SEJM
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 2 marca 2012 r.

Sygn. akt K 23/11
BAS-WPTK-1689/11

Trybunał Konstytucyjny

Na podstawie art. 34 ust. 1 w związku z art. 27 pkt 2 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643 ze zm.), w imieniu Sejmu Rzeczypospolitej Polskiej przedkładam wyjaśnienia w sprawie połączonych wniosków Rzecznika Praw Obywatelskich z 29 czerwca 2011 r. i 1 sierpnia 2011 r. (sygn. akt K 23/11), jednocześnie wnosząc o stwierdzenie, że:

1) art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2007 r. Nr 43, poz. 277 ze zm.), art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2011 r. Nr 116, poz. 675 ze zm.), 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 zm.), art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.), art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.), 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 zm.) **są zgodne** z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji;
2) art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2007 r. Nr 43, poz. 277 ze zm.), art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2011 r. Nr 116, poz. 675 ze zm.), art. 36b ust. 1 pkt 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.), art. 30 ust. 1 ustawy z dnia 24 sierpnia

2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zm.), art. 28 ust. 1 pkt 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.), art. 18 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.), art. 32 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zm.) **są niezgodne** z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.);

3) art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.), art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.), art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zm.), w zakresie, w jakim przepisy te, zezwalając na pozyskiwanie danych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.), nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, **są niezgodne** z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji; zaś art. 36b ust. 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.), w zakresie, w jakim nie przewiduje zniszczenia tych spośród pozyskanych danych, o jakich mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.), które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, **jest zgodny** z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

Ponadto, na podstawie art. 39 ust. 1 pkt 1 ustawy o Trybunale Konstytucyjnym, wnoszę o **umorzenie postępowania** w zakresie badania zgodności art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.) z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji, ze względu na niedopuszczalność wydania wyroku.

Uzasadnienie

I. Pominięcie prawodawcze

W zdecydowanej większości sformułowane przez Rzecznika Praw Obywatelskich (dalej jako RPO lub wnioskodawca) zarzuty niekonstytucyjności kwestionowanych przepisów skierowane są w istocie nie wobec zawartości normatywnej tych przepisów, lecz wobec tego, czego w nich zabrakło, a mianowicie: sprecyzowania „z jakich środków technicznych mogą korzystać służby w celu zdobycia informacji i dowodów" oraz „o jakie informacje i dowody chodzi" – w wypadku kontroli operacyjnej; obowiązku respektowania tajemnicy zawodowej, konieczności uprzedniego wykorzystania innych sposobów uzyskania potrzebnych informacji, kontroli sądowej, procedury niszczenia materiałów zbędnych – w wypadku pozyskiwania tzw. danych telekomunikacyjnych.

Powyższe nakazuje rozważyć, czy w niniejszej sprawie mamy do czynienia z – nieobjętym kognicją Trybunału Konstytucyjnego – zaniechaniem ustawodawczym, czy też ze – znajdującym się w ramach tej kognicji – uregulowaniem niepełnym (pomijającym). Trzeba przy tym przypomnieć, że zaniechanie ustawodawcze występuje wówczas, gdy ustawodawca celowo pozostawił określoną kwestię w całości poza uregulowaniem prawnym. Brak kognicji Trybunału Konstytucyjnego jest tu uzasadniony przypisaną mu rolą „negatywnego prawodawcy", a więc takiego, który deroguje unormowania już obowiązujące, nie zaś uzupełnia stan prawny o rozwiązania, jakie – zdaniem podmiotu inicjującego postępowanie – powinny znaleźć się w zaskarżonym akcie. Zaniechanie ustawodawcze należy jednak odróżnić od uregulowania niepełnego (pomijającego), które charakteryzuje się tym, że prawodawca unormował jakąś dziedzinę stosunków społecznych, lecz dokonał tego w sposób niepełny (fragmentaryczny). W odniesieniu do uregulowania niepełnego (pomijającego) Trybunał Konstytucyjny przyjmuje: „W przypadku (...) 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 pominął, choć postępując zgodnie z konstytucją powinien był unormować" (orzeczenie TK z 3 grudnia 1996 r., sygn. akt K 25/95; zob. też wyroki TK z: 9 października 2001 r., sygn. akt SK 8/00; 24 października 2001 r., sygn. akt SK 22/01; 10 maja 2004 r., sygn. akt SK 39/03; 16 listopada 2004 r., sygn. akt P 19/03; 8 listopada 2005 r., sygn. akt SK 25/02; 24 maja 2006 r., sygn. akt K 5/05; 27 lipca 2006 r., sygn. akt SK 43/04; 17 kwietnia 2007 r., sygn. akt SK 20/05; 14 października 2008 r., sygn. akt SK 6/07; 2 lipca 2009 r., sygn. akt K 1/07 oraz postanowienia TK z: 29 listopada 2005 r., sygn. akt P 10/05; 30 maja 2007 r., sygn. akt SK 3/06; 17 października 2007 r., sygn. akt P 29/07).

Mimo licznych wątpliwości, jakie mogą pojawić się przy odróżnianiu zaniechania ustawodawczego od uregulowania niepełnego, przedstawione przez RPO zarzuty niekonstytucyjności kwestionowanych przepisów i ich kontekst normatywny uzasadniają tezę, iż w niniejszej sprawie mamy do czynienia z uregulowaniem niepełnym (pomijającym). Ustawodawca unormował bowiem w odniesieniu do poszczególnych służb procedury prowadzenia kontroli operacyjnej oraz pozyskiwania tzw. danych telekomunikacyjnych, pominął jednak przy tym określone zagadnienia, na które wskazuje w swoim wniosku RPO.

II. Przedmiot kontroli

1. Wnioskodawca przedmiotem kontroli uczynił osiemnaście następujących przepisów:

1) art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2007 r. Nr 43, poz. 277 ze zm.; dalej jako ustawa o Policji), zgodnie z którym: „Kontrola operacyjna prowadzona jest niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".
2) art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2011 r. Nr 116, poz. 675 ze zm.; dalej jako ustawa o Straży Granicznej), zgodnie z którym: „Kontrola operacyjna jest prowadzona niejawnie i polega na: stosowaniu środków technicznych umożliwiających

uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

3) art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.; dalej jako ustawa o kontroli skarbowej), zgodnie z którym: „Kontrola operacyjna jest prowadzona niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych przy pomocy sieci telekomunikacyjnych".

4) 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 zm.; dalej jako ustawa o Żandarmerii Wojskowej), zgodnie z którym: „Kontrola operacyjna jest prowadzona niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

5) art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.; dalej jako ustawa o ABW), zgodnie z którym: „Kontrola operacyjna prowadzona jest niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

6) art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.; dalej jako ustawa o CBA), zgodnie z którym: „Kontrola operacyjna prowadzona jest niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

7) 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 zm.; dalej jako ustawa o Służbie Kontrwywiadu Wojskowego), zgodnie z którym: „Kontrola operacyjna prowadzona jest niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

8) art. 20c ust. 1 ustawy o Policji, zgodnie z którym: „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".

9) art. 10b ust. 1 ustawy o Straży Granicznej, zgodnie z którym: „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".

10) art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, zgodnie z którym: „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: 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»".

11) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej, zgodnie z którym: „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".

12) art. 28 ust. 1 pkt 1 ustawy o ABW, zgodnie z którym: „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: 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.)".

13) art. 18 ust. 1 pkt 1 ustawy o CBA, zgodnie z którym: „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: 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»".

14) art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego, zgodnie z którym: „Obowiązek uzyskania zgody sądu, o której mowa w art. 31 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez SKW [Służbę Kontrwywiadu Wojskowego – uwaga własna] zadań określonych w art. 5, w postaci danych: 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»".

15) art. 36b ust. 5 ustawy o kontroli skarbowej, zgodnie z którym: „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".

16) art. 28 ustawy o ABW, zgodnie z którym: „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" (ust. 1); „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" (ust. 2); „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" (ust. 3); „Udostępnienie 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" (ust. 4).

17) art. 18 ustawy o CBA, zgodnie z którym: „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" (ust. 1); „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" (ust. 2); „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" (ust. 3); „Udostępnienie CBA danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) sieć ta 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 uzyskiwanych danych; 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne CBA albo prowadzonych przez nie czynności" (ust. 4).

18) art. 32 ustawy o Służbie Kontrwywiadu Wojskowego, zgodnie z którym: „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" (ust. 1); „Udostępnienie 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" (ust. 2); „O udostępnieniu danych w trybie określonym w ust. 2 pkt 2 przedsiębiorca telekomunikacyjny lub operator świadczący usługi pocztowe informuje Szefa SKW" (ust. 3); „Przedsiębiorca telekomunikacyjny oraz operator świadczący usługi pocztowe są obowiązani udostępnić dane, o których mowa w ust. 1, funkcjonariuszom wskazanym we wniosku" (ust. 4); „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" (ust. 5); „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" (ust. 6).

2. W ślad za systematyką przyjętą we wnioskach RPO kwestionowane przepisy można uszeregować w trzy następujące grupy. Grupa pierwsza: 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, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA, art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego. Grupa druga: art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego. Grupa trzecia: art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW, art. 18 ustawy o CBA, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego.

III. Zasada określoności przepisów prawa i prawo do prywatności

1. Zarzuty wnioskodawcy

Według wnioskodawcy, pierwsza grupa kwestionowanych przepisów narusza art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji. W odniesieniu do tych przepisów RPO podnosi, że są one niezgodne z „konstytucyjnym standardem ochrony prawa do prywatności", gdyż umożliwiają służbom – w ramach kontroli operacyjnej – niejawne pozyskiwanie za pomocą wszelkich środków technicznych danych o jednostce (informacji i dowodów), których katalog nie został precyzyjnie określony.

W konsekwencji służby mogą na podstawie tych przepisów uzyskać każdą informację o jednostce i każdy dowód jej dotyczący.

Zarzuty wnioskodawcy sprowadzają się więc do tego, że ustawodawca nie skonkretyzował „z jakich środków technicznych mogą korzystać służby w celu zdobycia informacji i dowodów" oraz nie sprecyzował „o jakie informacje i dowody chodzi", czy też – innymi słowy – „w jakie prawnie chronione dobra jednostki mogą ingerować służby za pomocą tych środków". Zdaniem RPO, „owa kumulacja braku precyzji ustawodawczej" nie spełnia „standardów ochrony praw jednostki". Wnioskodawca wskazuje przy tym, że ustawodawca – nie precyzując w jakie prawnie chronione dobra jednostki mogą ingerować służby za pomocą środków technicznych – nie dostrzegł konieczności „zróżnicowania intensywności konstytucyjnej ochrony poszczególnych praw składających się na prawo do prywatności".

Wnioskodawca, odnosząc się do wymaganych standardów, jakie powinno spełniać „prawo zezwalające na niejawną ingerencję organów władzy publicznej (...) w prawa i wolności jednostki", wywodzi: „Ustawa dopuszczająca niejawną ingerencję w prawa i wolności jednostki musi (...) przede wszystkim konkretyzować przypadki, zakres, sposoby ingerencji, a także wskazywać jakich konkretnie sfer życia jednostki owa ingerencja dotyczy. Oznacza to, że regulując tę materię ustawodawca powinien zrezygnować z posługiwania się klauzulami generalnymi, powinien także unikać tworzenia otwartych katalogów. W przeciwnym przypadku przepisy ustawy tracą swój gwarancyjny charakter, skoro ostateczne i maksymalne kontury ograniczenia praw i wolności jednostki określają same służby, a nie ustawodawca".

2. Wzorce kontroli

1. Wnioskodawca, stawiając zarzut niekonstytucyjności pierwszej grupy kwestionowanych przepisów, odwołuje się m.in. do art. 2 ustawy zasadniczej, z którego wyprowadza „wymóg określoności regulacji ustawowej".

Zgodnie z utrwaloną linią orzeczniczą Trybunału Konstytucyjnego, art. 2 Konstytucji i wyrażona w nim generalna klauzula demokratycznego państwa prawnego „stanowi swego rodzaju zbiorcze wyrażenie szeregu reguł i zasad, które wprawdzie nie zostały *expressis verbis* ujęte w pisanym tekście konstytucji, ale w sposób immanentny wynikają z aksjologii oraz z istoty demokratycznego państwa prawnego. Owe reguły i zasady miały najróżniejszy charakter, odnosząc się zarówno

do prawa materialnego jak i do tzw. zasad przyzwoitej legislacji (np. zakaz stanowienia przepisów z mocą wsteczną, nakaz zachowania «odpowiedniej» *vacatio legis*, nakaz poszanowania praw słusznie nabytych), a ogólną podstawą było uznanie, że demokratyczne państwo prawne wymaga poszanowania zasady zaufania obywatela do państwa i stanowionego przez nie prawa" (wyrok TK z 16 czerwca 1999 r., sygn. akt P 4/98; zob. też np. wyroki TK z: 25 listopada 1997 r., sygn. akt K 26/97; 10 kwietnia 2006 r., sygn. akt SK 30/04).

Jedną z zasad wyprowadzanych z art. 2 Konstytucji jest zasada określoności przepisów prawa, zwana też zasadą określoności regulacji prawnych (zob. np. wyroki TK z: 4 listopada 2003 r., sygn. akt SK 30/02; 10 listopada 2004 r., sygn. akt Kp 1/04; 2 kwietnia 2007 r., sygn. akt SK 19/06; 12 czerwca 2008 r., sygn. akt K 50/05; 30 września 2008 r., sygn. akt K 44/07; postanowienie TK z 14 grudnia 2005 r., sygn. akt SK 24/05; B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, komentarz do art. 2, nb. 9; W. Sokolewicz [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. V, Warszawa 2007, komentarz do art. 2, s. 48 i n.). Wymaga ona, aby „przepisy prawne były formułowane w sposób poprawny, precyzyjny i jasny" (wyrok TK z 7 listopada 2006 r., sygn. akt SK 42/05; zob. też wyroki TK z: 11 stycznia 2000 r., sygn. akt K 7/99; 12 czerwca 2008 r., sygn. akt K 50/05; W. Sokolewicz [w:] *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 2, s. 49). Jak wskazuje Trybunał Konstytucyjny w wyroku z 21 marca 2001 r. (sygn. akt K 24/00): „Z tak ujętej zasady określoności wynika, że każdy przepis prawny winien być skonstruowany poprawnie z punktu widzenia językowego i logicznego – dopiero spełnienie tego warunku podstawowego pozwala na jego ocenę w aspekcie pozostałych kryteriów. Wymóg jasności oznacza nakaz tworzenia przepisów klarownych i zrozumiałych dla ich adresatów, którzy od racjonalnego ustawodawcy oczekiwać mogą stanowienia norm prawnych nie budzących wątpliwości co do treści nakładanych obowiązków i przyznawanych praw. Związana z jasnością precyzja przepisu winna przejawiać się w konkretności nakładanych obowiązków i przyznawanych praw tak, by ich treść była oczywista i pozwalała na wyegzekwowanie" (zob. też wyrok TK z 12 czerwca 2008 r., sygn. akt K 50/05; W. Sokolewicz [w:] *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 2, s. 48).

Należy również dodać, że „ocena zgodności przepisów prawa z zasadą określoności regulacji prawnych musi uwzględniać specyfikę poszczególnych gałęzi

prawa, charakter adresatów ustanowionych norm prawnych, a także wagę praw jednostki i interesów, których dotyczy dana regulacja. Mniejsza precyzja sformułowań może wynikać z konieczności uwzględnienia różnorodności sytuacji w określonej sferze życia społecznego. Szczególna precyzja i jednoznaczność norm prawnych wymagana jest natomiast w dziedzinie prawa karnego. Kwalifikowana niejasność przepisu uzasadniająca stwierdzenie niekonstytucyjności może wynikać m.in. z jego niezrozumiałości, a także z użycia pojęć o szczególnym stopniu nieostrości, stwarzających niebezpieczeństwo arbitralnej ingerencji w sferę praw i wolności konstytucyjnych" (wyrok TK z 7 listopada 2006 r., sygn. akt SK 42/05).

2. Zgodnie z art. 47 Konstytucji, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Już pobieżna analiza tego przepisu prowadzi do wniosku, że zostały w nim unormowane dwa aspekty prawa do prywatności. Pierwszy z nich wyraża się w prawie jednostki do ochrony prawnej życia prywatnego, rodzinnego, czci, dobrego imienia i wiąże się ze stosownymi pozytywnymi obowiązkami władzy państwowej. Natomiast drugi z tych aspektów, wyrażający się w prawie do decydowaniu o swoim życiu osobistym, ma w istocie charakter „wolności" i polega „na wykluczeniu wszelkiej postronnej ingerencji w sferę życia osobistego jednostki" (P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. III, Warszawa 2003, komentarz do art. 47, s. 1; por. również wyroki TK z: 2 kwietnia 2001 r., sygn. akt SK 10/00; 9 lipca 2009 r., sygn. akt SK 48/05).

Jak wskazuje Trybunał Konstytucyjny: „Koncepcja prawa do prywatności zaczęła stosunkowo niedawno odgrywać poważniejszą rolę w regulacjach konstytucyjnych i orzecznictwie sądowym. Zdołała już jednak zyskać sobie trwałe miejsce we współczesnych państwach demokratycznych. Stanowią ją zasady i reguły odnoszące się do różnych sfer życia jednostki, a ich wspólnym mianownikiem jest przyznanie jednostce prawa «do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej» (A. Kopff, *Koncepcje prawa do intymności i do prywatności życia. Zagadnienia konstrukcyjne*, Studia Cywilistyczne, t. XX/1972). Tak rozumiana prywatność odnosi się przede wszystkim do życia osobistego, rodzinnego, towarzyskiego i czasem jest określana jako «prawo do pozostawienia w spokoju» (zob. W. Sokolewicz, *Prawo do prywatności* [w:] *Prawa człowieka w Stanach Zjednoczonych*, Warszawa 1985,

s. 252). Na ogół przyjmuje się, że prywatność odnosi się też do ochrony informacji dotyczących danej osoby i gwarantuje m.in. pewien stan niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu" (orzeczenie TK z 24 czerwca 1997 r., sygn. akt K 21/96).

3. Prawo do prywatności nie ma charakteru absolutnego i jako takie może być limitowane. Podlega to jednak ocenie przez pryzmat art. 31 ust. 3 Konstytucji (zob. np. P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 47, s. 4; wyroki TK z: 21 października 1998 r., sygn. akt K 24/98; 11 kwietnia 2000 r., sygn. akt K 15/98; 20 listopada 2002 r., sygn. akt K 41/02; 20 marca 2006 r., sygn. akt K 17/05), który formułuje kumulatywnie ujęte przesłanki dopuszczalności ograniczeń w korzystaniu z konstytucyjnych praw i wolności. Są to: 1) ustawowa forma ograniczenia; 2) istnienie w państwie demokratycznym konieczności wprowadzenia ograniczenia; 3) funkcjonalny związek ograniczenia z realizacją wskazanych w art. 31 ust. 3 Konstytucji wartości (bezpieczeństwo państwa, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, wolności i praw innych osób); 4) zakaz naruszania istoty danego prawa lub wolności (zob. np. wyrok TK z 30 maja 2007 r., sygn. akt SK 68/06; por. również L. Garlicki [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. III, Warszawa 2003, komentarz do art. 31, s. 14 i n.; J. Zakolska, *Zasada proporcjonalności w orzecznictwie Trybunału Konstytucyjnego*, Warszawa 2008, s. 115-141).

3. Analiza formalnoprawna

Wnioskodawca przedmiotem kontroli uczynił m.in. art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, zgodnie z którym: „Kontrola operacyjna jest prowadzona niejawnie i polega na: stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych przy pomocy sieci telekomunikacyjnych". W związku z tym należy przypomnieć, że przepis ten był już przedmiotem rozstrzygnięcia Trybunału Konstytucyjnego w wyroku z 20 czerwca 2005 r. (sygn. akt K 4/04). W jego sentencji m.in. stwierdzono, iż art. 8 pkt 27 ustawy z dnia 27 czerwca 2003 r. o utworzeniu

Wojewódzkich Kolegiów Skarbowych oraz o zmianie niektórych ustaw regulujących zadania i kompetencje organów oraz organizację jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych (Dz. U. Nr 137, poz. 1302) w zakresie, w jakim ustala (aktualnie obowiązujące) brzmienie art. 36c ust. 4 ustawy o kontroli skarbowej, jest zgodny z art. 2 oraz z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Wymaga przy tym zauważenia, że specyficzne sformułowanie przedmiotu kontroli w sentencji przywołanego wyroku oparte zostało na następującej argumentacji: „Złożony przez grupę posłów wniosek obejmuje przepisy ustawy z dnia 27 czerwca 2003 r. o utworzeniu Wojewódzkich Kolegiów Skarbowych oraz o zmianie niektórych ustaw regulujących zadania i kompetencje organów oraz organizację jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych (Dz. U. Nr 137, poz. 1302; dalej: ustawa o w.k.s.). W szczególności wnioskodawca kwestionuje art. 1 ustawy o w.k.s., na podstawie którego utworzono Wojewódzkie Kolegia Skarbowe, art. 8 pkt 27 ustawy, w części nowelizującej art. 36-36e ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 1999 r. Nr 54, poz. 572 ze zm.; dalej: ustawa o kontroli skarbowej) oraz art. 15 pkt 1 lit. j i pkt 2 ustawy o w.k.s., na podstawie którego znowelizowano przepisy ustawy z dnia 21 czerwca 1996 r. o urzędach i izbach skarbowych (Dz. U. Nr 106, poz. 489 ze zm.; dalej: ustawa o urzędach i izbach skarbowych). W istocie rozpoznawany wniosek dotyczy trzech ustaw. W *petitum* wnioskodawca kwestionuje jedynie przepisy ustawy o w.k.s., jednakże w uzasadnieniu wniosku – w przypadku ustaw znowelizowanych – zarzuty niekonstytucyjności skierowano bezpośrednio wobec zmienionych przepisów ustawy o kontroli skarbowej (odnosząc je do poszczególnych ustępów art. 36-36e) oraz wobec przepisów ustawy o urzędach i izbach skarbowych (art. 5 ust. 9a-9c i art. 5a). Trybunał Konstytucyjny, związany granicami wniosku, w sentencji wyroku odniósł swoją ocenę do wskazanych w *petitum* wniosku przepisów ustawy o w.k.s. w zakresie, w jakim nowelizują poszczególne przepisy ustawy o kontroli skarbowej oraz ustawy o urzędach i izbach skarbowych". W świetle powyższego nie ulega wątpliwości, że przedmiotem rozpoznania Trybunału Konstytucyjnego w sprawie o sygn. akt K 4/04 była m.in. konstytucyjność art. 36c ust. 4 ustawy o kontroli skarbowej.

Kontrola art. 36c ust. 4 ustawy o kontroli skarbowej w sprawie o sygn. akt K 4/04 miała miejsce z perspektywy tych samych wzorców co w sprawie niniejszej,

a mianowicie art. 2 oraz art. 47 w związku z art. 31 ust. 3 Konstytucji (oprócz tego badano także zgodność z art. 49 i art. 51 ust. 2 Konstytucji). Podobnie podniesione przez wnioskodawców i analizowane przez Trybunał Konstytucyjny zarzuty w sprawie o sygn. akt K 4/04 były tożsame z zarzutami wskazanymi przez RPO. Dotyczyły one bowiem nieprecyzyjności (nadmiernej ogólności) kwestionowanego przepisu, która umożliwia pozyskiwanie wszelkich informacji o kontrolowanych podmiotach, według swobodnego uznania i z naruszeniem chronionej konstytucyjnie sfery prywatności jednostki („W ocenie wnioskodawcy, zakwestionowane przepisy sformułowane zostały tak ogólnie i nieprecyzyjnie, że dopuszczają możliwość uzyskiwania, gromadzenia, przetwarzania i wykorzystywania – w drodze czynności operacyjno-rozpoznawczych – wszelkich informacji o kontrolowanych podmiotach, według swobodnego uznania pracowników wywiadu skarbowego, z naruszeniem chronionej konstytucyjnie sfery prywatności jednostki"). Nie podzielając tych zarzutów, Trybunał Konstytucyjny uznał, że: „Z punktu widzenia zasady określoności przepisów art. 36c ustawy o kontroli skarbowej należy uznać za wystarczająco jasny i precyzyjny". Podkreślił przy tym, iż: „Ustawodawca, przyznając wywiadowi skarbowemu specjalne uprawnienia, zobowiązał jednocześnie jego pracowników do podejmowania działań tylko w określonym celu, według szczegółowo określonych procedur". Trybunał Konstytucyjny wskazał tu w szczególności na to, że: 1) „Kontrola operacyjna może być przeprowadzona w celu wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów przestępstw, enumeratywnie wskazanych w art. 36c ust. 1 pkt 1-5"; 2) „tylko wtedy, kiedy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne"; 3) „Kontrola operacyjna może być przeprowadzona na podstawie zarządzenia Sądu Okręgowego w Warszawie, wydanego w formie postanowienia, na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego. W przypadkach niecierpiących zwłoki, gdy zachodzi obawa utraty informacji lub zatarcia dowodów przestępstwa, kontrolę operacyjną może zarządzić Generalny Inspektor Kontroli Skarbowej, po uzyskaniu pisemnej zgody Prokuratora Generalnego, zwracając się jednocześnie do sądu z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od zarządzenia kontroli, Generalny Inspektor Kontroli Skarbowej wstrzymuje kontrolę operacyjną oraz nakazuje komisyjne zniszczenie materiałów zgromadzonych w wyniku jej stosowania"; 4) „Ustawa określa również szczegółowe

wymogi, jakie musi spełniać wniosek Generalnego Inspektora Kontroli Skarbowej"; 5) „a także określa dopuszczalny czas trwania kontroli". Trybunał Konstytucyjny wskazał również na przewidziane w ustawie o kontroli skarbowej komisyjne zniszczenie materiałów uzyskanych w czasie stosowania kontroli operacyjnej, niezawierających dowodów pozwalających na wszczęcie albo niemających znaczenia dla postępowania w sprawach o przestępstwa i wykroczenia, w tym skarbowe. Na tym tle sąd konstytucyjny wywiódł: „Uregulowania dotyczące kontroli operacyjnej pozwalają na stwierdzenie, że wynikająca z nich ingerencja w konstytucyjne prawo jednostki do ochrony życia prywatnego i autonomii informacyjnej (art. 47 i art. 51 ust. 2 Konstytucji) oraz wolność komunikowania się (art. 49 Konstytucji) mieści się w granicach dopuszczalnych przez Konstytucję, określonych w art. 31 ust. 3 Konstytucji. Ustawa ściśle określa sytuacje, które uzasadniają jej przeprowadzenie, a ich charakter wskazuje na istnienie konieczności zastosowania tego rodzaju ograniczeń. Skoro bowiem ustawodawca nakłada na organy kontroli skarbowej zadania polegające na rozpoznaniu i ujawnieniu przestępstw i wykroczeń w niej określonych oraz zapobieganiu im (art. 3 ust. 4 i 5 ustawy), to organy te muszą być wyposażone w instrumenty prawne pozwalające na wykonanie tych zadań. Ustawa szczegółowo reguluje procedurę związaną z przeprowadzeniem kontroli operacyjnej, dopuszczalny czas jej trwania i sposób postępowania z materiałami uzyskanymi w jej wyniku. Kontrola operacyjna zarządzana jest przy tym przez sąd, a to oznacza istnienie gwarancji ochrony praw człowieka".

Powyższe nakazuje stwierdzić, że podniesiony w niniejszej sprawie problem zgodności art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji był już przedmiotem wiążącego rozstrzygnięcia Trybunału Konstytucyjnego i w związku z tym – zgodnie z zasadą *ne bis in idem* uniemożliwiającą dwukrotne orzekanie w tej samej sprawie – nie może być obecnie przedmiotem wydania wyroku. W takim stanie rzeczy Trybunał Konstytucyjny powinien **umorzyć niniejsze postępowanie** w zakresie badania zgodności art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji ze względu na niedopuszczalność wydania wyroku (art. 39 ust. 1 pkt 1 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym, Dz. U. Nr 102, poz. 643 ze zm.; dalej jako ustawa o TK).

Wymaga jednocześnie podkreślenia, że dokonane w sprawie o sygn. akt K 4/04 ustalenia Trybunału Konstytucyjnego – oprócz tego, że przesądzają o konstytucyjności art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej – mają istotne znaczenie dla oceny konstytucyjności pozostałych zakwestionowanych w niniejszej sprawie przepisów zaliczonych do grupy pierwszej. Trzeba mieć bowiem na uwadze, że wszystkie te przepisy mają identyczną treść i umieszczone są w podobnym kontekście normatywnym. Wyrok Trybunału Konstytucyjnego w sprawie o sygn. akt K 4/04 nie tylko świadczy o konstytucyjnej dopuszczalności stosowania kontroli operacyjnej w określonym ustawowo kształcie, ale również unaocznia, że dokonując oceny tego typu regulacji, zarówno z perspektywy określoności jak i proporcjonalności ingerencji w prawo do prywatności, należy uwzględniać nie tylko brzmienie kwestionowanego przepisu, lecz także wszystkie inne regulacje o charakterze gwarancyjnym, które określają podstawy, granice i weryfikację kontroli operacyjnej. Nie można zatem analizować konstytucyjności pierwszej grupy kwestionowanych przepisów bez uwzględnienia takich zagadnień, jak np. ustawowe określenie okoliczności, uzasadniających zastosowanie kontroli operacyjnej; subsydiarność kontroli operacyjnej; sądowa weryfikacja czynności operacyjnych; czas trwania kontroli operacyjnej; istnienie procedur niszczenia materiałów kontroli operacyjnej, które okazały się zbędne z punktu widzenia jej celów.

4. Analiza zgodności

1. Odnosząc się do zarzutów RPO, na wstępie należy stwierdzić, że kontrola operacyjna, polegająca na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, ze swej istoty stanowi ingerencję w prawo do prywatności. Przy czym ingerencja ta dotyczy przede wszystkim tego aspektu prywatności, który związany jest z ochroną informacji dotyczących jednostki oraz z zapewnieniem jej autonomii w zakresie decydowania o udostępnianiu (ujawnianiu) tych informacji innym osobom czy też instytucjom.

Fakt, iż kontrola operacyjna ingeruje w prawo do prywatności nie oznacza jednak, że Konstytucja kategorycznie zabrania takich praktyk. Niekiedy bowiem niejawne wkroczenie w sferę prywatności jednostki jest konieczne dla realizacji celów, o których mowa w art. 31 ust. 3 ustawy zasadniczej. W wypadku pierwszej grupy kwestionowanych przepisów chodzi przede wszystkim o zapewnienie

bezpieczeństwa państwa, porządku publicznego, ochrony zdrowia oraz praw i wolności innych osób, co ma bezpośredni związek ze skuteczną realizacją zadań przez takie służby, jak np. Policja, Agencja Bezpieczeństwa Wewnętrznego, czy Centralne Biuro Antykorupcyjne (mowa tu przede wszystkim o zadaniach polegających na zapobieganiu, wykrywaniu, ustalaniu sprawców, a także uzyskiwaniu i utrwalaniu dowodów określonych przestępstw, godzących zarówno w interesy indywidualne jak i zbiorowe, w tym w interesy państwa). Jak wynika z wielu orzeczeń Trybunału Konstytucyjnego, jedną z istotnych funkcji demokratycznego państwa prawnego jest skuteczne zwalczanie negatywnych zjawisk, w tym przestępczości, które w skrajnym nasileniu mogą godzić w samo istnienie państwa. Dlatego ustawodawca ma nie tylko prawo, ale i obowiązek zwalczania owych negatywnych zjawisk poprzez nadawanie takich uprawnień organom kontroli czy też służbom, które to uprawnienia będą miały bezpośredni wpływ na zwiększenie sprawności ich działań. W konsekwencji Trybunał Konstytucyjny co do zasady dopuszcza wyposażenie organów kontroli czy też służb w specjalne uprawnienia, pozwalające na nawet daleko idące wkraczanie w sferę praw i wolności jednostki, w tym w prawo do prywatności (wyroki TK z: 13 lutego 2001 r., sygn. akt K 19/99; 20 czerwca 2005 r., sygn. akt K 4/04; 17 czerwca 2008 r., sygn. akt K 8/04; zob. także wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04, w którym w odniesieniu do pozyskiwania, w trybie czynności operacyjnych prowadzonych przez Policję, informacji i przechowywania tych informacji m.in. stwierdzono: „Czynności te są z natury rzeczy niejawne [także wobec zainteresowanego], prowadzone w warunkach dających policji szeroki margines uznaniowości, przy ograniczonych gwarancjach dla praw osoby poddanej tym czynnościom, a także okrojonej kontroli zewnętrznej, w tym sądowej. Ten sposób działania policji jest we współczesnym państwie nieodzowny. Przejrzystość czynności operacyjnych powodowałaby ich nieskuteczność. Współczesne państwo, zobowiązane do zapewnienia bezpieczeństwa [co także jest powinnością konstytucyjną], staje przed trudnym zadaniem, ze względu na zagrożenia terroryzmem, przestępczością [w tym także zorganizowaną]. Techniczne udogodnienia, wpływające na szybkość komunikowania się i przemieszczania, w równym stopniu mogą być wykorzystywane w celu ochrony bezpieczeństwa państwa, jak i przez przestępców. Działalność operacyjna policji, regulowana w ustawodawstwie zwykłym, realizowana w warunkach niejawności, pozostaje

w naturalnym, nieusuwalnym konflikcie z niektórymi prawami zasadniczymi jednostki. W szczególności dotyczy to prawa jednostki do prywatności, konstytucyjnej wolności komunikowania się i związanej z tym ochrony tajemnicy komunikowania się, ochrony autonomii informacyjnej [którą w Polsce określają art. 49 i 51 Konstytucji], a także z konstytucyjną gwarancją sądowej ochrony praw jednostki. Konflikt ten występuje powszechnie, jest znany we wszystkich demokratycznych państwach prawnych, a także na tle praktyki organów międzynarodowych").

Nie powinno ulegać wątpliwości, że regulacje uprawniające służby do niejawnego wkroczenia w sferę prywatności jednostki powinny odpowiadać określonym wymogom. Najogólniej rzecz ujmując muszą one pozostawać w zgodności ze standardami ochrony praw i wolności obywatelskich gwarantowanych Konstytucją. Jak zaznacza Trybunał Konstytucyjny, chodzi tu przede wszystkim o to, aby dokonywana przez służby ingerencja w sferę życia prywatnego jednostki spełniała warunki określone w art. 31 ust. 3 Konstytucji. Ponadto, „ustawodawca – w świetle art. 2 Konstytucji – ma konstytucyjny obowiązek określić przesłanki ingerencji w sferę prywatności w sposób możliwie precyzyjny, tak aby ograniczyć zakres swobody decyzyjnej pozostawionej organom stosującym prawo, a jednocześnie ma on obowiązek stworzyć odpowiednie mechanizmy kontroli nad aktami organów władzy publicznej dotykającymi tej sfery. W sytuacji gdy chodzi o ograniczenie konstytucyjnych wolności i praw człowieka i obywatela, przepisy muszą charakteryzować się należytą precyzją i jasnością. Nakaz ten jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa" (wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04; a także wyrok TK z 17 czerwca 2008 r., sygn. akt K 8/04).

2. Z przepisów zaliczonych do grupy pierwszej przede wszystkim wynika, że kontrola operacyjna prowadzona jest niejawnie i polega na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie. Ponadto przepisy te przykładowo wskazują, że chodzi tu „w szczególności" o treść rozmów telefonicznych i inne informacje przekazywane za pomocą sieci telekomunikacyjnych, a ustawa o Straży Granicznej i ustawa o Żandarmerii Wojskowej dodatkowo mówią o obrazie.

Powyższe przepisy regulują jeden z aspektów kontroli operacyjnej, która może być prowadzona przez uprawnione do tego służby. Należy mieć przy tym na uwadze,

że owa kontrola operacyjna nie ma charakteru nieograniczonego i podlega różnego rodzaju limitacjom. Do najważniejszych z nich należy zaliczyć następujące.

3. Po pierwsze, niejawna kontrola operacyjna może być stosowana tylko przez ściśle określone służby i w ramach realizacji ich ustawowych zadań. W realiach niniejszej sprawy służbami uprawnionymi do stosowania kontroli operacyjnej są: Policja, Straż Graniczna, Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego.

4. Po drugie, stosowanie niejawnej kontroli operacyjnej dopuszczalne jest tylko w określonych sytuacjach i dla realizacji określonych celów, co sprawia, że kontrola ta nie jest narzędziem uniwersalnym, które może być używane przy wykonywaniu wszelkich zadań uprawnionych służb.

Jeżeli chodzi o Policję, to kontrola operacyjna może być stosowana przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw: 1) przeciwko życiu, określonych w art. 148-150 Kodeksu karnego; 2) określonych w art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 211a, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1 -3, art. 258, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-3, art. 296a § 1, 2 i 4, art. 299 § 1-6 oraz art. 310 § 1, 2 i 4 Kodeksu karnego; 2a) określonych w art. 46 ust. 1, 2 i 4, art. 47 oraz art. 48 ust. 1 i 2 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. Nr 127, poz. 857); 3) przeciwko obrotowi gospodarczemu, określonych w art. 297-306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów; 4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów; 4a) skarbowych, o których mowa w art. 107 § 1 Kodeksu karnego skarbowego; 5) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją,

materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi; 6) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. – Przepisy wprowadzające Kodeks karny (Dz. U. Nr 88, poz. 554 i Nr 160, poz. 1083 oraz z 1998 r. Nr 113, poz. 715); 7) określonych w art. 43-46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. Nr 169, poz. 1411); 8) ściganych na mocy umów i porozumień międzynarodowych (art. 19 ust. 1 ustawy o Policji).

Jeżeli chodzi o Straż Graniczną, to kontrola operacyjna może być stosowana przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: 1) określonych w art. 163 § 1, art. 164 § 1, art. 165 § 1, art. 166 § 1 i 2, art. 167, art. 168, art. 171, art. 172, art. 173 § 1, art. 258, art. 264 § 2 i 3 i art. 299 § 1 Kodeksu karnego; 2) określonych w art. 270-275 Kodeksu karnego w zakresie dokumentów uprawniających do przekraczania granicy państwowej; 3) skarbowych, o których mowa w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów; 4) pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii; 5) określonego w art. 147 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach; 6) określonych w art. 228, 229 i 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej w związku z wykonywaniem obowiązków służbowych; 6a) określonych w art. 229 Kodeksu karnego, popełnionych przez osoby niebędące funkcjonariuszami lub pracownikami Straży Granicznej w związku z wykonywaniem czynności służbowych przez funkcjonariuszy lub pracowników Straży Granicznej; 7) ściganych na mocy umów międzynarodowych (art. 9e ust. 1 ustawy o Straży Granicznej).

Jeżeli chodzi o Żandarmerię Wojskową, to kontrola operacyjna może być stosowana przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych w granicach zadań tej służby, określonych w art. 4 ust. 1 ustawy

o Żandarmerii Wojskowej oraz w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, pkt 3 lit. b) i pkt 5 ustawy o Żandarmerii Wojskowej, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: 1) przeciwko pokojowi i ludzkości; 2) przeciwko Rzeczypospolitej Polskiej, z wyjątkiem przestępstw określonych w art. 127-132 Kodeksu karnego; 3) zamachu na jednostki i komórki organizacyjne Sił Zbrojnych; 4) zabójstwa; 5) uprowadzenia statku powietrznego lub wodnego; 6) użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym; 7) przyjęcia lub udzielenia korzyści majątkowej lub jej obietnicy w związku z pełnieniem funkcji publicznej; 8) uprowadzenia osoby; 9) handlu ludźmi; 10) wymuszenia okupu; 11) udziału w zorganizowanej grupie przestępczej; 12) nielegalnego wyrabiania, posiadania lub handlu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub psychotropowymi albo materiałami jądrowymi lub substancjami trującymi; 13) bezprawnego ujawnienia lub wykorzystania informacji niejawnych o klauzuli tajności „tajne" i „ściśle tajne"; 14) rozboju i kradzieży rozbójniczej; 15) dezercji z bronią lub dezercji wspólnie z innymi żołnierzami; 16) zaboru środków walki; 17) przestępstw ściganych na mocy umów i porozumień międzynarodowych (art. 31 ust. 1 ustawy o Żandarmerii Wojskowej).

Jeżeli chodzi o Centralne Biuro Antykorupcyjne, to kontrola operacyjna może być stosowana przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych w celu rozpoznawania, zapobiegania i wykrywania przestępstw, a także uzyskania i utrwalenia dowodów przestępstw: 1) określonych w art. 228-231, 250a, 258, 286, 296-297, 299, 310 § 1, 2 i 4 Kodeksu karnego; 2) skarbowych, o których mowa w art. 2 ust. 1 pkt 1 lit. d, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. Nr 200, poz. 1679, z 2004 r. Nr 240, poz. 2407 oraz z 2005 r. Nr 157, poz. 1314) (art. 17 ust. 1 ustawy o CBA).

Z nieco inną konstrukcją prawną mamy do czynienia w wypadku Agencji Bezpieczeństwa Wewnętrznego. Otóż przepis art. 27 ust. 1 ustawy o ABW stanowi jedynie, że kontrola operacyjna jest dopuszczalna przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Agencję Bezpieczeństwa Wewnętrznego w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2 tejże ustawy.

Nie oznacza to jednak, że kontrola operacyjna jest uniwersalnym narzędziem działań Agencji Bezpieczeństwa Wewnętrznego, gdyż spośród wielu zadań tej służby określonych w art. 5 ust. 1 ustawy o ABW, ustawodawca dopuszcza ją tylko przy realizacji jednego z nich, a mianowicie rozpoznawania, zapobiegania i wykrywania następujących przestępstw: a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa; b) godzących w podstawy ekonomiczne państwa; c) korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584, z 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375), jeśli może to godzić w bezpieczeństwo państwa; d) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa; e) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym – oraz ścigania ich sprawców. W związku z tym przepisem wypada wskazać, że postanowieniem z 15 listopada 2010 r. (sygn. akt S 4/10) Trybunał Konstytucyjny, na podstawie art. 4 ust. 2 ustawy o TK, przedstawił Sejmowi uwagi dotyczące uchybień stwierdzonych w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, których usunięcie jest niezbędne dla zapewnienia spójności systemu prawnego Rzeczypospolitej Polskiej. W uzasadnieniu tego postanowienia stwierdzono, że przepis ten „narusza standardy demokratycznego państwa prawnego, wynikające z Konstytucji i orzecznictwa Trybunału Konstytucyjnego", bowiem stanowiąc o przestępstwach godzących w podstawy ekonomiczne państwa, uniemożliwia identyfikację typów przestępstw określonych w ustawie karnej, których może dotyczyć kontrola operacyjna. Trzeba mieć jednak na uwadze, że w realiach niniejszej sprawy zarzut taki nie został postawiony, co wyklucza prowadzenie rozważań na jego temat.

Z podobną, jak w wypadku Agencji Bezpieczeństwa Wewnętrznego, konstrukcją prawną spotykamy się także na gruncie ustawy o Służbie Kontrwywiadu Wojskowego. Mianowicie, zgodnie z jej art. 31 ust. 1, kontrola operacyjna jest dopuszczalna przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Służbę Kontrwywiadu Wojskowego w celu realizacji zadań określonych w art. 5 ustawy o Służbie Kontrwywiadu Wojskowego.

Charakterystyczne jest jednak, że zakres realizowanych zadań, które uprawniają Służbę Kontrwywiadu Wojskowego do podjęcia kontroli operacyjnej jest – w odróżnieniu od pozostałych służb – bardzo szeroki i obejmuje nie tylko rozpoznawanie, zapobieganie oraz wykrywanie przestępstw określonych w art. 5 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego, lecz również m.in. „uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej SZ RP [Sił Zbrojnych Rzeczypospolitej Polskiej – uwaga własna] lub innych jednostek organizacyjnych MON, w zakresie określonym w pkt 1, oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń" (art. 5 ust. 1 pkt 4 ustawy o Służbie Kontrwywiadu Wojskowego), „uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia" (art. 5 ust. 1 pkt 6 ustawy o Służbie Kontrwywiadu Wojskowego); „ochrona bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa" (art. 5 ust. 1 pkt 7 ustawy o Służbie Kontrwywiadu Wojskowego); „ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez SZ RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez SZ RP i inne jednostki organizacyjne MON, w zakresie określonym w pkt 1" (art. 5 ust. 1 pkt 8 ustawy o Służbie Kontrwywiadu Wojskowego).

5. Po trzecie, stosowanie kontroli operacyjnej opiera się na zasadzie subsydiarności i niezbędności. Oznacza to, że jest ona dopuszczalna dopiero wówczas, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne (art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o Straży Granicznej, art. 31 ust. 1 ustawy o Żandarmerii Wojskowej, art. 27 ust. 1 ustawy o ABW, art. 17 ust. 1 ustawy o CBA, art. 31 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego). Wiążącej oceny w tym zakresie dokonuje sąd w procedurze udzielania zgody na kontrolę operacyjną (zob. wyrok TK z 20 kwietnia 2004 r., sygn. akt K 45/02).

6. Po czwarte, kontrola operacyjna podlega kontroli sądowej, która przybiera postać zgody uprzedniej (pierwotnej) lub następczej, uzyskiwanej na wniosek i przy udziale ściśle określonych podmiotów w stosunkowo sformalizowanej procedurze.

Jeżeli chodzi o Policję, to zgodnie z art. 19 ust. 1 ustawy o Policji „sąd okręgowy może, w drodze postanowienia, zarządzić kontrolę operacyjną, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody prokuratora okręgowego właściwego ze względu na siedzibę składającego wniosek organu Policji", zaś w myśl art. 19 ust. 3 ustawy o Policji: „W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Komendant Główny Policji lub komendant wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, o którym mowa w ust. 1, kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania".

Jeżeli chodzi o Straż Graniczną, to zgodnie z art. 9e ust. 1 ustawy o Straży Granicznej „sąd, na pisemny wniosek Komendanta Głównego Straży Granicznej, po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Straży Granicznej, po uzyskaniu pisemnej zgody właściwego prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną", zaś w myśl art. 9e ust. 4 ustawy o Straży Granicznej: „W przypadkach niecierpiących zwłoki, gdy mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa: 1) Komendant Główny Straży Granicznej, po uzyskaniu pisemnej zgody Prokuratora Generalnego, 2) komendant oddziału Straży Granicznej, po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 2, może zarządzić kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania".

Jeżeli chodzi o Żandarmerię Wojskową, to zgodnie z art. 31 ust. 1 ustawy o Żandarmerii Wojskowej „wojskowy sąd okręgowy, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej

zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej i pisemnej zgody właściwego wojskowego prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną", zaś w myśl art. 31 ust. 4 ustawy o Żandarmerii Wojskowej: „W przypadkach niecierpiących zwłoki, gdy mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa: 1) Komendant Główny Żandarmerii Wojskowej, po uzyskaniu pisemnej zgody Prokuratora Generalnego, 2) komendant oddziału Żandarmerii Wojskowej, po poinformowaniu Komendanta Głównego Żandarmerii Wojskowej i po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 2, może zarządzić kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo wojskowego sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania".

Jeżeli chodzi o Agencję Bezpieczeństwa Wewnętrznego, to zgodnie z art. 27 ust. 1 ustawy o ABW „sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną", zaś w myśl art. art. 27 ust. 3 ustawy o ABW: „W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Szef ABW może zarządzić, po uzyskaniu pisemnej zgody Prokuratora Generalnego, kontrolę operacyjną, zwracając się jednocześnie do sądu, o którym mowa w ust. 2, z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej Szef ABW wstrzymuje kontrolę operacyjną oraz poleca protokolarne, komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania".

Jeżeli chodzi o Centralne Biuro Antykorupcyjne, to zgodnie z art. 17 ust. 1 ustawy o CBA „sąd, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną", zaś w myśl art. 17 ust. 3 ustawy o CBA: „W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Szef CBA może zarządzić, po uzyskaniu zgody Prokuratora

Generalnego, kontrolę operacyjną, zwracając się jednocześnie z wnioskiem do sądu, o którym mowa w ust. 2, o wydanie postanowienia w tej sprawie. Sąd wydaje postanowienie w przedmiocie wniosku w terminie 5 dni. W przypadku nieudzielenia przez sąd zgody, Szef CBA wstrzymuje kontrolę operacyjną oraz poleca niezwłoczne, protokolarne, komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania".

Jeżeli chodzi o Służbę Kontrwywiadu Wojskowego, to zgodnie z art. 31 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego „sąd, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną", zaś w myśl art. 31 ust. 3 ustawy o Służbie Kontrwywiadu Wojskowego: „W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Szef SKW może zarządzić, po uzyskaniu pisemnej zgody Prokuratora Generalnego, kontrolę operacyjną, zwracając się jednocześnie do sądu, o którym mowa w ust. 2, z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej Szef SKW wstrzymuje kontrolę operacyjną oraz poleca niezwłoczne, protokolarne i komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania".

7. Po piąte, kontrola operacyjna jest limitowana czasowo, choć z możliwością wielokrotnego jej przedłużania, co następuje na wniosek i przy udziale ściśle określonych podmiotów w stosunkowo sformalizowanej procedurze.

Zgodnie z art. 19 ust. 8 ustawy o Policji: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może, na pisemny wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, o którym mowa w ust. 1, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny tej kontroli". Jak natomiast stanowi art. 19 ust. 9 ustawy o Policji: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać

postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa w ust. 8".

Zgodnie z art. 9e ust. 9 ustawy o Straży Granicznej: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może, na pisemny wniosek Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, złożony po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 1, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli". Jak natomiast stanowi art. 9e ust. 10 ustawy o Straży Granicznej: „W szczególnie uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu Straży Granicznej, na pisemny wniosek Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, złożony po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 1, może wydać postanowienie o kontroli operacyjnej prowadzonej przez czas oznaczony również po upływie okresów, o których mowa w ust. 9".

Zgodnie z art. 31 ust. 9 ustawy o Żandarmerii Wojskowej: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Wojskowy sąd okręgowy może, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej i właściwego prokuratora wojskowego, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli". Jak natomiast stanowi 31 ust. 10 ustawy o Żandarmerii Wojskowej: „W szczególnie uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, wojskowy sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu Żandarmerii Wojskowej, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej oraz właściwego prokuratora wojskowego, może

wydać postanowienie o kontroli operacyjnej prowadzonej przez czas oznaczony również po upływie okresów, o których mowa w ust. 9".

Zgodnie z art. 27 ust. 8 ustawy o ABW: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd, o którym mowa w ust. 2, może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli". Jak natomiast stanowi art. 27 ust. 9 ustawy o ABW: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa w ust. 8".

Zgodnie z art. 17 ust. 8 ustawy o CBA: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd, o którym mowa w ust. 2, może, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, na okres nie dłuższy niż kolejne 3 miesiące, jeżeli nie ustały przyczyny zarządzenia tej kontroli". Jak natomiast stanowi art. 17 ust. 9 ustawy o CBA: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa w ust. 8".

Zgodnie z art. 31 ust. 6 ustawy o Służbie Kontrwywiadu Wojskowego: „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd, o którym mowa w ust. 2, może, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli". Jan natomiast stanowi art. 31 ust. 7 ustawy o Służbie Kontrwywiadu Wojskowego: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne

dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa w ust. 6".

8. Po szóste, przepisy nie pozwalają na dowolne wykorzystanie dowodów uzyskanych za pomocą kontroli operacyjnej. Każda z kwestionowanych przez RPO ustaw zawiera unormowanie o identycznej treści, zgodnie z którym: „Wykorzystanie dowodu uzyskanego podczas stosowania kontroli operacyjnej jest dopuszczalne wyłącznie w postępowaniu karnym w sprawie o przestępstwo lub przestępstwo skarbowe, w stosunku do którego jest dopuszczalne stosowanie takiej kontroli przez jakikolwiek uprawniony podmiot" (art. 19 ust. 15a ustawy o Policji, art. 9e ust. 16a ustawy o Straży Granicznej, art. 31 ust. 16a ustawy o Żandarmerii Wojskowej, art. 27 ust. 15a ustawy o ABW, art. 17 ust. 15a ustawy o CBA, art. 31 ust. 14a ustawy o Służbie Kontrwywiadu Wojskowego). Przy czym, jeżeli w wyniku stosowania kontroli operacyjnej uzyskano dowód popełnienia przestępstwa lub przestępstwa skarbowego, w stosunku do którego można zarządzić kontrolę operacyjną, popełnionego przez osobę, wobec której była stosowana kontrola operacyjna, innego niż objęte zarządzeniem kontroli operacyjnej albo popełnionego przez inną osobę, o zgodzie na jego wykorzystanie w postępowaniu karnym orzeka postanowieniem sąd, który zarządził kontrolę operacyjną albo wyraził na nią zgodę, na wniosek prokuratora (Prokuratora Generalnego) – art. 19 ust. 15c ustawy o Policji, art. 9e ust. 16c ustawy o Straży Granicznej, art. 31 ust. 16c ustawy o Żandarmerii Wojskowej, art. 27 ust. 15c ustawy o ABW, art. 17 ust. 15c ustawy o CBA, art. 31 ust. 14c ustawy o Służbie Kontrwywiadu Wojskowego.

9. Po siódme, przepisy przewidują obowiązek niezwłocznego i komisyjnego zniszczenia tych materiałów uzyskanych w wyniku zastosowania kontroli operacyjnej, które nie zawierają dowodów pozwalających na wszczęcie postępowania karnego lub nie mają znaczenia dla toczącego się postępowania karnego (art. 19 ust. 17 ustawy o Policji, art. 9e ust. 18 ustawy o Straży Granicznej, art. 31 ust. 18 ustawy o Żandarmerii Wojskowej). Nieco innym sformułowaniem posługuje się tu ustawa o ABW, która w art. 27 ust. 16 stanowi o zniszczeniu materiałów uzyskanych

w wyniku zastosowania kontroli operacyjnej, które nie są istotne dla bezpieczeństwa państwa lub nie stanowią informacji potwierdzających zaistnienie przestępstwa. O zniszczeniu materiałów uzyskanych w wyniku zastosowania kontroli operacyjnej, które nie stanowią informacji potwierdzających zaistnienie przestępstwa mowa także w art. 17 ust. 16 ustawy o CBA i art. 31 ust. 15 ustawy o Służbie Kontrwywiadu Wojskowego.

10. Przywołane powyżej przepisy pozwalają stwierdzić, że niejawna kontrola operacyjna podlega licznym ograniczeniom o różnym charakterze. Ograniczenia te sprzeciwiają się przyjęciu, jak czyni to RPO, iż obowiązujące ustawodawstwo umożliwia służbom uzyskanie każdej informacji o jednostce i każdego dowodu jej dotyczącego. Takiemu stawianiu sprawy przez wnioskodawcę sprzeciwia się również orzecznictwo sądowe, gdzie przepisy normujące kontrolę operacyjną interpretowane są bardzo restrykcyjnie, czego przykładem są poniższe judykaty.

W uchwale składu 7 sędziów Sądu Najwyższego z 23 marca 2011 r. (sygn. akt I KZP 32/10) stwierdzono, że: „Dowodami uzyskanymi w wyniku kontroli operacyjnej, zarządzonej postanowieniem Sądu, wydanym na podstawie art. 17 ust. 1 i 2 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.), które pozwalają na wszczęcie postępowania karnego lub mają znaczenie dla toczącego się postępowania karnego (art. 17 ust. 15 tej ustawy), są jedynie dowody dotyczące przestępstw, określonych w jej art. 17 ust. 1, które zostały wskazane w postanowieniu o zastosowaniu kontroli operacyjnej lub w postanowieniu o udzieleniu tzw. zgody następczej, w tym wydanej także w toku kontroli operacyjnej (art. 17 ust. 3 ustawy), a popełnionych przez osobę, której dotyczyła zgoda pierwotna i osobę, co do której wydano zgodę następczą".

W postanowieniu Sądu Apelacyjnego w Warszawie z 18 maja 2007 r. (sygn. akt II AKz 288/07) uznano, że: „Ustawa o CBA wprowadza prawo korzystania z dowodów uzyskanych przez Centralne Biuro Antykorupcyjne w trybie art. 17 ust. 1 pkt 1 i 2 tej ustawy. Przepisy te nie wymieniają zbrodni zabójstwa, ani nieumyślnego spowodowania śmierci. Sprawia to, że uzyskane w tym trybie dowody nie mogą być podstawą ustaleń, jako zgromadzone w sposób sprzeczny z prawem, a tym samym nielegalnie".

W wyroku Sądu Apelacyjnego w Warszawie z 24 stycznia 2008 r. (sygn. akt II AKa 405/07) przyjęto w odniesieniu do ustawy o ABW: „Dowód w postaci informacji

uzyskanych z podsłuchu telefonicznego w trakcie rozmowy prowadzonej przez osobę, co do której właściwy Sąd wydał zezwolenie na stosowanie podsłuchu, z oskarżoną (...), co do której takiego zezwolenia nie uzyskano, nie może być procesowo wykorzystany, zarówno w postępowaniu przeciwko tej oskarżonej, jak i przeciwko oskarżonemu (...) którego m.in. ta rozmowa miała dotyczyć".

W uchwale Sądu Apelacyjnego w Gdańsku z 4 maja 2006 r. (sygn. akt ASDo 1/06) wywiedziono: „zamknięty katalog przestępstw, co do których możliwe jest uzyskanie zezwolenia na stosowanie podsłuchu, określony został w art. 19 ust. 1 ustawy o policji. Takie uregulowanie oznacza, że informacje uzyskane w drodze podsłuchu telefonicznego nie mogą stanowić dowodu w sprawie o przestępstwo inne, niż określone w wyżej wymienionym katalogu, zwłaszcza jeżeli dotyczy to innej osoby niż ta, przeciwko której prowadzone było postępowanie i wobec której zarządzono kontrolę rozmów".

11. Powyższy kontekst normatywny i orzeczniczy nie pozwala podzielić zaprezentowanej przez RPO krytycznej oceny pierwszej grupy kwestionowanych przepisów. Przewidziane przez prawo liczne normy gwarancyjne istotnie ograniczają możliwości i zakres stosowania kontroli operacyjnej, co sprawia, iż nie można tu mówić o nieograniczonej, dowolnej czy też niekontrolowanej ingerencji w prawo do prywatności. W szczególności za chybione należy uznać stanowisko, iż „tą drogą może być pozyskany każdy dowód i każda informacja o jednostce". Stawiając taką tezę wnioskodawca nie uwzględnia tego, że w świetle obowiązujących przepisów kontrola operacyjna nie jest i nie może być środkiem pozyskiwania jakichkolwiek dowodów lub informacji, lecz tylko tych z nich, które służą realizacji ustawowo określonych celów. I tak np. Policja może stosować kontrolę operacyjną tylko w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw wymienionych w art. 19 ust. 1 ustawy o Policji. Tym samym nie jest ona uprawniona do pozyskiwania w ten sposób innych informacji i dowodów. Nie jest oczywiście wykluczone, że wykonywane czynności operacyjno-rozpoznawcze (np. w postaci podsłuchu telefonicznego) doprowadzą do utrwalenia informacji, które nie mają znaczenia dla celów prowadzonej kontroli operacyjnej. Jest to jednak jedynie ich niezamierzony skutek, wynikający z określonych uwarunkowań technicznych (np. aparatura utrwalająca rozmowy telefoniczne nie dokonuje ich weryfikacji pod kątem

przydatności dla wykrycia określonego przestępstwa i w związku z tym nie może pominąć tych wątków utrwalanej rozmowy, które z tego punktu widzenia są zbędne). A ponadto, co istotniejsze, przepisy przewidują obowiązek niezwłocznego i komisyjnego zniszczenia tych materiałów uzyskanych w wyniku zastosowania kontroli operacyjnej, które nie mają znaczenia dla realizacji jej celów (np. nie zawierają dowodów pozwalających na wszczęcie postępowania karnego lub nie mają znaczenia dla toczącego się postępowania karnego – art. 19 ust. 17 ustawy o Policji).

12. Nie sposób jednocześnie podzielić zarzut RPO, zgodnie z którym o niekonstytucyjności pierwszej grupy kwestionowanych przepisów świadczy to, że nie określają one „z jakich środków technicznych mogą korzystać służby w celu zdobycia informacji i dowodów", co sprawia, iż służby te uprawnione są do posługiwania się wszelkimi środkami technicznymi.

Odnosząc się do powyższej kwestii należy w pierwszej kolejności stwierdzić, że wnioskodawca dokonał trafnej interpretacji pierwszej grupy kwestionowanych przepisów i prawidłowo ustalił, że przepisy te – *lege non distinguente* – dopuszczają stosowanie wszystkich dostępnych środków technicznych, umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie. Przy czym ustawodawca jedynie przykładowo wskazał w kwestionowanych przepisach, że może tu chodzić o takie środki techniczne, które pozwalają na pozyskiwanie i utrwalanie treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, a w wypadku niektórych z kwestionowanych przepisów – także obrazu. Taka zawartość normatywna kwestionowanych przepisów nie pozwala mówić o ich daleko idącej niedookreśloności. Już bowiem wskazanie w nich na środki techniczne zawęża zakres dopuszczalnych metod, którymi służby mogą posługiwać się dla uzyskiwania w sposób niejawny informacji i dowodów oraz ich utrwalania. Na podstawie pierwszej grupy kwestionowanych przepisów nie jest zatem dozwolone posługiwanie się wszelkimi metodami niejawnego uzyskiwania i utrwalania informacji i dowodów, lecz tylko tymi z nich, które przybierają postać stosowania środków technicznych. Tym samym służby w oparciu o pierwszą grupę kwestionowanych przepisów nie mogą przykładowo posługiwać się inwigilacją polegającą na bezpośredniej obserwacji danej osoby (śledzenie, podsłuch bezpośredni itp.), czy też bezpośrednim „wykradaniem" określonych informacji (np.

wyjęcie korespondencji ze skrzynki pocztowej). Ponadto, pierwsza grupa kwestionowanych przepisów wymaga, aby stosowane środki techniczne były środkami umożliwiającymi uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie. Z tego zaś wynika, że przepisy te nie pozwalają na stosowanie środków technicznych o innym charakterze, np. zakłócających lub uniemożliwiających połączenia telefoniczne bądź też połączenia z siecią komputerową.

W końcu należy zwrócić uwagę, że realizacja postulatu RPO, zgodnie z którym pierwsza grupa kwestionowanych przepisów powinna konkretyzować środki techniczne, jakimi mogą posługiwać się służby w celu zdobycia informacji i dowodów, prowadziłaby do konieczności zaprzeczenia abstrakcyjnego i ogólnego charakteru normy prawnej (na problem nadmiernej szczegółowości czy też kazuistyki przepisu, która przeczy abstrakcyjnemu i ogólnemu charakterowi zawartej w nim normy prawnej Trybunał Konstytucyjny wielokrotnie wskazywał w orzecznictwie dotyczącym określoności przepisów prawa karnego, a więc tych, w stosunku do których wymogi doprecyzowania są największe, np. „jakiekolwiek wskazanie ogólnikowe, umożliwiające daleko idącą swobodę interpretacji co do zakresu znamion czynu zabronionego czy pewnego typu kategorii zachowań, nie może być traktowane jako spełniające wymóg określoności na gruncie art. 42 ust. 1 Konstytucji. Nie oznacza to jednak, że ustawodawca nie może określać pewnych zachowań stanowiących czyn zabroniony w sposób na tyle ogólny, aby w ich zakresie mieściły się różne działania, które są zabronione np. ze względu na cel, jaki ma być osiągnięty przez ich realizację. Wniosek przeciwny należałoby uznać za absurdalny, bowiem w krańcowym ujęciu prowadziłby do konieczności zaprzeczenia abstrakcyjnego i ogólnego charakteru normy prawnej" – wyrok TK z 26 listopada 2003 r., sygn. akt SK 22/02; a także wyroki TK z: 5 maja 2004 r., sygn. akt P 2/03; 13 stycznia 2005 r., sygn. akt P 15/02; 28 czerwca 2005 r., sygn. akt SK 56/04; 17 grudnia 2008 r., sygn. akt P 16/08; 22 czerwca 2010 r., sygn. akt SK 25/08; 1 grudnia 2010 r., sygn. akt K 41/07). Kwestionowane przepisy musiałby bowiem kazuistycznie wymieniać trudną bliżej do określenia liczbę środków technicznych, które służą do prowadzenia kontroli operacyjnej (np. podsłuch elektroniczny, mikrofon kierunkowy, tzw. konie trojańskie i innego rodzaju komputerowe programy szpiegujące, GPS – *Global Positioning System*). Inną sprawą jest to, czy współczesny stan techniki (różnorodność urządzeń umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich

utrwalanie), a także jej dynamiczny rozwój, pozwalają na stworzenie na potrzeby regulacji prawnej enumeratywnego katalogu środków dopuszczalnej kontroli operacyjnej.

13. Zgodnie z kolejnym postulatem RPO, pierwsza grupa kwestionowanych przepisów powinna precyzyjnie określać katalog danych o jednostce, jakie można pozyskiwać poprzez kontrolę operacyjną (czy też wskazywać „w jakie prawnie chronione dobra jednostki mogą ingerować służby za pomocą tych środków" bądź „jakich konkretnie sfer życia jednostki owa ingerencja dotyczy"). Wnioskodawca zdaje się przy tym stać na stanowisku, że pewne informacje o jednostce (sfery życia jednostki) winny być wyłączone z kontroli operacyjnej (czy też ich kontrola operacyjna winna być istotnie zawężona bądź też zabezpieczona szczególnymi gwarancjami), przy czym nie wskazuje wyraźnie o jakie informacje tu chodzi, odwołując się do konieczności „zróżnicowania intensywności konstytucyjnej ochrony poszczególnych praw składających się na prawo do prywatności".

Stanowisko RPO o konieczności „zróżnicowania intensywności konstytucyjnej ochrony poszczególnych praw składających się na prawo do prywatności" zasługuje na aprobatę. Jak bowiem wskazał, odwołujący się w tym zakresie do orzecznictwa Europejskiego Trybunału Praw Człowieka (dalej jako ETPCz), Trybunał Konstytucyjny w wyroku z 23 czerwca 2009 r. (sygn. akt K 54/07): „Sfera prywatna jest zbudowana z różnych kręgów w mniejszym lub większym stopniu otwartych (prawnie) na oddziaływanie zewnętrzne, gdzie konstytucyjna aprobata dla władczego wkroczenia przez władzę nie jest jednakowa (...). Potrzeba wkroczenia w różne kręgi prywatności nie jest dla każdego kręgu taka sama. Nie bez przyczyny np. poszanowanie prywatności mieszkania stawia wyższe wymagania legalności ingerencji władzy stosującej podsłuchy niż wkroczenie w tajemnicę korespondencji (...)". Niemniej jednak, jak podnosi Trybunał Konstytucyjny w cytowanym wyroku, „w ramach standardów demokratycznego państwa prawa dopuszczalne jest nawet głębokie wkroczenie w sferę prywatności, o ile wkroczenie to opatrzone zostanie należytymi gwarancjami proceduralnymi i w efekcie nie doprowadzi do naruszenia godności osoby poddanej kontroli" (stanowisko takie Trybunał Konstytucyjny zajął również w wyroku z 12 grudnia 2005 r., sygn. akt K 32/04). Do owych należytych gwarancji proceduralnych Trybunał Konstytucyjny zalicza cztery elementy, które określa mianem celowości, subsydiarności i niezbędności działania, a także

efektywnej kontroli zapobiegającej ekscesowi („Prowadzona przez policję bądź CBA obserwacja ma za cel zapobieżenie, wykrycie, ustalenie sprawców określonych przestępstw i dowodów popełnienia tych przestępstw. Jednakże sama może być prowadzona tylko jako działalność subsydiarna, tj. gdy inne środki są nieprzydatne lub bezskuteczne. Stanowi o tym wyraźnie m.in. art. 19 ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji [...]. Obserwacja winna mieścić się w granicach niezbędności dla założonego celu obserwacji. Te trzy ograniczenia [celowości, subsydiarności działania, niezbędności prowadzonej obserwacji] służą minimalizacji niekoniecznych – z punktu widzenia celu działalności operacyjnej – wkroczeń w prywatność. Realizacja tej zasady wymaga ponadto efektywnej kontroli zapobiegającej ekscesowi" – wyrok TK z 23 czerwca 2009 r., sygn. akt K 54/07). Przedstawione już we wcześniejszej części niniejszego stanowiska liczne normy gwarancyjne, które istotnie ograniczają możliwości i zakres stosowania kontroli operacyjnej, spełniają wszystkie warunki nawet głębokiego wkroczenia w każdą sferę prywatności. Należy tu w szczególności przypomnieć, że stosowanie niejawnej kontroli operacyjnej dopuszczalne jest tylko w ustawowo określonych sytuacjach i dla realizacji ustawowo określonych celów (celowość) i dopiero wówczas, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne (subsydiarność i niezbędność). Ponadto kontrola operacyjna podlega weryfikacji sądowej.

Nie można jednocześnie tracić z pola widzenia tego, że wykluczenie czy też zawężenie kontroli operacyjnej w odniesieniu do określonych sfer życia prywatnego nie wydaje się być zasadne w świetle celowości prowadzenia owej kontroli. Trzeba bowiem pamiętać, że bezprawna działalność, której zapobieżeniu, wykryciu, czy też ustaleniu jej sprawców służy kontrola operacyjna, może być związana niemal z każdą sferą prywatności, a zatem niesłuszne byłoby wyłączenie którejś z tych sfer z niejawnego pozyskiwania informacji. I tak np. ze sferą życia seksualnego wiąże się informacja o popełnieniu przestępstwa z art. 200 § 1 Kodeksu karnego („Kto obcuje płciowo z małoletnim poniżej lat 15 lub dopuszcza się wobec takiej osoby innej czynności seksualnej lub doprowadza ją do poddania się takim czynnościom albo do ich wykonania"), które wymienione jest w katalogu przestępstw uprawniających Policję do podjęcia kontroli operacyjnej (art. 19 ust. 1 pkt 2 ustawy o Policji); informacja o stanie zdrowia może z kolei wiązać się z ustaleniami dotyczącymi, wymienionego w art. 19 ust. 1 pkt 7 ustawy o Policji, przestępstwa polegającego na pobieraniu komórek, tkanek lub narządów w celu ich przeszczepienia albo też na ich

przeszczepianiu bez wymaganego pozwolenia (art. 46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, Dz. U. Nr 169, poz. 1411 ze zm.); a informacja o zarobkach może się wiązać z ustaleniami dotyczącymi objętych kontrolą operacyjną przestępstw skarbowych.

Należy również wskazać, że realizacja postulatu RPO, zgodnie z którym pierwsza grupa kwestionowanych przepisów powinna precyzyjnie określać katalog danych o jednostce, jakie można pozyskiwać poprzez kontrolę operacyjną, czy też wskazywać „w jakie prawnie chronione dobra jednostki mogą ingerować służby za pomocą tych środków" („jakich konkretnie sfer życia jednostki owa ingerencja dotyczy") mogłaby – jak już wspomniano – doprowadzić do zaprzeczenia abstrakcyjnego i ogólnego charakteru normy prawnej. Obawa ta jest tym większa, że przywoływane w kontekście tego postulatu prawo do prywatności (życie prywatne), mimo licznych analiz, nie dało się precyzyjnie opisać i zamknąć w powszechnie akceptowaną definicję. Konsekwencją poważnych trudności związanych z precyzyjnym zdefiniowaniem życia prywatnego jest rezygnacja z podejmowania takich prób i skupienie się na kazuistyce. Polega ona na wskazywaniu konkretnych sytuacji, które należałoby zaliczyć w obręb życia prywatnego, bądź uznawaniu, że ingerencja w określoną sferę egzystencji człowieka stanowi naruszenie jego życia prywatnego (zob. J. Braciak, *Prawo do prywatności* [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002, s. 293 i n.; A. Sakowicz, *Prywatność jako samoistne dobro prawne (per se)*, „Państwo i Prawo" 2006, nr 1, s. 21-22). W takim stanie rzeczy precyzyjne opisanie sfer życia prywatnego w przepisie normującym kontrolę operacyjną jest raczej niemożliwe, a jeżeli byłoby nawet możliwe, to wymagałoby stworzenia niezwykle rozbudowanej i kazuistycznej jednostki redakcyjnej tekstu prawnego.

14. Mając na uwadze powyższe rozważania należy stwierdzić, że art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA, art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego **są zgodne** z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

IV. Wolność i ochrona tajemnicy komunikowania się

1. Zarzuty wnioskodawcy

W ocenie RPO, druga grupa kwestionowanych przepisów pozostaje w sprzeczności z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.; dalej jako EKPCz). Kwestionowane przepisy, jak przyjmuje wnioskodawca, uprawniają służby do pozyskiwania tzw. danych telekomunikacyjnych, objętych tajemnicą komunikowania się, do których należą m.in. dane dotyczące użytkownika, dane o próbach uzyskania połączenia, czy też dane niezbędne do określenia czasu trwania połączenia. Przy czym owe wkroczenie w sferę tajemnicy komunikowania się – w opinii RPO – z kilku powodów nie spełnia standardów konstytucyjnych i konwencyjnych. Przede wszystkim nie opiera się ono na precyzyjnej podstawie (kwestionowane przepisy „nie regulują w sposób precyzyjny celu gromadzenia danych"), lecz jedynie na odwołaniu się do zakresu zadań poszczególnych służb bądź na ogólnym stwierdzeniu, iż dane pozyskiwane są w celu zapobiegania lub wykrywania przestępstw. Ponadto, przepisy upoważniające służby do ingerencji w tajemnicę komunikowania się nie przewidują obowiązku respektowania tajemnicy zawodowej (np. adwokackiej) oraz konieczności uprzedniego wykorzystania innych sposobów pozyskania potrzebnych informacji (zasada subsydiarności). Co więcej, wkroczenie w sferę tajemnicy komunikowania się nie podlega kontroli sądowej.

2. Wzorce kontroli

1. Zgodnie z art. 49 Konstytucji: „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony". W przepisie tym wyeksponowano trzy zagadnienia: wolność komunikowania się (zdanie 1), ochrona tajemnicy komunikowania się (zdanie 1), ograniczenie wolności i ochrony tajemnicy komunikowania się (zdanie 2).

Wolność komunikowania się należy rozumieć jako swobodę porozumiewania się, obejmującą wszystkich uczestników tego procesu (zarówno komunikujących, jak i odbierających komunikat), którymi mogą być osoby fizyczne lub inne podmioty prawa prywatnego. Nie ma przy tym znaczenia sposób porozumiewania się (np. werbalny czy niewerbalny), użyte do tego środki (np. telefon, list, e-mail), ani też treść i charakter komunikatu (np. informacja, prośba, ostrzeżenie) – zob. np. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 49, nb. 1-2; P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. III, Warszawa 2003, komentarz do art. 49, s. 1 i n.

Z kolei ochrona tajemnicy komunikowania się oznacza, że: „Treści przekazywane podczas (...) porozumienia się przeznaczone są wyłącznie dla adresata (adresatów). Osoby porozumiewające się ani nie mogą być zmuszone do ich ujawnienia, ani nawet zmuszone do ujawnienia drugiej strony (odbiorcy lub nadawcy tych treści). Ochrona tajemnicy komunikowania się oznacza także zabezpieczenie przed każdą ingerencją w sam proces komunikowania się polegającą na zmianie przekazywanych treści lub na ich zniszczeniu. Ponadto jakikolwiek inny podmiot nie powinien mieć do nich dostępu i tym bardziej z dostępu tego czynić użytku polegającego na ich ujawnieniu publicznym lub ujawnieniu innej osobie niż adresat. Państwo powinno tutaj chronić jednostkę zarówno przed nielegalnymi działaniami własnych organów, jak i innych osób fizycznych oraz prawnych" (B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 49, nb. 3; zob. też P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 49, s. 3).

Ograniczenie wolności i ochrony tajemnicy komunikowania się może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Jak wskazuje Trybunał Konstytucyjny: „Oznacza to, że – po pierwsze – ustawodawca zwykły może decydować o zakresie wolności komunikowania się, jeśli – po drugie – uczyni to w akcie rangi ustawy, wskazującym – po trzecie – «określone przypadki» i «sposób ograniczenia» (wymóg konkretności, wyłączenie użycia w tych zakresach otwartych klauzul generalnych)" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04). Istotne jest także to, aby realizacja ograniczeń wolności i ochrony tajemnicy komunikowania się podlegała kontroli ze strony sądu lub innego niezależnego i bezstronnego organu (zob. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 49, nb. 6; P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej...*,

komentarz do art. 49, s. 3). Znajduje to potwierdzenie w orzecznictwie Trybunału Konstytucyjnego, który w odniesieniu do kontroli operacyjnej przewidzianej w ustawie o Policji stwierdził: „w demokratycznym państwie prawnym ograniczenia w zakresie wolności i praw – znajdujące uzasadnienie w takich wartościach konstytucyjnych, jak bezpieczeństwo i porządek publiczny – powinny być poddane kontroli sądu. (...) Gwarancyjny charakter kontroli zewnętrznej (niekoniecznie zresztą sądowej, ale akurat kontrola sądowa tworzy zasadę w wypadku polskiej ustawy o Policji) leży w niezależności i bezstronności organu sprawującego tę kontrolę" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04).

Przy ustanawianiu ograniczeń wolności i ochrony tajemnicy komunikowania się należy uwzględniać także treść art. 31 ust. 3 Konstytucji (zob. np. P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 49, s. 3; wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04), o którym była już mowa we wcześniejszej części niniejszego stanowiska.

2. Wolność i ochrona tajemnicy komunikowania się jest jednym z przejawów prawa do prywatności (zob. np. wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04). W związku z tym nie powinno dziwić, że RPO formułując zarzuty wobec drugiej grupy kwestionowanych przepisów odwołał się także do art. 8 EKPCz, wykorzystując go jako jeden z wzorców kontroli. Odnosząc się do tego wzorca, wskazać należy, iż dotyczy on szeroko rozumianego prawa do poszanowania prywatnej (indywidualnej) sfery życia jednostki, przy czym sfera ta wykracza poza tradycyjne pojmowanie prywatności i obejmuje cztery podstawowe, nieraz zachodzące na siebie, dziedziny: życie prywatne, życie rodzinne, mieszkanie oraz korespondencję (zob. L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz do artykułów 1-18*, t. I, red. L. Garlicki, Warszawa 2010, s. 481).

Prawo do prywatności na gruncie EKPCz nie ma wymiaru absolutnego i zgodnie z art. 8 ust. 2 EKPCz dopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, jednakże pod warunkiem, że jest to przewidziane w ustawie i konieczne w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. W odniesieniu do tej klauzuli limitacyjnej przyjmuje się m.in., że podstawa prawna ingerencji władzy publicznej

w korzystanie z prawa do prywatności musi być ujęta w sposób odpowiadający pewnym „wymaganiom jakościowym", w tym m.in. musi charakteryzować się dostatecznym stopniem określoności czy też precyzyjności (zob. L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 486-487). Ponadto, w systemie prawnym powinny istnieć „gwarancje przeciwko nadużyciu uprawnień władzy publicznej do ingerowania w prawa i wolności jednostki. Gwarancje te «muszą w precyzyjny sposób wytyczać zakres uznania pozostawionego władzom publicznym i definiować okoliczności jego stosowania» (...). Oznaczać to może, że materialne kompetencje władzy publicznej powinny zostać obudowane systemem regulacji proceduralnych i instytucjonalnych, tak aby stworzyć wystarczające zabezpieczenie przeciwko dyskrecjonalności ich wykorzystywania (...). Dotyczy to zwłaszcza sytuacji, gdy – np. ze względu na bezpieczeństwo państwa – działania władz publicznych podejmowane są poza wiedzą osób, których dotyczą (...). W takich wypadkach większy stopień swobody władz musi być rekompensowany istnieniem procedur, pozwalających - choćby *ex post* - na ocenę legalności i zasadności ich działań (...)" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 487 i przywołane tam orzecznictwo ETPCz).

W realiach niniejszej sprawy szczególnego znaczenia nabiera ten aspekt ingerencji w prawo do prywatności, który wiąże się z pozyskiwaniem przez służby specjalne i policję informacji o obywatelach. Za punkt wyjścia w tego typu sprawach przyjmuje się, że służby „znajdują legitymowane podstawy egzystencji w społeczeństwie demokratycznym". Ich działalność, polegająca na gromadzeniu, przechowywaniu i wykorzystywaniu niejawnych informacji o jednostkach, jest uzasadniona zwłaszcza wówczas, gdy w grę wchodzi bezpieczeństwo państwa. Jednocześnie podkreśla się, że wskazane kompetencje służb „są tolerowalne tylko w zakresie ściśle koniecznym dla ochrony demokratycznych instytucji", zaś inwigilowanym jednostkom muszą przysługiwać określone gwarancje (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 509 i przywołane tam orzecznictwo ETPCz).

Podejmując próbę scharakteryzowania tendencji orzeczniczych ETPCz w sprawach dotyczących – najogólniej rzecz ujmując – pozyskiwania przez służby informacji o obywatelach, w ślad za L. Garlickim ([w:] *Konwencja o Ochronie Praw Człowieka...*, s. 510-512), wskazać należy na trzy następujące kwestie.

Po pierwsze, ETPCz „uznaje istnienie szerokiego związku gromadzenia danych z «życiem prywatnym» jednostki". Ingerencją w sferę chronioną przez art. 8 jest nie tylko gromadzenie danych o czysto prywatnym charakterze, ale także danych związanych z działalnością publiczną danej osoby (...), czy działalnością gospodarczą (...)". Przy czym „dla pojawienia się ingerencji w «życie prywatne» wystarczy sam fakt gromadzenia danych o danej osobie, a nie ma już znaczenia sposób późniejszego wykorzystywania tych informacji, stopień ich delikatności czy negatywny wpływ na życie lub interesy zainteresowanego (...). W zasadzie więc, zawsze niejawne gromadzenie danych przez służby specjalne wchodzi w zakres chroniony przez art. 8, a tym samym nie stanowi «naruszenia» Konwencji tylko, gdy jest przewidziane przez prawo i konieczne w demokratycznym społeczeństwie" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 510 i przywołane tam orzecznictwo ETPCz).

Po drugie, ETPCz „szeroko pojmuje wymaganie, by działania służb specjalnych opierały się na dostatecznych podstawach prawnych", kładąc szczególny nacisk na dwa elementy: 1) tzw. przewidywalność – „skoro praktyczna realizacja [gromadzenia informacji] nie jest poddana kontroli ani osoby zainteresowanej, ani opinii publicznej, sformułowanie zakresu uznania organów wykonawczych w kategoriach niczym nieskrępowanej swobody, naruszałoby zasadę rządów prawa. Oznacza to, że ustawa musi z dostateczną jasnością wytyczać zakres tego uznania przyznany poszczególnym władzom oraz sposób jego wykonywania. Brać przy tym pod uwagę należy prawowitość celu, któremu służą dane działania, tak aby jednostce zapewnić należyte gwarancje przez arbitralnymi ingerencjami"; 2) gwarancje przeciwko nadużyciom – „ustawa musi tworzyć system adekwatnych i skutecznych zabezpieczeń, zwłaszcza nadzoru nad działaniami służb specjalnych. «Zasada rządów prawa (...) wymaga, aby – normalnie – nadzór ten sprawowany był przez sądy, w każdym razie w ostatecznej instancji, bo sądowa kontrola zapewnia najlepsze gwarancje niezawisłości, bezstronności i odpowiedniej procedury» (...). Gdyby zaś, wyjątkowo, pojawiła się konieczność ograniczenia kontroli sądowej, niezbędne jest stworzenie mechanizmów kontroli, zewnętrznych wobec władzy wykonawczej, a umieszczonych np. w parlamencie lub w urzędzie ombudsmana (...). Brak odpowiednio rozbudowanego uregulowania prawnego tworzy, sam przez się, sytuację naruszenia art. 8 EKPCz" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 510-511 i przywołane tam orzecznictwo ETPCz).

Po trzecie, „choć Trybunał nie ma wątpliwości, iż gromadzenie danych przez służby specjalne służy «ochronie bezpieczeństwa państwowego», to nie zawsze jest skłonny uznać, iż jest ono «konieczne w państwie demokratycznym». Nawet uznanie, że władzom krajowym przysługuje tu «szeroki margines oceny» nie przekreśla znaczenia kryterium proporcjonalności. Działania służb muszą ograniczać się do zakresu «ściśle koniecznego dla ochrony demokratycznych instytucji» (...)" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 511 i przywołane tam orzecznictwo ETPCz).

3. Analiza zgodności

1. Wszystkie kwestionowane przepisy zaliczone do grupy drugiej regulują kwestię dostępu służb do tzw. danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.; dalej jako Prawo telekomunikacyjne).

W art. 180c ust. 1 Prawa telekomunikacyjnego mowa jest o danych niezbędnych 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. Dane te zostały uszczegółowione w Rozporządzeniu 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), wydanym na podstawie upoważnienia zawartego w art. 180c ust. 2 Prawa telekomunikacyjnego. Rozporządzenie te zawiera szczegółowy i rozbudowany wykaz danych, takich jak np. imię i nazwisko abonenta sieci telekomunikacyjnej; data i godzina nieudanej próby połączenia lub zestawienia i zakończenia połączenia; czas trwania połączenia z dokładnością do 1 sekundy; adres lokalizacji telekomunikacyjnego urządzenia końcowego, z którego inicjowano połączenie i do którego jest kierowane połączenie; adres IP; data i godzina każdorazowego połączenia i rozłączenia z Internetem; data i godzina zalogowania i wylogowania z usługi poczty elektronicznej i telefonii internetowej.

Z kolei w art. 180d Prawa telekomunikacyjnego mowa jest o danych opisanych w art. 159 ust. 1 pkt 1 i 3-5 Prawa telekomunikacyjnego (dane dotyczące użytkownika; 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 przerwanie zestawianych połączeń), w art. 161 Prawa telekomunikacyjnego (chodzi tu o następujące dane użytkowników: nazwiska i imiona; imiona rodziców; miejsca i daty urodzenia; adresy miejsca zameldowania na pobyt stały; numery ewidencyjne PESEL – w przypadku obywatela Rzeczypospolitej Polskiej; nazwy, serie i numery dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numery paszportów lub kart pobytu; zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych; a także inne dane, co do których dostawca publicznie dostępnych usług telekomunikacyjnych uzyskał zgodę użytkownika na ich przetwarzanie, a w szczególności: numer konta bankowego lub karty płatniczej, adres korespondencyjny użytkownika, jeżeli jest on inny niż adres miejsca zameldowania na pobyt stały, adres poczty elektronicznej oraz numery telefonów kontaktowych) oraz w art. 179 ust. 9 Prawa telekomunikacyjnego (elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniający dane uzyskiwane przy zawarciu umowy).

Z powyższego wynika, że katalog tzw. danych telekomunikacyjnych jest bardzo rozbudowany i zróżnicowany. Obejmuje on przede wszystkim liczne informacje dotyczące połączeń telekomunikacyjnych i osoby użytkownika sieci telekomunikacyjnej. W katalogu tzw. danych telekomunikacyjnych nie znajduje się

natomiast treść połączeń w ramach sieci telekomunikacyjnej (np. rozmów telefonicznych, poczty elektronicznej). Trzeba mieć jednak na uwadze, że za ingerencję w tajemnicę komunikowania się (prawo do prywatności) uważa się wszelkie formy kontroli w sferze telekomunikacji. Chodzi tu więc nie tylko o podsłuchiwanie czy rejestrowanie treści prowadzonych rozmów lub innych form komunikowania się, lecz również np. o samo identyfikowanie osób porozumiewających się, czy też o ustalanie czasu trwania połączenia (zob. np. L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 543; orzeczenie ETPCz z 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79). Tym samym pozyskiwanie przez służby tzw. danych telekomunikacyjnych, nie obejmujących treści połączeń telekomunikacyjnych, niewątpliwie stanowi wkroczenie w tajemnicę komunikowania się (prawo do prywatności).

2. Z art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej i art. 30 ust. 1 ustawy o Żandarmerii Wojskowej wynika wprost, że Policja, Straż Graniczna i Żandarmeria Wojskowa mogą mieć udostępniane tzw. dane telekomunikacyjne i są uprawnione do ich przetwarzania, zaś wywiad skarbowy może mieć udostępniane te dane. Przy czym następuje to „w celu zapobiegania lub wykrywania przestępstw" (w wypadku Policji i Straży Granicznej), „w celu zapobiegania lub wykrywania przestępstw, w tym skarbowych" (w wypadku Żandarmerii Wojskowej), „w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b [ustawy o kontroli skarbowej; chodzi tu o przestępstwa stypizowane w art. 228-231 Kodeksu karnego, popełnione przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych – uwaga własna], oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12 [ustawy o kontroli skarbowej; chodzi tu o krajowe i wspólnotowe przepisy celne – uwaga własna]" (w wypadku wywiadu skarbowego).

Powyższe przepisy przyznają służbom dostęp do tzw. danych telekomunikacyjnych w celu zapobiegania lub wykrywania – *lege non distinguente* – wszelkich przestępstw (Policja i Straż Graniczna), wszelkich przestępstw i wszelkich przestępstw skarbowych (Żandarmeria Wojskowa), wszelkich przestępstw skarbowych oraz niektórych innych przestępstw i naruszeń przepisów (wywiad

skarbowy). Mamy tu więc do czynienia z sytuacją diametralnie różną od tej, jaka ma miejsce w wypadku kontroli operacyjnej. Mianowicie, w odróżnieniu od kontroli operacyjnej, nie zawężono czy też nie dookreślono tu katalogu przestępstw, które upoważniają służby do ingerencji w tajemnicę komunikowania się. Tym samym do ingerencji tej może dojść w wypadku działań podejmowanych w celu zapobiegania lub wykrywania jakichkolwiek przestępstw (przestępstw skarbowych), w tym nawet tych najbardziej „błahych" (dość wskazać, że omawiane tu przepisy upoważniają do pozyskiwania tzw. danych telekomunikacyjnych także w wypadku przestępstw prywatnoskargowych).

Należy mieć również na uwadze, że dostęp Policji, Straży Granicznej, wywiadu skarbowego i Żandarmerii Wojskowej do tzw. danych telekomunikacyjnych nie jest objęty kontrolą sądową. Przepisy regulujące ów dostęp, w odróżnieniu od przepisów normujących kontrolę operacyjną, nie przewidują procedury uzyskiwania przez te służby ani uprzedniej, ani też następczej zgody sądowej na pozyskanie tzw. danych telekomunikacyjnych. Co więcej, przepisy te nie ustanawiają w tym zakresie żadnej kontroli zewnętrznej (np. prokuratorskiej).

3. Inną konstrukcję mają pozostałe kwestionowane przepisy zaliczone do grupy drugiej, a mianowicie art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA i art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego. Przede wszystkim *expressis verbis* zwalniają one Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne i Służbę Kontrwywiadu Wojskowego z obowiązku uzyskania zgody sądu na dostęp do tzw. danych telekomunikacyjnych, który to obowiązek przewidziany jest dla prowadzenia kontroli operacyjnej. Przy czym owe dane telekomunikacyjne muszą stanowić informację niezbędną do:

1) realizacji przez Agencję Bezpieczeństwa Wewnętrznego zadań, o których mowa w art. 5 ust. 1 ustawy o ABW. Chodzi tu o: 1) rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa; 2) rozpoznawanie, zapobieganie i wykrywanie przestępstw: a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa, b) godzących w podstawy ekonomiczne państwa, c) korupcji osób pełniących funkcje publiczne,

o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584, z 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375), jeśli może to godzić w bezpieczeństwo państwa, d) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, e) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym – oraz ściganie ich sprawców; 3) realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych; 4) uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego; 5) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych;

2) realizacji przez Centralne Biuro Antykorupcyjne zadań określonych w art. 2 ustawy o CBA. Chodzi tu o: 1) rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko: a) działalności instytucji państwowych oraz samorządu terytorialnego, określonych w art. 228-231 Kodeksu karnego, a także o którym mowa w art. 14 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584, z 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375), b) wymiarowi sprawiedliwości, określonym w art. 233, wyborom i referendum, określonym w art. 250a, porządkowi publicznemu, określonym w art. 258, wiarygodności dokumentów, określonych w art. 270-273, mieniu, określonym w art. 286, obrotowi gospodarczemu, określonych w art. 296-297, 299 i 305, obrotowi pieniędzmi i papierami wartościowymi, określonym w art. 310 Kodeksu karnego, a także o których mowa w art. 585-592 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037 ze zm.) oraz określonych w art. 179-183 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. Nr 183, poz. 1538 ze zm.), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa, c) finansowaniu partii politycznych, określonych w art. 49d i 49f ustawy z dnia 27 czerwca 1997 r. o partiach politycznych (Dz. U.

z 2001 r. Nr 79, poz. 857 ze zm.), jeżeli pozostają w związku z korupcją, d) obowiązkom podatkowym i rozliczeniom z tytułu dotacji i subwencji, określonych w rozdziale 6 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2007 r. Nr 111, poz. 765 ze zm.), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa, e) zasadom rywalizacji sportowej, określonych w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. Nr 127, poz. 857), f) obrotowi lekami, środkami spożywczymi specjalnego przeznaczenia żywieniowego, wyrobami medycznymi określonymi w art. 54 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. Nr 122, poz. 696) – oraz ściganie ich sprawców; 2) ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne; 3) dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy z dnia 21 czerwca 1990 r. o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych (Dz. U. Nr 44, poz. 255 ze zm.); 4) 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, o których mowa w art. 1 ust. 4 oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych; 5) kontrolę prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, o których mowa w art. 115 § 19 Kodeksu karnego, składanych na podstawie odrębnych przepisów; 6) prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi; 7) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych;

3) realizacji przez Służbę Kontrwywiadu Wojskowego zadań określonych w art. 5 ustawy o Służbie Kontrwywiadu Wojskowego. Chodzi tu o: 1) rozpoznawanie, zapobieganie oraz wykrywanie popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników

SZ RP i innych jednostek organizacyjnych MON, przestępstw: a) przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w rozdziale XVI Kodeksu karnego, a także innych ustawach i umowach międzynarodowych, b) przeciwko Rzeczypospolitej Polskiej określonych w rozdziale XVII Kodeksu karnego, oraz takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność, c) określonych w art. 140 Kodeksu karnego, d) określonych w art. 228-230 Kodeksu karnego, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, e) przeciwko ochronie informacji określonych w rozdziale XXXIII Kodeksu karnego, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, a także takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność, f) określonych w art. 33 ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004 r. Nr 229, poz. 2315), g) związanych z działalnością terrorystyczną oraz innych niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność; 2) współdziałanie z Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania przestępstw wymienionych w pkt 1; 3) realizowanie, w granicach swojej właściwości, zadań określonych w przepisach ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228); 4) uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, w zakresie określonym w pkt 1, oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń; 5) prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy; 6) uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia; 7) ochrona bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa; 8) ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez SZ RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez SZ RP i inne jednostki

organizacyjne MON, w zakresie określonym w pkt 1; 9) podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana.

Jak widać chodzi tu o wszystkie zadania Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego i Służby Kontrwywiadu Wojskowego, w tym również planistyczne, analityczne i dokumentacyjne.

4. Jak już była o tym mowa, wkroczenie przez służby w sferę tajemnicy komunikowania się (prawo do prywatności) co do zasady nie stoi w sprzeczności z Konstytucją i EKPCz. Jednakże zestawienie konstytucyjnych i konwencyjnych standardów z treścią i kontekstem normatywnym art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego prowadzi do wniosku, iż żaden z tych przepisów nie spełnia wymogów, jakim powinny odpowiadać regulacje uprawniające służby do ingerencji w tajemnicę komunikowania się (prawo do prywatności). Przy czym liczba zarzutów, jakie można w tym kontekście postawić drugiej grupie kwestionowanych przepisów, nie pozostawia wątpliwości, że wszystkie one pozostają w sprzeczności ze wskazanymi przez RPO wzorcami kontroli.

Po pierwsze, kwestionowane przepisy zaliczone do grupy drugiej – jak zasadnie zauważa RPO – nie wskazują precyzyjnych podstaw, które upoważniają służby do uzyskania dostępu do tzw. danych telekomunikacyjnych. Podstawą taką jest bowiem realizacja celu w postaci zapobiegania lub wykrywania wszelkich przestępstw i wszelkich przestępstw skarbowych, bez żadnych zawężeń w tym zakresie (Policja, Straż Graniczna, wywiad skarbowy i Żandarmeria Wojskowa) bądź też realizacja wszelkich zadań Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego i Służby Kontrwywiadu Wojskowego. Brak jakichkolwiek ograniczeń wskazanych podstaw uzyskiwania przez służby dostępu do tzw. danych telekomunikacyjnych świadczy o tym, że działania tego typu zrównane są na gruncie kwestionowanych ustaw ze „zwykłą", niewymagającą odrębnego i zawężającego unormowania, działalnością tych służb. Takie rozwiązanie nie odpowiada opisanym powyżej konstytucyjnym i konwencyjnym wymogom określoności i konkretności (precyzyjności) podstaw ingerencji w tajemnicę komunikowania się (prawo do

prywatności). Rozwijając w tym miejscu nieco ten opis należy dodać, że w doktrynie i orzecznictwie uznaje się, iż wymóg precyzyjności podstaw ingerencji w tajemnicę komunikowania się (prawo do prywatności) nakazuje w szczególności „określenie charakteru przestępstw, przy ściganiu których dopuszczalne jest zastosowanie tego środka" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 545 i przywołane tam orzecznictwo ETPCz), czego w wypadku kwestionowanych przepisów zabrakło.

Po drugie, jak również zasadnie zauważa RPO, żaden z uregulowanych w drugiej grupie kwestionowanych przepisów przypadków dostępu służb do tzw. danych telekomunikacyjnych nie podlega kontroli sądowej, ani też innej niezależnej i bezstronnej kontroli zewnętrznej. Taki stan rzeczy nie odpowiada wskazywanym powyżej standardom konstytucyjnym i konwencyjnym. W tym miejscu warto przypomnieć wyrok Trybunału Konstytucyjnego z 12 grudnia 2005 r. (sygn. akt K 32/04), w którym organ ten, uznając że realizacja ograniczeń wolności i ochrony tajemnicy komunikowania się powinna podlegać kontroli ze strony sądu, stwierdził: „(...) w demokratycznym państwie prawnym ograniczenia w zakresie wolności i praw – znajdujące uzasadnienie w takich wartościach konstytucyjnych, jak bezpieczeństwo i porządek publiczny – powinny być poddane kontroli sądu. (...) Gwarancyjny charakter kontroli zewnętrznej (...) leży w niezależności i bezstronności organu sprawującego tę kontrolę". Nie sposób też nie odnotować tu wypowiedzi Trybunału Konstytucyjnego, zawartej w wyroku z 12 grudnia 2005 r. (sygn. akt K 32/04), iż „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. (...) 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 tych 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". Również

w orzecznictwie ETPCz eksponuje się konieczność sądowego nadzoru nad działalnością służb. Poszerzając poczynione już w tym zakresie rozważania można dodać, że „przepisy prawa muszą określać procedurę wydawania zgody na zastosowanie środków kontroli (...), zgoda ta musi mieć w zasadzie charakter uprzedni, a jej wydanie musi podlegać nadzorowi organu zewnętrznego. W zasadzie, organem tym powinien być sąd (...). (...) prawo nie może tworzyć sytuacji, gdy «jedyną władzą oceniającą uzyskiwane materiały pozostają służby specjalne» (...)" (L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 545-546 i przywołane tam orzecznictwo ETPCz).

Po trzecie, na co także słusznie zwraca uwagę RPO, przepisy normujące dostęp służb do tzw. danych telekomunikacyjnych nie przewidują żadnych ograniczeń podmiotowych związanych z koniecznością respektowania tajemnicy zawodowej (np. adwokackiej). O ile zarzut ten sam w sobie może budzić pewne zastrzeżenia (związane np. z wątpliwościami co do tego jakie dane telekomunikacyjne mogą być w ogóle objęte tajemnicą zawodową, bo trudno za takie uznać np. numer telefonu adwokata czy też jego imię i nazwisko jako użytkownika usług telekomunikacyjnych), o tyle w kontekście innych uchybień kwestionowanych przepisów (zwłaszcza braku sądowej kontroli) nie sposób go bagatelizować. Zwłaszcza, że kwestia ta znajduje się w kręgu zainteresowań ETPCz w związku z badaniem naruszenia art. 8 EKPCz w sprawach dotyczących niejawnego pozyskiwania informacji przez służby. W szczególności ETPCz wskazuje na konieczność respektowania szczególnego statusu szeroko rozumianej korespondencji (na gruncie EKPCz pod pojęciem korespondencji rozumie się nie tylko tradycyjne komunikowanie się za pomocą pisma, ale również wszelkie inne formy przekazywania informacji) między adwokatem a jego klientem (zob. np. L. Garlicki [w:] *Konwencja o Ochronie Praw Człowieka...*, s. 545; orzeczenie ETPCz z 25 marca 1998 r. w sprawie Kopp przeciwko Szwajcarii, skarga nr 23224/94).

Po czwarte, w kontekście spełnienia przez kwestionowane przepisy konstytucyjnego i konwencyjnego wymogu konieczności ingerencji w sferę tajemnicy komunikowania się (prawo do prywatności) w państwie demokratycznym, na aprobatę zasługuje zarzut RPO, iż dostęp służb do tzw. danych telekomunikacyjnych nie opiera się na, znanej kontroli operacyjnej, zasadzie subsydiarności i niezbędności, zgodnie z którą dostęp ten powinien być dopuszczalny dopiero wówczas, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne.

Pominięcie tej zasady oznacza, że służby mogą już w pierwszej kolejności zwracać się o udostępnienie tzw. danych telekomunikacyjnych, bez wcześniejszego badania, czy uzyskanych w ten sposób informacji nie można zdobyć w inny, mniej ingerujący w prywatność jednostki, sposób. Jak zaś wielokrotnie już zauważał Trybunał Konstytucyjny, w tym w związku z działaniami podejmowanymi przez służby w ramach kontroli skarbowej (wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04), wynikający z art. 31 ust. 3 ustawy zasadniczej wymóg niezbędności ograniczenia praw i wolności polega na zastosowaniu „środków niezbędnych, w tym sensie, że chronić one będą określone wartości w sposób bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych [mniej uciążliwych – uwaga własna] środków" (zob. też wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04, gdzie w nawiązaniu do orzecznictwa ETPCz stwierdzono, że „zbieranie informacji w trybie kontroli operacyjnej traktowane być musi w ustawodawstwie i – co więcej – w praktyce działania policji, jako tryb subsydiarny [...] tj. jeżeli nie jest możliwe posługiwanie się trybem normalnym").

5. W świetle powyższego należy stwierdzić, że art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego **są niezgodne** z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 EKPCz.

V. Prawo do ochrony danych osobowych

1. Zarzuty wnioskodawcy

Zdaniem wnioskodawcy, trzecia grupa kwestionowanych przepisów „w zakresie w jakim, przepisy te zezwalając na pozyskiwanie danych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (...) nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania", jest niezgodna z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. RPO podnosi tu, że dane zgromadzone przez służby nie podlegają zniszczeniu także

wtedy, gdy „okazały się nieprzydatne z punktu widzenia realizowanych zadań", czy też celów, dla których zostały zebrane. Pozwala to na gromadzenie i bezterminowe przechowywanie takich zbędnych danych.

2. Wzorce kontroli

1. Zgodnie z art. 51 ust. 2 Konstytucji: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Z tego, adresowanego do władz publicznych, przepisu wynika jednoznacznie, że dopuszczalne jest pozyskiwanie, gromadzenie i udostępnianie tylko takich informacji o obywatelach, które są niezbędne w demokratycznym państwie prawnym. Nie do końca jasne jest natomiast to, jakie informacje o obywatelach mogą być uznane za niezbędne w demokratycznym państwie prawnym. W doktrynie przyjmuje się, że chodzi tu o takie dane, które „umożliwiają normalne funkcjonowanie jednostki w zorganizowanym w państwo społeczeństwie" i bez posiadania których władze publiczne nie są „zdolne do podjęcia (czy zakończenia) działań w ramach przyznanych im kompetencji". Nie będą więc niezbędne w demokratycznym państwie prawnym takie informacje o obywatelach, których pozyskiwanie, gromadzenie i udostępnianie służy jedynie „wygodzie" organów władzy publicznej, czy też, które są potrzebne tym organom „na wszelki wypadek", np. gdyby dana osoba w przyszłości dopuściła się przestępstwa (zob. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej...*, komentarz do art. 51, nb. 6; I. Lipowicz [w:] *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998, s. 99).

Jak podnosi Trybunał Konstytucyjny, art. 51 ust. 2 ustawy zasadniczej „po pierwsze legalizuje – nieuchronne we współczesnym społeczeństwie – działania władz publicznych polegające na pozyskiwaniu, gromadzeniu i udostępnianiu informacji o jednostkach w sposób inny niż w drodze zgłoszenia takich danych przez samego obywatela, zobligowanego w trybie określonym w art. 51 ust. 1 Konstytucji. Po drugie (...) w sposób częściowo autonomiczny określa przesłanki legalności (granice) takich działań. Konstytucja realizuje jednak w ten sposób najbardziej zasadnicze elementy składające się na treść prawa do ochrony życia prywatnego: respekt dla autonomii informacyjnej jednostki, a więc sam obowiązek udostępnienia

danych ograniczony do ściśle określonych ustawowo sytuacji; ograniczenie arbitralności ustawodawcy – ustawa nie może bowiem zakresu obowiązku kształtować dowolnie (...). Zakres autonomii informacyjnej obejmuje zarówno dane o charakterze *stricte* personalnym (osobowym), jak i te dotyczące majątku i sfery ekonomicznej jednostki. W tym ostatnim zakresie Trybunał dopuszcza jednak łagodniejsze kryteria jej ograniczania niż w wypadku sfery czysto osobistej (...)" (wyrok TK z 17 czerwca 2008 r., sygn. akt K 8/04 i przywołane tam inne orzeczenia TK).

2. Wskazywany przez RPO jako wzorzec kontroli art. 51 ust. 2 Konstytucji pozostaje w ścisłym związku z jej art. 51 ust. 1 („Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby") i z unormowanym co do zasady w art. 47 ustawy zasadniczej prawem do prywatności. Trzeba mieć przy tym na uwadze, że wkroczenie w sferę życia prywatnego jednostki, w tym w jej autonomię informacyjną dopuszczalne jest na zasadach określonych w art. 31 ust. 3 Konstytucji. W tym kontekście: „Istnienie w art. 51 ust. 2 Konstytucji odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki należy tłumaczyć tym, że naruszenia 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, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Normatywne wyodrębnienie, ustanowienie 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 niedozwolone pozyskiwanie informacji o obywatelach, powinno odpowiadać wymaganiom określonym w art. 31 ust. 3 Konstytucji" (wyrok TK z 20 listopada 2002 r., sygn. akt

K 41/02). Do relacji między art. 31 ust. 3 i art. 51 ust. 2 Konstytucji odniósł się Trybunał Konstytucyjny także m.in. w wyroku z 17 czerwca 2008 r. (sygn. akt K 8/04), gdzie stwierdził: „Norma wysłowiona w art. 51 ust. 2 Konstytucji nie ma charakteru całkowicie samodzielnego. Wprawdzie ustrojodawca wskazał w powołanym przepisie *expressis verbis* na ograniczenie możliwości arbitralnego kształtowania zakresu informacji o obywatelach pozyskiwanych przez władze publiczne w ustawodawstwie zwykłym i podkreślił wymóg niezbędności takiego ograniczenia, oceniany wedle standardów obowiązujących w demokratycznym państwie prawnym, nie określił jednak katalogu interesów (wartości) konstytucyjnie chronionych, które – jego zdaniem – mogą być stawiane na szali w procesie oceny dopuszczalności takiego rozwiązania. W tym zakresie konieczne jest odwołanie się do ogólnej regulacji art. 31 ust. 3 Konstytucji, zgodnie z którym 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 i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw".

3. W celu wyjaśnienia ewentualnych wątpliwości godzi się w tym miejscu dodatkowo wskazać, że do zarzutów skierowanych przez RPO wobec trzeciej grupy kwestionowanych przepisów nie może znaleźć zastosowania norma wysłowiona w art. 51 ust. 4 Konstytucji („Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą"). Trzeba bowiem w szczególności pamiętać, że wnioskodawcy chodzi o wprowadzenie obowiązku zniszczenia tzw. danych telekomunikacyjnych, które zostały zebrane w sposób zgodny z ustawą, lecz następnie okazały się zbędne dla prowadzonego postępowania. W art. 51 ust. 4 Konstytucji nie ustanawia się natomiast prawa do żądania usunięcia informacji zbędnych.

3. Analiza zgodności

1. W pierwszej kolejności należy odnieść się do zarzutu niekonstytucyjności art. 36b ust. 5 ustawy o kontroli skarbowej, który to zarzut jawi się jako oczywiście chybiony. Zgodnie z kwestionowanym 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 lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, o którym mowa w ust. 2 [chodzi tu o wniosek o udostępnienie tzw. danych telekomunikacyjnych – uwaga własna], za nieuzasadnione". W opinii RPO, regulacja ta jest niewystarczająca, bowiem nakazuje wyłącznie „niezwłoczne zniszczenie tylko tych danych telekomunikacyjnych, które zostały zebrane na podstawie nieuzasadnionego wniosku o ich udostępnienie (...) nie przewiduje natomiast zniszczenia tych danych, które zostały zebrane na podstawie uzasadnionego wniosku, lecz nie mają znaczenia dla prowadzonego postępowania". Stawiając taki zarzut wnioskodawca nie dostrzega, że w ustawie o kontroli skarbowej zawarto art. 36d ust. 3, który stanowi, iż: „Materiały uzyskane w wyniku czynności podjętych na podstawie art. 36aa ust. 1, art. 36b ust. 1, art. 36c ust. 1 i 2 lub art. 36ca ust. 1, niezawierające dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe albo niemające znaczenia dla postępowania kontrolnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu". Regulacja ta nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie m.in. pozyskanych przez wywiad skarbowy tzw. danych telekomunikacyjnych („Materiały uzyskane w wyniku czynności podjętych na podstawie [...] art. 36b ust. 1"), jeżeli nie zawierają one dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe albo nie mają znaczenia dla postępowania kontrolnego. Tym samym unormowanie to w pełni spełnia oczekiwania wyrażone we wniosku RPO.

Zatem o ile rację ma wnioskodawca, że kwestionowany art. 36b ust. 5 ustawy o kontroli skarbowej nie przewiduje „zniszczenia tych spośród pozyskanych danych [telekomunikacyjnych – uwaga własna], które nie zawierają informacji mających znaczenie dla prowadzonego postępowania", o tyle nie można na tej podstawie formułować uzasadnionego zarzutu niekonstytucyjności, bowiem obowiązek

zniszczenia tych danych jest przewidziany w ustawie o kontroli skarbowej, tyle że w innej jednostce redakcyjnej niż kwestionowana przez RPO. Nie powinno zaś ulegać wątpliwości, że oceny kwestionowanych w postępowaniu przed Trybunałem Konstytucyjnym przepisów trzeba dokonywać z uwzględnieniem całego ich kontekstu normatywnego.

W świetle powyższego należy stwierdzić, że art. 36b ust. 5 ustawy o kontroli skarbowej, w zakresie, w jakim nie przewiduje zniszczenia tych spośród pozyskanych danych, o jakich mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, **jest zgodny** z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

2. Podzielić natomiast należy stanowisko RPO wyrażone w odniesieniu do pozostałych przepisów zaliczonych do grupy trzeciej, iż brak jest regulacji przewidującej obowiązek zniszczenia tych spośród pozyskanych tzw. danych telekomunikacyjnych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania. Rację ma również wnioskodawca, kiedy wskazuje, że taki stan rzeczy nie spełnia standardów konstytucyjnych.

Przede wszystkim należy wskazać, że z ingerencją w prawo do prywatności czy też w autonomię informacyjną jednostki mamy do czynienia nie tylko wówczas, gdy służby pozyskują czy też udostępniają tzw. dane telekomunikacyjne, lecz również wtedy, gdy dane takie przechowują (zob. np. wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04). Dlatego też nie powinno ulegać wątpliwości, że określony sposób postępowania z takimi przechowywanymi informacjami „należy do warunków istotnych, z punktu widzenia ochrony prawa do prywatności i autonomii informacji oraz wolności komunikowania się, a także zasady zaufania do państwa i stanowionego przez nie prawa", zaś „zniszczenie takich materiałów niezwłocznie po zakończeniu kontroli operacyjnej stanowi gwarancję, że nie zostaną one wykorzystane w sposób nieuprawniony" (wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04). Jak więc widać, zniszczenie zbędnych dla toczącego się postępowania informacji, które zostały zgromadzone przez służby, ma na celu przede wszystkim zapobieżenie ich nieuprawnionemu wykorzystaniu. Na kwestię tę zwraca uwagę Trybunał Konstytucyjny, wskazując m.in. na możliwość ujawnienia zgromadzonych informacji poprzez tzw. przecieki, które służą „celom lub metodom wykraczającym poza ochronę demokratycznego ładu, co jest celem i granicą legalności czynności

operacyjnych" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04). Na marginesie można również wskazać, że konieczność istnienia procedur niszczenia zgromadzonych przez służby informacji o jednostkach, które to informacje okazały się zbędne czy też nieistotne, dostrzegana jest także w orzecznictwie ETPCz (zob. np. orzeczenie ETPCz z 1 lipca 2008 r. w sprawie Liberty and Others przeciwko Wielkiej Brytanii, skarga nr 58243/00).

Wobec powyższego nie sposób nie zgodzić się z Trybunałem Konstytucyjnym, kiedy stwierdza: „W demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny" i „konieczne jest skonstruowanie takiego systemu zabezpieczeń proceduralnych, który w skuteczny sposób zabezpieczałby przed ekscesami ([...] niewłaściwe zabezpieczenie czy wykorzystanie zebranych danych)" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04).

Kwestionowane regulacje, nieprzewidujące obowiązku zniszczenia tzw. danych telekomunikacyjnych, które okazały się zbędne dla prowadzonego postępowania, pozwalają na przechowywanie tych danych tylko ze względu na ich potencjalną przydatność. Mogą być one również przechowywane bez żadnego celu i wiązać się wyłącznie z zaniechaniem dokonania prawidłowej weryfikacji ich znaczenia dla prowadzonego postępowania. Dysponowanie takimi zbędnymi informacjami niewątpliwie rodzi ryzyko ich nieuprawnionego wykorzystania. Zwłaszcza, że wobec zbędności tych informacji, możliwość ich uprawnionego wykorzystania w postępowaniu, dla potrzeb którego zostały zgromadzone, jest w zasadzie wykluczona.

Wobec powyższego należy uznać, że art. 28 ustawy o ABW, art. 18 ustawy o CBA, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego, w zakresie, w jakim przepisy te, zezwalając na pozyskiwanie danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, **są niezgodne** z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

VI. Dodatkowe wnioski Sejmu

W wypadku uznania przez Trybunał Konstytucyjny niekonstytucyjności przepisów kwestionowanych w niniejszej sprawie, Sejm wnosi o odroczenie o 18 miesięcy terminu utraty ich mocy obowiązującej (art. 190 ust. 3 Konstytucji). Analogicznie jak miało to miejsce w sprawie o sygn. akt K 32/04 dotyczącej konstytucyjności czynności operacyjno-rozpoznawczych uregulowanych w ustawie o Policji: „Zastosowanie uprawnienia do określenia innego, niż wejście w życie wyroku Trybunału, terminu utraty mocy obowiązującej niekonstytucyjnych aktów normatywnych" jest „zdeterminowane wagą kwestii prawnych regulujących kontrolę operacyjną oraz inne czynności operacyjno-rozpoznawcze podejmowane przez Policję [w niniejszej sprawie chodzi także o inne służby – uwaga własna] oraz koniecznością zapewnienia kontynuacji prowadzonych działań" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04).

MARSZAŁEK SEJMU

Ewa Kopacz