-rozpoznawcze, które przetwarzają dane osobowe. Propozycja taka stanowi przejaw wzmocnienia nadzoru wewnętrznego nad działalnością służb.

Niestety do takiego rozwiązania nie odnosi się w ogóle opiniowany projekt ustawy. Zdaniem Fundacji **należałoby powrócić do pomysłu zaproponowanego przez Komisję Praw Człowieka, Praworządności i Petycji**, jednak w miejsce kilku pełnomocników w poszczególnych służbach można rozważyć powołanie jednego pełnomocnika dla wszystkich służb, działającego np. przy Generalnym Inspektorze Ochrony Danych Osobowych, dysponującego kadrą i środkami do prowadzenia takiej bieżącej kontroli w sprawach danych osobowych jedynie w zakresie funkcjonowania służb policyjnych i specjalnych. Taki pełnomocnik mógłby np. rozpoznawać sprawozdania poszczególnych służb, które – w świetle opiniowanego projektu – będą kierowane do właściwych sądów okręgowych.

4. Podsumowanie

W ocenie Helsińskiej Fundacji Praw Człowieka projekt wymaga dalszych prac legislacyjnych, które dostosują go wymogów wynikających z wyroku Trybunału Konstytucyjnego, ale również do wytycznych zawartych w wyroku *Digitial Rights Ireland*. Projekt w obecnym kształcie nie wykonuje wyroku Trybunału Konstytucyjnego i całkowicie pomija wyrok Trybunału Sprawiedliwości UE, przez co jest również niezgodny z prawem Unii Europejskiej (m.in. dyrektywą 2002/58).

Helsińska Fundacja Praw Człowieka postuluje przede wszystkim o poszerzenie zakresu projektu o wytyczne wynikające z orzeczenia Trybunału Sprawiedliwości UE oraz o tezy raportu Najwyższej Izby Kontroli, tak jak czynił to projekt opracowany przez Komisję Praw Człowieka, Praworządności i Petycji. Projekt w obecnym kształcie nie realizuje wymogu zapewnienia zewnętrznej kontroli nad pozyskiwaniem danych telekomunikacyjnych. Uprzednia kontrola (sądowa) obejmuje jedynie bardzo wąski zakres danych (osób wykonujących zawody zaufania publicznego), przez co prawdopodobnie nie będzie obejmować zdecydowanej większości przypadków sięgania po te dane. Poważne wątpliwości co do skuteczności budzi także propozycja związana z fakultatywną kontrolą następczą opartą o sprawozdania służb.

Dlatego też zdaniem Fundacji należy powrócić do postulatu wyrażonego w raporcie ministra J. Cichockiego z 2011 r. powołania niezależnego organu kontrolującego pracę operacyjną służb

specjalnych. Zarówno raport, jak i projekt ustawy o Komisji Kontroli Służb Specjalnych przewidywał, że organ taki byłby powoływany przez Sejm i składał się m.in. z byłych sędziów posiadających doświadczenie w sprawach karnych. W założeniach miał on również posiadać prawo rozpatrywania skarg indywidualnych obywateli. Niestety kwestia związana ze stworzeniem skutecznego mechanizmu skargowego nie znajduje odzwierciedlenia w projekcie mimo iż wynika m.in. z art. 13 Europejskiej Konwencji Praw Człowieka[32].

Być może pewnym substytutem takiego rozwiązania byłoby skorzystanie z połączenia dwóch propozycji zawartych w projekcie Komisji Praw Człowieka, Praworządności i Petycji. Przewidywał on utworzenie w poszczególnych służbach pełnomocników ds. danych osobowych oraz umożliwienie Generalnemu Inspektorowi Ochrony Danych Osobowych prowadzenia kontroli nad służbami w zakresie udostępnienia danych telekomunikacyjnych. W ocenie Fundacji propozycja powołania kilku urzędów pełnomocników działających w ramach służb niezależnie od siebie może okazać się nie najlepszym rozwiązaniem z punktu widzenia zagwarantowania jednolitego poziomu ochrony danych osobowych we wszystkich służbach oraz nie realizuje w pełni wymogu niezależności (pomimo gwarancji istniejących na gruncie ustawy o CBA). Dlatego w ocenie Fundacji należy rozważyć umożliwienie GIODO prowadzenia kontroli nad pozyskiwaniem i przetwarzaniem danych telekomunikacyjnych przez służby. Mógłby to czynić wyszkolony w tym zakresie wyodrębniony zespół osób mających uprawnienia pozwalające na dostęp do informacji niejawnych, podlegający bezpośrednio GIODO oraz posiadający kompetencję do rozpoznawania skarg indywidualnych na działania służb.

Ponadto, projekt nie zawiera oceny skutków regulacji, m.in. dotyczących zmian w zakresie wymiaru sprawiedliwości. Projektodawca przewiduje, że sądy będą rozpatrywały sprawozdania poszczególnych służb w zakresie uzyskiwania i przetwarzania przez nich danych telekomunikacyjnych. Taki obowiązek sprawozdawczy został powiązany z fakultatywnym trybem kontroli takich sprawozdań, w szczególności poprzez zapoznanie się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych. Projektodawca nie przedstawia informacji czy będzie się to wiązało z potrzebą zapewnienia dodatkowych etatów sędziowskich oraz jak wpłynie to na obciążenie pracą sędziów. Na marginesie pragniemy również wskazać na prowadzone w Ministerstwie Sprawiedliwości prace nad ograniczeniem kognicji sądów powszechnych, których projekt nie uwzględnia.

Projekt opinii został sporządzony przez Barbarę Grabowską-Moroz w ramach programu „Monitoring procesu legislacyjnego w obszarze wymiaru sprawiedliwości" realizowanego przez Helsińską Fundację Praw Człowieka dzięki dotacji otrzymanej z programu „Obywatele dla Demokracji" finansowanego z Funduszy EOG.

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA ul. Zgoda 11 00-018 Warszawa

Z wyrazami szacunku,

Barbara Grabowska-Moroz
koordynator „Monitoringu procesu legislacyjnego w obszarze wymiaru sprawiedliwości"

dr Adam Bodnar
Wiceprezes Zarządu

32 Por.: Report on the Democratic Oversight of the Security Services (adopted by the Venice Commission, 1-2 June 2007), CDL-AD(2007)016, § 251-262.

KM 234/15
(pt. 20.07.2015)

Warszawa, dnia 16 lipca 2015 r.

KOMENDANT GŁÓWNY
STRAŻY GRANICZNEJ

BP-I-0206-[illegible]/15/MW/WP

16 LIP. 2015

Egz. nr 1

Pan Piotr Zientarski
Przewodniczący Komisji
Ustawodawczej
Senatu
Rzeczypospolitej Polskiej

Odpowiadając na pismo nr BPS/KU-034/967/11/15 z dnia 26 czerwca 2015 r. dot. projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967) przedstawiam poniżej opinię Straży Granicznej:

1) proponuję, aby zmieniany art. 9e ust. 7 w pkt 2 otrzymał brzmienie:
„2) podsłuchu lub podglądzie miejsc, środków transportu lub osób poza miejscem publicznym"

Uzasadnienie:
Przepis w brzmieniu zaproponowanym w projekcie niezasadnie wprowadza koniunkcję między wyrazami „podsłuch" i „podgląd". Kontrola operacyjna może bowiem polegać na stosowaniu zarówno odrębnie podsłuchu albo podglądu, jak i może polegać na łącznym stosowaniu podsłuchu i podglądu. Zatem właściwym jest zastosowanie w przedmiotowym przepisie alternatywy łącznej tj. spójnika „lub" zamiast koniunkcji. Ponadto w celu zachowania jednolitej nomenklatury z projektowanym art. 9e ust. 7 pkt 4, zasadnym jest posłużenie się określeniami „miejsce", „środek transportu". Jednocześnie zamiast spójnika „i" przed wyrazem „osób" należy użyć spójnika „lub", ponieważ podgląd może dotyczyć osoby i miejsca (środka transportu) łącznie lub też może dotyczyć tylko osoby albo tylko miejsca (środka transportu).

2) proponuję, aby, zmieniany art. 9e ust. 7 w pkt 3 otrzymał brzmienie:
„3) kontroli korespondencji, w tym korespondencji przesyłanej drogą elektroniczną"

Uzasadnienie:
Propozycja uzupełnienia przepisu o część dotyczącą korespondencji przesyłanej drogą elektroniczną, ma na celu wyeliminowanie ewentualnych wątpliwości, które mogą wystąpić po wejściu w życie projektowanych przepisów w zakresie możliwości stosowania kontroli operacyjnej w odniesieniu do korespondencji przesyłanej drogą elektroniczną. Tym bardziej, że takiego określenia używa się w analogicznej jak kontrola operacyjna instytucji uregulowanej w Kodeksie postepowania karnego tj. w przepisach dotyczącej procesowej kontroli i utrwalania rozmów (art. 241).

3) przepisy projektowanego art. 9e ust. 7 w sposób enumeratywny określają, na czym może polegać kontrola operacyjna. Jest to rozwiązanie dość ryzykowne biorąc pod uwagę

dynamiczny rozwój techniczny, który dostarcza ciągle nowych narzędzi wykorzystywanych w codziennym życiu człowieka. Tym bardziej, że forma otwartego katalogu znajdującego się w tych przepisach nie została zakwestionowana przez Trybunał Konstytucyjny, mimo, że przepis art. 9e ust. 7 pkt 3 był przedmiotem skargi. Trybunał stwierdził, że przepis ten, mimo, iż określa niezamknięty katalog wariantów kontroli operacyjnej, to jest on zgodny z Konstytucją, przy założeniu, że organ zarządzający kontrolę operacyjną wskazuje określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie. Na gruncie obowiązujących przepisów (art. 9e ust. 8 pkt 4 ustawy) wskazanie takiego środka następuje już we wniosku o zarządzenie kontroli operacyjnej, ponieważ przepis ten obliguje organ wnioskujący o zarządzenie kontroli operacyjnej do określenia m.in. sposobu stosowania „kontroli operacyjnej".

4) proponuję, aby, zmieniany art. 9e ust. 10 otrzymał brzmienie:
„10. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy na pisemny wniosek Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej złożony po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 1, może, również po upływie okresów, o których mowa w ust. 9, wydać postanowienie o przedłużeniu kontroli operacyjnej na czas oznaczony. Łączny czas stosowania kontroli operacyjnej nie może być dłuższy niż 18 miesięcy."

Uzasadnienie:
Projektowany przepis, ze względu na użyty zwrot: *„jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej na czas oznaczony jednak nie dłuższy niż 12 miesięcy"*, powoduje, że w przypadku, gdy zajdą okoliczności uzasadniające przedłużenie kontroli operacyjnej określone w tym ustępie, przedłużanie będzie następowało tylko jeden raz, na okres 12 miesięcy. Wydaje się, że korzystniejszym i właściwszym rozwiązaniem zarówno z punktu widzenia ochrony praw i wolności gwarantowanych przez Konstytucję, jak i efektywności w zakresie ścigania przestępstw jest określenie w przepisie maksymalnego czasu trwania kontroli operacyjnej względem danej osoby podejrzewanej o popełnienie danego przestępstwa. Tym bardziej, że zarówno w praktyce orzeczniczej (w tym również Trybunału Konstytucyjnego) jak i w doktrynie wskazuje się, jako kluczowe zachowanie (nieprzekroczenie) maksymalnego czasu stosowania kontroli operacyjnej. Gwarancyjny charakter ustawowo określonych terminów stosowania kontroli operacyjnej dotyczy bowiem kwestii łącznego czasu jej stosowania wobec danej osoby podejrzewanej o popełnienie danego przestępstwa. Wedle proponowanego wyżej przepisu art. 9e ust. 10, kontrola operacyjna na podstawie tego ustępu mogłaby być przedłużana zarówno jednokrotnie od razu na 12 miesięcy, jak i gdyby zaszła taka potrzeba byłaby przedłużana wielokrotnie na krótsze okresy (np. trzykrotnie po 4 miesiące), przy czym każdorazowo musiałby oczywiście zachodzić przesłanka do jej przedłużenia określona w tym ustępie, a łączny czas jej stosowania nie mógłby przekroczyć osiemnastu miesięcy.

5) w zakresie projektowanego art. 9e ust. 16f, kluczowym jest, aby wykonując wyrok Trybunału Konstytucyjnego, zapewnić w przepisach procedurę postępowania w sytuacji uzyskania w toku kontroli operacyjnej informacji objętych tajemnicą, o której mowa w art. 178, 178a lub 180 § 2 k.p.k., przy czym procedura ta powinna nie tylko zapewnić szybką reakcję w sytuacji zarejestrowania takich materiałów, ale także zapewnić jednocześnie zachowanie materiałów kontroli operacyjnej w formie, która nie będzie rzutowała na ich wiarygodność. Ponadto bardzo ważnym jest, aby ocena tych materiałów

była podejmowana w oparciu o wnikliwe ustalenia, które pozwolą dopiero odpowiednio sklasyfikować materiały uzyskane w toku kontroli operacyjnej.
W kontekście powyższego zasadnicze wątpliwości budzi proponowana treść art. 9e ust. 16f. Z projektowanego przepisu wynika bowiem, że materiały zawierające informacje objęte tajemnicą powinny zostać wytypowane przez organ Straży Granicznej. Powyższe nie budzi zastrzeżeń, jednakże już obowiązek dokonania ich oceny i kwalifikacji pod kątem, czy dana informacja stanowi tajemnicę, o której mowa w art. 178 lub 178a k.p.k., czy też tajemnicę, o której mowa w art. 180 § 2 k.p.k. jest zbyt daleko idący. Tym bardziej, że wskutek zakwalifikowania tych informacji jako tajemnicy wskazanej w art. 178 k.p.k. trzeba będzie dokonać ich niezwłocznego, protokolarnego i komisyjnego zniszczenia. W tym momencie pojawią się dwa problemy. Pierwszy – w jaki sposób dokonać tej oceny i klasyfikacji biorąc pod uwagę konieczność zachowania niejawności czynności operacyjno-rozpoznawczych i jednocześnie konieczność wnikliwego ustalenia ewentualnych relacji jakie łączą zarejestrowanych rozmówców. Dokonanie tych ustaleń na tak wczesnym etapie, w sposób rzetelny i jednoznaczny będzie zazwyczaj niemożliwe. Drugi problem to, kwestia wykonania niszczenia tych fragmentów rozmów, które z uwagi na ich treść zostały skalsyfikowane jako zwierające tajemnice, o których mowa w art. 178, 178a lub 180 § 2 k.p.k. Ingerencja w materiały kontroli operacyjnej, które stanowią dowody i zostały odpowiednio zabezpieczone m.in. poprzez zastosowanie sumy kontrolnej, będzie negatywnie skutkować dla ich wiarygodności. Tymczasem Trybunał Konstytucyjny w uzasadnieniu do wyroku z dnia 30 lipca 2014 r. w sprawie sygn. akt K 23/11 wskazał, że *„Konieczne jest także uregulowanie procedury raportowania z przeprowadzonych w sposób niejawny czynności i środków gwarantujących przekazanie zapisów w stanie nienaruszonym, umożliwiającym ich późniejszą weryfikację."* (uzasadnienie 5.1.3.4). Kwestia nienaruszalności materiałów kontroli operacyjnej, jako warunek jej wiarygodności dowodowej była także przedmiotem wystąpienia Prokuratora Generalnego, który w piśmie z dnia 10 maja 2010 r. (pismo nr PG VII G 502/5), określając zasady postępowania w przypadku zarejestrowania podczas kontroli operacyjnej rozmów zawierających w swej treści tajemnicę obrończą wskazał, że *„O ile bowiem sam fakt, zarejestrowania, w ramach legalnej kontroli operacyjnej lub procesowej rozmowy telefonicznej podejrzanego ze swoim obrońcą nie może być oceniany jako naruszenie wspomnianego zakazu dowodowego, o tyle za naruszenie tego zakazu należy uznać sporządzenie stenogramu z tej rozmowy, a tym bardziej wykorzystanie go w postępowaniu. Z samej bowiem technicznej specyfiki faktu rejestrowania rozmów telefonicznych, na podstawie stosownej decyzji sądu, wynika, iż może dojść do zarejestrowania również rozmowy podejrzanego ze swoim obrońcą. Jednak prokurator, jako prowadzący lub nadzorujący postępowania, jest odpowiedzialny za to, by treść tej rozmowy nie została w jakikolwiek sposób poznana, a przede wszystkim ujawniona, by stenogram takiej rozmowy nie został w szczególności sporządzony i włączony do akt prowadzonego postępowania przygotowawczego. Oczywistym przy tym jest, iż nie jest możliwa jakakolwiek ingerencja w techniczny zapis rozmowy na nośniku informatycznym, np. wykasowanie tej rozmowy."*. Należy podkreślić, że wobec konieczności zachowania wiarygodności uzyskanych materiałów, problematyczne będzie nie tylko zniszczenie rozmów telefonicznych (w szczególności problem będzie stanowić sytuacja, gdy np. w ramach jednego połączenia, z telefonu korzystała więcej niż jedna osoba, przy czym jedna z tych osób prowadziła rozmowę, która może być objęta tajemnicą), ale także, gdy w ramach podglądu i podsłuchu zarejestrowano spotkanie, w którym uczestniczyło kilka osób i podczas tego spotkania przeplatały się w prowadzonych rozmowach różne wątki, w tym również takie, co, do których zachodzi przypuszczenie, że mogą stanowić tajemnicę.

Biorąc pod uwagę powyższe, krytycznie należy ocenić propozycję wynikającą z projektu, aby to organ Straży Granicznej dokonywał ostatecznej oceny materiałów kontroli operacyjnej pod kątem wstępowania w nich treści stanowiących tajemnice, o których mowa

w art. 178, 178a lub 180 § 2 k.p.k. i następnie dokonywał ich niszczenia, jeśli stwierdzi, że jest to tajemnica, o której mowa w art. 178 lub 178a k.p.k. albo przekazywał materiały prokuratorowi, jeśli zawierają tajemnice, o których mowa w art. 180 § 2 k.p.k.
W naszej ocenie, projektowane przepisy powinny określać następujący sposób postępowania z materiałami z kontroli operacyjnej. W przypadku stwierdzenia przez organ Straży Granicznej, że zachodzi uzasadnione przypuszczenie, że w zarejestrowanych materiałach kontroli operacyjnej znajdują się informacje mogące stanowić tajemnicę, o której mowa w art. 178, 178a lub 180 § 2 k.p.k., przekazując po zakończeniu kontroli operacyjnej materiały prokuratorowi wskazywałby on fragmenty, które mogą zawierać te informacje, nie sporządzając jednocześnie z tej części rozmów pisemnej dokumentacji w postaci komunikatów. Po przekazaniu materiałów, ponownej oceny pod kątem występowania w nich ww. tajemnic powinien dokonać prokurator, który w zależności od wyników przeprowadzonej oceny decydując o potrzebie ich ewentualnego wykorzystania w postępowaniu karnym, powinien występować do sądu z wnioskiem o wydanie postanowienia wyrażającego zgodę na ich wykorzystanie, jako dowody w postępowaniu karnym albo o zarządzenie przez sąd ich zniszczenia. W przypadku niewyrażenia zgody, sąd powinien wskazywać fragmenty kontroli operacyjnej, które powinny zostać zniszczone. Dopiero na tej podstawie organ Straży Granicznej powinien dokonywać niszczenia materiałów w części zawierającej tajemnice, o których mowa w art. 178, 178a, 180 § 2. Przy czym niszczenie materiałów powinno być poprzedzone wykonaniem kopi zarejestrowanych materiałów w części niezwierającej informacji stanowiących tajemnice, o których mowa w art. 178, 178a lub 180 § 2 k.p.k.

Niezależnie od powyższych uwag i propozycji, jeśli chodzi o treść projektowanego art. 9e ust. 16f, w pkt 1 tego ustępu należy uwzględnić zawierający bezwzględny zakaz dowodowy art. 178a dodany nowelizacją Kodeksu postępowania karnego, która weszła w życie z dniem 1 lipca 2015 r. Ponadto przepis tego punktu powinien jednoznacznie wskazywać, że niszczenie materiałów dotyczy tej ich części, która zawiera informacje objęte tajemnicą, o której mowa a w art. 178 lub 178a k.p.k. Przepis ten powinien, zatem otrzymać brzmienie:

„1) zawierają informacje, o których mowa w art. 178 lub 178a Kodeksu postepowania karnego – Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej nakazują ich niezwłoczne, komisyjne i protokolarne zniszczenie w części, w jakiej zawierają te informacje;"

6) w zakresie projektowanego art. 9e ust. 16g, w celu sprecyzowania, że przedmiotem wniosku, a następnie decyzji sądu są informacje objęte tajemnicami, przepisy pkt 1 i 2 powinny otrzymać brzmienie:

„1) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym w części, w jakiej zwierają informacje, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym, i protokolarnym zniszczeniu w części, w jakiej zwierają informacje, o których mowa w art. 180 § 2 Kodeksu postępowania karnego"

7) w zakresie projektowanego art. 9e ust. 16h proponuję, aby, przepis otrzymał brzmienie:
„16h. Sąd w terminie 14 dni od złożenia wniosku przez prokuratora wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego albo zarządza ich zniszczenie."

Uzasadnianie:
W dodawanym ust. 16h należy doprecyzować, że 14 dniowy termin to czas określony dla sądu na wydanie postanowienia w przedmiocie niszczenia materiałów mogących zawierających tajemnice, a nie czas na wykonanie zarządzonego niszczenia przez organ Straży Granicznej. Ponadto w przepisie tym powinna być mowa o materiałach zawierających takie informacje, ponieważ sąd ten fakt już wówczas stwierdzi. Wydaje się, że przepis ten powinien zostać także uzupełniony o regulację dotyczącą przypadku, gdy sąd na tym etapie stwierdzi, że nie jest to tajemnica, o której mowa w art. 180 § 2, klasyfikując jednocześnie te materiały, jako informacje objęte tajemnicą, o której mowa w mowa w art. 178 lub 178a k.p.k.
Ponadto treść projektowanego ustępu należy uzupełnić o przepis określający prawo prokuratora do wniesienia zażalenia na decyzję sądu.

8) przepisy art. 9e ust. 19a projektu, zgodnie z uzasadnieniem, stanowić mają m. in. przeniesienie do materii ustawowej regulacji określającej, co stanowi dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej. Omawiana jednostka redakcyjna wprowadza do art. 9e ustawy o Straży Granicznej, wcześniej niewystępujące pojęcie „**dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej**". Analiza treści projektowanych ust. 19a-19c nie pozostawia wątpliwości, iż proponowany zabieg legislacyjny w sposób jednoznaczny różnicuje:
   a) *„materiały zgromadzone podczas stosowania kontroli operacyjnej"*, o jakich mowa w obowiązujących przepisach art. 9e w: ust. 4 pkt 2, ust. 11, ust. 16, ust. 16d, ust. 17 i ust. 18 od
   b) *„dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej"*, o jakich mowa w projektowanych przepisach ust. 19a-19c.

   Zróżnicowanie to wydaje się jednak mieć daleko idące konsekwencje negatywnie wpływające na całokształt uregulowań zawartych w art. 9e ustawy o Straży Granicznej. Należy mieć bowiem na uwadze iż, nowoprojektowany ust. 19a jako dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej wymienia:
   1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
   2) kopie wykonane z nośników, o których mowa w pkt 1;
   3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach lub ich kopiach, o których mowa w pkt 1 i 2.

   Jednocześnie zgodnie z nowoprojektowanym ust. 19b, ww. dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w ust. 16 – niezwłocznie po przekazaniu prokuratorowi materiałów, które dokumentuje, zaś w przypadku, o jakim mowa w ust. 18 – wraz z tymi materiałami.
   W tym miejscu należy zadać sobie pytanie, w jakiej formie organ realizujący kontrolę operacyjną przekazuje prokuratorowi „wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej"? Odpowiedź na to pytanie wydaje się oczywista. Biorąc pod uwagę istotę czynności stanowiących kontrolę operacyjną, materiały uzyskane podczas jej stosowania muszą być utrwalone na nośnikach lub w dokumentach sporządzonych na ich podstawie (komunikaty, streszczenia, tłumaczenia).
   Mając na uwadze powyższe, możliwość rozgraniczenia materiałów zgromadzonych podczas stosowania kontroli operacyjnej od „dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej" (w rozumieniu ust 19a), wydaje się iluzoryczna.

Jako przykład podać można kontrolę operacyjną polegającą na podglądzie i podsłuchu osób w określonym pomieszczeniu. Zapis obrazu i dźwięku rejestrowany jest w takim przypadku na dysku, w który wyposażone jest urządzenie użyte do realizacji kontroli. Dysk ten, zabezpieczony przed nieuprawnioną ingerencją w dane na nim zapisane, wraz z dokumentami sporządzonymi na podstawie informacji utrwalonych na dysku, przekazywany jest prokuratorowi w przypadku, o którym mowa w ust. 16 art. 19e ustawy o Straży Granicznej. W tej sytuacji przepisy projektowanego ust. 19b byłyby bezprzedmiotowe. Podobnie w przypadku zaistnienia sytuacji określonej w ust. 18 zapisy informacji utrwalone na dysku, stanowiące materiały zgromadzone podczas stosowania kontroli (lub cały dysk) podlegają protokolarnemu, komisyjnemu zniszczeniu. Nie ma więc możliwości ani potrzeby niszczenia *„dokumentacji materiałów zgromadzonych podczas stosowania kontroli"*, ponieważ nie ma potrzeby jej wytwarzania (ust 19b pkt 2).
Powyższe uwagi mają analogiczne zastosowanie do projektowanego ust 19c.
W związku z powyższym w celu ujednolicenia terminologii stosowanej w obrębie art. 9e proponuję jednostce redakcyjnej oznaczonej lit. g w pkt 1 art. 2 projektu ustawy nadać następujące brzmienie:

g) po ust. 19 dodaje się ust. 19a w brzmieniu:

„19a. Materiały zgromadzone podczas stosowania kontroli operacyjnej stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji, wyniki podsłuchu i podglądu albo treści korespondencji lub zawartość przesyłek;

2) kopie wykonane z nośników, o których mowa w pkt 1;

3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach lub ich kopiach, o których mowa w pkt1 i 2."

W przypadku uwzględnienia przytoczonej powyżej propozycji brzmienia przepisu projektowane przepisy ust. 19b staną się zbędne, jako powtórzenie unormowań obecnie obowiązujących w obrębie art. 9e ust. 16 i 18, zaś zapisy ust. 19c staną się zbędne, jako wcześniej uregulowane w projektowanych ust. 16f-16i. W przypadku uwzględnienia przytoczonej powyżej propozycji zbędnymi staną się także przepisy art. 14 projektu oraz zmianie ulec powinien przepis art. 9e ust. 20 pkt 3 w zakresie, w jakim mówi *o „sposobie dokumentowania materiałów"*.

9) w projektowanym art. 10b w ust. 2 w pkt 1 proponuję zastąpienie określenia „funkcjonariuszowi Straży Granicznej" określeniem „funkcjonariuszowi". Zapewni to jednolitość przepisów stosowanych w obrębie tego ustępu.

10) w projektowanym art. 10b ust. 5 i 6 proponuję nadać brzmienie:

„5. Jeżeli materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, zawierają dowody mające znaczenie dla postepowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazuje je właściwemu miejscowo lub rzeczowo prokuratorowi. W postepowaniu przed sądem, w odniesieniu do tych materiałów, stosuje się odpowiednio art. 393 § 1 zdanie pierwsze Kodeksu postepowania karnego.

6. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają dowodów mających znaczenie dla postepowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.".

Zaproponowane zmiany zapisów przedmiotowych jednostek redakcyjnych wynikają bezpośrednio z zaleceń Trybunału Konstytucyjnego, który wyraził pogląd, iż *„ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych"*. Niezależnie od tego zastosowane w projektowanym brzmieniu ust. 5 i 6 art. 10b, zapisy o treści: *„materiały uzyskane* ***w wyniku czynności związanych z udostępnieniem danych****, o których mowa w ust. 1 ..."* budzą istotne wątpliwości interpretacyjne, co do zakresu przekazywanych bądź niszczonych materiałów. Zarówno aktualnie obowiązujące uregulowania art. 10b w ust. 5 i 6 jak i powyżej zaproponowane brzmienie przepisu, wydają się precyzyjnie określać, iż niszczeniu podlegają materiały zawierające uzyskane dane, o jakich mowa w ust. 1 art. 10b. Zastosowane w projekcie przepisy rozszerzają zaś zakres przekazywanych bądź niszczonych materiałów o bliżej nieokreślone materiały uzyskane w wyniku czynności związanych z udostępnieniem danych.

11) w projektowanym art. 10b w ust. 8 proponuję usunąć fragment o treści: *„oraz materiały, o których mowa w ust. 6"*. Powyższe wynika z zaproponowanego powyżej brzmienia ust. 6 gdzie przewidziano już niezwłoczne, protokolarne i komisyjne zniszczenie materiałów. W aktualnym brzmieniu projektu ust. 6 również przewiduje niezwłoczne, protokolarne i komisyjne zniszczenie opisanych w nim materiałów. Wymienienie w ust. 8 materiałów, o których mowa w ust. 6 przeczy potrzebie niezwłocznego niszczenia zbędnych danych uzyskanych w wyniku czynności podjętych na podstawie ust. 2.

12) w projektowanym art. 10ba ust. 1 proponuję nadać brzmienie:
„1. Jeżeli z materiałów, o których mowa w art. 10b ust 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postepowania karnego, o okoliczności tej, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej informuje prokuratora."

Uzasadnienie:
Zaproponowane brzmienie przepisu wynika z faktu, iż zastosowane w ust. 1 art. 10ba odesłanie do materiałów, o których mowa w art. 10b ust. 5, wskazuje wystarczająco na obowiązek przekazania prokuratorowi materiałów zawierających informacje mające znaczenie dla postępowania karnego. Z tych tez względów przepis ust. 1 w art. 10ba, w jego aktualnym brzmieniu jest zbędny, jako normujący kwestię uregulowaną wcześniej.

13) w projektowanym art. 10ba w ust. 3 końcowy zapis o treści *„w terminie 14 dni od dnia złożenia wniosku przez prokuratora"* proponuję przenieść na początek tej jednostki redakcyjnej. Proponowany zabieg legislacyjny poprawi czytelność zapisów tego ustępu, wyraźnie wskazując, iż termin ten przeznaczony jest dla sądu. Przepis posiadłaby wówczas brzmienie analogiczne jak zaproponowany w pkt 7.
Niezależnie od powyższego zasadnym jest doprecyzowanie, iż sąd zarządza komisyjne i protokolarne zniszczenie materiałów zawierających dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postepowania karnego. Bez tego doprecyzowania zastosowanie ust. 3 art. 10ba doprowadzi do zniszczenia nie tylko materiałów zawierających dane, o których mowa w ust. 1 (tj. dotyczących

bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego), ale wszystkich przekazanych materiałów zawierających informacje mające znaczenie dla postępowania karnego, (ust. 3 zawiera odesłanie do ust. 1, ten zaś odsyła do art. 10b ust. 5).

14) projektowany art. 10ba w ust. 4 nakłada na organ SG obowiązek poinformowania sądu o wykonaniu zarządzenia sądu, o którym mowa w projektowanym art. 10ba ust. 3, z czego może pośrednio wynikać, iż to organ SG ma wykonać przedmiotowe zarządzenie, podczas gdy przepisy nie normują kwestii „zwrotnego" przekazywania materiałów, skierowanych przez prokuratora do sądu, w oparciu o projektowany przepis art. 10ba ust. 2.

15) w projektowanych art. 10ba, 10bb i 10bc używa się określenia „organ Straży Granicznej", podczas gdy w poprzedzających je przepisach jest mowa o Komendancie Głównym Straży Granicznej i komendancie oddziału Straży Granicznej. Wydaje się, że dla jasności uregulowań należałoby używać jednolicie pojęć: „Komendant Główny Straży Granicznej" i „komendant oddziału Straży Granicznej".

16) w projektowanym art. 10bc ust. 2 – podobnie jak w projektowanym brzmieniu art.10bb ust. 1 jest mowa o organie SG, który wystąpił z wnioskiem, podczas gdy zgodnie z art. 10b ust. 1 ustawy o SG, tryb, w którym organ SG występuje z wnioskiem, jest jednym z trzech trybów udostępniania danych telekomunikacyjnych. Ponadto proponuję doprecyzować, co należy rozumieć pod pojęciem „rodzaje przestępstw", którym posłużono się w pkt 3 analizowanego ustępu – czy autorom chodziło o wskazanie konkretnego przepisu karnego, czy o rodzajowe ujęcie grup przestępstw, w związku z zaistnieniem których wystąpiono o dane. Również w pkt 4 jest mowa o „liczbie przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane, co wydaje się wymagać wyjaśnienia. Taki podział spraw może mieć miejsce np. na gruncie projektowanych przepisów ustawy o Policji, gdzie przepisy przewidują możliwość uzyskiwania danych telekomunikacyjnych nie tylko w celu rozpoznawania, zapobiegania, wykrywania i zwalczania przestępstw.

Z poważaniem

gen. dyw. SG Dominik TRACZ

Zastępca Komendanta Głównego
Straży Granicznej

gen. bryg. SG Andrzej Pilaszkiewicz

Wyk. MW/WP, tel. 40-16, 40-29
Egz. nr 1- adresat
Egz. nr 2- a/a
Data 16 lipca 2015 r.

Ku 239/15

PREZES
NACZELNEJ RADY ADWOKACKIEJ
Andrzej Zwara

Warszawa, dnia 20 lipca 2015 roku

Ku/239

Szanowny Pan
Piotr Zientarski
Przewodniczący
Komisji Ustawodawczej
Senat RP

NRA-12-ST-1.9.2015

Szanowny Panie Przewodniczący,

W załączeniu uprzejmie przesyłam *Opinię Naczelnej Rady Adwokackiej do senackiego projektu ustawy o zmianie ustawy o policji oraz niektórych innych ustaw (Druk senacki Nr 967)* oraz do wiadomości pismo adresowane do Pani Ewy Kopacz, Prezesa Rady Ministrów.

Z poważaniem

Załączniki:

- Opinia Naczelnej Rady Adwokackiej do senackiego projektu ustawy o zmianie ustawy o policji oraz niektórych innych ustaw (Druk senacki Nr 967).
- Kopia pisma do Pani Ewy Kopacz, Prezesa Rady Ministrów.

OPINIA NACZELNEJ RADY ADWOKACKIEJ DO SENACKIEGO PROJEKTU USTAWY O ZMIANIE USTAWY O POLICJI ORAZ NIEKTÓRYCH INNYCH USTAW (DRUK SENACKI NR 967)

I. Uwagi ogólne

Opiniowany senacki projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)(dalej: Projekt) jak wskazuje się w jego uzasadnieniu, ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2015 r. sygn. K 23/11. Dostosowanie to ma polegać na wprowadzeniu zmian w obowiązujących przepisach, których niekonstytucyjność orzekł Trybunał Konstytucyjny, ale i w zakresie tych regulacji, gdzie mimo niestwierdzenia niezgodności z Konstytucją RP, dostrzeżone zostały pewne problemy interpretacyjne i praktyczne.

Przykładem jest tu proponowana w Projekcie zmiana brzmienia przepisów regulujących zakres środków możliwych do stosowania w ramach kontroli operacyjnej. Trybunał Konstytucyjny orzekł tu, że przepisy art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną wskazuje określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji RP. Wątpliwości budzić musi proponowany sposób określenia katalogu tych środków jako: podsłuch rozmów prowadzonych przy użyciu środków technicznych; podsłuch i podgląd pomieszczeń i osób poza miejscami publicznymi; kontrola treści korespondencji; nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu[1]. Wydaje się, że katalog

[1] Obecnie w ramach kontroli operacyjnej możliwe jest stosowanie: kontroli treści korespondencji; kontroli zawartości przesyłek; stosowanie środków technicznych umożliwiających uzyskiwanie w *sposób niejawny*

ten jest niezbyt precyzyjnie określony[2], zwłaszcza w kontekście ostatnich doniesień[3] na temat stosowania przez CBA narzędzia „Remote Control System". Ma ono umożliwiać monitorowanie komputerów i telefonów, pozyskiwanie danych przechowywanych na tych urządzeniach, nawet w sytuacji gdy użytkownik nie jest podłączony do Internetu oraz śledzenie korespondencji w Internecie. Rodzi się wątpliwości, czy projektowana definicja środków możliwych do stosowania kontroli operacyjnej, umożliwiać będzie korzystanie z tego typu narzędzi.

Należy jednocześnie podkreślić, że Projekt w ogóle nie wykonuje postanowienia sygnalizacyjnego Trybunału Konstytucyjnego z dnia 25 stycznia 2006 r. sygn. S 2/06, wydanego w następstwie wyroku z 12 grudnia 2005 r. sygn. K 32/04. Trybunał Konstytucyjny wskazał tu na potrzebę uregulowania obowiązku informowania osób objętych kontrolą operacyjną o fakcie jej prowadzenia. W uzasadnieniu Projektu (s. 5) twórcy projektu wskazują, że Trybunał Konstytucyjny dostrzega problem braku w obowiązujących przepisach obowiązku po stronie Policji i służb obowiązku poinformowania po zakończeniu czynności operacyjno – rozpoznawczych osoby, która tego typu czynnościom została poddana. Jednakże ich zdaniem, wprowadzenie tego typu regulacji w przepisach ww. ustaw policyjnych, stanowiłoby naruszenie reguł, na podstawie których działają służby i mogłoby osłabić ich skuteczność, jak i kłóciłoby się z ustawowym obowiązkiem ochrony form i metod ich działania. Wobec jasnego stanowiska przedstawionego przez Trybunał Konstytucyjny zarówno w wyroku z 12 grudnia 2005 r. oraz postanowieniu sygnalizacyjnym z 25 stycznia 2006 r. i okoliczności, że obowiązek takiego informowania ma silną konstytucyjną podstawę

---

informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, a także w przypadku niektórych służb rejestrowanie obrazu.

[2] W piśmiennictwie można spotkać bardziej precyzyjne określenie katalogu tych środków. A. Biernaczyk wskazuje, że do tego katalogu środków należą: podsłuchu w pomieszczeniu (PP), podsłuchu telefonu stacjonarnego (PT), podsłuchu telefonu komórkowego (PTK), podsłuchu faksu (PTFax), podglądu przy wykorzystaniu urządzeń do rejestracji obrazu i dźwięku (PDF), kontrolowania korespondencji w sieci internetowej (KKI), kontrolowania treści korespondencji pisemnej (KK), kontrolowania zawartości przesyłek (KZP). Zob. A. Biernaczyk, *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b ustawy z dnia 6 kwietnia 1990 r. o Policji* (w:) *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 116. O wiele bardziej precyzyjna była też propozycja przedstawiona w poselskim projekcie ustawy o czynnościach operacyjno – rozpoznawczych (Sejm VI kadencji, druk sejmowy nr 353).

[3] http://www.tokfm.pl/blogi/panoptykon/2015/07/legalne_ale_tajne_analiza_kontrowersji_wokol_rcs/1.

w art. 51 ust. 4 Konstytucji RP, takie stanowisko twórców Projektu musi spotkać się z dezaprobatą[4].

Ponadto krytycznie należy ocenić brak w Projekcie propozycji powołania zewnętrznego, eksperckiego organu, który odpowiadał by za kontrolę działalności służb z perspektywy respektowania praw i wolności konstytucyjnych[5].

II. Uwagi szczegółowe

Kontrola operacyjna a ochrona tajemnic prawnie chronionych

W wyroku z 30 lipca 2014 r. Trybunał Konstytucyjny orzekł, że art. 19 ustawy o Policji, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 17 ustawy o Centralnym Biurze Antykorupcyjnym **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**, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP.

Wykonując to rozstrzygnięcie Projekt wprost wskazuje, że w ramach kontroli operacyjnej może dochodzić do utrwalania treści zawierających chronione jako tajemnica zawodowa, w tym tak adwokacka, jak i obrończa. Z Projektu wynika bowiem w sposób oczywisty, że osoby obowiązane do ochrony tajemnicy obrończej i adwokackiej, nie są wykluczone spod działania

---

[4] Należy zauważyć, że podobny postulat dotyczący przekazania informacji o pozyskaniu danych telekomunikacyjnych, zainteresowanemu abonentowi, został wyrażony przez Najwyższą Izbę Kontroli przy okazji kontroli pt. „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne".

[5] Taki postulat poruszany jest w dyskusji nad problematyką kontroli nad działalnością służb specjalnych. Por. sprawozdanie z konferencji „Jak daleko sięgnie państwo? Retencja danych, bilingi, inwigilacja a gwarancje praw i wolności obywatelskich" w dniu 10 grudnia 2014 r. organizowanej przez Naczelną Radę Adwokacką oraz Krajową Radę Radców Prawnych dostępne na stronie: http://www.adwokatura.pl/z-zycia-nra/polsce-potrzebny-jest-niezalezny-organ-kontroli-retencji-danych/.

przepisów o kontroli operacyjnej. Projekt zakłada natomiast obowiązek dokonywania przez funkcjonariuszy prowadzących kontrolę operacyjną oceny, czy materiały w jej ramach zgromadzone zawierają dane objęte tajemnicą, o której mowa w art. 178 k.p.k. czy też tajemnicą, o której mowa w art. 180 § 2 k.p.k. W przypadku stwierdzenia, że chodzi o tajemnicę obrończą aktualizuje się obowiązek zniszczenia zgromadzonych danych. W przypadku zaś danych chronione jako tajemnica adwokacka, funkcjonariusz ma przekazać je prokuratorowi, a ten niezwłocznie będzie musiał wystąpić do sądu, celem wydania: 1) postanowienia o wyrażeniu zgody na wykorzystanie ich w postępowaniu karnym, albo 2) zarządzenia o niezwłocznym, komisyjnym i protokolarnym ich zniszczeniu.

Rozwiązanie, w którym to funkcjonariusz danej służby – zainteresowany wszczęciem i prowadzeniem postępowania karnego o przestępstwo, na którego okoliczność prowadzona jest kontrola operacyjna - ma ocenić czy zgromadzony materiał zawiera treści chronione jako tajemnica obrończa lub adwokacka należy ocenić krytycznie. Przede wszystkim, istnieje ryzyko, że z uwagi na wczesny – zazwyczaj przed procesowy charakter czynności operacyjno – rozpoznawczych, do których zalicza się kontrola operacyjna - materiał dotyczący każdego poufnego kontaktu adwokata z „figurantem", niebędącym formalnie jeszcze podejrzanym, uznawany będzie za niezawierający informacji chronionych, tudzież zawierający informacje objęte tajemnicą, o której mowa w art. 180 § 2 k.p.k. Taka praktyka w oczywisty sposób naruszać będzie prawo do obrony, które aktualizuje się z chwilą zgłoszenia się klienta do adwokata, nie zaś formalnego przedstawienia zarzutów. Ponadto w sytuacji, gdy kontrola operacyjna prowadzona będzie wobec osoby nieoznaczonej „NN", nie będzie możliwe ustalenie, czy zgromadzone materiały chronione są jako jedna z tajemnic zawodowych.

Krytycznie odnieść się należy także do proponowanego mechanizmu zwalniania z tajemnicy. Tryb ten zakłada poinformowanie aż dwóch podmiotów (prokuratora i sądu) o fakcie zarejestrowania w ramach kontroli operacyjnej materiałów chronionych jako tajemnica, o której mowa w art. 180 § 2 k.p.k. Zastrzeżenie budzi okoliczność, że funkcjonariusz nie będzie mógł sam zarządzić zniszczenia materiałów, zawierających dane objęte ochroną tajemnicy z art. 180 § 2 k.p.k. jak i wystąpić do sądu o podjęcie decyzji w sprawie zniszczenia lub wykorzystania tych materiałów, tylko musi je przekazać prokuratorowi. Niezrozumiała jest rola prokuratora, który wnioskuje jedynie do sądu o podjęcie decyzji w przedmiocie tych

danych. Procedura w tym kształcie powoduje, że taka chroniona na podstawie art. 180 § 2 k.p.k. treść stanie się znana różnym podmiotom. Ponadto proponowane regulacje w przeciwieństwie do art. 180 § 2 k.p.k.[6] nie przewidują jakichkolwiek przesłanek, którymi kierować powinien się sąd podejmując decyzję o wykorzystaniu informacji, co stwarza ryzyko decyzji arbitralnych w tym zakresie.

Krytycznie należy ocenić też sytuację, że projekt nigdzie nie przewiduje, by postanowienie o wyrażeniu zgody na wykorzystanie materiałów zawierających tajemnicę prawnie chronioną, miało by zawierać uzasadnienie. Stanowiące wzór dla tej instytucji, postanowienie wydane na podstawie art. 180 § 2 k.p.k. uzasadnienie takie natomiast zawiera.

Wreszcie Projekt nie przewiduje możliwości złożenia zażalenia przez osobę obowiązaną do ochrony tajemnicy obrończej i adwokackiej, na postanowienie o wykorzystaniu w postępowaniu karnym materiałów zawierających tą tajemnicę.

Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. odnosząc się do kwestii ochrony tajemnic prawnie chronionych i braku regulacji nakazujących niszczenie materiałów tę tajemnicę zawierających, wskazał, że zbliżone w swej istocie rozwiązania legislacyjne (do art. 180 § 2 k.p.k.) powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Zdaniem Trybunału Konstytucyjnego nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym, wręcz przeciwnie, standardy te – z uwagi na niejawność kontroli oraz jej ponadprocesowy charakter – powinny być co najmniej zbieżne ze standardami w postępowaniu karnym. W ocenie Naczelnej Rady Adwokackiej, wykonanie wyroku Trybunału Konstytucyjnego, w proponowanym kształcie tego wskazania Trybunału Konstytucyjnego nie realizuje, gdyż proponowany standard ochronny jest niższy niż obowiązujący na gruncie art. 180 § 2 k.p.k.

Pozyskiwanie danych telekomunikacyjnych a ochrona tajemnic zawodowych

[6] W art. 180 § 2 k.p.k. przesłankami zwolnienia z tajemnicy jest niezbędność dla dobra wymiaru sprawiedliwości oraz niemożliwość ustalenia danej okoliczności na podstawie innego dowodu.

Projekt wprowadza zmiany w przepisach ww. ustaw policyjnych, zasad pozyskiwania danych telekomunikacyjnych, o których mowa w art. 180c i 180d Prawo telekomunikacyjne. Jednakże mimo, że w uzasadnieniu wskazuje się, iż propozycja stanowi doprecyzowanie tychże zasad, to trudno nie oprzeć się wrażeniu, że proponowane ramy ustawowe będą stwarzać niezwykle szeroką możliwość pozyskania przedmiotowych danych. Jest to szczególnie widoczne w przypadku Policji, gdzie pozyskiwanie danych może dotyczyć ogólnie „przestępstw ściganych z oskarżenia publicznego". Oznacza to zaprzeczenie, celów jakim służyło wprowadzenie możliwości pozyskiwania danych telekomunikacyjnych, tj. zwalczanie szczególnie poważnych przestępstw i zagrożeń terrorystycznych. Twórcy projektu zrezygnowali przy tym ze wskazania w przepisach, że do pozyskania danych telekomunikacyjnych będzie dochodzić w warunkach subsydiarności, czyli tylko wtedy, gdy inne środki okazały się nieskuteczne.

Projektowane przepisy sankcjonują przy tym sytuację, gdy w ramach pozyskania danych telekomunikacyjnych, dochodzi do zebrania informacji o osobach, zobowiązanych na podstawie art. 180 § 2 k.p.k. do ochrony tajemnicy zawodowej. Projekt przewiduje, że w przypadku danych już zebranych, na wniosek prokuratora, któremu będą one przekazywane, sąd będzie rozstrzygać o możliwości ich wykorzystania lub konieczności ich zniszczenia. W sytuacji zaś, gdy dane mają zostać dopiero zebrane, sąd ma zdecydować o zgodzie na ich pozyskanie, chyba, że zajdzie przypadek „niecierpiący zwłoki", kiedy to funkcjonariusz będzie jednocześnie występował do operatora o przekazanie danych i występował do sądu o zgodę na ich wykorzystanie.

Kształt projektowanych przepisów musi niepokoić. Twórcy projektu z jednej strony przyjęli, że pozyskanie danych telekomunikacyjnych może naruszać co najwyżej tajemnicę z art. 180 § 2 k.p.k. Nie zauważają przy tym jednej istotnej okoliczności, iż zakres możliwych do pozyskania danych telekomunikacyjnych, jest tak szeroki, że na jego podstawie możliwe jest bieżące monitorowanie działalności osoby odpowiedzialnej do ochrony tajemnicy zawodowej, w szczególności tego, gdzie, z kim, w jakich godzinach, jak często, nawiązuje ona relacje z klientem.

Nie jest jasne przy tym, jak należy rozumieć użyte w Projekcie sformułowanie, iż dane mają *„bezpośrednio dotyczyć osoby wykonującej zawód lub funkcję, o której mowa w art. 180 § 2 k.p.k."* Literalnie wykładając ten przepis dojść należy do wniosku, że jego dyspozycja jest spełniona, gdy wniosek o pozyskanie danych dotyczy numeru abonenckiego, którego użytkownikiem jest osoba obowiązana do zachowania tajemnicy. Co jednak w sytuacji, gdy przy okazji, na zasadzie ekscesu zebrane zostaną dane dotyczące takiej osoby. Wydaje się, że także i w takiej sytuacji takie dane telekomunikacyjne podlegają ochronie jako tajemnica zawodowa.

Krytycznie odnieść należy się też do przyznania w Projekcie możliwości złożenia zażalenia na postanowienie sądu o braku zgody na pozyskanie danych telekomunikacyjnych osoby zobowiązanej do ochrony tajemnicy zawodowej organowi, który wystąpił o wyrażenie zgody i braku takiego środka odwoławczego dla osoby, której te dane dotyczą w przypadku wydania przez sąd postanowienia o możliwości wykorzystania lub przyszłego pozyskania tych danych.

Generalnie też krytycznie należy ocenić propozycję by pozyskiwanie danych telekomunikacyjnych tak jak dotychczas nie podlegało żadnej uprzedniej, zewnętrznej kontroli. Skutecznym mechanizmem kontroli nie będzie na pewno, projektowane wprowadzenie obowiązku sprawozdawczego wobec sądów. Powziąć należy w szczególności wątpliwość co do tego, czy na podstawie przekazanego sprawozdania – w takim kształcie jak proponowane w Projekcie – sąd będzie miał możliwość skontrolowania prawidłowości pozyskania danych do konkretnej sprawy.

III. Konkluzje

Projekt nie realizuje postulatów płynących z wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. w stopniu wystarczającym. Projektowane regulacje przede wszystkim nie wprowadzają efektywnych mechanizmów nadzoru i kontroli nad stosowaniem kontroli operacyjnej oraz pozyskiwaniem danych telekomunikacyjnych przez służby.

W szczególności świadczą o tym propozycje stworzenia mechanizmu weryfikacji, czy zgromadzone dane dotyczą okoliczności chronionych jako tajemnica zawodowa. Przewidują one bowiem, że decyzja co do zakresu ochrony tych informacji, podejmowana ma być arbitralnie i nie będzie podlegać kontroli przez osoby obowiązane do zachowania tajemnicy zawodowej.

PREZES
NACZELNEJ RADY ADWOKACKIEJ
Andrzej Zwara

Warszawa, dnia 20 lipca 2015 roku

Szanowna Pani
Ewa Kopacz
Prezes Rady Ministrów

NRA-12-ST-1.9.2015

Szanowna Pani Premier,

W związku z planowanym na dzień 21 lipca 2015 r. rozpoczęciem przez senackie Komisje Praw Człowieka, Praworządności i Petycji oraz Ustawodawczą prac nad projektem ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967), Naczelna Rada Adwokacka apeluje o wstrzymanie tych prac. Projekt w aktualnej postaci godziłby w prawa i wolności jednostki, stwarzając możliwości inwigilacji obywateli bez właściwego nadzoru oraz niedopuszczalnej ingerencji przez służby specjalne i policyjne w służące ochronie praw i wolności tajemnice zawodowe, szczególnie tajemnicę obrończą, adwokacką i radcowską.

Rzeczony projekt nowelizacji stanowi w ocenie Naczelnej Rady Adwokackiej próbę nieprawidłowego wykonania wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. **Projekt nie wprowadza rzetelnych i skutecznych mechanizmów zewnętrznej kontroli nad działalnością Policji oraz służb w zakresie stosowania czynności operacyjno-rozpoznawczych** (do których zalicza się m.in. kontrolę korespondencji, utrwalanie rozmów telefonicznych, pozyskiwanie danych telekomunikacyjnych).

Projekt ten **wprowadza także niepożądane w demokratycznym państwie prawnym, głębokie ograniczenia w zakresie ochrony tajemnic zawodowych,** w tym tej, której piastunem jest adwokat. W świetle projektowanych propozycji adwokaci będą mogli być poddawani najbardziej ingerencyjnym środkom pracy operacyjnej, tj. kontroli operacyjnej oraz pozyskiwaniu danych telekomunikacyjnych. Rozwiązanie to godzi w zaufanie obywateli wobec państwa i stanowi poważne ograniczenie w korzystaniu z ich praw i wolności konstytucyjnych. Projekt wprowadza w tym zakresie mechanizm zakładający, że to funkcjonariusz służby policji lub służb specjalnych, np. po zarejestrowaniu rozmowy adwokata z klientem, będzie oceniał, czy informacje z tej rozmowy chronione są tajemnicą

obrończą, czy też tajemnicą adwokacką. Zgodnie zatem z projektem, to funkcjonariusze policji i służb specjalnych, nie zaś adwokat, władni będą rozstrzygać co jest a co nie jest tajemnicą obrończą lub adwokacką. Oceny takie formułować będą, posiadając już wiedzę objętą tajemnicą adwokacką i obrończą. Mechanizm ten jest właściwy dla państw autorytarnych, naruszających tajemnicę adwokacką, a co za tym idzie prawa i wolności jednostki, chronione na drodze pomocy prawnej, udzielanej przez adwokatów i radców prawnych.

Podobnie w przypadku pozyskiwania danych telekomunikacyjnych dotyczących adwokata, **projekt wprost przewiduje, że służby będą mogły pozyskiwać dane telekomunikacyjne dotyczące jego osoby.** Mechanizm kontrolny zakłada dobrą wolę funkcjonariusza policji lub służb specjalnych i zakłada rozstrzygnięcie sądu, które nie będzie zaskarżalne przez osobę obowiązaną do zachowania tajemnicy, jak i nie będzie zawierać uzasadnienia.

Przepisy te stwarzają pole do ogromnych nadużyć. Wykonywanie szczególnie zawodu adwokata i świadczenie pomocy prawnej służyć ma respektowaniu wielu chronionych konstytucyjnie praw i wolności. Zdobywanie i wykorzystywanie przez służby tego typu danych, stanowić będzie naruszenie tych praw i wolności.

Z tych wszystkich powodów, dalsze prace nad wykonaniem wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. nie powinny być prowadzone w oparciu o ww. projekt senacki. Przyjęcie propozycji przewidzianych w projekcie nie usunie najpoważniejszych problemów naruszeń praw i wolności konstytucyjnych, do których dochodzi w ramach prowadzenia przez Policję i służby działalności operacyjnej, a stworzy pole do większych nadużyć.

z upoważnienia

Załączniki:

1. Opinia Naczelnej Rady Adwokackiej do senackiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967).

Do wiadomości:

1. Senator Wojciech Skurkiewicz, Przewodniczący Komisji Obrony Narodowej, Senat RP
2. Senator Michał Seweryński, Przewodniczący Komisji Praw Człowieka, Praworządności i Petycji, Senat RP.
3. Senator Piotr Zientarski, Przewodniczący Komisji Ustawodawczej, Senat RP.

Warszawa, 2015-07- 16

MINISTER OBRONY NARODOWEJ

300/1059/T61/15/JS

Pan Senator Piotr ZIENTARSKI

PRZEWODNICZĄCY KOMISJI USTAWODAWCZEJ

SENAT RZECZYPOSPOLITEJ POLSKIEJ

Szanowny Panie Przewodniczący,

W odpowiedzi na pismo Pana Przewodniczącego z dnia 26 czerwca br. (BPS/KU-034/967/20/15) dotyczące opinii resortu obrony narodowej odnośnie projektu ustawy ***o zmianie ustawy o Policji oraz niektórych innych*** **ustaw** (druk senacki nr 967) uprzejmie informuję, że resort obrony narodowej nie zgłasza zasadniczych uwag do tego projektu. Proponuje jednakże zmiany w art. 6 zmiana 3 projektu ustawy w zakresie nowelizacji ustawy z dnia 24 sierpnia 2001 r. ***o Żandarmerii Wojskowej i wojskowych organach porządkowych*** (Dz. U. z 2013 r. poz. 568 ze zm.) :

1. **Art. 31 ustępowi 1 proponuje się nadać brzmienie:**

„Art. 31 ust. 1. Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Żandarmerię Wojskową w granicach zadań określonych w art. 4 ust. 1 oraz w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, 3, 5 i 6, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, umyślnych przestępstw ściganych z oskarżenia publicznego:

1) przeciwko pokojowi i ludzkości,
2) przeciwko Rzeczypospolitej Polskiej, z wyjątkiem przestępstw określonych w art. 127-132 Kodeksu karnego,
3) przeciwko życiu, określonych w art. 148-150 Kodeksu karnego,
4) określonych w art 140, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 171 § 1, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 211a, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 1 i 2, art. 232, art. 245, art. 246, art. 252 § 1-3, art. 258, art. 263 § 1 i 2, art. 265, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1 i 2 , art. 299 § 1-6, art. 305, art. 310 § 1, 2 i 4, art. 339 § 2, art. 345 § 2 i 3 oraz art. 358 § 2 Kodeksu karnego,

5) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
6) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. – Przepisy wprowadzające Kodeks karny (Dz. U. Nr 88, poz. 554, z późn. zm.),
7) określonych w art. 43-44 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. z 2015 r. poz. 793),
8) określonych w art. 53 ust. 1, art. 56 ust. 1, art. 58 ust. 1, art. 59 ust. 1 oraz art. 62 ust. 1 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2012 r. poz. 124 oraz z 2015 r. poz. 28), ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w ustawie karnej polskiej

– gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, wojskowy sąd okręgowy, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej i pisemnej zgody właściwego wojskowego prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną."

Uzasadnienie:

Proponowane brzmienie różni się dodaniem do katalogu przestępstw uzasadniających zastosowanie kontroli operacyjnej czterech typów czynów zabronionych: art. 263 § 1 i 2 kk, art. 286 § 2 kk oraz art. 58 ust. 1 i art. 59 ust. 1 ustawy *o przeciwdziałaniu narkomanii*. Wymienione przestępstwa są objęte zakresem kontroli operacyjnej w aktualnym brzmieniu *ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych*, stąd ich brak w projekcie traktować należy jako przeoczenie wymagające uzupełnienia.

2. **Art. 31 ustępowi 10 proponuje się nadać brzmienie:**

„10. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, wojskowy sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu Żandarmerii Wojskowej, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej oraz właściwego prokuratora wojskowego, może wydawać, również po upływie okresów, o których mowa w ust. 9, kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.".

Uzasadnienie:

Rozwiązanie przyjęte w przesłanym projekcie pozwala najwyżej dwukrotnie przedłużyć kontrolę operacyjną (zarządzaną pierwotnie – zgodnie z art. 31 ust. 9 na okres nie dłuższy niż 3 miesiące) – po raz pierwszy zgodnie z zapisami art. 31 ust. 9 na 3 miesiące, i po raz drugi – zgodnie z zapisami art. 31 ust. 10 – aż na okres do 12 miesięcy. W praktyce projektowane rozwiązanie może pozostawać w sprzeczności z postanowieniami sądów, które – jak należy się spodziewać – będą wydawać postanowienia o przedłużeniu kontroli operacyjnej na 3 miesiące, ograniczając w konsekwencji czas prowadzenia przez Żandarmerię Wojskową kontroli operacyjnej do 9 miesięcy. Stąd właściwym rozwiązaniem wydaje się przyjęcie modelu zaproponowanego w projekcie dla Służby Kontrwywiadu Wojskowego, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego w zakresie przedłużenia okresu stosowania kontroli operacyjnej. Rozwiązanie to pozwala na przedłużenie kontroli operacyjnej na kolejne okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.

Należy również przypomnieć, że zgodnie z aktualnym brzmieniem przepisu art. 31 ust. 10 zmienianej ustawy *o Żandarmerii Wojskowej i wojskowych organach porządkowych*, liczba przedłużeń kontroli operacyjnej nie była limitowana ilościowo, a jedyne ograniczenie dotyczyło czasu trwania przedłużonej kontroli operacyjnej – do 3 miesięcy przy każdym postanowieniu o przedłużeniu.

z up. Robert KUPIECKI
PODSEKRETARZ STANU

U Z A S A D N I E N I E

1. Cel projektowanej ustawy

Projektowana ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), stwierdzającego niezgodność wybranych przepisów ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.), ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 i 529), ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.), ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, z późn. zm.), ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, z późn. zm.), ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.), ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r. poz. 1411 i 1822) oraz ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.) z Konstytucją Rzeczypospolitej Polskiej. Sentencja rozstrzygnięcia została ogłoszona dnia 6 sierpnia 2014 r. w Dz. U. poz. 1055.

2. Przedmiot i istota wypowiedzi Trybunału Konstytucyjnego oraz rozwiązania w innych krajach, w szczególności w krajach członkowskich OECD/UE

Trybunał na wnioski Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego zbadał konstytucyjność przepisów ustaw zawierających regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych w ustawach: o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego i Centralnym Biurze Antykorupcyjnym.

Zgodnie z sentencją orzeczenia:

1) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej „ustawą o ABW oraz AW" jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP;
2) art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, zwanej dalej „ustawą o SG", art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, zwanej dalej „ustawą o ŻW", art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, zwanej dalej „ustawą o SKW oraz SWW", art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, zwanej dalej „ustawą o CBA", art. 75d ust. 1 ustawy o Służbie Celnej, zwanej dalej „ustawą o SC" – przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP;
3) art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW oraz AW, art. 31 ustawy o SKW oraz SWW, art. 17 ustawy o CBA – 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, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP;
4) art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW, art. 18 ustawy o CBA – w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP;
5) art. 75d ust. 5 ustawy o SC w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, z późn. zm.), jest niezgodny z art. 51 ust. 4 Konstytucji RP.

W dotychczasowym orzecznictwie Trybunał Konstytucyjny kilkukrotnie wypowiadał się w sprawie konstytucyjności przepisów regulujących czynności operacyjno-rozpoznawcze prowadzące do ingerencji w sferę prywatności jednostek i tajemnicę komunikowania się.

Trybunał nie podważył dopuszczalności ich stosowania w demokratycznym państwie prawa. Przeciwnie, wyraźnie podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o obywatelach, w toku kontroli operacyjnej ukierunkowanej na zapobieganie przestępstwom, ich wykrywanie oraz zwalczanie, jest nieodzowne. Jawność tych czynności powodowałaby bowiem ich nieskuteczność, a to z kolei rzutowałoby na poziom bezpieczeństwa państwa i jego obywateli. Ocena ta wynikała z dostrzeżenia specyfiki działalności przestępczej i coraz trudniejszych warunków zapewnienia bezpieczeństwa spowodowanych zagrożeniem terroryzmem, zorganizowaną przestępczością czy wykorzystywaniem przez przestępców nowych technologii w celu komunikowania się między sobą i popełniania rozmaitych przestępstw (np. komputerowych).

Trybunał Konstytucyjny generalnie aprobował powierzenie kompetencji w zakresie prowadzenia czynności operacyjno-rozpoznawczych nie tylko Policji, Agencji Bezpieczeństwa Wewnętrznego czy Centralnego Biura Antykorupcyjnego, ale również organom kontroli skarbowej, które odpowiadają m.in. za zwalczanie negatywnych zjawisk w postaci niewywiązywania się z obowiązków daninowych wobec Państwa, prowadzenia nieujawnionej działalności gospodarczej, prania pieniędzy, niedozwolonego wykorzystywania powiązań kapitałowych między podmiotami.

Trybunał wielokrotnie wskazywał ustawodawcy warunki, jakie muszą spełniać normy prawne regulujące niejawne pozyskiwanie przez służby policyjne i służby ochrony państwa informacji na temat jednostek.

Zdaniem Trybunału, ograniczenia w korzystaniu z konstytucyjnych wolności i praw muszą być precyzyjne unormowanie w ustawie. Chodzi jednak nie tylko o formalne umiejscowienie przepisu ograniczającego w akcie normatywnym o randze co najmniej ustawy, ale również o „jakość" tego unormowania, które musi zapewniać przewidywalność rozstrzygnięć organów władzy publicznej wobec jednostek. Ustawowa forma ograniczeń prawa do ochrony prywatności (art. 47 Konstytucji RP), wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP) oraz autonomii informacyjnej (art. 51 ust. 1 Konstytucji RP) wynika bezpośrednio z art. 31 ust. 3 Konstytucji RP, a zapewnienie dostatecznej określoności przepisów także z zasady demokratycznego państwa prawa (art. 2 Konstytucji RP).

Trybunał w uzasadnieniu do wyroku przywołał minimalne elementy ustawowej regulacji czynności operacyjno-rozpoznawczych (niejawnego pozyskiwania przez władze publiczne informacji o jednostkach).

Według Trybunału, po pierwsze, ustawa ma precyzować przedmiotowe przesłanki zarządzenia takich czynności. Aby zachować standard konstytucyjny, nie wystarcza odwołanie się do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest zdefiniować zamknięty i możliwie wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki. (...) Nie jest wykluczone zastosowanie innych technik legislacyjnych (np. odwołanie się do konkretnych rozdziałów lub ustaw), jednakże w każdym wypadku powinno być możliwe zrekonstruowanie sytuacji, w których niejawne pozyskiwanie informacji przez organy państwa jest dopuszczalne. Precyzyjne ustawowe uregulowanie przedmiotowych przesłanek dopuszczalności kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych, jest tym bardziej konieczne, ponieważ w istocie to same służby – działając w ramach ich ustawowych zadań – definiują zagrożenia, którym mają następnie zapobiegać. O ile Trybunał nie kwestionuje ogólnego zakreślenia w ustawie zadań służb ochrony państwa, to już przesłanki niejawnego pozyskiwania informacji o osobach mają być zdefiniowane przez ustawodawcę wyczerpująco. Należy jeszcze raz podkreślić, że na podstawie brzmienia przepisu ustawy jednostka ma wiedzieć, jakie zachowania narażają ją nie tylko na ewentualną odpowiedzialność karną, lecz również umożliwią prowadzenie w stosunku do niej czynności operacyjno-rozpoznawczych, głęboko ingerujących w jej prywatność.

Po drugie, niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanych ich parametrów. Mając na uwadze zróżnicowane środki odpowiadające obecnym formom techniki i w efekcie m.in. możliwością komunikowania się, które stosowane są przez organy państwa w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna. Z punktu widzenia zasady określoności prawa istotne jest natomiast sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Raz jeszcze należy podkreślić, że nie chodzi o wskazanie parametrów technicznych, ale rodzajowych nazw poszczególnych środków

i informacji możliwych do pozyskania za ich pomocą (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej"). Zamknięty katalog rodzajów środków technicznych służących do niejawnego pozyskiwania informacji i dowodów ogranicza arbitralność organów państwa. Ponadto umożliwia sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobie.

Według Trybunału, najbardziej pożądanym rozwiązaniem z konstytucyjnego punktu widzenia jest uregulowanie rodzajów środków służących niejawnemu pozyskiwaniu informacji o jednostkach w ustawie. Precyzyjne określenie tej kwestii przez ustawodawcę nie tylko wiąże się z realizacją zasady określoności prawa wynikającą z art. 2 Konstytucji RP, ale przede wszystkim z tą częścią art. 31 ust. 3 Konstytucji RP, która przewiduje obowiązek unormowania ograniczeń w korzystaniu z wolności i praw konstytucyjnych w „ustawie", będącej aktem normatywnym pochodzącym od przedstawicielskiego organu Narodu – Sejmu (art. 4 w zw. z art. 104 ust. 1 Konstytucji RP).

Po trzecie, ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. Termin ten ma określić ustawodawca tak, aby umożliwiał osiągnięcie konstytucyjnie uzasadnionego celu. Nie może być to jednak termin ani nadmiernie długi, ani zbyt krótki, który nie pozwala na efektywną pracę operacyjno-rozpoznawczą. Ustawodawca musi mieć także na uwadze, że w demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów.

Po czwarte, w ustawie ma być uregulowana procedura zarządzania czynności operacyjno-rozpoznawczych, włączywszy w to powierzenie kompetencji do zarządzania tych czynności, a także badanie ich legalności przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej przez sąd. Ustawa ma wskazywać podstawowe elementy proceduralne, zasady wykorzystywania zgromadzonych materiałów oraz przesłanki czy tryb ich niszczenia. Z punktu widzenia ochrony konstytucyjnych wolności i praw niezbędne jest zobowiązanie organów wnoszących o zarządzenie kontroli do wskazania określonego w prawie środka pozyskiwania informacji i dowodów w konkretnej sprawie oraz nałożenie na

organy zarządzające takie czynności obowiązku wyrażenia zgody na konkretny rodzaj środka, służącego pozyskiwaniu informacji. Wreszcie konieczne jest także uregulowanie procedury raportowania z przeprowadzonych w sposób niejawny czynności i środków gwarantujących przekazanie zapisów w stanie nienaruszonym, umożliwiającym ich późniejszą weryfikację. W powyższym zakresie nie jest konstytucyjnie akceptowalne unormowanie istotnych elementów procedury w wewnętrznie obowiązujących aktach normatywnych ustanawianych w ramach struktury organizacyjnej danej służby prowadzącej te czynności.

Po piąte, ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu, z uwagi na ich zbędność lub nieprzydatność.

Trybunał Konstytucyjny w uzasadnieniu wyroku stwierdził ponadto, iż niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. W obecnym stanie prawym zasada subsydiarności obowiązuje w odniesieniu do kontroli operacyjnej – sąd może zarządzić kontrolę operacyjną, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne. Zastosowanie zasady subsydiarności przed wystąpieniem o udostępnienie danych telekomunikacyjnych w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudnić skuteczne ściganie ich sprawców (np. przestępstw popełnionych przy użyciu urządzeń telekomunikacyjnych oraz coraz popularniejszych przestępstw internetowych, gdy nie ma innych czynności, które można wykonać albo wykazać ich nieskuteczność). Podkreślenia wymaga także, że pozyskiwanie danych telekomunikacyjnych nie wiąże się z tak dużą ingerencją w sferę prywatności jednostek i tajemnicę komunikowania się jak kontrola operacyjna, ponieważ nie istnieje prawna możliwość pozyskiwania w tym trybie treści indywidualnych komunikatów przekazywanych za pomocą sieci telekomunikacyjnych.

Z przesłanką subsydiarności wiąże się wprowadzenie proceduralnego wymogu, którym jest kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa. Pożądane jest powierzenie kompetencji w tym zakresie niezależnym i niezawisłym sądom, dającym rękojmię odpowiednio wysokiego stopnia wiedzy i doświadczenia życiowego. Z punktu widzenia Konstytucji sądowa kontrola nad

czynnościami operacyjno-rozpoznawczymi jest rozwiązaniem optymalnym. Nie jest jednak bezwzględnie konieczna. Kompetencje tego rodzaju mogą zostać też powierzone innym organom państwa, których status ustrojowy i zakres ustawowych kompetencji gwarantuje efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa.

Odnosząc się do zagadnienia określenia w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, Trybunał wskazał, że ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu z uwagi na ich zbędność lub nieprzydatność.

W wyroku o sygn. akt K 32/04 Trybunał zaznaczył: „w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji". Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04, cz. III, pkt 4.7). TK nie wyklucza zróżnicowania ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski, jakkolwiek nie może być ono traktowane jako zasada, a w każdym wypadku – nie może prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich.

Od tak ujętej zasady jednakowej ochrony dopuszczalne może być wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, którzy podlegają polskiemu prawu. Powyższe założenie nie wyklucza dopuszczalności odmiennego określenia przesłanek pozyskiwania danych i postępowania z nimi w stosunku do osób niepodlegających polskiemu prawu (np. danych pozyskiwanych przez służby wywiadu o działalność obcych podmiotów za granicą), chociaż w każdym wypadku takie działania władz publicznych muszą mieścić się w ramach standardów państwa prawnego.

Trybunał w wyroku podniósł również kwestię ochrony tajemnicy zawodowej i wskazał, że jednym z instrumentów ochrony zaufania jest tajemnica zawodowa i gwarancje jej

poszanowania w postępowaniach sądowych. Zaliczają się do nich m.in. bezwarunkowe i warunkowe zakazy dowodowe w postępowaniu karnym.

Nie jest wykluczone umożliwienie służbom policyjnym i służbom ochrony państwa pozyskanie informacji o charakterze poufnym, przekazywanym podmiotom wykonującym zawody zaufania publicznego. Zważywszy na znaczenie nowych technologii w efektywnej walce z zagrożeniami, zdaniem Trybunału Konstytucyjnego, ogólne wyłączenie spod kontroli operacyjnej podmiotów zobowiązanych w ustawie do zachowania tajemnicy zawodowej, a nawet wyłączenie informacji uznawanych za stanowiące tajemnicę zawodową, jako bezwzględnie niedopuszczalnych do pozyskania w tym trybie, prowadziłoby do istotnych utrudnień w gromadzeniu materiału dowodowego niektórych rodzajów przestępstw, popełnianych np. z wykorzystaniem nowych technologii.

Zdaniem Trybunału, punkt ciężkości przesuwa się więc na zapewnienie stosownych gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne oraz służby ochrony państwa informacji, które – z uwagi na ich treść i okoliczności przekazania – powinny podlegać ochronie prawnej. Modelowym rozwiązaniem tego konfliktu dóbr jest przewidziany w art. 180 § 2 k.p.k. mechanizm zwolnienia z tajemnicy zawodowej przez sąd, jeżeli jest to konieczne dla dobra wymiaru sprawiedliwości, zaś dana okoliczność nie może zostać wykazana w inny sposób, niełamiący tajemnicy zawodowej. W ocenie Trybunału, zbliżone w swej istocie rozwiązania legislacyjne powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym. Przeciwnie, standardy te – z uwagi na niejawność kontroli oraz jej ponadprocesowy charakter – powinny być co najmniej zbieżne ze standardami w postępowaniu karnym.

Według Trybunału, niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych.

Trybunał zauważa potrzebę poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Trybunał ma świadomość, że w pewnych sytuacjach może być również uzasadnione odstąpienie od wspomnianego obowiązku informacyjnego. Dotyczy to w szczególności takich sytuacji, gdy dane zostały pozyskane

wyłącznie przypadkowo i nie podlegają dalszej analizie, czy też gdy pozyskano dane dostępne w publicznych rejestrach. Kwestie te musi rozstrzygnąć ustawodawca. Wprowadzenie obowiązku informowania osób w zakresie wskazanym przez Trybunał niesie za sobą szereg konsekwencji. W szczególności wiązałoby się to z naruszeniem podstawowych zasad na podstawie których funkcjonują służby i poważnie mogłoby zaważyć, nie tylko na skutecznym działaniu służb, ale także mogłoby zagrozić bezpieczeństwu Sił Zbrojnych RP oraz osób, które w sposób niejawny udzielają pomocy służbom. W praktyce wiązałyby się z tym m.in. trudności w ustaleniu danych osób z uwagi na znaczną skalę używania tzw. telefonów pre–paid. Ponadto obowiązek informowania pozostawałby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia.

Jednym z wymagań, które powinny spełniać przepisy ustawowe upoważniające służby do pozyskiwania danych telekomunikacyjnych, jest wykreowanie mechanizmu niezależnej kontroli. Skoro pozyskiwanie tych danych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji. (...) W takiej sytuacji tym większe znaczenie ma ustanowienie gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych. TK nie przesądza jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Zdaniem Trybunału, nie jest wykluczone (...) wprowadzenie, jako zasady, kontroli następczej. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb. Trybunał Konstytucyjny nie wymaga jednocześnie by kontrolę udostępniania danych

telekomunikacyjnych sprawowały sądy. Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności.

Rozwiązania w innych krajach, w szczególności w krajach członkowskich OECD/UE

W Wielkiej Brytanii istnieje wyspecjalizowana kontrola parlamentarna nad służbami specjalnymi (Agencies): Służbą Bezpieczeństwa (Security Service), Tajną Służbą Wywiadowczą (Secret Intelligence Service) oraz Służbą Nasłuchu Radioelektronicznego (Government Communications Headquarters). Kontrola jest sprawowana przez Parlamentarną Komisję ds. Służb Specjalnych (Intelligence and Security Committee). W jej skład wchodzi dziewięciu desygnowanych przez premiera reprezentantów obu izb parlamentu. Kompetencje komisji są jednak ograniczone do bieżącej kontroli wobec służb specjalnych, oceny wydatków przeznaczanych na ich działalność. Komisja jest zobowiązana do składania rocznych raportów ze swej pracy w Izbie Gmin. W pierwszej kolejności komisja składa raport premierowi, który może wyłączyć z niego treści, których ujawnienie mogłoby zagrażać bezpieczeństwu państwa. Kontrola sprawowana przez komisję jest w znacznym stopniu ograniczona, gdyż szefowie poszczególnych służb mogą odmówić udzielenia informacji członkom tego gremium ze względu na bezpieczeństwo państwa. W związku z tym, jej działalność kontrolna nie sięga całości działalności operacyjnej. W kontekście kontroli zewnętrznej nad działalnością operacyjną działa dwóch komisarzy. Są oni powoływani na trzyletnie kadencje przez premiera spośród osób pełniących uprzednio wyższe funkcje sędziowskie i w okresie pełnienia swojej funkcji są całkowicie niezależni od premiera. Każdy z nich składa szefowi gabinetu roczny raport ze swej działalności. Premier decyduje, podobnie jak w przypadku raportu Komisji ds. Służb Specjalnych, które treści nie powinny zostać upublicznione, ponieważ przyniosłoby to szkodę bezpieczeństwu państwa, utrudniło zapobieganie i wykrywanie poważnej przestępczości, godziło w brytyjską gospodarkę lub szkodziło interesom poszczególnych służb. Komisarze różnią się zakresem kontrolowanych czynności operacyjno-rozpoznawczych. Komisarz ds. Kontroli Korespondencji i Stosowania Podsłuchu Telefonicznego (Interception of Communications Commissioner) skupia się na weryfikacji wydawanych przez ministrów zezwoleń na zastosowanie kontroli korespondencji i podsłuchu telefonicznego. Z kolei Komisarz ds. Służb Specjalnych (Intelligence Services Commissioner) odpowiedzialny jest za stałą kontrolę nad wydawanymi przez ministrów zezwoleniami upoważniającymi do ingerencji w nienaruszalność mieszkania. Jest on także

odpowiedzialny za monitorowanie prowadzonej przez funkcjonariuszy służb specjalnych inwigilacji i pracy z osobowymi źródłami informacji. Osobne funkcje kontrolne powierzone zostały Trybunałowi ds. Uprawnień Śledczych (Investigatory Powers Tribunal). Jest to instytucja niezależna od rządu i składa się z wyższych rangą przedstawicieli zawodów prawniczych i sądownictwa. Jej podstawowym zadaniem jest rozpatrywanie skarg obywateli odnoszących się do korzystania przez funkcjonariuszy służb specjalnych z przyznanych im ustawowo uprawnień.

W Danii Krajowa Agencja Informatyczno–Telekomunikacyjna monitoruje spełnienie wymogów, zgodnie z którymi dostawcy sieci i usług łączności elektronicznej muszą dopilnować, aby sprzęt i systemy techniczne pozwoliły Policji na dostęp do informacji o ruchu telekomunikacyjnym.

W przypadku Irlandii wyznaczony sędzia ma prawo do prowadzenia dochodzenia oraz składania sprawozdania w sprawie tego, czy właściwe organy krajowe postępują zgodnie z przepisami prawa.

W Holandii Agencja Komunikacji Radiowej nadzoruje realizację zobowiązań przez dostawców Internetu i usług telefonicznych; organ ds. ochrony danych pełni ogólny nadzór nad przetwarzaniem danych osobowych.

W przypadku Bułgarii Komisja Ochrony Danych Osobowych monitoruje przetwarzanie i przechowywanie danych w celu zapewnienia zgodności z wymogami. Parlamentarna komisja w Zgromadzeniu Narodowym monitoruje procedury udzielania zezwoleń i dostępu do danych telekomunikacyjnych.

3. Różnice między dotychczasowym a projektowanym stanem prawnym

Realizując wyrok Trybunału Konstytucyjnego oraz uwzględniając część minimalnych wymagań, jakie łącznie powinny spełniać przepisy regulujące niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach, w projekcie ustawy:

3.1. Określono przesłanki stosowania kontroli operacyjnej i dostępu do danych telekomunikacyjnych.

Trybunał Konstytucyjny zwrócił uwagę na niedookreślony katalog sytuacji uzasadniających zarządzenie kontroli operacyjnej w toku czynności operacyjno-

rozpoznawczych prowadzonych przez Policję, Straż Graniczną, wywiad skarbowy, Żandarmerię Wojskową, Służbę Kontrwywiadu Wojskowego i Agencję Bezpieczeństwa Wewnętrznego w odniesieniu do „przestępstw ściganych na mocy umów i porozumień międzynarodowych", „przestępstw godzących w bezpieczeństwo państwa", „podstawy ekonomiczne państwa", czy „bezpieczeństwo Sił Zbrojnych, jednostek organizacyjnych MON i państw zapewniających wzajemność". Obowiązujące przepisy nie precyzują, o jakie dokładnie przestępstwa chodzi ani w jakich dokładnie aktach normatywnych mają być ujęte. Mając na uwadze powyższe, w projektowanych: art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 9 ustawy o ŻW, doprecyzowano, że kontrola operacyjna może zostać zarządzona w odniesieniu do przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej.

Ponadto w projektowanych:

- art. 9e ust. 1 pkt 4 ustawy o SG, doprecyzowano katalog przestępstw pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii;
- art. 5 ust. 1 ustawy o ABW i AW doprecyzowano katalog przestępstw, do których rozpoznawania, zapobiegania i zwalczania uprawniona jest ABW;
- art. 31 ust. 1 ustawy o ŻW wskazano zamknięty katalog przestępstw, w odniesieniu do których może zostać zarządzona kontrola operacyjna.

W zakresie udostępniania danych telekomunikacyjnych doprecyzowano, że dane telekomunikacyjne mogą być udostępniane w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw:

- ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych – art. 20c ust. 1 ustawy o Policji;
- określonych w art. 1 ust. 2 pkt 4 oraz ust. 2a ustawy o SG – art. 10b ust. 1 tej ustawy;
- skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego

pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b – art. 36b ust. 1 ustawy o kontroli skarbowej;

- popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 5 i 6 ustawy o ŻW albo w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych – art. 30 ust. 1 tej ustawy;
- wskazanych w projektowanym brzmieniu art. 5 ust. 1 pkt 1, 2 lub 5 ustawy o ABW i AW – art. 28 ust. 1 tej ustawy;
- wskazanych w art. 5 ust. 1 pkt 1, 7 i 8 oraz ust. 2 ustawy o SKW i SWW – art. 32 ust. 1 tej ustawy;
- wskazanych w art. 2 ust. 1 pkt 1, 2 i 4 ustawy o CBA – art. 18 ust. 1 tej ustawy;
- skarbowych, o których mowa w rozdziale 9 ustawy o SC, z wyłączeniem art. 108 § 2 Kodeksu karnego skarbowego.

Ponadto z zakresu reglamentowanego dostępu do danych telekomunikacyjnych wyłączono dane abonamentowe.

3.2. Określono rodzaje środków niejawnego pozyskiwania informacji.

W aktualnym stanie prawnym kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji;
2) kontrolowaniu zawartości przesyłek;
3) stosowaniu 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.

Wychodząc naprzeciw oczekiwaniom Trybunału, odnośnie sprecyzowania w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach, ustawodawca odpowiednio w art. 19 ust. 6 i 6a ustawy o Policji, art. 9e ust. 7 i 7a ustawy o SG, art. 36c ust. 4 i 4a ustawy o kontroli skarbowej, art. 31 ust. 7 i 7a ustawy o ŻW, art. 27 ust. 6 i 6a ustawy o ABW oraz AW, art. 31 ust. 4 i 4a ustawy o SKW oraz SWW oraz w art. 17 ust. 5 i 5a ustawy o CBA określił sposoby prowadzenia kontroli operacyjnej. Zgodnie z projektem, kontrola operacyjna prowadzona jest niejawnie i polega na: podsłuchu rozmów

prowadzonych przy użyciu środków technicznych, podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi, kontroli korespondencji, nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu oraz kontrolowaniu zawartości przesyłek. Ponadto, w celu przejrzystości regulacji, w projekcie zostały enumeratywnie wskazane czynności, które nie stanowią kontroli operacyjnej.

3.3. Określono rodzaj dokumentacji prowadzonej w związku ze stosowaniem kontroli operacyjnej.

Z obowiązujących aktów wykonawczych przeniesiono do materii ustawowej regulację określającą, co stanowi dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej oraz określającą rejestry dokumentacji związanej z jej prowadzeniem. Dokumentację materiałów stanowią: nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek; kopie wykonane z nośników oraz dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach. Natomiast organy uczestniczące w procesie stosowania kontroli operacyjnej będą obowiązane prowadzić rejestry postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.

3.4. Określono maksymalny okres prowadzenia kontroli operacyjnej.

W obecnym stanie prawnym przepisy nie przewidują maksymalnego czasu prowadzenia kontroli operacyjnej. Na przykładzie art. 19 ustawy o Policji, kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Niemniej sąd okręgowy może, na pisemny wniosek Komendanta Głównego Policji, Komendanta Centralnego Biura Śledczego Policji albo komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym jej przedłużeniu, jeżeli nie ustały przyczyny tej kontroli. Ponadto, w uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o prowadzeniu kontroli operacyjnej przez czas oznaczony również po upływie ww. okresów

Realizując postulat Trybunału, dotyczący sprecyzowania w ustawie maksymalnego czasu prowadzenia niejawnych czynności, po upływie których dalsze ich prowadzenie jest już

niedopuszczalne, ustawodawca odpowiednio w projektowanym art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o SG, art. 36c ust. 7 ustawy o kontroli skarbowej oraz art. 31 ust. 10 ustawy o ŻW wskazał maksymalny okres stosowania kontroli operacyjnej. W projekcie doprecyzowane zostało, że po upływie okresów, na które została zarządzona kontrola operacyjna, tj. nie dłużej niż 3 miesiące – pierwsze postanowienie sądu, nie dłużej niż kolejne 3 miesiące – jednorazowe przedłużenie kontroli operacyjnej postanowieniem sądu, możliwe będzie, również na podstawie postanowienia sądu, prowadzenie kontroli operacyjnej po upływie ww. okresów, jednak nie dłużej niż 12 miesięcy. Maksymalny, więc okres stosowania przez te służby kontroli operacyjnej będzie łącznie wynosił 18 miesięcy.

Ze względu na specyfikę zadań realizowanych przez służby specjalne, ograniczenia takie nie zostały wprowadzone w odniesieniu do kontroli operacyjnej stosowanej przez te służby. W projektowanych art. 27 ust. 9 ustawy o ABW i AW, art. 31 ust. 7 ustawy o SKW i SWW, art. 17 ust. 9 ustawy o CBA, określono, że kontrola operacyjna może być przedłużana na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy. O przedłużeniu kontroli, każdorazowo będzie decydować sąd, który wydał zgodę na jej prowadzenie, co zapewni kontrolę niezależnego organu nad prawidłowością działań podejmowanych przez służby. Przyjęcie takiego rozwiązania w odniesieniu do służb specjalnych jest niezbędne z perspektywy bieżących zagrożeń, m.in. w kontekście przyjmowanego obecnie modus operandi sprawców takich przestępstw jak przestępstwa o charakterze terrorystycznym, sabotaż, czy szpiegostwo, wykorzystujących tzw. „uśpione ogniwo". Trybunał wskazał, że 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. Specyfika działalności służb informacyjno–wywiadowczych oraz związany z tym relatywnie wąsko określony zakres ich ustawowych zadań, może uzasadniać odmienne ustalenie zasad prowadzenia takich czynności i wykorzystywania zgromadzonych materiałów, od reguł obowiązujących pozostałe organy państwa, a zwłaszcza służby policyjne, mające szeroki zakres działania. Takie zróżnicowanie zasad prowadzenia czynności operacyjno-rozpoznawczych nie uchyla oczywiście wymogu przestrzegania zasady proporcjonalności.

Regulacje prawne zawarte w art. 180a ust.1 pkt 1 ustawy – Prawo telekomunikacyjne przewidują obowiązek dla operatorów publicznej sieci telekomunikacyjnej oraz dostawców

publicznie dostępnych usług telekomunikacyjnych, do zatrzymywania i przechowywania, na własny koszt, danych o których mowa w art. 180c ustawy, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Zgodnie ze stanowiskiem reprezentowanym przez służby ochrony państwa, oceny zasadności przechowywania przez okres 12 miesięcy danych telekomunikacyjnych należy dokonać przez pryzmat przydatności możliwości pozyskiwania tych danych i ich skutecznego wykorzystania w realizowanych działaniach operacyjno-rozpoznawczych. Należy podkreślić, iż w ramach rozpoznawania, zapobiegania i wykrywania przestępstw, w tym w szczególności o charakterze szpiegowskim, terrorystycznym, czy udziału w zorganizowanej grupie lub związku przestępczym ważną rolę odgrywa praca analityczna. Uzyskanie informacji o określonej, niezgodnej z prawem działalności, uruchamia proces analityczny, którego jednym z ważnych celów jest wykazanie genezy rozpoznawanych powiązań przestępczych. Powyższe pozwala (np. w przypadku przestępstwa szpiegostwa) na określenie potencjalnych szkód wyrządzonych taką działalnością. Priorytetową rolę w tym zakresie odgrywają dane telekomunikacyjne, pozwalające niejednokrotnie na wychwycenie okresu nawiązania współpracy w ramach niezgodnej z prawem działalności. Dane telekomunikacyjne pozwalają również we właściwy sposób zaplanować kolejne – niejednokrotnie złożone – czynności operacyjno-rozpoznawcze w celu neutralizacji istniejących zagrożeń. Trybunał uzasadniając potrzebę skrócenia okresu przechowywania danych telekomunikacyjnych, wskazał na dane statystyczne, w świetle których większość przypadków udostępniania danych mieściła się w okresie pierwszych 6 miesięcy przechowywania. Nawet, jeżeli w późniejszym okresie obserwowane jest zmniejszenie liczby udostępnianych danych, pamiętać należy, że również w późniejszych etapach prowadzenia sprawy, pozyskane dane mogą być istotne dla sprawy i skutecznie wykorzystane.

Podkreślenia wymaga także, że okres przechowywania danych telekomunikacyjnych przez operatorów został już skrócony z 24 do 12 miesięcy (ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. poz. 1445), która obowiązuje od 21 stycznia 2013 r. Podobny termin zatrzymywania danych obowiązuje w większości państw członkowskich Unii Europejskiej.

3.5. Określono zasady i procedury dotyczące weryfikacji i niszczenia danych telekomunikacyjnych zbędnych dla prowadzonego postępowania.

W celu wykonania orzeczenia Trybunału stwierdzającego niezgodność przepisów ustawy o ABW i AW, ustawy SKW i SWW oraz ustawy CBA, w zakresie w jakim nie przewidują zniszczenia danych telekomunikacyjnych niemających znaczenia dla prowadzonego postępowania, w projekcie ustawy wprowadzono ujednolicone dla wszystkich służb procedury postępowania z materiałami uzyskanymi w wyniku czynności związanych z pozyskaniem tych danych. Zgodnie z projektowanymi: art. 20c ustawy o Policji, art. 10b ustawy o SG, art. 36ba ustawy o kontroli skarbowej, art. 30 ustawy o ŻW, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW, art. 18 ustawy o CBA oraz art. 75d ustawy o SC, materiały uzyskane w wyniku czynności związanych z udostępnianiem danych telekomunikacyjnych, które zawierają informacje mające znaczenie dla postępowania karnego lub mogące stanowić dowód w postępowaniu karnym, przekazywane są właściwemu prokuratorowi. Materiały, które nie zawierają takich informacji lub nie mogą stanowić dowodu w postępowaniu karnym, będą podlegać niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Jednocześnie, na wzór obecnie obowiązujących regulacji m.in. w art. 20c ust. 7 ustawy o Policji, art. 10b ust. 6 ustawy o SG, przyjęto, że zniszczeniu będą podlegać wszystkie materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych.

Dane będą mogły być przetwarzane przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym nie rzadziej niż co 3 lata dokonywana będzie weryfikacja potrzeby dalszego ich przetwarzania. W przypadku, gdy w wyniku weryfikacji ustalone zostanie, że dalsze przetwarzanie danych telekomunikacyjnych nie jest niezbędne materiały te nie później niż w terminie 14 dni od dnia zakończenia weryfikacji będą podlegać zniszczeniu.

Jednocześnie, pomimo, że Trybunał nie wykluczył możliwości zróżnicowania ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski, poprzez dopuszczalne wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, polegających na odmiennym określeniu przesłanek pozyskiwania danych i postępowania z nimi w stosunku do tych osób, w projekcie ustawy nie zdecydowano się na wprowadzenie rozwiązań pozwalających na dalsze przechowywanie danych cudzoziemców, które są nieprzydane w prowadzonym postępowaniu karnym.

3.6. Określono organy oraz procedurę kontroli pozyskiwania danych telekomunikacyjnych.

W odróżnieniu od procesu udostępniania danych telekomunikacyjnych, obowiązujące przepisy przewidują wzmocniony nadzór prokuratorski i sądowy w odniesieniu do kontroli operacyjnej prowadzonej przez uprawnione służby. Nadzór ten sprawowany jest od początkowej fazy uzyskiwania zgody na jej prowadzenie (kontrola operacyjna może być zarządzona lub przedłużona przez sąd, po uzyskaniu wcześniejszej zgody prokuratora), poprzez obowiązek informowania prokuratora o przebiegu i wynikach tej kontroli, obowiązujące zasady i procedury związane z wykorzystaniem materiałów w prowadzonych postępowaniach oraz niszczeniem tych materiałów, a skończywszy na obowiązkach informacyjnych wobec Sejmu i Senatu. Realizując wyrok Trybunału, stwierdzający za niezgodne z Konstytucją RP obecne uregulowania, które nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy – Prawo telekomunikacyjne w projekcie ustawy zaproponowano, aby podmiotem wyznaczonym do kontroli nad uzyskiwaniem danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku – w odniesieniu do Policji, Straży Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Udostępnianie danych telekomunikacyjnych będzie się odbywało z poszanowaniem zasady subsydiarności.

Jednocześnie na uprawnione formacje został nałożony obowiązek przekazywania, raz na 6 miesięcy, sprawozdań obejmujących: liczbę przypadków pozyskania danych telekomunikacyjnych lub pocztowych oraz ich rodzaj; podstawę prawną pozyskania danych; rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane; liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane. W ramach kontroli, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych telekomunikacyjnych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. O zarządzeniu zniszczenia danych formacja jest obowiązana do niezwłocznego poinformowania prokuratora, który skierował materiały do sądu.

Ponadto projekt ustawy przewiduje zobowiązanie prezesów (wojskowych) sądów okręgowych do corocznego przekazywania Ministrowi Sprawiedliwości informacji na temat przetwarzania danych telekomunikacyjnych (z podziałem na liczbę i rodzaj udostępnianych danych) oraz wyników przeprowadzonych kontroli, w terminie do dnia 31 marca roku następującego po roku nią objętym.

Minister Sprawiedliwości został zobowiązany do corocznego przedstawiania Sejmowi i Senatowi zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym.

W aktualnym stanie prawnym obowiązek informowania Sejmu i Senatu w odniesieniu do danych dotyczących kontroli operacyjnej prowadzonej przez uprawnione służby, spoczywa na Prokuratorze Generalnym, na podstawie art. 10ea ustawy o prokuraturze. Ponadto, zgodnie z art. 19 ust. 22 ustawy o Policji, minister właściwy do spraw wewnętrznych ma obowiązek przedstawiania Sejmowi i Senatowi informacji o działalności Policji określonej w art. 19 ust. 1–21 (kontrola operacyjna), w tym informacji i danych, o których mowa w art. 20 ust. 3 tej ustawy (tajemnica bankowa i ubezpieczeniowa). Powyższe informacje przedkładane są corocznie, najpóźniej do dnia 30 czerwca roku następnego po roku nią objętym.

3.7. Określono zasady postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową (notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną), albo objęte są zakazami dowodowymi.

W zakresie kontroli operacyjnej:

Wykonując wyrok Trybunału odnoszący się do niekonstytucyjności przepisów regulujących kontrolę operacyjną, ze względu na brak regulacji przewidującej gwarancję niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej, bądź uchylenie było niedopuszczalne, w poszczególnych ustawach pragmatycznych wprowadzono zasady postępowania z materiałami uzyskanymi w ramach czynności operacyjno-rozpoznawczych, które mogą zawierać informacje objęte tajemnicą zawodową. W projektowanych: art. 19 ust. 15f–15i ustawy o Policji, art. 9e ust. 16f–16i ustawy o SG, art. 36d ust. 1f–1h ustawy o kontroli skarbowej, art. 31 ust. 16f–16i ustawy o ŻW, art. 27 ust. 15h–15k ustawy o ABW i AW, art. 31 ust. 14f–14i ustawy o SKW i SWW,

art. 17 ust. 15e–15i ustawy o CBA, zaproponowano, aby w przypadku, w którym materiały uzyskane w wyniku kontroli operacyjnej będą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. (tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej), właściwy organ przekazując je prokuratorowi wskazywał fragmenty mogące je zawierać. Materiały te następnie kierowane będą do sądu, który zarządził kontrolę operacyjną wraz z wnioskiem o: wyrażenie zgody na ich wykorzystanie w postępowaniu karnym albo wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu. Sąd wydając postanowienie będzie obowiązany kierować się tymi samymi przesłankami, o których mowa w art. 180 § 2 k.p.k. tj. dobrem wymiaru sprawiedliwości oraz faktem, że okoliczność nie może być ustalona na podstawie innego dowodu. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym tych prokuratorowi będzie przysługiwało zażalenie.

O wykonaniu zarządzenia dotyczącego zniszczenia materiałów, właściwy podmiot niezwłocznie informuje sąd okręgowy.

W sytuacji, kiedy będzie zachodzić przypuszczenie, że materiały uzyskane w wyniku kontroli operacyjnej będą zawierać informacje objęte zakazami dowodowymi, o których mowa w art. 178 k.p.k., tj. dotyczących faktów, o których obrońca lub adwokat dowiedział się udzielając porady prawnej lub prowadząc sprawę, albo faktów, o których dowiedział się duchowny przy spowiedzi, proponuje się, aby właściwy organ wnioskujący o zarządzenie kontroli operacyjnej nakazywał niezwłoczne, komisyjne i protokolarne ich zniszczenie. Analogiczne rozwiązanie będzie miało zastosowanie dla objętych zakazami dowodowymi: tajemnicy mediatora oraz o źródle informacji dziennikarza.

W zakresie udostępniania danych telekomunikacyjnych:

Osoby, o których mowa w art. 180 § 2 k.p.k, zostały także objęte ochroną prawną w związku z pozyskiwaniem przez służby danych telekomunikacyjnych. W przypadkach, gdy z materiałów zgromadzonych w sprawie będzie wynikać, że pozyskane dane telekomunikacyjne lub pocztowe, mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k., zaproponowano następujące rozwiązania:

Jeżeli z materiałów sprawy, będzie wynikać, że materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych mające znaczenie dla

postępowania karnego lub mogące stanowić dowód w postępowaniu karnym, zawierają dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 k.p.k., właściwy organ występujący o ich udostępnienie, przekazując te materiały prokuratorowi, będzie wskazywać fragmenty, które zawierają te dane. Prokurator niezwłocznie po otrzymaniu tych materiałów będzie kierować je do właściwego miejscowo sądu okręgowego, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym. Następnie, sąd postanowi o ich dalszym wykorzystaniu, albo zarządzi komisyjne i protokolarne zniszczenie. Analogicznie do kontroli operacyjnej sąd przy wydawaniu postanowienia będzie obowiązany kierować się przesłankami wymienionymi w art. 180 § 2 k.p.k.,

Jeżeli w toku czynności ustalone zostanie, że konieczne jest pozyskanie danych telekomunikacyjnych dotyczących bezpośrednio osoby wykonującej zawód, o którym mowa w art. 180 § 2 k.p.k., uprawniony organ będzie występował do sądu o zgodę na pozyskanie tych danych i wykorzystanie w postępowaniu karnym. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, uprawniony organ będzie mógł wystąpić do podmiotu prowadzącego działalność telekomunikacyjną o przekazanie danych dotyczących bezpośrednio osoby wykonującej zawód, o którym mowa w art. 180 § 2 k.p.k., zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. Sąd także w tych przypadkach będzie kierował się przesłankami z art. art. 180 § 2 k.p.k.

Na postanowienie sądu wydane w sytuacjach, o których mowa w pkt 2 i 3 będzie przysługiwać zażalenie organowi wnioskującemu. Do zażalenia zastosowanie będą miały odpowiednio przepisy Kodeksu postępowania karnego. W przypadku, gdy sąd nie uwzględni zażalenia, właściwy organ formacji mundurowej, będzie zobowiązany do wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane bądź do poinformowania podmiotu prowadzącego działalność telekomunikacyjną o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane. W przypadku, gdy zgromadzone dane telekomunikacyjne nie będą zawierać informacji mających znaczenia dla prowadzonego postępowania, właściwy organ formacji mundurowej, który wnioskował o ich udostępnienie, zarządzi ich niezwłoczne, komisyjne i protokolarne zniszczenie. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia

danych telekomunikacyjnych, konieczne będzie niezwłoczne poinformowanie właściwego sądu

Powyższe propozycje, zostały wprowadzone odpowiednio w art. 20ca i art. 20cb ustawy o Policji, art. 10ba i 10bb ustawy o SG, art. 36bb i art. 36bc ustawy o kontroli skarbowej, art. 30b i 30c ustawy o ŻW, art. 28a i 28b ustawy o ABW oraz AW, art. 32a i 32b ustawy o SKW oraz SWW, art. 18a i art. 18b ustawy o CBA oraz art. 75da i art. 75db ustawy o SC.

3.8. Udostępnianie danych od operatorów świadczących usługi pocztowe.

Wypracowując kompleksowe rozwiązania dodatkowo, obok danych telekomunikacyjnych, objęty został kontrolą sądową proces udostępniania, od operatorów świadczących usługi pocztowe, na podstawie ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2012 r. poz. 1529), danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia tych usług lub korzystania z nich, do których uzyskiwania są obecnie uprawnione służby (tj. danych pocztowych). Pomimo, że wyrok TK nie obejmuje swoim zakresem danych uzyskiwanych na podstawie prawa pocztowego, powyższe znajduje uzasadnienie w tym, że działalność służb w tych obszarach w podobnym stopniu ingeruje w prawa i wolności obywatelskie jak proces pozyskiwania danych telekomunikacyjnych. Projekt przewiduje również takie same przesłanki udostępniania, procedury weryfikacji oraz niszczenia udostępnianych danych pocztowych zbędnych dla prowadzonego postępowania. Skorelowanie regulacji prawnych w stosunku do obu obszaru danych stanowi rozwiązanie systemowe służące pogłębieniu zaufania obywateli do organów państwowych.

3.9. Kontrola operacyjna oraz udostępnianie danych telekomunikacyjnych i pocztowych w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej.

W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej uznano za konieczne, iż postanowienie to, zamiast sądu okręgowego, będzie wydawał Pierwszy Prezes Sądu Najwyższego.

3.10. Nowelizacja ustawy – Prawo telekomunikacyjne.

W projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw uchylono art. 180g ustawy z dnia 16 lipca 2014 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198).

Konieczność uchylenia tego przepisu wynika z wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. (sprawy połączone C–293/12 i C–594/12). Trybunał w przedmiotowym wyroku stwierdził nieważność dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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 zmieniającej dyrektywę 2002/58/WE. W konsekwencji powyższego, utracił podstawę prawną zawarty w art. 180g ustawy obowiązek przekazywania przez przedsiębiorców telekomunikacyjnych Prezesowi Urzędu Komunikacji Elektronicznej informacji wskazanych w art. 180g ust. 1 i następnie obowiązek przekazywania tych informacji przez Prezesa UKE Komisji Europejskiej.

Projekt ustawy przewiduje natomiast obowiązek corocznego przedstawiania Sejmowi i Senatowi przez Ministra Sprawiedliwości, zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym.

3.11. Przepisy przejściowe.

Projekt przewiduje, że do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie projektowanej ustawy i nie została zakończona stosuje się przepisy w brzmieniu nadanym niniejszą ustawą w odniesieniu do materiałów, w stosunku do których zachodzi przypuszczenie, że zawierają informację o których mowa w art. 178 k.p.k. i art. 180 § 2 k.p.k. W stosunku do kontroli operacyjnej, która była przedłużona po upływie ustawowych okresów jej trwania, będzie ona mogła być nadal prowadzona nie dłużej niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy, chyba że termin jej zakończenia, określony w postanowieniu sądu, upływa wcześniej.

Poza powyższymi wyjątkami, kontrola operacyjna rozpoczęta przed dniem wejścia w życie niniejszej ustawy będzie prowadzona na podstawie przepisów dotychczasowych.

Projektowane regulacje zawierają obowiązek dla komendantów i szefów uprawnionych do stosowania kontroli operacyjnej służb nakazania w ciągu 30 dni od daty wejścia w życie niniejszej ustawy niezwłocznego, komisyjnego i protokolarnego zniszczenia dokumentacji

materiałów zgromadzonych podczas stosowania kontroli operacyjnej przed dniem wejścia w życie niniejszej ustawy. Obowiązkowi zniszczenia nie podlegają materiały, które są istotne dla bezpieczeństwa państwa.

4. Skutki projektowanej ustawy

Projekt uwzględnia stanowisko Trybunału w odniesieniu do: przepisów regulujących zakres przesłanek prowadzenia kontroli operacyjnej i udostępniania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku realizowanych czynności, niszczenia zbędnych danych telekomunikacyjnych, określenia zakresu i trybu kontroli nad pozyskiwaniem danych telekomunikacyjnych, określenia środków niejawnego pozyskiwania informacji o jednostkach, określenia maksymalnego okresu prowadzenia kontroli operacyjnej, podawania do publicznej wiadomości informacji o danych telekomunikacyjnych pozyskiwanych przez uprawnione służby. Ponadto wprowadzone zostały takie same gwarancje ochrony prawnej w stosunku do uzyskiwanych przez uprawnione służby danych pocztowych.

Wobec tego podstawowym skutkiem projektu będzie urzeczywistnienie zasad i gwarancji konstytucyjnych. Można oczekiwać, że wejście w życie projektowanej regulacji będzie sprzyjać budowaniu zaufania jednostek do działań o charakterze niejawnym podejmowanych przez służby policyjne oraz służby ochrony państwa, w szczególności poprzez zwiększenie przejrzystości przepisów oraz określenie precyzyjnych procedur obowiązujących w omawianym obszarze funkcjonowania Państwa.

Proponowana nowelizacja może przyczynić się do wzrostu wydatków budżetowych. Jednak określenie skali tego zjawiska nie jest możliwe, jako że będzie ono zależne od decyzji prezesów sądów okręgowych uprawnionych do przeprowadzania kontroli pozyskiwania przez służby danych telekomunikacyjnych i danych pocztowych.

Ustawa nie będzie miała natomiast skutków dla pozostałych jednostek sektora finansów publicznych, w tym jednostek samorządu terytorialnego.

Projekt oddziaływuje na:

1) sądy okręgowe i wojskowe sądy okręgowe, w zakresie jakim nadaje uprawnienie kontrolne nad uzyskiwaniem przez właściwe służby danych telekomunikacyjnych i pocztowych. W ramach przyznanych uprawnień sądy będą mogły zapoznawać się

z materiałami uzasadniającymi wystąpienia o dane telekomunikacyjne i pocztowe oraz z materiałami uzyskanymi w wyniku podjętych przez służby czynności;

2) funkcjonariuszy Policji, Straży Granicznej, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Służby Celnej, wywiadu skarbowego i żołnierzy Żandarmerii Wojskowej prowadzących czynności operacyjno-rozpoznawcze oraz mających dostęp do danych telekomunikacyjnych i pocztowych, poprzez wprowadzenie nowego trybu uzyskiwania tych danych, tj. przekazywania ich do organu kontrolnego oraz wprowadzenia trybu niszczenia zbędnych danych;

3) osoby objęte tajemnicą notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną, w zakresie zapewnienia procedur gwarantujących ochronę prawną pochodzących od nich informacji, które z uwagi na ich treść i okoliczności przekazania winny takiej ochronie podlegać

4) przedsiębiorców telekomunikacyjnych i Prezesa Urzędu Telekomunikacji Elektronicznej poprzez zniesienie obowiązku przekazywania informacji wskazanych w art. 180g ust. 1 ustawy – Prawo telekomunikacyjne i następnie obowiązku ich przekazywania przez Prezesa UKE do Komisji Europejskiej;

5) obywateli, którym projekt zapewnia zwiększenie ochrony konstytucyjnych wolności i praw.

Koszty wprowadzenia regulacji będą związane z nałożonym na sądy okręgowe zadaniem kontroli pozyskiwania przez uprawnione służby danych telekomunikacyjnych i pocztowych. Jednakże, w chwili obecnej, nie jest możliwe szczegółowe wyliczenie kosztów funkcjonowania takiej kontroli, gdyż prezesi sądów okręgowych mogą podjąć autonomiczne decyzje w zakresie zleconych czynności kontrolnych. Nie przewiduje się zwiększenia kosztów finansowych związanych z wprowadzeniem dodatkowych zadań dla służb.

5. Założenia podstawowych aktów wykonawczych do ustawy

Projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk 697) przewiduje w art. 1 pkt 1 lit. h, art. 2 pkt 1 lit. h, art. 3 pkt 1 lit. art. 3 pkt 3 lit. h, art. 6 pkt 3 lit. h, art. 7 pkt 1 lit. g, art. 9 pkt 1 lit. g, art. 10 pkt 1 lit. g, delegacje ustawowe do wydania aktów wykonawczych, na podstawie:

1) art. 19 ust. 21 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2015 r. poz. 355, z późn zm.);
2) art. 9e ust. 20 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.);
3) art. 36c ust. 17 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz.U. z 2015 r. poz. 553);
4) art. 31 ust. 20 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, z późn. zm.);
5) art. 27 ust. 18 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.) ;
6) art. 31 ust. 16 ustawy z dnia 9 czerwca o 2006 r. Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.);
7) art. 17 ust. 18 ustawy z dnia 9 czerwca 2006 r. Centralnym Biurze Antykorupcyjnym(Dz.U.z 2014 r. poz. 1411, z późn. zm.).

Zgodnie z upoważnieniami, w rozporządzeniach uregulowane zostaną: sposób dokumentowania kontroli operacyjnej, sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej, szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji, sposób prowadzenia rejestrów **oraz** wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów. Rozporządzenia mają uwzględniać potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.

Konieczność wydania nowych aktów wykonawczych wynika z nadania delegacjom ustawowym nowego brzmienia w związku z przeniesieniem do materii ustawowej wybranych przepisów rozporządzeń, dotyczących dokumentacji materiałów zgromadzonych podczas kontroli operacyjnej oraz prowadzenia przez poszczególne służby rejestrów wniosków i zarządzeń kontroli operacyjnej, która to tematyka powinna być, co do zasady, regulowana ustawą.

Zgodnie z art. 17 projektowanej ustawy obecnie obowiązujące rozporządzenia zachowują moc do dnia wydania nowych aktów, jednak nie dłużej jednak niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

6. Konsultacje

Opinie złożyli:

1) Prokuratoria Generalna Skarbu Państwa – która zgłosiła uwagi dotyczące transparentności danych statystycznych dotyczących czynności operacyjno-rozpoznawczych, materii upoważnienia do wydania aktu wykonawczego i rejestru postanowień, zarządzeń oraz wniosków dotyczących Służby Celnej w zakresie kontroli operacyjnej. W toku prac uwzględniono uwagę o charakterze porządkującym odesłanie;
2) Sąd Najwyższy, który nie zgłosił uwag;
3) Fundacja Panoptykon – która zgłosiła szereg uwag, uzasadniających stwierdzenie, iż ustawa nie wykonuje wyroku Trybunału Konstytucyjnego. Projekt uwzględnia jedną z zasadniczych uwag tj. dotyczącą wprowadzenia zasady subsydiarności w udostępnianiu służbom danych telekomunikacyjnych;
4) Prokurator Generalny – który wskazał na szereg nieścisłości i niekonsekwencji w projekcie ustawy. Do istotnych mankamentów zaliczono brak regulacji dotyczących zażalenia osób zainteresowanych oraz prokuratora na wykorzystanie danych telekomunikacyjnych przez osoby pełniące funkcje, o których mowa w art. 180 § 2 k.p.k. Uwagi dotyczyły także m.in. definicji kontroli operacyjnej, przedłużania kontroli, postępowania w sprawie udostępniania danych telekomunikacyjnych. Uwzględniono uwagi dotyczące zakazów dowodowych oraz przesłanek, jakimi sąd kieruje się wydając zgodę na wykorzystanie danych telekomunikacyjnych oraz uwagę dotyczącą zażalenia prokuratora;
5) Minister Sprawiedliwości – który wskazał na konieczność rozważenia zastąpienia zgody sądu kontrolującego udostępnianie danych telekomunikacyjnych zgodą prokuratora. Wskazano także na konieczność uwzględnienia tajemnicy mediatora w zakresie zakazu dowodowego;
6) Minister Finansów – który wskazał, iż ustawa uniemożliwi kontroli skarbowej skuteczną realizację zadań oraz będzie miała szkodliwy wpływ na ochronę interesów ekonomicznych Skarbu Państwa i przestawił szereg uwag usuwających to zagrożenie;
7) Helsińska Fundacja Praw Człowieka – która wskazała m.in. na nieprecyzyjność przepisów dotyczących katalogu środków kontroli operacyjnej, nadmiernie długi okres, o który można przedłużyć kontrolę operacyjną, brak przesłanek wyrażania zgody na wykorzystanie informacji dotyczących tajemnic zawodowych, niedoskonałość regulacji

dotyczących uzyskiwania danych telekomunikacyjnych (szczególności w zakresie braku poszanowania zasady subsydiarności oraz uprzedniej kontroli sądowej);

8) Komendant Główny Straży Granicznej – który przedstawił 16 uwag szczegółowych dotyczących m.in. okresu przedłużania kontroli operacyjnej, tajemnicy mediatora czy też dotyczących spójności terminologicznej ustawy;

9) Naczelna Rada Adwokacka – która zwróciła uwagę, iż tajemnica adwokacka nie jest dostatecznie chroniona zarówno w zakresie kontroli operacyjnej jak i w zakresie udostępniania danych telekomunikacyjnych;

10) Minister Administracji i Cyfryzacji – który wskazał na konieczność doprecyzowania upoważnienia do określenia wzorów rejestrów;

11) Generalny Inspektor Ochrony Danych Osobowych – który zwrócił uwagę na brak uprzedniej sądowej kontroli nad uzyskiwaniem danych telekomunikacyjnych, brak wskazania adekwatności, niezbędności i celowości uzyskiwania tych danych oraz ryzyko nieuzasadnionego bezterminowego przechowywania danych;

12) Krajowa Rada Sądownictwa – która wskazała na konieczność zapewnienia środków na zwiększone zadania sądów;

13) Szef Agencji Bezpieczeństwa Wewnętrznego – który przedstawił szereg uwag o charakterze porządkującym;

14) Prezes Urzędu ~~Tele~~komunikacji Elektronicznej – który przedstawił uwagi mające na celu wyjaśnienie wątpliwości terminologicznych oraz legislacyjno-porządkowych;

15) Szef Centralnego Biura Antykorupcyjnego – który wskazał m.in. iż niektóre z przepisów w zakresie ustawy o CBA nie są niezbędne do realizacji wyroku Trybunału Konstytucyjnego; wskazano także, iż decyzja o niszczeniu informacji objętych zakazami dowodowymi powinna należeć do sądu, a nie do szefa służby;

16) Minister Obrony Narodowej – który wskazał na konieczność uzupełnienia niektórych przepisów ustawy w zakresie Żandarmerii Wojskowej.

Ponadto Szef Biura Ochrony Rządu uznał za niemożliwe ustosunkowanie się do przedłożonego projektu ustawy.

7. Oświadczenie o zgodności z prawem Unii Europejskiej

Zakres przedmiotowy projektowanej ustawy jest zgodny z prawem Unii Europejskiej.