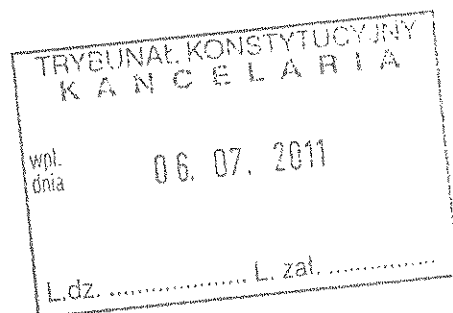




Warszawa, dnia 5 lipca 2011 r.

PG VIII TK 12/11

(K 2/11)



TRYBUNAŁ KONSTYTUCYJNY

W związku z wnioskiem Grupy posłów na Sejm Rzeczypospolitej Polskiej o stwierdzenie niezgodności przepisów:

I

- art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 ze zmianami),
- art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 ze zmianami),
- art. 31 ust. 7 pkt 3 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),
- art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),

- art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
 - art. 31 ust. 4 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)
- z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284);

II

Art. 180a ust. 1 oraz art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zmianami) w związku z:

- art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 ze zmianami),
- art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 ze zmianami),
- art. 30 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),
- art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
- art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),

- art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)
- z art. 2, art. 47, art. 49, art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej
- na podstawie art. 33 w związku z art. 27 pkt 5 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643 ze zmianami) –

przedstawiam następujące stanowisko:

I

przepisy:

- art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 ze zmianami),
- art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 ze zmianami),
- art. 31 ust. 7 pkt 3 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),

- art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
 - art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
 - art. 31 ust. 4 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)
- są niezgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61 poz. 284);

II

przepisy art. 180a ust. 1 oraz art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zmianami) w związku z:

- art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 ze zmianami),
- art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 ze zmianami).
- art. 30 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),

- art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
 - art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
 - art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)
- są niezgodne z art. 2, art. 47, art. 49, art. 51 ust. 1 i ust. 4 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.

UZASADNIENIE

W dniu 28 stycznia 2011 r. Grupa posłów na Sejm Rzeczypospolitej Polskiej zwróciła się do Trybunału Konstytucyjnego z wnioskiem o stwierdzenie niezgodności szeregu przepisów normujących kontrolę operacyjną, podejmowaną przez stosowne służby mundurowe lub specjalne, w ramach czynności operacyjno – rozpoznawczych, które to przepisy zostały zawarte w Prawie telekomunikacyjnym oraz w siedmiu ustawach regulujących funkcjonowanie tychże służb, z wzorcami kontroli zawartymi w ustawie zasadniczej oraz w Konwencji o ochronie praw człowieka i podstawowych wolności.

Pismem z dnia 8 czerwca 2011 r. Wnioskodawcy dokonali sprostowania oczywistej omyłki pisarskiej w punkcie I *petitum* wniosku, odnośnie przepisu ustawy o Policji poddanego zaskarżeniu, jak również uzupełnili argumentację

zawartą w uzasadnieniu, w zakresie punktu II tegoż wniosku, odnośnie oceny wskazanego przedmiotu zaskarżenia z punktu widzenia testu proporcjonalności.

Zdaniem Wnioskodawców, 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. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego godzą w art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, nie wskazując, jakich konkretnie środków mogą używać konkretne służby stosując kontrolę operacyjną oraz jakie konkretnie informacje mogą te służby pozyskiwać.

Grupa posłów podniosła również, że, redagując zakwestionowane wyżej przepisy, ustawodawca, z obrazą zasad prawidłowej legislacji, posłużył się pojęciami nieostryimi, jak „środki techniczne umożliwiające uzyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie” oraz „inne informacje przekazywane za pomocą sieci telekomunikacyjnych”, jak również sformułował otwarty katalog środków technicznych stosowanych podczas kontroli operacyjnej, godząc tym samym w unormowania art. 2 i art. 31 ust. 3 Konstytucji RP.

Uzasadnienie analizowanego wniosku zawiera również pogląd, że przepisy: art. 180a ust. 1 oraz art. 180c Prawa telekomunikacyjnego w związku z art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ustawy o Centralnym Biurze Antykorupcyjnym i art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz

Służbie Wywiadu Wojskowego są niezgodne z art. 47, art. 49, art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji RP, bowiem ustawodawca dopuścił się pominięcia legislacyjnego w sferze gwarancji proceduralnych i instytucjonalnych, dotyczących ochrony przed arbitralnością decyzji stosownych służb w zakresie pozyskiwania i przechowywania informacji. Pominięcie to dotyczy, w szczególności, braku regulacji nakładającej na służby prowadzące kontrolę operacyjną obowiązku:

- uzyskania zgody sądu na pozyskanie danych telekomunikacyjnych,
- poinformowania jednostki o pozyskiwaniu wspomnianych danych dotyczących jej osoby, nawet po zakończeniu postępowania,
- niszczenia danych niemających znaczenia dla potrzeb postępowania,
- powstrzymywania się od pozyskiwania danych objętych tak zwanymi zakazami dowodowymi.

Zgodnie ze stanowiskiem Wnioskodawców, zakwestionowane przepisy omawianych ustaw naruszają wymienione wyżej wzorce kontroli, godząc w prawo do prywatności, swobodę komunikowania się oraz autonomię informacyjną jednostki, jak również dopuszczając do ograniczenia tych praw w sposób nieproporcjonalny oraz w sytuacji, gdy nie jest to niezbędne w demokratycznym państwie, poprzez dopuszczenie do pozyskiwania informacji innych niż „niezbędne” (a więc także „użytecznych” lub „wygodnych” dla władzy) oraz poprzez rezygnację z zagwarantowania subsydiarności działania mającego na celu pozyskanie informacji.

W końcu, Grupa posłów wyraziła pogląd w uzasadnieniu wniosku, że zakwestionowane wyżej przepisy są niezgodne z wymienionymi unormowaniami ustawy zasadniczej wobec braku kontroli sądowej nad działalnością służb mundurowych i specjalnych w zakresie gromadzenia i przechowywania omawianych informacji. W tym miejscu wypada jednak odnotować, że ani w *petitum*, ani w uzasadnieniu wniosku nie zaproponowano art. 45 ust. 1 Konstytucji RP jako wzorca kontroli w niniejszej sprawie.

Nadto, Wnioskodawcy zakwestionowali, w *petitum* wniosku, omawiane unormowania w kontekście art. 2 ustawy zasadniczej, jednakże w uzasadnieniu tegoż wniosku nie zamieszczono pogłębionego wywodu uzasadniającego powyższe twierdzenie, ograniczając się jedynie do wykazania, że przepisy Prawa telekomunikacyjnego zostały doprecyzowane rozporządzeniem Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226, poz. 1828), co wskazywałoby, iż, zdaniem Grupy posłów, zaskarżone przepisy rangi ustawowej nie spełniają wymogu dookreśloności.

Ocena poglądów prawnych oraz zarzutów przedstawionych przez Grupę posłów w omawianym wniosku przedstawia się następująco.

Zakwestionowany we wniosku Grupy posłów przepis art. 19 ust. 6 pkt 3 ustawy o Policji ma następujące brzmienie:

„Art. 19. 6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Zakwestionowany przez Grupę posłów przepis art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej brzmi następująco:

„Art. 9e. 7. Kontrola operacyjna jest prowadzona niejawnie i polega na:
(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności

obrazu, treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Zakwestionowany we wniosku Grupy posłów przepis art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej ma następującą treść:

„Art. 36c. 4. Kontrola operacyjna jest prowadzona niejawnie i polega na:

(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych przy pomocy sieci telekomunikacyjnych.”.

Zakwestionowany przepis art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych ma następujące brzmienie:

„Art. 31. 7. Kontrola operacyjna jest prowadzona niejawnie i polega na:

(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Zakwestionowany we wniosku Grupy posłów przepis art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu brzmi następująco:

„Art. 27. 6. Kontrola operacyjna prowadzona jest niejawnie i polega na:

(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Zakwestionowany przepis art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym ma następującą treść:

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

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Zakwestionowany przez Wnioskodawców przepis art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ma następujące brzmienie:

„Art. 31. 4. Kontrola operacyjna prowadzona jest niejawnie i polega na:
(...)

- 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.”.

Wstępna analiza brzmienia przytoczonych wyżej przepisów wskazuje, że – nie licząc drobnych zmian stylistycznych – różnią się one merytorycznie jedynie w zakresie dotyczącym Straży Granicznej i wywiadu skarbowego, jako że opis środków technicznych, umożliwiających uzyskanie przez te dwie służby informacji i dowodów, obejmuje również „obraz”, podczas gdy w pozostałych przepisach mowa jedynie o „treści rozmów telefonicznych” oraz o „innych informacjach przekazywanych za pomocą sieci telekomunikacyjnych”.

Przechodząc do oceny kwestionowanych przez Wnioskodawców przepisów w kontekście powołanych we wniosku wzorców kontroli, należy odnotować, że, zgodnie z art. 2 ustawy zasadniczej, Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady

sprawiedliwości społecznej. Z kolei, art. 47 Konstytucji RP stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Nadto, zgodnie z art. 49 ustawy zasadniczej, zapewnia się wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. W końcu, art. 31 ust. 3 Konstytucji RP stanowi, że ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia, moralności publicznej, albo wolności i praw innych osób, a ograniczenia te nie mogą naruszać istoty wolności i praw.

W doktrynie przyjmuje się, że wolność komunikowania się, ze swej istoty, jako porozumiewanie się określonych osób, związana jest z poufnością, co tradycyjnie obejmuje się określeniem „tajemnica”. Polega ona zarówno na zakazie zmuszania adresatów do ujawniania treści otrzymywanych przekazów, jak i na zakazie adresowanym do wszystkich innych podmiotów, łącznie z organami władzy publicznej, podejmowania prób poinformowania się o tych treściach bez zgody adresata. Co więcej, obejmuje również poufność co do faktu, że jest się w ogóle adresatem określonych przekazów. Jako wolność o charakterze osobistym, także ona potwierdza w szczególny sposób godność osoby ludzkiej. Również na adresatach korespondencji, w wielu sytuacjach, spoczywać będzie obowiązek zachowania poufności, zwłaszcza gdyby ujawnianie treści stanowiło naruszenie prawnie chronionych interesów nadawców, a w szczególności ich prawa do prywatności (por. Paweł Sarnecki, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, III tom, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 49, s. 3).

W literaturze przedmiotu podnosi się również, że władza publiczna ma nie tylko powstrzymywać się od zachowań naruszających prywatność, ale także

respektować kierowany do niej nakaz wprowadzania pozytywnych mechanizmów służących jej efektywnej ochronie. Można zauważyć, że logika takich działań władzy publicznej wynika również w jakimś stopniu z samej zasady proporcjonalności, ponieważ każdej postaci ingerencji dopuszczalnej konstytucyjnie muszą towarzyszyć odpowiednie wymagania dotyczące jakości, precyzyjności regulacji prawnych, a więc rozwiązań pozytywnych, które umożliwiają ochronę przed arbitralnością (por. Marek Safjan, *Prawo do ochrony życia prywatnego i autonomia jednostki w orzecznictwie Trybunału Konstytucyjnego* [w:] *Księga XX – lecia orzecznictwa Trybunału Konstytucyjnego*, Wydawnictwa Trybunału Konstytucyjnego, Warszawa 2006, s. 436).

W nauce prawa konstytucyjnego podkreśla się również wymóg nakazu kompletności ustawowej regulacji ograniczeń praw jednostki. Nakaz kompletności unormowania ustawowego wymaga, aby ustawa samodzielnie określała wszystkie podstawowe elementy ograniczenia danego prawa i wolności (kompletny zarys ograniczenia), bez przekazywania swobody w tym zakresie organom administracji rządowej i samorządowej (por. Jerzy Oniszczyk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Zakamycze 2004, s. 419).

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, doniosłość prawa do prywatności (art. 47 Konstytucji) w systemie konstytucyjnej ochrony praw i wolności uwidacznia m. in. okoliczność, że prawo to jest – zgodnie z art. 233 ust. 1 Konstytucji – nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanie wojennym i wyjątkowym. Oznacza to, że nawet warunki tak wyjątkowe i ekstremalne nie zezwalają ustawodawcy na złagodzenie przesłanek, przy spełnieniu których można wkroczyć w sferę życia prywatnego nie narażając się na zarzut niekonstytucyjnej arbitralności (por. wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, OTK ZU Nr 6/A/2005, poz. 64, s. 813 oraz powołane tam orzecznictwo). Przejawem prawa do prywatności jest

również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe – art. 49 Konstytucji (*ibidem*)

Problematyka wzajemnych relacji pomiędzy unormowaniami dotyczącymi czynności operacyjno – rozpoznawczych, stosowanych przez poszczególne służby (z natury rzeczy niejawnych i dających służbom szeroki margines uznaniowości), a konstytucyjnymi wolnościami i prawami jednostki (zwłaszcza w kontekście gwarancji dla osób poddanych tym czynnościom, a także ograniczonej kontroli zewnętrznej) – niejednokrotnie stanowiła przedmiot rozważań Trybunału Konstytucyjnego.

W szczególności, Trybunał Konstytucyjny, delegalizując między innymi niektóre regulacje zawarte w art. 19 ustawy o Policji, podkreślił, iż „doświadczenia współczesnych państw demokratycznych wskazują, że władza wykonawcza odpowiedzialna za bezpieczeństwo i porządek publiczny, w tym podległe jej podmioty prowadzące czynności operacyjno – rozpoznawcze, dysponują środkami, których zastosowanie – w imię obrony porządku publicznego – może doprowadzić do zniszczenia instytucji demokratycznych i redukcji praw obywatelskich. Dzieje się tak zarówno dlatego, że poufność i brak zewnętrznej kontroli może prowadzić do nadmiernej autonomizacji czy subiektywizacji samego celu działalności operacyjnej oraz niezachowania w niej należytej wstrzemięźliwości przy wkraczaniu w prawa i wolności obywatelskie. Niekiedy zaś sytuacja taka może wynikać z nadmiernie eksponowanych względów ideologicznych czy politycznych w działaniu egzekutywy. Inaczej mówiąc, cecha niejawności kontroli operacyjnej czyni ją podatną na nadużycia. Bezpieczeństwo publiczne, jako dobro co do zasady usprawiedliwiające ograniczenie przez legislatora korzystania z wolności obywatelskich, wymaga więc zachowania proporcjonalności dopuszczalnego wkroczenia w imię ochrony bezpieczeństwa oraz sprawnego systemu kontroli zachowania tej proporcjonalności w praktyce. W przeciwnym razie środki ochrony tego

bezpieczeństwa, w postaci legalnie dopuszczalnej działalności operacyjnej, same w sobie stwarzają zagrożenie dla wolności. Będzie tak wtedy, gdy – po pierwsze – wprowadzane ograniczenia będą arbitralne, nieproporcjonalne do ewentualnych zagrożeń i – po drugie – gdy będą one wyłączone (czy to prawnie, czy faktycznie) spod kontroli sprawowanej przez instytucje demokratyczne. Konflikt między koniecznością istnienia legalnej, prawnie umocowanej działalności operacyjnej i zagrożeniem dla konstytucyjnych wolności i praw jednostki wymaga więc przede wszystkim wyważenia właściwej proporcji w prawnej ochronie obu sfer, pozostających w konflikcie (...). Instrumentarium prawne, umożliwiające wyważenie stosownego kompromisu obejmuje: - z jednej strony, regulację materialnoprawną (określającą granice stawiane przez system prawa wkroczeniu przez władzę w poszczególne sfery prywatności jednostki); - z drugiej zaś – gwarancje proceduralne, towarzyszące temu wkroczeniu, tj. konieczność zgłoszenia kontroli organowi pozapolicyjnemu i jej legalizacji przez ten organ, przesłanki i procedury legalizacji – przez organ zewnętrzny i poprzez udostępnienie zainteresowanemu (choćby w pewnym zakresie i od pewnego momentu czasowego) wiedzy o kontroli i jej rezultatach, środki kontroli na wypadek ekscesu organu przeprowadzającego kontrolę” (wyrok z dnia 12 grudnia 2005 r., sygn. K 32/04, OTK ZU Nr 11/A/2005, poz. 132, s. 1494).

W świetle orzecznictwa Trybunału Konstytucyjnego, zasada proporcjonalności pozostaje w immanentnej więzi z zakazem nadmiernej ingerencji w sferę praw i wolności konstytucyjnych jednostki. Przy ocenie, czy ingerencja była wyrazem konieczności i została przeprowadzona tylko w niezbędnym wymiarze, uwzględnia się specyfikę poszczególnych praw i wolności. Surowsze standardy dotyczą praw osobistych i politycznych niż ekonomicznych i socjalnych. W przypadku konkurencyjności chronionych konstytucyjnie dóbr – jaka występuje jako konflikt pomiędzy konstytucyjnym prawem do prywatności, tajemnicą porozumiewania się oraz ochroną autonomii

informacyjnej a względami bezpieczeństwa publicznego – konieczne jest zachowanie przez ustawodawcę czytelnej równowagi między interesami pozostającymi w kolizji. W ocenie Trybunału Konstytucyjnego, występuje nadto ścisły związek między zagrożeniami dla godności człowieka, stanowiącej podstawę konstytucyjnych wolności i praw jednostki, a wszelkimi czynnościami, które wkraczają w prywatność jednostki. W odniesieniu do prywatności (która na poziomie konstytucyjnym jest chroniona wieloaspektowo i obejmuje kilka praw oraz wolności – określonych w art. 47 – 51 Konstytucji) związek ten jest szczególnie (jakkolwiek nie taki sam w wypadku każdej z tych konstytucyjnych wolności i praw). Zachowanie godności człowieka wymaga poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność „bycia z innymi” czy dzielenia się z innymi przeżyciami czy doznaniem o intymnym charakterze (por. wyrok z dnia 23 czerwca 2009 r., sygn. K 54/07, OTK ZU Nr 6/A/2009, poz. 86, s. 910 oraz powołane tam orzecznictwo).

Wyrokiem z dnia 12 stycznia 2000 r., sygn. P 11/98, wydanym w pełnym składzie Trybunału Konstytucyjnego, Trybunał orzekł, że uzależnienie dopuszczalności ograniczeń praw i wolności od ich ustanowienia „tylko w ustawie” jest czymś więcej niż tylko przypomnieniem ogólnej zasady wyłączności ustawy dla normowania sytuacji prawnej jednostek, stanowiącej klasyczny element idei państwa prawnego. Jest to także sformułowanie wymogu odpowiedniej szczegółowości unormowania ustawowego. Skoro ograniczenia konstytucyjnych praw i wolności mogą być ustanawiane „tylko” w ustawie, to kryje się w tym nakaz kompletności unormowania ustawowego, które musi samodzielnie określać wszystkie podstawowe elementy ograniczenia danego prawa i wolności, tak aby już na podstawie lektury przepisów ustawy można było wyznaczyć kompletny zarys (kontur) tego ograniczenia (por. OTK ZU Nr 1/2000, poz. 3, s. 42).

W końcu, zgodnie z orzecznictwem Trybunału Konstytucyjnego, ustawodawca, ograniczając wskazane prawa i wolności konstytucyjne, winien jednocześnie stworzyć gwarancje prawne i instytucjonalne, pozwalające stosować określone działania tylko w zakresie koniecznym dla realizacji konstytucyjnych celów i w sposób charakteryzujący się jak najmniejszym stopniem dolegliwości dla obywateli i z zastosowaniem określonych procedur. Nakaz ten jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa. Zgodnie z art. 31 ust. 3 Konstytucji, ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności mogą być ustanawiane „tylko w ustawie”. Oznacza to nie tylko konieczność wskazania w akcie normatywnym tej rangi zakresu, w jakim konstytucyjne wolności lub prawa doznają ograniczenia. Z tych samych względów, dla których niedopuszczalne jest odsyłanie w tej materii do aktów wykonawczych, jako naruszenie wymagań konstytucyjnych oceniać należy tak niejasne i nieprecyzyjne formułowanie przepisu., które powoduje niepewność jego adresatów co do ich praw i obowiązków. Powoduje to bowiem stworzenie nazbyt szerokich ram dla organów stosujących ten przepis, które w istocie muszą zastępować prawodawcę w zakresie tych zagadnień, które uregulował on w sposób niejasny i nieprecyzyjny. Ustawodawca nie może poprzez niejasne formułowanie tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki. Założenie to można określić ogólnie jako zasadę określoności ustawowej ingerencji w sferę konstytucyjnych wolności i praw jednostki. Kierując się tą zasadą Trybunał Konstytucyjny reprezentuje stanowisko, iż przekroczenie pewnego poziomu niejasności przepisów prawnych stanowić może samoistną przesłankę stwierdzenia ich niezgodności zarówno z przepisem wymagającym regulacji ustawowej określonej dziedziny (np. ograniczeń w korzystaniu z konstytucyjnych wolności i praw, art. 31 ust. 3 zdanie 1 Konstytucji), jak

i z wyrażoną w art. 2 Konstytucji zasadą państwa prawnego (por. wyrok z dnia 20 kwietnia 2004 r., sygn. K 45/02, OTK ZU Nr 4/A/2004, poz. 30, s. 401 oraz powołane tam orzecznictwo).

Stosowanie kontroli operacyjnej przez służby mundurowe oraz specjalne zawsze stanowi głęboką ingerencję w konstytucyjne prawa i wolności jednostki, w tym w prawo do prywatności, prawo do komunikowania się oraz w autonomię informacyjną. Tym samym, w świetle przytoczonych wyżej poglądów doktryny i orzecznictwa Trybunału Konstytucyjnego, regulacje prawne, dotyczące wkraczania w powyższe prawa osobiste jednostki, muszą odpowiadać szczególnie surowym standardom. Przede wszystkim, regulacje te mogą być zawarte wyłącznie w aktach normatywnych rangi ustawy, przy czym muszą spełniać wymóg kompletności unormowania ustawowego, a więc muszą samodzielnie określać wszystkie podstawowe elementy ograniczenia danego prawa.

Wszystkie zakwestionowane przez Grupę posłów przepisy ustawowe, niezależnie od wykazanych wyżej różnic między nimi, zawierają otwarte katalogi środków technicznych umożliwiających prowadzenie kontroli operacyjnej, polegającej na uzyskiwaniu w sposób niejawną informacji i dowodów oraz ich utrwalaniu. Użycie przez ustawodawcę, w każdym z zaskarżonych unormowań, takich określeń, jak „w szczególności” czy też „i innych informacji” pozostawia organom stosującym omawiane przepisy (w praktyce – służbom mundurowym oraz specjalnym) zbyt szerokie ramy interpretacyjne. W konsekwencji, sprzyja to arbitralności decyzji podejmowanych przez te organy, tak w zakresie użycia poszczególnych rodzajów środków technicznych, jak i charakteru pozyskiwanych informacji, przekazywanych przy pomocy sieci telekomunikacyjnych.

Wspomniana wyżej, nadmierna swoboda interpretacyjna stosownych służb przy podejmowaniu decyzji odnośnie rodzajów stosowanych środków technicznych oraz charakteru pozyskiwanych informacji, może,

w konsekwencji, rodzić niepewność adresatów omawianych norm prawnych co do zakresu ich praw i obowiązków. W szczególności, obywatele nie mają możliwości uzyskania informacji, na podstawie samych przepisów ustawowych, za pomocą jakich konkretnie środków stosowne służby mogą, w sposób niejawnny, wkraczać w sferę konstytucyjnie chronionej ich prywatności oraz swobodę komunikowania się.

Uzasadnienie wniosku Grupy posłów zawiera między innymi wywód wskazujący, iż ustawodawca, formułując zakwestionowane przepisy, posłużył się nieostrym pojęciem „środki techniczne umożliwiające uzyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie”, co może prowadzić do legalizacji posługiwania się przez stosowne służby praktycznie każdym środkiem pozyskiwania informacji, bez żadnych ograniczeń natury technicznej. Analiza argumentacji Wnioskodawców, w omawianym zakresie, zdaje się skłaniać do uznania ich poglądów faktycznych oraz prawnych za zasadne, co jeszcze pogłębia wątpliwości natury konstytucyjnej odnośnie ocenianych unormowań prawnych.

Posłużenie się przez prawodawcę, w ocenianych ustawach, otwartym i nieostro sformułowaniem katalogiem środków umożliwiających uzyskiwanie informacji i dowodów oraz ich utrwalanie, przy faktycznym braku ograniczeń odnośnie rodzajów pozyskiwanych informacji przekazywanych za pomocą sieci telekomunikacyjnych, prowadzi do sytuacji, gdy praktycznym ograniczeniem służb w zakresie kontroli operacyjnej stają się ich możliwości finansowe i (jak słusznie zauważają Wnioskodawcy) dostęp do najnowocześniejszych zdobyczy technologicznych.

Biorąc powyższe pod uwagę, należy – jak się wydaje – uznać, 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 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. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego godzą w zasadę demokratycznego państwa prawnego, prawo do prywatności, prawo do komunikowania się oraz konstytucyjne gwarancje dopuszczalności ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw. Tym samym, zakwestionowane przepisy ustawowe są niezgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 ustawy zasadniczej.

Przechodząc do oceny kwestionowanych przez Wnioskodawców przepisów w kontekście art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, należy odnotować, że, zgodnie z ust. 1 wspomnianego artykułu, każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Z kolei, art. 8 ust. 2 Konwencji stanowi, że niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia, moralności lub ochronę praw i wolności innych osób.

W doktrynie przyjmuje się, że ustęp 2 art. 8 szczegółowo wylicza sytuacje, w których dopuszczalna jest ingerencja w prawo do prywatności, dodając przy tym zastrzeżenie, że musi być ona legalna, a więc przewidziana w prawie krajowym. Tak więc ingerencja w prawo do poszanowania prywatności, mimo iż dokonana w jednej z sytuacji przewidzianych wprost w ust. 2, uznana być może za naruszającą Konwencję, jeżeli nie ma wyraźnej podstawy ustawowej. I odwrotnie: pomimo oparcia ingerencji na prawie krajowym, może być ona uznana za pogwałcenie Konwencji, jeżeli nie jest np. konieczna w społeczeństwie demokratycznym (por. Piotr Hofmański,

Komentarz do wybranych przepisów Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności [w:] *Standardy Prawne Rady Europy, Teksty i komentarze, Tom III Prawo Karne*, Oficyna Naukowa, Warszawa 1997, s. 99).

We wspomnianym wyroku z dnia 23 czerwca 2009 r., sygn. K 54/07, Trybunał Konstytucyjny dokonał krytycznej oceny regulacji, dotyczących kontroli operacyjnej dokonywanej przez Centralne Biuro Antykorupcyjne, w kontekście art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności. Trybunał podzielił przy tym pogląd Europejskiego Trybunału Praw Człowieka, że ingerencja władzy ustawodawczej, wykonawczej lub sądowej w sferę prywatności jest dopuszczalna, o ile odpowiada określonym kryteriom. Każda ingerencja ograniczająca winna w szczególności sprostać wymogom trójszczeblowego testu oceny. Dotyczą one: źródła ograniczenia, jego potrzeby oraz wartości, ze względu na które ograniczenie się wprowadza. Niezbędne jest zaistnienie:

- a) dostatecznie precyzyjnej, a zarazem konkretnej podstawy prawnej wkroczenia w sferę wolności (praw) w drodze ustawy; nie jest dopuszczalne wprowadzania ograniczeń (tu: prywatności) aktami innej rangi,
- b) konieczności tego wkroczenia, rozważanej z punktu widzenia wymogów demokratycznego państwa prawa; niewystarczające jest odwołanie się li tylko do czynnika celowości; niezbędne jest wykazanie konieczności, i to co do konkretnego (opisanego co do zakresu i sposobu) ograniczenia wprowadzonego w ustawie zwykłej, respektującej standard państwa oświeconego, otwartego, tolerancyjnego, dysponującego fachowym aparatem policyjnym zdolnym działać w sposób rzetelny, profesjonalny i niemałostkowy, traktujący wkroczenie w sferę chronionych praw jednostki jako zło konieczne, a nie jako czynnik usprawniający pracę policji,

c) celu ingerencji (chronionego interesu publicznego), wymienionego w art. 8 Konwencji (tj. bezpieczeństwa państwowego, bezpieczeństwa publicznego, dobrobytu gospodarczego kraju, ochrony porządku i zapobiegania przestępstwom, ochrony zdrowia i moralności oraz wolności innych osób).

Nie wystarczy przy tym werbalne powołanie się na taki cel, aby skutecznie legitymizować ograniczenie. Konieczne jest wskazanie realnej potrzeby podjęcia środków ograniczających, i to w imię ochrony zasad demokratycznego porządku. Eksces polegający na tym, że „przy okazji” zbierania materiału operacyjnie przydatnego kontrola operacyjna zgromadzi także dane dotyczące kwestii prywatnych, oznacza działanie władzy poza zakresem dozwolonego wkroczenia w sferę prywatności (por. *op. cit.*, s. 911 – 912 oraz powołane tam orzecznictwo Europejskiego Trybunału Praw Człowieka).

Trybunał Konstytucyjny przypomniał również, że w orzecznictwie Europejskiego Trybunału Praw Człowieka podkreśla się konieczność zbadania, czy w konkretnym przypadku ingerencji w sferę prywatności istniały podstawy uprawniające działania państwa. Działania można uznać za usprawiedliwione, gdy służą celom wymienionym w klauzulach ograniczających (art. 8 ust. 2 Konwencji). Ingerencja musi być przewidziana przez prawo, co oznacza, że stosowane środki mają mieć podstawę w prawie krajowym, przy czym prawo to ma być dostępne osobom zainteresowanym oraz przewidywalne co do swoich skutków. Prawo musi być dostatecznie jasne w swych sformułowaniach, by dać obywatelom odpowiednie wskazówki odnośnie okoliczności i warunków, w jakich władze publiczne są uprawnione do działania w tajemnicy i do potencjalnie niebezpiecznej ingerencji w prawo do życia prywatnego i tajemnicę korespondencji (por. wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, *op. cit.*, s. 821, jak również powołane tam orzecznictwo Europejskiego Trybunału Praw Człowieka).

Jak wywiedziono we wcześniejszej części uzasadnienia niniejszego stanowiska, zakwestionowane przez Wnioskodawców przepisy pozostawiają służbom stosującym kontrolę operacyjną zbyt szeroki zakres swobody interpretacyjnej, poprzez formułowanie otwartych katalogów środków umożliwiających uzyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie, a także w następstwie posłużenia się przez ustawodawcę nieostrą aparaturą pojęciową. Wywody te w pełni zachowują aktualność również przy ocenie wspomnianych przepisów w kontekście art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

Możliwości posłużenia się przez służby mundurowe oraz specjalne określonymi środkami, umożliwiającymi uzyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie, są determinowane – w obowiązującym stanie prawnym – nie tyle unormowaniami ustawowymi, co wspomnianymi już możliwościami finansowymi oraz dostępem tychże służb do najnowszych zdobyczy techniki. Tym samym, możliwość wkraczania w życie prywatne i swobodę komunikowania się nie została w prawie polskim, na szczeblu ustawy, zdefiniowana w sposób wystarczająco jasny. Innymi słowy, dostępne dla obywateli przepisy prawne nie pozwalają tymże obywatelom na wystarczająco pełne rozeznanie, w jakich okolicznościach i na jakich warunkach władze publiczne są uprawnione do uciekania się do działań niejawnych, ingerujących w życie prywatne jednostki.

Biorąc powyższe pod uwagę, przepisy art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 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. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego

należy uznać za niezgodne z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

Zakwestionowane we wniosku Grupy posłów przepisy art. 180a ust. 1 oraz art. 180c Prawa telekomunikacyjnego mają następujące brzmienie:

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

- 1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone zgodnie z przepisami odrębnymi;
- 2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonym w przepisach odrębnych;
- 3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159 – 175 i art. 180e.”;

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

- 1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
 - a) inicjującego połączenie,
 - b) do którego kierowane jest połączenie;
- 2) określenia:
 - a) daty i godziny połączenia oraz czasu jego trwania,

- b) rodzaju połączenia,
- c) lokalizacji telekomunikacyjnego urządzenia końcowego.

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

- 1) szczegółowy wykaz danych, o których mowa w ust. 1;
- 2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych.”.

Zakwestionowany przez Wnioskodawców przepis art. 20c ustawy o Policji ma następujące brzmienie:

„Art. 20c. 1. 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 (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”, oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:

- 1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
- 2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
- 3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

2a. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.

5. Udostępnianie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:

- 1) wykorzystywane sieci telekomunikacyjne zapewniają:
 - a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
- 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.

6. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi.

7. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.”.

Zakwestionowany we wniosku Grupy posłów przepis art. 10b ustawy o Straży Granicznej brzmi następująco:

„Art. 10b. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”, w trybie:

- 1) pisemnego wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
 - 2) ustnego żądania funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
 - 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1
- oraz może przetwarzać te dane.

2. W przypadku, o którym mowa w ust. 1 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Straży Granicznej a tym podmiotem.

3. Podmiot wykonujący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne, funkcjonariuszowi wskazanemu we wniosku właściwego organu Straży Granicznej lub funkcjonariuszowi, o którym mowa w ust. 1 pkt 2 i 3.

4. Udostępnienie Straży Granicznej danych telekomunikacyjnych może nastąpić przy pomocy sieci telekomunikacyjnej, jeżeli:

- 1) wykorzystywane sieci telekomunikacyjne zapewniają:
 - a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w których zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
- 2) jest to uzasadnione specyfiką lub zakresem wykonywanych przez jednostki organizacyjne Straży Granicznej zadań albo prowadzonych przez nie czynności.

5. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego, Straż Graniczna przekazuje właściwemu prokuratorowi.

6. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznie komisyjnemu i protokolarnemu zniszczeniu.”.

Zakwestionowany przez Grupę posłów przepis art. 36b ustawy o kontroli skarbowej ma następującą treść:

„Art. 36b. 1. W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12, wywiad skarbowy może mieć udostępniane dane:

- 1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”,
- 2) identyfikujące podmiot korzystający z usług pocztowych oraz dotyczące faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług

- oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1:

- 1) na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej;
- 2) na pisemny wniosek pracownika wywiadu skarbowego posiadającego pisemne upoważnienie Generalnego Inspektora Kontroli Skarbowej do występowania w jego imieniu o udostępnienie danych, o których mowa w ust. 1;

- 3) za pośrednictwem sieci telekomunikacyjnej pracownikowi wywiadu skarbowego posiadającemu pisemne upoważnienie, o którym mowa w pkt 2.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Generalnym Inspektorem Kontroli Skarbowej a tym podmiotem.

4. Podmiot występujący z wnioskiem, o którym mowa w ust. 2, informację o wystąpieniu z wnioskiem przekazuje niezwłocznie ministrowi właściwemu do spraw finansów publicznych. Minister właściwy do spraw finansów publicznych w każdej chwili może zażądać od Generalnego Inspektora Kontroli Skarbowej informacji o przyczynach uzasadniających wystąpienie z wnioskiem, a także o sposobie wykorzystania danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe.

5. Minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, o którym mowa w ust. 2, za nieuzasadnione.

6. Udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:

- 1) możliwość ustalenia pracownika wywiadu skarbowego uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane;
- 2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych.

7. Udostępnianie wywiadowi skarbowemu danych, o których mowa w ust. 1, następuje na koszt podmiotu prowadzącego działalność telekomunikacyjną i operatora świadczącego usługi pocztowe.”.

Zakwestionowany we wniosku Grupy posłów przepis art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych ma następujące brzmienie:

„Art. 30. 1. W celu zapobiegania lub wykrywania przestępstw, w tym skarbowych, Żandarmeria Wojskowa, może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”, oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:

- 1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej,
- 2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
- 3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

2a. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem.

4. Udostępnianie Żandarmerii Wojskowej danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

- 1) wykorzystywane sieci i system teleinformatyczny zapewniają:

- a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostępu do danych,
- 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności.

5. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego, Żandarmeria Wojskowa przekazuje właściwemu prokuratorowi wojskowemu.

6. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.”.

Zakwestionowany przepis art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu brzmi następująco:

„Art. 28. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez ABW zadań, o których mowa w art. 5 ust. 1, w postaci danych:

- 1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);
- 2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Podmiot wykonujący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio:

- 1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ;

- 2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW;
- 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem.

4. Udostępnianie ABW danych, o których mowa w ust. 1 pkt 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:

- 1) możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane;
- 2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych.”.

Zakwestionowany przez Grupę posłów przepis art. 18 ustawy o Centralnym Biurze Antykorupcyjnym ma następującą treść:

„Art. 18. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 17, nie dotyczy informacji niezbędnych do realizacji przez CBA zadań określonych w art. 2, w postaci danych:

- 1) o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwanych dalej „danymi telekomunikacyjnymi”,
- 2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług

2. Podmiot wykonujący działalność telekomunikacyjną lub podmiot uprawniony do wykonywania działalności pocztowej udostępnia nieodpłatnie dane, o których mowa w ust. 1:

- 1) na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej;
- 2) na ustne żądanie funkcjonariusza CBA, posiadającego pisemne upoważnienie Szefa CBA lub osoby przez niego upoważnionej;
- 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi CBA posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

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

4. Udostępnienie CBA danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

- 1) sieć zapewnia:
 - a) możliwość ustalenia funkcjonariusza CBA uzyskującego te dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do uzyskanych danych;
- 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne CBA albo prowadzonych przez nie czynności.”.

Zakwestionowany we wniosku Grupy posłów przepis art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ma następujące brzmienie:

„Art. 32. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 31 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez SKW zadań określonych w art. 5, w postaci danych:

- 1) o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwanych dalej „danymi telekomunikacyjnymi”;

- 2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Udostępnianie przez przedsiębiorcę telekomunikacyjnego lub operatora świadczącego usługi pocztowe danych, o których mowa w ust. 1, następuje nieodpłatnie:

- 1) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej;
- 2) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW;
- 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW.

3. O udostępnieniu danych w trybie określonym w ust. 2 pkt 2 przedsiębiorca telekomunikacyjny lub operator świadczący usługi pocztowe informuje Szefa SKW.

4. Przedsiębiorca telekomunikacyjny oraz operator świadczący usługi pocztowe są obowiązani udostępnić dane, o których mowa w ust. 1, funkcjonariuszom wskazanym we wniosku.

5. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem SKW a tym podmiotem.

6. Udostępnienie SKW danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

- 1) wykorzystywane sieci i system teleinformatyczny zapewniają:
 - a) możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych;

- 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez SKW albo prowadzonych przez nią czynności.”.

Przed przystąpieniem do oceny zakwestionowanych przepisów w kontekście wskazanych przez Wnioskodawców wzorców kontroli, jak się wydaje, należałoby dokonać zwięzłego porównania niektórych regulacji zawartych w unormowaniach dotyczących prowadzenia kontroli operacyjnej przez poszczególne służby mundurowe i specjalne. Już wstępna analiza brzmienia wspomnianych unormowań pozwala na wysnucie wniosku, że regulacje w nich zawarte, w sposób istotny, różnią się merytorycznie między sobą, w zakresie stanowiącym przedmiot wniosku Grupy posłów (pomijając uprawnienia niektórych służb do pozyskiwania informacji od operatorów świadczących usługi pocztowe, jak również pomijając liczne różnice stylistyczno - językowe).

Policja, Straż Graniczna i Żandarmeria Wojskowa mogą mieć udostępniane dane telekomunikacyjne, jak również mogą je przetwarzać w celu zapobiegania lub wykrywania przestępstw (art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej oraz art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych). Analogiczne kompetencje wywiadu skarbowego zostały ograniczone do przestępstw skarbowych, jak również poszerzone o zapobieganie i wykrywanie naruszeń krajowych przepisów celnych oraz ściganie naruszeń krajowych lub wspólnotowych przepisów celnych przez wykonywanie nadzoru transgranicznego osób, miejsc, środków transportu i towarów oraz dostawy kontrolowanej, w rozumieniu Konwencji sporządzonej na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi, sporządzonej w Brukseli dnia 18 grudnia 1997 r. (art. 36b ust. 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej).

Nieporównanie szersze kompetencje w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych przyznał ustawodawca Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu oraz Służbie Kontrwywiadu Wojskowego. Wymienione wyżej służby uzyskały omawiane kompetencje odnośnie wszelkich informacji niezbędnych do realizacji ich zadań ustawowych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA oraz art. 32 ust. 1 ustawy o SKW oraz SWW). Kompetencje te nie ograniczają się do rozpoznawania, zapobiegania oraz wykrywania przestępstw. Przykładowo, należałoby odnotować, że w odniesieniu do ABW i SKW obejmują one również zadania związane z ochroną informacji niejawnych, w odniesieniu do ABW rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa, natomiast w odniesieniu do SKW – uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej jednostek organizacyjnych MON, uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia, ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami o przeznaczeniu wojskowym. Z kolei, zdecydowanie odmienny zakres zadań określił ustawodawca CBA, zlecając tej służbie kontrolę prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem

Skarbu Państwa lub innych państwowych osób prawnych, ujawnianie przypadków nieprzestrzegania określonych przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych. W końcu katalogi zadań wszystkich trzech omawianych tu służb mają charakter katalogów otwartych, zawierają bowiem klauzule o „podejmowaniu innych działań” określonych (przewidzianych) w odrębnych ustawach i umowach międzynarodowych (art. 5 ust. 1 pkt 5 ustawy o ABW oraz AW, art. 2 ust. 1 pkt 7 ustawy o CBA oraz art. 5 ust. 1 pkt 9 ustawy o SKW oraz SWW).

Innymi słowy, ustawodawca wyraźnie zróżnicował uprawnienia służb mundurowych i specjalnych odnośnie pozyskiwania i przetwarzania danych telekomunikacyjnych, odmiennie określając przypadki upoważniające do podejmowania tego rodzaju kontroli operacyjnej (nawiązujące do ustawowych zadań tychże służb) i przyznając zdecydowanie najszersze uprawnienia w tym zakresie funkcjonariuszom CBA.

Wydaje się, że już w tym miejscu należałoby również odnotować, iż funkcjonariusze ABW, CBA oraz SKW zostali zwolnieni przez ustawodawcę, w sposób wyraźny, z obowiązku uzyskania zgody sądu na pozyskiwanie danych telekomunikacyjnych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW oraz SWW). Na pozostałe, wymienione we wniosku Grupy posłów, służby ustawodawca nie nałożył obowiązku uzyskiwania takiej zgody podczas wykonywania omawianej kontroli operacyjnej. Tym samym, przepisy dotyczące ABW, CBA oraz SKW podlegają ocenie wprost w omawianym zakresie, zaś regulacje dotyczące pozostałych służb należałoby przeanalizować w tym zakresie w kontekście ewentualnego pominięcia legislacyjnego.

Z kolei, unormowania dotyczące prowadzenia kontroli operacyjnej przez Policję, Straż Graniczną i Żandarmerię Wojskową zawierają (dość syntetyczne skądinąd) regulacje przewidujące zniszczenie materiałów, które nie zawierają informacji mających znaczenie dla postępowania karnego (art. 20c ust. 7 ustawy o Policji, art. 10b ust. 6 ustawy o Straży Granicznej oraz art. 30 ust. 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Przepis art. 36b ust. 5 ustawy o kontroli skarbowej przewiduje dyskrecyjne uprawnienie ministra właściwego do spraw finansów, który nakazuje zniszczenie takich materiałów, o ile uzna za niezasadne wcześniejsze wystąpienie z wnioskiem przez Generalnego Inspektora Kontroli Skarbowej lub pracownika wywiadu skarbowego o udostępnienie tychże danych. Analizowane przepisy ustaw: o ABW oraz AW, o CBA ani o SKW oraz SWW stosownych regulacji, dotyczących ewentualnego niszczenia materiałów nieprzydatnych dla dalszego prowadzenia postępowania, nie zawierają.

W końcu, żaden z omawianych przepisów, normujących uzyskiwanie danych telekomunikacyjnych przez stosowne służby, nie zawiera regulacji przewidujących obowiązek poinformowania jednostki o pozyskiwaniu wspomnianych wyżej danych, dotyczących jej osoby, chociażby po zakończeniu postępowania, ani unormowań ograniczających możliwość pozyskiwania danych, które nie mogą być wykorzystywane dla potrzeb postępowania karnego (to jest informacji chronionych na podstawie tajemnicy lekarskiej, obrończej, dziennikarskiej itp.).

Reasumując tę część rozważań, należałoby odnotować, że część zarzutów, podniesionych przez Wnioskodawców w stosunku do unormowań dotyczących poszczególnych służb prowadzących kontrolę operacyjną, dotyczy regulacji zawartych w zaskarżonych przepisach, ale wiele z tych zarzutów dotyczy materii, które w analizowanych przepisach nie zostały unormowane. W tej sytuacji istotnego znaczenia nabiera kwestia dopuszczalnego kształtu zarzutów formułowanych w stosunku do norm prawnych w postępowaniu przed

Trybunałem Konstytucyjnym, a zwłaszcza rozróżnienia pomiędzy zaniechaniem prawodawczym a pominięciem prawodawczym.

W literaturze przedmiotu przyjmuje się, że w przypadku aktu ustawodawczego wydanego i obowiązującego, Trybunał Konstytucyjny ma kompetencję do oceny jego konstytucyjności z tego punktu widzenia, czy w jego przepisach nie brakuje unormowań, bez których, ze względu naturę objętej aktem regulacji, może on budzić wątpliwości natury konstytucyjnej. Zarzut niekonstytucyjności może więc dotyczyć zarówno tego, co ustawodawca w danym akcie unormował, jak i tego, co w akcie tym pomiął, choć, postępując zgodnie z Konstytucją, powinien był unormować (por. Jerzy Oniszczyk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Zakamycze 2000, s. 758).

W doktrynie dominuje pogląd, że z podlegającym kognicji Trybunału Konstytucyjnego pominięciem prawodawczym mamy do czynienia, gdy jakiś akt normatywny lub jego część ma zbyt wąski zakres zastosowania lub normowania, co jest niezgodne z Konstytucją (por. Piotr Tuleja, *Podstawowe problemy związane z interpretacją Konstytucji Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego. Trybunał Konstytucyjny – między hierarchiczną kontrolą norm a ochroną praw człowieka* [w:] *Księga XX – lecia orzecznictwa Trybunału Konstytucyjnego*, Trybunał Konstytucyjny, Wydawnictwa, Warszawa 2006, s. 223).

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, Trybunał nie ma kompetencji do orzekania o zaniechaniach ustawodawcy polegających na niewydaniu aktu ustawodawczego, choćby obowiązek jego wydania wynikał z norm konstytucyjnych. W przypadku natomiast aktu ustawodawczego wydanego i obowiązującego Trybunał Konstytucyjny ma kompetencję do oceny jego konstytucyjności również z tego punktu widzenia, czy w jego przepisach nie brakuje unormowań, bez których, ze względu na naturę objętej aktem regulacji, może on budzić wątpliwości natury

konstytucyjnej. Zarzut niekonstytucyjności może więc dotyczyć zarówno tego, co ustawodawca w danym akcie unormował, jak i tego, co w akcie tym pomiął, choć, postępując zgodnie z Konstytucją, powinien był unormować. Prowadzi to do wniosku, że o ile parlamentowi przysługuje bardzo szerokie pole decyzji, jakie materie wybrać dla normowania w drodze stanowionych przez siebie ustaw, to skoro decyzja taka zostanie już podjęta, regulacja danej materii musi zostać dokonana przy poszanowaniu wymagań konstytucyjnych (por. wyrok z dnia 24 października 2001 r., sygn. SK 22/01, OTK ZU Nr 7/2001, poz. 216, s. 1092 oraz powołane tam orzecznictwo).

W tym miejscu należałoby również odnotować, że wspomnianym już wyrokiem z dnia 20 kwietnia 2004 r., sygn. K 45/02, Trybunał Konstytucyjny orzekł m. in. o niekonstytucyjności przepisu normującego czynności operacyjno – rozpoznawcze Agencji Bezpieczeństwa Wewnętrznego (art. 23 ust. 1 pkt 6 ustawy o ABW oraz AW), wobec jego kolizji z szeregiem wzorców kontroli (w tym z art. 51 ust. 2 Konstytucji RP), podkreślając, że kontrola konstytucyjności dotyczyła w tym wypadku obowiązującego aktu normatywnego, z punktu widzenia tego, czy w jego przepisach nie brakuje unormowań, bez których może on budzić wątpliwości natury konstytucyjnej (por. *op. cit.*, s. 402).

W świetle przytoczonych wyżej poglądów doktryny oraz orzecznictwa Trybunału Konstytucyjnego wydaje się, że wskazane przez Wnioskodawców materie, których nie unormowano w zaskarżonych przepisach, mają istotne znaczenie z punktu widzenia chronionych przez ustawę zasadniczą praw do prywatności i tajemnicy komunikowania się oraz autonomii informacyjnej. Tym samym, jak się wydaje, można bronić poglądu, że w analizowanych unormowaniach zachodzą przypadki pominięcia prawodawczego, podlegającego kognicji Trybunału Konstytucyjnego.

Przechodząc do oceny kwestionowanych przez Grupę posłów przepisów w kontekście prawa do autonomii informacyjnej, wypada odnotować, że, zgodnie z art. 51 ust. 2 Konstytucji RP, władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Z kolei, art. 51 ust. 4 Konstytucji RP stanowi, że każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a ograniczenia tego prawa może określać ustawa. Wnioskodawcy zaproponowali również kontrolę zaskarżonych przepisów w kontekście omawianych już wcześniej wzorców zawartych w art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 ustawy zasadniczej. W końcu, jak się wydaje, nie sposób pominąć w tym miejscu art. 51 ust. 5 Konstytucji RP, zgodnie z którym zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

W doktrynie przyjmuje się, że, gwarantując prawo do prywatności, nie może Konstytucja – w sposób generalny – pozwalać organom władzy publicznej ani na dokumentowanie dla własnych celów tzw. danych osobowych, czyli informacji o osobowych właściwościach (indywidualnych cechach) konkretnych jednostek, ani też zezwalać owym organom na penetrowanie i dokumentowanie zachowań osób prywatnych, ani też w końcu zmuszać te osoby do ujawniania swych cech, właściwości oraz swego osobistego postępowania, i tu już nie tylko wobec wspomnianych organów, ale wobec kogokolwiek. Z kolei, gdy, w dopuszczalnych granicach ustawowych, zbiory danych osobowych wytworzone przez uprawnione podmioty (organy władzy publicznej, i to tylko we wskazanym zakresie) już funkcjonują – prawo do prywatności, ale również wymóg ochrony godności ludzkiej, sama natura praw osobistych, do których i one należą, oraz zasada demokratycznego państwa prawnego – wymagają zagwarantowania dostępu do takich danych, wnoszenia sprostowań oraz ewentualnie żądania usunięcia pewnych z nich (por. Paweł Sarnecki

[w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Tom III, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 51, s. 3).

W literaturze przedmiotu podnosi się również, że niezwykle istotne jest stworzenie bariery w nieograniczonym pozyskiwaniu, gromadzeniu i udostępnianiu informacji o osobach przez władze publiczne, nawet za (konieczną w świetle ust. 1 art. 51 Konstytucji RP) zgodą ustawodawcy. Jak wykazują doświadczenia innych państw, administracja i inne władze publiczne skłonne są do gromadzenia nadmiernych ilości informacji o obywatelach i zbędnego – w świetle ustrojowej zasady pomocniczości – wkraczania w ich życie prywatne i rodzinne. Informacja, jako część wstępnej fazy procesu decyzyjnego, jest jego podstawą i przygotowaniem. Powinna więc być uzasadniona potrzebami wspólnoty, interesem demokratycznego państwa prawnego. Tylko informacje naprawdę niezbędne w takim państwie mogą być pozyskiwane, gromadzone (w tym elektronicznie przetwarzane) i udostępniane przez władze publiczne. W przypadku sporu, czy ustawodawca nie posunął się za daleko w nałożeniu obowiązków informacyjnych albo w wyposażeniu organów państwa w kompetencje do pozyskiwania, gromadzenia i udostępniania informacji, co może nastąpić również bez zgody obywatela, rozstrzygać o stopniu „niezbędności” informacji ma Trybunał Konstytucyjny, który, w tym znaczeniu, ma stać się podmiotem chroniącym przed „złym ustawodawcą” (por. Irena Lipowicz [w:] *Konstytucje Rzeczypospolitej oraz Komentarz do Konstytucji RP z 1997 roku*, Wrocław 1998, s. 99).

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, ochrona życia prywatnego, gwarantowana konstytucyjnie co do zasady w art. 47, obejmuje sobą także autonomię informacyjną (art. 51 Konstytucji RP), oznaczającą prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów (por.

wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, *op. cit.*, s. 813 oraz powołane tam orzecznictwo).

W świetle orzecznictwa Trybunału Konstytucyjnego, istnienie w art. 51 ust. 2 Konstytucji odrębnej regulacji, dotyczącej proporcjonalności wkraczania w prywatność jednostki, należy tłumaczyć tym, że naruszenie autonomii informacyjnej, poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki. Autonomia informacyjna, której wyodrębnienie normatywne z całości ochrony prywatności przewiduje art. 51 ustawy zasadniczej, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Normatywne wyodrębnienie, ustanowione w art. 51 ust. 2 Konstytucji, odrębnego zakazu – ułatwia dostrzeżenie takiego wkroczenia i upraszcza przedmiot dowodu, iż takie wkroczenie nastąpiło. Przedmiotem dowodu staje się wtedy bowiem tylko to, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne” lub „użyteczne” dla władzy. Dowodu wymaga, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym. Analiza relacji przepisów art. 31 ust. 3 i art. 51 ust. 2 Konstytucji uzasadnia stwierdzenie, że naruszenie autonomii informacyjnej przez pozyskiwanie informacji o obywatelach powinno odpowiadać wymaganiom określonym w art. 31 ust. 3 Konstytucji (por. wyroki: z dnia 20 listopada 2002 r., sygn. K 41/02, OTK ZU Nr 6/A/2002, poz. 83, s. 1112 oraz z dnia 17 czerwca 2008 r., sygn. K 8/04, OTK ZU Nr 5/A/2008, poz. 81, s. 812 – 813).

Trybunał Konstytucyjny podkreślał również, że czynności operacyjne służb państwowych pozostają usprawiedliwione, o ile ich celem jest obrona wartości demokratycznych państwa prawnego. Wymogiem konstytucyjnym jest to, by sprostąły one testowi „konieczności w demokratycznym państwie prawnym”. Nie wystarczy ich celowość, użyteczność, taniość czy łatwość

posługiwania się przez władzę. Nie ma rozstrzygającego znaczenia argument, że podobne środki są stosowane w innych państwach. Usprawiedliwione jest stosowanie środków niezbędnych w tym sensie, że chronią wartości istotne w państwie demokratycznym, i to w sposób (bądź w stopniu), który nie mógłby zostać osiągnięty przy stosowaniu innych środków. Jednocześnie winny to być „środki najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają – w wyniku stosowania tych środków – ograniczeniu” (por. wyrok z dnia 23 czerwca 2009 r., sygn. K 54/07, *op. cit.*, s. 910 oraz powołane tam orzecznictwo).

W końcu, zgodnie z orzecznictwem Trybunału Konstytucyjnego, dotyczącym kontroli konstytucyjności czynności operacyjno - rozpoznawczych (realizowanych tak przez Policję, jak i przez Centralne Biuro Antykorupcyjne), gdy idzie o autonomię informacyjną, art. 51 Konstytucji kreuje m. in., oprócz obowiązków ciążących na władzy państwowej, dwa prawa podmiotowe:

- dostępu do dokumentów i zbiorów danych (przy czym ustawodawca zwykły może tu określić ograniczenia, co wynika z art. 51 ust. 3 Konstytucji, a jego swoboda w tym zakresie jest większa, niż na tle ograniczeń przewidzianych w art. 49 Konstytucji),
- prawo „każdego” do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych oraz zebranych w sposób sprzeczny z ustawą (art. 51 ust. 4 Konstytucji). Charakterystyczny jest sposób ujęcia tego ostatniego prawa. Nie przewiduje ono – w przeciwieństwie do prawa z art. 51 ust. 3 Konstytucji – w ogóle możliwości ograniczeń wprowadzonych w drodze ustawy zwykłej. Pod tym względem art. 51 ust. 4 jest skonstruowany identycznie jak art. 47 Konstytucji. Artykuł 51 ust. 4 mówi o szczególnym uprawnieniu wynikającym z ogólnej zasady art. 47 Konstytucji, obejmującej prawo do przedstawiania/kształtowania swego publicznego obrazu, rysującego się na tle danych zebranych przez władzę. Prawo to obejmuje żądanie sprostowań oraz usunięcia informacji niepełnych, nieprawdziwych lub zebranych w sposób

sprzeczny z ustawą. Spod działania tego prawa nie są bynajmniej wyłączone informacje zebrane w drodze działalności operacyjnej. Ponieważ jednak dane pochodzące z kontroli operacyjnej nie są ujawniane wobec zainteresowanego przy rozpoczęciu i w czasie trwania kontroli operacyjnej, przeto możliwość skorzystania z uprawnienia, o którym mowa w art. 51 ust. 4 Konstytucji, *de facto* jest ograniczona. Należy zauważyć, że na tle systematyki art. 51 Konstytucji regulacja prawa podmiotowego z art. 51 ust. 4 wyprzedza regulację zawartą w art. 51 ust. 5 Konstytucji. W tym ostatnim przepisie mówi się, że ustawa zwykła może określać zasady i tryb gromadzenia oraz udostępniania informacji. Argument *a rubrica* wskazuje więc na to, że na tle polskiej Konstytucji jakkolwiek przedmiot, zakres i gwarancje związane z prowadzeniem działań operacyjnych (niezbędnych – co do zasady – we współczesnym państwie) są regulowane przez ustawodawstwo zwykłe (art. 51 ust. 5 Konstytucji), to jednak takie ustawodawstwo musi obracać się w konstytucyjnych ramach wskazanych w art. 49 i art. 51, przewidujących możliwość i zasady współokreślania (ujętego zresztą w różny sposób na tle każdego z tych przepisów) przez ustawodawcę zwykłego kwestii uregulowanych w art. 49, a także w art. 51 ust. 1, 2 (w związku z ust. 5) i 3 Konstytucji. Nie przewidziano natomiast takiej możliwości współdziałania ustawodawcy zwykłego dla prawa uregulowanego przez art. 51 ust. 4 Konstytucji. Ustawodawca zwykły, nawet nie wykonując konstytucyjnego upoważnienia do współokreślania (przez kształtowanie wyjątków) konstytucyjnie chronionych wolności/praw, lecz wykonujący swoją „zwyczajną” działalność, normując jakieś inne kwestie, może jednak, niejako przypadkiem, wkroczyć w sferę wolności/praw konstytucyjnych. W takim wypadku ocena proporcjonalności wkroczenia musi jednak odbywać się wedle surowszych kryteriów, niż w wypadku, gdy sama Konstytucja przyznaje ustawodawcy możliwość kreacji ograniczeń, w odniesieniu do konstytucyjnie normowanej wolności/prawa. Inaczej mówiąc: na tle unormowań w art. 49

i art. 51 ust. 4 Konstytucji proporcjonalność wkroczenia ustawodawcy zwykłego będzie oceniana wedle kryteriów łagodniejszych – w pierwszym i surowszych – w drugim wypadku (por. wyroki: z dnia 12 grudnia 2005 r., sygn. K 32/04, *op. cit.*, s. 1499 – 1500 oraz z dnia 23 czerwca 2009 r., sygn. K 54/07, *op. cit.*, s. 911).

Obowiązek operatora publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych udostępniania danych telekomunikacyjnych omawianym w uzasadnieniu niniejszego stanowiska służbom stanowi wyjątek od zasady zobowiązującej wspomniane wyżej podmioty do zachowania tajemnicy telekomunikacyjnej i szerszej zasady ochrony danych osobowych. Zgodnie z art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami), za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Z kolei, art. 160 ust. 1 Prawa telekomunikacyjnego stanowi, że podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące są obowiązane do zachowania tajemnicy telekomunikacyjnej. Nadto, zgodnie z art. 159 ust. 1 Prawa telekomunikacyjnego, tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana „tajemnicą telekomunikacyjną”, obejmuje: dane dotyczące użytkownika; treści indywidualnych komunikatów; dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku; dane o próbach uzyskania połączenia między zakończeniami sieci,

w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwania zestawianych połączeń. W końcu, art. 159 ust. 4 Prawa telekomunikacyjnego stanowi, że z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej.

Wspomniane wyżej unormowania prawne przesądzają, że tajemnica telekomunikacyjna obejmuje nie tylko samą treść przekazu (komunikatu, rozmowy), ale również dane dotyczące użytkowników, dane lokalizacyjne urządzenia końcowego czy też dane o próbach uzyskania połączeń. Wkraczanie w sferę tajemnicy telekomunikacyjnej możliwe jest, co do zasady, jedynie w drodze aktu normatywnego rangi ustawy (co będzie jeszcze przedmiotem rozważań w dalszej części uzasadnienia niniejszego stanowiska). Wydaje się natomiast, że w pierwszej kolejności należałoby rozważyć problematykę konieczności i proporcjonalności ograniczeń prawa do prywatności, swobody komunikowania się oraz autonomii informacyjnej wprowadzanych przez kwestionowane unormowania, a także zakres regulacji gwarancyjnych, mających chronić jednostkę przed nieuzasadnionym lub nadmiernym wkraczaniem przez omawiane służby w jej prawa i wolności konstytucyjne.

Analiza zakwestionowanych przez Grupę posłów przepisów pozwala na wysnucie wniosku, że decyzja o pozyskaniu danych telekomunikacyjnych pozostaje w gestii stosownych służb mundurowych bądź specjalnych. Jak wspomniano we wcześniejszej części uzasadnienia niniejszego stanowiska, w praktyce dane takie udostępniane są funkcjonariuszowi (żołnierzowi, pracownikowi) wskazanemu w pisemnym wniosku jego przełożonego odpowiedniej rangi lub posiadającemu pisemne upoważnienie takiego przełożonego bądź takiemu funkcjonariuszowi – za pośrednictwem sieci

telekomunikacyjnej (art. 20c ust. 2 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 2 ustawy o kontroli skarbowej, art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 2 ustawy o ABW oraz AW, art. 18 ust. 2 ustawy o CBA oraz art. 32 ust. 2 ustawy o SKW oraz SWW). Obowiązek udostępnienia danych telekomunikacyjnych przez operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych zachodzi w każdym przypadku, gdy zwrócić się o to uprawnione służby (art. 180a ust. 1 pkt 2 w związku z art. 180c ust. 1 Prawa telekomunikacyjnego).

W przeciwieństwie do przepisów normujących kontrolę operacyjną w postaci, przykładowo, podsłuchu (art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o Straży Granicznej, art. 36c ust. 1 ustawy o kontroli skarbowej, art. 31 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA, jak również art. 31 ust. 1 ustawy o SKW oraz SWW), omawiane regulacje nie przyjmują subsydiarnego charakteru pozyskiwania danych telekomunikacyjnych. Tym samym, uprawnione służby zawsze mogą domagać się udostępnienia danych telekomunikacyjnych lub pobierać je samodzielnie, a nie tylko wtedy, gdy inne środki pozyskania informacji okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne. Innymi słowy, oceniane unormowania, ze względów oczywistych, nie są w stanie sprostać testowi „konieczności w demokratycznym państwie prawnym” w rozumieniu przytoczonego wyżej orzecznictwa Trybunału Konstytucyjnego.

Zarzut braku ustanowienia przez ustawodawcę warunku subsydiarności pozyskiwania przez służby danych telekomunikacyjnych nabiera szczególnej ostrości w przypadku, gdy służby te realizują swe uprawnienia w omawianym zakresie nie tylko w celu zapobiegania lub wykrywania przestępstw (zwłaszcza tych najgroźniejszych), ale w celu realizacji innych zadań ustawowych. Tytułem przykładu można tu wymienić chociażby pozyskiwanie przez funkcjonariuszy

Centralnego Biura Antykorupcyjnego danych telekomunikacyjnych w celu przeprowadzenia kontroli prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, przy wcześniejszym pominięciu jakichkolwiek innych czynności, które mogłyby doprowadzić do uzyskania koniecznych informacji (art. 2 ust. 1 pkt 5 ustawy o CBA).

W tym miejscu należałoby również odnotować, że brak regulacji, statuujących zasadę subsydiarności przy pozyskiwaniu danych telekomunikacyjnych przez stosowne służby, zakwestionował również (w kontekście art. 49 w związku z art. 31 ust. 3 Konstytucji RP) Rzecznik Praw Obywatelskich w wystąpieniu do Prezesa Rady Ministrów z dnia 17 stycznia 2011 r., nr RPO – 662587 – II – 10/ST. W wystąpieniu tym podkreślono między innymi, że przepisy dotyczące udostępniania danych, o których mowa w art. 180c i 180d Prawa telekomunikacyjnego, nie wprowadzają zasady subsydiarności. Obowiązek udostępnienia danych aktualizuje się po stronie podmiotu wykonującego działalność telekomunikacyjną w każdym przypadku, gdy zwrócić się o to odpowiednie służby, a nie tylko wówczas, gdy inne środki podejmowane w celu realizacji ustawowego celu okazały się bezskuteczne (por. s. 11 powołanego pisma RPO).

Jak wspomiano we wcześniejszej części uzasadnienia niniejszego stanowiska, ustawodawca zwolnił funkcjonariuszy ABW, CBA oraz SKW z obowiązku uzyskania zgody sądu na pozyskiwanie danych telekomunikacyjnych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW oraz SWW). Na pozostałe, wymienione we wniosku Grupy posłów, służby ustawodawca nie nałożył obowiązku uzyskiwania takiej zgody podczas wykonywania omawianej kontroli operacyjnej. Tym samym, ocenione działania służb nie zostały poddane żadnej kontroli ze strony sądu (ani wstępnej, ani nawet następcej), pomimo że ustawodawca wprowadził taką kontrolę w przypadku podejmowania przez

służby kontroli operacyjnej, ograniczającej te same prawa i wolności konstytucyjnie chronione, to jest w przypadku podsłuchu (art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o Straży Granicznej, art. 36c ust. 1 ustawy o kontroli skarbowej, art. 31 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA, jak również art. 31 ust. 1 ustawy o SKW oraz SWW).

Rezygnując z sądowej kontroli omawianej postaci kontroli operacyjnej, ustawodawca usunął podstawowy czynnik gwarancyjny, mający chronić obywateli przed nieuprawnionym wkraczaniem służb w sferę prywatności, swobody komunikowania się i autonomii informacyjnej jednostki. Innymi słowy, jak się wydaje, należałoby podzielić pogląd Grupy posłów, wyrażony w analizowanym wniosku, iż brak sądowej kontroli pozyskiwania przez służby danych telekomunikacyjnych przesądza o deficycie regulacji gwarancyjnych w zakresie kontroli zewnętrznej omawianej działalności tychże służb.

We wspomnianym wystąpieniu Rzecznika Praw Obywatelskich z dnia 17 stycznia 2011 r. zawarto pogląd prawny, iż w polskiej rzeczywistości konstytucyjnej ramy kontroli zewnętrznej wyznacza przede wszystkim art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP. Treść art. 77 ust. 2 Konstytucji RP przesądza w zasadzie o tym, że w sprawach dotyczących konstytucyjnych wolności i praw (a więc także w sprawie objętej zakresem art. 49 Konstytucji RP) takim zewnętrznym organem kontroli powinien być sąd (por. s. 21 wystąpienia).

Wnioskodawcy nie zaproponowali kontroli zakwestionowanych unormowań również w kontekście wzorców zawartych w art. 45 ust. 1 i art. 77 ust. 2 ustawy zasadniczej. W związku z powyższym, nie wydaje się konieczne przedstawianie w tym miejscu pogłębionego wywodu w przedmiocie zgodności zakwestionowanych przez Wnioskodawców przepisów ze wspomnianymi wyżej wzorcami kontroli. Jednakże całkowita rezygnacja z przedstawienia chociażby

kilku zwięzłych uwag, dotyczących tego aspektu kwestionowanych we wniosku Grupy posłów unormowań, jak się wydaje, również nie byłaby zasadna.

Zgodnie z art. 45 ust. 1 ustawy zasadniczej, każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. Z kolei, art. 77 ust. 2 Konstytucji RP stanowi, że ustawa nie może nikomu zamykać drogi sądowej dochodzenia naruszonych wolności lub praw.

Jak wynika z orzecznictwa Trybunału Konstytucyjnego, prawo do sądu obejmuje w szczególności 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 (por. wyrok 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).

Z kolei, zakres podmiotowy prawa do sądu został wyznaczony przez konstytucyjne pojęcie „sprawy”. Ustalając znaczenie tego terminu, Trybunał Konstytucyjny 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 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 10 maja 2000 r., sygn. K. 21/99, OTK ZU Nr 4/2000, poz. 109, s. 555,

z dnia 18 maja 2004 r., sygn. SK 28/03, OTK ZU Nr 5/A/2004, poz. 45, s. 629 oraz z dnia 11 czerwca 2002 r., sygn. SK 5/02, OTK ZU Nr 4/A/2002, poz. 41, s. 554).

Trybunał Konstytucyjny stoi na stanowisku, że o ile przepis art. 45 ust. 1 Konstytucji RP pozytywnie formułuje prawo do sądu, o tyle art. 77 ust. 2 zawiera zakaz zamykania drogi sądowej dla dochodzenia naruszonych wolności i praw, stanowi zatem dopełnienie (uzupełnienie, rozwinięcie) prawa do sądu. Prawo każdego do sądu oznacza, że nikomu nie można zamykać drogi sądowej – w zakresie wyznaczonym w art. 77 ust. 2 Konstytucji (por. wyroki: z dnia 10 maja 2000 r., sygn. K. 21/99, *op. cit.*, s. 557, z dnia 9 czerwca 1998 r., sygn. K. 28/97, OTK ZU Nr 4/1998, poz. 50, s. 300 oraz z dnia 8 listopada 2001 r., sygn. P 6/01, OTK ZU Nr 8/2001, poz. 248, s. 1245).

Problematyka ochrony prywatności, swobody komunikowania się oraz autonomii informacyjnej przed ograniczaniem tych praw konstytucyjnych przez służby mundurowe oraz specjalne poprzez nieuprawnione pozyskiwanie danych telekomunikacyjnych niewątpliwie stanowi „sprawę” w rozumieniu przytoczonego orzecznictwa Trybunału Konstytucyjnego. W konsekwencji, wszelkie unormowania prawne i pominięcia legislacyjne ze strony ustawodawcy, zmierzające do wyeliminowania sądu z procedury ograniczania wymienionych praw konstytucyjnych, należałoby ocenić zdecydowanie negatywnie.

O ile regulacje wyłączające konieczność uzyskania zgody sądu na pozyskiwanie danych telekomunikacyjnych oraz brak regulacji wprowadzających obowiązek uzyskania takiej zgody przez stosowne służby eliminuje podstawowy czynnik gwarancyjny, chroniący jednostkę przed nieuprawnionym wkraczaniem w sferę jej wolności i praw konstytucyjnych, to brak unormowań nakładających obowiązek powiadamiania obywatela o pozyskiwaniu dotyczących go danych (choćby po zakończeniu kontroli operacyjnej) uniemożliwia temuż obywatelowi podjęcie jakichkolwiek działań

zmierzających do ochrony wspomnianych wolności i praw. Tym samym, kontrola operacyjna, w omawianym zakresie, wyłączona została również spod jakiegokolwiek kontroli osoby, wobec której jest stosowana, a więc podmiotu najbardziej zainteresowanego.

Brak wiedzy o samym fakcie pozyskiwania danych telekomunikacyjnych przez stosowne służby, nawet w przypadku podejrzeń lub wątpliwości co do prawidłowości postępowania przez te służby, uniemożliwia samemu zainteresowanemu nie tylko poszukiwanie pomocy u czynników zewnętrznych (sąd, Rzecznik Praw Obywatelskich itp.), ale nawet zwrócenie się do przełożonych funkcjonariuszy dokonujących kontroli operacyjnej o zbadanie postępowania podwładnych.

Szczegółnej ostrości nabiera powyższy zarzut na gruncie art. 51 ust. 4 ustawy zasadniczej. Unormowanie to daje każdemu prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Brak wiedzy osoby zainteresowanej nawet o fakcie pozyskiwania danych telekomunikacyjnych przez stosowne służby powoduje, że wspomniane prawo, gwarantowane przez Konstytucję RP, pozostaje prawem nierealizowalnym, a więc martwym. W omawianym przypadku nie sposób zresztą mówić o ograniczeniu prawa konstytucyjnie chronionego, skoro brak stosownego powiadomienia zainteresowanego (nawet po zakończeniu kontroli operacyjnej) godzi, jak się wydaje, w samą istotę tegoż prawa.

Analiza przepisów zakwestionowanych przez Grupę posłów pozwala na wysnucie wniosku, że ustawodawca nie wyłączył żadnej kategorii użytkowników telekomunikacyjnych urządzeń końcowych z kręgu podmiotów, których dane telekomunikacyjne mogą być pozyskiwane przez stosowne służby. Najwyraźniej, ustawodawca pominął fakt, że dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską.

Zgodnie z przepisem art. 180 § 1 Kodeksu postępowania karnego, osoby obowiązane do zachowania tajemnicy służbowej lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania tajemnicy. Z kolei § 2 wspomnianego art. 180 stanowi, że osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, lekarskiej lub dziennikarskiej mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W końcu, zgodnie z § 3 tegoż art. 180, zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.

Zasadnicze znaczenie ma brzmienie przepisu art. 178 Kodeksu postępowania karnego, zgodnie z którym, nie wolno przesłuchiwać jako świadków: obrońcy lub adwokata działającego na podstawie art. 245 § 1, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę oraz duchownego co do faktów, o których dowiedział się przy spowiedzi.

W doktrynie przyjmuje się, że zakaz przewidziany w ostatnim przytoczonym wyżej przepisie ma charakter bezwzględny; nie może być uchylony przez organ procesowy, jak również osoby te nie mogą być przesłuchiwane chociażby chciały lub domagał się tego oskarżony. W ogóle wyłączona jest możliwość przesłuchania tych osób w charakterze świadka. Zakaz trwa także po ustaniu wykonywania obowiązków obrońcy lub duchownego. Zakaz jest skierowany do wszystkich organów procesowych, tj. prowadzących dochodzenie lub śledztwo, jak i do sądu (por. Ryszard Stefański

[w:] *Kodeks Postępowania Karnego, Komentarz, Tom I*, Dom Wydawniczy ABC, 2003, s. 786 oraz powołane tam poglądy doktryny).

W literaturze przedmiotu podnosi się również, że przepis art. 178 formułuje bezwzględne zakazy dowodowe, które w żadnych warunkach nie mogą być uchylone, co oznacza, że osoby te, co do tych okoliczności, nie mogą zostać przesłuchane, a gdyby zostały wezwane w charakterze świadków, mają prawo i obowiązek, wynikający z innych unormowań, odmowy złożenia w tym zakresie zeznań. Zakazu tego nie uchyla nawet zgoda wszystkich zainteresowanych osób (por. Jan Grajewski, Lech Paprzycki, Sławomir Steinborn, *Kodeks postępowania karnego, Komentarz, Tom I*, Zakamycze 2006, Komentarz do art. 178, System Informacji Prawnej Lex (Lex Omega), 20/2011).

W tym miejscu wypada odnotować, że problematyka wyłączenia użytkowników telekomunikacyjnych urządzeń końcowych, będących adwokatami, spośród podmiotów, których dane telekomunikacyjne mogą być pozyskiwane przez stosowne służby (jako element ochrony tajemnicy obrończej, w tym poufności kontaktów oskarżonego z jego obrońcą), nabiera szczególnego znaczenia wobec ujęcia, przez ustrojodawcę, prawa do obrony na gruncie ustawy zasadniczej. Zgodnie z art. 42 ust. 2 Konstytucji RP, każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu.

W doktrynie przyjmuje się, że twórca Konstytucji uznał, iż w procesach karnych, w których zagrożone są najcenniejsze dla człowieka dobra osobiste, należy potwierdzić możliwość powoływania pełnomocników procesowych, a w pewnych sytuacjach tacy pełnomocnicy muszą działać nawet bez względu na wolę tudzież możliwości podejrzanego (por. Paweł Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz, Tom III*, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 42, s. 9).

Przedstawiciele nauki prawa konstytucyjnego prezentują również pogląd, że oskarżonego w żadnych okolicznościach nie można pozbawić prawa zarówno do obrony możliwej, jak i do obrony obligatoryjnej. Wynika to z niebudzącej wątpliwości regulacji konstytucyjnej, przy czym sytuację oskarżonego (terminem tym można objąć także podejrzanego i skazanego) w świetle wymogów publicznoprawnych należy zakwalifikować do rzędu publicznych praw podmiotowych, które istnieją i które muszą być zrealizowane, i których nie może pozbawić nawet ustawodawca w drodze ustawy (por. Zdzisław Kegel [w:] *Konstytucje Rzeczypospolitej oraz Komentarz do Konstytucji RP z 1997 roku*, Wrocław 1998, s. 87).

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, konstytucyjne prawo do obrony należy rozumieć szeroko, jest ono bowiem nie tylko fundamentalną zasadą procesu karnego, ale też elementarnym standardem demokratycznego państwa prawnego. Prawo to przysługuje każdemu od chwili wszczęcia przeciwko niemu postępowania karnego (w praktyce od chwili przedstawienia zarzutów), aż do wydania prawomocnego wyroku; obejmuje również etap postępowania wykonawczego. Prawo do obrony w procesie karnym ma wymiar materialny i formalny. Obrona materialna to możliwość bronięcia przez oskarżonego jego interesów osobiście (np. możliwość odmowy składania wyjaśnień, prawo wglądu do akt i składania wniosków dowodowych). Obrona formalna to prawo do korzystania z pomocy obrońcy z wyboru lub z urzędu (por. wyroki: z dnia 19 marca 2007 r., sygn. K 47/05, OTK ZU Nr 3/A/2007, poz. 27, s. 268 oraz z dnia 9 lipca 2009 r., sygn. K 31/08, OTK ZU Nr 7/A/2009, poz. 107, s. 1092)

Trybunał Konstytucyjny podkreślał również, że proces karny jest ze swej istoty kontradyktoryjny, stanowi on spór równouprawnionych stron przed bezstronnym sądem. W postępowaniu przygotowawczym, którym kieruje prokurator, owa kontradyktoryjność jest w pewnym zakresie ograniczona, co nie oznacza jednak, iż ograniczenia te mogą naruszać istotę prawa do obrony. Stąd

też zachowane są pewne uprawnienia obrońcy, takie jak: prawo składania wniosków o dokonanie czynności śledztwa lub dochodzenia (art. 315 § 1 Kodeksu postępowania karnego), prawo do udziału w czynnościach niepowtarzalnych (art. 316 § 1 K.p.k.) oraz w innych czynnościach postępowania (art. 317 § 1 K.p.k.), a także prawo udziału w czynnościach zapoznawania podejrzanego z materiałami postępowania przygotowawczego (art. 321 § 3 K.p.k.). Uprawnienia obrońcy to nie tylko możliwość przeglądania akt postępowania karnego – zapoznawania się z materiałem dowodowym, ale przede wszystkim kontakt z jego mocodawcą. To na podstawie osobistego kontaktu obrońca pozyskuje faktyczną wiedzę o czynie sprawcy oraz okolicznościach zdarzenia będącego przedmiotem postępowania, buduje strategię obrony, zgłasza wnioski dowodowe i współdziała z innymi obrońcami występującymi w sprawie (por. wyrok z dnia 17 lutego 2004 r., sygn. SK 39/02, OTK ZU Nr 2/A/2004, poz. 7, s. 115).

Na marginesie wypada również odnotować (o czym przypomniał Trybunał Konstytucyjny we wspomnianych wyżej wyroku z dnia 17 lutego 2004 r., sygn. SK 39/02), że prawo oskarżonego do swobodnych kontaktów z obrońcą należy do podstawowych standardów prawa międzynarodowego. Art. 14 ust. 3 lit. b oraz d Międzynarodowego Paktu Praw Obywatelskich i Politycznych stanowi m. in., że każda osoba oskarżona o popełnienie przestępstwa ma prawo do dysponowania odpowiednim czasem i możliwościami w celu przygotowania obrony i porozumienia się ze swoim obrońcą, a jeśli nie posiada obrońcy – do bycia poinformowanym o prawie do jego wyboru, ponadto zaś – gdy dobro wymiaru sprawiedliwości tego wymaga – do otrzymania obrońcy z urzędu bezpłatnie, jeśli nie jest w stanie samodzielnie pokryć kosztów obrony. Podobne rozwiązanie przewiduje Konwencja o ochronie praw człowieka i podstawowych wolności, uznając (w art. 6 ust. 3 lit. b oraz c), że prawo do osobistej obrony lub przez ustanowionego przez siebie obrońcę stanowi gwarancję rzetelnego procesu sądowego (por. *op. cit.*, s. 116).

O ile regulacje dotyczące ochrony tajemnicy obrończej, w tym poufności kontaktów oskarżonego z jego obrońcą, w toku postępowania procesowego, zawarte w Kodeksie postępowania karnego (art. 73, art. 178 pkt 1, art. 180 § 1 i § 2, art. 225 § 3, Kodeksie karnym wykonawczym (art. 8 § 3) oraz Prawie o adwokaturze (art. 6), zdają się spełniać wymogi konstytucyjności, w rozumieniu orzecznictwa Trybunału Konstytucyjnego, to brak takich regulacji odnośnie prowadzenia czynności operacyjno-rozpoznawczych przez uprawnione służby (w tym pozyskiwania danych telekomunikacyjnych) nasuwa poważne wątpliwości w omawianym zakresie.

W szczególności, pominięcie przez ustawodawcę regulacji wyłączających pozyskiwanie przez służby danych telekomunikacyjnych dotyczących obrońcy podejrzanego lub oskarżonego może zostać zinterpretowane przez te służby jako pozostawienie możliwości swojego rodzaju „obejścia prawa”, gwarantującego poufność kontaktów tegoż podejrzanego lub oskarżonego z jego obrońcą.

Powyższy wywód, dotyczący zdecydowanie negatywnej oceny pozyskiwania przez służby mundurowe i specjalne danych telekomunikacyjnych obrońcy, może, w pewnym zakresie, znaleźć odpowiednie odniesienie również w stosunku do kolizji, w jakiej pozostaje pozyskiwanie tychże danych z innymi zakazami dowodowymi, wynikającymi z przepisów obowiązującej procedury karnej.

Problemem związanym z brakiem ograniczeń w zakresie pozyskiwania przez służby danych telekomunikacyjnych jest kwestia usuwania przez te służby danych, o których mowa w art. 180c (a wydaje się, że również art. 180d) Prawa telekomunikacyjnego. Pewne regulacje, w omawianym zakresie, zawierają ustawy: o Policji (art. 20c ust. 7), o Straży Granicznej (art. 10b ust. 6), o kontroli skarbowej (art. 36b ust. 5) oraz o Żandarmerii Wojskowej i wojskowych organach porządkowych (art. 30 ust. 6). Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne ani Służba Kontrwywiadu

Wojskowego nie zostały natomiast zobligowane przez ustawodawcę do niszczenia, w jakiejkolwiek sytuacji, pozyskanych danych telekomunikacyjnych.

Zgodnie z obowiązującym stanem prawnym, Policja, Straż Graniczna i Żandarmeria Wojskowa są zobowiązane do zniszczenia jedynie materiałów, które nie zawierają informacji mających znaczenie dla postępowania karnego. Wspomniany obowiązek nie obejmuje materiałów pozyskanych nieprawidłowo, zawierających informacje mogące zostać użyte do obejścia istniejących zakazów dowodowych itp. Wymienione wyżej regulacje nie przewidują również możliwości realizacji litery art. 51 ust. 4 Konstytucji RP, to jest „usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą” na żądanie osoby zainteresowanej.

Z kolei, w myśl art. 36b ust. 5 ustawy o kontroli skarbowej, minister właściwy do spraw finansów publicznych nakazuje niezwłoczne komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną, w przypadku, gdy uzna wystąpienie z wnioskiem o przekazanie tych danych za nieuzasadnione. Wspomniana regulacja nie przewiduje więc zniszczenia danych, jeżeli nie zawierają one informacji mających znaczenie dla prowadzonego przez organ skarbowy postępowania (nie mówiąc już o danych pozyskanych nieprawidłowo), lecz tylko wtedy, gdy sam wniosek o ich udostępnienie został uznany przez ministra za niezasadny. Tym samym, ustawodawca dopuścił sytuację, gdy sam wniosek o udostępnienie danych był uzasadniony, zaś zgromadzone w wyniku jego realizacji dane nie zostaną zniszczone, mimo że nie mają one znaczenia dla prowadzonego postępowania.

W końcu brak jakichkolwiek regulacji, dotyczących niszczenia materiałów zgromadzonych przez funkcjonariuszy ABW, CBA lub SKW w toku kontroli operacyjnej, w zakresie pozyskiwania danych telekomunikacyjnych, należałoby uznać za przykład zakwestionowanej przez Trybunał Konstytucyjny,

w przytoczonym orzecznictwie, praktyki zbierania i przetrzymywania przez służby mundurowe i specjalne najrozmaitszych informacji nie tylko „koniecznych w demokratycznym państwie” dla ochrony wykazanych w ustawie zasadniczej wartości, ale również „wygodnych” lub „użytecznych” dla tychże służb.

Kolejnym problemem wymagającym, jak się wydaje, omówienia w uzasadnieniu niniejszego stanowiska, pozostaje kwestia dookreśloności i konkretności zakwestionowanych przez Grupę posłów unormowań. Ustawodawca, jak wspomniano, upoważnił Policję, Straż Graniczną oraz Żandarmerię Wojskową do pozyskiwania i przetwarzania danych telekomunikacyjnych w celu zapobiegania lub wykrywania przestępstw (art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej oraz art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych). Analogiczne uprawnienia wywiadu skarbowego (ograniczone do przestępstw skarbowych) zostały poszerzone o zapobieganie i wykrywanie naruszeń przepisów celnych (art. 36b ust. 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej). W końcu ABW, CBA i SKW uzyskały kompetencję do pozyskiwania i przetwarzania informacji niezbędnych do realizacji ich zadań ustawowych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA oraz art. 32 ust. 1 ustawy o SKW oraz SWW).

Określenie przez ustawodawcę celu pozyskiwania i przetwarzania danych telekomunikacyjnych jako „zapobieganie i wykrywanie przestępstw” lub „zapobieganie i wykrywanie naruszeń przepisów celnych” wydaje się nadzwyczaj lakoniczne w kontekście wymogu dookreśloności i konkretności unormowań ograniczających prawa i wolności konstytucyjne. Znacznie poważniejsze zastrzeżenia nasuwa analiza przepisów określających wspomniane zadania ustawowe ABW, CBA oraz SKW (art. 5 ust. 1 ustawy o ABW oraz AW, art. 2 ust. 1 ustawy o CBA oraz art. 5 ust. 1 ustawy o SKW oraz SWW). Użycie przez ustawodawcę, we wspomnianych przepisach, takich pojęć, jak

„informacje mogące mieć znaczenie”, „informacje mogące mieć istotne znaczenie” czy „przeciwdziałanie przypadkom nieprzestrzegania przepisów”, w połączeniu z otwartym katalogiem ustawowych zadań omawianych służb, zdają się wykluczać możliwość uznania, że analizowane unormowania dostarczają obywatelom wystarczających wskazówek, w jakiej sytuacji służby uzyskują prawo wkraczania w sferę objętą konstytucyjną ochroną prawa do prywatności, swobody komunikowania się oraz autonomii informacyjnej.

W tym miejscu wypadałoby odnotować, że w pełni zachowują aktualność wywody, zawarte we wcześniejszej części uzasadnienia niniejszego stanowiska, dotyczące niedopuszczalności stanowienia przez prawodawcę otwartego i nieostro sformułowanego katalogu sytuacji, uprawniających służby mundurowe oraz specjalne do wkraczania w sferę konstytucyjnie chronionych praw i wolności jednostki. Tym samym, sposób określenia przez ustawodawcę przypadków uprawniających służby do pozyskiwania i przetwarzania danych telekomunikacyjnych należałoby uznać za zdecydowanie wadliwy.

Podobne zastrzeżenia nasuwa nieprecyzyjne sformułowanie zakresu danych telekomunikacyjnych w zakwestionowanym przez Grupę postów przepisie art. 180c ust. 1 pkt 1 Prawa telekomunikacyjnego. Jak już wspomniano, zgodnie ze wspomnianą regulacją operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani, między innymi, zatrzymywać, przechowywać i udostępniać dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest to połączenie. Ustawodawca nie określił jednak w omawianym przepisie wszystkich konkretnych danych użytkownika końcowego, podlegających zatrzymaniu, przechowywaniu i udostępnianiu.

Wydaje się, że uprawnione byłoby przypuszczenie, że ustawodawca zdawał sobie sprawę z niekompletności powyższej regulacji, skoro w art. 180c

ust. 2 Prawa telekomunikacyjnego upoważnił ministra właściwego do spraw łączności, by ten, w porozumieniu z ministrem właściwym do spraw wewnętrznych, określił, w drodze rozporządzenia, między innymi szczegółowy wykaz omawianych danych.

Zaskarżając przepis art. 180c ust. 2, Wnioskodawcy nie wskazali w *petitum* swego wniosku wzorca kontroli zawartego w art. 92 ust. 1 Konstytucji RP. Wprawdzie ocena zakwestionowanego unormowania byłaby możliwa przy ograniczeniu się do regulacji ustawy zasadniczej wskazanych przez Grupę posłów, a w szczególności do art. 2, art. 31 ust. 3 zdanie pierwsze, art. 49 oraz art. 51 ust. 4 i ust. 5, nakazujących kompletne unormowanie w ustawie wszelkich przejawów ograniczania konstytucyjnych praw i wolności jednostki oraz zakazujących wkraczania w sferę tychże praw i wolności w drodze podustawowego aktu normatywnego, jednakże wydaje się, że ocena wspomnianego art. 180c ust. 2 Prawa telekomunikacyjnego mogłaby być pełniejsza przy uwzględnieniu również art. 92 ust. 1 ustawy zasadniczej.

Zgodnie ze wspomnianym przepisem ustawy zasadniczej, rozporządzenia są wydawane przez organy wskazane w Konstytucji, na podstawie szczegółowego upoważnienia zawartego w ustawie i w celu jej wykonania. Upoważnienie powinno określać organ właściwy do wydania rozporządzenia i zakres spraw przekazanych do uregulowania oraz wytyczne dotyczące treści aktu.

W literaturze przedmiotu podnosi się, że powiązanie unormowań art. 87 ust. 1 i art. 92 Konstytucji z ogólnymi konsekwencjami zasady demokratycznego państwa prawnego (art. 2 Konstytucji) prowadzi do wniosku, iż nie może obecnie, w systemie prawa powszechnie obowiązującego, pojawiać się żadna regulacja podustawowa, która nie służy wykonaniu ustawy. W tym sensie wyłączność ustawy nabrała zupełnego charakteru, bo nie ma takich materii, w których mogłyby być stanowione regulacje podustawowe (o charakterze powszechnie obowiązującym), bez uprzedniego ustawowego

unormowania tych materii (por. Jerzy Oniszczyk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Zakamycze 2004, s. 796).

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, przepis art. 92 ust. 1 Konstytucji RP określa wymogi konstytucyjne w odniesieniu do przepisów upoważniających do wydania rozporządzenia, a mianowicie, że przepisy te winny wskazywać jednoznacznie organy upoważnione do wydania rozporządzenia, określać zakres spraw przekazanych do uregulowania oraz wytyczne dotyczące treści aktu wydawanego na podstawie upoważnienia. Upoważnienie, zgodnie z art. 92 ust. 1 Konstytucji, powinno być „szczegółowe”, a wydana na jego podstawie regulacja prawna winna realizować cel wynikający z przepisów upoważniających (por. wyrok, wydany w pełnym składzie Trybunału, z dnia 2 grudnia 2009 r., sygn. U 10/07, OTK ZU Nr 11/A/2009, poz. 163, s. 1764 oraz powołane tam orzecznictwo).

Trybunał Konstytucyjny podkreślał również niejednokrotnie, że ustawodawca nie może udzielać upoważnienia do wydania aktu normatywnego, dotyczącego materii zastrzeżonych dla ustawy, które nie zostały uregulowane w danej ustawie. Materie uregulowane w rozporządzeniu muszą być jednorodne z tymi, które są uregulowane w ustawie. Należy pamiętać, że sprawy przekazane do uregulowania w akcie wykonawczym nie powinny mieć zasadniczego znaczenia z punktu widzenia konstrukcji całej ustawy (por. wyrok z dnia 12 lipca 2007 r., sygn. U 7/06, OTK ZU Nr 7/A/2007, poz. 76, s. 1029 – 1030 oraz powołane tam orzecznictwo).

W świetle utrwalonego orzecznictwa Trybunału Konstytucyjnego, wykonawczy charakter rozporządzenia determinuje treść upoważnienia do jego wydania. Upoważnienie to musi być sformułowane w taki sposób, aby odsyłało do unormowania tylko takich spraw, które są przedmiotem ustawy i które służą realizacji tych samych celów, jakie znajdują wyraz w przepisach ustawy. Dlatego przepisy ustawy upoważniającej, a w szczególności przepis

upoważniający, powinny wyznaczać co najmniej w sposób ogólny, lecz jednocześnie dostatecznie wyraźny, kierunek unormowań, które mają nastąpić w drodze rozporządzenia. Nie można bowiem wykonywać w drodze rozporządzenia tego, co nie zostało uregulowane w ustawie (por. wyrok z dnia 31 marca 2009 r., sygn. K 28/08, OTK ZU Nr 3/A/2009, poz. 28, s. 300 oraz powołane tam orzecznictwo).

W końcu, Trybunał Konstytucyjny zwracał szczególną uwagę na to, że nakaz zamieszczania wszystkich zasadniczych elementów regulacji prawnej bezpośrednio w ustawie, połączony z zakazem regulowania ich w rozporządzeniu, jako akcie podstawowym, dotyczy zwłaszcza materii odnoszącej się do praw i wolności jednostki lub do władczych form działania władzy publicznej wobec obywateli. Wymaganie umieszczenia bezpośrednio w tekście ustawy wszystkich zasadniczych elementów regulacji prawnej musi być stosowane ze szczególnym rygoryzmem, gdy regulacja ta dotyczy władczych form działania organów administracji publicznej wobec obywateli, praw i obowiązków organu administracji i obywatela w ramach stosunku publicznoprawnego lub korzystania przez obywateli z ich praw i wolności (por. wyrok, wydany w pełnym składzie Trybunału, z dnia 10 marca 2010 r., sygn. U 5/07, OTK ZU Nr 3/A/2010, poz. 20, s. 347 oraz powołane tam orzecznictwo).

Wydane na podstawie zakwestionowanego przez Grupę posłów upoważnienia ustawowego, zawartego w art. 180c ust. 2 Prawa telekomunikacyjnego, rozporządzenie Ministra Infrastruktury w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, deklaruje w § 1, że określa, między innymi, szczegółowy wykaz danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, jak również

ustalenie zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie. Pozostałe dane wymienione w przepisie (określenie daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, jak również lokalizacji telekomunikacyjnego urządzenia końcowego) stanowią powtórzenie regulacji zawartych w art. 180c ust. 1 pkt 2 Prawa telekomunikacyjnego.

Wspomniane wyżej wykazy danych, odrębnie dla stacjonarnej publicznej sieci telekomunikacyjnej, ruchomej publicznej sieci telekomunikacyjnej, jak również usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej, zostały określone, odpowiednio, w przepisach § 3 – 7 omawianego rozporządzenia. Powyższe dane dotyczą nie tylko parametrów technicznych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, w postaci numeru zakończenia stacjonarnej publicznej sieci telefonicznej, z którego inicjowane jest połączenie, lub do którego kierowane jest połączenie (§ 3 pkt 1 lit a oraz pkt 2 lit a), numeru przydzielonego użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej, użytkownika końcowego inicjującego połączenie, lub do którego kierowane jest połączenie (§ 4 pkt 1 lit a oraz pkt 2 lit a), międzynarodowego numeru przydzielonego karcie identyfikacyjnej użytkownika w ruchomej publicznej sieci telefonicznej, użytkownika końcowego, inicjującego połączenie, lub do którego kierowane jest połączenie (§ 4 pkt 1 lit c oraz pkt 2 lit c), pierwsze 14 cyfr indywidualnego międzynarodowego numeru identyfikującego telekomunikacyjne urządzenie końcowe, używane w ruchomej publicznej sieci telefonicznej lub międzynarodowego numeru przydzielonego karcie identyfikującej użytkownika w ruchomej sieci telefonicznej, urządzenia końcowego, inicjującego połączenie, lub do którego kierowane jest połączenie (§ 4 pkt 1 lit d oraz pkt 2 lit d), numeru przydzielonego użytkownikowi końcowemu, korzystającemu z dostępu do sieci Internet za pośrednictwem publicznej sieci telefonicznej (§ 6 pkt 1 lit b), numeru przydzielonego

użytkownikowi końcowemu, do którego jest kierowane połączenie w telefonii internetowej (§ 7 pkt 1 lit a) itp. Omawiane dane obejmują również imię i nazwisko albo nazwę oraz adres użytkownika końcowego (§ 3 pkt 1 lit b oraz pkt 2 lit b, § 4 pkt 1 lit b oraz pkt 2 lit b, § 5, § 6 pkt 1 lit e, § 7 pkt 1 lit b).

W tym miejscu wypada odnotować, że, zgodnie z art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zaś art. 6 ust. 2 tejże ustawy stanowi, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Z kolei, zgodnie z art. 159 ust. 1 pkt 1 ustawy – Prawo telekomunikacyjne, tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana „tajemnicą telekomunikacyjną”, obejmuje dane dotyczące użytkownika.

Zgodnie z wyrokiem Naczelnego Sądu Administracyjnego w Warszawie z dnia 18 listopada 2009 r., sygn. I OSK 667/09, dane osobowe to zespół wiadomości (komunikatów) o konkretnym człowieku na tyle zintegrowany, że pozwala na jego zindywidualizowanie. Obejmuje co najmniej informacje niezbędne do identyfikacji (imię, nazwisko, miejsce zamieszkania), jednakże do tego się nie ogranicza, bowiem mieszczą się w nim również dalsze informacje, wzmacniające stopień identyfikacji (por. LEX nr 588798, System Informacji Prawnej Lex – Lex Omega – 20/2011).

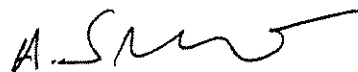
Omawiany we wcześniejszej części uzasadnienia niniejszego stanowiska przepis art. 180c ust. 1 pkt 1 Prawa telekomunikacyjnego nakazuje operatorom publicznej sieci telekomunikacyjnej oraz dostawcom publicznie dostępnych usług telekomunikacyjnych udostępnianie uprawnionym służbom, między innymi, danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego

inicjującego połączenie oraz do którego kierowane jest połączenie. Regulacja ta nie wymienia wprost, wśród wspomnianych danych, ani imienia i nazwiska, ani adresu użytkownika końcowego. Skoro powyższe dane objęte są tajemnicą telekomunikacyjną, to obowiązek udostępniania imienia i nazwiska oraz adresu użytkownika końcowego nie może być dorozumiany, ale winien wynikać wprost z ustawy. Tym samym, upoważnienia zawartego w art. 180c ust. 2 Prawa telekomunikacyjnego, jak się wydaje, nie należy traktować jako upoważnienia do uzupełnienia (poprawienia) ustawy poprzez zobowiązanie operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych do dostarczania stosownym służbom danych obejmujących imię i nazwisko oraz adres użytkownika końcowego korzystającego ze wspomnianych sieci lub usług, skoro ustawodawca nie był uprawniony przez ustrojodawcę do cedowania na organ władzy wykonawczej swoich uprawnień prawodawczych w omawianym zakresie.

Reasumując powyższe wywody, należałoby uznać, że zakwestionowane przez Grupę posłów przepisy godzą w prawo do prywatności, swobodę komunikowania się, autonomię informacyjną oraz zasadę demokratycznego państwa prawnego, poprzez brak precyzji, niedookreśloność i niepełność przyjętych regulacji, brak zasady subsydiarności wkraczania przez stosowne służby w sferę konstytucyjnych praw i wolności jednostki, brak sądowej kontroli pozyskiwania danych telekomunikacyjnych przez służby, brak regulacji o powiadamianiu zainteresowanych o prowadzonej wobec nich kontroli operacyjnej (choćby po zakończeniu tej kontroli), brak respektowania tajemnicy zawodowej wskazanych kategorii osób oraz związanych z tym zakazów dowodowych, jak również wadliwość lub brak regulacji dotyczących niszczenia danych zgromadzonych przez służby z uwagi na ich nieprzydatność dla dalszego postępowania, nieprawidłowe pozyskanie lub nieprawdziwość. Tym samym, przepisy art. 180a ust. 1 i art. 180c Prawa telekomunikacyjnego w związku z art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej,

art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ustawy o Centralnym Biurze Antykorupcyjnym, jak również art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego są niezgodne z art. 2, art. 47, art. 49 i art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji RP.

Z tych wszystkich względów, wnoszę jak na wstępie.



Andrzej Seremet