80/7/A/2014

WYROK
z dnia 30 lipca 2014 r.
Sygn. akt K 23/11*

W imieniu Rzeczypospolitej Polskiej

Trybunał Konstytucyjny w składzie:

Andrzej Rzepliński – przewodniczący, II sprawozdawca
Stanisław Biernat
Maria Gintowt-Jankowicz
Mirosław Granat
Wojciech Hermeliński
Leon Kieres
Marek Kotlinowski
Teresa Liszcz
Małgorzata Pyziak-Szafnicka
Stanisław Rymar
Piotr Tuleja
Sławomira Wronkowska-Jaśkiewicz
Andrzej Wróbel
Marek Zubik – I sprawozdawca,

protokolant: Grażyna Szałygo, Krzysztof Zalecki,

po rozpoznaniu, z udziałem wnioskodawców oraz Sejmu i Prokuratora Generalnego, na rozprawie w dniach 1, 2 i 3 kwietnia oraz 30 lipca 2014 r., połączonych wniosków:

1) Rzecznika Praw Obywatelskich z 29 czerwca 2011 r. o zbadanie zgodności:
   a) art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277, ze zm.),
   b) art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675),
   c) art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214),
   d) 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.),
   e) art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, ze zm.),
   f) 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.),
   g) 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.)

* Sentencja została ogłoszona dnia 6 sierpnia 2014 r. w Dz. U. poz. 1055.

– z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji,

2) Rzecznika Praw Obywatelskich z 1 sierpnia 2011 r. o zbadanie zgodności:
   a) art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego 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.),
   b) art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ustawy o Centralnym Biurze Antykorupcyjnym, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego 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, z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji,

3) Rzecznika Praw Obywatelskich z 15 listopada 2011 r. o zbadanie zgodności:
   a) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa”,
   b) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b oraz c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu
   – z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności,

4) Prokuratora Generalnego z 7 marca 2012 r. o zbadanie zgodności:
   a) art. 19 ust. 1 pkt 8 ustawy o Policji,
   b) art. 9e ust. 1 pkt 7 ustawy o Straży Granicznej,
   c) art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej,
   d) art. 31 ust. 1 pkt 17 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
   e) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych”,
   f) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż

wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność",

g) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego
– z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności,

5) Rzecznika Praw Obywatelskich z 27 kwietnia 2012 r. o zbadanie zgodności:
   a) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. Nr 168, poz. 1323, ze zm.) z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji,
   b) art. 75d ust. 5 ustawy o Służbie Celnej z art. 51 ust. 4 Konstytucji,

6) Prokuratora Generalnego z 21 czerwca 2012 r. o zbadanie zgodności:
   a) art. 20c ust. 1 ustawy o Policji w związku z art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.), art. 45, art. 46 ust. 1, art. 49 i art. 49a ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, ze zm.), art. 34 pkt 2, 3 i 4 ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (Dz. U. Nr 92, poz. 881, ze zm.), art. 33 ustawy z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach (Dz. U. Nr 63, poz. 322), art. 77 pkt 2, 2a i 3 ustawy z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2008 r. Nr 213, poz. 1342, ze zm.) i w związku z art. 52 pkt 2 i 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie (Dz. U. z 2005 r. Nr 127, poz. 1066, ze zm.),
   b) art. 10b ust. 1 ustawy o Straży Granicznej w związku z art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 Kodeksu karnego, art. 45, art. 46 ust. 1, art. 49 i art. 49a Prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych i ich mieszaninach, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt i w związku z art. 52 pkt 2 i 4 Prawa łowieckiego,
   c) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych w związku z art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 Kodeksu karnego, art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2007 r. Nr 111, poz. 765, ze zm.), art. 45, art. 46 ust. 1, art. 49 i art. 49a Prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych i ich mieszaninach, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt i w związku z art. 52 pkt 2 i 4 Prawa łowieckiego,

d) art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej w związku z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 Kodeksu karnego skarbowego,
e) art. 36b ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej w związku z art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 Kodeksu karnego skarbowego oraz w związku z art. 100 ust. 1 i art. 101 ust. 1 ustawy z dnia 19 marca 2004 r. – Prawo celne (Dz. U. Nr 68, poz. 622, ze zm.),
f) art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa”,
g) art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b oraz c, jak również pkt 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
h) art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych”,
i) art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność”,
j) art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
k) art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o Centralnym Biurze Antykorupcyjnym w związku z art. 4, art. 12 ust. 3-6, art. 13 oraz art. 15 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, ze zm.),
l) art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o Centralnym Biurze Antykorupcyjnym w związku z art. 8 ust. 1 i 3 oraz art. 10 ust. 1, 2, 5 i 6 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, art. 35 ust. 1 ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2011 r. Nr 7, poz. 29, ze zm.), art. 87 § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070, ze zm.), art. 38 ustawy z dnia 23 listopada 2002 r. o Sądzie Najwyższym (Dz. U. Nr 240, poz. 2052, ze zm.), art. 49a ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r. Nr 270, poz. 1599, ze zm.), art. 24h ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591, ze zm.), art. 25c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592, ze zm.) oraz w związku z art. 27c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 1590, ze zm.),

ł) art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym w związku z art. 1 ust. 1 i 2 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.),

m) art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 4 ustawy o Centralnym Biurze Antykorupcyjnym w związku z art. 200 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz. 759, ze zm.), art. 46 ust. 1, art. 75 ust. 1-4 i art. 110 ust. 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2010 r. Nr 220, poz. 1447, ze zm.) oraz w związku z art. 3 ust. 1, art. 20a ust. 1-3, art. 31a, art. 36 ust. 1, art. 39 ust. 1 i art. 69e ustawy z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji (Dz. U. z 2002 r. Nr 171, poz. 1397, ze zm.),

n) art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o Centralnym Biurze Antykorupcyjnym,

o) art. 75d ust. 1 w związku z ust. 5 ustawy o Służbie Celnej w związku z art. 108 § 2 i art. 109 Kodeksu karnego skarbowego

– z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności,

7) Prokuratora Generalnego z 13 listopada 2012 r. o zbadanie zgodności art. 19 ustawy o Policji, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 17 ustawy o Centralnym Biurze Antykorupcyjnym, art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego z powodu pominięcia w zakwestionowanych przepisach regulacji wyłączającej z kręgu podmiotów, które mogą być poddane kontroli operacyjnej, kategorie osób, od których pozyskanie informacji objętych tajemnicą adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego i lekarską podlega zakazom dowodowym, w zakresie objętym zakazami, z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji, jak również z art. 6 ust. 3 lit. b oraz c, art. 8 i art. 10 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności,

o r z e k a:

I

1)

a) art. 19 ust. 1 pkt 8 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, z 2012 r. poz. 627, 664, 908, 951 i 1529, z 2013 r. poz. 628, 675, 1351, 1635 i 1650 oraz z 2014 r. poz. 24, 486, 502, 538 i 616)**,**

b) art. 9e ust. 1 pkt 7 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675, Nr 117, poz. 677, Nr 170, poz. 1015, Nr 171,

poz. 1016 i Nr 230, poz. 1371, z 2012 r. poz. 627, 664, 769 i 951, z 2013 r. poz. 628, 675, 829, 1351 i 1650 oraz z 2014 r. poz. 486, 502, 616 i 619)**,**

c) art. 36c ust. 1 pkt 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, Nr 53, poz. 273, Nr 230, poz. 1371 i Nr 240, poz. 1439, z 2012 r. poz. 362 i 1544, z 2013 r. poz. 628 i 1145 oraz z 2014 r. poz. 915)**,**

d) art. 31 ust. 1 pkt 17 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 i 628)

– **rozumiane w ten sposób, że dotyczą określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2** (Dz. U. z 1993 r. Nr 61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962, z 2001 r. Nr 23, poz. 266, z 2003 r. Nr 42, poz. 364 oraz z 2010 r. Nr 90, poz. 587)**,**

2) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, Nr 182, poz. 1228 i Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273, Nr 84, poz. 455, Nr 117, poz. 677 i Nr 230, poz. 1371, z 2012 r. poz. 627 i 908, z 2013 r. poz. 628, 675 i 1351 oraz z 2014 r. poz. 502, 544 i 616) **jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji,**

3)

a) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa”,

b) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

c) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253 i 502) **w zakresie, w jakim obejmuje zwrot „a także innych ustawach i umowach międzynarodowych”**

– **są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności,**

4)

a) art. 19 ust. 6 pkt 3 ustawy o Policji,

b) art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej,

c) art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej,

d) art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

e) art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

f) art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie

Wywiadu Wojskowego,

g) art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, 627 i 664, z 2013 r. poz. 628, 675 i 1351 oraz z 2014 r. poz. 502 i 616)

– rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną wskazuje określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji,

5)

a) art. 20c ust. 1 ustawy o Policji,
b) art. 10b ust. 1 ustawy o Straży Granicznej,
c) art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej,
d) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
e) art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
f) art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
g) art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym,
h) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 oraz z 2014 r. poz. 486)

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

6)

a) art. 19 ustawy o Policji,
b) art. 9e ustawy o Straży Granicznej,
c) art. 36c ustawy o kontroli skarbowej,
d) art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
e) art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
f) art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
g) art. 17 ustawy o Centralnym Biurze Antykorupcyjnym

– w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji,

7) art. 36b ust. 5 ustawy o kontroli skarbowej jest zgodny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji,

8)

a) art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
b) art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
c) art. 18 ustawy o Centralnym Biurze Antykorupcyjnym
– w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji,

9) art. 75d ust. 5 ustawy o Służbie Celnej w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, ze zm.)**, jest niezgodny z art. 51 ust. 4 Konstytucji.**

II

Przepisy wymienione w części I w punktach 2, 5, 6 i 8, w zakresach w nich wskazanych, tracą moc obowiązującą z upływem 18 (osiemnastu) miesięcy od dnia ogłoszenia wyroku w Dzienniku Ustaw Rzeczypospolitej Polskiej.

Ponadto p o s t a n a w i a:

na podstawie art. 39 ust. 1 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643, z 2000 r. Nr 48, poz. 552 i Nr 53, poz. 638, z 2001 r. Nr 98, poz. 1070, z 2005 r. Nr 169, poz. 1417, z 2009 r. Nr 56, poz. 459 i Nr 178, poz. 1375, z 2010 r. Nr 182, poz. 1228 i Nr 197, poz. 1307 oraz z 2011 r. Nr 112, poz. 654) **umorzyć postępowanie w pozostałym zakresie.**

UZASADNIENIE

I

1. Stanowisko wnioskodawców.

1.1. We wniosku z 29 czerwca 2011 r. Rzecznik Praw Obywatelskich zakwestionował zgodność art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277, ze zm.; dalej: ustawa o Policji); art. 9e ust. 7 pkt 3 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675; dalej: ustawa o SG); art. 36c ust. 4 pkt 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214; dalej: ustawa o kontroli skarbowej); 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: ustawa o ŻW); art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, ze zm.; dalej: ustawa o ABW); 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: ustawa o CBA); 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: ustawa o SKW) z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

Zaskarżone przepisy, regulujące zasady prowadzenia kontroli operacyjnej przez służby policyjne i ochrony państwa, mają zbliżoną treść normatywną. Zgodnie z nimi, kontrola operacyjna prowadzona jest niejawnie i polega na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych. A w wypadku kontroli operacyjnej prowadzonej przez Straż Graniczną i Żandarmerię Wojskową ustawodawca przewidział dodatkowo możliwość uzyskiwania i utrwalania „obrazu" przez te służby w toku kontroli operacyjnej.

Wnioskodawca zarzucił zakwestionowanym przepisom nadmierną nieprecyzyjność. W jego ocenie, ustawodawca pozostawił otwarty katalog środków technicznych, które mogą być wykorzystywane przez służby w toku kontroli operacyjnej, a także otwarty katalog informacji i dowodów, jakie mogą być pozyskiwane w tej procedurze. Na podstawie zakwestionowanych przepisów służby mogą przez to ingerować w różne sfery prywatności jednostek, nie tylko w tajemnicę komunikowania się i wizerunek jednostki, ale również nienaruszalność mieszkania, wolność poruszania się czy też autonomię informacyjną. W ocenie Rzecznika, ustawodawca – wyznaczając ramy kontroli operacyjnej nie dostrzegł zróżnicowanego poziomu intensywności i zakresu konstytucyjnej ochrony poszczególnych sfer prywatności.

Zdaniem wnioskodawcy, z postanowień ustawy sformułowanych w sposób jasny oraz precyzyjny, powinny wynikać zakres oraz głębokość ingerencji organów władzy publicznej w konstytucyjne wolności i prawa jednostek. Ustawa musi konkretyzować wypadki, zakres, sposoby ingerencji, a także – co istotne – wskazywać, jakich konkretnie sfer życia jednostki ta ingerencja dotyczy. Ustawodawca nie może zatem posługiwać się klauzulami generalnymi i powinien unikać tworzenia otwartych katalogów, jak to uczynił w zaskarżonych przepisach, tym bardziej że kontrola operacyjna prowadzona jest niejawnie. Zakwestionowane przepisy nie spełniają konstytucyjnego standardu wynikającego z art. 47 w związku z art. 31 ust. 3 oraz z art. 2 Konstytucji przez to, że nie określają wszystkich podstawowych elementów regulacji upoważniającej do niejawnej ingerencji państwa w prawo do prywatności, sformułowanych w orzecznictwie Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka, a ponadto – obowiązujące unormowania są nieprecyzyjne. Służby mogą zatem pozyskiwać w rozmaity sposób – jeżeli chodzi o środki techniczne – nie tylko treść rozmów telefonicznych, ale również inne, bliżej niesprecyzowane informacje o jednostce. Ponadto ustawy regulujące kompetencje służb nie uwzględniają wymogu, aby pewne wolności i prawa (jak np. nienaruszalność mieszkania) były chronione intensywniej niż inne (np. tajemnica komunikowania się).

1.2. We wniosku z 1 sierpnia 2011 r. Rzecznik Praw Obywatelskich zakwestionował konstytucyjność dwóch grup przepisów. Na pierwszą grupę składają się: art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW. Mają być one niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962, z

2001 r. Nr 23, poz. 266, z 2003 r. Nr 42, poz. 364 oraz z 2010 r. Nr 90, poz. 587; dalej: Konwencja). Drugą grupę przepisów stanowią z kolei: art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW w zakresie, w jakim – zezwalając na pozyskiwanie 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.; dalej: prawo telekomunikacyjne) – nie przewidują zniszczenia tych spośród pozyskanych danych, które pozbawione są znaczenia dla prowadzonego postępowania. Przepisy te Rzecznik uważa za sprzeczne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

Treść zakwestionowanych przepisów jest zasadniczo zbliżona. Przyznają one służbom policyjnym i służbom ochrony państwa kompetencje pozyskiwania i przetwarzania danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego w celu zapobiegania i wykrywania przestępstw albo realizacji ustawowych zadań służb. Dane wymienione w przepisach prawa telekomunikacyjnego, do których odsyłają zaskarżone przepisy, obejmują: dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego (inicjującego połączenie i do którego kierowane jest połączenie), daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, oraz lokalizacji telekomunikacyjnego urządzenia końcowego. Ponadto służby mają prawo pozyskiwać i przetwarzać dane dotyczące użytkownika wymienione w art. 159 ust. 1 pkt 1, 3-5; art. 161 oraz art. 179 ust. 9 prawa telekomunikacyjnego. Dane te udostępniane są Policji, Straży Granicznej oraz Żandarmerii Wojskowej w celu zapobiegania i wykrywania wszelkich czynów stanowiących przestępstwo. Wywiad skarbowy może pozyskiwać i przetwarzać je w celu zapobiegania i wykrywania przestępstw skarbowych oraz przestępstw, o których mowa w art. 228-231 k.k. popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych, a także naruszeń krajowych i unijnych przepisów celnych. Natomiast funkcjonariuszom CBA, SKW i ABW dane te są udostępniane w celu realizacji wszystkich, bez wyjątku, ustawowych zadań.

Wnioskodawca sformułował kilka zarzutów pod adresem tych regulacji. Po pierwsze, jego zdaniem, w sposób nieprecyzyjny regulują one cel gromadzenia danych przez służby, gdyż odwołują się do zakresu zadań poszczególnych służb bądź ogólnego wymogu, by dane te były pozyskiwane w celu zapobiegania bądź wykrywania przestępstw. Po drugie, ustawodawca nie wyłączył żadnej kategorii podmiotów, których dane mogą być pozyskiwane w tym trybie, choćby były one objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską (art. 180 § 2 k.p.k.). Po trzecie, ustawodawca odstąpił od zasady subsydiarności pozyskiwania tych danych. Obowiązek udostępnienia danych przez operatorów aktualizuje się zawsze, gdy zwrócą się o to upoważnione podmioty, a nie tylko i wyłącznie, kiedy jest to niezbędne dla prowadzonego postępowania, czyli gdy inne dowody są niewystarczające. Po czwarte, zakwestionowane przepisy nie przewidują wymogu uzyskania zgody sądu na pozyskanie danych objętych tajemnicą telekomunikacyjną. W odniesieniu do ABW, CBA, SKW i SWW ustawodawca *expressis verbis* przewidział brak konieczności uzyskania zgody sądu, natomiast w wypadku pozostałych służb – nie ustanowił przepisu, który takowej zgody by wymagał. Ustawodawca nie przewidział ponadto żadnego nadzoru zewnętrznych organów nad sposobem korzystania z uprawnień przyznanych służbom. Po piąte, ustawa o ABW, ustawa o CBA oraz ustawa o SKW w ogóle nie przewidują zniszczenia zgromadzonych materiałów, które nie zawierają informacji mających znaczenie dla postępowania karnego. Z kolei art. 36b ust. 5 ustawy o kontroli skarbowej znacznie zawęża przesłanki niszczenia

danych. W świetle tego przepisu zniszczeniu podlegają tylko te dane, które zebrano w sytuacji niezasadności wniosku o ich zgromadzenie.

Odwołując się do orzecznictwa Europejskiego Trybunału Praw Człowieka (dalej też: ETPC) i Trybunału Konstytucyjnego, Rzecznik zajął stanowisko, w myśl którego z art. 49 Konstytucji oraz art. 8 Konwencji wynika ciążący na państwie obowiązek ochrony danych zawartych w bilingach telefonicznych. Tajemnicą komunikowania objęty jest sam fakt skomunikowania się jednostek oraz miejsce i czas jego trwania. Wnioskodawca zwrócił uwagę na nieokreśloność zakwestionowanych regulacji, które – jako dotykające sfery prywatności jednostki – muszą być kompletnie unormowane w ustawie. Odnosząc się do braku subsydiarności sięgania przez służby po dane telekomunikacyjne, Rzecznik zaznaczył, że narusza to zasadę proporcjonalności określoną w art. 31 ust. 3 Konstytucji, a dokładnie – wymóg konieczności. Pozyskiwanie danych objętych tajemnicą komunikowania się powinno stanowić *ultima ratio* i być dopuszczalne tylko gdy jest to konieczne, a inne środki okazały się nieskuteczne lub nieprzydatne.

1.3. We wniosku z 27 kwietnia 2012 r. Rzecznik Praw Obywatelskich zakwestionował zgodność art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. Nr 168, poz. 1323, ze zm.; dalej: ustawa o SC) z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 75d ust. 5 ustawy o SC z art. 51 ust. 4 Konstytucji.

W odniesieniu do art. 75d ust. 1 tej ustawy wnioskodawca podniósł zarzuty generalnie zbieżne z przywołanymi we wniosku z 1 sierpnia 2011 r. W jego ocenie, przepis ten pozwala organom Służby Celnej ingerować w sferę prywatności oraz tajemnicę komunikowania się w każdym wypadku, gdy pozyskanie danych telekomunikacyjnych służy zapobieganiu lub wykrywaniu przestępstw skarbowych przeciwko organizacji gier hazardowych. Niejawna ingerencja nie odbywa się zatem na zasadzie subsydiarności, a więc wtedy gdy określonych danych nie można pozyskać, wykorzystując mniej dolegliwe dla jednostki środki. Naruszać ma to wymóg proporcjonalności ograniczenia prawa do ochrony prywatności oraz ochrony tajemnicy komunikowania się. Ponadto, zdaniem Rzecznika, zakwestionowany przepis jest niezgodny ze wskazanymi wzorcami kontroli, gdyż nie wymaga uzyskania zgody sądu bądź innego organu spoza segmentu władzy wykonawczej na pozyskanie tych danych przez Służbę Celną. Wymóg taki ma gwarantować przestrzeganie zasady legalności działania tej służby.

Zgodnie z art. 75d ust. 5 ustawy o SC, materiały uzyskane przez służbę celną od podmiotu prowadzącego działalność telekomunikacyjną, niezawierające informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis ten – w ocenie wnioskodawcy – pozwala Służbie Celnej zachować te materiały pozyskane w toku kontroli operacyjnej, które wskazują na popełnienie jakiegokolwiek wykroczenia skarbowego lub przestępstwa skarbowego. Jak argumentuje Rzecznik, Służba Celna na podstawie art. 75d ust. 1 może pozyskiwać oraz przetwarzać dane telekomunikacyjne tylko w celu zapobiegania oraz wykrywania przestępstw przeciwko organizacji gier hazardowych, natomiast zniszczeniu mają podlegać te dane, które nie zawierają informacji mających znaczenie dla postępowania w jakichkolwiek sprawach o wykroczenia skarbowe lub przestępstwa skarbowe. Inny jest cel pozyskiwania danych telekomunikacyjnych, inny zaś ich przechowywania. Zdaniem RPO, wykorzystanie tych danych, zebranych w celu określonym w art. 75d ust. 1, na inne potrzeby narusza art. 51 ust. 4 Konstytucji, gdyż są to dane zebrane w sposób sprzeczny z ustawą.

1.4. Zarządzeniami Prezesa Trybunału Konstytucyjnego z 1 września 2011 r. oraz z 8 maja 2012 r. wnioski te zostały połączone do łącznego rozpoznania.

1.5. We wniosku z 15 listopada 2011 r. Rzecznik Praw Obywatelskich zakwestionował zgodność art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", a także zgodność art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji.

Zdaniem wnioskodawcy, zakwestionowane przepisy nie spełniają wynikającego z art. 2 Konstytucji wymogu określoności prawa i naruszają zasadę proporcjonalności. Posługują się bowiem wyrażeniami niedookreślonymi, takimi jak „innych przestępstw godzących w bezpieczeństwo państwa" czy „przestępstwa godzące w podstawy ekonomiczne państwa". Uniemożliwiają one ustalenie typów przestępstw, których wykrywanie i zapobieganie uzasadnia zastosowanie kontroli operacyjnej. Wyrażenia te nie nawiązują do terminologii z ustaw karnych. Pozostawia to uprawnionym podmiotom zbyt szeroki margines swobody decyzyjnej co od zakresu kontroli operacyjnej, ingerującej w chronione konstytucyjnie prawo do prywatności i tajemnicę komunikowania się. Z brakiem określoności wiąże się również naruszenie zasady proporcjonalności. Zdaniem Rzecznika, skoro ustawodawca nie wskazał precyzyjnie typów przestępstw, co do których ABW została uprawniona do prowadzenia kontroli operacyjnej, to nie jest możliwe precyzyjnie określenie celów kontroli. W istocie określenie granicy ingerencji ABW w sferę prywatności jednostki pozostawiono tej służbie ochrony państwa. Naruszać ma to wymóg proporcjonalnej ingerencji w wolności i prawa jednostek. Z tych samych powodów zakwestionowane przepisy nie spełniają wymogów przewidzianych w Konwencji.

1.6. We wniosku z 7 marca 2012 r. Prokurator Generalny zakwestionował zgodność art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW, art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych", art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

Zakwestionowane przepisy – zdaniem wnioskodawcy – są blankietowe. Nie spełniają wymogu określoności prawa i wymogu ustawowej formy ograniczenia konstytucyjnych wolności i praw. Nie wskazują dokładnie, w jakich sytuacjach może nastąpić ingerencja przez daną służbę w sferę konstytucyjnych wolności oraz praw. Pozostawiają więc służbom policyjnym i służbom ochrony państwa zbyt szeroki margines swobody decydowania o tym, czy i ewentualnie w jakim zakresie można wkroczyć w sferę prywatności jednostek. Katalogi przestępstw przewidziane w przepisach, co do których może być podejmowana kontrola operacyjna, mają charakter otwarty, odwołując się do zobowiązań Polski wynikających z nieskonkretyzowanych umów i porozumień międzynarodowych. Jak się wydaje, ustawodawca upoważnił tym samym służby do podejmowania – w przyszłości – kontroli operacyjnej na podstawie tych aktów prawa międzynarodowego, których Rzeczpospolita Polska jeszcze nie zawarła, a tym samym ich treść nie była znana w czasie uchwalania kwestionowanych ustaw, jak również może nie być znana w chwili obecnej. Wnioskodawca ponadto wskazał na niedopuszczalność

unormowania przesłanek kontroli operacyjnej w innych aktach prawa międzynarodowego niż umowy międzynarodowe ratyfikowane za zgodą wyrażoną uprzednio w ustawie.

Jak podkreślił Prokurator Generalny, w wypadku SKW kontrola operacyjna może być ponadto zarządzona w sytuacji popełnienia przestępstw określonych w przepisach o randze ustawy, które jednak nie zostały dokładnie zdefiniowane. Takie sformułowanie przepisu może sprzyjać arbitralności czynności operacyjno-rozpoznawczych, a przez to rodzić niepewność jednostek co do przysługujących im praw i obowiązków. Z tych samych powodów naruszony został art. 8 Konwencji.

1.7. We wniosku z 21 czerwca 2012 r. Prokurator Generalny zakwestionował zgodność z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji następujących przepisów:

- art. 20c ust. 1 ustawy o Policji w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.; dalej: k.k.), art. 45, art. 46 ust. 1, art. 49 i art. 49a ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, ze zm.; dalej: prawo prasowe); z art. 34 pkt 2, 3 i 4 ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (Dz. U. Nr 92, poz. 881, ze zm.; dalej: ustawa o wyrobach budowlanych), art. 33 ustawy z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach (Dz. U. Nr 63, poz. 322; dalej: ustawa o substancjach chemicznych), art. 77 pkt 2, 2a i 3 ustawy z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2008 r. Nr 213, poz. 1342, ze zm.; dalej: ustawa o ochronie zdrowia zwierząt) i w związku z art. 52 pkt 2 i 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie (Dz. U. z 2005 r. Nr 127, poz. 1066, ze zm.; dalej: prawo łowieckie);
- art. 10b ust. 1 ustawy o SG w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt i w związku z art. 52 pkt 2 i 4 prawa łowieckiego;
- art. 30 ust. 1 ustawy o ŻW w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2007 r. Nr 111, poz. 765, ze zm.; dalej: k.k.s.), art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, z art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt i w związku z art. 52 pkt 2 i 4 prawa łowieckiego;
- art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej w związku z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 k.k.s.;
- art. 36b ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej, w związku z art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 k.k.s. oraz w związku z art. 100 ust. 1 i art. 101 ust. 1 ustawy z dnia 19 marca 2004 r. – Prawo celne (Dz. U. Nr 68, poz. 622, ze zm.; dalej: prawo celne);
- art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa”;

- art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b oraz c, jak również pkt 5 ustawy o ABW;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych”;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „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”;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW;
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o CBA w związku z art. 4, art. 12 ust. 3-6, art. 13 oraz art. 15 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, ze zm.; dalej: ustawa o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne);
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA w związku z art. 8 ust. 1 i 3 oraz art. 10 ust. 1, 2, 5 i 6 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, z art. 35 ust. 1 ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2011 r. Nr 7, poz. 29, ze zm.; dalej: ustawa o wykonywaniu mandatu), z art. 87 § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070, ze zm.; dalej: p.u.s.p.), z art. 38 ustawy z dnia 23 listopada 2002 r. o Sądzie Najwyższym (Dz. U. Nr 240, poz. 2052, ze zm.; dalej: ustawa o SN), z art. 49a ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r. Nr 270, poz. 1599, ze zm.; dalej: ustawa o prokuraturze), z art. 24h ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591, ze zm.; dalej: u.s.g.), z art. 25c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592, ze zm.; dalej: u.s.p.) oraz w związku z art. 27c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 1590, ze zm.; dalej: u.s.w.);
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o CBA w związku z art. 1 ust. 1 i 2 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.; dalej: ustawa o zwrocie korzyści);
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 4 ustawy o CBA w związku z art. 200 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz. 759, ze zm.; dalej: u.p.z.p.), art. 46 ust. 1, art. 75 ust. 1-4 i art. 110 ust. 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2010 r. Nr 220, poz. 1447, ze zm.; dalej: u.s.d.g.) oraz w związku z art. 3 ust. 1, art. 20a ust. 1-3, art. 3la, art. 36 ust. 1, art. 39 ust. 1 i art. 69e ustawy z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji (Dz. U. z 2002 r. Nr 171, poz. 1397, ze zm.; dalej: ustawa o komercjalizacji);
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o CBA;
- art. 75d ust. 1 w związku z ust. 5 ustawy o SC w związku z art. 108 § 2 i art. 109 k.k.s.

Wnioskodawca powtórzył wiele argumentów zawartych we wniosku z 7 marca 2012 r. Podkreślił konieczność precyzyjnej oraz kompletnej ustawowej regulacji ograniczeń praw i wolności konstytucyjnych, a także zwrócił uwagę na doniosłość konstytucyjnego prawa do prywatności.

Zakwestionowane regulacje uprawniają służby policyjne i ochrony państwa do gromadzenia i przetwarzania danych telekomunikacyjnych osób podejrzewanych o popełnienie drobnych przestępstw o niskiej społecznej szkodliwości, dopuszczających się

naruszeń prawa celnego niebędących przestępstwami skarbowymi, ani nawet wykroczeniami skarbowymi, przewinień służbowych bądź zachowań będących podstawą do zastosowania sankcji administracyjnej i dyscyplinarnej. W związku z tym mają stanowić nieproporcjonalną ingerencję w konstytucyjnie chroniony status jednostki. Czyny tego rodzaju nie uzasadniają, w ocenie wnioskodawcy, ograniczenia prawa do prywatności i tajemnicy komunikowania się. Nie tylko nie są koniecznymi ograniczeniami, ale wręcz pozyskiwanie danych tego rodzaju w ogóle nie służy zapobieganiu lub wykrywaniu przestępstw, wykroczeń lub innych naruszeń prawa. Nie spełniają zatem wymogu adekwatności wynikającego z zasady proporcjonalności (art. 31 ust. 3 Konstytucji). Powyższych wymogów nie spełniają również unormowania określające uprawnienia funkcjonariuszy CBA dotyczące pozyskiwania danych telekomunikacyjnych w toku kontroli rzetelności i prawdziwości oświadczeń majątkowych, oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne oraz uczestników postępowań o udzielenie zamówienia publicznego czy procesu komercjalizacji i prywatyzacji, zwłaszcza gdy nie ma przesłanek wskazujących na popełnienie jakiegokolwiek przestępstwa przez te osoby.

Zakwestionowane przepisy naruszać mają także zasadę określoności prawa. Jednostka nie otrzymuje na podstawie lektury przepisów ustawowych nawet ogólnej wskazówki, w jakim akcie normatywnym powinna poszukiwać określenia sytuacji prawnej, w której służby są uprawnione do wkroczenia w jej konstytucyjnie chronioną sferę praw i wolności, poprzez pozyskanie danych telekomunikacyjnych. Wynika to również w pewnym stopniu z otwartego katalogu przestępstw, których wykrywanie oraz ściganie umożliwia udostępnienie służbom danych telekomunikacyjnych, i braku jakiejkolwiek kontroli zewnętrznej działalności służb w tym zakresie. Powyższe argumenty przemawiać mają za niezgodnością zaskarżonych przepisów m.in. z art. 8 Konwencji.

1.8. Zarządzeniem Prezesa Trybunału Konstytucyjnego z 5 lipca 2012 r. wniosek Rzecznika Praw Obywatelskich z 15 listopada 2011 r. oraz wnioski Prokuratora Generalnego z 7 marca 2012 r. i 21 czerwca 2012 r. zostały połączone do łącznego rozpoznania pod sygn. K 23/11.

1.9. We wniosku z 13 listopada 2012 r. Prokurator Generalny zakwestionował zgodność art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA, art. 31 ustawy o SKW z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji, jak również z art. 6 ust. 3 lit. b oraz c, art. 8 i art. 10 ust. 1 Konwencji z powodu niewyłączenia z kręgu poddanych kontroli operacyjnej osób, od których pozyskiwanie informacji objętych tajemnicą adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego lub lekarską podlega zakazom dowodowym – w zakresie objętym tymi zakazami.

Zdaniem wnioskodawcy, ustawodawca nie wytyczył prawidłowo granic czynności operacyjno-rozpoznawczych w odniesieniu do sfery objętej zakazami dowodowymi, które są przewidziane w procesie karnym. Zaskarżone przepisy nie wyłączają bowiem żadnej kategorii podmiotów z kręgu potencjalnie poddanych kontroli operacyjnej. Jeśli Kodeks postępowania karnego istotnie ogranicza procesowe wykorzystanie materiałów zawierających informacje objęte tajemnicą obrończą, adwokacką, notarialną, radcy prawnego, doradcy podatkowego, lekarską bądź dziennikarską, to już samo pozyskanie tych informacji przez służby policyjne i służby ochrony państwa nie może być uznane za konieczne w demokratycznym państwie. Nie

jest przy tym wystarczające unormowanie obligujące do niszczenia zgromadzonych materiałów, które są zbędne lub niedopuszczalne. Jak wynika z uzasadnienia wniosku, jedynym unormowaniem akceptowanym konstytucyjnie byłoby zupełne wyłączenie tej kategorii osób spod czynności operacyjno-rozpoznawczych, w zakresie objętym zakazami dowodowymi.

Szczególnych gwarancji wymaga tajemnica obrończa oraz tajemnica dziennikarska. Uzasadniając to stanowisko, Prokurator Generalny wskazał na znaczenie tajemnicy obrończej dla prawidłowego toku postępowania karnego, a zwłaszcza dla realizacji prawa oskarżonego do obrony, którego treścią jest poufność kontaktów z obrońcą. Skoro ustawodawca zapewnił daleko idące gwarancje tajemnicy obrończej w procesie karnym, zakazując przesłuchiwania obrońcy o faktach poznanych podczas udzielania porady prawnej lub prowadzenia sprawy, to możliwość niejawnego uzyskiwania informacji w toku kontroli operacyjnej w zakresie objętym tą tajemnicą, sama przez się, narusza prawo do obrony. Wnioskodawca zwrócił także uwagę na znaczenie tajemnicy dziennikarskiej w demokratycznym państwie prawa. Mając na uwadze orzecznictwo TK i ETPC oraz obowiązujące unormowania procesu karnego i prawa prasowego, Prokurator Generalny wskazał, że skoro zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację jego źródła informacji, zaś ujawnienie przez dziennikarza danych jego informatorów jest przestępstwem, to w takiej sytuacji nie sposób zaakceptować dopuszczalności ustalenia danych osobowych takich informatorów przez służby w drodze kontroli operacyjnej.

2. Stanowiska uczestników postępowania.

2.1. W pismach z 2 marca, 15 czerwca, 30 sierpnia, 30 października 2012 r. oraz z 13 maja 2013 r. stanowisko w imieniu Sejmu zajął Marszałek Sejmu.

2.1.1. Odnosząc się do wniosków Rzecznika Praw Obywatelskich z 29 czerwca i 1 sierpnia 2011 r., wniósł on o stwierdzenie, że :

- art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy z o CBA, art. 31 ust. 4 pkt 3 ustawy o SKW są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.
- art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW są niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.
- art. 28 ustawy o ABW, art. 18 ustawy o CBA, art. 32 ustawy o SKW 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, a 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.

Ponadto Marszałek Sejmu wniósł o umorzenie postępowania 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. Wskazał, że przepis ten był już przedmiotem kontroli Trybunału, który w wyroku z 20 czerwca 2005 r.

(sygn. K 4/04) uznał, że 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 brzmienie art. 36c ust. 1 i 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. Zdaniem Marszałka Sejmu, zarówno przedmiot kontroli, jak i powołane przez wnioskodawców wzorce oraz zarzuty i argumenty w obydwu sprawach są tożsame. Aktualizuje się zatem zakaz *ne bis in idem*, uniemożliwiający dwukrotne orzekanie w tej samej sprawie.

Zdaniem Marszałka Sejmu, wyrok w sprawie o sygn. K 4/04 istotnie rzutuje na ocenę konstytucyjności pozostałych zarzutów co do art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy z o CBA i art. 31 ust. 4 pkt 3 ustawy o SKW. Mają one niemal tożsamą treść normatywną z art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, uznanym za zgodny z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji. W związku z tym odnośnie do powyższych przepisów Marszałek Sejmu wniósł o orzeczenie ich zgodności z powołanymi wzorcami kontroli.

Według Marszałka Sejmu, samo istnienie niejawnej kontroli prowadzonej przez służby ochrony państwa, ingerującej w prawo do prywatności i autonomię informacyjną jednostki, ma istotne znaczenie z perspektywy m.in. zapewnienia bezpieczeństwa państwa i porządku publicznego. Kontrola sprawowana na podstawie przepisów zaskarżonych przez Rzecznika nie może być prowadzona dowolnie. Po pierwsze, może być stosowana przez ściśle określone służby w ramach realizacji ich ustawowych zadań. Po drugie, stosowanie kontroli operacyjnej dopuszczalne jest w określonych ustawowo sytuacjach oraz dla realizacji określonych celów. Po trzecie, opiera się ona na zasadzie subsydiarności, a zatem może być zastosowana dopiero, gdy inne środki okazały się bezskuteczne lub nieprzydatne. Po czwarte, podlega kontroli sądowej w postaci zgody pierwotnej bądź następczej, w ustawowo unormowanej procedurze. Po piąte, kontrola operacyjna jest limitowana czasowo, choć z możliwością jej przedłużenia. Po szóste, przepisy nie pozwalają służbom na niekontrolowane wykorzystanie dowodów uzyskanych w toku kontroli operacyjnej. Wykorzystanie dowodu uzyskanego w ten sposób możliwe jest w innej sprawie, niemniej jednak pod warunkiem, że uzyskano dowód popełnienia przestępstwa lub przestępstwa skarbowego, w stosunku do którego można zarządzić kontrolę operacyjną (tj. przestępstwa katalogowego). Zgodę na jego wykorzystanie wyraża sąd, który zarządził kontrolę lub wyraził na nią zgodę. Po siódme, przepisy przewidują obowiązek niezwłocznego i komisyjnego zniszczenia materiałów, które nie zawierają dowodów pozwalających na wszczęcie postępowania karnego bądź też nie mają znaczenia dla toczącego się postępowania karnego. Marszałek Sejmu zwrócił uwagę na dość restrykcyjne orzecznictwo sądowe, w tym Sądu Najwyższego, dotyczące przepisów o kontroli operacyjnej, wyznaczające wąskie ramy dla służb prowadzących kontrolę operacyjną. W jego ocenie, nie można podzielić zarzutu RPO, że w kontroli operacyjnej można pozyskać każdy dowód o jednostce. Mogą być bowiem pozyskane jedynie dowody, które służą zapobieganiu albo wykrywaniu ustawowo określonych ustawowo typów przestępstw. Marszałek Sejmu nie podzielił też zarzutu braku precyzyjnego ustawowego unormowania środków technicznych. Przede wszystkim przepisy te nie pozwalają w toku kontroli operacyjnej stosować wszelkich metod kontroli, lecz tylko środki techniczne. Ponadto ustawowe określenie katalogu środków kontroli operacyjnej, ze względu na wielość dostępnych środków technicznych, prowadziłoby do zaprzeczenia abstrakcyjnemu i generalnemu charakterowi normy prawnej.

Marszałek Sejmu nie podzielił również zarzutu braku dostatecznego określenia przez ustawodawcę, w jakie dobra konstytucyjnie chronione mogą ingerować służby. Bezprawna działalność może być bowiem związania niemal z każdą sferą prywatności, w tym również życiem seksualnym, stanem zdrowia czy majątkiem, co wymaga, by i w tych newralgicznych sferach służby mogły skutecznie wykonywać swe ustawowe kompetencje.

Odnosząc się do przepisów regulujących dostęp do danych telekomunikacyjnych, Marszałek Sejmu podzielił stanowisko wnioskodawcy. Zakwestionowane regulacje określają w sposób bardzo szeroki dostęp do tych danych przez poszczególne służby. Nie odpowiada to konstytucyjnym oraz konwencyjnym wymogom określoności i precyzyjności unormowania wkraczającego w sferę objętą tajemnicą komunikowania się czy prawem do prywatności. Ustawodawca powinien był precyzyjnie określić charakter przestępstw, w ściganiu których dopuszczalne jest stosowanie kontroli operacyjnej, wprowadzić wymóg uzyskania uprzedniej zgody sądu na pozyskanie danych, wprowadzić przepisy respektujące tajemnicę zawodową. Zakwestionowane przepisy tych wymogów nie spełniają. Marszałek Sejmu podzielił ponadto zarzut wnioskodawcy co do niespełnienia wymogu subsydiarności tych środków.

Odnosząc się do zarzutu braku regulacji nakazującej zniszczenie danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, Marszałek Sejmu podzielił zarzuty wnioskodawcy w odniesieniu do części zaskarżonych przepisów. Jak podkreślił, ingerencją w prawo do prywatności jest również sam fakt przechowywania przez służby informacji o jednostce. Zniszczenie zgromadzonych danych, które są zbędne z punktu widzenia prowadzonego postępowania, zapobiega ich nieuprawnionemu wykorzystaniu. Mając powyższe na uwadze, art. 28 ustawy o ABW, art. 18 ustawy o CBA, art. 32 ustawy o SKW 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. Natomiast zarzut niekonstytucyjności art. 36b ust. 5 ustawy o kontroli skarbowej jest oczywiście chybiony. W innej bowiem jednostce redakcyjnej ustawy – w art. 36d ust. 3 – ustawodawca przewidział, że materiały uzyskane w toku kontroli, które nie zawierają dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe lub niemające znaczenia dla postępowania kontrolnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Marszałek Sejmu wniósł dodatkowo, w sytuacji orzeczenia o niekonstytucyjności zaskarżonych przepisów, o odroczenie terminu utraty ich mocy obowiązującej o 18 miesięcy.

2.1.2. Odnosząc się do wniosku Rzecznika Praw Obywatelskich z 15 listopada 2011 r., Marszałek Sejmu wniósł o stwierdzenie niezgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa”, oraz art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 ust. 1 Konwencji.

W ocenie Marszałka Sejmu, zakwestionowane przepisy nie spełniają konstytucyjnego standardu określoności przepisów upoważniających do niejawnego wkroczenia w prywatność i tajemnicę komunikowania się. W art. 5 ust. 1 pkt 2 lit a, b i c nie wskazano konkretnych typów przestępstw upoważniających do zarządzenia kontroli operacyjnej w trybie art. 27 ust. 1 ustawy o ABW. Taki stan rzeczy stwarza ponadto ryzyko niecelowej lub nieuzasadnionej ingerencji w prywatność jednostki.

Marszałek Sejmu zwrócił też uwagę na wskazania w postanowieniu sygnalizacyjnym TK z 15 listopada 2010 r. (sygn. S 4/10), które nie zostały dotąd wykonane. Krytycznie odniósł się do sformułowanego tam wymogu wskazania w ustawie „typów przestępstw", w odniesieniu do których dopuszczalna jest kontrola operacyjna. Podkreślił mianowicie, że dotychczas Trybunał nie stawiał tak wysokich wymagań odnośnie do regulacji czynności operacyjno-rozpoznawczych. Zdaniem Marszałka Sejmu, Trybunał Konstytucyjny, wymagając określenia „typów przestępstw" uzasadniających stosowanie kontroli operacyjnej, odrzucił znaną prawu represyjnemu metodę konstruowania przepisów, polegającą na oznaczeniu katalogu czynów przestępnych nie przez wyliczenie numerów artykułów albo nazw przestępstw – jak to rozumie Sejm – ale prawnie chronionych dóbr.

Marszałek Sejmu nie zgodził się z twierdzeniem wnioskodawcy, jakoby zaskarżone przepisy skutkowały zbyt szerokim marginesem swobody organów egzekutywy, a zwłaszcza umożliwiały ABW samodzielne określenie, jak głęboko zaingeruje w sferę prywatności jednostki i tajemnicy komunikowania się. Zarządzenie kontroli operacyjnej następuje bowiem na wniosek Szefa ABW, który musi uzyskać pisemną zgodę Prokuratora Generalnego, zaś w ostatecznym rozrachunku kontrolę tę zarządza sąd. Każdy z tych organów jest uprawniony i zobowiązany weryfikować, czy w konkretnym wypadku spełnione są ustawowe przesłanki zarządzenia kontroli operacyjnej.

2.1.3. Odnosząc się do wniosku Prokuratora Generalnego z 7 marca 2012 r., Marszałek Sejmu wniósł o stwierdzenie niezgodności wszystkich zakwestionowanych przepisów z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

Zakwestionowane przepisy regulujące kontrolę operacyjną nie spełniają, zdaniem Marszałka Sejmu, konstytucyjnego standardu określoności regulacji upoważniających do niejawnego wkroczenia w prywatność oraz w wolność komunikowania się. Ustawodawca – wbrew wymogom skonkretyzowanym w dotychczasowym orzecznictwie TK – nie wskazał typów przestępstw, którym zapobieganie oraz których rozpoznawanie i wykrywanie upoważnia do zarządzenia kontroli operacyjnej. Trudno jest zwłaszcza ustalić, jakie przestępstwa kryją się pod pojęciem „przestępstw ściganych na mocy umów i porozumień międzynarodowych", zważywszy, że nie określono, czy pod pojęciem umów i porozumień międzynarodowych mają się mieścić wszystkie tego rodzaju akty normatywne, bez względu nawet na to, czy zostały w ogóle ratyfikowane. Nieprecyzyjność zakwestionowanych regulacji, pozwalająca na prowadzenie kontroli operacyjnej w wypadkach bliżej nieokreślonych przestępstw, rodzi ponadto niebezpieczeństwo niecelowej i nieuzasadnionej ingerencji w sferę prywatności i tajemnicę komunikowania się. Marszałek Sejmu wyraził swoje wątpliwości i sugestie co do zasadności podniesienia przez TK standardu konstytucyjnego, jaki powinny spełniać przepisy regulujące kontrolę operacyjną.

2.1.4. Odnosząc się do wniosku Prokuratora Generalnego z 21 czerwca 2012 r., Marszałek Sejmu wniósł o stwierdzenie, że:

- art. 20c ust. 1 ustawy o Policji w związku z art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt, art. 52 pkt 2 i 4 prawa łowieckiego, jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 10b ust. 1 ustawy o SG w związku z art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy

substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt, art. 52 pkt 2 i 4 prawa łowieckiego, jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

- art. 30 ust. 1 ustawy o ŻW w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 95 § 1 oraz art. 109 k.k.s., art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt, art. 52 pkt 2 i 4 prawa łowieckiego, jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej w związku z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 95 § 1 oraz art. 109 k.k.s., jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 36b ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej, w związku z art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 k.k.s., jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b i c oraz pkt 5 ustawy o ABW, jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych", jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o CBA w związku z art. 4, art. 12 ust. 3-6, art. 13 i art. 15 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA w związku z art. 8 ust. 1 i 3 oraz art. 10 ust. 1, 2, 5 i 6 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, art. 35 ust. 1 ustawy o wykonywaniu mandatu, art. 87 § 1 p.u.s.p., art. 38 ustawy o SN, z art. 49a ust. 1 ustawy o prokuraturze, art. 24h ust. 1 u.s.g., art. 25c ust. 1 u.s.p., art. 27c ust. 1 u.s.w. jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o CBA w związku z art. 1 ust. 1 i 2 ustawy o zwrocie korzyści jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 4 ustawy o CBA w związku z art. 200 u.p.z.p., art. 46 ust. 1, art. 75 ust. 1-4 i art. 110 ust. 1 u.s.d.g., art. 3 ust. 1, art. 20a ust. 1-3, art. 31a, art. 36 ust. 1, art. 39 ust. 1 i art. 69e ustawy ustawa o komercjalizacji jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o CBA jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 75d ust. 1 w związku z ust. 5 ustawy o SC w związku z art. 109 k.k.s. jest zgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

W pozostałym zakresie Marszałek Sejmu wniósł o umorzenie postępowania z uwagi na utratę mocy obowiązującej art. 46 ust. 1 prawa prasowego, powołanego przez Prokuratora Generalnego jako jeden z przepisów związkowych. Wniósł też o umorzenie postępowania z uwagi na niedopuszczalność orzekania, w związku z brakiem dostatecznego uzasadnienia zarzutu niekonstytucyjności powołanych przepisów ustaw regulujących gromadzenie danych telekomunikacyjnych przez służby w odniesieniu do niektórych, wskazanych jako związkowe przepisów (art. 221 k.k., art. 45 prawa prasowego). Ponadto, w ocenie Marszałka Sejmu, wnioskodawca nie wyjaśnił zarzutu naruszenia art. 2 Konstytucji przez przepisy wymienione w pkt 1-5, 11-14 i 16 *petitum* wniosku. Z tego też względu w tym zakresie postępowanie musi być umorzone.

Zdaniem Marszałka Sejmu, Prokurator Generalny chciałby w istocie wkroczyć w materię zastrzeżoną dla ustawodawcy. Jego zamierzeniem zdaje się być współkształtowanie katalogu czynów zabronionych, którym zapobieganie oraz których wykrywanie lub ściganie upoważnia do pozyskiwania danych telekomunikacyjnych.

Odnosząc się do *meritum*, Marszałek Sejmu nie podzielił zarzutu Prokuratora Generalnego, jakoby dopuszczalność udostępniania służbom danych telekomunikacyjnych w wypadku przestępstw ściganych w trybie prywatnoskargowym lub wnioskowym była nieproporcjonalna. W interesie państwa i społeczeństwa leży penalizacja takich czynów, a co za tym idzie służby muszą dysponować efektywnym instrumentem, pozwalającym skutecznie ścigać ich sprawców.

Marszałek Sejmu nie zgodził się również z zarzutami wnioskodawcy dotyczącymi dopuszczalności pozyskiwania danych telekomunikacyjnych w odniesieniu do przestępstw stypizowanych w art. 278, art. 284, art. 288 oraz art. 290 k.k. W jego ocenie, argumentacja wnioskodawcy jest nietrafna, gdyż opiera się na bardzo kazuistycznej analizie charakteru tych przestępstw, ograniczającej się w dodatku do sytuacji granicznych.

Marszałek Sejmu nie podzielił również zarzutów dotyczących niedopuszczalności pozyskiwania danych telekomunikacyjnych odnośnie do przestępstw stypizowanych w innych ustawach niż Kodeks karny lub Kodeks karny skarbowy. Nie można bowiem zakładać, że przestępstwa nieujęte wprost w ustawach *stricte* karnych są mniej społecznie niebezpieczne, niż przestępstwa unormowane w kodeksach. Ponadto nie ma żadnych uzasadnionych podstaw do stwierdzenia, jakoby świadomość prawna jednostek o penalizacji określonych zachowań była większa w wypadku unormowania tego w kodeksach niż w innych ustawach karnych.

Marszałek Sejmu nie zgodził się również z zarzutem wnioskodawcy dotyczącym pozyskiwania danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego w odniesieniu do czynów zabronionych – uznanych przez Prokuratora Generalnego za czyny „mniejszej wagi" – które określono w art. 60, art. 61, art. 62, art. 80 oraz w art. 95 k.k.s. Argumentacja wnioskodawcy skoncentrowana jest bowiem w istocie na potencjalnych błędach w stosowaniu tych przepisów przez organy władzy publicznej i nieuzasadnionym korzystaniu z danych telekomunikacyjnych.

Podobnie Marszałek Sejmu nie podzielił zarzutów dotyczących niedopuszczalności pozyskiwania danych telekomunikacyjnych w celu ścigania oraz wykrywania wykroczeń

skarbowych unormowanych w art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 k.k.s. Zdaniem Marszałka Sejmu, różnice między przestępstwami skarbowymi a wykroczeniami skarbowymi – wbrew tezom wnioskodawcy – zacierają się, przez co nie sposób mówić, że wykroczenia skarbowe są w każdym wypadku mniejszej wagi aniżeli przestępstwa skarbowe. W konsekwencji w pełni uzasadnione jest utrzymanie kompetencji służb policyjnych i ochrony państwa w zakresie dostępu do danych telekomunikacyjnych w odniesieniu do wyżej wskazanych przepisów k.k.s., które stanowią wykroczenia skarbowe.

Zdaniem Marszałka Sejmu, przepisy zakwestionowane w pkt 6-10 *petitum* wniosku Prokuratora Generalnego z 21 czerwca 2012 r. nie spełniają standardu określoności prawa, wymaganego od regulacji umożliwiających niejawną ingerencję w status jednostki. Argumenty powołane przez Marszałka Sejmu w tym zakresie są zbieżne z podniesionymi przez niego w stanowisku dotyczącym kontroli operacyjnej (zob. cz. I, pkt 2.1.1 uzasadnienia). Z odmienną oceną spotkały się zarzuty sformułowane w punktach 11-14 *petitum*, dotyczące ustawy o CBA. W ocenie Marszałka Sejmu, pozyskiwanie danych telekomunikacyjnych w celu ujawniania i przeciwdziałania przypadkom nieprzestrzegania ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, kontroli oświadczeń majątkowych takich osób, wykrywania wypadków uszczupleń należności publicznoprawnych, a ponadto na przykład podejmowania oraz realizacji decyzji dotyczących prywatyzacji, komercjalizacji, wsparcia finansowego, zamówień publicznych, rozporządzania mieniem publicznym, spełnia wymagania konstytucyjne. Dotyczy bowiem sytuacji, które mogą godzić w bezpieczeństwo publiczne czy dobrobyt gospodarczy kraju. Nie spełnia natomiast wymagań konstytucyjnych pozyskiwanie danych telekomunikacyjnych w związku z działalnością analityczną, jak również pozyskiwanie tychże danych w celach określonych w innych ustawach i umowach międzynarodowych.

2.1.5. W piśmie z 13 maja 2013 r. Marszałek Sejmu zajął stanowisko w odniesieniu do wniosku Prokuratora Generalnego z 13 listopada 2012 r. Wskazał on na konieczność umorzenia postępowania w zakresie badania zgodności zakwestionowanych przepisów z art. 2 i art. 54 ust. 1 Konstytucji oraz z art. 8 Konwencji z uwagi na niedopuszczalność wydania wyroku. Wnioskodawca nie uzasadnił bowiem zarzutu naruszenia przez zaskarżone przepisy powyższych wzorców kontroli.

Z kolei w wypadku wniosku o stwierdzenie niezgodności art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA i art. 31 ustawy o SKW z art. 47, art. 49 oraz art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, zdaniem Marszałka Sejmu, zarzuty zostały uzasadnione bardzo ogólnie, a sama argumentacja koncentruje się na ingerencyjnym charakterze kontroli operacyjnej, jako takiej, nie zaś na pominięciu prawodawczym, które w istocie kwestionuje wnioskodawca. Ponadto zasadnicza część argumentacji zdaje się świadczyć o tym, że wnioskodawca chce zainicjować badanie poziomej zgodności ustaw regulujących kontrolę operacyjną z przepisami k.p.k. dotyczącymi zakazów dowodowych i chronionych ustawowo tajemnic zawodowych. Prokurator Generalny ujmuje wartość, jaką jest tajemnica zawodowa, niejako autonomicznie, bez wykazywania jej ściślejszych związków z konkretnymi wolnościami i prawami jednostki. Nie sposób jednak uznać, by tajemnica zawodowa byłą wartością samoistną. W szczególności nie można konstruować swoistego prawa do ochrony tajemnicy zawodowej przysługującego przedstawicielom określonych profesji. Ewentualna ocena konstytucyjności zaskarżonych unormowań może być przeprowadzona tylko z perspektywy konstytucyjnych wolności i praw przysługujących osobom korzystającym z usług wykonujących zawody zaufania

publicznego. W konkluzji Marszałek Sejmu dostrzegł konieczność umorzenia postępowania w powyższym zakresie z uwagi na niedopuszczalność wydania wyroku.

Zakwestionowane przepisy mogą podlegać merytorycznej kontroli tylko z art. 42 ust. 2 Konstytucji oraz z art. 6 ust. 3 lit. b i c Konwencji w kontekście tajemnicy obrończej oraz art. 10 Konwencji w kontekście tajemnicy dziennikarskiej.

Zdaniem Marszałka Sejmu, umożliwienie służbom policyjnym oraz służbom ochrony państwa zapoznania się, w drodze kontroli operacyjnej, z komunikatami objętymi tajemnicą obrończą stanowi poważną ingerencję w prawo do obrony. Mając zaś na uwadze, że poufny kontakt oskarżonego z obrońcą służy przede wszystkim ustaleniu jak najskuteczniejszej linii obrony, to pozyskanie wiedzy o treści przekazywanych informacji, a nawet sama świadomość istnienia takiej możliwości, może niweczyć cele tego prawa, czyniąc je iluzorycznym.

W ocenie Marszałka Sejmu, obowiązujące przepisy nie zapewniają efektywnej ochrony poufności kontaktów oskarżonego z obrońcą. Nie wynika z nich obowiązek niszczenia takich materiałów zebranych w trakcie kontroli operacyjnej, które obejmują treści objęte tajemnicą obrończą. Ponadto wykluczenie możliwości wykorzystania zgromadzonych materiałów jako dowodu w procesie karnym nie stoi na przeszkodzie ich wykorzystaniu w innych sprawach. To znaczy, że obowiązujące unormowania nie chronią w wystarczającym stopniu prawa do obrony. Choć zakwestionowane przepisy wprost nie gwarantują poufności relacji obrończej, to w orzecznictwie sądowym wykształciła się linia orzecznicza eksponująca bezwzględny zakaz wkraczania w poufność stosunku obrończego w postępowaniu karnym. Zasługuje ona na aprobatę. Podniesione przez wnioskodawcę zastrzeżenia natury konstytucyjnej mogą więc zostać usunięte w związku z tym przez wykładnię tych przepisów w zgodzie z Konstytucją. Z tego powodu jest w pełni usprawiedliwione wydanie wyroku afirmatywnego, który wzmocni kształtującą się linię orzeczniczą.

W ocenie Marszałka Sejmu, intencją wnioskodawcy było zakwestionowanie przepisów regulujących kontrolę operacyjną również w odniesieniu do tajemnicy dziennikarskiej, jednak tylko w zakresie ochrony dziennikarskich źródeł informacji. Akcentując znaczenie ochrony tajemnicy zawodowej dziennikarza, dostrzeżono brak dostatecznych gwarancji jej ochrony w powyższym zakresie, zwłaszcza przed pozyskiwaniem informacji w toku czynności pozaprocesowych. Jednakże możliwe jest, zdaniem Marszałka Sejmu, podobnie jak w odniesieniu do tajemnicy obrończej, wyprowadzenie adekwatnych gwarancji poufności w drodze wykładni zakwestionowanych unormowań w zgodzie z Konstytucją. W związku z tym wniesiono o stwierdzenie, że art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA i art. 31 ustawy o SKW, rozumiane w ten sposób, że nie jest dopuszczalna kontrola operacyjna dziennikarskich przekazów informacji w zakresie, w jakim pozwala na identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowana, jeżeli osoby te zastrzegły nieujawnienie powyższych danych z wyjątkiem sytuacji gdy informacja dotyczy przestępstwa, o którym mowa w art. 240 § 1 k.k., są zgodne z art. 10 ust. 1 Konwencji.

2.2. W pismach z 28 października 2011 r., 6 lutego i 11 czerwca 2012 r. stanowisko w sprawie wniosków Rzecznika Praw Obywatelskich z 29 czerwca, 1 sierpnia i 15 listopada 2011 r. oraz 27 kwietnia 2012 r. zajął Prokurator Generalny.

2.2.1. Odnosząc się do wniosków Rzecznika Praw Obywatelskich z 29 czerwca i 1 sierpnia 2011 r., wniósł o stwierdzenie, że

– art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3

ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA, art. 31 ust. 4 pkt 3 ustawy o SKW są niezgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji;

- art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW są niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;
- art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW, art. 18 ustawy o CBA, art. 32 ustawy o SKW 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.

Prokurator Generalny podzielił stanowisko wnioskodawcy odnośnie do naruszenia przez zakwestionowane przepisy wskazanych wzorców konstytucyjnych. Podkreślił on, że stosowanie kontroli operacyjnej przez służby policyjne i służby ochrony państwa stanowi zawsze głęboką ingerencję w prawo do prywatności, wolność komunikowania się, a ponadto w autonomię informacyjną i nienaruszalność mieszkania. Tym samym regulacje dotyczące wkraczania w powyższe dobra muszą odpowiadać szczególnie surowym standardom, zważywszy, że czynności operacyjno-rozpoznawcze mają charakter niejawny. W przeciwieństwie zatem do czynności procesowych trudniej zapewnić stosowną kontrolę korzystania z nich. W ocenie Prokuratora Generalnego, wszystkie zakwestionowane przepisy, niezależnie od istniejących między nimi różnic, zawierają otwarte katalogi środków technicznych, umożliwiających prowadzenie kontroli operacyjnej, jak również pozwalają na pozyskiwanie niczym w praktyce nieograniczonego zakresu informacji. Sprzyja to arbitralności decyzji podejmowanych przez te organy. Obywatele w związku z tym nie wiedzą, za pomocą jakich środków oraz jakie konkretnie dane na ich temat mogą być pozyskane. Jedynym w zasadzie ograniczeniem służb policyjnych i służb ochrony państwa w zakresie kontroli operacyjnej stają się nie tyle uwarunkowania prawne, ile możliwości finansowe służb i dostęp do najnowocześniejszych zdobyczy technologicznych.

Prokurator Generalny podzielił pogląd wnioskodawcy odnośnie do istnienia różnych kręgów prywatności, wymagających zróżnicowanego stopnia ochrony. W tym też kontekście podniósł, że zakwestionowane przepisy naruszają konstytucyjne prawo jednostki do ochrony nienaruszalności mieszkania.

Zdaniem Prokuratora Generalnego, art. 51 Konstytucji kreuje dwa prawa podmiotowe. Po pierwsze, wyrażone w ust. 3 prawo dostępu do dokumentów i zbiorów danych, które – co wyraźnie wynika z brzmienia tego przepisu – może być ograniczone. Po drugie, wynikające z ust. 4 prawo do żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych i zebranych w sposób sprzeczny z ustawą. Sformułowanie tego przepisu prowadzi do wniosku, że na ustawodawcy ciążą surowsze wymogi związane z uzasadnieniem ingerencji w prawo wyrażone w ust. 4.

Odnosząc się do drugiej grupy zakwestionowanych przepisów, Prokurator Generalny wskazał, że zdecydowanie nie spełniają one wymogu konieczności. Służby policyjne i służby ochrony państwa zostały bowiem upoważnione do pozyskiwania i przetwarzania danych telekomunikacyjnych nie tylko w celu zapobiegania i wykrywania przestępstw określonych w Kodeksie karnym i Kodeksie karnym skarbowym, ale też innych przestępstw określonych w ustawach szczególnych. Szacunkowo można przyjąć, że katalogi przestępstw, których zwalczanie upoważnia służby do pozyskania danych telekomunikacyjnych, obejmują co najmniej dwukrotnie więcej pozycji niż katalogi przestępstw uzasadniające stosowanie kontroli operacyjnej. Katalogi te ponadto nie

spełniają wymogu dostatecznej określoności. Jednostka nie otrzymuje nawet na ich podstawie ogólnej wskazówki, w którym akcie poszukiwać zdefiniowania sytuacji prawnej, w jakiej służby będą uprawnione do sięgnięcia po dane telekomunikacyjne. Szczególnej uwagi w tym kontekście wymaga kompetencja organów kontroli skarbowej do ścigania naruszeń krajowych lub wspólnotowych przepisów celnych. Z brzmienia poszczególnych przepisów wynika, że nie tylko zdekodowanie ich treści normatywnej, ale nawet odszukanie stosowanych przepisów krajowego oraz unijnego prawa celnego wymaga specjalistycznej wiedzy. Co więcej, katalogi przestępstw uzasadniających pozyskiwanie i przetwarzanie przez służby objętych tajemnicą komunikowania się danych są nieracjonalnie obszerne. Obejmują wszystkie, bez wyjątku, przestępstwa i przestępstwa skarbowe, liczne i często niedookreślone przypadki przekraczania przepisów celnych, które przestępstwami nie są, liczne działania kontrolne podejmowane w wypadkach, gdy nawet nie wiadomo, czy jakiekolwiek naruszenie prawa miało miejsce, a także – działalność analityczną i planistyczną służb. Ponadto szereg omawianych katalogów ma charakter otwarty. Liczba sytuacji, w których służby mogą sięgać po dane telekomunikacyjne, może oscylować wokół kilkuset. Jednocześnie Prokurator Generalny wskazał, że brak wymogu subsydiarności sięgania po dane telekomunikacyjne świadczy o nieproporcjonalnej ingerencji, niespełniającej warunku konieczności. Zwrócił on ponadto uwagę na bezpośrednie lub pośrednie wyłączenie kontroli sądowej czy nawet jakiejkolwiek innej kontroli nad pozyskiwaniem danych objętych tajemnicą komunikowania się, pod względem legalności, prawidłowości oraz rzetelności. Zakwestionowane przepisy prowadzą przez to do naruszenia konstytucyjnego prawa do sądu i zakazu zamykania drogi sądowej ochrony konstytucyjnych wolności i praw (art. 45 ust. 1 i art. 77 ust. 2) – choć taki zarzut nie był przez wnioskodawcę stawiany. Zdaniem Prokuratora Generalnego, problematyka ochrony prywatności, tajemnicy komunikowania się i autonomii informacyjnej przed ograniczeniami ze strony służb policyjnych i ochrony państwa stanowi „sprawę" w rozumieniu konstytucyjnym. Tym samym musi istnieć sądowa kontrola nad pozyskiwaniem takich informacji przez te służby. Unormowania lub pominięcia skutkujące wyeliminowaniem sądu w procesie pozyskiwania danych telekomunikacyjnych należałoby ocenić w związku z tym jako niekonstytucyjne. Wyłączenie kontroli zewnętrznej, zwłaszcza sądowej, nad działalnością służb policyjnych i służb ochrony państwa wywołuje także skutek w postaci braku możliwości podjęcia przez jednostkę ochrony przysługujących jej wolności oraz praw.

2.2.2. Odnosząc się do wniosku Rzecznika Praw Obywatelskich z 15 listopada 2011 r., Prokurator Generalny w piśmie z 6 lutego 2012 r. podzielił stanowisko wnioskodawcy. Katalog przestępstw ujęty w art. 5 ust. 1 pkt 2 lit. a-c ustawy o ABW ma, zdaniem Prokuratora Generalnego, charakter otwarty. Rodzi to niepewność, które z przestępstw przewidzianych przez ustawy karne uzasadniają zarządzenie kontroli operacyjnej, prowadzonej przez ABW. Pozostawia to organom stosującym prawo zbyt szeroki margines swobody, sprzyjając arbitralności ich decyzji. Odwołując się do wcześniejszych stanowisk w sprawie, Prokurator Generalny podkreślił, że skoro nie można precyzyjnie ustalić celu kontroli operacyjnej, gdyż przesłanki jej zarządzenia są niejednoznaczne, to przepisy te nie spełniają wymogu proporcjonalnej ingerencji w prawo do prywatności, a także w wolność i tajemnicę komunikowania się. Te same argumenty przemawiają za niezgodnością tych przepisów z art. 8 Konwencji.

2.2.3. W piśmie z 11 czerwca 2012 r. Prokurator Generalny zajął stanowisko odnośnie do wniosku Rzecznika Praw Obywatelskich z 27 kwietnia 2012 r. dotyczącego przepisów ustawy o SC uprawniających tę służbę do gromadzenia i przetwarzania danych telekomunikacyjnych. Podzielił stanowisko RPO o niezgodności zaskarżonych przepisów ze wskazanymi wzorcami kontroli. Zdaniem Prokuratora Generalnego, Rzecznik w istocie

kwestionuje pominięcie legislacyjne, które podlega kontroli Trybunału. Ustawodawca nie przewidział bowiem wymogu subsydiarności ani jakiejkolwiek kontroli zewnętrznej nad pozyskiwaniem przez Służbę Celną danych telekomunikacyjnych. Aktualność zachowują argumenty podnoszone przez Prokuratora Generalnego we wcześniejszych pismach w tej sprawie. Odnosząc się natomiast do zarzutu naruszenia art. 51 ust. 4 Konstytucji przez art. 75d ust. 5 ustawy o SC, Prokurator Generalny zwrócił dodatkowo uwagę, że przepis ten – przez swoją niejasność oraz dopuszczenie przechowywania danych w szerszym celu aniżeli ustawowy cel gromadzenia danych – może stanowić zachętę do „arbitralnego podejmowania decyzji o przetwarzaniu bilingów".

3. Wyjaśnienia organów administracji publicznej.

3.1. W piśmie z 18 kwietnia 2012 r. Trybunał Konstytucyjny zwrócił się do Prezesa Urzędu Komunikacji Elektronicznej o udzielenie informacji na temat statystyk udostępniania danych telekomunikacyjnych uprawnionym podmiotom w Polsce.

W piśmie z 24 maja 2012 r. Prezes UKE poinformował Trybunał o unormowaniach dotyczących zatrzymywania oraz udostępniania danych telekomunikacyjnych uprawnionym podmiotom i metodologii opracowania corocznego sprawozdania dla Komisji Europejskiej, sporządzanego na podstawie art. 10 dyrektywy o zatrzymywaniu danych telekomunikacyjnych i art. 180g ust. 2 prawa telekomunikacyjnego. Sprawozdanie to zawiera zbiorcze zestawienie dotyczące liczby żądań udostępnienia danych telekomunikacyjnych pochodzących od uprawnionych podmiotów, w tym sądów i prokuratorów, skierowanych do przedsiębiorców telekomunikacyjnych. Ponadto Prezes UKE zwrócił uwagę na brak jednolitej metodologii opracowania statystyk dotyczących zatrzymywania oraz udostępniania danych telekomunikacyjnych w państwach członkowskich Unii Europejskiej, przez co nie ma możliwości ich porównania. Do swego pisma Prezes UKE załączył sprawozdanie z 1 marca 2012 r. dla Komisji Europejskiej za 2011 r.

3.2. W piśmie z 11 października 2012 r. Trybunał Konstytucyjny wystąpił do Prezesa UKE o przedstawienie dodatkowych wyjaśnień w zakresie różnic w metodologii sporządzania statystyk zatrzymywania i udostępniania danych telekomunikacyjnych w Polsce, Niemczech, Francji i Szwecji. W odpowiedzi z 13 grudnia 2012 r. Prezes UKE wyjaśnił, że pomimo podjętych starań nie udało się ustalić stosowanych w państwach członkowskich UE metod analizowania procesu zatrzymywania i udostępniania danych telekomunikacyjnych. Wynika to z niskiego stopnia harmonizacji przepisów w ramach UE, jak również braku jakichkolwiek jednolitych rozwiązań lub standardów. W załączeniu do tego pisma, Prezes UKE przekazał sprawozdanie Komisji Europejskiej dla Rady i Parlamentu Europejskiego z oceny dyrektywy o zatrzymywaniu danych telekomunikacyjnych z 18 kwietnia 2011 r., znak: KOM (2011) 225.

3.3. W pismach z 11 października 2012 r. Trybunał Konstytucyjny wystąpił do Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego ŻW, Generalnego Inspektora Kontroli Skarbowej, Szefa SKW, Szefa ABW, Szefa CBA oraz Szefa Służby Celnej o przedstawienie statystyk dotyczących zarządzania kontroli operacyjnej za lata 2009-2011, w tym: liczby wniosków sporządzonych przez uprawnione podmioty, liczby wniosków zatwierdzonych przez Prokuratora Generalnego lub odpowiednio prokuratorów okręgowych oraz liczby postanowień sądu odmawiających zarządzenia kontroli operacyjnej. Trybunał zwrócił się ponadto o wskazanie, jaki jest odsetek spraw, w których stosowana jest kontrola operacyjna wśród wszystkich spraw oraz

wśród tych spraw, w których ustawodawca dopuścił stosowanie tej kontroli. Trybunał Konstytucyjny wystąpił również o przedstawienie statystyk dotyczących zapytań skierowanych przez upoważnionych funkcjonariuszy w latach 2009-2011 do operatorów telekomunikacyjnych o udostępnienie danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, a w szczególności o wskazanie liczby osób (posiadaczy numeru telefonicznego), których dane telekomunikacyjne służby pozyskiwały, wskazanie liczby zapytań o dane osobowe abonenta, wykaz połączeń i dane lokalizacyjne. Trybunał wystąpił o udostępnienie statystyk dotyczących rodzaju spraw, w których służby sięgają po dane telekomunikacyjne.

3.3.1. Z udzielonych odpowiedzi wynikają następujące wnioski:

Po pierwsze, w odpowiedziach wskazywano na brak jednolitej metodologii zbierania i analizowania danych statystycznych udostępniania danych telekomunikacyjnych, a także brak prawnego obowiązku sporządzania takich statystyk przed 2011 r. Z tego powodu dane za lata 2009-2010 r. są niepełne oraz oparte wyłącznie na incydentalnie prowadzonych statystykach, niekiedy w ramach pojedynczych oddziałów/komórek organizacyjnych poszczególnych służb. Obowiązek gromadzenia i opracowywania danych statystycznych wprowadzono dopiero od 1 stycznia 2011 r. Na polecenie Sekretarza Kolegium do Spraw Służb Specjalnych zalecono też, aby informacje dotyczące liczby zapytań telekomunikacyjnych gromadzone były z podziałem na zapytania dotyczące odpowiednio: wykazów połączeń z numeru telefonu (tzw. bilingów), lokalizację użytkownika telefonu komórkowego, danych abonenta i pozostałych sprawdzeń.

Po drugie, nie jest możliwe ustalenie ogólnej liczby podmiotów (osób fizycznych), w stosunku do których pozyskiwano dane telekomunikacyjne. Nie jest także możliwe ustalenie, w odniesieniu do jakich konkretnie typów przestępstw – wśród wszystkich, w których ustawa dopuszcza udostępnianie służbom danych telekomunikacyjnych – dane te były pozyskiwane. W kontekście pytania TK dotyczącego wniosku Prokuratora Generalnego z 21 czerwca 2012 r. kwestionującego m.in. konstytucyjność art. 10b ust. 1 ustawy o SG w związku z enumeratywnie wskazanymi przepisami ustaw karnych, Komendant Główny Straży Granicznej zaznaczył, że czyny zabronione penalizowane w tych przepisach nie należą do właściwości Straży Granicznej. W konsekwencji Straż Graniczna nie kierowała zapytań o dane telekomunikacyjne w tym zakresie.

Po trzecie, liczba zapytań o dane telekomunikacyjne na podstawie zakwestionowanych przepisów nie odzwierciedla rzeczywistej liczby abonentów, których dane telekomunikacyjne pozyskiwano. Wskazano, że nie ma w ogóle możliwości ustalenia tego w sposób precyzyjny. Jak wynika z udzielonych wyjaśnień najwięcej zapytań (około 50%) dotyczy ustalenia danych osobowych abonenta. Wynika to z braku centralnej bazy abonentów, z której można pobrać stosowne dane, a także z dużej liczby użytkowników telefonów komórkowych korzystających z tzw. kart przedpłaconych *pre paid* (według przekazanych Trybunałowi danych, około 52% użytkowników telefonów komórkowych w Polsce korzysta z tej formy rozliczeń). Karty te nie są rejestrowane i imiennie przypisane do konkretnych podmiotów. W związku z tym ustalenie posiadacza karty tego rodzaju wymaga dokonania dodatkowych sprawdzeń, w konsekwencji generując większą liczbę zapytań o dane telekomunikacyjne. Czynnikiem zwiększającym liczbę zapytań o dane telekomunikacyjne jest też konieczność kierowania ich do wszystkich największych operatorów, ponieważ nie ma możliwości ustalenia – wyłącznie na podstawie numeru telefonu – jaki operator obsługuje danego abonenta, a co za tym idzie – do kogo ma być skierowane zapytanie. W odpowiedziach zwrócono też uwagę na ograniczenia systemów informatycznych i brak jednolitych reguł udostępniania danych telekomunikacyjnych przez operatorów, które także wpływają na wzrost sumarycznej liczby zapytań.

Po czwarte, relatywnie niewielki jest odsetek spraw, w których zarządzano kontrolę operacyjną wśród wszystkich spraw, co do których ustawodawca dopuścił jej zarządzenie (w 2011 r.: Policja – ok 3,5%; Straż Graniczna – ok. 6%; wywiad skarbowy – ok. 0,6%; ABW – poufne; SKW – poufne; CBA – ok. 12%). Zdecydowanie większy jest natomiast odsetek spraw, w których służby policyjne i ochrony państwa pozyskiwały dane telekomunikacyjne. Wynika to głównie z braku zamkniętego katalogu przestępstw, którym zapobieganie oraz których wykrywanie i ściganie uzasadniać może udostępnienie danych telekomunikacyjnych poszczególnym służbom. W świetle odpowiedzi udzielonych Trybunałowi, Straż Graniczna pozyskiwała dane telekomunikacyjne w 2011 r. w około 66% spraw, ABW – 19%, SKW – poufne; Służba Celna (od 14 lipca 2011 r. do końca 2011 r.) – 0,97% spraw. Od pozostałych służb, do których Trybunał zwrócił się z pytaniem, nie uzyskano odpowiedzi w tym zakresie, przede wszystkim – jak wyjaśniano – z powodu niemożliwości przypisania liczby zapytań telekomunikacyjnych do liczby prowadzonych spraw.

Po piąte, co znajduje zresztą potwierdzenie w informacjach przedkładanych Sejmowi i Senatowi przez Prokuratora Generalnego na podstawie art. 10ea ustawy o prokuraturze (zob. druk nr 1267/VII kadencja Senatu, druk nr 64/VIII kadencja Senatu, druk nr 1229/VII kadencja Sejmu), od 2010 r. systematycznie spada liczba zarządzanych kontroli operacyjnych. Ponadto relatywnie niewielki jest odsetek negatywnych opinii Prokuratora Generalnego oraz prokuratorów okręgowych w zakresie wniosku o zarządzenie kontroli operacyjnej przez sąd, a także odsetek odmowy zarządzenia kontroli operacyjnej przez sąd, mimo pozytywnej opinii Prokuratora Generalnego lub prokuratorów okręgowych (w obydwu wypadkach co do zasady nie przekracza on 1% wszystkich wniosków).

3.3.2. Szef SKW przekazał odpowiedź na wszystkie pytania Trybunału w piśmie z 7 listopada 2012 r. opatrzonym klauzulą „poufne". Natomiast Szef ABW oprócz odpowiedzi udzielonych w pismach jawnych z 7 listopada 2012 r. i 15 stycznia 2013 r. na pytanie dotyczące liczby spraw, w których sąd zarządził na wniosek ABW kontrolę operacyjną, wśród wszystkich prowadzonych przez nią spraw i wśród spraw, w których ustawodawca upoważnił do stosowania kontroli operacyjnej, udzielił odpowiedzi w piśmie z 15 stycznia 2013 r. oznaczonym klauzulą „poufne". Przesłał jednocześnie Trybunałowi kopię raportu ABW z 13 sierpnia 2012 r. dotyczącego statystyki zapytań o dane telekomunikacyjne i ustalenia abonenckie przez uprawnione podmioty w latach 2010-2011. Raport ten został opatrzony klauzulą „zastrzeżone". Nie zawiera on jednak danych statystycznych, ale jest to jedynie omówienie najważniejszych problemów wpływających na wielkości statystyczne.

3.4. W piśmie z 5 marca 2013 r. Trybunał Konstytucyjny wystąpił do Komendanta Głównego Policji o przesłanie Trybunałowi kopii wszystkich przepisów prawa wewnętrznego w tym o charakterze niejawnym, regulujących stosowanie kontroli operacyjnej i gromadzenie oraz przetwarzanie danych telekomunikacyjnych.

W piśmie z 15 marca 2013 r. Komendant Główny Policji przekazał kopię decyzji nr 774 z 19 grudnia 2008 r. w sprawie określenia podziału zadań służbowych policjantów wykonujących czynności w zakresie sporządzania i przekazywania dokumentacji kontroli operacyjnej. Natomiast pismem z 20 marca 2013 r. Minister Spraw Wewnętrznych przekazał wyciąg z zarządzenia Komendanta Głównego Policji nr pf-634 z 30 czerwca 2006 r. i aktów zmieniających to zarządzenie w zakresie regulujących kontrolę operacyjną.

3.5. W piśmie z 27 marca 2013 r. Trybunał Konstytucyjny wystąpił do Prezesa NIK o poinformowanie o wynikach kontroli dotyczącej stosowania przepisów regulujących

udostępnianie uprawnionym podmiotom danych telekomunikacyjnych, o których mowa w art.180c i art. 180d prawa telekomunikacyjnego.

W odpowiedzi z 26 kwietnia 2013 r., Prezes NIK przedstawił wnioski pokontrolne w 17 załącznikach, w tym jeden niejawny.

Informacja o wynikach kontroli została zatwierdzona przez Prezesa NIK 2 czerwca 2013 r. Najwyższa Izba Kontroli oceniła pozytywnie, mimo stwierdzonych nieprawidłowości, działalność kontrolowanych podmiotów w zakresie uzyskiwania i przetwarzania przez nie danych telekomunikacyjnych. Negatywnie oceniona została działalność Prezesa UKE, który – zdaniem NIK – nie sprawował odpowiedniego nadzoru nad wywiązywaniem się przez przedsiębiorców telekomunikacyjnych z nałożonych na nich obowiązków. Opracowywane przez Prezesa UKE informacje w zakresie wykorzystania zgromadzonych danych nie odpowiadały stanowi rzeczywistemu. Zdaniem NIK, prezentowane informacje były niepełne, a przedstawiane przez poszczególne podmioty dane nieporównywalne. Ze względu na błędy metodologiczne, jakiekolwiek wnioskowanie statystyczne dotyczące zakresu zatrzymywania danych w Polsce jest, w ocenie NIK, nieuprawnione.

Stwierdzone nieprawidłowości u pozostałych kontrolowanych podmiotów wiązały się z nieprzestrzeganiem obowiązujących przepisów, zasad i procedur oraz naruszeniami tajemnicy telekomunikacyjnej, pozyskiwaniem danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych niespełniających wymagań technicznych i organizacyjnych; żądaniem udostępnienia danych telekomunikacyjnych za okres przekraczający 24 miesiące; nieusuwaniem zbędnych danych telekomunikacyjnych.

W ocenie NIK, obowiązujące przepisy, w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych, nie chronią dostatecznie wolności i praw jednostek przed nadmierną ingerencją państwa. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych telekomunikacyjnych może nasuwać wątpliwości co do proporcjonalności stosowanych ograniczeń konstytucyjnych wolności i praw człowieka. NIK zwróciła ponadto uwagę, że system zbierania informacji o zakresie wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, nie pozwala na określenie rzeczywistej liczby dokonywanych sprawdzeń. Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania.

W ocenie NIK, należałoby rozważyć podjęcie działań w czterech zasadniczych obszarach: zakresu i celu pozyskiwania danych, kontroli nad procesem pozyskiwania danych, niszczenia pozyskanych danych w sytuacji, gdy nie są już niezbędne dla osiągnięcia celów prowadzonego postępowania, a ponadto stworzenia mechanizmów sprawozdawczych, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych.

3.6. W piśmie z 23 września 2013 r. Trybunał Konstytucyjny zwrócił się do Prezesa Rady Ministrów o przedstawienie opinii w sprawie.

Prezes Rady Ministrów w piśmie z 24 stycznia 2014 r. odniósł się do połączonych wniosków Rzecznika Praw Obywatelskich i Prokuratora Generalnego. Wniósł o stwierdzenie, że:

1) art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA, art. 31 ust. 4 pkt 3 ustawy o SKW są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji;

2) art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW, art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w części obejmującej zwrot „a także innych ustawach i umowach międzynarodowych" w zakresie, w jakim odnoszą się do ratyfikowanych umów międzynarodowych, są zgodne, natomiast w zakresie dotyczącym umów międzynarodowych innych niż ratyfikowane umowy międzynarodowe oraz porozumień międzynarodowych są niezgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

3) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW, art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW, są zgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

4) art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA oraz art. 31 ustawy o SKW w zakresie, w jakim nie przewidują regulacji wyłączającej z kręgu podmiotów, które mogą być poddane kontroli operacyjnej, kategorie osób, od których uzyskanie informacji objętych tajemnicą adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego i lekarską podlega zakazom dowodowym, w zakresie objętym zakazami są zgodne z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2, art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji, a także z art. 6 ust. 3 lit. b i c, art. 8 i art. 10 ust. 1 Konwencji;

5) art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW, art. 75d ust. 1 ustawy o SC są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

6) art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b i c, a także pkt 5 ustawy o ABW, art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnoszą się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW, art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o CBA są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

7) art. 32 ust. 1 pkt 1 w związku z art. 5 ust 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnoszą się do zwrotu „a także innych ustawach i umowach międzynarodowych" w części dotyczącej ratyfikowanych umów międzynarodowych, są zgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji;

8) art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW 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;

9) art. 75d ust. 5 ustawy o SC w zakresie, w jakim nie przewiduje zniszczenia zebranych danych telekomunikacyjnych niezawierających informacji mających znaczenie w sprawach o przestępstwa skarbowe, jest niezgodny z art. 51 ust. 4 Konstytucji;

10) art. 20c ust. 1 ustawy o Policji w związku z art. 278 § 1, 2 i 5, art. 284 § 1 i 2, art. 288 § 1 k.k. oraz w związku z art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt, art. 10b ust. 1 ustawy o SG w związku z art. 278 § 1, 2 i 5, art. 284 § 1 i 2, art. 288 § 1 k.k. oraz w związku z art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia, art. 30 ust. 1 ustawy o ŻW w związku z art. 278 § 1, 2 i 5, art. 284 § 1 i 2, art. 288 § 1 k.k. oraz w związku z art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt, są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

Odnosząc się do zarzutów dotyczących przepisów regulujących kontrolę operacyjną, Prezes Rady Ministrów uznał ją za niewątpliwie istotnie ingerującą w prywatność jednostek. Niemniej jednak, jego zdaniem, unormowania ustawowe regulujące jej prowadzenie spełniają wymagania konstytucyjne. Przede wszystkim kontrolę operacyjną zarządza sąd, po uprzednim uzyskaniu zgody Prokuratora Generalnego albo prokuratorów okręgowych na wystąpienie z wnioskiem do sądu. Ponadto sąd wyznacza w postanowieniu o zarządzeniu kontroli rodzaj informacji i dowodów, które mogą być zgromadzone. Weryfikacja wniosków o zarządzenie kontroli operacyjnej dokonywana przez sądy nie może być uznana za pozorną, gdyż sąd ma obowiązek ocenić całokształt materiału i podjąć decyzję o tym, czy w danej sprawie kontrola operacyjna jest zasadna. Tym samym niezasadny jest zarzut RPO, jakoby zakres informacji i dowodów o jednostce gromadzonych przez służby był wyznaczany przez same służby.

Odnosząc się do zarzutów Prokuratora Generalnego kwestionującego brak gwarancji ochrony osób zobowiązanych do zachowania tajemnic zawodowych, Prezes Rady Ministrów wskazał, że wnioskodawca mylnie utożsamia gwarancje wynikające z zakazów dowodowych z podmiotowym wyłączeniem spośród grupy podmiotów wobec których może być stosowana kontrola operacyjna, zobowiązanych do zachowania tajemnicy zawodowej. Zdaniem Prezesa Rady Ministrów, intencją wnioskodawcy zdaje się doprowadzenie do wyłączenia określonych osób, zobowiązanych do zachowania tajemnicy zawodowej, spod możliwości pozyskiwania informacji w drodze kontroli operacyjnej. Tego rodzaju podmiotowe wyłączenie oznaczonej kategorii podmiotów nie ma żadnego konstytucyjnego uzasadnienia. Niezależnie od tego nie jest możliwe z przyczyn technicznych wyłączenie na etapie prowadzenia kontroli operacyjnej tych wypowiedzi, które miałyby być objęte zakazami dowodowymi.

Odnosząc się do zarzutów dotyczących możliwości stosowania kontroli operacyjnej w celu zapobiegania przestępstwom ściganym na mocy umów międzynarodowych czy ich wykrywania Prezes Rady Ministrów zaznaczył, że wszystkie ratyfikowane umowy międzynarodowe, bez względu na ich formalną procedurę poprzedzającą ratyfikację przez prezydenta, są źródłem powszechnie obowiązującego prawa (art. 87 ust. 1 Konstytucji). Są one ogłaszane, a więc dostępne. Ponadto umowy międzynarodowe regulujące problematykę ścigania określonego rodzaju przestępczości zwykle nie zawierają precyzyjnych znamion czynu zabronionego, lecz wskazują zagadnienia, które państwa mają dopiero unormować w wewnętrznym (krajowym) ustawodawstwie.

Analizując zarzuty dotyczące przepisów o pozyskiwaniu danych telekomunikacyjnych, Prezes Rady Ministrów wyjaśnił przyczyny odmiennego standardu regulacji pozyskiwania tych danych w porównaniu z kontrolą operacyjną. Jego zdaniem, ustawodawca posłużył się „właściwą i adekwatną do charakteru oraz zakresu ingerencji w prawa i wolności techniką”. Oceniając konstytucyjność tych przepisów, trzeba mieć na

względzie cel regulacji, jakim jest możliwość efektywnego i szybkiego zwalczania i wykrywania przestępstw. Ponadto stopień ingerencji w prywatność jednostek w związku z pozyskiwaniem danych telekomunikacyjnych jest istotnie mniejsza niż ingerencja w związku z prowadzeniem kontroli operacyjnej. Dane te są częstokroć jedynym sposobem uzyskiwania dowodów w wypadku takich przestępstw, jak np. uporczywe nękanie (stalking), oszustwa internetowe, rozpowszechnianie pornografii dziecięcej czy innych przestępstw popełnianych za pomocą sieci telekomunikacyjnych. Tego rodzaju środek pozwala również na szybką reakcję służb w wypadkach wielu dolegliwych przestępstw, jak chociażby kradzieże telefonów.

Prezes Rady Ministrów wniósł jednocześnie – na wypadek stwierdzenia niezgodności zaskarżonych przepisów z Konstytucją – o odrodzenie o 18 miesięcy terminu utraty mocy obwiązującej niekonstytucyjnych unormowań.

3.7. W piśmie z 23 września 2013 r. Trybunał Konstytucyjny zwrócił się do Ministra Spraw Zagranicznych o udzielenie informacji, czy Rzeczpospolita Polska złożyła pisemne obserwacje w sprawach toczących się przed Trybunałem Sprawiedliwości UE wszczętych przez High Court of Ireland (sygn. C-293/12), Verfassungsgerichtshof (sygn. C-594/12) i Datenschutzkommission z Austrii (sygn. C-46/13), a jeśli tak – o przesłanie kopii tych pism.

W odpowiedzi z 26 września 2013 r. Minister Spraw Zagranicznych przesłał kopię pisemnego stanowiska w sprawie o sygn. C-293/12, informując, że w pozostałych sprawach nie zajął stanowiska.

3.8. W piśmie z 23 września 2013 r. Trybunał Konstytucyjny zwrócił się do Prezesów Izby Karnej oraz Izby Wojskowej Sądu Najwyższego o poinformowanie, czy w orzecznictwie sądowym istnieje jednolite i utrwalone rozumienie następujących pojęć zawartych w zakwestionowanych przepisach: „przestępstwa ścigane na mocy umów i porozumień międzynarodowych", „przestępstwa ścigane na mocy umów międzynarodowych", „przestępstwa godzące w bezpieczeństwo państwa", „przestępstwa godzące w podstawy ekonomiczne państwa", „przestępstwa 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"; „przestępstwa godzące w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność".

Trybunał Konstytucyjny zwrócił się także o wyjaśnienie, czy w świetle orzecznictwa sądowego można potwierdzić, że zarządzając kontrolę operacyjną, o której mowa w art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA i art. 31 ust. 4 pkt 3 ustawy o SKW, sąd określa w postanowieniu o zarządzeniu tej kontroli konkretny rodzaj (typ) środka technicznego, który w danej sprawie może być zastosowany. Ponadto Trybunał wystąpił o informację, czy w świetle orzecznictwa sądowego istnieją dostateczne gwarancje ochrony osób zobowiązanych do zachowania tajemnicy obrończej, dziennikarskiej, adwokackiej, radcy prawnego, notarialnej, doradcy podatkowego i lekarskiej w toku kontroli operacyjnej, a w szczególności czy wykształciła się stała i jednolita linia orzecznicza wyłączająca możliwość zarządzenia kontroli operacyjnej wobec osób zobowiązanych do zachowania tajemnicy zawodowej bądź obligująca do zniszczenia materiałów

zawierających treści – uznawane na gruncie Kodeksu postępowania karnego – za objęte bezwarunkowymi oraz warunkowymi zakazami dowodowymi.

3.8.1. W piśmie 9 października 2013 r. udzielił odpowiedzi Prezes Izby Wojskowej SN. Wskazał, że w Izbie Wojskowej Sądu Najwyższego, sprawującej nadzór judykacyjny nad sądami wojskowymi, takie sprawy nie były przedmiotem analiz. W piśmie ograniczono się do spraw rozpatrywanych przez Izbę Wojskową SN działającą jako sąd odwoławczy od orzeczeń wojskowych sądów okręgowych.

Z odpowiedzi wynika, że pojęcia „przestępstwa ścigane na mocy umów i porozumień międzynarodowych" oraz „przestępstwa godzące w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", nie były przedmiotem rozważań składów orzekających.

Zarządzając kontrolę operacyjną, sąd określa w postanowieniu w sposób szczegółowy i niebudzący wątpliwości konkretny typ (rodzaj) środka technicznego, który w danej sprawie może być zastosowany.

Prezes Sądu Najwyższego zwrócił uwagę na brak dostatecznej ochrony podmiotów zobowiązanych do zachowania tajemnicy zawodowej. W szczególności nie wykształciła się stała i jednolita linia orzecznicza, wyłączająca możliwość zarządzenia takiej kontroli bądź obligująca zniszczenie materiałów zawierających treści uznawane na gruncie przepisów k.p.k. za objęte bezwarunkowymi i warunkowymi zakazami dowodowymi.

3.8.2. W piśmie z 26 listopada 2013 r. udzielił odpowiedzi Prezes Izby Karnej Sądu Najwyższego. Wskazał on, że wyrażenia ustawowe: „przestępstwa ścigane na mocy umów i porozumień międzynarodowych", „przestępstwa ścigane na mocy umów międzynarodowych", „przestępstwa godzące w bezpieczeństwo państwa", „przestępstwa godzące w podstawy ekonomiczne państwa", „przestępstwa 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", nie były przedmiotem wykładni Sądu Najwyższego ani sądów apelacyjnych, wobec czego nie można mówić o ich jednolitym bądź utrwalonym rozumieniu.

W odniesieniu do pozostałych pytań Trybunału Konstytucyjnego, Prezes Izby Karnej Sądu Najwyższego odmówił udzielenia odpowiedzi. W jego ocenie, istotą tych pytań nie jest ustalenie wykładni obowiązującego prawa, ale chodzi o wyjaśnienie dotyczące praktyki orzeczniczej sądów powszechnych oraz opinię co do dostatecznej gwarancyjności zaskarżonych przepisów.

3.9. W piśmie z 19 grudnia 2013 r. Trybunał Konstytucyjny zwrócił się do Ministra Spraw Zagranicznych o przekazanie wykazu wszystkich aktualnie obowiązujących umów i porozumień międzynarodowych zobowiązujących Rzeczpospolitą Polską do ścigania przestępstw, a jeśli nie były publikowane – o ich kopie.

W piśmie z 8 stycznia 2014 r. Minister Spraw Zagranicznych przedstawił wykaz obejmujący 105 dwustronnych oraz 32 wielostronnych umów międzynarodowych, których Polska jest stroną, dotyczących ścigania przestępstw. Przekazał ponadto kopie niepublikowanych umów oraz porozumień międzynarodowych w tym zakresie. Jak dodatkowo wyjaśnił, MSZ nie może zagwarantować kompletności tego wykazu, gdyż przepisy prawa nakładają na Ministra Spraw Zagranicznych obowiązek przechowywania jedynie umów międzynarodowych. Informacje o porozumieniach są przekazywane MSZ na zasadzie dobrowolności przez zawierające je ministerstwa.

3.10. W piśmie z 19 grudnia 2013 r. Trybunał Konstytucyjny zwrócił się do Ministra Sprawiedliwości o wskazanie listy wszystkich czynów stanowiących przestępstwa ścigane na mocy wiążących Rzeczpospolitą Polską umów i porozumień międzynarodowych w rozumieniu art. 19 ust. 1 pkt 8 ustawy o Policji i odpowiednio art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW, art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW, a ponadto o wskazanie, które z powyższych przestępstw są objęte przepisami art. 19 ust. 1 pkt 1-7 ustawy o Policji i odpowiednio art. 9e ust. 1 pkt 1-6 ustawy o SG, art. 36c ust. 1 pkt 1-4 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW.

W piśmie z 16 stycznia 2014 r. Minister Sprawiedliwości przekazał Trybunałowi tabelaryczne zestawienie zawierające listę 35 konwencji i porozumień międzynarodowych, które zobowiązują do ścigania przestępstw w nich zawartych, oraz wskazanie, czy i w jakim zakresie przestępstwa określone przez te umowy międzynarodowe są objęte przepisami art. 19 ust. 1 pkt 1-7 ustawy o Policji, art. 9e ust. 1 pkt 1-6 ustawy po SG oraz art. 36c ust. 1 pkt 1-4 ustawy o kontroli skarbowej.

3.11. W piśmie z 19 grudnia 2013 r. Trybunał Konstytucyjny zwrócił się do prezesów wszystkich sądów apelacyjnych, a także do prezesów sądów okręgowych mających siedzibę w miastach będących siedzibą apelacji o poinformowanie, czy w świetle ich orzecznictwa można stwierdzić jednolite oraz utrwalone rozumienie następujących wyrażeń zawartych w zakwestionowanych przepisach: „przestępstwa ścigane na mocy umów i porozumień międzynarodowych", „przestępstwa ścigane na mocy umów międzynarodowych", „przestępstwa godzące w bezpieczeństwo państwa", „przestępstwa godzące w podstawy ekonomiczne państwa", „przestępstwa 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". Ponadto Trybunał zwrócił się o wskazanie, jakie przestępstwa są zaliczane do tego katalogu.

Trybunał Konstytucyjny zwrócił się dodatkowo o wyjaśnienie, czy w postanowieniu o zarządzeniu kontroli operacyjnej sąd określa konkretny rodzaj (typ) środka technicznego, który w danej sprawie może być zastosowany, oraz czy wykształciła się praktyka orzecznicza dotycząca zarządzenia kontroli operacyjnej wobec podmiotów obowiązanych do zachowania tajemnicy zawodowej, obligująca do zniszczenia materiałów zawierających treści uznawane przez kodeks postępowania karnego za objęte bezwarunkowymi lub warunkowymi zakazami dowodowymi.

W wypadku sądów apelacyjnych, Trybunał wystąpił także o wskazanie, ile wniosków o zarządzenie kontroli operacyjnej było rozpoznawanych przez sądy okręgowe w obszarze właściwości danego sądu apelacyjnego odpowiednio w latach 2010, 2011, 2012 i 2013 oraz ilu sędziów orzekało w sprawach zarządzenia takiej kontroli.

3.11.1. Z odpowiedzi sądów wynikają następujące wnioski:

Po pierwsze, nie można mówić o wykształceniu się w orzecznictwie sądowym stałej i jednolitej praktyki orzeczniczej co do rozumienia wyżej wymienionych wyrażeń zawartych w przepisach będących przedmiotem kontroli Trybunału. Przepisy te były bowiem dość rzadko stosowane przez sądy, jako podstawa zarządzenia kontroli operacyjnej.

Po drugie, co do zasady, sądy nie określają w postanowieniu o zarządzeniu kontroli operacyjnej rodzaju środka technicznego, jaki w danej sprawie ma być zastosowany. Jedynie z odpowiedzi Prezesa Sądu Okręgowego w Poznaniu oraz Prezesa Sądu Okręgowego w Rzeszowie wynika, że określały one rodzaj środka technicznego. Jak

wskazał Prezes Sądu Okręgowego w Poznaniu, w sądzie tym określa się rodzaj środka przez wskazanie, że kontrola operacyjna ma polegać na przykład na podsłuchu telefonu komórkowego wraz z sms o wskazanym numerze bądź numerze IMEI, podsłuchu telefonu stacjonarnego o wskazanym numerze, podsłuchu konkretnego pomieszczenia, kontroli korespondencji internetowej wskazanego adresu e-mail.

Po trzecie, nie wykształciła się utrwalona praktyka orzecznicza odnosząca się do stosowania kontroli operacyjnej wobec osób zobowiązanych do zachowania tajemnicy zawodowej ani zasad postępowania z materiałami zawierającymi informacje objęte tajemnicą zawodową. Sądy najczęściej nie rozważały bowiem, czy osób poddanych kontroli operacyjnej dotyczą zakazy dowodowe. Nie wiedzą jak wykorzystano materiały i czy zniszczono te spośród nich, które zawierają informacje objęte tajemnicą zawodową.

Po czwarte, sumaryczna liczba kontroli operacyjnych zarządzanych w poszczególnych latach w powiązaniu z sumaryczną liczbą sędziów orzekających w tych sprawach w każdym z sądów objętych zakresem zapytania wskazuje, że prawdopodobne jest sprawowanie przez sąd efektywnego nadzoru nad wnioskami o zarządzanie takiej kontroli. Co do zasady bowiem na jednego sędziego przypadało do rozpoznania kilka lub kilkanaście wniosków o zarządzenie kontroli operacyjnej rocznie. Nie przesądza to o sposobie merytorycznego badania tych wniosków przez sądy.

3.11.2. W piśmie z 7 stycznia 2014 r. Prezes Sądu Okręgowego w Warszawie odmówiła udzielenia odpowiedzi na zadane pytania. Uzasadniła to tym, że żądane informacje mają charakter niejawny w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228; dalej: u.o.i.n.). Nie ma tym samym podstaw prawnych do ich przekazania Trybunałowi.

W piśmie z 21 stycznia 2014 r. Trybunał Konstytucyjny ponownie zażądał od Prezesa Sądu Okręgowego w Warszawie wykonania obowiązku określonego w art. 21 ust. 1 ustawy o TK. Trybunał Konstytucyjny zwrócił ponadto uwagę, że zgodnie z art. 23 ust. 2 ustawy o TK sędziowie Trybunału są upoważnieni do dostępu do informacji niejawnych związanych z rozpoznawaną przez Trybunał sprawą. Niezależnie od tego, nawet gdyby uznać informacje dotyczące stosowania prawa za niejawne w rozumieniu przepisów u.o.i.n., ustawa ta określa tryb przekazania takich informacji uprawnionym podmiotom.

Mimo ponownego wezwania do wykonania obowiązku przewidzianego w art. 21 ust. 1 ustawy o TK, Prezes Sądu Okręgowego w Warszawie odmówiła przedstawienia żądanych informacji. W piśmie z 28 lutego 2014 r., stanowiącym odpowiedź na ponowne wezwanie Trybunału z 21 stycznia 2014 r., podniosła dodatkowo, że żądane informacje nie wiążą się z rozpoznawaną przez Trybunał sprawą o sygn. K 23/11. Nie może ona w związku z tym udzielić odpowiedzi.

W związku z zaistniałą sytuacją, Trybunał Konstytucyjny zwrócił się pismem z 11 marca 2014 r. do Prezesa Sądu Apelacyjnego o podjęcie czynności mających na celu spowodowanie wykonania przez Prezesa Sądu Okręgowego w Warszawie ustawowego obowiązku udzielenia pomocy Trybunałowi.

W piśmie z 13 marca 2014 r. Prezes Sądu Apelacyjnego poinformowała Trybunał o podjętych w tej sprawie czynnościach nadzorczych. W jej ocenie, Prezes Sądu Okręgowego w Warszawie udzieliła odpowiedzi na pisma Trybunału. Prezes Sądu Apelacyjnego, w ramach sprawowanego nadzoru nad działalnością administracyjną prezesów sądów okręgowych, nie ma kompetencji do oceny wykładni przez prezesów sądów przepisów dotyczących przekazywania informacji niejawnych zawartych w aktach spraw sądowych.

Trybunał Konstytucyjny wezwał Prezesa Sądu Okręgowego w Warszawie do udziału w rozprawie wyznaczonej na 1-3 kwietnia 2014 r. Wskazał, że oczekuje przedstawienia mu informacji, o które wystąpił pismem z 19 grudnia 2013 r.

Na rozprawie Prezes Sądu Okręgowego była reprezentowana przez wiceprezesa tegoż sądu do spraw karnych. Na pytania formułowane przez członków składu orzekającego będące powtórzeniem pytań zawartych w piśmie z 19 grudnia 2013 r. przedstawicielka Prezesa Sądu Okręgowego w Warszawie nie udzieliła odpowiedzi, podnosząc generalnie te same argumenty, które były zawarte w dotychczasowej korespondencji.

W postanowieniu pełnego składu z 2 kwietnia 2014 r., Trybunał zobowiązał Prezesa Sądu Okręgowego w Warszawie do udzielania odpowiedzi na pytania dotyczące stosowania przez ten sąd przepisów regulujących kontrolę operacyjną, a będących przedmiotem zaskarżenia w sprawie o sygn. K 23/11, w terminie do 5 maja 2014 r.

Prezes Sądu Okręgowego udzieliła następujących wyjaśnień: Sąd Okręgowy w Warszawie, zarządzając kontrolę operacyjną, wskazuje w postanowieniu rodzaj środka technicznego, jaki ma być zastosowany w konkretnej sprawie. Nie wykształciła się natomiast linia orzecznicza dotycząca ochrony osób zobowiązanych do zachowania tajemnicy zawodowej. W wypadku pytania o interpretację wyrażeń: „przestępstwa ścigane na mocy umów i porozumień międzynarodowych", „przestępstwa ścigane na mocy umów międzynarodowych", „przestępstwa godzące w bezpieczeństwo państwa", „przestępstwa godzące w podstawy ekonomiczne państwa", „przestępstwa 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" – Prezes Sądu Okręgowego w Warszawie ponownie odmówiła odpowiedzi. Podtrzymała swoje dotychczasowe stanowisko, że informacje objęte żądaniem Trybunału Konstytucyjnego mają charakter informacji niejawnych. Nie ma wobec tego prawnych możliwości badania orzecznictwa dotyczącego zarządzania kontroli operacyjnej. Sprawy te są bowiem rozpoznawane w trybie niejawnym, przez co w zakresie jej ustawowych kompetencji nie mieści się dostęp do akt takich spraw. Prezes Sądu Okręgowego w Warszawie zwróciła też uwagę, że postanowienia sądu o zarządzeniu kontroli operacyjnej – w wypadku wyrażenia zgody na taką kontrolę – nie są uzasadniane. Jedynie w wypadkach odmowy sporządza się uzasadnienia. To również przyczynia się do niemożliwości udzielenia odpowiedzi na pytania Trybunału o praktykę stosowania zaskarżonych przepisów.

Prezes Sądu Okręgowego zadeklarowała zarazem możliwość dostarczenia akt spraw sądowych dotyczących zarządzenia kontroli operacyjnej do siedziby Trybunału Konstytucyjnego z zachowaniem warunków ochrony informacji niejawnych lub umożliwienia przejrzenia repertoriów oraz akt takich spraw przez sędziów Trybunału w siedzibie Sądu Okręgowego w Warszawie.

Trybunał nie podziela poglądu Prezesa Sądu Okręgowego w Warszawie co do braku możliwości udzielenia informacji o praktyce orzeczniczej przepisów będących przedmiotem kontroli w postępowaniu przed TK. Trybunał Konstytucyjny zwraca uwagę, że art. 22 § 1 pkt 2 p.u.s.p. nie wyłącza z zakresu realizacji określonego w nim obowiązku nałożonego na prezesów sądów analizy orzecznictwa pod względem poziomu jednolitości jakichkolwiek kategorii spraw, a zatem i spraw związanych z zarządzaniem kontroli operacyjnej. Nie można zgodzić się w konsekwencji ze stanowiskiem o niedopuszczalności zapoznania się przez Prezesa Sądu Okręgowego w Warszawie z „całym orzecznictwem Sądu dotyczącym wyrażania zgody na kontrolę operacyjną". Wbrew stanowisku Prezesa Sądu Okręgowego, trudno ponadto w tym wypadku mówić o jakiejkolwiek ingerencji w niezawisłość sędziowską. Trybunał nie podziela także poglądu, jakoby Prezes Sądu Okręgowego w Warszawie nie miała dostępu do informacji niejawnych w zakresie odnoszącym się do orzeczeń o zarządzeniu kontroli operacyjnej

przez ten sąd. Przepis art. 85 § 4 zdanie trzecie p.u.s.p. uprawnia do udostępniania informacji niejawnych nie tylko sędziom orzekającym („w zakresie niezbędnym do pełnienia urzędu na stanowisku sędziowskim"), ale także innym sędziom – w zakresie niezbędnym dla pełnienia powierzonej funkcji lub wykonywania powierzonych czynności. Funkcją taką jest funkcja prezesa sądu, a realizowanym zadaniem – obowiązek analizy orzecznictwa w zakresie wskazanym w art. 22 § 1 pkt 2 p.u.s.p. Nie można w tym kontekście zgodzić się z tezą postawioną przez Prezesa Sądu Okręgowego w Warszawie, że między art. 21 a art. 22 ustawy o TK nie istnieje relacja norma szczególna – norma ogólna, która miałaby świadczyć o wykluczeniu stosowania art. 21 ustawy o TK w wypadkach, w których chodzi o informację o praktyce orzeczniczej. Udzielenie informacji o praktyce orzeczniczej nie stanowi wykładni przepisów. Na marginesie należy zauważyć, że treść art. 22 ustawy o TK nie wyklucza zwrócenia się w trybie art. 21 ustawy o TK do innych, niż SN lub NSA, sądów o stosowne informacje, w tym dotyczące wykładni przepisu w orzecznictwie danego sądu. Tym samym istnieją wystarczające podstawy prawne do wykonania nałożonego na Prezesa Sądu Okręgowego w Warszawie obowiązku udzielenia pomocy Trybunałowi, o której mowa w art. 21 ust. 1 ustawy o TK, w zakresie określonych w pismach Trybunału z 19 grudnia 2013 r. i 21 stycznia 2014 r. oraz w postanowieniu z 2 kwietnia 2014 r.

Mając na uwadze potrzebę wyjaśnienia wszystkich okoliczności rozpatrywanej sprawy i brak odpowiedzi na pytania dotyczące stosowania przepisów regulujących kontrolę operacyjną, a także ze względu na istotną rolę Sądu Okręgowego w Warszawie w procedurze zarządzania kontroli operacyjnej, sędziowie Trybunału Konstytucyjnego: Andrzej Rzepliński – przewodniczący składu orzekającego i II sprawozdawca, Marek Zubik – I sprawozdawca oraz Wojciech Hermeliński – członek składu orzekającego, udali się 2 czerwca 2014 r. do Sądu Okręgowego w Warszawie w celu zapoznania się na miejscu z repertoriami oraz wybranymi aktami zakończonych spraw dotyczących zarządzania kontroli operacyjnej. Wgląd w akta spraw sądowych w siedzibie Sądu Okręgowego w Warszawie nie oznacza jednak akceptacji Trybunału dla sposobu rozumienia ciążącego na sądach i innych organach władzy publicznej obowiązku udzielenia pomocy Trybunałowi, o którym mowa w art. 21 ust. 1 ustawy o TK.

Z analizy repertoriów i akt zakończonych spraw sądowych przez sędziów Trybunału nie wynika, że istnieje utrwalona linia orzecznicza dotycząca rozumienia wyrażeń zawartych w przepisach regulujących przesłanki zarządzenia kontroli operacyjnej, będących przedmiotem kontroli Trybunału. Wyniki analizy akt spraw sądowych nie potwierdzają również tezy, jakoby Sąd Okręgowy w Warszawie określał w postanowieniu rodzaj środka technicznego, który ma być stosowany w konkretnej sprawie. Środek ten wskazywany jest generalnie we wnioskach kierowanych do sądu przez szefów poszczególnych służb.

3.12. W piśmie z 28 maja 2014 r. Trybunał Konstytucyjny zwrócił się do Ministra Sprawiedliwości o udzielenie dodatkowych wyjaśnień w kwestii wykazu wiążących Polskę umów międzynarodowych zobowiązujących do ścigania przestępstw, a w szczególności wyjaśnienia rozbieżności między wykazem umów w zakresie przestępczości sporządzonym i przekazanym Trybunałowi przez Ministra Spraw Zagranicznych.

W odpowiedzi z 11 czerwca 2014 r. Minister Sprawiedliwości zajął stanowisko w tej kwestii. Występujące w zakwestionowanych przepisach wyrażenie „przestępstw ściganych na mocy umów i porozumień międzynarodowych" powinien być rozumiany ściśle, jako odnoszące się tylko do takich umów i porozumień międzynarodowych, które obligują do penalizacji w prawie krajowym określonych w nich zachowań, zawierają

definicję przestępstw oraz regulują inne istotne zagadnienia odnoszące się do ścigania przestępstw, jak np. jurysdykcję.

4. Stanowisko organów samorządów zawodowych.

4.1. W piśmie z 4 maja 2012 r. opinię odnoszącą się do wniosków Rzecznika Praw Obywatelskich z 29 czerwca i 1 sierpnia 2011 r. przedstawiła Naczelna Rada Adwokacka. Jak wynika z uzasadnienia tej opinii, została ona sformułowana m.in. na podstawie doświadczeń adwokatów na tle stosowania zakwestionowanych przepisów.

Naczelna Rada Adwokacka zwróciła uwagę na brak dostatecznych mechanizmów ochrony tajemnicy adwokackiej i obrończej w wypadku pozyskiwania danych telekomunikacyjnych i stosowania kontroli operacyjnej. W obecnym stanie prawnym nie można bowiem wykluczyć sytuacji, że służby odpowiedzialne za ściganie przestępstw mogą zapoznać się z materiałami objętymi tymi tajemnicami, w tym sporządzić akt oskarżenia na tej podstawie. Naczelna Rada Adwokacka dostrzegła ponadto problem braku sądowej kontroli zasadności, celowości i prawidłowości czynności operacyjno-rozpoznawczych. Jej zdaniem, skoro niejawne czynności prowadzone przez służby policyjne i ochrony państwa skutkują wkroczeniem w prywatność i autonomię informacyjną, to osobom, o których informacje są niejawnie pozyskiwane, muszą przysługiwać środki zaskarżenia, chociażby o charakterze następczym (*ex post*). Zaskarżone przepisy nie przewidują nawet odroczonej kontroli w tym zakresie. Zdaniem Naczelnej Rady Adwokackiej, kolejnym mankamentem zakwestionowanych przepisów regulujących dostęp służb do danych telekomunikacyjnych jest brak zamkniętego katalogu czynów zabronionych, co do których dane te mogą być pozyskane. Organy ścigania mogą żądać takich danych w wypadku wszystkich przestępstw, nawet o niskiej społecznej szkodliwości. Mają one pełną dowolność w powyższym zakresie, co jest niedopuszczalne i grozi notorycznym naruszaniem praw podstawowych.

4.2. W związku z wnioskiem Prokuratora Generalnego z 13 listopada 2012 r., a także pismem Naczelnej Rady Adwokackiej z 31 grudnia 2012 r. o umożliwienie jej przedstawienia dodatkowej opinii w tej sprawie, Prezes Trybunału Konstytucyjnego – w piśmie z 14 stycznia 2013 r. – zwrócił się do Naczelnej Rady Adwokackiej, Krajowej Rady Radców Prawnych, Krajowej Rady Doradców Podatkowych, Krajowej Rady Notarialnej, Naczelnej Rady Lekarskiej oraz Stowarzyszenia Dziennikarzy Polskich o ustosunkowanie się do zarzutów sformułowanych w tym wniosku w zakresie stosowania kontroli operacyjnej przez służby policyjne oraz służby ochrony państwa w perspektywie ochrony tajemnicy zawodowej osób reprezentowanych przez poszczególne samorządy.

4.2.1. W piśmie z 1 lutego 2013 r. Krajowa Rada Notarialna – wyjaśniając znaczenie tajemnicy zawodowej notariusza, jako fundamentu funkcjonowania notariatu, służącej przede wszystkim ochronie interesu klientów – podzieliła w pełni zarzuty Prokuratora Generalnego.

4.2.2. W piśmie z 8 lutego 2013 r. Naczelna Rada Lekarska podzieliła argumenty zawarte we wniosku Prokuratora Generalnego z 13 listopada 2012 r. i wnioskach Rzecznika Praw Obywatelskich. Chociaż wniosek Prokuratora Generalnego koncentruje się w zasadzie na ochronie tajemnicy obrończej, to jednak zdaniem NRL przesłanki przemawiające za ścisłą ochroną informacji objętych tajemnicą lekarską są równie doniosłe, jak te przemawiające za ochroną tajemnicy obrończej.

4.2.3. W piśmie z 13 lutego 2013 r. Krajowa Rada Radców Prawnych, odnosząc się do wniosku z 13 listopada 2012 r., wskazała na możliwość podsłuchiwania rozmów radcy prawnego nie tylko podczas czynności operacyjno-rozpoznawczych prowadzonych przez

służby policyjne i ochrony państwa (tzw. podsłuchu pozaprocesowego), ale również w toku procesu karnego. W obydwu wypadkach ustawodawca nie przewidział jednak żadnych przepisów chroniących tajemnicę zawodową radcy prawnego. Zdaniem KRRP, problem nie sprowadza się jednakże do pominięcia prawodawczego, polegającego na niedopuszczalności stosowania wobec radców prawnych kontroli operacyjnej, ale w istocie do wykorzystywania informacji uzyskanych w trakcie takiej kontroli, w zakresie objętym zakazami dowodowymi (art. 3 ust. 5 ustawy z dnia 6 lipca 1982 r. o radcach prawnych, Dz. U. z 2010 r. Nr 10, poz. 65, ze zm. w związku z art. 180 § 2 k.p.k.). Ujawnienie materiałów, które zebrano w toku kontroli operacyjnej, nie może powodować obejścia przepisów o tajemnicach ustawowo chronionych. Jak wskazano, wnioskodawca był niekonsekwentny, domagając się – z jednej strony – wyłączenia spod kontroli operacyjnej radców prawnych, z drugiej natomiast twierdząc, że zebrane materiały nie mogą być wprowadzone do procesu karnego. Zdaniem KRRP, istotnym problemem pojawiającym się na tle wniosku Prokuratora Generalnego jest brak spójnego unormowania podsłuchu procesowego i pozaprocesowego oraz związana z tym niejednoznaczność ochrony tajemnicy zawodowej.

4.2.4. W piśmie z 21 lutego 2013 r. Krajowa Rada Doradców Podatkowych podzieliła zarzuty Prokuratora Generalnego. Odwołując się do orzecznictwa TK oraz sądów powszechnych, wskazano, że uchylenie tajemnicy zawodowej doradcy podatkowego jest dopuszczalne wyłącznie w procesie karnym (nie zaś w innych postępowaniach sądowych i administracyjnych), a zakres okoliczności uzasadniających zwolnienie z tajemnicy musi być określony precyzyjnie w ustawie. Ogólnikowe unormowanie przesłanek prowadzenia kontroli operacyjnej umożliwia nie tylko pozyskiwanie informacji o osobach bezpośrednio objętych niejawną obserwacją, ale także o utrzymujących kontakt z tymi osobami. Może to prowadzić do nieuprawnionego poszerzenia podmiotowego zakresu kontroli operacyjnej bez uprzedniej zgody sądu, również o doradców podatkowych, świadczących usługi na rzecz ich klientów, co może skutkować naruszeniem tajemnic zawodowych oraz zakazów dowodowych. Przyznanie służbom policyjnym i ochrony państwa kompetencji umożliwiających pozyskiwanie w niejawny sposób informacji objętych tajemnicą zawodową, w konsekwencji drastycznie obniżających gwarancję, jakiej ustawodawca udzielił zawodom zaufania publicznego, narusza wynikającą z art. 2 Konstytucji zasadę demokratycznego państwa prawa.

4.2.5. W piśmie z 27 lutego 2013 r. Naczelna Rada Adwokacka podzieliła zarzuty Prokuratora Generalnego dotyczące przepisów regulujących kontrolę operacyjną, w zakresie odnoszącym się do ochrony tajemnicy adwokackiej i obrończej oraz ochrony konstytucyjnych wolności i praw jednostek związanych ze świadczeniem pomocy prawnej przez adwokatów. Przedstawiła dodatkowo obszerne stanowisko dotyczące konstytucyjnych mankamentów obowiązujących unormowań kontroli operacyjnej, związanych z możliwością stosowania tej kontroli bez zgody sądu w sytuacjach niecierpiących zwłoki i konsekwencjami takich czynności dla podsądnego i obrońcy. Wskazano ponadto na konieczność umożliwienia zaskarżenia postanowienia sądu zarządzającego kontrolę operacyjną, chociażby *ex post*, przez osobę poddaną tej kontroli, ewentualnie wprowadzeniu do postępowania instytucji rzecznika osoby kontrolowanej, który mógłby ją reprezentować niejako w zastępstwie.

Odnosząc się do *meritum* problemu, zwrócono uwagę, że pomoc prawna świadczona przez adwokata nie zawsze sprowadza się do postępowania sądowego. Może ona dotyczyć doradztwa pozaprocesowego lub alternatywnych metod rozwiązywania sporów. W każdym z tych wypadków niezbędne jest istnienie zaufania klienta do adwokata, a także obowiązywanie stosownych gwarancji prawnych tego zaufania, czyli tajemnicy zawodowej. Wyłącznie w warunkach pełnego zaufania możliwe jest

świadczenie rzetelnej pomocy prawnej i efektywne działanie adwokata na rzecz klienta. Zdaniem NRA, sama świadomość naruszenia tajemnicy obrończej oraz adwokackiej polegająca na możliwości zastosowania podsłuchu operacyjnego, będzie mogła skutecznie powstrzymać klientów przed ujawnianiem informacji adwokatowi, co istotnie utrudnia analizę sprawy i udzielenie profesjonalnej pomocy prawnej.

W ocenie Naczelnej Rady Adwokackiej, ustawodawca nie zagwarantował należytej ochrony tajemnicy adwokackiej ani – wymagającej szczególnej ochrony prawnej – tajemnicy obrończej w ramach czynności operacyjno-rozpoznawczych. Co więcej, wskazano, że nie jest konstytucyjnie dopuszczalne tak daleko idące zróżnicowanie ochrony tajemnicy zawodowej, w zależności od tego, czy chodzi o podsłuch procesowy, unormowany w k.p.k., czy kontrolę operacyjną wynikającą z zaskarżonych przepisów.

Zdaniem NRA, możliwość pozyskiwania informacji stanowiących tajemnicę obrończą może być traktowane jako naruszające istotę konstytucyjnego prawa do obrony, a w każdym razie nie spełnia wymogów wynikających z zasady proporcjonalności.

4.2.6. W piśmie z 5 marca 2013 r. Stowarzyszenie Dziennikarzy Polskich poparło zarzuty sformułowane przez Prokuratora Generalnego. Zdaniem SDP, obowiązujące obecnie unormowanie kontroli operacyjnej uczyniło tajemnicę dziennikarską w istocie fikcją. Zakazy i ograniczenia wynikające z prawa prasowego oraz k.p.k. nie mają bowiem zastosowania do czynności operacyjno-rozpoznawczych. Wystarczającej ochrony nie zapewnia także prawny obowiązek komisyjnego niszczenia zgromadzonych zapisów, gdyż cechować ma się to niską skutecznością. Stowarzyszenie odniosło się ponadto do problematyki pozyskiwania danych telekomunikacyjnych przez uprawnione służby. Tego rodzaju inwigilacja dziennikarzy – w ocenie SDP – może prowadzić do naruszenia tajemnicy dziennikarskiej, a w konsekwencji do sytuacji, w której informatorzy będą odmawiać przekazywania dziennikarzom istotnych dla społeczeństwa demokratycznego informacji. Godzi to w podstawową funkcję mediów będących kontrolerem działań władz publicznych.

5. Stanowisko organizacji społecznych.

5.1. W piśmie z 19 marca 2012 r. opinię w sprawie przedstawiła Fundacja Panoptykon, podzielając stanowisko RPO dotyczące niekonstytucyjności przepisów, które regulują udostępnianie służbom policyjnym i ochrony państwa danych telekomunikacyjnych. Fundacja zwróciła także uwagę, że zaskarżone przepisy wprowadzono do polskiego systemu prawnego na skutek implementacji dyrektywy o zatrzymywaniu danych telekomunikacyjnych. Akt ten, przewidujący nałożenie na operatorów telekomunikacyjnych państw członkowskich UE obowiązku zatrzymywania danych o połączeniach telekomunikacyjnych oraz udostępnianie ich odpowiednim organom, w celu wykrywania i ścigania poważnych przestępstw, budzi poważne wątpliwości ze względu na możliwość nieproporcjonalnej ingerencji w podstawowe prawa obywatelskie.

Zdaniem Fundacji, ustawodawca przyznał służbom szersze uprawnienia, niż wynika to z przepisów dyrektywy o zatrzymywaniu danych telekomunikacyjnych, która zastrzegła wykorzystywanie tych danych wyłącznie w celach ścigania i zapobiegania najpoważniejszym tylko przestępstwom, podczas gdy w Polsce mogą być one wykorzystywane w odniesieniu do każdego przestępstwa. Fundacja zwróciła uwagę na niepokojącą praktykę nadmiernego wykorzystywania przez sądy, a także Policję danych telekomunikacyjnych. Polska znajduje się w czołówce państw europejskich pod względem wykorzystywania przez służby danych telekomunikacyjnych. Fundacja stwierdziła ponadto, że brak jest w obowiązujących przepisach wystarczających zewnętrznych form

kontroli nad retencją danych, co może prowadzić do pozyskiwania ich w sposób bezprawny. Problemem związanym z implementacją dyrektywy do polskiego porządku prawnego jest brak gwarancji realizacji tajemnicy zawodowej: lekarskiej, adwokackiej, notarialnej lub dziennikarskiej. Zwróciła ona również uwagę na brak obowiązku niszczenia zbędnych danych w wypadku niektórych służb.

5.2. W piśmie z 13 czerwca 2012 r. opinię w sprawie przedstawiła Helsińska Fundacja Praw Człowieka. Podzieliła stanowisko przedstawione we wniosku Rzecznika Praw Obywatelskich z 29 czerwca 2011 r.

Zdaniem Helsińskiej Fundacji Praw Człowieka, kontrola operacyjna stanowi głęboką i istotną ingerencję w konstytucyjne prawa i wolności jednostki, w szczególności w prawo do prywatności. Odwołując się do wyroku ETPC w sprawie Uzun przeciwko Niemcom (nr skargi 35623/05), podkreślono, że wyłącznie jasno i precyzyjne sformułowane ramy prawne legitymują państwo do ograniczenia wolności i prawa jednostki przez stosowanie środków niejawnego pozyskiwania informacji o jednostkach. W aktualnym stanie prawnym w Polsce ram takich brakuje.

Po pierwsze, podstawę ingerencji w sferę prawa do prywatności stanowią aktualnie nie tylko przepisy ustawy, lecz także swobodne uznanie władz publicznych. Szczególny nacisk położono w tym kontekście na wykorzystywanie urządzeń GPS w toku kontroli operacyjnej. Zdaniem Fundacji nie ma jednoznacznych podstaw prawnych do stosowania tego środka technicznego w Polsce. Na skutek braków regulacji ustawowej doprecyzowanie kompetencji służb, np. Policji, w zakresie ingerencji w wolności i prawa jednostki następuje w aktach wewnętrznych, często o charakterze poufnym, jak np. poufne zarządzenia Komendanta Głównego Policji. Z doświadczenia HFPC wynika, że służby ochrony państwa utrudniają dostęp do informacji dotyczących przeprowadzanych kontroli operacyjnych, zasłaniając się ochroną informacji niejawnych.

Po drugie, zaskarżone przepisy nie spełniają testu proporcjonalności. Nie wyznaczają w wystarczający sposób organom władzy granic ingerencji w sferę praw i wolności jednostki. Jednocześnie jednostkę pozbawia się prawa do zapoznania się z rodzajem działań, jakie organy mogą podjąć w jej sprawie. Nie została tym samym zachowana proporcja pomiędzy koniecznością zapewnienia bezpieczeństwa publicznego a ograniczeniem prywatności.

Zdaniem Fundacji, katalog środków technicznych powinien zostać przeniesiony w całości na poziom ustawowy, a wprowadzanie wszelkich nowych metod inwigilacji powinno następować jedynie w drodze nowelizacji ustawy. Dzięki temu sąd – kontrolując zasadność przeprowadzenia kontroli operacyjnej – będzie mógł sprawdzić, czy doszło do zastosowania środka z katalogu. To rozwiązanie stanowiłoby efektywną gwarancję prawa do prywatności.

Helsińska Fundacja Praw Człowieka przekazała także Trybunałowi oryginał i własne tłumaczenie wyroku Sądu Najwyższego USA w sprawie Stany Zjednoczone przeciwko Antoine Jones (sygn. 131 S. Ct. 3064) dotyczącego niejawnego zastosowania urządzeń GPS.

5.3. W piśmie z 11 czerwca 2013 r. Helsińska Fundacja Praw Człowieka przedstawiła Trybunałowi opracowanie „Sądowa kontrola wniosków o zarządzenie kontroli operacyjnej", przygotowaną na podstawie informacji udzielonych Fundacji przez szefów poszczególnych służb, w kompetencji których leży stosowanie kontroli operacyjnej, a także prezesów sądów okręgowych zarządzających taką kontrolę. W opracowaniu uwzględniono też dane zawarte w stosownych sprawozdaniach Prokuratora

Generalnego i Ministra Spraw Wewnętrznych, które są sporządzane na podstawie art. 10ea ustawy o prokuraturze i odpowiednio art. 19 ust. 22 ustawy o Policji.

W ocenie Fundacji, po analizie powyższych informacji można sformułować następujące konkluzje. Po pierwsze, sądy okręgowe i wojskowe sądy okręgowe w znacznej liczbie spraw (nierzadko ponad 90%) pozytywnie rozpatrują wniosek o zarządzenie kontroli operacyjnej, co może budzić wątpliwości, czy nadzór sądowy tego rodzaju spełnia właściwą rolę. Po drugie, w sytuacji nieuwzględnienia wniosku o zarządzenie kontroli operacyjnej bardzo rzadko były wnoszone zażalenia, a jeśli zostały wniesione, brakuje pełnych danych obrazujących sposób rozpoznania środka odwoławczego. Po trzecie, różna pozostaje częstotliwość stosowania kontroli operacyjnej przez poszczególne służby. Na częstotliwość składania wniosków o zarządzenie kontroli operacyjnej wpływały, zdaniem Fundacji, następujące czynniki:

- pojawienie się nowych rodzajów przestępczości i rozbudowanie ustawowych katalogów przestępstw uzasadniających zarządzenie kontroli operacyjnej;
- usunięcie barier biurokratycznych związanych z procedurą zarządzania kontroli;
- nieskuteczność dotychczasowych instrumentów pracy operacyjnej;
- pojawienie się nowych narzędzi technologicznych, dających możliwość pozyskania istotnych dla postępowania karnego danych o jednostkach, a nieobarczonych tak restrykcyjnymi wymaganiami, jak kontrola operacyjna (np. pozyskiwanie danych telekomunikacyjnych);
- zmiany możliwości finansowych i kadrowych służb.

W piśmie zwrócono uwagę na mało przejrzyste przepisy regulujące m.in. okoliczności uzasadniające zarządzenie kontroli operacyjnej, a także środki pozyskiwania informacji i dowodów, które mogą być w jej ramach stosowane (np. niejasność pojęcia „inne środki techniczne"). Dostrzeżono też mankamenty proceduralne sądowego nadzoru. Nie jest bowiem jasne, czy *de lege lata* sąd może żądać przedstawienia mu całości akt operacyjnych. Wydając zaś postanowienie o zarządzeniu kontroli, nie jest obowiązany go uzasadnić. Osoba poddana kontroli operacyjnej nie ma ponadto możliwości zażalenia, a jedynym środkiem ochrony jej wolności i praw jest droga cywilna. Zwrócono ponadto uwagę – powołując się na wypowiedzi samych sędziów – na niedostateczne przygotowanie merytoryczne kadry sędziowskiej do rozpoznawania wniosków dotyczących kontroli operacyjnej, nieznaczny dorobek orzeczniczy i doktrynalny co do tego zagadnienia, a także powszechnie znane obłożenie sądów okręgowych. Na zarządzanie kontroli operacyjnej przez sąd wpływa również istnienie uprzedniej weryfikacji wniosków przez prokuratorów, co eliminuje te nienależycie przygotowane.

5.4. W piśmie z 30 kwietnia 2014 r. Helsińska Fundacja Praw Człowieka – powołując się na wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. stwierdzający nieważność dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE i wydane przez słowacki sąd konstytucyjny postanowienie zawieszające obowiązywanie przepisów prawa słowackiego implementujących tę dyrektywę – zwróciła się do Trybunału Konstytucyjnego o rozważenie wydania postanowienia sygnalizacyjnego. Przedmiotem tego postanowienia miałoby być wskazanie ustawodawcy na konieczność dokonania zmian prawa regulującego zatrzymywanie danych telekomunikacyjnych i ich udostępnienie uprawnionym podmiotom.

II

1. Na rozprawę w dniach 1-3 kwietnia 2014 r. stawili się uczestnicy postępowania: przedstawiciele Rzecznika Praw Obywatelskich, Prokuratora Generalnego i Sejmu. Do udziału w rozprawie, na podstawie art. 38 pkt 4 ustawy o TK, zostali również wezwani: Prezes Rady Ministrów, Minister Sprawiedliwości, Komendant Główny Policji, Komendant Główny Straży Granicznej, Generalny Inspektor Kontroli Skarbowej, Komendant Główny Żandarmerii Wojskowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Centralnego Biura Antykorupcyjnego, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Celnej, Prezes Najwyższej Izby Kontroli, Prezes Urzędu Komunikacji Elektronicznej, Naczelna Rada Adwokacka, Krajowa Rada Radców Prawnych i Naczelna Rada Lekarska. Ponadto do udziału w rozprawie został wezwany Prezes Sądu Okręgowego w Warszawie.

2. Wnioskodawcy podtrzymali zarzuty sformułowane we wnioskach. Rzecznik Praw Obywatelskich, jak i Prokurator Generalny – odnosząc się do swoich wniosków – podkreślili, że nie kwestionują dopuszczalności stosowania przez właściwe organy kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych. Problemem zakwestionowanych przepisów jest natomiast niedostateczny poziom gwarancji proceduralnych. Jak zaznaczył Prokurator Generalny, państwo nie może zrezygnować z obydwu tych metod działalności operacyjnej, umożliwiających w szczególności zwalczanie najpoważniejszej przestępczości godzącej w bezpieczeństwo państwa, porządek publiczny, życie lub zdrowie obywateli. Mając jednakże na uwadze, że czynności te prowadzone są niejawnie, bez wiedzy jednostek, których dotyczą, przepisy regulujące kontrolę operacyjną oraz udostępnianie danych telekomunikacyjnych właściwym służbom muszą spełniać rygorystyczne standardy ochrony jednostek przed arbitralną ingerencją w sferę wolności i praw konstytucyjnych.

3. Pierwszą kwestią, którą Trybunał starał się wyjaśnić, było funkcjonowanie mechanizmu kontroli nad działalnością operacyjną służb przez uprawnione organy państwa. Odpowiadając na pytania członków składu orzekającego, przedstawiciel Sejmu wyjaśnił, że Komisja do spraw Służb Specjalnych zwraca wprawdzie uwagę na liczbę kontroli operacyjnych i realność danych statystycznych podawanych w informacjach składanych przez Ministra Spraw Wewnętrznych na podstawie art. 19 ust. 22 ustawy o Policji, jednakże danych tych nie weryfikuje. Nie można tym samym potwierdzić tezy sformułowanej m.in. w informacji Ministra Spraw Wewnętrznych za rok 2012 (druk sejmowy nr 1450/VII kadencja), że w praktyce kontrola operacyjna jest stosowana w wypadku najpoważniejszych przestępstw wymienionych w art. 19 ust. 1 ustawy o Policji.

Ponadto, jak wynika z wypowiedzi przedstawiciela Sądu Okręgowego w Warszawie, postanowienia wyrażające zgodę na zarządzenie kontroli operacyjnej nie są uzasadnianie. Sąd sporządza uzasadnienia tylko w wypadkach odmowy wyrażenia zgody.

Jak natomiast wskazał przedstawiciel Prokuratora Generalnego, prokuratorzy biorący udział w procedurze zarządzania kontroli operacyjnej nie poprzestają na formalnej analizie wniosku i jego akceptacji. Są również wypadki odmowy wyrażenia zgody na jej zarządzenie, a także następuje skrócenie czasu kontroli, o który początkowo występowały służby.

Podczas rozprawy pojawiły się rozbieżne stanowiska w kwestii efektywności nadzoru Prezesa Urzędu Komunikacji Elektronicznej nad przedsiębiorcami świadczącymi usługi telekomunikacyjne w Polsce, w tym lokalizacji serwerów, na których dane są zatrzymywane na podstawie polskich przepisów implementujących dyrektywę 2006/24/WE. Jak wyjaśnił przedstawiciel Prezesa UKE, przedsiębiorcy zastrzegają

informacje dotyczące umiejscowienia serwerów lub dotyczące własnej sieci, jako tajemnicę przedsiębiorstwa. Organ ten nie zna więc miejsca ich przechowywania.

4. Odnosząc się do pytań dotyczących określenia w ustawie rodzajów przestępstw, wnioskodawcy zgodnie stwierdzili, że z przepisu ustawy jednoznacznie musi wynikać, do jakich czynów zabronionych można stosować kontrolę operacyjną. Ustawodawca może w tym zakresie wskazać enumeratywnie jednostki redakcyjne ustawy, bądź odesłać do całych rozdziałów. W tym zakresie odmienne stanowisko zajął przedstawiciel Ministra Sprawiedliwości. W jego ocenie wystarczające byłoby posłużenie się rodzajową nazwą przestępstwa lub jego elementami definicyjnymi.

Uczestnicy postępowania byli zgodni co do tego, że niejawne pozyskiwanie informacji o jednostkach może być dopuszczalne wyłącznie w odniesieniu do poważnych przestępstw. Rzecznik nie wykluczałby akceptacji takiego rozwiązania legislacyjnego, które zezwala na dostęp do danych abonenckich w odniesieniu do każdego przestępstwa, natomiast pozostałe dane (o ruchu i lokalizacji) mogłyby być udostępniane, jeśli dotyczą przestępstw poważnych.

Jeśli chodzi o kryterium, na podstawie którego należałoby ustalać katalog przestępstw, wskazywano, że może być nim górny bądź dolny wymiar kary wymierzanej w warunkach podstawowych. Odpowiadając na pytanie dotyczące przepisów regulujących udostępnianie służbom danych telekomunikacyjnych, przedstawiciel Prezesa Rady Ministrów podniósł, że oprócz zagrożenia karą, powinna być brana pod uwagę również społeczna uciążliwość danego czynu, jego częstotliwość lub dolegliwość.

5. Odnosząc się do pytań dotyczących udostępnia danych statystycznych, generalnie uczestnicy postępowania zajmowali stanowisko, zgodnie z którym obowiązek publikowania ogólnych, zagregowanych danych statystycznych co do stosowania czynności operacyjno-rozpoznawczych w skali kraju nie stanowi zagrożenia dla bezpieczeństwa państwa.

6. W świetle wypowiedzi uczestników postępowania konstytucyjnie uzasadnione mogłoby być zróżnicowanie ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, jaki podmiot stosuje czynności operacyjno-rozpoznawcze. Wolności lub prawa jednostek mogłyby być ograniczone w nieco szerszym zakresie, jeśli ingerencji miałyby dokonywać służby wywiadowcze i zajmujące się ochroną bezpieczeństwa zewnętrznego państwa, a nie służby policyjne. Co do zasady uczestnicy postępowania byli zgodni, że byłoby konstytucyjnie dopuszczalne wprowadzenie odmiennych regulacji dotyczących pozyskiwania informacji o obywatelach polskich i nieobywatelach. Zwrócono jednak uwagę, że w tym zakresie niektóre wolności i prawa przynależą wszystkim podmiotom znajdującym się pod władzą Rzeczypospolitej Polskiej, bez względu na obywatelstwo.

7. Jak stwierdził Prokurator Generalny, podstawowym problemem – w odniesieniu do przepisów odwołujących się do kategorii „przestępstw ściganych na mocy umów i porozumień międzynarodowych”, które to kwestionuje we wniosku z 7 marca 2012 r. – jest zarówno brak określenia w ustawie, o jakie rodzaje przestępstw chodzi, jak również objęcie przestępstw o relatywnie niskim stopniu szkodliwości społecznej. Odpowiadając na pytania członków składu orzekającego, podkreślił, że nawet jeśli dokona się prokonstytucyjnej wykładni zaskarżonych przepisów i przyjmie, że chodzi tu o przestępstwa ścigane na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą w ustawie, problem pozostanie. W dalszym ciągu nie będzie bowiem możliwe

ustalenie, jakie przestępstwa stypizowane w polskiej ustawie karnej mogłyby być uznane za „ścigane na mocy umów międzynarodowych". Przepisy zawierające to wyrażenie nie spełniają więc wymogu dostatecznej określoności prawa, wynikającego z art. 2 Konstytucji. Jak podkreślił przedstawiciel Ministra Sprawiedliwości, umowy międzynarodowe z reguły nie zawierają opisu penalizowanego czynu, ale zobowiązują państwa do ścigania określonego przestępstwa i ewentualnie jego penalizacji w prawie krajowym. Może to prowadzić do sytuacji, w której ustawodawca przeniesie do ustawy karnej znamiona danego przestępstwa opisanego w umowie międzynarodowej w sposób nieprecyzyjny. To z kolei rzutuje na niejednoznaczność kwalifikacji danego czynu, jako ściganego na mocy umów międzynarodowych, przez organy uczestniczące w procedurze zarządzania i prowadzenia kontroli operacyjnej. Problem dotyczy zwłaszcza starszych umów międzynarodowych, które opisywały czyny zabronione w sposób ogólny. W konsekwencji utrudnia to znacząco odnalezienie ich odpowiedników w polskiej ustawie karnej.

Uczestnicy postępowania zgodnie przyznali też, że w przepisach, które posługują się pojęciem „przestępstw ściganych na mocy umów i porozumień międzynarodowych", może chodzić wyłącznie o przestępstwa wymienione w umowach ratyfikowanych za uprzednią zgodą wyrażoną w ustawie (art. 89 ust. 1 Konstytucji), a nie w umowach niepodlegających ratyfikacji lub ratyfikowanych bez uprzedniej zgody parlamentu. W ich ocenie, art. 9 Konstytucji zobowiązujący do przestrzegania wiążącego prawa międzynarodowego nie może uzasadniać odstąpienia od precyzyjnego unormowania w ustawie przesłanek ingerencji w wolności i prawa jednostek (art. 31 ust. 3 Konstytucji).

W świetle wypowiedzi uczestników postępowania można przyjąć, że art. 19 ust. 1 pkt 8 ustawy o Policji (oraz analogiczne przepisy pozostałych ustaw) rozszerzają katalog sytuacji, w których może być zarządzona kontrola operacyjna.

Odnosząc się do sposobu stosowania zaskarżonych przepisów, Komendant Główny Policji zaznaczył, że art. 19 ust. 1 pkt 8 ustawy o Policji, odwołujący się do „przestępstw ściganych na mocy umów i porozumień międzynarodowych", w latach 2006-2014 był powoływany jako podstawa prawna kontroli operacyjnej tylko 160 razy, najczęściej jednak w związku z przepisami art. 19 ust. 1 pkt 1-7 ustawy o Policji. Odpowiadając na pytanie, czy art. 19 ust. 1 pkt 8 ustawy o Policji był kiedykolwiek wskazany jako samodzielna i jedyna podstawa, przedstawiciel Komendanta Głównego Policji wskazał, że zna jeden taki wypadek odnoszący się do przestępstwa pedofilii, które wówczas nie było wymienione w art. 19 ust. 1 pkt 1-7 ustawy o Policji.

Przedstawiciele służb mających prawo stosowania kontroli operacyjnej stwierdzili, że stwierdzenie niekonstytucyjności przepisów odwołujących się do przestępstw ściganych na mocy umów i porozumień międzynarodowych nie uszczupli efektywności ich działań.

Niedookreślenie okoliczności, w jakich może być stosowana kontrola operacyjna, nie tylko jest niekorzystne z punktu widzenia wolności i praw jednostek. Stwarza także problemy organom uczestniczącym w procedurze jej zarządzania. Brak konkretyzacji w ustawie rodzajów przestępstw – na co zwrócił uwagę przedstawiciel RPO, odnosząc się do sformułowań zawartych w zaskarżonych we wniosku z 15 listopada 2011 r. przepisów ustawy o ABW – może prowadzić do odmiennych ocen szefa służby, prokuratora i sądu.

Jeśli chodzi o art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a-c ustawy o ABW, to zdaniem uczestników postępowania, do zaakceptowania byłaby taka konstrukcja legislacyjna, jaka została zaproponowana w projektowanym art. 26b ustawy o ABW (druk sejmowy nr 633/VII kadencja). W projekcie przyjmuje się wymienienie nazw rodzajowych przestępstw lub przepisów ustaw karnych i dookreślenie, że mają jednocześnie godzić w bezpieczeństwo państwa lub podstawy ekonomiczne państwa. Takie stanowisko zajął również przedstawiciel ABW, wskazując, że odesłanie do całych rozdziałów kodeksu

karnego byłoby zbyt szerokie, gdyż nie każde z nich powinno być rozpoznawane przez służbę ze względu na swoją wagę. Na problem niedookreśloności ustawowych przesłanek zarządzenia kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych w ustawie o SKW zwrócił ponadto uwagę przedstawiciel SKW.

8. Przedstawiciel Rzecznika Praw Obywatelskich, odpowiadając na pytania członków składu orzekającego co do wniosku z 29 czerwca 2011 r. dotyczącego przepisów regulujących stosowanie środków technicznych w celu pozyskiwania informacji i dowodów, początkowo zajmował stanowisko, że centralnym problemem jest brak określenia w ustawie rodzajów informacji (danych) o jednostce, jakie mogą być pozyskiwane w drodze kontroli operacyjnej. Ostatecznie uznał, że problem konstytucyjny rozwiązywałoby określenie przez prawo rodzajów środków technicznych. Nie chodzi tutaj o wskazanie w ustawie parametrów technicznych samych urządzeń, lecz o rodzajowe określenie metody pozyskiwania informacji. Należy przez to rozumieć np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „przechwytywanie wiadomości przekazywanych za pomocą sieci telekomunikacyjnych"; „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu" – tzw. GPS, „nadzór elektroniczny środków łączności przewodowej lub radiowej"). Stanowisko to podzielił Prokurator Generalny. Przedstawiciele służb zwrócili też uwagę, że rodzajowe (bez wskazywania parametrów technicznych) określenie środków technicznych nie ograniczy możliwości ich działania.

Z wypowiedzi przedstawicieli służb wynika, że we wniosku o zarządzenie kontroli operacyjnej nie indywidualizuje się środka technicznego, przez wskazanie ich parametrów technicznych. Co do zasady precyzuje się natomiast „sposób prowadzenia" tej kontroli, określając, że jest to np. kontrola poczty elektronicznej pod danym adresem lub podsłuch rozmów telefonicznych prowadzonych pod numerem telefonu określonym we wniosku. Brak jest tu jednolitej praktyki w poszczególnych służbach. Wynika to do pewnego stopnia z odrębności unormowania wzorów wniosków o zarządzenie kontroli operacyjnej zawartych w załącznikach do rozporządzeń regulujących dokumentowanie kontroli operacyjnej.

9. W ocenie RPO, pozyskiwanie danych telekomunikacyjnych jest mniej dolegliwym dla jednostek sposobem ingerencji w prywatność i tajemnicę komunikowania się niż kontrola operacyjna. Na podstawie danych telekomunikacyjnych nie można się bowiem zapoznać z treścią komunikatów. Rzecznik nie wykluczył zatem odmiennych ustawowych wymagań proceduralnych kontroli operacyjnej od pozyskiwania danych telekomunikacyjnych.

Jak przyznali uczestnicy postępowania, z uwagi na zróżnicowany charakter danych telekomunikacyjnych, byłyby dopuszczalne różne wymagania proceduralne związane z istnieniem kontroli zewnętrznej. O ile w wypadku danych dotyczących połączeń lub danych lokalizacyjnych musi istnieć zewnętrzna i niezależna kontrola, przy czym nie jest wymagane, by była to kontrola sądowa, o tyle w wypadku pozyskiwania przez służby policyjne i ochrony państwa danych o abonencie taka kontrola nie jest zawsze konieczna.

10. Przedstawiciel Prokuratora Generalnego – odnosząc się do wniosku z 13 listopada 2012 r. dotyczącego ochrony tajemnicy zawodowej w toku kontroli operacyjnej – zaznaczył, że problemem konstytucyjnym jest pozyskiwanie, w ramach kontroli operacyjnej, informacji objętych zakazami dowodowymi na gruncie postępowania karnego z uwagi na ochronę tajemnicy zawodowej. Sprecyzował też, że domaga się wyłączenia

spod kontroli operacyjnej określonych informacji stanowiących tajemnicę zawodową. Nie jest natomiast wystarczające następcze zniszczenie materiałów zawierających treści objęte taką tajemnicą. Wnioskodawca ma jednak świadomość trudności związanych z legislacyjnym wyrażeniem jego postulatów. Zdaniem Prokuratora Generalnego, na etapie poprzedzającym ewentualną decyzję o wszczęciu postępowania karnego powinien być zachowany podobny standard postępowania jak na etapie procesowym.

W ocenie RPO, nie ma podstaw do podmiotowego wyłączenia określonych kategorii osób spod kontroli operacyjnej. Z punktu widzenia wolności i praw jednostek konieczne jest natomiast unormowanie sposobu postępowania z materiałami zgromadzonymi w toku kontroli operacyjnej, a w szczególności przesłanek uchylania tajemnicy zawodowej oraz niszczenia materiałów, jeśli uchylenie tajemnicy nie jest niezbędne dla dobra wymiaru sprawiedliwości.

Zdaniem przedstawicieli służb, wyłączenie osób zobowiązanych do zachowania tajemnicy zawodowej lub nawet samych przekazów stanowiących taką tajemnicę nie jest do zaakceptowania z punktu widzenia skutecznej walki z zagrożeniami. W szczególności – na co zwrócił uwagę Szef CBA – mogłoby to doprowadzić do faktycznego wyłączenia szerokiej grupy osób spod działań operacyjnych.

Stanowisko Prokuratora w tym zakresie w pełni poparli przedstawiciele Naczelnej Rady Adwokackiej, Krajowej Rady Radców Prawnych i Naczelnej Izby Lekarskiej. Zdaniem przedstawiciela NRA, nie chodzi o stworzenie podmiotowego wyłączenia określonej kategorii osób spod kontroli operacyjnej, lecz chodzi o wyłączenie podmiotowo-przedmiotowe. Z punktu widzenia ochrony zaufania klienta do osoby wykonującej zawód zaufania publicznego istotne jest to, by z rozmowami tych osób nie mogły w ogóle zapoznać się organy państwa. Zdaniem przedstawiciela NRA, silniejszej ochronie musi podlegać tajemnica obrończa niż pozostałe tajemnice zawodowe. Przedstawiciel Krajowej Rady Radców Prawnych zwrócił uwagę, że w związku z umożliwieniem pełnienia funkcji obrońcy radcom prawnym analogiczne gwarancje ochrony tajemnicy obrończej powinni mieć także radcowie prawni.

11. Przedstawiciel Najwyższej Izby Kontroli przedstawił Trybunałowi najważniejsze ustalenia zawarte w informacji pokontrolnej dotyczącej udostępniania uprawnionym organom danych telekomunikacyjnych. Zwrócił uwagę na problemy, jakie pojawiły się w trakcie kontroli w Sądzie Okręgowym w Warszawie. Prezes tego sądu odmówiła udzielenia wyjaśnień i uniemożliwiła dokończenie czynności kontrolnych.

12. Trybunał otrzymał od przedstawiciela Sądu Okręgowego w Warszawie wyjaśnienia o przyczynach odmowy udzielenia przez ten sąd pomocy prawnej Trybunałowi w zakresie przedstawienia praktyki orzeczniczej dotyczącej zarządzania kontroli operacyjnej.

Na rozprawie 2 kwietnia 2014 r. Trybunał wydał postanowienie, w którym ponownie zobowiązał Prezesa Sądu Okręgowego w Warszawie do udzielenia pomocy prawnej w zakresie objętym treścią pism z 19 grudnia 2013 r. i 21 stycznia 2014 r. w terminie do 5 maja 2014 r. (zob. szerzej cz. I, pkt 3.11.2 uzasadnienia).

13. Na rozprawie 30 lipca 2014 r. uczestnicy postępowania i podmioty wezwane do udziału w rozprawie odpowiedzieli na dodatkowe pytania członków składu orzekającego.

Przedstawiciel Prokuratora Generalnego cofnął w części wniosek z 21 czerwca 2012 r. dotyczący zbadania zgodności art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG i art. 30 ust. 1 ustawy o ŻW w związku z art. 46 ust. 1 prawa prasowego, wskazując na utratę mocy obowiązującej tego przepisu prawa prasowego.

Po wysłuchaniu wniosków końcowych, Trybunał Konstytucyjny uznał sprawę za dostatecznie wyjaśnioną do rozstrzygnięcia i zamknął rozprawę.

III

Trybunał Konstytucyjny zważył, co następuje:

1. Wolność człowieka a ochrona bezpieczeństwa państwa i porządku publicznego w erze cyfrowej.

1.1. Status człowieka w demokratycznym państwie prawa opiera się na poszanowaniu jego przyrodzonej i niezbywalnej godności (art. 30 Konstytucji), a także wynikającej z niej wolności (autonomii), czyli swobodzie decydowania o swym postępowaniu, zgodnie z własną wolą (art. 31 ust. 1 i 2). Jednoznacznie dano temu wyraz również we wstępie do Konstytucji, mianowicie wszyscy stosujący jej postanowienia, mają czynić to, „dbając o zachowanie przyrodzonej godności człowieka, jego prawa do wolności (…) a poszanowanie tych zasad mieli za niewzruszoną podstawę Rzeczypospolitej Polskiej".

1.2. Ustrojodawca wyszedł z założenia konieczności zapewnienia możliwie jak najszerszej prawnej ochrony wolności człowieka, będącej naturalnym atrybutem prawnego statusu jednostki. Wynika to jednoznacznie z art. 31 ust. 1 Konstytucji, zgodnie z którym wolność każdego – bez względu na to, jakiej sfery życia dotyczy – podlega ochronie prawnej. Jak przyjęto w orzecznictwie Trybunału Konstytucyjnego, jest ona chroniona zarówno w jej aspekcie pozytywnym i negatywnym. „Aspekt pozytywny «wolności jednostki» polega na tym, że jednostka może swobodnie kształtować swoje zachowania w danej sferze, wybierając takie formy aktywności, które jej samej najbardziej odpowiadają, lub powstrzymywać się od podejmowania jakiejkolwiek działalności. Aspekt negatywny «wolności jednostki» polega na prawnym obowiązku powstrzymania się – kogokolwiek – od ingerencji w sferę zastrzeżoną dla jednostki. Obowiązek taki ciąży na państwie i na innych podmiotach – nie wyłączając samorządów zawodowych zawodów zaufania publicznego. Odstąpienie od respektowania «aspektu negatywnego» wolności konstytucyjnych jest możliwe tylko na zasadach, w zakresie i w formie przewidzianej w art. 31 ust. 3 Konstytucji, ze względu na wymienione tam – enumeratywnie – wartości i przy spełnieniu wymogu proporcjonalności ograniczeń" (wyrok TK z 18 lutego 2004 r., sygn. P 21/02, OTK ZU nr 2/A/2004, poz. 9, cz. III, pkt 4).

Konstytucyjna ochrona wolności człowieka odnosi się przede wszystkim do sfery jego prywatności. Ustrojodawca statuuje prywatność jednostki, nie jako nadane konstytucyjnie prawo podmiotowe, ale jako wolność konstytucyjnie chronioną ze wszystkimi wynikającymi z tego konsekwencjami. Przede wszystkim oznacza to swobodę działania jednostek w ramach wolności, aż do granic ustanowionych w ustawie. Dopiero jednoznaczna regulacja ustawowa może nakładać ograniczenia w zakresie podejmowania określonych zachowań mieszczących się w ramach konkretnej wolności. Niedopuszczalne jest domniemywanie kompetencji władz publicznych w zakresie ingerencji w wolność jednostki. Immanentnym elementem wszystkich konstytucyjnych wolności człowieka jest spoczywający na państwie obowiązek ich prawnego poszanowania i ochrony, a także powstrzymywania się od ingerowania w wolności zarówno przez państwo, jak i podmioty prywatne (*vide:* art. 31 ust. 2 zdanie pierwsze i ust. 3 Konstytucji). Standard ten odnosi się do wszystkich konstytucyjnych wolności człowieka, w szczególności zaś do wolności osobistych, do których – oprócz prywatności – zaliczają się m.in.: wolność

komunikowania się (art. 49 Konstytucji), nienaruszalność mieszkania (art. 50 Konstytucji) czy szeroko rozumiana autonomia informacyjna (art. 51 Konstytucji).

1.3. Poszanowanie i ochronę prywatności przez władze publiczne oraz generalny zakaz ingerencji w tę sferę gwarantuje art. 47 Konstytucji. Gwarancji tych dopełnia art. 51 Konstytucji, wyrażający tzw. autonomię informacyjną. Ochrona prywatności i autonomii informacyjnej, jak już podkreślono, jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka (art. 30 Konstytucji). Jak wskazywano w dotychczasowym orzecznictwie, zachowanie przez człowieka godności wymaga poszanowania jego czysto osobistej sfery, w której nie jest narażony na konieczność „bycia z innymi" czy „dzielenia się z innymi" swoimi przeżyciami czy doznaniami (zob. wyroki TK z: 12 grudnia 2005 r., sygn. K 32/04, OTK ZU nr 11/A/2005, poz. 132, cz. III, pkt 3.2; 23 czerwca 2009 r., sygn. K 54/07, OTK ZU nr 6/A/2009, poz. 86, cz. III, pkt 5).

Jak przyjmuje się w orzecznictwie, art. 47 i art. 51 Konstytucji chronią tę samą wartość konstytucyjną – sferę prywatności. Autonomia informacyjna stanowi istotny element składowy prawa do ochrony prywatności, a polega na samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi informacjami, nawet jeśli znajdują się w posiadaniu innych osób (zob. wyroki TK z: 19 lutego 2002 r., sygn. U 3/01, OTK ZU nr 1/A/2002, poz. 3; 20 listopada 2002 r., sygn. K 41/02, OTK ZU nr 6/A/2002, poz. 83; 13 grudnia 2011 r., sygn. K 33/08, OTK ZU nr 10/A/2011, poz. 116). Trybunał podkreślał równocześnie, że art. 51 Konstytucji ustanawia szczególny środek ochrony tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji (zob. wyrok TK z 12 listopada 2002 r., sygn. SK 40/01, OTK ZU nr 6/A/2002, poz. 81).

Trybunał Konstytucyjny wielokrotnie orzekał w sprawie zgodności przepisów ustaw z art. 51 Konstytucji statuującym autonomię informacyjną jednostki oraz art. 47 Konstytucji gwarantującym prawo do ochrony prywatności. W niektórych sprawach jako wzorce kontroli wskazywane były obydwa powołane wyżej przepisy. W takich sytuacjach Trybunał zwykle badał zgodność określonego przepisu z tymi wzorcami w ramach jednego zarzutu (zob. np. wyroki TK z 19 maja 1998 r., sygn. U 5/97, OTK ZU nr 4/1998, poz. 46; 13 grudnia 2011 r., sygn. K 33/08).

Z ochroną prywatności i autonomii informacyjnej koresponduje też prawo do ochrony tajemnicy komunikowania się, ustanowione w art. 49 Konstytucji. W piśmiennictwie wskazuje się niekiedy, że wolność komunikowania się dotyczy raczej porozumiewania się za pomocą pewnego środka przekazu, nie zaś bezpośredniej rozmowy osób w jakimś miejscu, albowiem to ostatnie jest raczej wyrazem prawa do prywatności (zob. P. Sarnecki, uwaga 3 do art. 49, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III , red. L. Garlicki, Warszawa 2007, s. 3). Trybunał Konstytucyjny przyjmuje jednak szersze rozumienie wolności komunikowania się, nie przeciwstawiając jej tak kategorycznie prawu do ochrony prywatności (por. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04). Konstytucyjną ochroną wynikającą z art. 49 Konstytucji objęta jest tym samym treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania się na odległość. Według Trybunału, „przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe" (wyrok TK z 20 czerwca 2005 r., sygn. K 4/04, OTK ZU nr 6/A/2005, poz. 64). Z punktu widzenia prawa do ochrony tajemnicy komunikowania się (art. 49 Konstytucji) „sposób porozumiewania się istotny jest tylko o tyle, o ile jego zastosowanie w danych warunkach (okolicznościach) pozbawia osoby trzecie, które nie są adresatami danych treści, możliwości zapoznania się z nimi. Tylko wtedy bowiem można sensownie mówić o istnieniu jakiejś «tajemnicy», którą można byłoby objąć ochroną. W

konsekwencji, w tym jedynie znaczeniu forma komunikacji może mieć *in casu* wpływ na zakres prawa do ochrony tajemnicy komunikowania się" (wyrok TK z 2 lipca 2007 r., sygn. K 41/05, OTK ZU nr 7/A/2007, poz. 72, cz. III, pkt 5.2).

1.4. Mając powyższe na uwadze, Trybunał Konstytucyjny stwierdza, że konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI. W ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się nadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnie dostępnych. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej.

Trybunał Konstytucyjny zwraca ponadto uwagę na jeszcze jedną kwestię. Mianowicie w demokratycznym państwie prawnym zorganizowanie życia społecznego i publicznego musi zakładać możliwość występowania jednostek w przestrzeni publicznej w sposób anonimowy. Przynajmniej tam, gdzie korzystają one ze swych wolności, nie jest zasadniczo konieczne zrezygnowanie z anonimowości, tak w stosunku do państwa, jak też podmiotów prywatnych. Inaczej rzecz się ma natomiast z korzystaniem z praw podmiotowych. Ich realizacja wymaga bowiem aktywności podmiotu tego prawa, najczęściej w celu weryfikacji przysługującego mu uprawnienia.

1.5. Rozwój technologiczny poszerza sferę funkcjonowania człowieka. Otwiera nowe i nieznane dotąd możliwości korzystania z konstytucyjnie gwarantowanych wolności i praw. Nowe technologie umożliwiają w niespotykany dotąd sposób pokonywanie bariery czasu i przestrzeni w komunikowaniu się, umożliwiając przez to przekazywanie informacji na każdy temat oraz w dowolnej formie, bez względu na odległość dzielącą rozmówców. Stwarzają ponadto nowe możliwości nabywania dóbr i usług czy decydowania o sposobach realizowania własnych potrzeb. Jednocześnie odgrywają nieocenioną rolę w zapewnieniu bezpieczeństwa osobom i mieniu, umożliwiając monitoring osób i miejsc czy ich elektroniczny nadzór, dzięki któremu – niezależnie od zdarzeń losowych – możliwa jest geograficzna ich lokalizacja.

Szczególną rolę we współczesnym świecie odgrywa Internet. Przestał być on obecnie środkiem komunikowania się i przekazywania informacji na odległość. Stał się natomiast wielowymiarowym narzędziem tworzenia, przechowywania i przekazywania danych o zróżnicowanym charakterze, a jednocześnie narzędziem umożliwiającym funkcjonowanie jednostki w społeczeństwie.

Trybunał Konstytucyjny zwraca uwagę, że chociaż Konstytucja wprost nie odnosi się do funkcjonowania jednostki w wirtualnej przestrzeni, to ochrona konstytucyjnych wolności i praw jednostek w związku z korzystaniem z Internetu oraz innych

elektronicznych sposobów porozumiewania się na odległość nie różni się niczym od ochrony dotyczącej tradycyjnych form komunikowania się czy też innej aktywności. Dane przekazywane za pomocą Internetu nie mogą być postrzegane jako funkcjonujące niejako obok, czy na marginesie konstytucyjnie chronionych form aktywności człowieka. Nie ma tym samym uzasadnionych powodów, które pozwalałyby oderwać przekazywanie danych czy komunikowanie się za pomocą Internetu od sfery wolności i praw konstytucyjnych. Ze względu na złożoność zjawiska, jakim jest Internet, aktywność jednostek w tej sferze odpowiada właściwym postaciom aktywności chronionej konstytucyjnie. I tak przekazywanie korespondencji drogą elektroniczną (np. e-mail) podlega takiej samej ochronie konstytucyjnej, jak przekazywanie listu w tradycyjnie formie papierowej (art. 47, art. 49, art. 51). Przekazywanie informacji obrońcy za pomocą Internetu lub innych środków komunikacji elektronicznej – takim samym gwarancjom, jak przekazanie ich w rozmowie osobistej (art. 42). Ochrona intymności w kontaktach z osobami wykonującymi zawód zaufania publicznego jest jednakowa bez względu na formę komunikowania się (art. 47). Wyrażanie poglądów, pozyskiwanie i rozpowszechnianie informacji drogą elektroniczną podlega w pełni ochronie przewidzianej w art. 54 Konstytucji. Podobnie ochrona wolności prasy i środków społecznego przekazu jest taka sama, bez względu na formę korzystania z tej wolności (art. 14, art. 54). Konstytucyjna ochrona wolności działalności gospodarczej (art. 20 i art. 22) obejmuje swym zakresem również podejmowanie oraz prowadzenie tej działalności w Internecie lub za pomocą innych form komunikacji elektronicznej. To samo dotyczy też ochrony wolności wyboru i wykonywania zawodu (art. 65), wolności twórczości artystycznej, badań naukowych oraz ogłaszania ich wyników, jak również wolności nauczania i wolności korzystania z dóbr kultury (art. 73) czy prawa składania petycji, wniosków oraz skarg do organów władzy publicznej (art. 63).

Internet powinien być postrzegany tym samym jako jedno z narzędzi umożliwiających korzystanie z wolności i praw podmiotowych, a nie jako sfera odrębna czy wymykająca się konstytucyjnej ochronie. W tym stanie rzeczy ocena przepisów umożliwiających ingerencję w wolności i prawa podmiotowe, odnoszące się do korzystania przez jednostki m.in. z Internetu, powinna być przeprowadzana z uwzględnieniem treści normatywnej właściwych w danym wypadku przepisów Konstytucji gwarantujących ochronę praw podstawowych. Taka ocena rzutuje na granice swobody interpretacji przepisów ustawowych. Dotyczy to również tych regulacji odnoszących się do kompetencji organów państwa, których zadaniem jest ochrona bezpieczeństwa państwa. Na obecnym etapie rozwoju elektronicznych form komunikowania się nie jest zatem dopuszczalne, w ocenie Trybunału, przeciwstawianie ustawowej ochrony korespondencji tradycyjnej – pozostałym formom korespondencji przekazywanej za pomocą sieci telekomunikacyjnych.

1.6. W obliczu rosnącego znaczenia nowych technologii wzrasta jednocześnie ryzyko wykorzystywania ich do popełniania przestępstw i naruszania prawa. Mogą być one bowiem wykorzystywane do nieuprawnionego pozyskiwania wiedzy o zachowaniach współobywateli, w tym o treściach oraz formach przekazywanych komunikatów, gromadzenia tychże danych na własne potrzeby i ich przetwarzania. Mogą ponadto stanowić narzędzie służące popełnianiu specjalistycznych i wyrafinowanych przestępstw zagrażających rozmaitym dobrom lub służyć komunikowaniu się czy integracji osób naruszających prawo. Zjawisko to jest niebezpieczne, ponieważ komunikowanie się za pomocą nowych technologii i przestępstwa popełniane z ich wykorzystaniem generalnie wymykają się spod kontroli społeczeństwa. Niejednokrotnie utrudnia to ustalenie

tożsamości osób naruszających prawo, a w konsekwencji zapobieżenie i wykrycie takich zagrożeń.

Rozwój technologiczny doprowadził zarazem, z jednej strony, do wykształcenia się nowych form popełniania „tradycyjnych" przestępstw. Internet i środki komunikowania się na odległość są dodatkowym, specjalistycznym narzędziem w rękach przestępców, istniejącym niejako równolegle do dotychczas wykorzystywanych technik. Z drugiej strony, wykształciły się nowe, nieistniejące wcześniej rodzaje przestępstw, możliwe do popełnienia wyłącznie z użyciem nowych technologii (tzw. cyberprzestępczość związana m.in. z nieuprawnionym dostępem do danych komputerowych).

1.7. Trybunał Konstytucyjny przyjmuje, że zasygnalizowana wyżej specyfika nowych technologii i ocena zagrożeń z nimi związanych uzasadnia powierzenie wyspecjalizowanym organom władzy publicznej, jakimi są służby policyjne i służby ochrony państwa (*vide:* art. 103 ust. 2 Konstytucji), adekwatnych uprawnień, dzięki którym będą one w stanie zapobiegać przestępstwom i je wykrywać, ścigać ich sprawców, a także dostarczać informacji na temat zagrożeń dóbr prawnie chronionych. Demokratyczne państwo prawne nie może bowiem ignorować rosnącego znaczenia nowych technologii, a ponadto skali ich wykorzystywania, niekiedy również w celu naruszania prawa. Wymaga to wyposażenia tych służb w stosowne uprawnienia i stworzenia im warunków finansowych i organizacyjnych, umożliwiających efektywną walkę z naruszeniami prawa. Organy władzy publicznej powinny dysponować prawną i faktyczną możliwością wykrywania popełnianych przestępstw i działalności skierowanej przeciwko państwu czy jego konstytucyjnym organom. Powinny one też móc wyprzedzać działania osób naruszających prawo, nie dopuszczając do wystąpienia zagrożeń. W warunkach globalnej przestępczości i przekraczającego granice państw terroryzmu czy przestępczości zorganizowanej istotna jest także prewencja zagrożeń, których wystąpienie może wyrządzić nieodwracalne straty dla dóbr prawnie chronionych.

Zdaniem Trybunału brak wyposażenia służb policyjnych oraz służb ochrony państwa w możliwość korzystania ze zdobyczy nowoczesnej techniki, a nawet wyposażenie ich w taką możliwość, lecz w niewystarczającym zakresie, może oznaczać niewywiązanie się państwa z jego konstytucyjnego zadania strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli (art. 5 Konstytucji), czy naruszać zasadę sprawności działania instytucji publicznych (wstęp do Konstytucji). Niekiedy może powodować naruszenie obowiązków wiążących Polskę umów międzynarodowych zobowiązujących do współdziałania w walce z międzynarodową przestępczością i terroryzmem.

Dostrzegając rolę nowych technologii teleinformatycznych w pozyskiwaniu wiedzy o działalności przestępczej, ustawodawca uprawniający służby policyjne oraz służby ochrony państwa do niejawnego uzyskiwania informacji i dowodów za pomocą nowych technologii nie może ignorować specyfiki naruszeń prawa dokonanych z ich wykorzystaniem ani skali zjawiska w polskich realiach. Nie ma bowiem żadnego znaczenia, czy podobne rozwiązania funkcjonują w innych państwach (zob. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 3.1).

1.8. Trybunał Konstytucyjny zwraca uwagę na jeszcze jedną okoliczność. Ciążący na organach państwa obowiązek zagwarantowania wolności i praw oznacza nie tylko zakaz nadmiernej ingerencji, w tym polegającej na niejawnym pozyskiwaniu przez organy państwa informacji o osobach, ale ma szerszy wymiar. Zdaniem Trybunału, wynika z niego obowiązek stworzenia przez państwo warunków, w których obywatele z zagwarantowanych im wolności i praw mogą swobodnie korzystać. Warunkiem

zapewnienia wolności i praw jest zaś poczucie bezpieczeństwa w państwie i braku zagrożeń obywateli. Osiągnięcie tego stanu możliwe jest m.in. przez zwalczanie przestępczości mogącej zagrażać wolności człowieka, korzystaniu z własności czy podejmowaniu działalności gospodarczej. Z drugiej strony, zdaniem Trybunału, korelatem konstytucyjnego obowiązku państwa, o którym mowa w art. 5 Konstytucji, jest także prawo obywateli do ochrony ich bezpieczeństwa przed zewnętrznymi i wewnętrznymi zagrożeniami, w tym terroryzmem i przestępczością. Nie istnieje zatem niedająca się przezwyciężyć „naturalna antynomia" między zapewnieniem bezpieczeństwa i porządku publicznego a ochroną wolności i praw konstytucyjnych. Niekiedy bowiem wykorzystanie niejawnych metod pracy operacyjnej umożliwia ograniczenie skali przestępczości, a to przekłada się na podniesienie stopnia poczucia bezpieczeństwa obywateli i większą swobodę korzystania z zagwarantowanych im wolności i praw.

1.9. Jednym z powszechnie uznanych instrumentów wykrywania zagrożeń i ścigania naruszeń prawa są czynności operacyjno-rozpoznawcze. Obejmują m.in. kontrolę operacyjną (w szczególności z wykorzystaniem środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, przekazywanych za pomocą sieci telekomunikacyjnych), a także gromadzenie i przetwarzanie danych telekomunikacyjnych. Najogólniej rzecz ujmując, czynności te mają umożliwiać zapobieganie i zwalczanie zagrożeń w stopniu dotąd niespotykanym i niemożliwym do osiągnięcia za pomocą tradycyjnych metod analizy kryminalnej i pracy wywiadowczej (zob. szerzej cz. III, pkt 6 uzasadnienia wyroku).

Po pierwsze, znacznie ułatwiają walkę z tradycyjną przestępczością, gdyż komunikaty przekazywane za pośrednictwem sieci teleinformatycznych w postaci rozmów telefonicznych, wiadomości tekstowych lub multimedialnych, a nawet metadane dotyczące nawiązywanego połączenia (dane o ruchu i lokalizacji) pozwalają na rekonstrukcję społecznych zachowań jednostek objętych obserwacją, bez potrzeby osobistego prowadzenia działań operacyjnych wymagających zaangażowania wielu osób, długiego czasu oraz ponadprzeciętnej ostrożności przed dekonspiracją. Analiza materiałów zgromadzonych w kontroli operacyjnej, czy analiza danych telekomunikacyjnych umożliwia uzyskanie materiałów o unikatowym znaczeniu, pozwalając na precyzyjną rekonstrukcję procesów decyzyjnych w grupach przestępczych oraz wzajemnych powiązań między komunikującymi się osobami. Ponadto, analiza takich danych umożliwia błyskawiczne wykrycie sprawców zagrożenia istotnych dóbr, jak życie albo zdrowie jednostek. Należy mieć też na uwadze, że nowe technologie wykorzystywane w toku czynności operacyjno-rozpoznawczych umożliwiają utrwalenie i następcze zrekonstruowanie treści wiadomości głosowych, tekstowych lub multimedialnych przekazywanych za pomocą sieci telekomunikacyjnych. Możliwe jest dzięki nim pozyskanie wiedzy, która dotychczas nie była dostępna organom państwa.

Po drugie, nowe technologie stanowią w zasadzie jedyny sposób umożliwiający walkę z szeroko rozumianą tzw. cyberprzestępczością, to znaczy przestępstwami popełnianymi z wykorzystaniem nowych technologii teleinformatycznych. Zastosowanie czynności operacyjno-rozpoznawczych jest nie tyle udogodnieniem w pracy operacyjnej, lecz stanowi w większości wypadków praktycznie jedyny sposób zapobieżenia przestępstwu lub wykrycia ich sprawców.

Dostrzegając odmienności związane z wykorzystywaniem nowych technologii w celu popełniania tradycyjnych przestępstw i w celu popełniania szeroko rozumianych przestępstw komputerowych, niezbędne jest, zdaniem Trybunału, wypracowanie zróżnicowanego podejścia do oceny proporcjonalności przepisów uprawniających do stosowania nowych technologii dla zapobiegania naruszeniom prawa, ich zwalczania i

wykrywania, w zależności od sposobu użycia nowych technologii w celach niezgodnych z prawem.

1.10. Umożliwienie służbom policyjnym i ochrony państwa pozyskiwania wiedzy o treści, czasie i formach komunikowania się jednostek, a także monitorowania ich aktywności życiowej w inny sposób, nieuchronnie popada w kolizję z prawem do ochrony prywatności, ochroną tajemnicy komunikowania się, autonomią informacyjną, a w niektórych wypadkach (podsłuchu lub monitoringu zainstalowanego w mieszkaniu) z nienaruszalnością mieszkania. Co więcej, samo istnienie przepisów uprawniających organy władzy wykonawczej do takiego rodzaju czynności winno być postrzegane jako ingerencja w konstytucyjnie chroniony status człowieka i obywatela, którego źródłem jest przyrodzona i niezbywalna godność. Prawna dopuszczalność pozyskiwania informacji o jednostkach, niekiedy o sferach istotnych z punktu widzenia ich uczestnictwa w życiu publicznym, negatywnie wpływa na korzystanie przez nie z konstytucyjnych wolności i praw. Niezależnie od konkretnych, niekiedy zróżnicowanych form wkroczenia w sferę życia prywatnego, sama nawet świadomość znajdowania się pod ciągłym nadzorem władz publicznych może zniechęcać jednostki do swobodnego korzystania z zagwarantowanych im konstytucyjnych wolności i praw. Może to rodzić obawy, że organy władzy publicznej będą w nieuprawniony sposób gromadzić i wykorzystywać informacje o osobach. Obawy te są wyjątkowo silne w polskim społeczeństwie, które przez dziesięciolecia reżimu komunistycznego było inwigilowane przez tajne służby bezpieczeństwa, najczęściej nie służące dobrze rozumianym interesom własnego państwa i jego współobywateli.

Z punktu widzenia konstytucyjnych gwarancji prawa do ochrony prywatności, a także ochrony tajemnicy komunikowania się, zdaniem Trybunału, ingerencją władzy publicznej w tę sferę jest nie tylko pozyskanie przez władze publiczne danych o jednostce po raz pierwszy. Ochrona prawa do prywatności i tajemnicy komunikowania się rozciąga się bowiem na cały proces pozyskiwania, gromadzenia, przechowywania oraz przetwarzania (w tym analizowania i porównywania) informacji o jednostkach. Dlatego też jako odrębne przejawy ingerencji w konstytucyjnie chroniony status jednostki – wymagające każdorazowo odrębnej legitymizacji konstytucyjnej – należałoby traktować pozyskiwanie informacji m.in. o treści komunikatów przekazywanych za pomocą sieci teleinformatycznych w toku kontroli operacyjnej, nałożenie na dostawców usług telekomunikacyjnych obowiązku zatrzymywania danych o ruchu i lokalizacji, dostęp do tych danych, ich następczą weryfikację czy przekazanie innym organom (por. wyrok Federalnego Sądu Konstytucyjnego Niemiec z 2 marca 2010 r., sygn. 1 BvR 256/08, pkt 190).

1.11. Powierzenie służbom odpowiedzialnym za bezpieczeństwo i porządek publiczny kompetencji do niejawnego pozyskiwania informacji o jednostkach zasadniczo jest powiązane z utworzeniem zbiorów danych o osobach poddanych kontroli. Zbiory te mają zróżnicowany charakter i strukturę. Mogą służyć przechowywaniu i analizowaniu danych zgromadzonych przez same służby podczas wykonywanych czynności. Mogą być również zbiorami danych prowadzonymi przez podmioty publiczne i prywatne, z których służby korzystają następczo w celu realizowania powierzonych im ustawowo zadań. Zdaniem Trybunału prawna możliwość przechowywania danych o jednostkach w stosownych rejestrach i zbiorach – jeżeli dane te są gromadzone w celu realizowania zadań publicznych, w tym zapobiegania, zwalczania albo wykrywania przestępczości – pozostaje w konflikcie z autonomią informacyjną jednostki i jej prawem do ochrony życia prywatnego.

Trybunał Konstytucyjny zwraca w tym kontekście szczególną uwagę na dalekosiężne i dotkliwe skutki prewencyjnego przechowywania danych telekomunikacyjnych (tzw. danych o ruchu i lokalizacji). Świadomość istnienia rejestrów,

w których gromadzone są choćby tylko dane o ruchu i lokalizacji użytkowników korzystających z sieci teleinformatycznych, sama w sobie poważnie narusza prawa podstawowe. Stwarza bowiem wrażenie znajdowania się pod nieustannym nadzorem. Ponadto wejście w posiadanie stosownych danych o jednostce przez funkcjonariuszy służb następuje w sposób praktycznie niezauważalny dla zainteresowanego. Zazwyczaj nie wie on nawet, że dane dotyczące jego osoby zostały pozyskane lub zatrzymane ani jak szeroka jest wiedza służb policyjnych bądź służb ochrony państwa na jego temat, czy w jakich sytuacjach wiedza ta zostanie potem wykorzystana.

Chociaż na podstawie pojedynczych danych, w tym danych telekomunikacyjnych, zebranych w toku czynności operacyjno-rozpoznawczych, nie sposób jeszcze zrekonstruować całej społecznej aktywności jednostek, to po szczegółowej ich analizie możliwe jest zbudowanie profilu osobowego osób uczestniczących w procesie komunikacji, a co za tym idzie ustalanie ich trybu życia, przynależności do organizacji społecznych czy politycznych, kontaktów z takimi organizacjami, a także osobistych upodobań i skłonności osób poddanych obserwacji (zob. np. wyrok TSUE z 8 kwietnia 2014 r., sygn. C-293/12, pkt 27). Niewątpliwie powierzenie służbom policyjnym i służbom ochrony państwa możliwości pozyskiwania danych o ruchu i lokalizacji ułatwia i przyspiesza walkę z przestępczością, niemniej bardzo intensywnie ingeruje w sferę prywatności jednostki. Dlatego także przepisy regulujące dostęp do takich danych wymagają uzasadnienia w świetle zasady proporcjonalności.

Gromadzenie i przetwarzanie danych w rozmaitych zautomatyzowanych bazach rodzi jeszcze inne zagrożenie konstytucyjnych wolności i praw człowieka i obywatela. Istnieje bowiem niebezpieczeństwo wycieku informacji spowodowanego zachowaniami podmiotów odpowiedzialnych za ich gromadzenie, jak też ograniczonymi możliwościami zabezpieczeń technicznych. Skoro w obowiązującym reżimie prawnym dane telekomunikacyjne określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, ze zm.; dalej: prawo telekomunikacyjne) są zatrzymywane i przechowywane w bazach administrowanych i finansowanych przez prywatnych dostawców usług telekomunikacyjnych (art. 180d prawa telekomunikacyjnego), a zatem podmiotów funkcjonujących w warunkach rynkowej presji kosztów, znacząco rośnie ryzyko niedostatecznego zabezpieczenia ich przed nieuprawnionym dostępem osób trzecich.

1.12. Konstytucyjne prawo do ochrony prywatności – jakkolwiek nie jest absolutne – ma charakter szczególny w systemie wolności i praw konstytucyjnych. Jak już wspomniano, wynika to ze szczególnego zakotwiczenia tej wartości w godności człowieka. Świadczy o tym również art. 233 ust. 1 Konstytucji, jednoznacznie zawężający swobodę ustawodawcy w zakresie ograniczania tego prawa, nawet w stanie wojennym i wyjątkowym. Z uwzględnieniem tych ogólnych wskazań, płynących z umiejscowienia i rangi prawa do ochrony prywatności wśród gwarantowanych konstytucyjnie wolności i praw, należy oceniać regulacje ustanawiające wyjątki od chronionej prywatności (zob. wyrok z 20 marca 2006 r., sygn. K 17/05, OTK ZU nr 3/A/2006, poz. 30, cz. III, pkt 3).

Mając powyższe na uwadze, pozyskiwanie informacji o życiu prywatnym jednostek przez organy władzy publicznej, zwłaszcza niejawnie, musi być ograniczone do koniecznych sytuacji, dopuszczalnych w demokratycznym państwie wyłącznie dla ochrony konstytucyjnie uznanych wartości i zgodnie z zasadą proporcjonalności. Warunki gromadzenia i przetwarzania tych danych przez władze publiczne muszą być unormowane w ustawie w sposób jak najbardziej przejrzysty, wykluczający arbitralność i dowolność ich stosowania.

Choć czynności operacyjno-rozpoznawcze popadają w konflikt z prawem do ochrony prywatności, wolnością i ochroną tajemnicy komunikowania się czy autonomią informacyjną, mogą być uznane za konieczne w demokratycznym państwie prawa z uwagi na ochronę bezpieczeństwa państwa, porządku publicznego bądź ochronę wolności i praw innych osób. Dopuszczalność stosowania kontroli operacyjnej, a także gromadzenia i przetwarzania danych telekomunikacyjnych zależy od przestrzegania konstytucyjnych wymagań, mających chronić jednostki przed ekscesami w stosowaniu prawa i nadmiernym wkroczeniem w sferę ich prywatności, a ponadto zabezpieczać przed wpływaniem służb policyjnych i ochrony państwa na demokratyczny mechanizm sprawowania władzy w państwie. Wymagania te są, zdaniem Trybunału Konstytucyjnego, tym surowsze, im bardziej dane czynności – w szczególności prowadzone w warunkach niejawności oraz poza ramami postępowania sądowego – ingerują w konstytucyjnie chroniony status człowieka i obywatela.

1.13. Trybunał zwraca uwagę na jeszcze jedną kwestię, mającą istotne znaczenie w dobie globalizacji i międzynarodowej przestępczości. Organy władzy publicznej zobowiązane są do ochrony prywatności własnych obywateli również przed zagrożeniami płynącymi spoza samego państwa. Obowiązek państwa rozciąga się w konsekwencji na zapewnienie ochrony prywatności przed monitorowaniem rozmaitych sfer aktywności życiowej obywateli, w tym wiadomości przesyłanych za pomocą sieci telekomunikacyjnych przez podmioty zagraniczne, a zwłaszcza państwa obce. Naruszenie prawa do ochrony prywatności zagwarantowanego w art. 47 Konstytucji może bowiem nastąpić nie tylko przez bezpośrednie działanie polskich organów państwa, pozyskujących informacje o jednostkach w sposób niejawny. Nastąpi to również w sytuacji braku dostatecznej ochrony obywateli przez państwo przed ingerencją w tę wolność, spowodowaną działaniami innych podmiotów.

Trybunał Konstytucyjny podkreśla, że ingerencja władzy publicznej w prywatność czy autonomię informacyjną jednostek jest dopuszczalna wyłącznie na zasadach określonych w Konstytucji, co w pełni dotyczy podejmowania zobowiązań międzynarodowych przez władze Rzeczypospolitej Polskiej.

1.14. Niezależnie od szczegółowych formalnych i materialnych wymagań, jakim muszą sprostać regulacje dotyczące czynności operacyjno-rozpoznawczych umożliwiających niejawne pozyskiwanie informacji o jednostkach, nie jest dopuszczalne w demokratycznym państwie prawnym rejestrowanie całokształtu życia prywatnego jednostek, zwłaszcza w sposób umożliwiający rekonstrukcję wszelkich przejawów ich życiowej aktywności. Stanowiłoby to naruszenie istoty prawa do prywatności, tajemnicy komunikowania się i autonomii informacyjnej, czego bezwzględnie zabrania art. 31 ust. 3 zdanie drugie Konstytucji.

2. Wybrane orzecznictwo Europejskiego Trybunału Praw Człowieka w Strasburgu.

2.1. Ochronę prywatności jednostki w systemie Rady Europy gwarantuje art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962, z 2001 r. Nr 23, poz. 266, z 2003 r. Nr 42, poz. 364 oraz z 2010 r. Nr 90, poz. 587; dalej: Konwencja), w myśl którego każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Warunki ograniczania tego prawa ustanawia z kolei art. 8 ust. 2

Konwencji, zgodnie z którym niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa wyrażonego w art. 8 ust. 1, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Przepis art. 8 ust. 1 Konwencji dotyczy szeroko rozumianego prawa do poszanowania prywatnej sfery życia człowieka, stanowiąc tym samym najbardziej ogólną afirmację autonomii jednostki w zakresie kształtowania wszelkich aspektów jej życia oraz własnej osobowości. Istotą tego prawa jest zapewnienie każdej jednostce sfery prywatności (autonomii) chronionej przed ingerencją zewnętrzną, pochodzącą zarówno od państwa, jak i podmiotów prywatnych (zob. np. L. Garlicki, uwaga 21 do art. 8, [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1-18*, red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010, s. 491).

Przepis art. 8 ust. 1 Konwencji wskazuje cztery podstawowe dziedziny podlegające ochronie prawnej, a mianowicie: życie prywatne, życie rodzinne, mieszkanie i korespondencja. Sfery prywatności wymienione w tym przepisie nie mogą być ujmowane rozłącznie, lecz w pewnym zakresie nakładają się na siebie, tworząc tym samym szereg szczegółowych praw i odpowiadających im negatywnych i pozytywnych obowiązków władzy publicznej. Ich celem jest w konsekwencji ochrona godności człowieka i jego wolności (zob. L. Garlicki, tamże).

W świetle orzecznictwa ETPC kwestie związane z wkroczeniem państwa w sferę prywatności wynikającą z zastosowania środków niejawnego pozyskiwania informacji o osobach były rozpatrywane przede wszystkim jako ingerencja w „życie prywatne" i „korespondencję". Pojęcie „życia prywatnego", o którym mowa w art. 8 ust. 1, nie może być redukowane do spraw ściśle osobistych i wewnętrznych człowieka, lecz powinno być rozumiane także w wymiarze społecznym, jako możność rozwijania kontaktów z innymi i interakcji ze światem zewnętrznym. Z kolei „korespondencja" obejmuje rozmaite sposoby wymiany wiadomości między oznaczonymi podmiotami, zarówno w postaci pisemnej, jak i za pośrednictwem faksu, poczty elektronicznej czy innych kanałów transmisji danych w ramach sieci internetowej. W orzecznictwie strasburskim nie wykluczono równocześnie, by zastosowanie podsłuchu rozmów stanowiło ingerencję w prawo do poszanowania mieszkania (zob. orzeczenie ETPC z 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom, skarga nr 5029/71, § 41 uzasadnienia).

2.2. Europejski Trybunał Praw Człowieka nie zanegował dopuszczalności niejawnego pozyskiwania informacji o osobach przez władze publiczne. Wskazywał wręcz na ich niezbędność, jako narzędzia umożliwiającego efektywne zagwarantowanie bezpieczeństwa oraz ochronę instytucji demokratycznego państwa przed wyrafinowanymi formami zagrożeń, zwłaszcza szpiegostwem czy terroryzmem (zob. m.in. orzeczenie ETPC z 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom, § 48 uzasadnienia). Niemniej jednak przejawy niejawnego pozyskiwania informacji o jednostkach, a nawet obowiązywanie przepisów dopuszczających inwigilację, koliduje z prawem jednostek wynikającym z art. 8 Konwencji. Wpływa bowiem na wolność komunikowania się użytkowników usług telekomunikacyjnych, i to niezależnie od tego, czy przewidziane prawem środki niejawnego pozyskiwania informacji wobec konkretnych podmiotów zastosowano (zob. orzeczenia ETPC z 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom, § 41 uzasadnienia; 24 kwietnia 1990 r. w sprawie Kruslin przeciwko Francji, skarga nr 11801/85, § 26 uzasadnienia; 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00, § 77-79 uzasadnienia; 3 kwietnia

2007 r. w sprawie Copland przeciwko Wielkiej Brytanii, skarga nr 62617/00, § 43-44 uzasadnienia; 1 lipca 2007 r. w sprawie Liberty i inni przeciwko Wielkiej Brytanii, skarga nr 58243/00, § 56 uzasadnienia; 28 czerwca 2007 r. w sprawie Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii, skarga nr 62540/00, § 69 uzasadnienia; 10 lutego 2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, skarga nr 25198/02, § 34 uzasadnienia; 23 października 2012 r. w sprawie Hadzhiev przeciwko Bułgarii, skarga nr 22373/04, § 44 uzasadnienia; 4 grudnia 2012 r. w sprawie Lenev przeciwko Bułgarii, skarga nr 41452/07, § 144 uzasadnienia).

2.3. Na tle spraw rozpoznawanych przez ETPC problem ingerencji w prawo do poszanowania życia prywatnego i korespondencję, o którym mowa w art. 8 ust. 1 Konwencji, w związku ze stosowaniem środków inwigilacji (ang. *secret surveillance measures*), najczęściej wynikał ze stosowania przez organy państwa rozmaitych form podsłuchu telefonicznego i stacjonarnego (rozmów telefonicznych, rozmów w pomieszczeniach). Europejski Trybunał Praw Człowieka wielokrotnie stwierdzał, że niejawne przechwytywanie rozmów stanowi ingerencję w prawo wyrażone w art. 8 ust. 1 Konwencji (zob. orzeczenia ETPC z 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom, § 41 uzasadnienia; 16 lutego 2000 r. w sprawie Amann przeciwko Szwajcarii, skarga nr 27798/95, § 56 uzasadnienia; 10 lutego 2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, § 29 uzasadnienia; 27 października 2012 r. w sprawie Savovi przeciwko Bułgarii, skarga nr 7222/05, § 52 uzasadnienia; 25 czerwca 2013 r. w sprawie Valentino Acatrinei przeciwko Rumunii, skarga nr 18540/04, § 57-58 uzasadnienia). Stosowanie urządzeń podsłuchowych narusza prawa wszystkich tych osób, które korzystają z telefonu objętego podsłuchem bądź znajdują się w pomieszczeniu, w którym zainstalowano podsłuch, choćby nawet inwigilacja nie była skierowana bezpośrednio przeciwko nim (zob. orzeczenia ETPC z 24 kwietnia 1990 r. w sprawie Kruslin przeciwko Francji, § 26 uzasadnienia; 25 września 2001 r. w sprawie P. G. i J. H. przeciwko Wielkiej Brytanii, skarga nr 44787/98, § 37-38 uzasadnienia). Za ingerencję w prawo gwarantowane w art. 8 Konwencji uznano także stosowanie urządzenia podsłuchowego zainstalowanego na ciele osoby, w celu zarejestrowania prowadzonych przez nią rozmów z innymi podmiotami (zob. orzeczenie ETPC z 1 marca 2007 r. w sprawie Heglas przeciwko Czechom, skarga nr 5935/02).

2.3.1. Ochrona wynikająca z art. 8 ust. 1 Konwencji rozciąga się nie tylko na treść rozmów telefonicznych (i innych form przekazywania informacji jak np. poczta, faks, czy e-mail), ale też obejmuje swym zakresem informacje dotyczące dat oraz długości rozmów telefonicznych, a ponadto danych połączeń przychodzących i wychodzących, czyli informacji zawartych w tzw. bilingach. Dane te stanowią integralny element komunikacji telefonicznej (ang. *integral element in the communications made by telephone* – zob. np. orzeczenia ETPC z 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79, § 83-85; 25 września 2001 r. w sprawie P. G. i J. H. przeciwko Wielkiej Brytanii, § 42 uzasadnienia; 1 marca 2007 r. w sprawie Heglas przeciwko Czechom, § 60-61 uzasadnienia; 3 kwietnia 2007 r. w sprawie Copland przeciwko Wielkiej Brytanii, § 43-44 uzasadnienia), a ich pozyskiwanie musi być rozpatrywane, co do zasady, jako ingerencja w prawo wyrażone w art. 8 ust. 1 Konwencji. W wyroku w sprawie Malone przeciwko Wielkiej Brytanii ETPC podkreślił, że pozyskiwanie danych zawartych w tzw. bilingach nie może wprawdzie być utożsamiane z podsłuchem rozmów telefonicznych, jednakże ujawnienie policji tego rodzaju danych bez zgody abonenta powinno być traktowane jako równoważne ingerencji w prawo zagwarantowane w art. 8 ust. 1 Konwencji (§ 84 uzasadnienia ww. orzeczenia). Podobne stanowisko zajął ETPC w sprawie Copland przeciwko Wielkiej Brytanii, rozpoznając sprawę pracownicy

publicznego *college* (chodziło o to, że pracodawca monitorował jej służbowy telefon i komputer). Europejski Trybunał Praw Człowieka uznał, że gromadzenie i przechowywanie osobistych informacji na temat skarżącej bez jej wiedzy, a związanych z korzystaniem przez nią ze służbowego telefonu, poczty elektronicznej czy Internetu stanowi ingerencję w prawo określone art. 8 ust. 1 Konwencji, nawet jeśli powyższe dane mogłoby zostać legalnie pozyskane na podstawie analizy rachunków telefonicznych (zob. § 43-44 uzasadnienia ww. orzeczenia). Natomiast w wyroku w sprawie P. G. i J. H. przeciwko Wielkiej Brytanii Europejski Trybunał Praw Człowieka zwrócił uwagę, że nie w każdym wypadku pozyskiwanie danych zawartych w bilingach stanowi naruszenie art. 8 ust. 1 Konwencji i powinno być w związku z tym utożsamiane z przechwytywaniem rozmów. Zdaniem ETPC nie narusza art. 8 Konwencji korzystanie z bilingów, a co za tym idzie – przetwarzanie zawartych w nich danych dla celów rozliczeniowych przez przedsiębiorców telekomunikacyjnych (zob. § 42 uzasadnienia ww. orzeczenia).

2.3.2. Ingerencję w życie prywatne i korespondencję stanowią nie tylko indywidualne środki niejawnej kontroli skierowane przeciwko oznaczonym podmiotom, ale też strategiczny monitoring połączeń i pozyskiwanie związanych z tym danych osobowych komunikujących się podmiotów. Kwestia ta była rozpatrywana w sprawie Weber i Saravia przeciwko Niemcom, w której zakwestionowano niemieckie przepisy regulujące strategiczny monitoring połączeń telekomunikacyjnych polegający na utrwalaniu rozmów telefonicznych nieoznaczonego kręgu rozmówców, a następnie identyfikowaniu, za pomocą słów kluczy, informacji zawartych w tych rozmowach, które mogą potencjalnie identyfikować sprawców przestępstw lub plany ich popełnienia. W ocenie ETPC doszło do ingerencji w „tajemnicę telekomunikacyjną" (ang. *secrecy of telecomunications*) chronioną przez art. 8 Konwencji (zob. § 76 uzasadnienia ww. orzeczenia), chociaż spełnia ona wszystkie wymagania jej dopuszczalności wynikające z Konwencji. Europejski Trybunał Praw Człowieka przychylił się zarazem do poglądu Federalnego Sądu Konstytucyjnego Niemiec, potwierdzając, że również na gruncie Konwencji każde przekazywanie zgromadzonych danych i ich wykorzystywanie przez inne służby państwowe w celu wszczęcia i prowadzenia postępowania karnego stanowi kolejną odrębną ingerencję (ang. *further separate interference*) w prawo gwarantowane w art. 8 Konwencji (§ 79 uzasadnienia ww. orzeczenia).

2.3.3. W świetle orzecznictwa ETPC ingerencją w sferę prywatności jednostek będzie także stosowanie przez organy władzy publicznej rozmaitych specjalnych środków inwigilacji (ang. *special means of surveillance*), takich jak urządzenia techniczne umożliwiające m.in. niejawne rejestrowanie dźwięku oraz obrazu, w tym robienie zdjęć i filmowanie (zob. przede wszystkim w sprawach dotyczących przepisów bułgarskich: orzeczenia ETPC z 28 czerwca 2007 r. w sprawie Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii; 23 października 2012 r. w sprawie Hadzhiev przeciwko Bułgarii).

2.3.4. Ingerencją w prawo zagwarantowane w art. 8 Konwencji jest także stosowanie środków niejawnego monitorowania obecności jednostki w przestrzeni publicznej. W wyroku z 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05, ETPC oceniał dopuszczalność instalowania urządzenia GPS (ang. *Global Positioning System*) w samochodzie należącym do osoby trzeciej – wspólnika skarżącego. Zebrane w ten sposób informacje były wykorzystane w postępowaniu karnym jako dowody przestępstw zarzucanych skarżącemu. Choć ostatecznie ETPC nie stwierdził naruszenia art. 8 Konwencji, uznawszy obowiązujące w niemieckim systemie prawnym gwarancje proceduralne za wystarczające, to jednak zwrócił uwagę, że inwigilacja za pomocą GPS ze swej natury różni się od pozostałych form wizualnej lub akustycznej kontroli. Ma bowiem na celu rejestrowanie przemieszczania się jednostek w przestrzeni, co

do zasady, publicznie dostępnej dla innych. Pozyskiwanie w ten sposób informacji ma charakter systematyczny, pozwalając precyzyjnie ustalić m.in. schematy poruszania się czy ułatwiać dalsze gromadzenie dowodów bez narażenia się na dekonspirację. Europejski Trybunał Praw Człowieka zwrócił uwagę, że takie systematyczne gromadzenie i przechowywanie danych może być uznawane za ingerujące w prawo wyrażone w art. 8 ust. 1 Konwencji.

2.3.5. W świetle orzecznictwa ETPC ingerencją w sferę prywatności jednostki jest też gromadzenie i przechowywanie danych na temat jednostek przez służby państwowe, niezależnie od sposobu, w jaki zostały zgromadzone (zob. orzeczenia ETPC z 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii, skarga nr 28341/95, § 43-44 uzasadnienia oraz 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, § 46 uzasadnienia). ETPC zwracał uwagę, że wystarczające dla stwierdzenia ingerencji w prawo zagwarantowane przez art. 8 Konwencji jest zgromadzenie danych o jednostkach, bez względu na to, w jaki sposób będą one w przyszłości wykorzystane.

2.4. Mając powyższe na uwadze, ETPC sformułował szereg warunków, którym muszą odpowiadać unormowania dotyczące inwigilacji, by mogły być uznane za zgodne z art. 8 Konwencji. Orzecznictwo to można uznać za dostatecznie utrwalone i tworzące pewien minimalny standard, który musi być przestrzegany w państwach członkowskich Rady Europy. Należy podkreślić, że standardy wypracowane w orzecznictwie ETPC w odniesieniu do poszczególnych rodzajów niejawnego pozyskiwania informacji są zróżnicowane. Europejski Trybunał Praw Człowieka wskazywał konieczność zachowania surowszych wymagań odnoszących się do jakości regulacji podsłuchów oraz przechwytywania informacji stanowiących integralny element porozumiewania się za pomocą sieci teleinformatycznych, tj. szeroko rozumianego przechwytywania obrazu i dźwięku, niż w wypadku monitorowania aktywności jednostek w przestrzeni publicznie dostępnej za pomocą urządzeń lokalizacyjnych (zob. orzeczenie ETPC z 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, § 66 uzasadnienia). Inwigilacja za pomocą GPS stanowić ma bowiem, zdaniem ETPC, mniej dolegliwą dla jednostki ingerencję w życie prywatne, niż pozyskiwanie treści korespondencji, za pośrednictwem której przekazywane bywają informacje intymne.

2.4.1. Przede wszystkim ingerencja państwa w sferę prywatności jednostki musi mieć dostatecznie precyzyjną podstawę w obowiązującym prawie. Prawo ma jednocześnie spełniać wymogi jakościowe, a zatem być dostępne oraz przewidywalne dla jednostek. To nie znaczy – jak podkreślał ETPC – jakoby jednostka mogła przewidzieć dokładny moment ingerencji w jej wolności lub prawa. Z prawa mają natomiast wynikać okoliczności i warunki, w których władze publiczne są uprawnione do pozyskiwania informacji na temat jednostek w ten sposób (zob. orzeczenie ETPC z 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, § 93 uzasadnienia i przywołane tam orzecznictwo). Jest to tym bardziej istotne, jeśli pozyskiwanie informacji o jednostkach dokonuje się niejawnie i przy użyciu wyrafinowanych urządzeń technicznych (tamże). Precyzja regulacji prawnej tej materii ma bowiem zapobiegać ryzyku arbitralności niejawnych działań podejmowanych przez organy władzy publicznej, które z natury rzeczy pozostają poza zasięgiem kontroli publicznej (zob. § 94 uzasadnienia ww. orzeczenia).

2.4.2. W orzecznictwie dotyczącym podsłuchów rozmów, a także przechwytywania informacji stanowiących integralny element procesu komunikowania się Europejski Trybunał Praw Człowieka wskazał, że minimalnym standardem konwencyjnym regulacji tej materii jest określenie w prawie:

– rodzaju przestępstw (ang. *nature of the offences*), w odniesieniu do których organy państwa mogą pozyskiwać niejawnie informacje o osobach; nie jest przy tym

wystarczające, aby prawodawca wskazał, że chodzi o poważne przestępstwa, nawet jeśli definiuje to pojęcie w ustawie. W sprawie Iordachi i inni przeciwko Mołdawii ETPC stwierdził naruszenie art. 8 Konwencji, ponieważ mołdawskie przepisy umożliwiały stosowanie podsłuchu m.in. w celu zapobiegania poważnym, bardzo poważnym i wyjątkowo poważnym przestępstwom, a zatem przestępstwom zagrożonym zgodnie z tamtejszym prawem karą pozbawienia wolności do 15 lat lub surowszą. W świetle przedstawionych statystyk zarządzenie tego rodzaju kontroli było możliwe w odniesieniu aż w ok. 60% przestępstw stypizowanych w ustawie karnej (§ 44 uzasadniania ww. orzeczenia). Prawodawstwo nie precyzowało także przesłanek zarządzenia kontroli rozmów, jakimi były wówczas „bezpieczeństwo narodowe", „porządek publiczny", „ochrona zdrowia", „ochrona moralności", „ochrona praw i interesów innych osób", „interes gospodarczy kraju", „utrzymanie porządku prawnego" (§ 46 uzasadnienia ww. orzeczenia). Europejski Trybunał Praw Człowieka uznał takie rozwiązanie za niewystarczające z punktu widzenia „jakości regulacji prawnej ingerencji". Nie stwierdzono z kolei naruszenia art. 8 Konwencji przez przepisy niemieckie regulujące strategiczny monitoring połączeń telekomunikacyjnych. Dotyczyły bowiem 6 rodzajów najpoważniejszych i precyzyjnie zdefiniowanych w prawie krajowym przestępstw, do których zaliczały się: zbrojna napaść na RFN, międzynarodowe ataki terrorystyczne w RFN, międzynarodowy handel bronią oraz zakazany handel zagraniczny towarami, programami lub technologiami o istotnym znaczeniu dla bezpieczeństwa; import narkotyków w znacznych ilościach do RFN; fałszowanie pieniędzy popełnione za granicą oraz pranie pieniędzy (zob. § 27 i § 96 uzasadnienia orzeczenia w sprawie Weber i Saravia przeciwko Niemcom). Z reguły w sprawach rozpoznawanych przez ETPC stosowanie przez organy państwa niejawnych środków pozyskiwania informacji miało miejsce w związku z podejrzeniem poważnych przestępstw (np. handlu narkotykami – orzeczenia ETPC z 22 października 2002 r. w sprawie Taylor-Sabori przeciwko Wielkiej Brytanii, nr skargi 47114/99; 12 maja 2000 r. w sprawie Khan przeciwko Wielkiej Brytanii, nr skargi 35394/97, kradzieży mienia o wartości około 9000 euro – w sprawie Heglas przeciwko Czechom; zamachu bombowego i zaangażowania w działalność organizacji terrorystycznej – w sprawie Uzun przeciwko Niemcom);

– rodzaju środka niejawnego pozyskiwania informacji, który musi być określony przez prawo w momencie jego zastosowania (zob. np. w sprawie Heglas przeciwko Czechom, gdzie ETPC stwierdził naruszenie art. 8 Konwencji, ponieważ w chwili zarządzenia podsłuchu zamontowanego na ciele osoby środek taki nie był przewidziany przez obowiązujące wówczas prawo). ETPC badał przy tym nie tylko treść przepisów, ale też stosowanie ich przez sądy. W sprawie Uzun przeciwko Niemcom ETPC nie stwierdził naruszenia art. 8 Konwencji, choć ustawodawstwo niemieckie nie przewidywało wprost możliwości wykorzystania urządzeń GPS do niejawnego kontrolowania jednostek. Uznał bowiem, że ustawowy termin „inne specjalne środki techniczne służące inwigilacji" jest zrozumiały w orzecznictwie, i nie budziło wątpliwości, że obejmował dopuszczalność stosowania GPS. Podobnie ETPC stwierdził w sprawie Taylor-Sabori przeciwko Wielkiej Brytanii dotyczącej użycia tzw. klonu pagera pozwalającego na przechwycenie wysyłanych jednostce wiadomości, uznając, że w relewantnym dla sprawy okresie nie obowiązywał żaden przepis regulujący przechwytywanie wiadomości przekazywanych za pomocą pagera (§ 19 uzasadnienia ww. orzeczenia);

– kategorii podmiotów, w stosunku do których mogą być pozyskiwanie w sposób niejawny informacje; w szczególności kładziono nacisk na zapewnienie ochrony osób postronnych, tj. podsłuchanych przypadkowo lub „koniecznych uczestników" rozmowy z osobą, względem której zastosowano podsłuch. W wyroku w sprawie Amann przeciwko Szwajcarii ETPC zwrócił uwagę, że chociaż ustawa definiowała, jakie podmioty mogą być

objęte niejawną kontrolą rozmów, to jednak nie zawierała żadnych środków ostrożności, które powinny być podjęte w odniesieniu do osób trzecich (§ 61 uzasadnienia), a to naruszało konwencyjny wymóg „zgodności z prawem". Natomiast w sprawie Iordachi i inni przeciwko Mołdawii ustawa dopuszczała zarządzenie kontroli rozmów w odniesieniu do podejrzanego, oskarżonego, i – co wzbudziło zastrzeżenia ETPC – innych osób zaangażowanych w działania przestępcze (ang. *other person involved in a criminal offence*). Nie precyzowała jednak, o jakie dokładnie podmioty chodzi. Również w tym wypadku ETPC dopatrzył się naruszenia konwencyjnego wymogu „zgodności z prawem";

– maksymalnego czasu stosowania niejawnej kontroli, który ma mieć charakter oznaczony i definitywny. W sprawie Uzun przeciwko Niemcom, gdzie problem dotyczył m.in. czasu stosowania kontroli za pomocą urządzeń GPS, Europejski Trybunał Praw Człowieka stwierdził, że chociaż prawodawstwo obowiązujące w czasie stosowania tego środka wobec skarżącego nie przewidywało ograniczenia czasu prowadzenia kontroli tego rodzaju, to jednak sądy w sprawie badały proporcjonalność poddania skarżącego niejawnej kontroli (§ 69 uzasadniania);

– procedury wyrażania zgody na zastosowanie środka niejawnego pozyskiwania informacji, która musi mieć co do zasady charakter uprzedni i pisemny i nie może ograniczać się jedynie do kwestii formalnych. Właściwym organem uprawnionym do wydania stosownej zgody powinien być niezależny i zewnętrzny w stosunku do organów władzy wykonawczej organ – najlepiej sąd. Nie jest jednak wystarczające, by uprawnionym do zarządzania niejawnej kontroli był prokurator, jeśli pozostaje uzależniony od władzy wykonawczej (zob. orzeczenie ETPC z 26 kwietnia 2007 r. w sprawie Dumitru Popescu przeciwko Rumunii, skarga nr 71525/01, § 71 uzasadnienia). Nadzór następczy, polegający na dyskwalifikowaniu przez sąd jako dowodu w postępowaniu karnym zgromadzonych niejawne materiałów, jest jedynie wystarczający w odniesieniu do monitorowania jednostek w przestrzeni publicznej, na co ETPC zwrócił uwagę – w kontekście stosowania urządzeń GPS – w sprawie Uzun przeciwko Niemcom (§ 71 uzasadnienia);

– procedury badania, wykorzystywania i przechowywania uzyskanych danych przez organ zewnętrzny i niezależny w stosunku do organów upoważnionych do niejawnego pozyskiwania informacji i okoliczności, w jakich zapisy mają być usunięte lub zniszczone. Prawo ma regulować środki ostrożności przy przekazywaniu danych dalszym podmiotom, wykluczając m.in. przekazywanie innym organom materiałów dobranych w sposób dowolny lub niekompletny. Na te kwestie zwrócono uwagę w sprawie Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii. Bułgarskie ustawodawstwo nie spełniało konwencyjnego wymogu „jakości prawa", bo nie przewidywało nadzoru następczego nad procedurą stosowania niejawnej kontroli ani nad postępowaniem z materiałami uzyskanymi w jej toku; nie precyzowało w dostatecznym stopniu sposobu weryfikacji zgromadzonych materiałów, zabezpieczenia ich integralności czy zasad niszczenia; nie udzielało ponadto kompetencji żadnemu niezależnemu organowi, który badałby i kontrolował funkcjonowanie niejawnego pozyskiwania informacji w państwie. Zdaniem ETPC, minister spraw wewnętrznych nie może być uznany za organ niezależny i spełniający wymagania konwencyjne (§ 85-88 uzasadnienia);

– obowiązku poinformowania osoby, której dane niejawnie pozyskiwano i warunki zaniechania takiej informacji; poinformowanie jednostki powinno jednak nastąpić w momencie, gdy nie zagrozi celom tej kontroli. W pewnych sytuacjach możliwe jest również zaniechanie następczego poinformowania.

2.4.3. W świetle orzecznictwa ETPC, każda regulacja upoważniająca do niejawnego pozyskiwania informacji musi być konieczna w społeczeństwie

demokratycznym oraz służyć ochronie wartości zdefiniowanych w art. 8 ust. 2 Konwencji. Co znamienne, jest relatywnie niewiele spraw, w których ETPC oceniał prawo krajowe w świetle zasady proporcjonalności, gdyż w znakomitej większości spraw poprzestawano na stwierdzeniu naruszenia Konwencji z powodów formalnych, wynikających z niedostatecznej jakości regulacji prawnej.

Jeżeli już ETPC badał spełnienie wymagań materialnych określonych w art. 8 ust. 2 Konwencji, oceniał, czy przesłanki zarządzenia niejawnej kontroli służą celom, określonym w tym przepisie, a także czy – w okolicznościach konkretnej sprawy – niejawne pozyskiwanie informacji miało charakter subsydiarny oraz trwało relatywnie krótko (zob. np. orzeczenia ETPC z 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, § 103 i n. uzasadnienia; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, § 75 i n. uzasadnienia).

3. Retencja danych telekomunikacyjnych w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej i wybranych sądów konstytucyjnych państw członkowskich.

3.1. Pozyskiwanie i gromadzenie danych telekomunikacyjnych w państwach członkowskich Unii Europejskiej regulowała dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. U. UE 1 105 z 15.03.2006, s. 54; dalej: dyrektywa 2006/24/WE lub dyrektywa). Dyrektywę tę wprowadzono w celu zbliżenia przepisów państw członkowskich w zakresie obowiązków dostawców usług łączności elektronicznej lub publicznych sieci łączności (zwanych także przedsiębiorcami telekomunikacyjnymi) w zakresie zatrzymywania generowanych lub przetwarzanych przez nie danych o ruchu i lokalizacji w celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego (por. art. 1 dyrektywy). Dyrektywa nie odnosiła się natomiast do kwestii zatrzymywania i udostępniania treści komunikatów przekazywanych za pomocą sieci teleinformatycznych. Zgodnie z jej art. 6 zatrzymywane danych zostało dopuszczone na okresy nie krótsze niż 6 miesięcy oraz nie dłuższe niż 2 lata od daty połączenia.

Choć w niniejszej sprawie nie zakwestionowano bezpośrednio obowiązku nałożonego na dostawców usług telekomunikacyjnych polegającego na zatrzymywaniu (retencji) danych tego rodzaju przez określony ustawowo czas, to jednak sformułowane w orzecznictwie sądów konstytucyjnych poglądy stanowią wyraz uniwersalnego, europejskiego standardu w zakresie gromadzenia i przetwarzania danych o jednostce przez władze publiczne, w związku z czym zasługują na szczególną uwagę.

3.2. Przepisy dyrektywy w sprawie zatrzymywania danych telekomunikacyjnych były przedmiotem kontroli Trybunału Sprawiedliwości UE m.in. w wyroku z 8 kwietnia 2014 r. w połączonych sprawach High Court of Ireland i Verfassungsgerichtshof z Austrii (sygn. C-293/12). W wyroku tym Trybunał Sprawiedliwości orzekł o nieważności całej dyrektywy z uwagi na naruszenie praw podstawowych zagwarantowanych w art. 7 (prawo do ochrony życia prywatnego) i art. 8 (prawo do ochrony danych osobowych) Karty praw podstawowych Unii Europejskiej; Dz. U. UE C 303 z 14.12.2007, s. 1; dalej: Karta.

3.2.1. Trybunał Sprawiedliwości stwierdził, że dyrektywa 2006/24/WE stanowi głęboką ingerencję w prawa podstawowe zagwarantowane w art. 7 i art. 8 Karty, jakkolwiek nie narusza istoty tych praw.

Jak wyjaśnił TSUE, z uwagi na duże znaczenie środków komunikacji elektronicznej we współczesnym świecie, dane zatrzymywane na podstawie kontrolowanej dyrektywy dają krajowym organom ścigania dodatkowe możliwości wyjaśniania okoliczności poważnych przestępstw. Stanowią tym samym cenne narzędzie przy prowadzeniu czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych. Zdaniem TSUE, zatrzymywanie tego rodzaju danych należy uznać za odpowiednie dla realizacji celów, jakie zakłada ta dyrektywa. Ponadto walka z poważną przestępczością, w tym z przestępczością zorganizowaną i terroryzmem, ma istotne znaczenie dla zagwarantowania bezpieczeństwa publicznego, a jej skuteczność może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik operacyjnych. Zdaniem TSUE, rzeczywisty cel dyrektywy, jakim jest ułatwienie walki z poważnymi przestępstwami, można uznać za uzasadniony w ramach interesu ogólnego UE.

Z punktu widzenia zasady proporcjonalności, zastrzeżenia Trybunału Sprawiedliwości wzbudził jednak brak jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w odniesieniu do zatrzymywania takich danych. Przepisy dyrektywy mają zastosowanie nawet wobec osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami. Ponadto dyrektywa ta nie przewiduje żadnych wyjątków o charakterze podmiotowym, a więc w rezultacie stosuje się nawet wobec tych osób, których komunikacja na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową. Dyrektywa nie wymaga wykazania przez organy państwa żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego. W szczególności nie ogranicza się do zatrzymywania danych dotyczących określonego obszaru geograficznego lub kręgu osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem lub z innych powodów przyczynić się do zapobiegania poważnym przestępstwom, ich wykrywania i ścigania. Dyrektywa nie określa obiektywnego kryterium, które gwarantowałoby, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać tylko w celu zapobiegania przestępstwom oraz wykrywania i ścigania przestępstw, jakie – z uwagi na zakres oraz wagę ingerencji w prawa podstawowe ustanowione w art. 7 i art. 8 Karty – można uznać za wystarczająco poważne, aby tego rodzaju ingerencję uzasadnić. Samo odesłanie do kategorii „poważnych przestępstw" określonych w ustawodawstwie państw członkowskich, zdaniem TSUE, jest niewystarczające z punktu widzenia zasady proporcjonalności. W dyrektywie nie przewidziano też gwarancji proceduralnych zapobiegających nadużyciom. Zwłaszcza nie wprowadzono obowiązku uzyskania uprzedniej zgody sądu lub innego niezależnego organu na udostępnianie czy wykorzystywanie danych telekomunikacyjnych.

W konsekwencji Trybunał Sprawiedliwości stwierdził, że dyrektywa 2006/24/WE nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i art. 8 Karty.

3.2.2. Jakkolwiek skutki wyroku stwierdzającego nieważność aktu prawa pochodnego w trybie pytania prejudycjalnego nie są jednoznacznie oceniane w doktrynie, uznaje się je za porównywalne z tymi, które wywołuje stwierdzenie nieważności aktu prawodawczego w trybie skargi na nieważność, na podstawie art. 263 TFUE (zob. A. Grzelak, *Granica między skuteczną walką z przestępczością a prawem do prywatności i do ochrony danych osobowych. Glosa do wyroku TS z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12*, „Europejski Przegląd Sądowy" 7/2014, s. 51-52).

Trybunał Konstytucyjny przyjmuje wobec tego, że wyrok TSUE z 8 kwietnia 2014 r. w sprawie sygn. C-293/12 ma charakter ostateczny. Wiąże nie tylko instytucje i organy UE, ale również wszystkie organy państw członkowskich, w tym sądy i organy stosujące

przepisy regulujące dostęp do danych telekomunikacyjnych. W związku z tym, że TSUE nie ograniczył w wyroku jego skutków w czasie, należałoby przyjąć, że w zakresie nieważności dyrektywy w sprawie zatrzymywania danych wyrok wywiera skutek *ex tunc*.

3.2.3. Zakwestionowane w niniejszej sprawie przepisy ustawowe regulujące przesłanki udostępniania właściwym służbom zatrzymanych danych telekomunikacyjnych nie stanowią bezpośrednio implementacji dyrektywy 2006/24/WE. Wyrok TSUE z 8 kwietnia 2014 r. w sprawie C-293/12 nie wiąże zatem bezpośrednio Trybunału Konstytucyjnego w procedurze kontroli konstytucyjności przepisów krajowych. Mając jednak na uwadze, że zakwestionowane przepisy pozostają w funkcjonalnym związku z dyrektywą 2006/24/WE, a zarazem poziom ochrony prywatności w kontekście gromadzenia i przetwarzania danych osobowych przez organy władzy publicznej wynikający z Konstytucji jest co najmniej nie niższy od ochrony zagwarantowanej w art. 7 i art. 8 Karty, Trybunał Konstytucyjny uznaje za celowe uwzględnienie tego wyroku jako tła decyzyjnego podczas oceny konstytucyjności przepisów krajowych o udostępnianiu danych telekomunikacyjnych służbom policyjnym i ochrony państwa.

3.2.4. Przepisy ustawowe dotyczące udostępniania służbom policyjnym i ochrony państwa danych telekomunikacyjnych mają pośredni związek z obowiązkiem implementacji przepisów prawa unijnego (tj. dyrektywy 2006/24/WE).

Jak wskazywano w dotychczasowym orzecznictwie, przewidziana w art. 188 pkt 1-3, art. 79 ust. 1 oraz art. 193 Konstytucji kompetencja do badania konstytucyjności aktów normatywnych odnosi się także do sytuacji, gdy zarzut niekonstytucyjności dotyczy zakresu ustawy służącego zapewnieniu skuteczności prawa stanowionego przez Unię Europejską w polskim porządku prawnym (zob. wyroki TK z: 27 kwietnia 2005 r., sygn. P 1/05, OTK ZU nr 4/A/2005, poz. 42, cz. III, pkt 2.4; 3 grudnia 2009 r., sygn. Kp 8/09, OTK ZU nr 11/A/2009, poz. 164, cz. III, pkt 4). Trybunał Konstytucyjny w niniejszej sprawie podziela to stanowisko. Zarówno w trakcie obowiązywania, jak i po uchyleniu dyrektywy Trybunał ma kognicję do kontroli konstytucyjności obowiązujących przepisów prawa polskiego mających związek z implementacją prawa UE.

3.3. Przepisy krajowe implementujące dyrektywę 2006/24/WE i przepisy regulujące udostępnianie takich danych organom władzy publicznej były dotychczas kontrolowane m.in. przez sądy konstytucyjne niektórych państw członkowskich Unii Europejskiej.

3.4. W wyroku z 11 grudnia 2008 r. (nr 13627) Naczelny Sąd Administracyjny Bułgarii orzekł o niekonstytucyjności art. 5 rozporządzenia nr 40 z dnia 7 stycznia 2008 r. (stanowiącego implementację dyrektywy 2006/24/WE do bułgarskiego porządku prawnego), w zakresie, w jakim dotyczy przesłanek przekazywania danych podlegających retencji przez dostawców publicznych usług telekomunikacyjnych. Przepis art. 5 ust. 1 rozporządzenia nie ograniczał zakresu udostępnianych danych. Ponadto sformułowanie tego przepisu, zgodnie z którym przekazywane dane mają służyć „dla celów działalności operacyjnej", Naczelny Sąd Administracyjny uznał za zbyt ogólne i niedające się pogodzić z konstytucyjnymi wymogami ingerencji w prywatność jednostek. Uznany za niekonstytucyjny przepis rozporządzenia nie zawierał także mechanizmów przeciwdziałających nadużyciom, zwłaszcza nieuprawnionemu pozyskiwaniu danych przez służby ochrony państwa. Jak wskazał w wyroku NSA Bułgarii, normy prawa krajowego muszą szanować art. 8 Konwencji. W związku z tym konieczne jest precyzyjne unormowanie w obowiązującym prawodawstwie podstaw dostępu do danych osobowych obywateli i procedury ich pozyskiwania. Wymogów tych nie spełniał zaskarżony przepis.

3.5. W wyroku z 8 grudnia 2009 r. (nr 1258) Sąd Konstytucyjny Rumunii orzekł o niezgodności całej ustawy nr 298/2008 z konstytucją. Jak podkreślił Sąd Konstytucyjny, ograniczenia w zakresie prawa do życia prywatnego, tajemnicy korespondencji oraz wolności wypowiedzi muszą być sformułowane w sposób jasny, przewidywalny i jednoznaczny, wykluczając – na ile to możliwe – arbitralność i nadużycia. Nie mieści się w standardzie konstytucyjnym unormowanie zezwalające na udostępnianie danych telekomunikacyjnych w celu zwalczania „zagrożeń dla bezpieczeństwa państwa", gdyż jest zbyt ogólne. Ponadto w wypadku retencji danych telekomunikacyjnych podstawa prawna musi być wyjątkowo precyzyjna. Wynika to z natury i specyfiki ograniczanego prawa do prywatności oraz tajemnicy komunikowania się, a także konsekwencji, jakie może wywołać dla jednostek potencjalne naruszenie tych praw. Negatywna ocena przepisów obligujących do retencji danych telekomunikacyjnych wynikała także z tego, że zatrzymywanie danych ma charakter ciągły. Zdaniem Sądu Konstytucyjnego, prowadzi to do nieustannej inwigilacji wszystkich ludzi, przez co nie jest możliwa efektywna ochrona ich prywatności. W wyroku zwrócono uwagę, że istnieją inne efektywne metody zwalczania przestępczości i zapobiegania jej, znacznie mniej ingerujące w konstytucyjny status jednostki, z których prawodawca powinien skorzystać.

3.6. W wyroku Federalnego Sądu Konstytucyjnego Niemiec z 2 marca 2010 r. (sygn. 1 BvR 256/08) przepisy § 113a i § 113b niemieckiego prawa telekomunikacyjnego (dodane na mocy ustawy implementującej dyrektywę 2006/24/WE) zostały uznane za niezgodne z art. 10 ust. 1 Ustawy zasadniczej, wyrażającym wolność i gwarantującym poszanowanie tajemnicy komunikowania się. Za niezgodny z tym przepisem Ustawy zasadniczej uznany został także § 100g tamtejszego kodeksu postępowania karnego, który zezwalał na gromadzenie danych telekomunikacyjnych dotyczących sprawcy oraz uczestnika przestępstwa bez ich wiedzy.

Odnosząc się do prewencyjnego zatrzymywania danych telekomunikacyjnych, FSK nie zakwestionował wprawdzie dopuszczalności zatrzymywania tychże danych przez 6 miesięcy, niemniej jednak uznał to rozwiązanie za proporcjonalne tylko w ściśle określonych celach, takich jak zapewnienie bezpieczeństwa państwa czy porządku publicznego. Zarazem z wyroku tego sądu wynika, że 6-miesieczny okres zatrzymywania danych telekomunikacyjnych ma być traktowany jako maksymalny.

Pozyskiwanie i bezpośrednie wykorzystywanie danych ma jedynie wówczas charakter proporcjonalny, gdy w szczególny sposób służy realizacji istotnych zadań w zakresie ochrony prawnej. Udostępnienie danych uzasadniać może przede wszystkim: podejrzenie popełnienia ciężkiego przestępstwa, potwierdzone określonymi faktami oraz po wykazaniu rzeczywistych przesłanek konkretnego zagrożenia dla zdrowia, życia lub bezpieczeństwa ludzi, integralności lub bezpieczeństwa państwa, bądź kraju związkowego i w wypadku zagrożenia o charakterze ogólnym.

Niezbędne jest ponadto ustanowienie wystarczająco wymagających i jasnych regulacji w zakresie bezpieczeństwa i sposobów wykorzystania danych oraz przejrzystości i ochrony prawnej. W wypadku bezpieczeństwa danych niezbędne jest stworzenie przepisów, które w jasny i wiążący sposób ustanowią szczególnie wysokie standardy w zakresie bezpieczeństwa. W każdym razie przepisy prawa powinny zagwarantować, że standardy te będą stanowiły odzwierciedlenie aktualnego stanu wiedzy naukowej, uwzględniając na bieżąco nowe wyniki badań.

Zdaniem FSK niezbędnym wymogiem jest transparentność wykorzystywania danych, co przede wszystkim przejawiać ma się w konieczności powiadamiania podmiotu

poddanego inwigilacji o pozyskaniu dotyczących go danych. Od zasady poinformowania można odstąpić jedynie wyjątkowo.

Po wyroku FSK z 2 marca 2010 r. stwierdzającym niekonstytucyjność przepisów krajowych implementujących dyrektywę 2006/24/WE, oraz mając na względzie spodziewany wyrok TSUE dotyczący zgodności dyrektywy z Kartą, nie podjęto prac legislacyjnych nad ustanowieniem nowych przepisów, dostosowujących niemiecki system prawny do wymagań określonych przez tamtejszy sąd konstytucyjny.

3.7. W wyroku pełnego składu z 22 marca 2011 r. (Pl. ÚS 24/10), Sąd Konstytucyjny Republiki Czeskiej stwierdził niekonstytucyjność § 97 ust. 3 i 4 ustawy nr 127/2005 z dnia 31 marca 2005 r. o komunikacji elektronicznej oraz o zmianie niektórych innych ustaw, a także orzekł o niekonstytucyjności rozporządzenia z dnia 7 grudnia 2005 r., nr 485/2005.

W ocenie tego sądu, zakwestionowane przepisy zawierały ogólne określenie obowiązków nałożonych na dostawców publicznych usług telekomunikacyjnych. Nie wskazywały natomiast precyzyjnie właściwych organów uprawnionych do dostępu do danych ani też nie precyzowały okoliczności ich gromadzenia oraz przetwarzania. Ponadto cel przekazania danych właściwym organom nie został jasno i precyzyjnie zdefiniowany w obowiązującym prawie. Tym samym nie można ustalić, czy spełnia on wymóg konieczności.

Zakwestionowane przepisy określające warunki wykorzystania danych retencyjnych w postępowaniu karnym nie ograniczały możliwości wykorzystania ich wyłącznie w celu dochodzenia, wykrywania i ścigania poważnych przestępstw, tak jak przewiduje to dyrektywa 2006/24/WE. Zaskarżona regulacja nie nakładała też obowiązku poinformowania jednostki o pozyskaniu w sposób niejawny dotyczących niej danych telekomunikacyjnych. Wprawdzie wykorzystanie zatrzymanych danych telekomunikacyjnych podlegało kontroli sądowej, lecz ustawa nie definiowała precyzyjnie przesłanek i warunków ich udostępniania.

Kontrolowane przepisy w niedostatecznym stopniu gwarantowały bezpieczeństwo danych podlegających retencji, w szczególności zaś nie ograniczały dostępu do danych osób trzecich i nie zapewniały zachowania integralności danych. Nie wskazywały także procedury ich usuwania. Regulacja nie zawierała ponadto innych istotnych, z punktu widzenia jednostki, gwarancji proceduralnych.

3.8. W postanowieniu z 23 kwietnia 2014 r. (sygn. PL. ÚS 10/2014) słowacki Trybunał Konstytucyjny przyjął do rozpoznania wniosek o stwierdzenie niekonstytucyjności przepisów ustawy o łączności implementujących dyrektywę w sprawie zatrzymywania danych. Wydał ponadto postanowienie tymczasowe, w którym zawiesił stosowanie zaskarżonych przepisów.

3.9. W wyroku z 27 lipca 2014 r. (sygn. G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012) austriacki Trybunał Konstytucyjny stwierdził niezgodność z austriacką konstytucją i Konwencją przepisów upoważniających do przekazywania właściwym służbom danych telekomunikacyjnych, zatrzymywanych na podstawie unormowań implementujących dyrektywę 2006/24/WE. Wyrok ten został wydany po stwierdzeniu przez TSUE w wyroku z 8 kwietnia 2014 r. – m.in. w związku z pytaniem prejudycjalnym austriackiego sądu konstytucyjnego – nieważności tej dyrektywy.

Austriacki sąd konstytucyjny podkreślił, że jakkolwiek mechanizm retencyjny sprzyja zwalczaniu zagrożeń, to dopuszczalność gromadzenia danych telekomunikacyjnych przez podmioty prywatne w celu ich udostępnienia właściwym

organom państwa, zależy od spełnienia właściwych wymagań proceduralnych. Jak zaznaczył, mechanizm zatrzymywania i udostępniania danych telekomunikacyjnych może być w świetle konstytucji dopuszczalny tylko pod warunkiem istnienia sądowej kontroli i w celu zwalczania poważnych przestępstw. Doniosłość przestępstw należałoby oceniać m.in. przez pryzmat wysokości kary grożącej za popełnienie danego czynu. Muszą zarazem istnieć skuteczne mechanizmy niszczenia danych, których w austriackim systemie prawnym brakowało. Jak ponadto podkreślił austriacki sąd, zasady gromadzenia i udostępniania danych telekomunikacyjnych muszą być unormowane w sposób precyzyjny, bez konieczności dokonywania złożonych zabiegów interpretacyjnych.

3.10. W wyroku z 3 lipca 2014 r. słoweński Trybunał Konstytucyjny orzekł o uchyleniu mocy obowiązującej przepisów ustawy o komunikacji elektronicznej implementujących dyrektywę 2006/24/WE. Przepisy krajowe zostały uznane za ingerujące nieproporcjonalnie w prawo do ochrony danych osobowych (art. 38 konstytucji). Słoweński Trybunał zobligował również przedsiębiorców zatrzymujących dotąd dane telekomunikacyjne na podstawie niekonstytucyjnych przepisów do zniszczenia danych, niezwłocznie po opublikowaniu orzeczenia.

W ocenie Trybunału, cel zatrzymywania danych określony w prawie może być uznany za konstytucyjnie legitymowany. Ustawodawca dopuścił bowiem zatrzymywanie tych danych dla potrzeb postępowania karnego oraz w celu zagwarantowania bezpieczeństwa narodowego, porządku konstytucyjnego, a także interesów państwa z zakresu bezpieczeństwa, polityki i gospodarki. Zdaniem Trybunału, tak szeroki zakres dopuszczalności wykorzystania danych – nieograniczony wyłącznie do poważnych przestępstw, czego wymaga dyrektywa – oznacza nieproporcjonalną ingerencję w prawo do ochrony danych osobowych.

Powołując się na wyrok TSUE z 8 kwietnia 2014 r., słoweński Trybunał Konstytucyjny uznał za niekonieczne prewencyjne zatrzymywanie danych telekomunikacyjnych dotyczących wszelkich połączeń wszystkich osób, przez 14 lub 8 miesięcy. Ustawodawca nie wskazał przekonująco konieczności tych rozwiązań. Zakwestionowane przepisy nie przewidywały zarazem żadnego wyjątku umożliwiającego anonimowe korzystanie z usług telekomunikacyjnych. Tak szeroki podmiotowy, przedmiotowy i czasowy zakres zatrzymywania danych telekomunikacyjnych może stwarzać wrażenie znajdowania się pod stałym nadzorem. Stanowi to bardzo poważną ingerencję w autonomię informacyjną. Wpływa także na korzystanie przez obywateli z innych wolności i praw.

4. Dotychczasowe orzecznictwo Trybunału Konstytucyjnego.

W dotychczasowym orzecznictwie Trybunał Konstytucyjny kilkukrotnie wypowiadał się w sprawie konstytucyjności przepisów regulujących czynności operacyjno-rozpoznawcze prowadzące do ingerencji w sferę prywatności jednostek i tajemnicę komunikowania się (zob. wyroki TK z: 20 kwietnia 2004 r., sygn. K 45/02, OTK ZU nr 4/A/2004, poz. 30; 12 grudnia 2005 r., sygn. K 32/04; 23 czerwca 2009 r., sygn. K 54/07; a także postanowienia z: 25 stycznia 2006 r., sygn. S 2/06, OTK ZU nr 1/A/2006, poz. 13 i 15 listopada 2010 r., sygn. S 4/10, OTK ZU nr 9/A/2010, poz. 111). Trybunał Konstytucyjny nie podważył dopuszczalności ich stosowania w demokratycznym państwie prawa. Przeciwnie, wyraźnie podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o obywatelach, w toku kontroli operacyjnej ukierunkowanej na zapobieganie przestępstwom, ich wykrywanie oraz zwalczanie, jest nieodzowne. Jawność tych czynności powodowałaby bowiem ich nieskuteczność, a to z kolei rzutowałoby na

poziom bezpieczeństwa państwa i jego obywateli (zob. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 1.1). Ocena ta wynikała z dostrzeżenia specyfiki działalności przestępczej i coraz trudniejszych warunków zapewnienia bezpieczeństwa spowodowanych zagrożeniem terroryzmem, zorganizowaną przestępczością czy wykorzystywaniem przez przestępców nowych technologii w celu komunikowania się między sobą i popełniania rozmaitych przestępstw specjalistycznych (np. komputerowych).

Trybunał Konstytucyjny generalnie aprobował powierzenie kompetencji w zakresie prowadzenia czynności operacyjno-rozpoznawczych nie tylko Policji, ABW czy CBA (zob. np. wyroki TK z 20 kwietnia 2004 r., sygn. K 45/02; 12 grudnia 2005 r., sygn. K 32/04; 23 czerwca 2009 r., sygn. K 54/07), ale również organom kontroli skarbowej, które odpowiadają m.in. za zwalczanie negatywnych zjawisk w postaci niewywiązywania się z obowiązków daninowych, prowadzenia nieujawnionej działalności gospodarczej, „prania pieniędzy", niedozwolonego wykorzystywania powiązań kapitałowych między podmiotami (zob. wyroki TK z: 13 lutego 2001 r., sygn. K 19/99, OTK ZU nr 2/2001, poz. 30; 20 czerwca 2005 r., sygn. K 4/04, OTK ZU nr 6/A/2005, poz. 64; 17 czerwca 2008 r., sygn. K 8/04, OTK ZU nr 5/A/2008, poz. 81, cz. III, pkt 2).

Trybunał wielokrotnie wskazywał również na konieczność odczytywania przepisów konstytucyjnych dotyczących ochrony prywatności i autonomii informacyjnej przez pryzmat wartości i standardów wynikających z Konwencji, a uzewnętrznionych w orzecznictwie ETPC. Mając na uwadze wyższy standard, jaki ustanawia Konstytucja odnośnie do formy aktu stanowienia prawa, Trybunał Konstytucyjny zajmował stanowisko, że to w ustawie, a nie w aktach podustawowych, powinny być określone przesłanki podmiotowe i przedmiotowe niejawnego pozyskiwania informacji o jednostce i dowodów w danej sprawie.

Trybunał wielokrotnie wskazywał ustawodawcy warunki, jakie muszą spełniać normy prawne regulujące niejawne pozyskiwanie przez służby policyjne i służby ochrony państwa informacji na temat jednostek. Wymagania te – o charakterze formalnym, materialnym oraz proceduralnym – pozostają generalnie zbieżne z wypracowanymi przez ETPC na gruncie wykładni Konwencji (zob. cz. III, pkt 2 uzasadnienia).

Wskazywano ponadto, że „nie można mówić o osiągnięciu właściwego kompromisu wówczas, gdy poziom ochrony materialnoprawnej będzie wprawdzie wysoki, jednak na poziomie proceduralnym będzie brakowało efektywnych, a więc «dających się uruchomić» przez poszkodowanego, procedur i środków umożliwiających realizację ochrony zagwarantowanej w przepisach materialnoprawnych, a także – dostępnej dla zainteresowanego – ochrony przed ekscesami i szykanami" (wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 1.1).

5. Konstytucyjne przesłanki dopuszczalności czynności operacyjno-rozpoznawczych.

Trybunał Konstytucyjny w obecnym składzie podziela i podtrzymuje dotychczasową linię orzeczniczą w zakresie wymagań, jakie muszą spełniać unormowania prawne dotyczące niejawnej ingerencji w konstytucyjnie chronione wolności i prawa jednostek w związku ze stosowaniem czynności operacyjno-rozpoznawczych. Uwzględniwszy jednak brak należytej reakcji ustawodawcy na wskazania Trybunału wynikające z dotychczasowego orzecznictwa, pojawienie się w ostatnim czasie nieznanych dotychczas form niejawnego pozyskiwania informacji za pomocą nowych technologii, poszerzenia kręgu organów państwa mających kompetencję do stosowania kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych, a ponadto biorąc pod uwagę sposób stosowania prawa przez organy państwa niezbędne jest, zdaniem Trybunału, nie

tylko obszerniejsze przypomnienie ustawodawcy dotychczasowych ustaleń, ale również ich rozwinięcie i uzupełnienie.

5.1. Wymagania formalne – ustawowa forma ograniczenia i określoność prawa.

5.1.1. Ograniczenia w korzystaniu z konstytucyjnych wolności i praw muszą być precyzyjne unormowane w ustawie. Chodzi jednak nie tylko o formalne umiejscowienie przepisu ograniczającego w akcie normatywnym o randze co najmniej ustawy, ale również o „jakość" tego unormowania, które musi zapewniać przewidywalność rozstrzygnięć organów władzy publicznej wobec jednostek. Ustawowa forma ograniczeń prawa do ochrony prywatności (art. 47), wolności i ochrony tajemnicy komunikowania się (art. 49) oraz autonomii informacyjnej (art. 51 ust. 1 Konstytucji) wynika bezpośrednio z art. 31 ust. 3 Konstytucji, a zapewnienie dostatecznej określoności przepisów także z zasady demokratycznego państwa prawa (art. 2 Konstytucji). Wymóg ustawowego unormowania kwestii gromadzenia i udostępniania informacji został ustanowiony w art. 51 ust. 5 Konstytucji.

Trybunał Konstytucyjny zrekapitulował swoje dotychczasowe orzeczenia dotyczące zasady dostatecznej określoności prawa w wyroku o sygn. Kp 3/09. Stwierdził, że „norma konstytucyjna nakazująca zachowanie odpowiedniej określoności regulacji prawnych ma charakter zasady prawa. Nakłada to na ustawodawcę obowiązek jej optymalizacji w procesie stanowienia prawa. Ustawodawca powinien dążyć do możliwie maksymalnej realizacji wymogów składających się na tę zasadę. Tym samym stopień określoności konkretnych regulacji podlega każdorazowej relatywizacji w odniesieniu do okoliczności faktycznych i prawnych, jakie towarzyszą podejmowanej regulacji. Relatywizacja ta stanowi naturalną konsekwencję nieostrości języka, w którym redagowane są teksty prawne oraz różnorodności materii podlegającej normowaniu" (wyrok TK z 28 października 2009 r., sygn. Kp 3/09, OTK ZU nr 9/A/2009, poz. 138, cz. III, pkt 6.2). Na ustawodawcy ciąży zatem obowiązek tworzenia przepisów prawa możliwie najbardziej określonych w danym wypadku pod względem zarówno ich treści, jak i formy. W związku z powyższym każde unormowanie regulujące status jednostki w państwie powinno cechować się „poprawnością", „precyzyjnością" i „jasnością". Każdy przepis prawny winien być skonstruowany poprawnie z punktu widzenia językowego i logicznego. Dopiero po spełnieniu tego podstawowego warunku można ocenić przepis w aspekcie pozostałych kryteriów wynikających z zasady określoności prawa (zob. wyrok TK z 10 listopada 1998 r., sygn. K 39/97, OTK ZU nr 6/1998, poz. 99, cz. IV, pkt 2.2). Przepisy ustawowe ograniczające konstytucyjne wolności lub prawa muszą być zatem sformułowane w sposób pozwalający jednoznacznie ustalić, kto i w jakiej sytuacji podlega ograniczeniom przez organy państwa; muszą być na tyle precyzyjne, by je stosowano i interpretowano w jednolity sposób; wreszcie muszą być tak ujęte, by zakres ich zastosowania obejmował wyłącznie sytuacje, w których racjonalny ustawodawca zamierzał wprowadzić regulację ograniczającą korzystanie z konstytucyjnych wolności i praw (zob. wyrok TK z 30 października 2001 r., sygn. K 33/00, OTK ZU nr 7/2001, poz. 217, cz. III, pkt 3). Przekroczenie pewnego poziomu niejasności przepisów prawnych stanowić może samoistną przesłankę ich niezgodności z przepisem wymagającym regulacji ustawowej określonej dziedziny oraz wyrażoną w art. 2 Konstytucji zasadą państwa prawnego (zob. wyroki TK z: 30 października 2001 r., sygn. K 33/00, cz. III, pkt 3; 20 kwietnia 2004 r., sygn. K 45/02, cz. III, pkt 2).

Jak wskazał Trybunał w cytowanym wyżej wyroku w sprawie o sygn. Kp 3/09, „ocena konstytucyjności aktu normatywnego zawsze musi mieć charakter złożony. W wypadku określoności, złożoność tego procesu dostrzegana jest na dwóch płaszczyznach. Po pierwsze, w odniesieniu do analizy samej określoności uwzględnić należy najpierw

wspomniane wyżej aspekty testu określoności (precyzyjność, jasność, poprawność), a następnie we właściwej proporcji odnieść je do charakteru badanej regulacji. Drugą płaszczyznę stanowi kontekst aksjologiczny, w jakim przeprowadzana jest kontrola konstytucyjności norm. Na kontekst ten składa się wykładnia całości reguł, zasad i wartości konstytucyjnych, z którymi skonfrontowana musi zostać badana norma, wyinterpretowana z przepisu poddanego wcześniej kontroli z formalnego punktu widzenia (określoności właśnie)" (wyrok TK z 28 października 2009 r., sygn. Kp 3/09, cz. III, pkt 6.3.1).

Trybunał Konstytucyjny stwierdza, że zakres akceptacji stopnia niejasności przepisów nie jest jednakowy dla całości ustawodawstwa. Im bardziej przepisy oddziałują na wolności i prawa konstytucyjne, zwłaszcza o charakterze osobistym, tym większy rygoryzm towarzyszyć musi ocenie precyzyjności unormowania. Trybunał podkreśla ponadto, że ponieważ wolności osobiste – w świetle systematyki Konstytucji – są wyjątkowo silnie eksponowane, to ustawowe ograniczenia w korzystaniu z nich powinny być możliwe do ustalenia już na podstawie wykładni językowej przepisów ustawy, bez potrzeby odwoływania się do wykładni systemowej czy funkcjonalnej. Zdaniem Trybunału, w wypadku wolności osobistych nie jest dopuszczalne skorygowanie niekonstytucyjnej normy prawnej wyprowadzonej za pomocą wykładni językowej przez odwołanie się do pozostałych, pozajęzykowych metod wykładni, aby wreszcie odnaleźć – czasami gdzieś na bezdrożach systemu prawnego – rozumienie przepisu ograniczającego konstytucyjne wolności osobiste, które będzie zgodne z Konstytucją.

5.1.2. Przekładając powyższe ustalenia na unormowanie ingerencji w wolności i prawa konstytucyjne w związku ze stosowaniem przez służby policyjne lub służby ochrony państwa czynności operacyjno-rozpoznawczych, zdaniem TK, jednostka na podstawie przepisu ustawy powinna wiedzieć, kto oraz w jakim zakresie podmiotowym, przedmiotowym i czasowym jest uprawniony do niejawnej ingerencji w szeroko rozumianą sferę prywatności. Kryterium przewidywalności nie oznacza jednakże – na co też kładzie się nacisk w orzecznictwie ETPC – że jednostka będzie mogła dokładnie przewidzieć moment, w którym organy władzy publicznej zarejestrują jej zachowania lub pozyskają o niej inne informacje, a co za tym idzie będzie mogła dostosować do tej sytuacji własne zachowanie (np. unikając prowadzenia rozmów telefonicznych i kontaktowania się z innymi). Prawo musi być natomiast wystarczająco precyzyjne, aby dać odpowiednie wskazania co do okoliczności i warunków, w których organy państwa mogą zastosować któryś z takich środków. Trybunał Konstytucyjny stwierdza, że ustalone w orzecznictwie ETPC standardy w powyższym zakresie zachowują pełną aktualność oraz mają swe odzwierciedlenie w treści zasady demokratycznego państwa prawnego wynikającej z art. 2 Konstytucji, jak i w tej części art. 31 ust. 3 Konstytucji, który dla ograniczeń wolności i praw wymaga ustawowej formy regulacji.

Podstawowym celem precyzyjnego określenia w prawie przesłanek dopuszczalności czynności operacyjno-rozpoznawczych jest wyznaczenie organom władzy wykonawczej możliwie jak najściślejszych ram działania. Zapobiegać ma to arbitralności stosowania prawa, a zwłaszcza przenoszeniu na organy stosujące prawo ciężaru faktycznego wyznaczenia granic wolności człowieka. Trybunał Konstytucyjny zwraca ponadto uwagę, że im większa jest skala stosowania czynności operacyjno-rozpoznawczych, a więc wzrasta – choćby potencjalnie – częstotliwość ingerencji w konstytucyjne wolności i prawa, tym bardziej unormowanie ustawowe musi cechować się zupełnością i maksymalną precyzją.

5.1.3. Na tle dotychczasowych ustaleń Trybunał zwraca uwagę na konieczne elementy ustawowej regulacji czynności operacyjno-rozpoznawczych (niejawnego pozyskiwania przez władze publiczne informacji o jednostkach).

5.1.3.1. Po pierwsze, to ustawa ma precyzować przedmiotowe przesłanki zarządzenia takich czynności. Aby zachować standard konstytucyjny, nie wystarcza odwołanie się do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest wobec tego zdefiniować zamknięty i możliwe wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki. Wbrew twierdzeniom Marszałka Sejmu w pismach procesowych z 15 czerwca oraz 30 sierpnia 2012 r., jakoby intencją Trybunału wyrażoną w postanowieniu sygnalizacyjnym o sygn. S 4/10 była konieczność określenia w ustawie „typów przestępstw" wyłącznie przez odwołanie się do konkretnych przepisów ustawy karnej, Trybunał takiego wymogu nie formułuje wobec ustawodawcy. Przez „typy przestępstw określone przez ustawę karną", o których mowa w powyżej przywołanym postanowieniu o sygn. S 4/10, należy rozumieć określenie przestępstw ich nazwą rodzajową (np. przestępstwo zabójstwa, rozboju, oszustwa*)*, a nie wskazanie jednostek redakcyjnych ustawy karnej – przepisów, w których są penalizowane. Nie jest wykluczone zastosowanie również innych technik legislacyjnych (np. odwołanie się do konkretnych rozdziałów lub ustaw), jednakże w każdym wypadku powinno być możliwe zrekonstruowanie sytuacji, w których niejawne pozyskiwanie informacji przez organy państwa jest dopuszczalne.

Precyzyjne ustawowe uregulowanie przedmiotowych przesłanek dopuszczalności kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych jest tym bardziej konieczne, ponieważ w istocie to same służby – działając w ramach ich ustawowych zadań – definiują zagrożenia, którym mają następnie zapobiegać. O ile Trybunał nie kwestionuje ogólnego zakreślenia w ustawie zadań służb ochrony państwa, to już przesłanki niejawnego pozyskiwania informacji o osobach mają być zdefiniowane przez ustawodawcę wyczerpująco w sposób zamknięty. Odwołując się do utrwalonego orzecznictwa ETPC oraz Trybunału Konstytucyjnego, należy raz jeszcze podkreślić, że na podstawie brzmienia przepisu ustawy jednostka ma wiedzieć, jakie zachowania narażają ją nie tylko na ewentualną odpowiedzialność karną, lecz również umożliwią prowadzenie w stosunku do niej czynności operacyjno-rozpoznawczych, głęboko ingerujących w jej prywatność.

5.1.3.2. Po drugie, niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Mając na uwadze ogromną liczbę środków stosowanych przez organy państwa przydatnych w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna. Rozwiązanie to mogłoby kolidować z wymogiem abstrakcyjności normy prawnej. Jak wielokrotnie wskazywał Trybunał, również w perspektywie określoności przepisów represyjnych, przestrzeganie wymogów wynikających z zasady dostatecznej określoności prawa nie może prowadzić do kazuistyki unormowania (zob. wyroki TK z: 26 listopada 2003 r., sygn. SK 22/02, OTK ZU nr 9/A/2003, poz. 97, cz. III, pkt 4; 5 maja 2004 r., sygn. P 2/03, OTK ZU nr 5/A/2004, poz. 39, cz. III, pkt 3.5; 13 stycznia 2005 r., sygn. P 15/02, OTK ZU nr 1/A/2005, poz. 4, cz. III, pkt 2; 28 czerwca 2005 r., sygn. SK 56/04, OTK ZU nr 6/A/2005, poz. 67, cz. V, pkt 1; 17 grudnia 2008 r., sygn. P 16/08, OTK ZU nr 10/A/2008, poz. 181, cz. IV, pkt 8.2.2; 22 czerwca 2010 r., sygn. SK 25/08, OTK ZU nr 5/A/2010, poz. 51 cz. III, pkt 4.1-4.2; 1 grudnia 2010 r., sygn. K 41/07, OTK ZU nr 10/A/2010, poz. 127, cz. III, pkt 3.2). Podobnie uznał TK w wyroku dotyczącym przepisów regulujących prowadzenie kontroli operacyjnej przez wywiad skarbowy (zob. wyrok TK z 20 czerwca 2005 r., sygn. K 4/04, cz. V, pkt 2.6), akceptując – po spełnieniu kilku warunków – pewien stopień ogólności unormowania sposobów kontroli operacyjnej prowadzonej przez wywiad skarbowy. Należałoby mieć także na uwadze, że w dobie rozwoju technologicznego,

wielości form popełniania przestępstw i kanałów komunikowania się przestępców nie wydaje się realne stworzenie zamkniętego katalogu środków technicznych, które mogą być stosowane w celu uzasadnionego konstytucyjnie niejawnego pozyskiwania informacji, bez uszczerbku dla efektywnej walki z zagrożeniami czy dekonspiracji działalności operacyjnej.

Z punktu widzenia zasady określoności prawa istotne jest natomiast sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Raz jeszcze należy podkreślić, że nie chodzi o wskazanie parametrów technicznych, ale rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania za ich pomocą (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej"). Zamknięty katalog rodzajów środków technicznych służących do niejawnego pozyskiwania informacji i dowodów ogranicza arbitralność organów państwa. Ponadto umożliwia sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobach.

Według Trybunału, najbardziej pożądanym rozwiązaniem z konstytucyjnego punktu widzenia jest uregulowanie rodzajów środków służących niejawnemu pozyskiwaniu informacji o jednostkach w ustawie. Precyzyjne określenie tej kwestii przez ustawodawcę nie tylko wiąże się z realizacją zasady określoności prawa wynikającą z art. 2 Konstytucji, ale przede wszystkim z tą częścią art. 31 ust. 3 Konstytucji, która przewiduje obowiązek unormowania ograniczeń w korzystaniu z wolności i praw konstytucyjnych „w ustawie", będącej aktem normatywnym pochodzącym od przedstawicielskiego organu Narodu – Sejmu (art. 4 w związku z art. 104 ust. 1 Konstytucji). Uregulowanie w ustawie rodzajów środków technicznych powoduje, że organ mający demokratyczną legitymację suwerena bierze na siebie ciężar politycznej odpowiedzialności za zakres dopuszczalnej inwigilacji i legitymizuje sposoby wkraczania służb policyjnych i ochrony państwa w sferę prywatności jednostek. Zasadne jest tym samym, by to parlament zaakceptował dopuszczalność stosowania rodzajów środków technicznych, które w szerokim zakresie ingerują w wolności i prawa człowieka.

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

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

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

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

5.2. Wymagania materialne i proceduralne – zasada proporcjonalności.

5.2.1. Czynności operacyjno-rozpoznawcze są konstytucyjnie usprawiedliwione tylko o tyle, o ile ich celem jest obrona wartości demokratycznego państwa prawnego. Muszą zatem sprostać wymaganiom „konieczności w demokratycznym państwie prawnym" (*vide:* art. 31 ust. 3, art. 51 ust. 2 Konstytucji). Nie wystarczy więc ich celowość, użyteczność, taniość bądź łatwość posługiwania się nimi przez organy władzy publicznej. Nie ma także przesądzającego znaczenia, czy podobne środki są wykorzystywane w innych państwach (zob. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 3.1). Niejawne pozyskiwanie informacji przez służby policyjne i ochrony państwa ma bowiem służyć wzmocnieniu poziomu ochrony wartości istotnych w państwie demokratycznym w sposób niemożliwy do osiągnięcia z wykorzystaniem innych rozwiązań, mniej ingerujących w sferę wolności lub praw jednostek. Jednocześnie muszą to być środki najmniej uciążliwe dla podmiotów, których wolności lub prawa ulegają ograniczeniu, stosowane absolutnie wyjątkowo, w celu wykrywania i ściganiu poważnych przestępstw. W przeciwnym razie demokratyczne państwo stałoby się w rzeczywistości państwem policyjnym.

5.2.2. Cel ograniczenia konstytucyjnych wolności i praw w związku z dopuszczeniem czynności operacyjno-rozpoznawczych nie może być dowolny. Legitymizowane są wyłącznie takie ograniczenia, które służą ochronie wartości wyraźnie wymienionych w art. 31 ust. 3 lub innych szczegółowych przepisach Konstytucji. Nie wystarczy przy tym werbalne powołanie się przez ustawodawcę na realizację jednej z wartości konstytucyjnie chronionych. Konieczne jest bowiem istnienie i wykazanie potrzeby jej wprowadzenia w warunkach demokratycznego państwa prawa. W konsekwencji nie jest dopuszczalne gromadzenie ani przetwarzanie danych o jednostce przez organy władzy publicznej bez powodu, w nieokreślonych lub niemożliwych do osiągnięcia celach. Ustawodawca musi mieć równocześnie na uwadze, że każde niejawne pozyskiwanie informacji o jednostce powinno być środkiem przydatnym dla ochrony tych wartości. Muszą one więc umożliwiać osiągnięcie założonego i konstytucyjnie uzasadnionego celu, zgodnie z aktualnie dostępną, sprawdzalną i powszechnie uznawaną wiedzą naukową. Jeśli z dużym prawdopodobieństwem nie da się wykazać, że wprowadzone albo projektowane rozwiązania prawne prowadzą do wzrostu wykrywalności przestępstw, podniesienia stanu bezpieczeństwa państwa lub obywateli, nie spełnią one przesłanki przydatności ograniczenia.

Ograniczenie konstytucyjnych wolności i praw w świetle zasady proporcjonalności wymaga oceny, czy korzyści wprowadzonych ograniczeń pozostają w odpowiedniej proporcji do uszczerbku doznawanego przez jednostki. Innymi słowy, musi występować

odpowiednie zbilansowanie konkurujących ze sobą wartości. Oczywiście tego rodzaju ocena jest możliwa do przeprowadzenia wyłącznie w konkretnym wypadku. W tym miejscu Trybunał formułuje więc jedynie ogólne warunki, jakie muszą być każdorazowo brane pod uwagę w toku badania proporcjonalności unormowania.

5.2.3. Niejawne pozyskiwanie informacji o jednostkach w demokratycznym państwie prawa, za pomocą czynności operacyjno-rozpoznawczych, jest dopuszczalne jedynie w celu zapobiegania poważnym przestępstwom, ich ścigania i wykrywania. Nie jest rolą Trybunału – jako sądu nad prawem – definiowanie katalogu takich przestępstw. Należy to do ustawodawcy, który dysponuje w tym zakresie pewnym marginesem swobody. Ustalając katalog przestępstw, co do których dopuszczalne są czynności operacyjno-rozpoznawcze, ustawodawca nie może odrywać się od obiektywnie mierzalnej hierarchii dóbr, której wyraz daje Konstytucja. Nie może także abstrahować od uwarunkowań historycznych i społecznych, determinujących stopień zagrożenia, jakie niosą ze sobą poszczególne czyny w skali całego państwa. Nieuprawniona jest natomiast, zdaniem Trybunału, teza jakoby sama penalizacja jakiegoś czynu w ustawach karnych, a nawet zobowiązanie do jego ścigania na mocy umów międzynarodowych, były wystarczającymi przesłankami uznania go za poważny w stopniu uzasadniającym dopuszczalność niejawnego pozyskiwania informacji i dowodów za pomocą czynności operacyjno-rozpoznawczych, które prowadzą do ingerencji w prywatność, tajemnicę komunikowania się czy autonomię informacyjną.

Trybunał zwraca nadto uwagę na konieczność nieustannej weryfikacji katalogu takich przestępstw. Z biegiem czasu niektóre przestępstwa – uznawane dotąd za poważne zagrożenia – mogą zmieniać swoją kwalifikację. Katalog poważnych przestępstw, co do których może być dopuszczalne niejawne pozyskiwanie informacji o osobach przez organy państwa, musi być tym samym ciągle przez ustawodawcę aktualizowany.

Przepisy regulujące niejawne pozyskiwanie informacji o jednostkach przez władze publiczne nie mogą ujmować przesłanek ich zarządzenia w sposób abstrakcyjny, w oderwaniu od rzeczywistego stopnia wywoływanego zagrożenia dla określonych dóbr w danej sprawie. Aby unormować przesłanki zarządzenia czynności operacyjno-rozpoznawczych, trzeba zatem precyzyjnie określić katalog poważnych przestępstw, ale także wskazać dodatkowe okoliczności, umożliwiające niuansowanie zasadności tego rodzaju sposobu pozyskiwania informacji i dowodów w konkretnych sprawach, z uwzględnieniem m.in. ciężaru gatunkowego lub rozmiarów wyrządzonej szkody.

Trybunał nie neguje możliwości pozyskiwania informacji o jednostkach za pomocą czynności operacyjno-rozpoznawczych także w celu zapobiegania poważnym przestępstwom, czyli podejmowania działań przeciwdziałających popełnianiu przestępstw. Nie podważa nadto dopuszczalności wykorzystywania tych czynności w celu rozpoznawania zagrożeń, to jest pozyskiwania informacji o sytuacjach sprzyjających popełnieniu przestępstw. Dotyczy to w szczególności podejmowania tych działań przez służby ochrony państwa stojące na straży jego bezpieczeństwa zewnętrznego i wewnętrznego. W świetle standardu konstytucyjnego zarządzenie kontroli operacyjnej lub pozyskanie danych telekomunikacyjnych może nastąpić jednak w takich wypadkach, w których prawdopodobieństwo popełnienia przestępstwa jest realne, a nie tylko hipotetyczne. Ciężar wykazania prawdopodobieństwa zagrożenia przestępstwem ma przy tym spoczywać na organach państwa wnoszących o umożliwienie im niejawnego gromadzenia informacji i podlegać ocenie sądu lub innego niezależnego organu.

Choć inne są cele czynności operacyjno-rozpoznawczych prowadzonych przez służby odpowiedzialne za utrzymanie porządku (np. Policję), inne zaś przez służby informacyjno-wywiadowcze (np. ABW, SKW), to z punktu widzenia naruszenia wolności i praw jednostki nie ma znaczenia, jaki organ władzy publicznej oraz na jakiej podstawie

pozyskuje niejawnie informacje na jej temat. Stopień naruszenia prywatności i tajemnicy komunikowania się jest bowiem taki sam, bez względu na to, czy chodzi o ingerencję służb policyjnych, czy służb ochrony państwa. Trybunał zwraca uwagę, że specyfika działalności służb informacyjno-wywiadowczych oraz związany z tym relatywnie wąsko określony zakres ich ustawowych zadań, może uzasadniać odmienne ustalenie zasad prowadzenia takich czynności i wykorzystywania zgromadzonych materiałów, od reguł obowiązujących pozostałe organy państwa, a zwłaszcza służby policyjne, mające szeroki zakres działania. Takie zróżnicowanie zasad prowadzenia czynności operacyjno-rozpoznawczych nie uchyla oczywiście wymogu przestrzegania zasady proporcjonalności.

5.2.4. Niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. To znaczy, że niejawna ingerencja w wolności i prawa, ma stanowić *ultima ratio*. Dotyczy to w takiej samej mierze kontroli operacyjnej, jak i udostępniania danych telekomunikacyjnych czy innych form pracy operacyjno-rozpoznawczej o podobnym skutku dla jednostek.

5.2.5. Z przesłanką subsydiarności wiąże się wprowadzenie proceduralnego wymogu, którym jest kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa. Pożądane jest powierzenie kompetencji w tym zakresie niezależnym i niezawisłym sądom, dającym rękojmię odpowiednio wysokiego stopnia wiedzy i doświadczenia życiowego. Z punktu widzenia Konstytucji sądowa kontrola nad czynnościami operacyjno-rozpoznawczymi jest rozwiązaniem optymalnym. Nie jest jednak bezwzględnie konieczna. Kompetencje tego rodzaju mogą zostać też powierzone innym organom państwa, których status ustrojowy i zakres ustawowych kompetencji gwarantuje efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa.

Ustawowe unormowania kontroli muszą wykluczać jej fasadowość. Ustawodawca jest zatem obowiązany wyposażyć sądy bądź inne organy w kompetencje pozwalające na ocenę celowości i subsydiarności czynności operacyjno-rozpoznawczych, jak również sposobów ich prowadzenia w indywidualnej sprawie względem konkretnych podmiotów. Niezbędnym warunkiem rzetelności tej kontroli jest generalny obowiązek uzasadniania decyzji w sprawie wyrażenia zgody na ich podjęcie, a także wskazania podmiotu, czasu prowadzenia kontroli, a także szczegółowego zakresu pozyskiwanych informacji. Trybunał przyjmuje, że podstawową rolę należy przypisać kontroli uprzedniej (*ex ante*), która powinna być traktowana jako zasada przynajmniej wtedy, gdy organy państwa pozyskują w sposób niejawny informacje o jednostkach związane z treścią przekazywanych wiadomości. Nie jest jednakże wykluczone wprowadzenie kontroli następczej, czyli legalizującej uprzednio podjęte zgodnie z ustawową procedurą czynności operacyjno-rozpoznawcze. To jednak rozwiązanie winno być wyjątkiem dopuszczalnym wówczas, gdy uzyskanie zgody uprzedniej zagrażałoby szczególnie cennym dobrom, znacząco osłabiało efektywność działania bądź prowadziło do bezpowrotnej utraty informacji o szczególnym znaczeniu dla bezpieczeństwa państwa i porządku publicznego.

Trybunał Konstytucyjny nie wyklucza, by ustawodawca – w pewnych okolicznościach – odstąpił do ustanowienia zewnętrznego nadzoru nad niejawnym pozyskaniem informacji o jednostce w drodze czynności operacyjno-rozpoznawczych. Dotyczyć może to pozyskiwania jedynie takich danych, które są ogólnie dostępne w publicznych rejestrach lub upublicznione dobrowolnie i świadomie przez jednostki, zwłaszcza w sieciach telekomunikacyjnych (np. w Internecie).

5.2.6. Niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych.

Przede wszystkim ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie. Tego wymagania nie uchyla wprowadzenie innych, zastępczych rozwiązań, jak choćby pełnomocnika osoby kontrolowanej. Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r., sygn. S 2/06). Zapewnienie informacji jest przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji prawa dostępu do urzędowych dokumentów i zbiorów danych. Co do zasady, wszystkie zgromadzone i przetwarzane przez władze publiczne dane o jednostce – chociażby nawet nie tworzyły jednego zorganizowanego zbioru – powinny być udostępniane tej osobie, jeżeli wystąpi ze stosownym żądaniem. Warunkiem (i to podstawowym) skorzystania z prawa unormowanego w art. 51 ust. 3 Konstytucji jest wiedza o zgromadzeniu określonych danych i istnieniu ich zbioru. Zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji – ponieważ dokonało się to w sposób niejawny, bez jej wiedzy i zgody – nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji. Obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności.

Trybunał ma świadomość, że w pewnych sytuacjach może być również uzasadnione odstąpienie od wspomnianego obowiązku informacyjnego. Dotyczy to w szczególności takich sytuacji, gdy dane zostały pozyskane wyłącznie przypadkowo i nie podlegają dalszej analizie, czy też gdy pozyskano dane dostępne w publicznych rejestrach. Kwestie te musi rozstrzygnąć ustawodawca.

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

5.3. Standard konstytucyjny – podsumowanie.

Uwzględniając dotychczasowe ustalenia Trybunału Konstytucyjnego i Europejskiego Trybunału Praw Człowieka, a także Trybunału Sprawiedliwości Unii Europejskiej dotyczące przepisów regulujących niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach, Trybunał uznaje za konieczne przypomnienie minimalnych wymagań, jakie łącznie muszą spełniać przepisy ograniczające konstytucyjne wolności i prawa. Są one następujące:

– gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, dopuszczalne jest wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy (zob. m.in. wyroki TK z: 12 grudnia 2005 r., sygn. K 32/04; 23 czerwca 2009 r., sygn. K 54/07);

– konieczne jest precyzyjne określenie w ustawie organów państwa upoważnionych do gromadzenia oraz przetwarzania danych o jednostce, w tym do stosowania czynności operacyjno-rozpoznawczych;

– w ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi są: wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im; ustawa powinna wskazywać rodzaje takich przestępstw (zob. np. postanowienie TK z 15 listopada 2010 r., sygn. S 4/10; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 10 lutego 2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, skarga nr 25198/02);

– ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze (zob. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 16 lutego 2000 r. w sprawie Amann przeciwko Szwajcarii, skarga nr 27798/95; 10 lutego 2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, skarga nr 25198/02);

– pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków;

– czynności operacyjno-rozpoznawcze winny być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób (zob. wyroki TK z: 12 grudnia 2005 r., sygn. K 32/04; 23 czerwca 2009 r., sygn. K 54/07);

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

– niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji (zob. np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05);

– precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych (zob. np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04);

– zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów;

– unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności

zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo (zob. np. postanowienie TK z 25 stycznia 2006 r., sygn. S 2/06);

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

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

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

6. Ogólna charakterystyka zakwestionowanych unormowań.

6.1. Kontrola operacyjna.

6.1.1. Kontrola operacyjna jest jedną z form czynności operacyjno-rozpoznawczych, które mogą prowadzić Policja, Straż Graniczna, wywiad skarbowy, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Agencja Bezpieczeństwa Wewnętrznego oraz Centralne Biuro Antykorupcyjne. Ma ona charakter niejawny.

6.1.2. Ustawodawca przewidział trzy rodzaje kontroli operacyjnej dla każdej z wyżej wymienionych służb: Może ona polegać na kontroli treści korespondencji, kontroli zawartości przesyłek oraz „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”. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675, ze zm.; dalej: ustawa o SG), ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, ze zm.; dalej: ustawa o kontroli skarbowej) i ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 i 628; dalej: ustawa o ŻW) wskazano dodatkowo „obraz”, jako podlegający utrwaleniu za pomocą środka technicznego.

Sieciami telekomunikacyjnymi – w rozumieniu art. 2 pkt 35 prawa telekomunikacyjnego – są systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych oraz innych wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju. Informacjami przekazywanymi za pomocą sieci telekomunikacyjnych są więc rozmowy telefoniczne, wiadomości w postaci SMS, MMS lub przekazywane za pomocą faksu, a także inne informacje przekazywane drogą radiową i internetową, w tym poczta elektroniczna, treści zamieszczane na forach internetowych lub czatach. Katalog takich informacji możliwych do pozyskania w toku kontroli operacyjnej ma charakter otwarty (zob. np. D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 162-163).

Ustawodawca nie zdefiniował w żadnym z przepisów ustawowych, jak należy rozumieć termin „środek techniczny”, o którym mowa w zakwestionowanych przepisach. Z wykładni językowej art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze zm.; dalej: ustawa o Policji), art. 9e ust. 7 pkt 3 ustawy o

SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, ze zm.; dalej: ustawa o ABW), art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, ze zm.; dalej: ustawa o CBA oraz art. 31 ust. 4 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, ze zm.; dalej: ustawa o SKW) wynika, że środek taki musi mieć dwojakiego rodzaju właściwości. Po pierwsze, ma mieć charakter techniczny, czyli być w jakiś sposób oparty na nowych technologiach, a po drugie – powinien pozwalać nie tylko pozyskiwać informacje, ale równocześnie je utrwalać.

Pojęcie kontroli operacyjnej jest więc bardzo pojemne. Taka kontrola umożliwia pozyskiwanie różnego rodzaju informacji o jednostce, przede wszystkim związanych z komunikowaniem się (treść korespondencji lub rozmów, zawartość przesyłek) i innymi formami przekazywania wiadomości. Mając powyższe na uwadze, Trybunał przyjmuje, że zakwestionowane przepisy – co wynika już z językowej ich wykładni – umożliwiają m.in. podsłuch osób i pomieszczeń, w tym rozmów za pośrednictwem telefonii stacjonarnej, bezprzewodowej (komórkowej) i internetowej, pozyskiwanie treści wiadomości tekstowych i multimedialnych przesyłanych za pomocą urządzeń telefonicznych oraz innych urządzeń służących do komunikowania się na odległość, stosowanie urządzeń rejestrujących położenie osób i rzeczy wykorzystujących nawigację satelitarną lub przechwytywanie ulotu elektromagnetycznego (zob. J. Kudła, *Wybrana problematyka czynności operacyjno-rozpoznawczych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 533-534; J. Widacki, *Kryminalistyka*, Warszawa 2012, s. 135-137).

6.1.3. Jak podkreśla się zazwyczaj w literaturze przedmiotu, kontrola operacyjna polegająca na stosowaniu środków technicznych jest czymś innym niż kontrola treści korespondencji. Przyjmuje się bowiem, że kontrola treści korespondencji obejmuje wyłącznie zatrzymywanie korespondencji w postaci listów, kart pocztowych lub innych form przekazywania wiadomości za pomocą tradycyjnych form porozumiewania się (por. J. Kudła, *Wybrana…*, *op.cit.* s. 533; D. Szumiło-Kulczycka, *op.cit*, s. 162). Natomiast, zdaniem przedstawicieli doktryny, w sytuacji gdy informacja przekazywana jest za pomocą sieci telekomunikacyjnych – chociażby stanowiła szeroko rozumianą korespondencję – właściwą podstawą zarządzenia tej kontroli jest art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA oraz art. 31 ust. 4 pkt 3 ustawy o SKW. Trybunał Konstytucyjny nie wypowiada się natomiast w kwestii dopuszczalności takiej wykładni przepisów regulujących kontrolę operacyjną w świetle art. 49 Konstytucji.

6.1.4. Zakres przedmiotowy kontroli operacyjnej, a zarazem jej cel, został określony odmiennie dla każdej ze służb uprawnionych do jej stosowania. W świetle przepisów ustawy o Policji, ustawy o SG oraz ustawy o ŻW kontrola operacyjna może być zarządzona w celu: zapobiegania umyślnym przestępstwom ściganym z oskarżenia publicznego (tzw. przestępstw katalogowych), wykrywania i ustalenia ich sprawców oraz uzyskania i utrwalania dowodów takich czynów. Przestępstwa te są wymienione w art. 19 ust. 1 pkt 1-8 ustawy o Policji, art. 9e ust. 1 pkt 1-7 ustawy o SG, art. 31 ust. 1 pkt 1-17 ustawy o ŻW. Wywiad skarbowy może prowadzić kontrolę operacyjną w celu wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów przestępstw katalogowych wymienionych w art. 36c ust. 1 pkt 1-5 ustawy o kontroli skarbowej. Zgodnie z art. 17 ust.

1 ustawy o CBA, służba ta może prowadzić kontrolę operacyjną w celu rozpoznawania i wykrywania przestępstw określonych w art. 17 ust. 1 pkt 1 i 2 ustawy o CBA, zapobiegania im oraz uzyskania i utrwalenia ich dowodów. W wypadku ABW ustawodawca przewidział możliwość zarządzenia kontroli operacyjnej w celu rozpoznawania i wykrywania przestępstw określonych w art. 5 ust. 1 pkt 2 ustawy o ABW oraz zapobiegania im. Nie przewidział natomiast możliwości stosowania tej kontroli w celu uzyskiwania i utrwalania dowodów tych przestępstw. Z kolei w świetle ustawy o SKW kontrola operacyjna może być zarządzona w celu rozpoznawania i wykrywania przestępstw określonych w art. 5 ustawy o SKW oraz zapobiegania im, a także wykonywania innych zadań określonych w tym przepisie.

Katalogi przestępstw, w wypadku których może być prowadzona kontrola operacyjna, zostały przez ustawodawcę określone z użyciem różnych technik legislacyjnych: przez wskazanie jednostek redakcyjnych ustaw karnych, określenie przestępstw nazwą rodzajową, a niekiedy odesłanie do całych rozdziałów lub ustaw szczególnych, w których są unormowane. Ustawodawca posłużył się również – co zarzucili wnioskodawcy – sformułowaniami na tyle ogólnymi, że katalogi przestępstw uzasadniających kontrolę operacyjną przybrały charakter w istocie otwarty. Umożliwił bowiem m.in. zarządzenie kontroli operacyjnej w odniesieniu do „przestępstw ściganych na mocy umów i porozumień międzynarodowych", nie precyzując, o jakie dokładnie przestępstwa chodzi ani w jakich dokładnie aktach normatywnych mają być ujęte. Natomiast w ustawie o ABW oraz ustawie o SKW ustawodawca posłużył się wyrażeniami nieostrymi o wysokim stopniu ogólności, takimi jak „przestępstwa godzące w bezpieczeństwo państwa", „podstawy ekonomiczne państwa", czy „bezpieczeństwo Sił Zbrojnych, jednostek organizacyjnych MON i państw zapewniających wzajemność".

6.1.5. Zakres podmiotowy kontroli operacyjnej jest, co do zasady, nieograniczony. Wyłącznie w ustawie o ŻW przewidziano, że kontrolę operacyjną można zarządzić w ramach czynności operacyjno-rozpoznawczych prowadzonych w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, pkt 3 lit. b i pkt 5 ustawy o ŻW. Chodzi o żołnierzy pełniących czynną służbę wojskową, pracowników zatrudnionych w jednostkach wojskowych w związku z popełnieniem przez nich czynu zabronionego przez ustawę pod groźbą kary, wiążącego się z tym zatrudnieniem, a także innych osób niż określone w art. 3 ust. 2 pkt 1-4 ustawy o ŻW, podlegających orzecznictwu sądów wojskowych albo jeśli wynika to z odrębnych przepisów. Pośrednio ograniczony jest podmiotowy zakres stosowania kontroli operacyjnej w przepisach ustawy o SKW, gdyż w świetle art. 5 ust. 1 pkt 1 ustawy służba ta może prowadzić czynności operacyjno-rozpoznawcze w sprawach przestępstw popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON.

6.1.6. Kontrola operacyjna ma charakter subsydiarny. Może być zatem zarządzona tylko wtedy, gdy inne środki okazały się bezskuteczne lub są nieprzydatne. Przez pojęcie „innych środków" należy rozumieć pozostałe formy czynności operacyjno-rozpoznawczych, niebędące kontrolą operacyjną. „Bezskuteczność" oznacza nieprzynoszenie spodziewanych rezultatów, zaś „nieprzydatność" – brak możliwości osiągnięcia zamierzonych rezultatów za pomocą określonego środka. Jak przyjmuje się w piśmiennictwie, wnosząc o zarządzenie kontroli operacyjnej, właściwy organ ma wykazać bezskuteczność dotychczasowych działań lub uprawdopodobnić nieprzydatność tradycyjnych metod analizy kryminalnej (zob. W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [w:] *Praktyczne elementy…*, s. 511).

6.1.7. Ustawowa regulacja procedury zarządzania kontroli operacyjnej w odniesieniu do służb policyjnych i ochrony państwa jest w istocie zbliżona do siebie. Co do zasady może być zastosowana po jej zarządzeniu przez właściwy sąd okręgowy na pisemny wniosek szefa danej służby, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego lub prokuratorów okręgowych. Wyłącznie w sytuacjach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji, zatarcie lub zniszczenie dowodów przestępstwa, ustawodawca dopuścił możliwość zarządzenia kontroli operacyjnej przez szefów służb, po uzyskaniu zgody Prokuratora Generalnego lub prokuratorów okręgowych. W takiej sytuacji organ zarządzający kontrolę musi wystąpić do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie (zatwierdzenie lub odmowę zatwierdzenia kontroli operacyjnej – tzw. zgoda następcza). Wnoszący wniosek, który powinien zawierać m.in. opis przestępstwa wraz z podaniem kwalifikacji prawnej, powinien dołączyć do niego materiały uzasadniające potrzebę zastosowania kontroli operacyjnej, a także wskazać jej cel, czas oraz rodzaj. Sąd okręgowy orzeka w sprawie wniosku o zarządzenie bądź zatwierdzenie kontroli operacyjnej jednoosobowo, a czynności sądu związane z rozpoznaniem tych wniosków są wykonywane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych. W posiedzeniu sądu może uczestniczyć przedstawiciel organu wnoszącego o zarządzenie kontroli oraz prokurator.

6.1.8. Organ wnioskujący o zarządzenie kontroli operacyjnej zobowiązany jest po jej zakończeniu poinformować właściwego prokuratora o wynikach, a na jego żądanie również o przebiegu kontroli. Materiały zgromadzone w trakcie stosowania tej kontroli, jeżeli stanowią dowód popełnienia przestępstwa lub przestępstwa skarbowego uzasadniającego zarządzenie takiej kontroli, mogą być bezpośrednio wprowadzone do postępowania sądowego, bez potrzeby ich następczego przetworzenia. Jeśli uzyskano dowód przestępstwa, co do którego można zarządzić kontrolę operacyjną w stosunku do osoby poddanej kontroli, lecz nieobjętego zarządzeniem sądu, możliwe jest następcze (legalizujące) zezwolenie na procesowe wykorzystanie tych materiałów. Rozstrzyga o tym sąd uprawniony do zarządzenia kontroli, na wniosek Prokuratora Generalnego lub odpowiednio prokuratora okręgowego.

6.1.9. Ustawodawca przewidział w każdej z ustaw regulujących kontrolę operacyjną ramowe zasady niszczenia materiałów utrwalonych w czasie jej prowadzenia, niemających znaczenia dla ustawowo określonych celów. Nie są one jednakowe dla poszczególnych służb i nie ustanawiają tym samym jednolitych gwarancji. I tak, zgodnie z art. 19 ust. 17 ustawy o Policji, art. 9e ust. 18 ustawy o SG i art. 31 ust. 18 ustawy o ŻW zniszczeniu podlegają materiały niezawierające dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla postępowania karnego. Z kolei art. 36d ust. 3 ustawy o kontroli skarbowej obowiązkiem zniszczenia obejmuje materiały niezawierające dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe albo niemające znaczenia dla postępowania kontrolnego. W art. 17 ust. 16 ustawie o CBA i art. 31 ust. 15 ustawy o SKW ustawodawca przewidział nakaz niszczenia tylko materiałów, które nie stanowią informacji potwierdzających zaistnienie przestępstwa, a zgodnie z art. 27 ust. 16 ustawy o ABW obowiązkowi niszczenia podlegają tylko materiały, które nie są istotne dla bezpieczeństwa państwa lub nie stanowią informacji potwierdzających zaistnienie przestępstwa.

6.2. Udostępnianie danych telekomunikacyjnych.

6.2.1. W ramach czynności operacyjno-rozpoznawczych służby policyjne i służby ochrony państwa mogą pozyskiwać dane telekomunikacyjne, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, a także mogą je gromadzić i przetwarzać.

6.2.2. W myśl art. 180c ust. 1 prawa telekomunikacyjnego udostępnia się dane dotyczące ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie i do którego kierowane jest połączenie, a także określające datę i godzinę połączenia oraz czas jego trwania, rodzaj połączenia, a także lokalizację telekomunikacyjnego urządzenia końcowego. Doprecyzowanie katalogu danych, o których mowa w art. 180c ust. 1, zawiera wydane na podstawie art. 180c ust. 2 rozporządzenie 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; dalej: rozporządzenie Ministra Infrastruktury).

Z kolei art. 180d prawa telekomunikacyjnego, do którego odsyłają zakwestionowane art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW i art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, ze zm.; dalej: ustawa o SC), samoistnie nie określa katalogu danych podlegających udostępnieniu służbom. Odsyła on do innych przepisów tej ustawy, tj. art. 159 ust. 1 pkt 1 i 3-5, art. 161 oraz art. 179 ust. 9 prawa telekomunikacyjnego. W tym wypadku mamy do czynienia z odesłaniem złożonym drugiego stopnia o charakterze statycznym. Tego rodzaju konstrukcja legislacyjna – chociaż sama w sobie nie jest wykluczona na gruncie Konstytucji – musi być wyjątkowo ostrożnie stosowana w wypadku, gdy reguluje ingerencję organów władzy publicznej w status prawny jednostki.

Uwzględniając powyższe przepisy, ustawodawca zezwolił na pozyskiwanie przez uprawnione podmioty danych dotyczących użytkownika, danych transmisyjnych (tj. danych przetwarzanych 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), danych o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, danych o próbach uzyskania połączenia między zakończeniami sieci, w tym 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 świetle art. 161 prawa telekomunikacyjnego, dostawca publicznie dostępnych usług telekomunikacyjnych może też gromadzić następujące dane, o które mogą występować uprawnione organy władzy publicznej: dane osobowe abonenta obejmujące nazwisko i imiona; imiona rodziców; miejsce i datę urodzenia; adres miejsca zamieszkania i adres korespondencyjny, jeżeli jest on inny niż adres miejsca zamieszkania; numer PESEL – w wypadku obywatela polskiego; nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w wypadku cudzoziemca niebędącego obywatelem państwa członkowskiego UE albo Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu; dane zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Jeśli dostawca publicznie dostępnych usług telekomunikacyjnych uzyskał zgodę użytkownika będącego osobą fizyczną na przetwarzanie innych danych tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, adres korespondencyjny użytkownika (jeżeli jest on inny niż adres miejsca zamieszkania), a

ponadto adres poczty elektronicznej oraz numery telefonów kontaktowych, również i tego rodzaju dane, znajdujące się w dyspozycji dostawcy publicznie dostępnych usług telekomunikacyjnych, mogą być pozyskiwane i przetwarzane przez służby policyjne i służby ochrony państwa w celach określonych w ustawach. Ponadto służby te mogą otrzymywać dane wskazane w art. 179 ust. 9 prawa telekomunikacyjnego, czyli zawarte w prowadzonym obligatoryjnie przez każdego przedsiębiorcę telekomunikacyjnego wykazie abonentów, użytkowników lub zakończeń sieci, dane uzyskiwane podczas zawarcia umowy.

Podsumowując, na podstawie art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW i art. 75d ust. 1 ustawy o SC możliwe jest pozyskanie trojakiego rodzaju danych: o abonencie, o ruchu (tzw. dane bilingowe), a także o lokalizacji. Nie istnieje natomiast prawna możliwość pozyskiwania w tym trybie treści indywidualnych komunikatów przekazywanych za pomocą sieci telekomunikacyjnych.

6.2.3. Udostępnianie danych telekomunikacyjnych na podstawie zaskarżonych przepisów może opierać się na bezpośrednim dostępie upoważnionych funkcjonariuszy do tych danych, bez udziału lub z niezbędnym udziałem pracowników podmiotu prowadzącego działalność telekomunikacyjną. Dokonuje się to za pomocą sieci teleinformatycznej, która musi spełniać wymogi bezpieczeństwa. W szczególności niezbędne jest umożliwienie identyfikacji osób uzyskujących dane, ich rodzaju oraz czasu, w którym zostały uzyskane (*vide:* art. 20c ust. 5 ustawy o Policji, art. 10b ust. 4 ustawy o SG, art. 36b ust. 6 ustawy o kontroli skarbowej, art. 30 ust. 4 ustawy o ŻW, art. 28 ust. 4 ustawy o ABW, art. 18 ust. 4 ustawy o CBA, art. 32 ust. 6 ustawy o SKW, art. 75d ust. 4 ustawy o SC). Drugą przewidzianą przez ustawodawcę procedurą pozyskiwania danych telekomunikacyjnych jest skierowanie przez upoważnionego do tego funkcjonariusza ustnego albo pisemnego wniosku do podmiotu prowadzącego działalność telekomunikacyjną.

6.2.4. Ustawowa regulacja dotycząca wykorzystywania danych telekomunikacyjnych przez służby policyjne i ochrony państwa jest lakoniczna. Jedynie w art. 20c ust. 6 i 7 ustawy o Policji, art. 10b ust. 5 i 6 ustawy o SG oraz w art. 30 ust. 5 i 6 ustawy o ŻW przewidziano, że materiały zawierające informacje mające znaczenie z punktu widzenia postępowania karnego służba przekazuje właściwemu prokuratorowi, natomiast niemające takiego znaczenia podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Nieco inaczej zagadnienie to unormowano w art. 75d ust. 5 ustawy o SC, wskazując, że obowiązek niszczenia dotyczy materiałów niezawierających informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe. Z kolei w świetle art. 36d ust. 3 ustawy o kontroli skarbowej, niszczeniu podlegają materiały niezawierające dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe albo niemające znaczenia dla postępowania kontrolnego. Analogicznych regulacji nie przewidują ustawa o ABW, ustawa o CBA i ustawa o SKW.

Kontrowersje budzi dopuszczalność wykorzystania danych telekomunikacyjnych w postępowaniu sądowym. Wskazuje się niekiedy, że bardzo duża liczba żądań o udostępnienia danych telekomunikacyjnych w Polsce w istocie wynika z konieczności niejako podwójnego występowania o te same dane – pierwszy raz w celach operacyjno-rozpoznawczych, a drugi raz, gdy toczy się już postępowania karne – w celach dowodowych. Praktyka ta ma wynikać z braku dostatecznych podstaw prawnych, które pozwalałyby na wykorzystanie zgromadzonych w toku czynności operacyjno-rozpoznawczych materiałów w procesie karnym jako dowodów. Definiując cele

pozyskiwania oraz przetwarzania danych telekomunikacyjnych przez służby policyjne i ochrony państwa, ustawodawca pominął cel dowodowy. Ograniczył się tylko do wskazania, że dane te mogą być udostępniane służbom w celu zapobiegania przestępstwom bądź ich wykrywania, a także wykonywania ustawowo określonych zadań służb o charakterze analitycznym i planistycznym. W literaturze wskazuje się jednak, że na podstawie wykładni funkcjonalnej przepisów regulujących pozyskiwanie danych telekomunikacyjnych można uznać wykorzystanie danych pozyskanych na etapie przedprocesowym, jako dowodów w postępowaniu karnym (zob. D. Szumiło-Kulczycka, *op.cit.*, s. 270-271).

Trybunał dostrzega, że ponowne występowanie o dane telekomunikacyjne w celach dowodowych, po uprzednim żądaniu takich danych w celach operacyjno-rozpoznawczych, może rzutować na rzeczywistą skalę pozyskiwania danych telekomunikacyjnych w Polsce, zawyżając ją. Rodzi to konieczność doprecyzowania tej materii przez ustawodawcę.

6.2.5. Obowiązujące obecnie unormowanie dotyczące gromadzenia i przetwarzania danych telekomunikacyjnych przez organy państwa są związane z implementacją dyrektywy 2006/24/WE (cz. III, pkt 3.1 uzasadnienia). Implementacja nastąpiła ustawą z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 716; dalej: ustawa implementująca). Ustawa ta nałożyła na przedsiębiorców telekomunikacyjnych obowiązek zatrzymywania i przechowywania, a następnie – na żądanie określonych organów – udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego. Stworzyła ona zarazem prawne ramy dostępu do tychże danych przez upoważnione podmioty. Należy tu zaznaczyć, że możliwość żądania od przedsiębiorców telekomunikacyjnych danych dotyczących okoliczności i rodzaju połączenia bądź też prób uzyskania połączenia była znana porządkowi prawnemu jeszcze przed uchwaleniem dyrektywy 2006/24/WE. Ustanowienie tej dyrektywy doprecyzowało natomiast zakres obowiązków przedsiębiorców do zatrzymywania danych.

Polski ustawodawca implementował dyrektywę 2006/24/WE w sposób ekstensywny. Po pierwsze, początkowo przewidział obowiązek zatrzymywania danych przez maksymalny przewidziany w dyrektywie okres 24 miesięcy (co było ewenementem wśród państw członkowskich UE). Dopiero ustawą z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. poz. 1445), która obowiązuje od 21 stycznia 2013 r., skrócono ten termin do 12 miesięcy. Podobny termin zatrzymywania danych obowiązuje w większości państw członkowskich UE. Po drugie, ustawodawca upoważnił do żądania danych telekomunikacyjnych nie tylko w celu dochodzenia, wykrywania lub ścigania poważnych przestępstw, jak stanowiła dyrektywa 2006/24/WE, ale także w celu zwalczania przestępstw o relatywnie niskim stopniu szkodliwości, a nawet czynów niebędących przestępstwami, bądź w celu wykonywania zadań analityczno-planistycznych. Po trzecie, kompetencje do żądania zatrzymanych danych telekomunikacyjnych ma w Polsce wyjątkowo duża, w porównaniu z innymi państwami europejskimi, liczba podmiotów. Dostęp do tych danych mają wszystkie sądy i prokuratorzy (art. 218 ust. 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego; Dz. U. Nr 89, poz. 555, ze zm.; dalej: k.p.k.) oraz, co jest przedmiotem tej sprawy, aż osiem służb policyjnych i ochrony państwa.

6.2.6. Uwzględniając dane statystyczne zawarte w najnowszej „Informacji dla Komisji Europejskiej dotyczącej udostępniania danych telekomunikacyjnych zatrzymywanych przez przedsiębiorców telekomunikacyjnych i operatorów w roku 2013”, sporządzonej 17 marca 2014 r. przez Prezesa Urzędu Komunikacji Elektronicznej, Trybunał Konstytucyjny zwraca uwagę, że 12-miesięczny okres zatrzymania danych telekomunikacyjnych jest stosunkowo długi, wziąwszy pod uwagę istotną ingerencję w

wolności i prawa konstytucyjne wynikające z zatrzymywania dotyczących ich danych telekomunikacyjnych. Ocena taka jest tym bardziej uzasadniona, że w świetle powyższej informacji, około 49% wypadków udostępnienia danych mieściło się w okresie pierwszych 2 miesięcy przechowywania, a około 69% – w okresie pierwszych 4 miesięcy. Od 6 do 11 miesiąca przechowywania maleją one od 3,6% do 2,9% ogólnej liczby udostępnianych danych. Pewien wzrost obserwowany jest w ostatnim, 12 miesiącu (do 8,37% ogólnej liczby wypadków), co może wynikać z opieszałości organów państwa chcących pozyskać te dane. Obserwacja ta może uprawdopodabniać tezę, że chociaż upoważnione organy mogły pozyskiwać dane telekomunikacyjne znacznie wcześniej, zwlekały z tym do ostatniego miesiąca. W kontekście tej statystyki może budzić wątpliwości, czy zatrzymywanie danych o ruchu i lokalizacji na czas dłuższy niż 6 miesięcy spełnia konstytucyjny wymóg przydatności, wynikający z zasady proporcjonalności. Kwestia ta pozostaje jednakże poza zakresem zaskarżenia.

Jak już wskazano wcześniej (zob. cz. III, pkt 3.1-3.3 uzasadnienia), z wyjaśnień Prezesa UKE oraz szefów poszczególnych służb wynika, że zakres danych przekazywanych przez przedsiębiorców telekomunikacyjnych jest wypadkową kilku czynników. Zwracali na to uwagę również przedstawiciele Prezesa NIK oraz Prezesa UKE na rozprawie. Warunkują go niejednokrotnie konkretne rozwiązania techniczne wykorzystywane przez przedsiębiorców telekomunikacyjnych. Brak jest jednolitych standardów obowiązujących wszystkie podmioty obowiązane do zatrzymywania danych telekomunikacyjnych w Polsce, określających sposób realizacji żądania pochodzącego od każdej ze służb uprawnionych do dostępu do tych danych, co zresztą zostało krytycznie ocenione przez Najwyższą Izbę Kontroli (zob. *Informacja o wynikach kontroli. Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, znak: KPB-P/12/191, wersja jawna, podpisana w dniu 12 czerwca 2013 r.). Sytuacja ta może prowadzić m.in. do niejednoznaczności upublicznianych statystyk obrazujących skalę sięgania po dane telekomunikacyjne przez służby policyjne i ochrony państwa. Zdaniem Trybunału, brak jednolitych standardów w tym zakresie stanowi istotny konstytucyjny mankament obowiązujących unormowań.

7. Dopuszczalność orzekania – przesłanki formalne.

7.1. Wśród przepisów będących przedmiotem kontroli w tej sprawie, Rzecznik Praw Obywatelskich zakwestionował zgodność art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji. Norma prawna wynikająca z tego przepisu – w brzmieniu analogicznym do obecnie obowiązującej – była już przedmiotem kontroli Trybunału Konstytucyjnego. W wyroku z 20 czerwca 2005 r. (sygn. K 4/04), Trybunał stwierdził, że 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; dalej: ustawa o w.k.s.) – w zakresie, w jakim ustala brzmienie art. 36c ust. 1 i 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. Jakkolwiek wyrok Trybunału w powołanej sprawie odnosił się do innej jednostki redakcyjnej (przepisu ustawy zmieniającej), to jednak nie powinno ulegać wątpliwości, że kontrola dotyczyła w istocie normy prawnej wywodzonej z tego przepisu, regulującej sposób prowadzenia kontroli operacyjnej, której treść jest identyczna z normą prawną obowiązującą obecnie. W związku z tożsamością

kontrolowanej normy oraz wzorców kontroli w niniejszej sprawie ze sprawą rozstrzygniętą przez Trybunał, jak również w związku ze stanowiskiem Marszałka Sejmu, który wniósł o umorzenie postępowania w zakresie badania konstytucyjności art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, należy rozważyć, czy nie zachodzi ujemna przesłanka procesowa nakazująca umorzenie postępowania w sprawie.

7.2. Zgodnie z 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: ustawa o TK) Trybunał umarza postępowanie, jeśli wydanie orzeczenia jest zbędne lub niedopuszczalne. W świetle orzecznictwa TK uprzednie rozpoznanie sprawy konstytucyjności zakwestionowanej normy prawnej z punktu widzenia tych samych wzorców kontroli, co do zasady, skutkuje zbędnością wydania wyroku z uwagi na zakaz *ne bis in idem* (zob. postanowienia TK z: 3 października 2001 r., sygn. SK 3/01, OTK ZU nr 7/A/2001, poz. 218; 25 października 2011 r., sygn. K 36/09, OTK ZU nr 8/A/2011, poz. 93; wyrok z 27 marca 2007 r., sygn. SK 3/05, OTK ZU nr 3/A/2007, poz. 32). Taka sytuacja występuje zawsze, gdy Trybunał stwierdzi niezgodność zakwestionowanej normy z Konstytucją, nawet jeśli inicjator postępowania wskazał dodatkowe, obok będących wcześniej podstawą orzeczenia o niekonstytucyjności, wzorce kontroli (zob. postanowienie TK z 28 lipca 2003 r., sygn. P 26/02, OTK ZU nr 6/A/2003, poz. 73). Jednakże w orzecznictwie przyjmuje się, że zasada *ne bis in idem* nie znajduje zastosowania, gdy TK orzekł wcześniej o zgodności zaskarżonej normy, a wnioskodawca wskazał nowe wzorce kontroli lub przedstawił niepowoływane wcześniej argumenty, okoliczności lub dowody uzasadniające prowadzenie postępowania i wydanie wyroku (zob. wyroki TK z: 5 września 2006 r., sygn. K 51/05, OTK ZU nr 8/A/2006, poz. 100; 12 września 2006 r., sygn. SK 21/05, OTK ZU nr 8/A/2006, poz. 103). Wskazanie nowych wzorców kontroli, zarzutów bądź argumentów może bowiem spowodować odmienny kierunek rozstrzygnięcia przez Trybunał w sprawie konstytucyjności przepisu.

7.3. Mając powyższe na uwadze najważniejsze jest rozważenie, czy występuje tożsamość sprawy o sygn. K 4/04 ze sprawą obecnie rozpoznawaną.

W sprawie o sygn. K 4/04 grupa posłów zgłosiła szereg zarzutów pod adresem art. 8 pkt 27 ustawy o w.k.s. nadającym nowe brzmienie przepisom rozdziału 4 ustawy o kontroli skarbowej, zatytułowanym „Wywiad skarbowy". Niektóre z nich dotyczyły poszczególnych rozwiązań przewidzianych w tej ustawie, inne z kolei – kwestionowały mechanizm działania wywiadu skarbowego w ogólności. Orzekając o konstytucyjności normy wynikającej z art. 36c ust. 4 ustawy o kontroli skarbowej, Trybunał uznał część zarzutów za nieuzasadnione. Niemniej jednak merytorycznie odniósł się do zarzutów skierowanych wobec art. 36c ust. 4 ustawy o kontroli skarbowej, który – w ocenie wnioskodawców – miał być niedostatecznie określony. Trybunał nie podzielił zarzutów wnioskodawcy.

Z analizy uzasadnienia zarzutów wnioskodawców i – co ważniejsze – rozstrzygnięcia Trybunału Konstytucyjnego zawartego w wyroku o sygn. K 4/04, a także zarzutów Rzecznika Praw Obywatelskich w obecnej sprawie, wynika, że nie zachodzi w rozpoznawanej aktualnie sprawie ujemna przesłanka procesowa w postaci zakazu *ne bis in idem*. Trybunał stwierdza, że Rzecznik Praw Obywatelskich wskazał dodatkowe zarzuty i argumenty mające przemawiać za niekonstytucyjnością przepisu, które nie były rozważane przez TK w wyroku o sygn. K 4/04, a mianowicie: brak katalogu danych, jakie służby mogą pozyskiwać o jednostce, a także brak ustawowego katalogu środków technicznych, z których służby mogą korzystać, prowadząc kontrolę operacyjną. Zaskarżony przepis

ustawy o kontroli skarbowej może tym samym podlegać merytorycznej kontroli w niniejszej sprawie. Konstatacja ta nie przesądza jeszcze o kierunku rozstrzygnięcia.

8. Zakres przedmiotowy kontroli operacyjnej.

8.1. Pierwszym problemem konstytucyjnym wskazanym przez wnioskodawców jest niedookreślony katalog sytuacji uzasadniających zarządzenie kontroli operacyjnej w toku czynności operacyjno-rozpoznawczych prowadzonych przez Policję, Straż Graniczną, wywiad skarbowy, Żandarmerię Wojskową, Służbę Kontrwywiadu Wojskowego i Agencję Bezpieczeństwa Wewnętrznego.

Wnioskodawcy wskazali jako przedmiot kontroli art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW, art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW, art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych", art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność" i art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW.

W ocenie wnioskodawców, zakwestionowane przepisy naruszają art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, a ponadto art. 8 Konwencji. Unormowanie przesłanek zarządzenia kontroli operacyjnej jest w istocie blankietowe, a przez to pozostawia władzy wykonawczej nadmierny margines swobody ingerencji w konstytucyjne wolności i prawa jednostek. Ustawodawca nie określił bowiem dokładnie typów przestępstw, których zwalczanie uprawniałoby poszczególne służby do stosowania kontroli operacyjnej. W konsekwencji (zwrócił uwagę Prokurator Generalny we wniosku z 7 marca 2012 r.) Policja, Straż Graniczna, wywiad skarbowy, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego oraz Agencja Bezpieczeństwa Wewnętrznego mogą przeprowadzać kontrolę operacyjną łącznie w ponad 200 sytuacjach, a liczba ta systematycznie rośnie w związku z przyjmowaniem przez Polskę kolejnych zobowiązań międzynarodowych.

Zastrzeżenia Prokuratora Generalnego wzbudziło głównie odesłanie przez ustawodawcę do bliżej niesprecyzowanych umów i porozumień międzynarodowych, które mogą obejmować nie tylko umowy międzynarodowe ratyfikowane za uprzednią zgodą wyrażoną w ustawie, ale również akty normatywne niemieszczące się w konstytucyjnym katalogu prawa powszechnie obowiązującego. Po pierwsze, Konstytucja nie przewiduje „porozumień międzynarodowych" jako źródeł prawa powszechnie obowiązującego, mogących kształtować sytuację jednostek. Literalna wykładnia art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 17 ustawy o ŻW i art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW może prowadzić do konstatacji, że „ustawodawca dopuścił stosowanie przez służby kontroli operacyjnej w oparciu o umowy międzynarodowe, ratyfikowane w inny sposób niż po uprzednim wyrażeniu na to zgody przez Parlament, oraz w oparciu o umowy międzynarodowe, które ratyfikacji nie wymagają, co wydaje się absolutnie niedopuszczalne". Zdaniem wnioskodawcy, niesprecyzowanie umów lub porozumień międzynarodowych, w których unormowano ściganie przestępstw, może też wskazywać na zmienność okoliczności uzasadniających zarządzenie kontroli operacyjnej oraz potencjalne

ich poszerzanie się wraz z przyjmowaniem przez Polskę kolejnych zobowiązań międzynarodowych w tej materii. Każde bowiem nowe zobowiązanie się władz publicznych do ścigania określonych przestępstw automatycznie poszerza katalog sytuacji pozwalających na zarządzenie kontroli operacyjnej. Skoro nie można na podstawie zaskarżonych przepisów określić rodzajów przestępstw, przepisy te – zdaniem Prokuratora Generalnego – mają mieć charakter blankietowy.

Tożsame argumenty Prokurator Generalny podniósł w odniesieniu do art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a oraz art. 5 ust. 1 pkt 9 ustawy o SKW uprawniających do „podejmowania kontroli operacyjnej w oparciu o nieokreślone regulacje zawarte w bliżej nieokreślonych aktach normatywnych rangi ustawy", innych niż ustawa o SKW, a nawet takie ustawy, które w chwili obecnej nie zostały jeszcze nawet uchwalone. Zdaniem wnioskodawcy, nie jest wobec tego możliwe wskazanie zamkniętego katalogu przestępstw uzasadniających stosowanie kontroli operacyjnej. Podobnie występujące w art. 5 ust. 1 pkt 1 lit. g ustawy o SKW pojęcie przestępstw „godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność" nie pozwala na identyfikację konkretnych typów przestępstw określonych w ustawie karnej, a co za tym idzie nie pozwala sprecyzować sytuacji, w których dopuszczalne jest zarządzenie kontroli operacyjnej. Wnioskodawca odwołał się do postanowienia sygnalizacyjnego TK o sygn. S 4/10, dotyczącego przesłanek zarządzenia kontroli w ustawie o ABW, które – jego zdaniem – zachowuje w tej sprawie pełną aktualność. Prokurator Generalny wyjaśnił również, że w szczególności ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.; dalej: k.k.) nie zawiera żadnego rozdziału grupującego przestępstwa godzące w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych i jednostek organizacyjnych MON. Żaden z aktów normatywnych nie definiuje też na czym miałoby polegać działanie lub zaniechanie sprawcy godzące w te dobra. Rodzi to trudności w ustaleniu przesłanek niejawnej ingerencji w konstytucyjne wolności i prawa jednostek.

Z kolei Rzecznik Praw Obywatelskich, odnosząc się do regulacji kontroli operacyjnej prowadzonej przez ABW, zarzucił, że art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", a także art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW, nie pozwalają określić precyzyjnie okoliczności zarządzenia kontroli operacyjnej. Kodeks karny ani inne ustawy nie posługują się sformułowaniem „przestępstwo godzące w bezpieczeństwo państwa" i „przestępstwo godzące w podstawy ekonomiczne państwa". Tym samym zakwestionowane przepisy nie spełniają konstytucyjnego standardu określoności prawa, nie pozwalając ponadto ustalić rzeczywistego zakresu ingerencji w sferę prywatności jednostki. Mając na względzie nieostrość przepisów, a także związaną z tym niemożność zdefiniowania precyzyjnych celów ingerencji, zdaniem RPO, zaskarżone przepisy nie mogą przejść pozytywnie testu proporcjonalności. Skoro nie jest możliwe ustalenie dokładnych okoliczności, w jakich kontrola operacyjna może być zarządzona, nie ma możliwości oceny, czy regulacja ta jest w stanie doprowadzić do zakładanego skutku. Stwarza ponadto ryzyko arbitralnego wkraczania w prywatność jednostki.

8.2. Ocena zgodności art. 19 ust. 1 pkt 8 ustawy o Policji z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

8.2.1. Zakwestionowany art. 19 ust. 1 pkt 8 ustawy o Policji ma następującą treść:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i

utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw (…) ściganych na mocy umów i porozumień międzynarodowych, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, 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".

8.2.2. Zakwestionowany przepis stanowi podstawę zarządzenia kontroli operacyjnej w ramach czynności operacyjno-rozpoznawczych w ściśle określonym celu, a mianowicie: wykrycia, ustalenia sprawców, uzyskania i utrwalenia dowodów umyślnych przestępstw ściganych z oskarżenia publicznego, a także im zapobiegania.

Katalog przestępstw uzasadniających kontrolę operacyjną w świetle ustawy o Policji jest przez ustawodawcę wyrażony w art. 19 ust. 1 w sposób *prima facie* zamknięty. Jak zaznaczył SN, „katalog zawarty w art. 19 ust. 1 ustawy o Policji kreowany powinien być w oparciu o ścisłe przestrzeganie zasady proporcjonalności i poszanowania prywatności jednostki. Skoro ustawodawca posiadający przymiot racjonalności postanowił, mając na uwadze powyższe, zawęzić spektrum typów czynów zabronionych, w stosunku do których kontrola operacyjna może być prowadzona przez Policję, nie ma argumentów (poza celowościowymi) do dowolnego rozszerzania tego katalogu na inne przestępstwa. Fakt podobieństwa, czy podobnego poziomu zagrożenia ustawowego przestępstw zawartych w omawianym katalogu do innych, ustanowionych w naszym porządku prawnym przestępstw nie może przesądzać o odstąpieniu od ścisłej wykładni literalnej art. 19 ust. 1 ustawy o Policji" (wyrok SN z 30 stycznia 2013 r., sygn. akt III KK 130/12, niepubl.; podobnie postanowienia SN z: 10 października 2012 r., sygn. akt II KK 336/11, OSNKW nr 1/2013, poz. 6; 26 kwietnia 2007 r., sygn. akt I KZP 6/07, OSNKW nr 5/2007, poz. 37). Przestępstwa zawarte w tym katalogu zostały w zasadzie opisane nazwami rodzajowymi, zwykle z przywołaniem przepisów ustawy karnej, w których zostały one stypizowane. Niekiedy ustawodawca dookreślił kategorię przestępstw, powiązując ją ze stopniem zagrożenia dla dóbr prawnie chronionych, którego wystąpienie uzasadniać może zarządzenie kontroli operacyjnej (*vide:* art. 19 ust. 1 pkt 4).

W ramach tego katalogu ustawodawca przewidział w zaskarżonym art. 19 ust. 1 pkt 8 ustawy o Policji możliwość zarządzenia kontroli operacyjnej w celu wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów przestępstw ściganych na mocy umów lub porozumień międzynarodowych oraz zapobiegania takim przestępstwom. W tym wypadku ustawodawca nie wskazał tego, w jakich konkretnie umowach oraz porozumieniach międzynarodowych mają być określone te przestępstwa, ani nie sprecyzował, o jakie rodzaje przestępstw chodzi, czy też jakim dobrom prawnym mają zagrażać. Jedynym w zasadzie ograniczeniem jest, aby były przestępstwami umyślnymi ściganymi z oskarżenia publicznego (art. 19 ust. 1 *in principio* ustawy o Policji), czyli przestępstwami ściganymi przez organy państwa z urzędu lub na wniosek, jeśli sprawca miał zamiar ich popełnienia (chciał je popełnić) albo przewidując możliwość ich popełnienia, na to się godził (art. 9 § 1 k.k.).

Podsumowując, wnioskodawca sformułował trzy zarzuty wobec art. 19 ust. 1 pkt 8 ustawy o Policji. Pierwszy zarzut jest natury formalnej. Dotyczy możliwości zarządzenia kontroli operacyjnej w sytuacjach w istocie zdefiniowanych w aktach podustawowych oraz w aktach niemieszczących się w katalogu źródeł prawa powszechnie obowiązującego. Drugi z kolei zarzut dotyczy niedookreśloności, czy wręcz „blankietowości", przepisu ustalającego przesłanki zarządzenia kontroli operacyjnej, na podstawie którego nie sposób jest ustalić zamkniętego katalogu sytuacji, w jakich nastąpi ingerencja w status jednostki. Trzeci zarzut – ściśle powiązany z drugim – wiąże się z naruszeniem zasady

proporcjonalności przez to, że ustawodawca umożliwił Policji prowadzenie kontroli operacyjnej w zbyt wielu sytuacjach, w związku z czym nie sposób ocenić, czy niejawna ingerencja w prawo do ochrony prywatności oraz wolność i tajemnicę komunikowania się nie jest nadmierna.

8.2.3. Odnosząc się do pierwszego zarzutu, to jest szerokiego rozumienia wyrażenia „umowy i porozumienia międzynarodowe", Trybunał dostrzega wątpliwości interpretacyjne powstające na tle językowej interpretacji tego przepisu. Wykładnia językowa prowadzi do konstatacji, że ustawodawca dopuścił kontrolę operacyjną w odniesieniu do każdego czynu uznawanego za umyślne przestępstwo ścigane z oskarżenia publicznego w świetle wiążących Polskę umów międzynarodowych, zarówno ratyfikowanych za uprzednią zgodą wyrażoną w ustawie (art. 89 ust. 1 Konstytucji), jak i umów ratyfikowanych bez takiej zgody, a nawet umów i innych porozumień niepodlegających ratyfikacji, które byłyby źródłami powszechnie obowiązującego prawa.

Trybunał Konstytucyjny zwraca jednak uwagę na możliwość przyjęcia wykładni art. 19 ust. 1 pkt 8 ustawy o Policji w sposób eliminujący te zastrzeżenia wnioskodawcy. Skoro kwestionowany przepis upoważnia Policję do niejawnej ingerencji w konstytucyjne wolności i prawa jednostek, polegającej na poddaniu kontroli operacyjnej i pozyskaniu za jej pomocą informacji dotyczących ich życia prywatnego lub objętych tajemnicą komunikowania się, to w świetle art. 31 ust. 3 Konstytucji sprecyzowanie okoliczności, w jakich ingerencja taka będzie konstytucyjnie dopuszczalna, może mieć miejsce wyłącznie w aktach normatywnych o randze co najmniej ustawy. Uwzględniając zatem, że kontrola operacyjna dotyczy wolności i praw konstytucyjnych jednostek, a jednocześnie – w świetle Konstytucji – wymaga unormowania ustawowego (*vide:* art. 89 ust. 1 pkt 2 i 5 Konstytucji), warunek ten będą spełniały wyłącznie umowy międzynarodowe ratyfikowane za uprzednią zgodą w ustawie. Wobec tego, nie sposób podzielić poglądu Prezesa Rady Ministrów wyrażonego w opinii przedstawionej w niniejszej sprawie, jakoby procedura poprzedzająca ratyfikację umowy międzynarodowej nie miała znaczenia dla oceny zgodności zakwestionowanego przepisu z Konstytucją. Inaczej rzecz ujmując, jedyną akceptowalną konstytucyjnie interpretacją art. 19 ust. 1 pkt 8 ustawy o Policji jest przyjęcie, że mowa jest w nim o umowach międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie. Niedopuszczalne jest wobec tego zarządzenie kontroli operacyjnej, jeśli ściganie przestępstw przewidują źródła prawa międzynarodowego, które w polskim systemie prawnym mają rangę niższą niż ustawa. Należy podkreślić, że na równi z umowami ratyfikowanymi za uprzednią zgodą wyrażoną w ustawie są również takie umowy, o których mowa w art. 241 ust. 1 Konstytucji. W tym stanie rzeczy przestępstwa przewidziane w umowach międzynarodowych ratyfikowanych poprawnie na podstawie przepisów obowiązujących przed wejściem w życie Konstytucji z 1997 r. będą także mogły uzasadnić – w świetle zakwestionowanego przepisu – zarządzenie przez sąd kontroli operacyjnej.

Istotna w sprawie była jeszcze jedna okoliczność. Wnioskodawca nie przedstawił – również na rozprawie – żadnych przekonujących argumentów, a w szczególności nie wskazał przykładów niepodlegających ratyfikacji umów oraz porozumień międzynarodowych, które zobowiązywałyby Polskę do ścigania przestępstw, w odniesieniu do których możliwe jest zastosowanie kontroli operacyjnej, a które nie mieszczą się w katalogu zdefiniowanym w art. 19 ust. 1 pkt 1-7 ustawy o Policji. Trybunał Konstytucyjny – po analizie wyjaśnień Ministra Spraw Zagranicznych, Ministra Sprawiedliwości, sądów okręgowych i apelacyjnych odnoszących się do rozumienia wyrażenia „przestępstwa ścigane na mocy umów i porozumień międzynarodowych" nie dostrzega, by było ono interpretowane szeroko i obejmowało również przestępstwa

określone w innych źródłach prawa niż umowy międzynarodowe ratyfikowane w trybie określonym w art. 89 ust. 1 Konstytucji.

Trybunał Konstytucyjny stwierdza, że art. 19 ust. 1 pkt 8 ustawy o Policji musi być rozumiany w zgodzie z Konstytucją jako odnoszący się jedynie do przestępstw umyślnych ściganych z oskarżenia publicznego na mocy wiążących Polskę umów międzynarodowych, o których mowa w art. 89 ust. 1 Konstytucji, a ponadto mających status umowy ratyfikowanej za uprzednią zgodą wyrażoną w ustawie, o których mowa w art. 241 ust. 1 Konstytucji. Dokonanie przez Trybunał prokonstytucyjnej wykładni art. 19 ust. 1 pkt 8 ustawy o Policji nie oznacza wyłączenia obowiązku ciążącego na ustawodawcy zachowania należytej precyzji podczas formułowania przepisów. W szczególności ustawodawca musi uwzględnić rozróżnienie przez obecną Konstytucję typów umów międzynarodowych i wynikające stąd konsekwencje.

8.2.4. Trybunał Konstytucyjny nie podziela także innego zarzutu, jakoby zaskarżony przepis był niekonstytucyjny z tego powodu, że nie określa zamkniętego katalogu poważnych przestępstw. Liczba ratyfikowanych umów międzynarodowych, a zatem i liczba przestępstw umyślnych ściganych z oskarżenia publicznego jest bowiem skończona. Katalog ten jest zatem zamknięty, choć dość obszerny.

8.2.5. Wyrażenie „przestępstwa ścigane na mocy umów i porozumień międzynarodowych" z art. 19 ust. 1 pkt 8 ustawy o Policji – przy uwzględnieniu powyższego zawężenia wyłącznie do umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie – nie jest jednoznaczne. Zakwestionowany art. 19 ust. 1 pkt 8 ustawy o Policji mógłby być bowiem rozumiany co najmniej dwojako. Po pierwsze, jako uprawniający do stosowania kontroli operacyjnej w celu zapobiegania przestępstwom ujętym w ratyfikowanych umowach międzynarodowych, które unormowano w polskiej ustawie karnej, a także ich wykrywania i ścigania. Jak można zakładać, byłyby to przestępstwa inne niż wskazane w art. 19 ust. 1 pkt 1-7 ustawy o Policji. W tym wypadku prawną podstawą zarządzenia kontroli operacyjnej byłby art. 19 ust. 1 pkt 8 ustawy o Policji w związku z odpowiednim przepisem polskiej ustawy karnej, penalizującej przestępstwo ścigane na mocy ratyfikowanej umowy międzynarodowej. Po drugie natomiast, jako upoważniający do stosowania kontroli operacyjnej co do przestępstw ściganych na mocy ratyfikowanych umów międzynarodowych, niezależnie od tego, czy ustawodawca uregulował ściganie przestępstw tego rodzaju w polskiej ustawie karnej. Przyjąwszy takie założenie, podstawą zarządzenia kontroli operacyjnej byłby art. 19 ust. 1 pkt 8 ustawy o Policji w związku z odpowiednim przepisem umowy międzynarodowej penalizującej określone zachowanie.

W świetle poglądów prezentowanych w nauce prawa karnego, przepisy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, co do zasady, nie mogą stanowić samodzielnej podstawy postępowania karnego. Przestępstwa penalizowane w tych aktach normatywnych są bowiem opisane w sposób ogólny. Zazwyczaj umowy te nie określają precyzyjnie znamion czynów zabronionych ani sankcji za ich popełnienie. Z reguły państwa sygnatariusze mają prawno-międzynarodowy obowiązek unormowania tych kwestii w ustawodawstwie wewnętrznym, tak by wypełnić ciążące na nich zobowiązanie międzynarodowe, a w konsekwencji zapewnić w krajowym porządku prawnym ściganie tych przestępstw (zob. uchwała SN z 30 lipca 2002 r., sygn. akt I KZP 19/02, OSNKW nr 9-10/2002, poz. 67; por. także A. Marek, *Prawo karne*, Warszawa 2011, s. 81, A. Sakowicz, uwaga 4 do art. 113, [w:] *Kodeks karny. Część ogólna. Tom II. Komentarz do art. 32–116*, red. M. Królikowski, A. Zawłocki, Warszawa 2011, s. 1052). W tym sensie, powyżej wymienione umowy międzynarodowe trudno uznać za umowy w pełni samowykonalne, w rozumieniu art. 91 ust. 1 *in fine* Konstytucji. Nie jest tym samym możliwie na ich podstawie wszczęcie ani prowadzenie postępowania

karnego w odniesieniu do penalizowanych przez nie przestępstw, przynajmniej tak długo, jak długo ich znamiona i sankcje za ich popełnienie nie zostaną doprecyzowane w polskiej ustawie karnej.

Trybunał Konstytucyjny podziela w tym zakresie zawężające rozumienie zaskarżonego przepisu proponowane m.in. przez Ministra Sprawiedliwości zawarte w piśmie z 11 czerwca 2014 r. Tym samym wyrażenie zawarte w art. 19 ust. 1 pkt 8 ustawy o Policji musi być rozumiane wąsko, jako odnoszące się do umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, zobowiązujących państwa strony do penalizacji w prawie krajowym – jako przestępstw – określonych zachowań, zawierających definicję przestępstw i ewentualnie regulujących inne kwestie związane z postępowaniem karnym.

Katalog przestępstw, które mogą być uznane za przestępstwa ścigane na mocy umów międzynarodowych ratyfikowanych za zgodą wyrażoną w ustawie, jest obszerny. Jednakże – jak wynika z opracowania przedstawionego Trybunałowi Konstytucyjnemu przez Ministra Sprawiedliwości w piśmie z 16 stycznia 2014 r., uzupełnionego pismami z 13 maja i 11 czerwca 2014 r. – większość przestępstw przewidzianych w tych umowach jest objęta zakresem normowania art. 19 ust. 1 pkt 1-7 ustawy o Policji. Trybunał przyjmuje te ustalenia na potrzeby rozstrzygnięcia sprawy jako własne. Zaskarżony przez Prokuratora Generalnego przepis będzie mógł stanowić podstawę prawną zarządzenia kontroli operacyjnej wyjątkowo, to jest gdy przestępstwo nie zostało przewidziane w katalogu ustalonym w art. 19 ust. 1 pkt 1-7 ustawy o Policji, a jednocześnie jest unormowanym w polskiej ustawie karnej przestępstwem ściganym na mocy umów międzynarodowych ratyfikowanych za zgodą w ustawie. Jak wynika z wyżej wymienionych pism, takich przestępstw będzie relatywnie niewiele. Potwierdzają to również wyjaśnienia udzielone na rozprawie przez przedstawiciela Komendanta Głównego Policji. W latach 2006-2014 art. 19 ust. 1 pkt 8 ustawy o Policji był podstawą zarządzenia kontroli operacyjnej w około 160 sprawach. Przepis ten był zazwyczaj wskazywany jako dodatkowa (uzupełniająca) podstawa prawna kontroli operacyjnej, oprócz jednego z punktów z art. 19 ust. 1 pkt 1-7. W latach 2006-2014 tylko w kilku wypadkach art. 19 ust. 1 pkt 8 ustawy o Policji był samoistną podstawą zarządzenia kontroli operacyjnej.

Uwzględniając powyższe, Trybunał stwierdza, że art. 19 ust. 1 pkt 8 ustawy o Policji obejmuje swoim zakresem normowania niewielką liczbę przestępstw uznawanych za ścigane na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie i – dodatkowo – stypizowanych w polskiej ustawie karnej, którym zapobieganie oraz których wykrywanie i ściganie należy do właściwości Policji, a które nie mieszczą się w katalogu ustalonym w art. 19 ust. 1 pkt 1-7 tej ustawy. Wbrew twierdzeniom wnioskodawcy, możliwe jest wobec tego ustalenie, o jakie rodzaje przestępstwa chodzi. Trudno więc uznać za zasadny zarzut naruszenia art. 2 Konstytucji.

8.2.6. Przestępstwa ścigane na mocy umów międzynarodowych mających status umów ratyfikowanych za uprzednią zgodą w ustawie mogą być także uznane za przestępstwa poważne w stopniu uzasadniającym dopuszczalność zarządzenia kontroli operacyjnej w celu określonym w art. 19 ust. 1 ustawy o Policji.

Penalizacja czynów w ratyfikowanej umowie międzynarodowej oraz zobowiązanie się Polski do ich ścigania, same w sobie, nie świadczą o tym, że przestępstwo to jest poważne (zob. cz. III, pkt 5.2 uzasadnienia). Obowiązek przestrzegania wiążącego prawa międzynarodowego (art. 9 Konstytucji) nie jest również wystarczającym uzasadnieniem upoważnienia służb policyjnych i ochrony państwa do prowadzenia kontroli operacyjnej. W świetle obecnie obowiązującego stanu prawnego przestępstwa ścigane na mocy umów międzynarodowych nie mogą być jednakże uznane za oczywiście nieproporcjonalnie

ingerujące w prawo do ochrony prywatności i tajemnicę komunikowania się gwarantowane przez art. 47, art. 49 Konstytucji i art. 8 Konwencji. Co do zasady, zobowiązują do ścigania zagrożeń o poważnym ciężarze gatunkowym zagrażającym takim wartościom jak życie, zdrowie czy bezpieczeństwo publiczne. Jednocześnie nie sposób uznać, aby stosowanie zakwestionowanego przepisu przez organy państwa, a zwłaszcza przez Policję i sądy, prowadziło do nadania mu treści niezgodnej z normami, zasadami i wartościami konstytucyjnymi.

Dla Trybunału znaczenie ma jeszcze jedna okoliczność. Wnioskodawca nie wykazał we wniosku ani na rozprawie, odnośnie do których dokładnie rodzajów przestępstw ściganych na mocy umów międzynarodowych ingerencja ustawodawcy w prywatność oraz tajemnicę komunikowania się byłaby nieproporcjonalna. Mając to na uwadze, Trybunał Konstytucyjny stwierdza, że nie obalono domniemania konstytucyjności i konwencyjności zakwestionowanych przepisów.

Uwzględniwszy powyższe, Trybunał Konstytucyjny stwierdza, że art. 19 ust. 1 pkt 8 ustawy o Policji, rozumiany w ten sposób, że dotyczy określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

8.3. Ocena zgodności art. 9e ust. 1 pkt 7 ustawy o SG z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

8.3.1. Zakwestionowany art. 9e ust. 1 pkt 7 ustawy o SG ma następującą treść:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Straż Graniczną w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw (…) ściganych na mocy umów międzynarodowych, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, 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”.

8.3.2. Wnioskodawca sformułował wobec niego takie same zarzuty jak w odniesieniu do art. 19 ust. 1 pkt 8 ustawy o Policji. Analogiczne są również uzasadnienie oraz dowody na jego poparcie. W ocenie Trybunału Konstytucyjnego, nie ma także żadnych okoliczności, m.in. związanych z zakresem ustawowych zadań tej formacji przewidzianych w art. 1 ust. 2 ustawy o SG, które mogłyby determinować odmienną ocenę tego przepisu w porównaniu z art. 19 ust. 1 pkt 8 ustawy o Policji.

W związku z powyższym Trybunał Konstytucyjny stwierdza, że art. 9e ust. 1 pkt 7 ustawy o SG, rozumiany w ten sposób, że dotyczy określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

8.4. Ocena zgodności art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

8.4.1. Zakwestionowany art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej ma następującą treść:

„W ramach czynności operacyjno-rozpoznawczych, podejmowanych przez wywiad skarbowy w celu wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów przestępstw (…) ściganych na mocy umów i porozumień międzynarodowych, jeżeli inne

środki okazały się bezskuteczne albo będą nieprzydatne, Sąd Okręgowy w Warszawie, zwany dalej «Sądem», na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

8.4.2. Wnioskodawca podniósł wobec art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej takie same zarzuty jak w stosunku do art. 19 ust. 1 pkt 8 ustawy o Policji. Tożsame są ponadto uzasadnienie oraz dowody na jego poparcie. W ocenie Trybunału Konstytucyjnego, nie ma też żadnych szczególnych okoliczności, zwłaszcza związanych z zakresem ustawowych zadań tej formacji, określonych w art. 2 tej ustawy, które mogłyby determinować odmienną ocenę tego przepisu w porównaniu z art. 19 ust. 1 pkt 8 ustawy o Policji.

W związku z powyższym Trybunał Konstytucyjny stwierdza, że art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, rozumiany w ten sposób, że dotyczy określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

8.5. Ocena zgodności art. 31 ust. 1 pkt 17 ustawy o ŻW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

8.5.1. Zakwestionowany przepis ma następującą treść:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Żandarmerię Wojskową w granicach zadań określonych w art. 4 ust. 1 oraz w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, pkt 3 lit. b i pkt 5, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw (…) 17) przestępstw ściganych na mocy umów i porozumień międzynarodowych – gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, wojskowy sąd okręgowy, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej i pisemnej zgody właściwego wojskowego prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

8.5.2. Prokurator Generalny podniósł wobec art. 31 ust. 1 pkt 17 ustawy o ŻW takie same zarzuty jak w stosunku do art. 19 ust. 1 pkt 8 ustawy o Policji. Tożsame są ponadto uzasadnienie oraz dowody na jego poparcie.

W ocenie Trybunału Konstytucyjnego, nie ma też żadnych szczególnych okoliczności, które mogłyby nakazywać odmienną ocenę tego przepisu w porównaniu z art. 19 ust. 1 pkt 8 ustawy o Policji. Trybunał Konstytucyjny zwraca dodatkowo uwagę, że ustawodawca zawęził – w porównaniu z pozostałymi służbami – podmiotowy zakres kontroli operacyjnej. Czynności operacyjno-rozpoznawcze mogą być realizowane przez ŻW w granicach ustawowych zadań określonych art. 4 ust. 1 oraz wyłącznie w odniesieniu do osób wymienionych w art. 3 ust. 2 pkt 1, pkt 3 lit. b i pkt 5 ustawy o ŻW. O ile zatem pierwsze zawężenie, tj. ograniczenie dopuszczalności prowadzenia kontroli operacyjnej tylko w ramach ustawowych zadań tej formacji *implicite* funkcjonuje w pozostałych ustawach, o tyle już ustawa o Policji, ustawa o SG, a także ustawa o kontroli skarbowej nie zawężają kręgu podmiotów poddanych kontroli operacyjnej. W myśl art. 3 ust. 2 pkt 1, pkt 3 lit. b i pkt 5 ustawy o ŻW, Żandarmeria Wojskowa wykonuje czynności określone w ustawie w stosunku do żołnierzy pełniących czynną służbę wojskową, pracowników zatrudnionych w jednostkach wojskowych w związku z popełnieniem przez nich czynu zabronionego przez ustawę pod groźbą kary, wiążącego się z tym zatrudnieniem, a także

innych osób niż określone w art. 3 ust. 2 pkt 1-4, podlegających orzecznictwu sądów wojskowych albo jeżeli wynika to z odrębnych przepisów.

W związku z powyższym Trybunał Konstytucyjny stwierdza, że art. 31 ust. 1 pkt 17 ustawy o ŻW, rozumiany w ten sposób, że dotyczy określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

8.6. Ocena zgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

8.6.1. Zakwestionowany art. 27 ust. 1 ustawy o ABW ma następujące brzmienie:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez ABW w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

Z kolei przepis art. 5 ust. 1 pkt 2 lit. b ustawy o ABW brzmi:

„Do zadań ABW należy: rozpoznawanie, zapobieganie i wykrywanie przestępstw godzących w podstawy ekonomiczne państwa".

8.6.2. Rzecznik Praw Obywatelskich zakwestionował obydwa przepisy wyznaczające przedmiotowy zakres kontroli operacyjnej prowadzonej przez ABW, ujmując je związkowo. Nie kwestionuje natomiast ustawowego zakresu zadań tej formacji, wyznaczonego w art. 5 ustawy o ABW. Problem konstytucyjny wynika stąd, iż w przepisie regulującym kompetencję Agencji Bezpieczeństwa Wewnętrznego do stosowania kontroli operacyjnej, tj. art. 27 ust. 1, ustawodawca samodzielnie nie określił jej przedmiotowego zakresu, jak uczynił to chociażby w ustawie o Policji, lecz odesłał do przepisu ogólnie definiującego zadania tej formacji, tj. art. 5 ust. 1 pkt 2 ustawy o ABW. Zdaniem wnioskodawcy zakwestionowane przepisy nie pozwalają rozstrzygnąć, w jakich wypadkach dopuszczalne jest zarządzenie kontroli operacyjnej, a w związku z tym jest możliwe niejawne pozyskiwanie informacji o osobach. Żaden przepis ustawy o ABW nie definiuje wyrażenia „przestępstwa godzące w podstawy ekonomiczne państwa", o którym mowa w art. 5 ust. 1 pkt 2 lit. b. Tego wyrażenia nie można też zrekonstruować na podstawie treści innych aktów normatywnych. W tej sytuacji ciężar wyznaczenia rzeczywistej granicy wolności i praw człowieka został przeniesiony na organy stosujące prawo – sąd okręgowy i ABW. Na poparcie swojej argumentacji Rzecznik przywołał postanowienie sygnalizacyjne o sygn. S 4/10, w którym TK zwrócił uwagę na konieczność dokonania zmian w ustawie o ABW, tak aby ustawa precyzowała rodzaje przestępstw co do których możliwe jest zarządzenie kontroli operacyjnej.

8.6.3. Trybunał Konstytucyjny w obecnym składzie podziela zarzuty Rzecznika Praw Obywatelskich co do niezgodności z Konstytucją art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW.

Trybunał podtrzymuje równocześnie stanowisko zajęte w postanowieniu o sygn. S 4/10. Jak wskazał wówczas: „Sąd Okręgowy w Warszawie, zarządzając kontrolę operacyjną, winien wskazać konkretną osobę oraz typ przestępstwa określonego w ustawie karnej, którego ma dotyczyć kontrola operacyjna. Jednakże w przypadku zarządzenia przez sąd kontroli operacyjnej, w zakresie przestępstw określonych w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, tzn. w zakresie przestępstw «godzących w podstawy ekonomiczne państwa», nie jest to możliwe, gdyż wyrażenie «przestępstwa godzące w podstawy ekonomiczne państwa» uniemożliwia identyfikację typów przestępstw, określonych przez ustawę karną. Niemożność identyfikacji typów przestępstw, określonych przez ustawę

karną, cechująca przepis art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, powoduje w konsekwencji uchybienie dotyczące art. 27 ust. 1 ustawy o ABW. Z przepisu tego nie wynika bowiem, w związku z jakim typem przestępstwa, określonego przez ustawę karną, sąd zarządza kontrolę operacyjną, gdy powołuje się na zadania ABW – w zakresie rozpoznawania, zapobiegania i wykrywania «przestępstw godzących w podstawy ekonomiczne państwa», o których mowa w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW".

Powyższe uwagi zachowują aktualność w niniejszej sprawie. Kodeks karny ani inne ustawy nie posługują się wyrażeniem „przestępstwa godzące w podstawy ekonomiczne państwa", zarówno gdy chodzi o nazwy rodzajowe poszczególnych czynów zabronionych, ich elementy definicyjne, czy tytuły rozdziałów ustaw karnych, w których zebrane są przestępstwa danego rodzaju. Wyrażenie to występowało wprawdzie w nieobowiązującej już ustawie z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz. U. Nr 30, poz. 180, ze zm.); na mocy ustawy z dnia 21 lipca 1995 r. o zmianie ustaw: o urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa, o Straży Granicznej oraz niektórych innych ustaw (Dz. Nr 104, poz. 515) do zadań Urzędu Ochrony Państwa dodano „rozpoznawanie i zapobieganie przestępstwom godzącym w podstawy ekonomiczne państwa i ściganie ich sprawców". Ustawodawca nie sprecyzował jednakże, o jakiego rodzaju przestępstwa chodzi. Wykładnia historyczna nie pozwala również na rekonstrukcję możliwego zakresu normowania obecnie obowiązującej regulacji.

Jak wynika z wyjaśnień na rozprawie, przedstawiciele Prokuratora Generalnego oraz Agencji Bezpieczeństwa Wewnętrznego, czyli organów uczestniczących w przeprowadzaniu kontroli operacyjnej, wskazywali na szeroki i niedookreślony charakter art. 5 ust. 1 pkt 2 lit. b ustawy o ABW. Jak wskazywał przedstawiciel Prokuratora Generalnego, wyrażenie „przestępstwa godzące w podstawy ekonomiczne państwa" jest niejednoznaczne. Nie da się go zawęzić do przestępstw stypizowanych w określonych przepisach ani nawet rozdziałach ustaw karnych. Jego zdaniem, może mieć zastosowanie jako podstawa zarządzenia kontroli operacyjnej m.in. w wypadku przestępstw związanych z obrotem gospodarczym, obrotem pieniędzmi lub innymi środkami płatniczymi, a nawet – co nie jest wykluczone – przestępstw niemających charakteru ściśle ekonomicznego (gospodarczego), lecz wywołujących negatywny skutek dla gospodarki państwa. Z wyjaśnień przedstawiciela ABW wynika z kolei, że na podstawie art. 5 ust. 1 pkt 2 lit. b ustawy o ABW kontrolę operacyjną stosuje się najczęściej w odniesieniu do przestępstw skarbowych oraz innych przestępstw związanych z uszczupleniem należności Skarbu Państwa i nieprawidłowościami w rozliczaniu się z danin publicznych, generalnie popełnianych w związkach lub grupach mających na celu popełnianie przestępstw.

Ustalenie zakresu normowania art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW nie jest także możliwe przez odwołanie się do praktyki orzeczniczej. Trybunał nie uzyskał bowiem od Sądu Okręgowego w Warszawie, w którego kompetencji leży podejmowanie rozstrzygnięć w sprawie kontroli operacyjnej przeprowadzanej przez ABW, wyjaśnień co do rozumienia przez ten sąd wyrażenia „przestępstwa godzące w podstawy ekonomiczne państwa".

Nie bez znaczenia jest ponadto następująca okoliczność. Sąd Okręgowy w Warszawie nie uzasadnia postanowień o zarządzeniu kontroli operacyjnej. Potwierdził to przedstawiciel tego sądu na rozprawie i w pismach kierowanych do Trybunału Konstytucyjnego (zob. cz. I, pkt 3.11.2 uzasadnienia). Niejawny charakter czynności sądowych związanych z rozpoznawaniem wniosków dotyczących kontroli operacyjnej przewidziany w art. 27 ust. 11 ustawy o ABW i wspomniany brak uzasadniania postanowień o zarządzeniu tej kontroli utrudnia wykształcenie się jednolitej linii orzeczniczej co do interpretacji nieostrego wyrażenia zawartego w będącym przedmiotem kontroli art. 5 ust. 1 pkt 2 lit. b ustawy o ABW. Nie jest więc możliwe usunięcie

niejasności tego przepisu dzięki sądowej wykładni, a w rezultacie dostarczenie jednostkom wiedzy o rzeczywistym zakresie ograniczeń prywatności i legalnej ingerencji w tajemnicę komunikowania się.

Trybunał Konstytucyjny podziela stanowisko uczestników postępowania, zgodnie z którym, wobec posłużenia się przez ustawodawcę nieostrym wyrażeniem, odwołującym się do bliżej nieokreślonych „przestępstw godzących w podstawy ekonomiczne państwa", faktyczne granice niejawnej ingerencji w wolności oraz prawa człowieka nie są wyznaczone w sposób dostatecznie określony przez ustawodawcę, a determinują je organy stosujące prawo. Taki stan rzeczy nie jest do pogodzenia z konstytucyjną zasadą określoności prawa (art. 2 Konstytucji) i zasadą ustawowej formy ograniczeń wolności i praw konstytucyjnych (art. 31 ust. 3 Konstytucji).

W ocenie Trybunału Konstytucyjnego, nie jest generalnie niezgodne z Konstytucją zdefiniowanie ustawowych zadań organu państwa – w tym wypadku służby ochrony państwa właściwej w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (art. 1 ustawy o ABW) – w sposób ogólny, z wykorzystaniem pojęć nieostrych. Czymś innym jest natomiast określenie kompetencji powierzonych danej formacji, w następstwie których dochodzić może do niejawnej ingerencji w wolności osobiste. W tym zakresie, jak już wskazano wcześniej (cz. III, pkt 5.1.1 uzasadnienia), ustawodawca powinien wykazać się daleko idącą precyzją, tak by ustawowe przesłanki niejawnej ingerencji możliwe były do ustalenia na podstawie wykładni językowej przepisów ustawy, bez odwoływania się do wykładni systemowej czy funkcjonalnej.

Zakwestionowany przepis – przez zastosowanie nieostrego wyrażenia – nie wyklucza niejawnego pozyskiwania informacji o osobach również w celu rozpoznawania i wykrywania przestępstw, czy zapobiegania przestępstwom, które trudno uznać za poważne i w związku z tym uzasadniające głęboką ingerencję w sferę prywatności i tajemnicę komunikowania się. Na ten problem także zwracali uwagę uczestnicy postępowania w toku rozprawy, podkreślając brak jakiegokolwiek przedmiotowego ograniczenia w zaskarżonym przepisie, np. co do szkodliwości popełnionego czynu czy rozmiarów wyrządzonej szkody.

Trybunał podziela też stanowisko Rzecznika Praw Obywatelskich, zgodnie z którym skoro nie jest możliwe ustalenie, w jakich dokładnie sytuacjach ABW może stosować kontrolę operacyjną, powołując się na przesłankę zawartą w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, to nie sposób uznać, że ten środek pozyskiwania informacji o osobach jest przydatny i konieczny, w rozumieniu art. 31 ust. 3 Konstytucji, w każdym ustawowo dopuszczalnym wypadku.

Mając powyższe na uwadze, Trybunał Konstytucyjny podziela zarzuty wnioskodawcy i stanowisko zajęte przez uczestników niniejszego postępowania co do niezgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

8.7. Ocena zgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji i art. 8 ust. 1 Konwencji.

Rzecznik Praw Obywatelskich, zarzucił kontroli operacyjnej prowadzonej przez ABW, że art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", a także art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. b i c ustawy o ABW nie pozwalają określić precyzyjnie okoliczności zarządzenia kontroli operacyjnej. Kodeks karny ani inne ustawy nie posługują się sformułowaniem „przestępstwo godzące w bezpieczeństwo państwa" i „przestępstwo godzące w podstawy ekonomiczne państwa". Tym samym

zakwestionowane przepisy nie spełniają konstytucyjnego standardu określoności prawa, nie pozwalając ponadto ustalić rzeczywistego zakresu ingerencji w sferę prywatności jednostki. Mając na względzie nieostrość przepisów, a także związaną z tym niemożność zdefiniowania precyzyjnych celów ingerencji, zdaniem RPO, zaskarżone przepisy nie mogą przejść pozytywnie testu proporcjonalności. Skoro nie jest możliwe ustalenie dokładnych okoliczności, w jakich kontrola operacyjna może być zarządzona, nie ma możliwości oceny, czy regulacja ta jest w stanie doprowadzić do zakładanego skutku. Stwarza to ponadto ryzyko arbitralnego wkraczania w prywatność jednostki.

8.7.1. Przepis art. 5 ust. 1 pkt 2 lit. a brzmi następująco:

„Do zadań ABW należy: rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa".

Rzecznik Praw Obywatelskich zakwestionował zgodność art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW tylko w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji. W ocenie wnioskodawcy, nie można na podstawie lektury tego przepisu wskazać, jakie przestępstwa uzasadniają kontrolę operacyjną, prowadzącą do ingerencji w prawo do ochrony prywatności, a także tajemnicę komunikowania się.

8.7.2. Trybunał Konstytucyjny zwraca uwagę, że pojęcie „przestępstw godzących w bezpieczeństwo państwa" – w przeciwieństwie chociażby do „przestępstw godzących w podstawy ekonomiczne państwa" – występujące w uznanym w niniejszej sprawie za niekonstytucyjny art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, jest znane w systemie prawnym. Nie budzi także zasadniczych wątpliwości interpretacyjnych. Do tego pojęcia odnosi się zwłaszcza art. 112 pkt 1 k.k., zgodnie z którym niezależnie od przepisów obowiązujących w miejscu popełnienia czynu zabronionego, ustawę karną polską stosuje się do obywatela polskiego oraz cudzoziemca w razie popełnienia przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej.

8.7.3. Trybunał w dotychczasowym orzecznictwie akceptował różny stopień określoności przepisów związanych z dokonywaniem ingerencji w wolności i prawa jednostek. Istotny jest tu wyrok w sprawie o sygn. K 51/07 (cz. III, pkt 6.1 uzasadnienia), w którym sąd konstytucyjny wypowiedział się m.in. o zgodności z zasadą dostatecznej określoności prawa art. 70a ust. 1 ustawy z dnia 9 czerwca 2006 r. – Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz ustawę o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. Nr 104, poz. 711, ze zm.; dalej: przepisy wprowadzające ustawę o SKW). Przepis ten stanowił, że Przewodniczący Komisji Weryfikacyjnej, w terminie wyznaczonym przez Prezesa Rady Ministrów, sporządza Raport m.in. „o innych działaniach wykraczających poza sprawy obronności państwa i bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polskiej". Trybunał Konstytucyjny w przywołanym wyroku stwierdził: „terminy «obronność państwa» i «bezpieczeństwo Sił Zbrojnych RP» charakteryzują się odpowiednią precyzją dla potrzeb określania zakresu działania organów władzy publicznej. Każda nazwa w języku naturalnym cechuje się pewnym stopniem niedookreśloności, co wiąże się z istotą samego języka. Osiągnięcie wyższego stopnia precyzji przy redagowaniu tekstów aktów normatywnych nie jest możliwe. Ryzyko arbitralnego działania organów władzy publicznej pojawia się przede wszystkim w sytuacjach, w których prawo nie przewiduje sądowej kontroli stosowania prawa przez organy władzy wykonawczej".

Z tej racji Trybunał nie stwierdził w sprawie o sygn. K 51/07 naruszenia zasady dostatecznej określoności prawa (art. 2 Konstytucji). Argumentem, który przesądził o

niekonstytucyjności art. 70a w tej sprawie było wykluczenie przez ustawodawcę sądowej kontroli decyzji podejmowanych przez Przewodniczącego Komisji Weryfikacyjnej (art. 45 ust. 1 Konstytucji) (zob. cz. III, pkt 4.2, 4.7, 4.8 i 6.1 uzasadnienia wyroku o sygn. K 51/07).

8.7.4. Sądową kontrolę czynności operacyjno-rozpoznawczych przewiduje właśnie kwestionowany w niniejszej sprawie art. 27 ust. 1 ustawy o ABW. Stąd Trybunał w rozpatrywanej sprawie podziela podejście w przywołanej sprawie o sygn. K 51/07. Znajduje ono zastosowanie również do pojęcia „przestępstwo godzące w bezpieczeństwo państwa".

8.7.5. Rzecznik Praw Obywatelskich, kwestionując art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa", ograniczył się do przytoczenia judykatów Trybunału Konstytucyjnego oraz ETPC na temat treści prawa do prywatności oraz konstytucyjnych i konwencyjnych wymogów określoności (jakości) prawa dopuszczającego ingerencję w tę jedną z najbardziej podstawowych wolności człowieka. Wnioskodawca nie przeprowadził próby określenia normy prawnej zawartej w art. 5 ustawy o ABW. Pominął, przytaczając (nienależycie precyzyjnie i bez wskazania odpowiednich paragrafów uzasadnienia) wyroki ETPC, z akcentowaną tam szczególnie koniecznością sądowej kontroli decyzji organów policji kryminalnej czy policji bezpieczeństwa skutkujących ingerencją w prywatność tajnym, acz niezbędnym w okolicznościach prowadzonej sprawy, zbieraniem informacji o osobach. W sprawie Klass i inni przeciwko Niemcom (orzeczenie z 6 września 1978 r.), jest o tym mowa w § 56-57, 73-74; w sprawie Malone przeciwko Wielkiej Brytanii (orzeczenie z 2 sierpnia 1984 r.), jest o tym mowa w § 69, 79, 86; w sprawie Kruslin przeciwko Francji (orzeczenie z 24 kwietnia 1990 r.), jest o tym mowa w § 30, 34-35; w sprawie Uzun przeciwko Niemcom (orzeczenie z 2 września 2010 r.), jest o tym mowa w § 63.

8.7.6. Prokurator Generalny, który zgodnie z art. 27 ust. 1 ustawy o ABW, na pisemny wniosek Szefa ABW, występuje (albo nie występuje – bez prawa Szefa ABW do zażalenia) do Sądu Okręgowego w Warszawie o to, aby jeśli inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd ten rozstrzygnął, czy kontrola operacyjna będzie w ogóle dopuszczalna w danej sprawie operacyjnej przeciwko obywatelowi polskiemu lub cudzoziemcowi, nie przedstawił w stanowisku przedłożonym Trybunałowi choćby jednego argumentu dotyczącego sposobu stosowania kontrolowanych tu przepisów. Nie wskazał, że Prokurator Generalny, rozstrzygając o przekazaniu wniosku szefa ABW, albo Sąd Okręgowy w Warszawie, dopuszczając kontrolę operacyjną w sprawie o rozpoznanie lub wykrycie „innego przestępstwa godzącego w bezpieczeństwo państwa", czy zapobieżenie takiemu przestępstwu, mieli problemy wynikające z niedookreśloności tego pojęcia.

8.7.7. Wziąwszy to pod uwagę, Trybunał podkreśla, że w kontroli konstytucyjności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa", z art. 2, art. 47 i art. 49 Konstytucji nie sposób ignorować normy, jaka wynika z całego art. 5 tej ustawy. Z analizy tego przepisu, wyznaczającego katalog zadań Agencji Bezpieczeństwa Wewnętrznego, wynikają następujące wnioski:

8.7.7.1. Ustawowa regulacja całego art. 5 i związku tego przepisu z art. 27 ustawy o ABW, w tym ust. 1, jest kompleksowa, spójna, a także konstrukcyjnie, aksjologicznie i prakseologicznie racjonalna.

8.7.7.2. Błędne jest – z punktu widzenia ustalenia rzeczywistej treści normatywnej regulacji prawnej – wyizolowanie z treści art. 5 jedynie ust. 1 pkt 2 lit. a ustawy o ABW. Prowadzi to do niewłaściwej oceny konstytucyjności tego kompleksowego przepisu.

8.7.7.3. Kompleksowość regulacji całego art. 5 ustawy o ABW wynika z identyfikowania przez prawodawcę chronionych wartości oraz określenia przedmiotu działania ABW za pomocą zastosowania formuły wyznaczenia zadań tego organu policji bezpieczeństwa – właściwego w sprawach ochrony bezpieczeństwa wewnętrznego i porządku konstytucyjnego naszego państwa.

8.7.7.4. Chronione w art. 5 ustawy o ABW wartości są objęte treścią pojęć: bezpieczeństwo państwa, bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, suwerenność i międzynarodowa pozycja państwa, nienaruszalność jego terytorium, obronność państwa, podstawy ekonomiczne państwa, a także m.in. moralność publiczna i sprawność funkcjonowania instytucji państwa (ust. 1 pkt 2 lit. c), zobowiązania prawnomiędzynarodowe państwa z ich przesłankami aksjologicznymi (ust. 1 pkt 5).

Z natury swojej te konstytucyjnie istotne wartości nie mogą być w ustawie szczegółowo wyspecyfikowane, stąd konieczność posłużenia się przez prawodawcę pojęciem ogólnym, „zbierającym" wartości szczegółowe.

8.7.7.5. Spójność regulacji art. 5 ustawy o ABW zapewniają rozstrzygnięcia jej przedmiotu oraz katalog typów zadań nałożonych na ABW, a także ich plasowanie w zazębiających się fazach (stadiach działania).

Z punktu widzenia kontroli konstytucyjnej w niniejszej sprawie szczególnie ważna jest relacja w art. 5 ust. 1 pkt 1 do pkt 2, tzn. zadania w obszarze zagrożeń godzących we wskazane wartości konstytucyjne oraz rozpoznania i ścigania ich sprawców, przy czym w obu tych stadiach realizacji zadań ustawodawca przyjął spójną (identyczną) charakterystykę czasowo-merytoryczną działań: „rozpoznanie, zapobieganie, zwalczanie" (pkt 1) i „rozpoznanie, zapobieganie, wykrywanie" (pkt 2).

8.7.7.6. Ustawodawca zadbał o spójność działań realizujących zadania, stosując formułę dopełnienia (pkt 1 „w szczególności…", pkt 2 lit. a „i innych przestępstw godzących w bezpieczeństwo państwa"), będącą jedyną możliwą do zastosowania przy bogactwie faktycznym i aksjologicznym przedmiotu regulacji. Kierowanie do ustawodawcy postulatu wyczerpującego wyliczenia typów przestępstw w oderwaniu od ogólnego kwalifikatora („godzenie w bezpieczeństwo państwa"), jeśli w ogóle byłoby możliwe, to ocierałoby się o granice legislacyjnej poprawności.

8.7.7.7. Kompletne zindywidualizowanie przestępstw w kontekście normy zawartej w art. 5 ustawy o ABW prowadziłoby do pozostawienia poza regulacją stanów faktycznych i prawnych „godzących w bezpieczeństwo państwa", co bezpośrednio naruszałoby art. 1 Konstytucji oraz mogłoby także bezpośrednio i pośrednio godzić w wolności naszych obywateli gwarantowane zasadą zaufania obywateli do państwa, w tym kontekście – jego zdolności do skutecznej ochrony wartości zawartych w ust. 1 art. 5 tej ustawy.

8.7.7.8. Treść normatywną, w tym wyznaczenie zakresu typologicznego przestępstw, określa także kompleksowe zestawienie wszystkich typów przestępstw w art. 5 ust. 1 pkt 2 lit. a-e ustawy o ABW, tzn. opatrzenie ich kwalifikatorem „bezpieczeństwo państwa" oraz treścią ust. 1, w istocie dookreśla zbiór wszystkich, w tym innych przestępstw, a nie otwiera na zupełnie nowe, nieznane oderwane od treści tego przepisu przestępstwa.

8.7.7.9. Racjonalność prakseologiczna związku art. 5 ust. 1 pkt 2 lit. a z art. 27 ust. 1 ustawy o ABW opisana jest relacją „przedmiot – forma", przy czym ustawodawca wyposażył Sąd Okręgowy w Warszawie w instrumenty decydowania o dopuszczalności kontroli operacyjnej, poprzedzonej przecież rozbudowaną procedurą wstępną (wniosek Szefa ABW – pisemna zgoda Prokuratora Generalnego – możliwość zażądania przez sąd dodatkowych materiałów i wyjaśnień).

8.7.7.10. Pojęcie: bezpieczeństwo państwa, podobnie jak pojęcie: życie prywatne – są szerokimi terminami, niepodlegającymi wyczerpującemu zdefiniowaniu. Mają one kluczowe znaczenie w ważeniu interesu indywidualnego oraz interesu wspólnego w sprawach bezpieczeństwa, w tym bezpieczeństwa prawnego każdego człowieka znajdującego się w obszarze jurysdykcji państwa prawnego. W ważeniu tych interesów główne znaczenie ma w naszym porządku prawnym Sąd Okręgowy w Warszawie orzekający na wniosek Szefa ABW o dopuszczalności kontroli operacyjnej w konkretnej sprawie (zobacz też: § 43 § 77 w przywołanym orzeczeniu ETPC w sprawie Uzun przeciwko Niemcom).

8.7.8. Na końcu tej procedury jest właśnie Sąd Okręgowy w Warszawie, który ma konstytucyjny obowiązek niezawiśle rozważyć treść wniosku, wraz z materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej, Szefa ABW, złożonego po uzyskaniu pisemnej zgody Prokuratora Generalnego, w świetle przedstawionych i – w razie potrzeby uzupełnionych przez wnioskodawcę – okoliczności faktycznych sprawy operacyjnej: rozpoznania / zapobieżenia / wykrycia czynu / czynów mających godzić w bezpieczeństwo państwa). Czyny te, nawet jeśli jednostkowo będące występkami, muszą stwarzać zagrożenie dla dóbr indywidualnych / narodowych / ogólnoludzkich chronionych w rozdziałach XVI, XVII oraz XVIII k.k.

Sąd ten orzeka nie tylko o zgodzie, ale również o określonym we wniosku celu, czasie i rodzaju tej kontroli operacyjnej. Orzekając, Sąd Okręgowy w Warszawie, ma obowiązek w każdej sprawie ważyć wartości określone we wskazanych przez wnioskodawcę wzorcach kontroli: art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 ust. 1 Konwencji.

8.7.9. Rzecznik Praw Obywatelskich i Prokurator Generalny w przedstawionych Trybunałowi pismach zaniechali rozważenia tych argumentów.

8.7.10. Z przedstawionych racji Trybunał orzeka, że kwestionowane w tym punkcie art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa”, jest zgodny z przywołanymi wzorcami: z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji.

8.8. Ocena zgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji i art. 8 ust. 1 Konwencji.

8.8.1 Zgodnie z art. 5 ust. 1 pkt 2 lit. c:

„Do zadań ABW należy rozpoznawanie, zapobieganie i wykrywanie przestępstw 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”.

8.8.2. Trybunał Konstytucyjny nie podziela zarzutów Rzecznika Praw Obywatelskich wobec tego przepisu. Jakkolwiek rację ma wnioskodawca podnosząc, że użyte w zakwestionowanym przepisie sformułowanie „jeśli może to godzić w bezpieczeństwo państwa” może rodzić pewne trudności interpretacyjne, to jednak zdaniem Trybunału, nie ma dostatecznych podstaw, by stwierdzić przekroczenie akceptowalnego konstytucyjnie poziomu nieostrości regulacji ingerującej w prawo do ochrony prywatności i tajemnicę komunikowania się. Przede wszystkim ustawodawca dostatecznie precyzyjnie określił rodzaj przestępstwa co do którego może być zarządzona kontrola operacyjna. Zgodnie z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW mogą być to jedynie „przestępstwa

korupcji". Trybunał Konstytucyjny nie podziela przy tym zastrzeżeń wnioskodawcy i uczestników postępowania, jakoby wyrażenie „korupcja" nie dało się zdefiniować na gruncie obowiązującego ustawodawstwa. Ustawodawca nie posłużył się nim wprawdzie wprost w kodeksie karnym, jednak jest ono znane w polskim systemie prawnym. Możliwe jest wobec tego ustalenie, jakie zachowania mają charakter przestępstw korupcyjnych (*vide:* art. 2 ustawy o CBA czy Prawnokarna konwencja o korupcji sporządzona w Strasburgu dnia 27 stycznia 1999 r., Dz. U z 2005 r. Nr 29, poz. 249). Posłużenie się kodeksowymi wyrażeniami niewątpliwie wzmacniałoby poziom ochrony jednostek. Zdaniem Trybunału, nie jest to jednak bezwzględnie konstytucyjnie wymagane.

Trybunał Konstytucyjny zwraca uwagę, że ustawodawca – oprócz określenia rodzaju (natury) przestępstwa – dookreślił również podmiotową stronę przestępstwa korupcji. Wskazał bowiem, że chodzi o takie przestępstwa korupcji, które są popełnione przez osoby wskazane enumeratywnie w art. 1 i 2 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne.

Trybunał stwierdza, że kontestowane przez wnioskodawcę sformułowanie zawarte w art. 5 ust. 1 pkt 2 lit. c ustawy o ABW zawęża zakres przedmiotowy kontroli operacyjnej, a nie poszerza go. Nie każde bowiem przestępstwo korupcji popełnione przez osoby pełniące funkcje publiczne, o których mowa w art. 1 i art. 2 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, uzasadniać może zarządzenie kontroli operacyjnej, lecz tylko takie, które spełnia kwalifikowany warunek, a mianowicie może godzić w bezpieczeństwo państwa. Wbrew twierdzeniom wnioskodawcy, kwestionowany przepis nie tylko nie osłabia ochrony jednostek przed arbitralnością organów władzy publicznej, ale wręcz ją wzmacnia. W konsekwencji art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW spełnia minimalne wymagania konstytucyjne. Nie można też uznać, że dochodzi do naruszenia art. 8 ust. 1 Konwencji.

Wnioskodawca nie wykazał ponadto, że zakwestionowany przepis – umożliwiając zarządzenie kontroli operacyjnej w celu rozpoznawania i wykrywania przestępstw korupcji popełnianym przez ściśle określone osoby pełniące funkcje publiczne, a zarazem godzącym w bezpieczeństwo państwa czy zapobiegania takim przestępstwom – stanowił nieproporcjonalną ingerencję w wolność i tajemnicę komunikowania się. Zjawisko korupcji było uznawane w orzecznictwie Trybunału Konstytucyjnego za szkodliwe dla interesu publicznego, zwłaszcza dla sprawności i rzetelności działania instytucji publicznych, czego wymaga Konstytucja. Ustawodawca jest więc legitymowany, by takim zjawiskom przeciwdziałać i je zwalczać (por. wyroki TK z: 8 października 2001 r., sygn. K 11/01, OTK ZU nr 7/2001, poz. 210; 13 lipca 2004 r., sygn. K 20/03, OTK ZU nr 7/A/2004, poz. 63; 23 czerwca 2009 r., sygn. K 54/07). Nie sposób uznać wobec tego, że przestępstwa korupcyjne godzące w bezpieczeństwo państwa nie mogą w świetle norm, zasad i wartości konstytucyjnych uzasadniać pozyskiwania w sposób niejawny informacji o osobach. Trybunał stwierdza zatem, że wnioskodawca nie obalił domniemania konstytucyjności zakwestionowanego przepisu.

Mając powyższe na uwadze, Trybunał Konstytucyjny stwierdza, że art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW jest zgodny z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

8.9. Ocena zgodności art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

8.9.1. Zakwestionowany art. 31 ust. 1 ustawy o SKW ma następującą treść:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez SKW w celu realizacji zadań określonych w art. 5, gdy inne środki okazały się

bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

Z kolei art. 5 ust. 1 pkt 1 lit. a ustawy o SKW brzmi następująco:

„Do zadań SKW należy 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 (…) przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w rozdziale XVI ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.), a także innych ustawach i umowach międzynarodowych".

Prokurator Generalny zakwestionował art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW jedynie w zakresie, w jakim odnosi się do wyrażenia „a także innych ustawach i umowach międzynarodowych".

8.9.2. Trybunał Konstytucyjny nie podziela tych zarzutów Prokuratora Generalnego. Ustawodawca sprecyzował bowiem podmiotową i przedmiotową stronę przestępstw, których rozpoznawanie, wykrywanie i ściganie uzasadnia zarządzenie kontroli operacyjnej. Nie wskazał natomiast konkretnych aktów normatywnych, w jakich czyny te są penalizowane. Jednak wbrew twierdzeniom wnioskodawcy takie ujęcie redakcyjne umożliwia ustalenie, kto i w jakiej sytuacji podlegać ma ograniczeniom w zakresie korzystania z wolności lub praw konstytucyjnych. Ustawodawca wskazał jednoznacznie w art. 5 ust. 1 pkt 1 lit. a ustawy o SKW, że chodzi tu o przestępstwa popełniane wyłącznie przez ściśle określone podmioty (tj. żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego, a także pracowników Sił Zbrojnych i innych jednostek organizacyjnych Ministerstwa Obrony Narodowej). Ponadto zastrzegł możliwość zarządzenia kontroli operacyjnej jedynie w określonym celu, jakim jest rozpoznawanie oraz wykrywanie przestępstw przeciwko konkretnym dobrom prawnie chronionym: pokojowi, ludzkości oraz przestępstw wojennych, a także zapobieganie takim przestępstwom. Innymi słowy, określił w ustawie rodzaje (naturę) przestępstw uzasadniających kontrolę operacyjną. Nie dookreślił jedynie, w jakich konkretnie aktach normatywnych, poza wskazanym wprost rozdziałem XVI kodeksu karnego, przestępstwa te mają być penalizowane. Ustalenie, o jakie czyny zabronione chodzi, nie powinno stwarzać ponadprzeciętnych trudności (zob. Statut Międzynarodowego Trybunału Wojskowego – Porozumienie międzynarodowe w przedmiocie ścigania i karania głównych przestępstw wojennych Osi Europejskiej, Dz. U. z 1947 r. Nr 63, poz. 367).

Przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne stanowią najpoważniejsze zagrożenia uznanych konstytucyjnie dóbr (o czym może świadczyć wyłączenie przedawnienia przestępstw przeciw pokojowi i ludzkości w art. 43 Konstytucji czy treść art. 55 ust. 3 Konstytucji), co nie budzi jakichkolwiek wątpliwości. Zapobieganie tym przestępstwom, a także ich wykrywanie i ściganie może – zdaniem Trybunału Konstytucyjnego – uzasadniać wykorzystywanie przez służby ochrony państwa rozmaitych metod niejawnego pozyskiwania informacji. Trudno jest w konsekwencji stwierdzić, że stosowanie kontroli operacyjnej w tym wypadku stanowi nieproporcjonalną ingerencję w wolności i prawa zagwarantowane w art. 47 i art. 49 Konstytucji. Trudno również znaleźć racjonalne argumenty za naruszeniem art. 8 ust. 1 Konwencji.

Sugerowane przez Prokuratora Generalnego ustanowienie statycznego odesłania do konkretnych jednostek redakcyjnych ustawy karnej typizujących przestępstwa wzmacniałoby niewątpliwie poziom ochrony jednostki przed potencjalnym ryzykiem arbitralności organów władzy publicznej. Argument ten nie przesądza jednakże o niedostatecznej określoności zakwestionowanego unormowania ani o

nieproporcjonalnej ingerencji w konstytucyjne prawo do ochrony prywatności i tajemnicę komunikowania się.

Mając powyższe na uwadze, Trybunał Konstytucyjny stwierdza, że art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim obejmuje zwrot „a także innych ustawach i umowach międzynarodowych", jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 ust. 1 Konwencji.

8.10. Inne uwagi.

Na marginesie Trybunał Konstytucyjny zwraca uwagę na szczególne językowe uchybienia dotyczące art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o SG i art. 31 ust. 1 ustawy o ŻW. Po pierwsze, w związku z zastosowaną w tych przepisach interpunkcją – wbrew intencjom ustawodawcy – nieczytelny może stawać się cel kontroli operacyjnej. I tak, z brzmienia art. 19 ust. 1 ustawy o Policji wynikałoby, że kontrola operacyjna może zostać zarządzona nie w celu uzyskania i utrwalenia dowodów umyślnych przestępstw ściganych z oskarżenia publicznego, ale w celu „uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego". Innymi słowy, wynika stąd nielogiczny wniosek, jakoby ustawodawcy chodziło w tym przepisie o dowody ścigane z oskarżenia publicznego, a nie o przestępstwa ścigane z oskarżenia publicznego. Podobnym uchybieniem obarczone są art. 9e ust. 1 ustawy o SG i art. 31 ust. 1 ustawy o ŻW. Po drugie, w świetle brzmienia art. 31 ust. 1 pkt 17 ustawy o ŻW nie jest dostatecznie jasne, czy intencją ustawodawcy było umożliwienie zarządzenia kontroli operacyjnej w celu zapobieżenia jedynie umyślnym przestępstwom ściganym z oskarżenia publicznego na mocy umów lub porozumień międzynarodowych, czy wszystkim przestępstwom ściganym na mocy takich aktów normatywnych, a także wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów jednego lub drugiego typu przestępstw.

Dostosowując do standardu konstytucyjnego ustawową regulację czynności operacyjno-rozpoznawczych, ustawodawca powinien dołożyć szczególnej staranności w kwestii sposobu ich językowego zredagowania.

9. Sposób prowadzenia kontroli operacyjnej.

9.1. Drugim problemem konstytucyjnym, podniesionym we wniosku Rzecznika Praw Obywatelskich z 29 czerwca 2011 r., jest sposób prowadzenia kontroli operacyjnej z wykorzystaniem środków technicznych. Regulują to: art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA i art. 31 ust. 4 pkt 3 ustawy o SKW. Rzecznik Praw Obywatelskich zarzucił naruszenie art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji. W uzasadnieniu wniosku powołał także inne przepisy konstytucyjne gwarantujące m.in. wolność i ochronę tajemnicy komunikowania się (art. 49), nienaruszalność mieszkania (art. 50), autonomię informacyjną (art. 51), a także wolność poruszania się (art. 52 ust. 1 Konstytucji). Zdaniem wnioskodawcy, zakwestionowane przepisy są niezgodne z zasadą określoności prawa, gdyż nie precyzują środków technicznych, które mogą być wykorzystywane przez służby policyjne i ochrony państwa w celu niejawnego pozyskiwania informacji o jednostkach. Standard konstytucyjny byłby zachowany w sytuacji precyzyjnego (enumeratywnego) wymienienia w ustawie dopuszczalnych prawnie środków technicznych, z których poszczególne służby mogą korzystać, a także precyzyjnego wskazania w ustawie, jakiego rodzaju informacje i dowody o jednostce mogą być pozyskane za ich pomocą. Nieprecyzyjność unormowania sprawiać ma, że uprawnione podmioty mogą pozyskiwać

praktycznie każdego rodzaju informacje o jednostce, dotyczące każdej sfery jej życiowej aktywności.

9.2. Ocena zgodności art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA i art. 31 ust. 4 pkt 3 ustawy o SKW z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

9.2.1. Zakwestionowane przepisy mają następującą treść:

Art. 19 ust. 6 pkt 3 ustawy o Policji:

„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”.

Art. 9e ust. 7 pkt 3 ustawy o SG:

„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”.

Art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej:

„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”.

Art. 31 ust. 7 pkt 3 ustawy o ŻW:

„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”.

Art. 27 ust. 6 pkt 3 ustawy o ABW:

„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”.

Art. 17 ust. 5 pkt 3 ustawy o CBA:

„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”.

Art. 31 ust. 4 pkt 3 ustawy o SKW:

„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”.

9.2.2. Zakwestionowane przepisy regulują sposób prowadzenia kontroli operacyjnej za pomocą „środków technicznych”. Ustawodawca we wszystkich zaskarżonych w ramach tej grupy przepisach wymienił przykładowo, jakiego rodzaju informacje i dowody mogą być na ich podstawie pozyskiwane. Są to: „treści rozmów telefonicznych”, a także „inne informacje przekazywane za pomocą sieci telekomunikacyjnych”. W ustawie o SG, ustawie o kontroli skarbowej i ustawie o ŻW przewidziano dodatkowo „obraz” jako treść podlegającą pozyskaniu i utrwaleniu. Z wykładni językowej tych przepisów wynika, że

środki te powinny mieć kwalifikowany charakter. Z jednej strony, mają być oparte na rozwiązaniach technicznych. Wykluczone jest zatem pozyskiwanie na ich podstawie informacji w inny sposób (np. przez śledzenie kogoś, bezpośrednie przejmowanie korespondencji ze skrzynki pocztowej). Z drugiej strony, środki te muszą pozwalać uzyskiwać o jednostce informacje i – kumulatywnie – utrwalić je, w sposób umożliwiający ich następcze wykorzystanie (np. w ramach dalszej analizy kryminalnej czy w procesie karnym). Taka redakcja zaskarżonych przepisów wyklucza dopuszczalność stosowania w toku kontroli operacyjnej, prowadzonej na podstawie art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA i art. 31 ust. 4 pkt 3 ustawy o SKW, środków mających wprawdzie charakter techniczny, lecz niepozwalających utrwalać informacji. Z tego choćby powodu zarzut wnioskodawcy, że katalog środków technicznych, jakie mogą stosować służby policyjne i ochrony państwa, jest nieograniczony, nie zasługuje na uwzględnienie. Jak wcześniej wskazano (cz. III, pkt 5.1.3.2 uzasadnienia), z punktu widzenia zasady określoności prawa i ustawowej formy ograniczeń konstytucyjnych wolności i praw nie jest bezwzględnie konieczne stworzenie zamkniętego katalogu środków technicznych kontroli operacyjnej. W niektórych wypadkach może być to wręcz szkodliwe dla sprawności oraz efektywności działań operacyjnych służb, zważywszy, że sposoby przekazywania informacji są coraz bardziej wyrafinowane. To z kolei mogłoby ograniczać sprawność działania organów państwa odpowiedzialnych za jego bezpieczeństwo i porządek publiczny, prowadząc w konsekwencji do niewywiązywania się państwa z jednego z podstawowych jego zadań, jakim jest ochrona bezpieczeństwa obywateli (art. 5 Konstytucji). Uwzględniwszy warunki ustawowego unormowania czynności operacyjno-rozpoznawczych (zob. cz. III, pkt 5.1 uzasadnienia), Trybunał nie podziela stanowiska wnioskodawcy, jakoby zakwestionowane przepisy były niekonstytucyjne tylko z tego powodu, że nie określają zamkniętego katalogu środków technicznych, a także informacji i dowodów pozyskiwanych za ich pomocą.

9.2.3. We wniosku z 29 czerwca 2011 r. Rzecznik Praw Obywatelskich domaga się, by to przepis ustawy determinował nie tylko rodzaje informacji i dowodów, jakie mogą zostać pozyskane w toku kontroli operacyjnej realizowanej za pomocą środków technicznych, ale również aby ustawodawca sprecyzował, jakie sfery (kręgi) prywatności ingerencja taka może objąć. Zdaniem Trybunału Konstytucyjnego, wątpliwości te są nieuzasadnione. To, jakiej sfery prywatności dotyczy uzyskana informacja, nie jest z reguły uzależnione od formy komunikowania się, a w konsekwencji od sposobu pozyskiwania informacji w trakcie kontroli operacyjnej, lecz od treści wiadomości. Konkretna treść utrwalonej wiadomości może dopiero przesądzić, czy odnosi się ona do sfery życia rodzinnego, intymnego czy zawodowego. Tym samym nie wydaje się możliwie ustalenie *a priori* kręgów prywatności, których może dotykać ingerencja dokonywana na podstawie zaskarżonych przepisów. Zarazem, jak trafnie podnosi Marszałek Sejmu w piśmie z 2 marca 2012 r., „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” (s. 38). Na przykład informacje dotyczące życia seksualnego mogą mieć znaczenie dla zapobieżenia przestępstwu przewidzianemu w art. 200 § 1 k.k. (obcowanie płciowe z małoletnim poniżej 15 roku życia), jego wykrycia i ścigania, zaś informacje o stanie majątkowym, jeśli

chodzi o przestępstwa o charakterze korupcyjnym, które mieszczą się m.in. w zakresie art. 19 ust. 1-7 ustawy o Policji.

Należy mieć ponadto na względzie, że pożądanego przez Rzecznika dookreślenia sfer prywatności nie zawierają pozostałe, niezaskarżone przez niego, przepisy określające sposoby prowadzenia kontroli operacyjnej, tj. kontrola korespondencji i kontrola zawartości przesyłek.

9.2.4. Trybunał Konstytucyjny zwraca uwagę na jeszcze jedną okoliczność, rzutującą na ocenę konstytucyjności zakwestionowanych przepisów. Zdaniem Trybunału zakres normowania art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA oraz art. 31 ust. 4 pkt 3 ustawy o SKW jest węższy, niż to przyjmuje się w doktrynie (zob. cz. III, 6.1.3 uzasadnienia). W rezultacie węższy jest także katalog informacji i dowodów, jakie mogą być pozyskiwane na ich podstawie.

W piśmiennictwie przeciwstawia się co do zasady „kontrolę korespondencji", o której mowa w art. 19 ust. 6 pkt 1 ustawy o Policji, art. 9e ust. 7 pkt 1 ustawy o SG, art. 36c ust. 4 pkt 1 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 1 ustawy o ŻW, art. 27 ust. 6 pkt 1 ustawy o ABW, art. 17 ust. 5 pkt 1 ustawy o CBA oraz art. 31 ust. 4 pkt 1 ustawy o SKW, „stosowaniu środków technicznych", o których mowa w zaskarżonych przepisach (zob. cz. III, pkt 6.1 uzasadnienia). Przyjmuje się mianowicie, że pojęcie korespondencji jest wąskie i obejmuje swym zakresem wyłącznie wiadomości przekazywane za pomocą pisma. Natomiast kontrolę korespondencji elektronicznej, w tym przekazywanej za pomocą Internetu (e-mail) oraz sieci telefonicznych (SMS, MMS itp.), można zarządzić tylko na podstawie art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA i w art. 31 ust. 4 pkt 3 ustawy o SKW. Takie stanowisko zajmowali również przedstawiciele służb na rozprawie.

W ocenie Trybunału, taka zawężająca interpretacja nie jest uzasadniona. Z systemowej wykładni zakwestionowanych przepisów wynika, że stanowią one uzupełnienie i rozszerzenie możliwości pozyskiwania informacji i dowodów ponad to, co umożliwiają m.in. art. 19 ust. 6 pkt 1 i 2 ustawy o Policji, art. 9e ust. 7 pkt 1 i 2 ustawy o SG, art. 36c ust. 4 pkt 1 i 2 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 1 i 2 ustawy o ŻW, art. 27 ust. 6 pkt 1 i 2 ustawy o ABW, art. 17 ust. 5 pkt 1 i 2 ustawy o CBA czy art. 31 ust. 4 pkt 1 i 2 ustawy o SKW. Inaczej mówiąc, zakwestionowane przepisy pozwalają kontrolować inne informacje, niż „treść korespondencji" lub „zawartość przesyłek". Zdaniem Trybunału, wyrażenie „kontrola treści korespondencji" nie zawęża się jedynie do tradycyjnej formy wymiany informacji, lecz obejmuje każdy sposób przekazywania informacji pomiędzy jednostkami, bez względu na formę (tradycyjna poczta, e-mail, SMS, MMS itp.).

9.2.5. Trybunał Konstytucyjny nie znajduje argumentów za uznaniem naruszenia przez zaskarżone przepisy art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji. Podziela w tym kontekście stanowisko Marszałka Sejmu zajęte w piśmie z 2 marca 2012 r., wskazujące na dostateczny poziom gwarancji proceduralnych przeciwdziałających ekscesom organów uprawnionych do stosowania kontroli operacyjnej. W szczególności Trybunał zwraca uwagę, że zarządzenie kontroli operacyjnej następuje w toku kilkuetapowej procedury. Po pierwsze, ustawodawca wymaga pisemnego wniosku szefa danej służby. Po drugie, na wystąpienie z tym wnioskiem do sądu ma wyrazić zgodę Prokurator Generalny bądź prokurator okręgowy właściwy ze względu na siedzibę organu wnoszącego o zarządzenie tej kontroli. Po trzecie, dopiero po uzyskaniu zgody właściwego prokuratora możliwe jest skierowanie wniosku do sądu. Tym samym ograniczono

margines uznania służb policyjnych i ochrony państwa, jeśli chodzi o ingerencję w sferę prywatności jednostek. Nie bez znaczenia jest również precyzyjne określenie w ustawie wymagań formalnych wniosku o jej zarządzenie. Musi on zawierać m.in.: opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej, okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków, dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania, a także cel, czas i rodzaj prowadzonej kontroli operacyjnej (zob. art. 19 ust. 7 ustawy o Policji). Organ wnoszący o zarządzenie kontroli operacyjnej ma ponadto przedstawić sądowi okręgowemu materiały uzasadniające potrzebę jej zastosowania w konkretnym wypadku i w odniesieniu do osób wskazanych we wniosku (art. 19 ust. 1a ustawy o Policji).

Z powyższych przepisów ustaw regulujących kontrolę operacyjną wynika więc istotny wymóg formalny dopuszczalności rozpoznania wniosku o zarządzenie kontroli operacyjnej. Jest nim zdefiniowanie przez organ składający wniosek „sposobu stosowania kontroli operacyjnej" oraz „rodzaju kontroli operacyjnej". Jak wynika z wypowiedzi przedstawicieli służb policyjnych i ochrony państwa obecnych na rozprawie, jest to określane. Niezależnie od sposobu stosowania prawa – zdaniem Trybunału – z treści przepisów ustawowych oraz wydanych na ich podstawie aktów wykonawczych wynika obowiązek wskazania przez organ wnoszący o zarządzenie kontroli operacyjnej nie tylko, której z trzech ustawowych form kontroli żąda (tzn. kontroli korespondencji, zawartości przesyłek lub polegającej na stosowaniu innych środków technicznych), ale także, na czym ma polegać ta kontrola i za pomocą jakich środków będzie przeprowadzona. Określenie „sposobu stosowania kontroli operacyjnej" umożliwia zarazem ocenę, jakiego rodzaju informacje będą mogły zostać pozyskane w czasie jej trwania (np. zapisy rozmów telefonicznych, wiadomości tekstowych lub multimedialnych, rejestracja tras przemieszczania się).

Trybunał Konstytucyjny zwraca uwagę, że organ wnoszący o zarządzenie kontroli operacyjnej ma obowiązek wskazać nie jakikolwiek sposób prowadzenia kontroli operacyjnej, ale wyłącznie sposób przewidziany przez prawo. Jest to konsekwencją konstytucyjnej zasady legalizmu, zgodnie z którą wszystkie organy władzy publicznej mają działać na podstawie i w granicach prawa (art. 7 Konstytucji). A zatem, obowiązujące prawo musi precyzować dopuszczalne dla każdej ze służb „sposoby stosowania kontroli operacyjnej", spośród których organ składający wniosek o taką kontrolę ma dopiero wskazać rekomendowany w danej sprawie. Odpowiada to również wymaganiom stawianym przez Europejski Trybunał Praw Człowieka, który wielokrotnie podkreślał, że środki niejawnego pozyskiwania informacji (ang. *measures of secret surveillance*) powinny być określone przez prawo (ang. *prescribed by law*) (zob. cz. III, pkt 2 uzasadnienia).

Ustawodawca nie sprecyzował elementów, jakie ma zawierać postanowienie sądu o zarządzeniu kontroli operacyjnej, w przeciwieństwie do wymagań wniosku pochodzącego od szefa właściwej służby. Jak ustalił Trybunał Konstytucyjny w toku rozpoznawania niniejszej sprawy (zob. cz. I, pkt 3.11.1 uzasadnienia), w orzecznictwie sądów okręgowych istnieje rozbieżna praktyka dotycząca wskazywania w postanowieniu o zarządzeniu kontroli operacyjnej rodzaju środka technicznego, o którym mowa w art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA oraz art. 31 ust. 4 pkt 3 ustawy o SKW. Co do zasady, sądy nie wskazują w postanowieniu środka technicznego, ograniczając się jedynie do

zdefiniowania, że chodzi o środek techniczny. Mimo braku jednolitej praktyki orzeczniczej w tym zakresie, Trybunał Konstytucyjny uznał za wystarczające dla urzeczywistnienia gwarancji konstytucyjnych przyjęcie takiej wykładni zakwestionowanych przepisów, że organ zarządzający kontrolę operacyjną jest obowiązany do zindywidualizowania w każdej sprawie środka technicznego, jaki ma być stosowany. Z punktu widzenia wymagań konstytucyjnych dopuszczalne jest zastosowanie tylko takiego środka, który przewidziany został przez prawo i może być stosowany przez organ wnoszący o zarządzenie kontroli operacyjnej. Trybunał zwraca ponadto uwagę, że ustrojowa pozycja sądów – jako organów niezależnych od władzy wykonawczej oraz postawionych na straży konstytucyjnych wolności i praw podmiotowych (art. 10, art. 77 ust. 2 Konstytucji) predestynuje je do przeprowadzania kompleksowej oceny wniosków o zarządzenie kontroli operacyjnej, a w konsekwencji także do precyzyjnego wyznaczania jej zakresu oraz sposobów pozyskiwania informacji. Dotyczy to konsekwentnie wskazania w postanowieniu sądu rodzaju środka technicznego, za pomocą którego mają być pozyskiwanie informacje i dowody dotyczące jednostki.

Trybunał Konstytucyjny zauważa dodatkowo, że w świetle wyjaśnień otrzymanych od prezesów sądów apelacyjnych (zob. cz. I, pkt 3.11.1 uzasadnienia) liczba sędziów zajmujących się oceną wniosków o zarządzenie kontroli operacyjnej nie wskazuje, by dochodziło do dysfunkcjonalności systemowej co do oceny przedstawionego sądowi materiału. Nie ma tym samym podstaw do stwierdzenia, jakoby nadzór sądowy, w jego obecnej formie, był fasadowy i nieefektywny, toteż utrudniał lub wręcz uniemożliwiał prowadzenie wnikliwej kontroli wniosków o zarządzenie kontroli operacyjnej pod kątem legalności stosowanych środków technicznych i adekwatności środków, o które wnoszono w konkretnej sprawie.

Mając powyższe na uwadze, Trybunał Konstytucyjny stwierdza, że art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o SG, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o ŻW, art. 27 ust. 6 pkt 3 ustawy o ABW, art. 17 ust. 5 pkt 3 ustawy o CBA oraz art. 31 ust. 4 pkt 3 ustawy o SKW – rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną ma obowiązek wskazać określony w prawie rodzaj środka technicznego pozyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

10. Udostępnianie danych telekomunikacyjnych.

10.1. Trzecim problemem konstytucyjnym jest nieproporcjonalne ograniczenie prawa do ochrony prywatności oraz tajemnicy komunikowania się przez ustawowe unormowanie procedury udostępniania służbom danych telekomunikacyjnych, o których mowa w art. 180c oraz w art. 180d prawa telekomunikacyjnego. Regulują to: art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW i art. 75d ust. 1 ustawy o SC.

Rzecznik Praw Obywatelskich we wniosku z 1 sierpnia 2011 r. wniósł o stwierdzenie niezgodności art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji. W stosunku do tej grupy przepisów wnioskodawca sformułował następujące zarzuty. Po pierwsze, zakwestionowane przepisy umożliwiają Policji, Straży Granicznej i Żandarmerii Wojskowej pozyskanie danych telekomunikacyjnych w celu zapobiegania wszelkim

czynom stanowiącym przestępstwo oraz ich wykrywania, bez względu na doniosłość czynu. Wywiad skarbowy może mieć udostępnione te dane w celu zapobiegania wszystkim przestępstwom skarbowym i przestępstwom korupcji, o których mowa w art. 228-231 k.k., popełnianym przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych, a ponadto naruszeniom krajowych i wspólnotowych przepisów celnych, czyli czynom niebędącym nawet w świetle prawa przestępstwami oraz wykrywania takich przestępstw i deliktów. Natomiast funkcjonariusze CBA, SKW i ABW mogą uzyskiwać te dane w celu realizacji swych wszystkich ustawowych zadań. Po drugie, pozyskiwanie danych telekomunikacyjnych na podstawie zakwestionowanych przepisów nie ma charakteru subsydiarnego. Jest ono dopuszczalne w każdym wypadku, gdy tylko zwrócą się o to odpowiednie służby. Warunkiem uzyskania dostępu do tych danych nie jest wyczerpanie innych środków prawnych, mniej ingerujących w sferę prywatności oraz w tajemnicę komunikowania się. Po trzecie, ustawodawca nie przewidział obowiązku uzyskania zgody sądu ani innego niezależnego organu na pozyskanie tych danych, co *implicite* wynika z art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW. Zdaniem wnioskodawcy, jest to pominięcie prawodawcze, którego ocena mieści się w ramach kognicji Trybunału Konstytucyjnego. Z kolei 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 SKW wyłączają zgodę sądową w sposób wyraźny. Optymalnym rozwiązaniem byłoby powierzenie w tym zakresie kompetencji sądom. Standard konstytucyjny byłby także zachowany wówczas, gdyby kontrolę tę sprawował inny zewnętrzny i niezależny od władzy wykonawczej organ władzy publicznej. Podsumowując, zakwestionowane przepisy w sposób nieproporcjonalny ingerują w wolność i ochronę tajemnicy komunikowania się wynikające z art. 49 Konstytucji, a zarazem – z tych samych powodów – naruszają art. 8 Konwencji.

We wniosku z 27 kwietnia 2012 r. RPO wniósł o stwierdzenie niezgodności art. 75d ust. 1 ustawy o SC z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji. Podniósł w istocie takie same argumenty jak we wniosku z 1 sierpnia 2011 r., rozszerzając jednak wzorce kontroli o art. 47 Konstytucji wyrażający prawo do ochrony prywatności. Rzecznik zwrócił uwagę, że zaskarżony przepis relatywnie wąsko – w porównaniu z wskazanymi wyżej art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW – reguluje przesłanki pozyskania przez Służbę Celną danych telekomunikacyjnych. Dane te mogą być bowiem udostępnione w celu zapobiegania przestępstwom skarbowym, o których mowa w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, ze zm.; dalej: k.k.s.) lub ich wykrywania. Spełniony jest zatem konstytucyjny warunek konkretności unormowania ograniczającego konstytucyjne wolności i prawa. Przepis ten obarczony jest jednakże pozostałymi mankamentami, jak wspomniane wyżej. W szczególności ustawodawca umożliwił udostępnianie Służbie Celnej danych telekomunikacyjnych, nawet gdy istnieją inne mniej dolegliwe dla jednostki sposoby pozyskiwania informacji. Nad pozyskiwaniem danych telekomunikacyjnych nie przewidział również niezależnej zewnętrznej kontroli. W związku z tym art. 75d ust. 1 ustawy o SC narusza art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

Rozszerzenie oraz uzupełnienie argumentów podniesionych we wnioskach Rzecznika Praw Obywatelskich z 1 sierpnia 2011 r. i 27 kwietnia 2012 r. w powyższym zakresie stanowi wniosek Prokuratora Generalnego z 21 czerwca 2012 r. Prokurator Generalny zaskarżył:

– art. 20c ust. 1 ustawy o Policji w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 45, art. 46 ust. 1, art. 49 i art. 49a ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, ze zm.; dalej: prawo prasowe), art. 34 pkt 2, 3 i 4 ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (Dz. U. Nr 92, poz. 881, ze zm.; dalej: ustawa o wyrobach budowlanych), art. 33 ustawy z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach (Dz. U. Nr 63, poz. 322; dalej: ustawa o substancjach chemicznych), art. 77 pkt 2, 2a i 3 ustawy z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2008 r. Nr 213, poz. 1342, ze zm.; dalej: ustawa o ochronie zdrowia zwierząt) i w związku z art. 52 pkt 2 i 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie (Dz. U. z 2013 r. poz. 1226, ze zm.; dalej: prawo łowieckie);

– art. 10b ust. 1 ustawy o SG w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt i w związku z art. 52 pkt 2 i 4 prawa łowieckiego;

– art. 30 ust. 1 ustawy o ŻW w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1-3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 k.k.s., art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt w związku z art. 52 pkt 2 i 4 prawa łowieckiego;

– art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej w związku z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 k.k.s.;

– art. 36b ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej, w związku z art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 k.k.s. oraz w związku z art. 100 ust. 1 i art. 101 ust. 1 ustawy z dnia 19 marca 2004 r. – Prawo celne (Dz. U. Nr 68, poz. 622, ze zm.; dalej: prawo celne);

– art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa”;

– art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b oraz c, jak również pkt 5 ustawy o ABW;

– art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych”;

– art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW w zakresie, w jakim odnosi się do zwrotu „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność”;

– art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW;

– art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o CBA w związku z art. 4, art. 12 ust. 3-6, art. 13 i art. 15 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne;

– art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA w związku z art. 8 ust. 1 i 3 oraz art. 10 ust. 1, 2, 5 i 6 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, art. 35 ust. 1 ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2011 r. Nr 7, poz. 29, ze zm.; dalej: ustawa o wykonywaniu mandatu), art. 87 § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070, ze zm.; dalej: p.u.s.p.), art. 38 ustawy z dnia 23 listopada 2002 r. o Sądzie Najwyższym (Dz. U. Nr 240, poz. 2052, ze zm.; dalej: ustawa o SN), art. 49a ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r. Nr 270, poz. 1599, ze zm.; dalej: ustawa o prokuraturze), art. 24h ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591, ze zm.; dalej: u.s.g.), art. 25c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592, ze zm.; dalej: u.s.p.) oraz w związku z art. 27c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 1590, ze zm.; dalej: u.s.w.);

– art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o CBA w związku z art. 1 ust. 1 i 2 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.; dalej: ustawa o zwrocie korzyści);

– art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 4 ustawy o CBA w związku z art. 200 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz. 759, ze zm.; dalej: u.p.z.p.), art. 46 ust. 1, art. 75 ust. 1-4 i art. 110 ust. 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2010 r. Nr 220, poz. 1447, ze zm.) oraz w związku z art. 3 ust. 1, art. 20a ust. 1-3, art. 3la, art. 36 ust. 1, art. 39 ust. 1 i art. 69e ustawy z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji (Dz. U. z 2002 r. Nr 171, poz. 1397, ze zm.; dalej: ustawa o komercjalizacji);

– art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o CBA;

– art. 75d ust. 1 w związku z ust. 5 ustawy z dnia 27 sierpnia 2009 r. o SC w związku z art. 108 § 2 i art. 109 k.k.s.

Jako wzorce kontroli Prokurator Generalny wskazał art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, a także art. 8 Konwencji. Argumentacja wnioskodawcy opiera się na następującym rozumowaniu: w odniesieniu do wskazanych przez wnioskodawcę rodzajów przestępstw oraz przestępstw skarbowych – określanych przez niego jako „drobne" lub o „niskiej szkodliwości społecznej", a nadto w odniesieniu do niektórych naruszeń prawa niebędących przestępstwami, ingerencja w prywatność jednostki i tajemnicę komunikowania się ma być nadmierna. Prokurator Generalny podważa dopuszczalność udostępniania danych telekomunikacyjnych w wypadkach wskazanych przez niego we wniosku z dwóch powodów. Po pierwsze, dostęp do danych telekomunikacyjnych nie jest środkiem przydatnym do zapobiegania niektórym przestępstwom ani do ich wykrywania, a także realizacji ustawowych zadań danej służby. Po drugie, w wielu wypadkach waga dobra chronionego przez penalizację danego czynu, co do którego mogą być udostępniane dane telekomunikacyjne, lub ewentualnie efektywność wykonywania zadań analityczno-planistycznych, w ramach których mogą być udostępniane te dane, są mniejszej wagi niż ochrona prywatności jednostek oraz zagwarantowanie tajemnicy komunikowania się. Innymi słowy, kolidujące ze sobą dobra nie są właściwie wyważone.

10.2. W niniejszej sprawie Trybunał Konstytucyjny rozpoznaje połączone wnioski Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego, a zatem podmiotów

mających nieograniczoną legitymację do inicjowania postępowania przed Trybunałem Konstytucyjnym. Z punktu widzenia celów niniejszego postępowania, a także ekonomii procesowej, Trybunał Konstytucyjny, uwzględniając argumentację zawartą we wszystkich wnioskach dotyczących gromadzenia i przetwarzania danych telekomunikacyjnych, postanowił najpierw poddać kontroli art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW z art. 49 w związku z art. 31 ust. 3 Konstytucji, a także art. 75d ust. 1 ustawy o SC z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji. Stwierdzenie niekonstytucyjności tych przepisów w całości będzie czyniło zbędnym rozpoznawanie szczegółowych zarzutów Prokuratora Generalnego, ujmujących je w związku z konkretnymi przepisami innych ustaw.

10.3. Trybunał Konstytucyjny zwraca uwagę, że wnioskodawcy nie zakwestionowali przepisów prawa telekomunikacyjnego nakładających na przedsiębiorców telekomunikacyjnych obowiązek zatrzymywania danych telekomunikacyjnych (tzw. retencji danych). Poza zakresem zaskarżenia znajduje się w rezultacie problem dopuszczalności i proporcjonalności tego obowiązku, zakresu danych podlegających retencji i obowiązkowego okresu ich zatrzymywania. Zarzuty wnioskodawców związane z wykorzystywaniem danych telekomunikacyjnych koncentrują się tylko na stosunkowo wąskim problemie udostępniania służbom policyjnym i ochrony państwa – w ramach czynności operacyjno-rozpoznawczych – zatrzymanych danych telekomunikacyjnych. Tak więc zakres zaskarżenia jest stosunkowo wąski. Oceniając jednakże konstytucyjność przepisów kompetencyjnych, które upoważniają organy władzy publicznej do wykorzystywania tych danych w pracy operacyjno-rozpoznawczej, Trybunał nie może ignorować otoczenia normatywnego, w jakim zaskarżone przepisy funkcjonują, oraz sposobu ich stosowania przez właściwe organy. Nie może również pominąć znaczenia wyroku Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. o sygn. C-293/12, który orzekł o nieważności dyrektywy 2006/24/WE (zob. cz. III, pkt 3 uzasadnienia).

10.4. Ocena zgodności art. 20c ust. 1 ustawy o Policji z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.4.1. Zakwestionowany przepis ma następującą treść:

„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".

10.4.2. Zaskarżony przepis upoważnia funkcjonariuszy Policji do gromadzenia oraz przetwarzania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, a także określa przedmiotowe przesłanki udostępniania tych danych na żądanie funkcjonariuszy Policji. Jak wskazano, chodzi tu o dane umożliwiające identyfikację abonenta, dane o ruchu i dane lokalizacyjne (zob. szerzej cz. III, pkt 6.2 uzasadnienia).

Z wykładni językowej art. 20c ust. 1 ustawy o Policji wynika, że funkcjonariuszom Policji mogą być udostępnione dane telekomunikacyjne w celu „zapobiegania lub wykrywania" każdego czynu uznawanego za przestępstwo, a nawet – co nie jest definitywnie wykluczone – również przestępstwo skarbowe. Jedynym ograniczeniem jest to, by zapobieganie określonemu przestępstwu lub jego wykrywanie mieściło się w ramach ustawowych zadań tej formacji, określonych w art. 1 ustawy o Policji. Katalog owych

zadań jest jednak szeroki. Ustawodawca przewidział, że do zadań Policji należy m.in. ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra (art. 1 ust. 2 pkt 1); ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania (art. 1 ust. 2 pkt 2), czy wreszcie wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców (art. 1 ust. 2 pkt 4). Zwłaszcza z brzmienia art. 1 ust. 2 pkt 4 można wyprowadzić wniosek, zgodnie z którym do zadań Policji należy wykrywanie każdego czynu uznawanego za przestępstwo w świetle prawa polskiego. Odnosząc te ustalenia do wykładni zakwestionowanego art. 20c ust. 1 ustawy o Policji, należałoby w konsekwencji przyjmować, że żądanie udostępnienia danych telekomunikacyjnych będzie również możliwe w celu zapobiegania wszelkim czynom przestępnym lub ich wykrywania. Tym samym uzasadnione jest stwierdzenie, że ustawodawca określił cel udostępnienia Policji danych telekomunikacyjnych w sposób bardzo ogólny.

10.4.3. Trybunał Konstytucyjny przypomina, że ingerencja w konstytucyjne prawo do ochrony prywatności (art. 47) i tajemnicę komunikowania się (art. 49 Konstytucji) może mieć miejsce nie tylko w wypadku zapoznawania się organów władzy publicznej z samą treścią komunikatów przekazywanych między jednostkami, ale również w sytuacji pozyskania przez władze informacji towarzyszących temu procesowi (zob. szerzej cz. III, pkt 1.4, 1.10, 6.2 uzasadnienia). Takie stanowisko – jak zwrócono wcześniej uwagę – zajął również TSUE w wyroku z 8 kwietnia 2014 r., stwierdzając nieważność dyrektywy 2006/24/WE. Oznacza to, że udostępnienie Policji danych, o których mowa w art.180c i art.180d prawa telekomunikacyjnego, stanowi ingerencję w prawo do ochrony prywatności i ochrony tajemnicy komunikowania się. Jakkolwiek tego rodzaju ingerencja jest obecnie nieunikniona, bo Policja musi dysponować instrumentarium pozwalającym jej na efektywną walkę z przestępczością, to jednak dopuszczalność tego środka uzależniona jest od spełnienia wymagań wynikających z zasady proporcjonalności (art. 31 ust. 3 Konstytucji).

10.4.4. Trybunał Konstytucyjny podziela zarzuty wnioskodawców co do niezgodności art. 20c ust. 1 ustawy o Policji z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

W pierwszej kolejności Trybunał postanowił odnieść się do zarzutu niedostatecznych gwarancji proceduralnych, związanych z brakiem zewnętrznej kontroli udostępniania danych telekomunikacyjnych. Zarzut ten pozostaje bowiem wspólny dla wszystkich przepisów, które są zakwestionowane w ramach tej grupy. Stwierdzenie ich niekonstytucyjności uczyni zbędnym odnoszenie się do pozostałych zarzutów sformułowanych przez wnioskodawców, a związanych z dopuszczalnością pozyskiwania danych również w celu zapobiegania przestępstwom o relatywnie niewielkim stopniu społecznej szkodliwości oraz ich ścigania, czy z brakiem przesłanki subsydiarności.

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

organów państwa do niejawnego pozyskiwania informacji. Policja może pozyskiwać dane telekomunikacyjne nie tylko dla zwalczania poważnych przestępstw, ale także w sprawach mniejszej wagi, czy wręcz – jak to określił w piśmie z 2 marca 2012 r. Marszałek Sejmu – w sprawach błahych. Przykłady przestępstw, co do których mogą być udostępniane Policji dane telekomunikacyjne, podaje we wniosku z 21 czerwca 2012 r. Prokurator Generalny. Zaliczają się do nich m.in. przestępstwo zniesławienia (art. 212 k.k.), wchodzenia w posiadanie bezprawnie pozyskanej tuszy oraz trofeów zwierząt łownych, a także hodowli lub trzymania bez zezwolenia chartów rasowych i ich mieszańców (art. 52 pkt 2 i 4 prawa łowieckiego. Co więcej, ustawodawca nie uzależniał możliwości żądania danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie – wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji. W takiej sytuacji tym większe znaczenie ma ustanowienie gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych.

Zakwestionowany art. 20c ust. 1 ustawy o Policji, ani żaden inny przepis, nie nakłada obowiązku uzyskania zgody sądu (bądź innego organu, który byłby niezależny od organów żądających udostępnienia tych danych lub organów nad nimi nadrzędnych) na udostępnienie Policji danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego. Procedura ta – jak zresztą wcześniej podkreślono – nie wymaga nawet uzyskania zgody prokuratora. Ustawodawca nie przewidział też zrębowych elementów kontroli *ex post* legalizującej podjęte działania. Pozyskiwanie danych telekomunikacyjnych przez funkcjonariuszy Policji pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane.

Trybunał Konstytucyjny dostrzega, że ustawodawca przewidział w przepisach ustawy o Policji pewne ograniczenia dostępu do danych telekomunikacyjnych. Nie każdy bowiem funkcjonariusz może – w ramach wykonywanych przez siebie czynności – mieć udostępnione te dane. Zgodnie z art. 20c ust. 2 ustawy o Policji, dane telekomunikacyjne, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, mogą być udostępniane funkcjonariuszom, którzy otrzymali stosowne upoważnienie Komendanta Głównego Policji lub komendanta wojewódzkiego Policji. Tego rodzaju gwarancja jest jednakże niewystarczająca, aby zapobiec nadużyciom. Obowiązujące ograniczenia dostępu do danych telekomunikacyjnych zawarte w obecnie obowiązujących przepisach, jakkolwiek potrzebne, nie znoszą obowiązku zapewnienia niezależnej kontroli nad pozyskiwaniem danych telekomunikacyjnych.

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

może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca.

Trybunał Konstytucyjny nie wymaga jednocześnie – przychylając się do argumentacji wnioskodawców i pozostałych uczestników postępowania – by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to należałoby uznać za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także ETPC i TSUE (zob. cz. III, pkt 2 i 3 uzasadnienia).

Mając powyższe na uwadze, art. 20c ust. 1 ustawy o Policji przez to, że nie przewiduje niezależnej kontroli nad udostępnieniem danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, jest niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.5. Ocena zgodności art. 10b ust. 1 ustawy o SG z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.5.1. Zakwestionowany przepis ma następującą treść:

„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”.

10.5.2. Wnioskodawcy sformułowali wobec tego przepisu takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji.

Mimo niemalże tożsamej treści normatywnej art. 10b ust. 1 ustawy o SG oraz art. 20c ustawy o Policji, które przewidują możliwość udostępnienia danych telekomunikacyjnych „w celu zapobiegania lub wykrywania przestępstw”, Trybunał Konstytucyjny zwraca uwagę, że zakwestionowany przepis ustawy o SG musi być odczytywany także w kontekście art. 1 ust. 2 ustawy o SG, regulującego zadania tej formacji. W szczególności art. 1 ust. 2 pkt 4 definiuje rodzaje przestępstw, których rozpoznawanie oraz wykrywanie i którym zapobieganie, a także ściganie ich sprawców należy do właściwości Straży Granicznej.

Trybunał Konstytucyjny stwierdza, że nie jest konieczne rozpoznawanie zarzutów co do zakresu przedmiotowego udostępniania danych telekomunikacyjnych w ustawie o SG ani odnoszenie się do zarzutu braku klauzuli subsydiarności. Art. 10b ust. 1 ustawy o SG ani żaden inny przepis, nie zawiera bowiem minimalnych gwarancji proceduralnych, do których należy konieczność ustanowienia niezależnej kontroli pozyskiwania danych. Stwierdzenie braku tego mechanizmu wystarcza do orzeczenia o niekonstytucyjności zakwestionowanego przepisu.

Mając to na uwadze, art. 10b ust. 1 ustawy o SG przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, jest niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.6. Ocena zgodności art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.6.1. Zakwestionowany przepis ma następującą treść:

„W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b, oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12, wywiad skarbowy może mieć udostępniane dane: 1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej «danymi telekomunikacyjnymi», (…) – oraz może je przetwarzać".

10.6.2. Wnioskodawcy sformułowali wobec tego przepisu takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji.

Trybunał Konstytucyjny zwraca uwagę na odmienności zakwestionowanego przepisu ustawy o kontroli skarbowej od art. 20c ustawy o Policji. Przede wszystkim ustawodawca nie odesłał do wszystkich przestępstw, ale doprecyzował, w jakich wypadkach funkcjonariusze wywiadu skarbowego mogą mieć udostępnione dane telekomunikacyjne. Zgodnie z wykładnią tego przepisu, pozyskiwanie tych danych jest prawnie możliwie w odniesieniu do wszystkich bez wyjątku przestępstw skarbowych, przestępstw określonych w art. 228-231 k.k. popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych, a także do zapobiegania naruszeniom krajowych przepisów celnych i ich wykrywania oraz ścigania naruszeń krajowych lub wspólnotowych przepisów celnych przez wykonywanie nadzoru transgranicznego osób, miejsc, środków transportu i towarów oraz dostawy kontrolowanej, w rozumieniu Konwencji sporządzonej na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi, sporządzonej w Brukseli dnia 18 grudnia 1997 r. (Dz. U. z 2008 r. Nr 6, poz. 31).

10.6.3. Trybunał Konstytucyjny nie przesądza w tym miejscu, czy zakres przedmiotowy dostępu wywiadu skarbowego do danych telekomunikacyjnych spełnia wymagania zasady proporcjonalności. Żaden przepis tej ustawy, ani innego aktu normatywnego, nie ustanawia jednak nawet minimalnych gwarancji proceduralnych, do których należy istnienie niezależnej kontroli udostępniania danych telekomunikacyjnych. Stwierdzenie przez Trybunał braku takiego mechanizmu wystarczy do orzeczenia o niekonstytucyjności zakwestionowanego przepisu.

Mając to na uwadze, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, jest niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.7. Ocena zgodności art. 30 ust. 1 ustawy o ŻW z art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.7.1. Zakwestionowany przepis ma następującą treść:

„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".

10.7.2. Wnioskodawcy sformułowali wobec tego przepisu takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji.

Trybunał Konstytucyjny zwraca uwagę, że ustawodawca węziej unormował przesłanki udostępnienia Żandarmerii Wojskowej danych telekomunikacyjnych, niż przesłanki udostępnienia ich funkcjonariuszom Policji. Z brzmienia zakwestionowanego przepisu wynikałoby wprawdzie, że Żandarmeria Wojskowa może mieć udostępnione dane, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, w celu zapobiegania wszystkim przestępstwom i przestępstwom skarbowym oraz ich wykrywania. Takie stanowisko zajmują też zresztą wnioskodawcy. Należy jednak mieć na uwadze, że ustawodawca ograniczył podmiotowy zakres właściwości Żandarmerii Wojskowej. Zgodnie z art. 4 ust. 1 pkt 4 ustawy o ŻW do jej zadań należy m.in. wykrywanie przestępstw i wykroczeń, w tym skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 tej ustawy, czyli żołnierzy i osób niebędących żołnierzami, jeśli współdziałają one z żołnierzami w popełnianiu przestępstw, przebywają na terenie jednostek wojskowych lub podlegają orzecznictwu sądów wojskowych.

10.7.3. Trybunał Konstytucyjny stwierdza, że niezależnie od tego typu podmiotowego ograniczenia w zakresie przestępstw oraz przestępstw skarbowych, co do których Żandarmerii Wojskowej mogą być udostępnione dane telekomunikacyjne, zakwestionowany przepis, ani żaden inny przepis ustawy nie przewiduje minimalnych gwarancji proceduralnych, do których należy niezależna kontrola udostępniania tych danych. Jej brak jest wystarczającą przesłanką stwierdzenia niekonstytucyjności zakwestionowanego przepisu.

Mając to na uwadze, art. 30 ust. 1 ustawy o ŻW przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, jest niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.8. Ocena zgodności art. 28 ust. 1 pkt 1 ustawy o ABW z art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.8.1. Zakwestionowany przepis ma następujące brzmienie:

„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.)”.

10.8.2. Przepis ten w inny sposób, niż rozpatrywane wyżej, reguluje pozyskiwanie danych telekomunikacyjnych. W przeciwieństwie do przepisu ustawy o Policji, ustawy o SG, ustawy o kontroli skarbowej i ustawy o ŻW, art. 28 ust. 1 ustawy o ABW *expressis verbis* wyłącza obowiązek uzyskania zgody sądu (a ściśle: wydania postanowienia wyrażającego zgodę na udostępnienie funkcjonariuszom ABW danych telekomunikacyjnych). Należy zaznaczyć, że ustawodawca nie przewidział jednocześnie innego, alternatywnego mechanizmu niezależnej kontroli nad pozyskiwaniem tych danych przez funkcjonariuszy ABW, który mógłby zostać uznany za spełniający standard konstytucyjny.

Ponadto ustawodawca upoważnił ABW do pozyskania danych telekomunikacyjnych nie tylko w celu rozpoznawania, wykrywania i ścigania przestępstw (które są uregulowane w art. 5 ust. 1 pkt 2), ale również innych zadań, o których mowa w art. 5 ust. 1 ustawy o ABW. Zaliczają się do nich: rozpoznawanie 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 oraz zapobieganie takim zagrożeniom (pkt 1), 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 (pkt 3), uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (pkt 4) oraz podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (pkt 5). Jednocześnie niektóre zadania w postaci rozpoznawania i wykrywania przestępstw wymienionych w art. 5 ust. 1 pkt 2 ustawy o ABW i zapobiegania takim przestępstwom zostały sformułowane w sposób na tyle ogólny, że nie można na ich podstawie zdefiniować konkretnych okoliczności, w których mogą być udostępniane funkcjonariuszom ABW dane telekomunikacyjne.

10.8.3. Trybunał Konstytucyjny raz jeszcze podkreśla, że relatywnie ogólne wskazanie zadań organu władzy publicznej (w tym wypadku ABW) samo w sobie nie jest niezgodne z Konstytucją. Problem powstaje natomiast wtedy, gdy w ramach takich zadań, organy władzy publicznej mogą podejmować działania ingerujące w wolności i prawa jednostek polegające na niejawnym pozyskiwaniu informacji. Ilekroć organ władzy publicznej jest uprawniony do pozyskiwania informacji o życiu prywatnym jednostek, w tym danych telekomunikacyjnych, konieczne jest bardzo precyzyjne określenie w ustawie przedmiotowego zakresu, w jakich te działania mogą być realizowane.

10.8.4. Mając na uwadze wyjątkowo szeroki zakres okoliczności, w jakich ABW może mieć udostępnione dane telekomunikacyjne, a zarazem jednoznaczne wyłączenie obowiązku uzyskania zgody sądu oraz braku obowiązku uzyskania zgody jakiegokolwiek niezależnego organu na ich pozyskanie, Trybunał stwierdza, że zakwestionowany przepis nie zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia Konstytucji. Jest to wystarczające do stwierdzenia niezgodności art. 28 ust. 1 pkt 1 ustawy o ABW przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.8.5. Na marginesie Trybunał zwraca uwagę na szczególne językowe uchybienia art. 28 ust. 1 ustawy o ABW. Jest on obarczony błędem językowym – niewłaściwą konstrukcją zdania, która utrudnia zrozumienie jego treści. Błąd ten polega na oddaleniu wyrażenia przyimkowego „w postaci danych” od rzeczownika „informacji”. Wyrazy te tworzą związek składniowy. W tym wypadku jest to tzw. związek przynależności, w którym wyrażenie przyimkowe „w postaci danych” pełni funkcję przydawki przyimkowej, będącej określeniem rzeczownika „informacje”.

Zakwestionowany przepis narusza zarówno ogólną regułę naturalnego sąsiedztwa wyrazów, jak i szczegółową regułę umieszczania przydawki przyimkowej zaraz po wyrazie przez nią określanym. Między rzeczownikiem „informacje” a wyrażeniem przyimkowym „w postaci danych” występuje kilkanaście wyrazów. Co więcej, na podstawie językowej analizy przepisu nie jest wykluczone, że w związek składniowy z wyrażeniem przyimkowym „w postaci danych” wchodzi nie rzeczownik „informacje”, lecz rzeczownik „zadania”. Warto również zauważyć, że rzeczownik „informacje” jest określany przez przydawkę przymiotną „niezbędne”. Jeżeli dany rzeczownik jest określany jednocześnie za pomocą przydawki przymiotnej i przydawki przyimkowej, to – aby uniknąć nieporozumienia lub niezręczności stylistycznej – należy go powtórzyć przy każdej przydawce. Zakwestionowany przepis nie respektuje także tej reguły składni polskiej.

Trybunał Konstytucyjny przypomina, że – po pierwsze – „przepisy prawne jako zdania w sensie gramatycznym mają być budowane zgodnie z regułami składni języka polskiego, przyjętymi i stosowanymi powszechnie. Nie ma jakichś swoistych dla tekstu prawnego reguł składni; są one takie same, jak w języku wszelkich innych tekstów” (M. Zieliński, komentarz do § 7 Zasad techniki prawodawczej, [w:] S. Wronkowska, M.

Zieliński, *Komentarz do Zasad techniki prawodawczej z dnia 20 czerwca 2002 r.*, Warszawa 2012, s. 39). Po drugie, poprawność składniowa przepisu, przejrzysta budowa zdań i większych całości, to jeden z podstawowych warunków zrozumiałości tekstów prawnych i tekstów w ogóle (por. H. Jadacka, *Od czego zależy zrozumiałość tekstu?*, [w:] „Przegląd Legislacyjny", nr 4/1995, s. 190). Kwestię tę powinien wziąć pod rozwagę ustawodawca, dokonując zmiany niekonstytucyjnego przepisu.

10.9. Ocena zgodności art. 18 ust. 1 pkt 1 ustawy o CBA z art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.9.1. Zakwestionowany przepis ma następujące brzmienie:

„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»".

10.9.2. Wnioskodawcy sformułowali wobec tego przepisu takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji oraz art. 28 ust. 1 pkt 1 ustawy o ABW. Jednocześnie konstrukcja legislacyjna tego przepisu jest zbliżona do art. 28 ust. 1 pkt 1 ustawy o ABW.

Trybunał Konstytucyjny zwraca uwagę na bardzo szeroki zakres zadań, w wypadku których funkcjonariusze CBA mogą mieć udostępnione dane telekomunikacyjne. Zadania te – co zresztą trafnie wskazał Prokurator Generalny we wniosku z 21 czerwca 2012 r. – nie obejmują wyłącznie rozpoznawania i ścigania poważnych przestępstw oraz zapobiegania im, ale również wykonywanie innych zadań, w tym ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (art. 2 ust. 1 pkt 2 ustawy o CBA), dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych (art. 2 ust. 1 pkt 3 ustawy o CBA), czy wreszcie – 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 (art. 2 ust. 1 pkt 6 ustawy o CBA).

10.9.3. Mając na uwadze wyjątkowo szeroki zakres okoliczności, w jakich CBA może mieć udostępnione dane telekomunikacyjne, a zarazem jednoznaczne wyłączenie obowiązku uzyskania zgody sądu oraz brak obowiązku uzyskania zgody jakiegokolwiek niezależnego organu na ich pozyskanie, Trybunał stwierdza, że zakwestionowany przepis nie zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia Konstytucji. Jest to wystarczające do orzeczenia o niezgodności art. 18 ust. 1 pkt 1 ustawy o CBA przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.10. Ocena zgodności art. 32 ust. 1 pkt 1 ustawy o SKW z art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.10.1. Zakwestionowany przepis ma następującą treść:

„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»".

10.10.2. Wnioskodawcy sformułowali wobec tego przepisu takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji oraz art. 28 ust. 1 pkt 1 ustawy o ABW.

10.10.3. Trybunał Konstytucyjny zwraca uwagę na bardzo szeroki zakres zadań, co do których Służba Kontrwywiadu Wojskowego może pozyskiwać dane telekomunikacyjne. Nie zawężają się do rozpoznawania oraz wykrywania przestępstw wymienionych w art. 5 ust. 1 pkt 1, popełnionych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych i innych jednostek organizacyjnych MON, czy zapobiegania takim przestępstwom. Obejmują też zadania polegające m.in. na uzyskiwaniu, gromadzeniu, analizowaniu, przetwarzaniu i przekazywaniu właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych lub innych jednostek organizacyjnych MON, w zakresie przestępstw określonych w art. 5 ust. 1 pkt 1, a ponadto podejmowanie działań w celu eliminowania ustalonych zagrożeń (art. 5 ust. 1 pkt 6), uczestnictwa w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia (art. 5 ust. 1 pkt 4), czy rozpoznawanie i wykrywanie przestępstw, o których mowa w art. 5 ust. 1, popełnionych we współdziałaniu z żołnierzami pełniącymi czynną służbę wojskową, funkcjonariuszami SKW i SWW lub pracownikami Sił Zbrojnych i innych jednostek organizacyjnych MON.

Jakkolwiek specyfika wojskowej służby kontrwywiadowczej, właściwej w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej, może uzasadniać – do pewnego stopnia – szerszy zakres kompetencji w zakresie pozyskiwania danych telekomunikacyjnych, to jednak zdaniem Trybunału Konstytucyjnego niezbędne jest istnienie gwarancji proceduralnych, które zapobiegną nadużywaniu prawa.

Zakwestionowany przepis ustawy o SKW wprost wyłącza obowiązek uzyskania zgody sądu na uzyskanie dostępu do danych telekomunikacyjnych. Nie przewiduje zarazem innego, alternatywnego mechanizmu kontroli udostępniania funkcjonariuszom SKW tych danych. Nie ma zarazem żadnych argumentów za odstąpieniem od tego wymagania w wypadku tej formacji. Zakwestionowany przepis nie zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia Konstytucji. Mając to na uwadze, Trybunał stwierdza niezgodność art. 32 ust. 1 pkt 1 ustawy o SKW przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.11. Ocena zgodności art. 75d ust. 1 ustawy o SC z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

10.11.1. Zakwestionowany przepis ma następującą treść:

„W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służbie Celnej mogą być udostępniane dane, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej «danymi telekomunikacyjnymi». Służba Celna może przetwarzać udostępnione dane telekomunikacyjne".

10.11.2. Rzecznik Praw Obywatelskich we wniosku z 27 kwietnia 2012 r. sformułował pod adresem art. 75d ust. 1 ustawy o SC, co do zasady, takie same zarzuty i argumenty za jego niezgodnością z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, jak w odniesieniu do art. 20c ust. 1 ustawy o Policji. Nie postawił jednak zarzutu braku konkretności unormowania, ponieważ ustawodawca wyraźnie w art. 75d ust. 1 wskazał, że funkcjonariuszom tej służby dane telekomunikacyjne mogą być udostępniane w ściśle określonym celu, to jest celu zapobiegania przestępstwom skarbowym, o których mowa w rozdziale 9 k.k.s. oraz ich wykrywania. Natomiast przepis ten nie zawiera innych wymaganych konstytucyjnie gwarancji, zwłaszcza nie przewiduje uprzedniej kontroli sądowej ani przesłanki subsydiarności.

10.11.3. Zakwestionowany przepis spełnia kryteria określoności, jakich racjonalnie można wymagać od ustawodawcy. Odsyłając do kodeksu karnego skarbowego, ustawodawca zawęził przedmiotowy zakres pozyskiwania danych telekomunikacyjnych do przestępstw unormowanych w rozdziale 9 tej ustawy. Jednak – na co zwrócił uwagę Prokurator Generalny we wniosku z 21 czerwca 2012 r. – nie wszystkie przestępstwa przewidziane w tym rozdziale są na tyle poważne, by usprawiedliwiały ingerencję w prawo do ochrony prywatności oraz w tajemnicę komunikowania się. Jego zdaniem, charakteru poważnych przestępstw skarbowych nie mają określone w art. 108 § 2 i art. 109 k.k.s. Pierwszy z nich penalizuje urządzanie lub prowadzenie, wbrew przepisom ustawy lub warunkom zezwolenia, loterii fantowej, gry bingo fantowe, loterii promocyjnej lub loterii audioteksowej, gdy nadwyżka z loterii fantowej, gry bingo fantowe, loterii promocyjnej lub loterii audioteksowej była przeznaczona na cel społecznie użyteczny, w szczególności dobroczynny. Przestępstwo takie zagrożone jest karą grzywny do 120 stawek dziennych. Drugi wskazany przez Prokuratora Generalnego czyn, o którym mowa w art. 109 k.k.s., polega na uczestnictwie w grze losowej, zakładzie wzajemnym, grze na automacie, urządzonych lub prowadzonych wbrew przepisom ustawy lub warunkom koncesji lub zezwolenia. Zagrożony jest on także karą grzywny do 120 stawek dziennych.

10.11.4. Trybunał Konstytucyjny stwierdza, że niezależnie od poziomu określoności przedmiotowego zakresu udostępniania Służbie Celnej danych telekomunikacyjnych, art. 75d ust. 1 ustawy o SC, ani żaden inny przepis tej ustawy, nie przewiduje minimalnych gwarancji proceduralnych, do których należy niezależna kontrola nad procesem udostępniania Służbie Celnej danych telekomunikacyjnych.

Mając to na uwadze, Trybunał stwierdza, że art. 75d ust. 1 ustawy o SC przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, jest niezgodny z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

11. Ochrona tajemnicy zawodowej.

11.1. Czwartym problemem konstytucyjnym jest pominięcie prawodawcze polegające na braku unormowania wyłączającego stosowanie czynności operacyjno-rozpoznawczych (tj. kontroli operacyjnej oraz pozyskiwania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego) w odniesieniu do podmiotów zobowiązanych do zachowania tajemnicy zawodowej.

11.2. We wniosku z 13 listopada 2012 r. Prokurator Generalny postawił zarzut pominięcia prawodawczego w art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA oraz art. 31 ustawy o SKW, ponieważ przepisy te nie wyłączają z kręgu podmiotów

poddanych kontroli operacyjnej takich osób, od których pozyskanie informacji objętych tajemnicą adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego oraz lekarską „podlega zakazom dowodowym, w zakresie objętym zakazami". Zdaniem wnioskodawcy, naruszać ma to art. 2, art. 42 ust. 2, art. 47, art. 49 art. 51 ust. 2 oraz art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji, a także art. 6 ust. 3 lit. b oraz c, a ponadto art. 8 i art. 10 ust. 1 Konwencji. Nie została natomiast zakwestionowana dopuszczalność stosowania kontroli operacyjnej w stosunku do duchownego zobowiązanego do zachowania tajemnicy spowiedzi, co do którego również obowiązuje bezwarunkowy zakaz dowodowy (zob. art. 178 pkt 2 k.p.k.).

11.2.1. Rozumowanie wnioskodawcy opiera się na następującym założeniu. Skoro w świetle przepisów postępowania karnego niektóre informacje nie mogą być generalnie wykorzystane jako dowody w postępowaniu karnym, gdyż objęte są bezwarunkowymi albo warunkowymi zakazami dowodowymi, ich pozyskiwanie w drodze kontroli operacyjnej tym bardziej trudno uznać za niezbędne w demokratycznym państwie oraz spełniające wymagania wynikające z zasady proporcjonalności. Zdaniem Prokuratora Generalnego, standard konstytucyjny byłby zachowany, gdyby ustawa nie tylko przewidywała niezwłoczne, komisyjne oraz protokolarne zniszczenie materiałów zebranych w trakcie kontroli operacyjnej niezawierających dowodów pozwalających na wszczęcie postępowania karnego albo dowodów niemających znaczenia dla toczącego się postępowania karnego, lecz wyłączała określone podmioty spod tego rodzaju sposobu pozyskiwania informacji w zakresie, w jakim informacje pozyskiwanie w kontroli operacyjnej objęte są na gruncie postępowania karnego tak zwanymi zakazami dowodowymi. Problem konstytucyjny dotyczy niedopuszczalności pozyskiwania w trakcie kontroli operacyjnej tych informacji, które z uwagi na ich naturę i znaczenie dla wolności i praw jednostek nie mogą być generalnie dostępne osobom trzecim, a szczególnie organom władzy publicznej.

Sposób rozumowania Prokuratora Generalnego może sugerować, jakoby jego intencją było doprowadzenie do poziomej kontroli ustawowej regulacji kontroli operacyjnej z jednej strony z ustawowym unormowaniem zakazów dowodowych z drugiej. Wskazuje na to ujęcie *petitum* wniosku kontestującego przepisy regulujące kontrolę operacyjną „w zakresie objętym zakazami" dowodowymi. Na taki problem zwraca uwagę w swym piśmie Marszałek Sejmu. Mimo pewnych mankamentów argumentacji wniosku Prokuratora Generalnego z 13 listopada 2012 r., zdaniem Trybunału, jego intencje są dostatecznie czytelne. Z treści wniosku wynika bowiem, że istotą postawionych zarzutów jest uregulowanie kontroli operacyjnej w sposób nieprecyzyjny i niegwarantujący dostatecznej ochrony konstytucyjnych wolności oraz praw osób, w interesie których ustanowiono obowiązek zachowania tajemnicy zawodowej i tak zwane zakazy dowodowe. Potwierdza to fragment uzasadnienia, w którym Prokurator Generalny stwierdza, że zaskarżone przez niego przepisy pozostawiają służbom policyjnym oraz służbom ochrony państwa „zbyt szeroki zakres swobody przy stosowaniu kontroli operacyjnej, a tym samym nie pełnią funkcji gwarancyjnej wobec jednostek podlegających takiej kontroli, w zakresie ochrony konstytucyjnych praw i wolności tych jednostek" (s. 55 wniosku). Wnioskodawca potwierdził to również na rozprawie. Dlatego nie ma podstaw do umorzenia postępowania w powyższym zakresie, o co wnosi Marszałek Sejmu, chociaż trudno odmówić słuszności jego twierdzeniu o słabości argumentacji i braku dostatecznej precyzji rozumowania wnioskodawcy.

Wnioskodawca położył nacisk na ochronę tajemnicy obrończej oraz dziennikarskiej. W jego ocenie, brak możliwości nieskrępowanego kontaktu oskarżonego z obrońcą, a nawet świadomość ewentualnego rejestrowania tych rozmów, stanowi naruszenie konstytucyjnego i konwencyjnego prawa do obrony, wyrażonego w art. 42 ust.

2 Konstytucji i art. 6 ust. 3 lit. b i c Konwencji. Naruszanie tej tajemnicy jest niedopuszczalne w demokratycznym państwie prawa. W odniesieniu do tajemnicy dziennikarskiej Prokurator Generalny wskazał, że ochrona dziennikarskich źródeł informacji jest jednym z filarów funkcjonowania wolnych mediów. Możliwość pozyskiwania takich informacji, zwłaszcza jeśli nie mogą być następnie wykorzystane w postępowaniu karnym z uwagi na zakaz dowodowy, godzi w istotę tajemnicy dziennikarskiej.

11.2.2. Trybunał Konstytucyjny, mając na uwadze stanowisko Marszałka Sejmu co do konieczności częściowego umorzenia postępowania w tej sprawie z uwagi m.in. na brak uzasadnienia (s. 9-18 pisma z 13 maja 2013 r.), uznał za niezbędne odniesienie się do kwestii formalnych. Trybunał podziela zastrzeżenia Marszałka Sejmu, że wnioskodawca w żaden sposób nie udowodnił, ani nie uprawdopodobnił, naruszenia art. 2 Konstytucji. W tym zakresie postępowanie podlega umorzeniu z uwagi na niedopuszczalność wydania wyroku (art. 39 ust. 1 pkt 1 ustawy o TK).

Nie ma natomiast podstaw do umorzenia postępowania w odniesieniu do wzorców art. 42 ust. 2, 47, art. 49 i art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji oraz powołanych przez wnioskodawcę przepisów Konwencji, z powodów braków formalnych. Jak wskazano, uzasadnienie w tym zakresie jest częściowo niewystarczające. Niemniej jednak, w ocenie TK, możliwe jest odczytanie intencji wnioskodawcy, kwestionującego – po pierwsze – nadmierną ingerencję w szeroko rozumianą sferę prywatności, a po drugie – naruszenie wolności prasy i jej koniecznego elementu, jakim jest ochrona tajemnicy dziennikarskiej. Trybunał stwierdza wobec tego, że wskazane przepisy konstytucyjne są adekwatnymi wzorcami kontroli i nie ma przeszkód formalnych do ich uwzględnienia w toku oceny badanych regulacji, w zakresie zaskarżonym przez wnioskodawcę.

11.3. Rzecznik Praw Obywatelskich we wniosku z 1 sierpnia 2011 r., kwestionując przepisy o gromadzeniu i przetwarzaniu danych telekomunikacyjnych, również wskazał na niepełność regulacji. W jego ocenie, ustawodawca nie wyłączył w zakwestionowanych przepisach żadnej kategorii osób korzystających z sieci teleinformatycznych z kręgu podmiotów, których dane mogą być pozyskane. W szczególności nie są, zdaniem Rzecznika, uwzględnione szczególne rygory ochrony informacji objętych tajemnicami zawodowymi (adwokacką, notarialną, radcy prawnego, dziennikarską, lekarską – *vide*: art. 180 § 2 k.p.k.), których zniesienie jest możliwe wyłącznie wówczas, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a określonej okoliczności nie można ustalić na podstawie innych dowodów.

Poza ogólnie sformułowanym zarzutem, Rzecznik nie przywołał żadnych argumentów na jego poparcie. Wniosek Rzecznika Praw Obywatelskich nie spełnia w powyższym zakresie wymagań formalnych wynikających z art. 32 ust. 1 pkt 4 ustawy o TK, czyli nie zawiera uzasadnienia z powołaniem dowodów na poparcie postawionego zarzutu. Tym samym postępowanie w powyższym zakresie także podlega umorzeniu na podstawie art. 39 ust. 1 pkt 1 ustawy o TK.

11.4. Odnosząc się do zarzutów sformułowanych przez Prokuratora Generalnego, w ocenie Trybunału Konstytucyjnego, nie znajduje uzasadnienia bezwarunkowe wyodrębnienie jakiejkolwiek kategorii podmiotów spod dopuszczalności objęcia czynnościami operacyjno-rozpoznawczymi, w tym pozyskiwania informacji w trybie kontroli operacyjnej. Konstytucja nie przewiduje w tym zakresie żadnych podmiotowych wyłączeń. Nie oznacza to bynajmniej dopuszczalności pozyskiwania informacji w takim trybie od wszystkich osób w jednakowym stopniu i na jednakowych zasadach. Zdaniem

Trybunału Konstytucyjnego, wyższe standardy konstytucyjności regulacji niejawnego pozyskiwania informacji o jednostkach dotyczą wiadomości przekazywanych osobom wykonującym zawody zaufania publicznego w ramach wykonywanych przez nie funkcji. Jak trafnie zwraca uwagę Naczelna Rada Adwokacka w swojej opinii przedłożonej w niniejszym postępowaniu, tego rodzaju kontakty, zwłaszcza związane z udzielaniem pomocy prawnej, opierają się na szczególnym zaufaniu klientów nie tylko do kwalifikacji zawodowych, ale też do zachowania w dyskrecji przekazywanych treści nierzadko o charakterze ściśle osobistym czy intymnym. Ochrona poufności takich przekazów – a nie osób, którym te informacje powierzono – jest istotnym elementem budującym klimat wzajemnego zaufania i koniecznym warunkiem jego ochrony, w wymiarze indywidualnym i społecznym. Z tego powodu ustawodawca jest zobowiązany chronić poufność wiadomości przekazywanych w warunkach dyskrecji osobom wykonującym zawody zaufania publicznego znacznie intensywniej niż poufność innych informacji przekazywanych między jednostkami. Raz jeszcze należy podkreślić, że ochronie prawnej ma podlegać poufność informacji nie tyle ze względu na osobę depozytariusza tajemnicy, ile raczej z uwagi na charakter przekazywanej informacji.

11.5. Jednym z instrumentów ochrony zaufania jest tajemnica zawodowa i gwarancje jej poszanowania w postępowaniach sądowych. Zaliczają się do nich m.in. bezwarunkowe i warunkowe zakazy dowodowe w postępowaniu karnym, które wskazuje w swoim wniosku Prokurator Generalny i niejako przez pryzmat których domaga się oceny konstytucyjności zakwestionowanych przepisów. W tym kontekście Trybunał Konstytucyjny zwraca uwagę, że ochrona tajemnicy zawodowej, jak i ściśle związane z nią zakazy dowodowe w postępowaniu karnym nie są wartościami autotelicznymi. Jakkolwiek zachowanie poufności przez podmioty wykonujące zawody zaufania publicznego musi być zawsze widziane jako integralna wartość demokratycznego państwa prawa, to jednak podstawową ich funkcją jest ochrona wolności i praw konstytucyjnych jednostek przekazujących w dyskrecji pewne informacje na swój temat osobom wykonującym zawody zaufania publicznego (por. wyrok TK z 2 lipca 2007 r., sygn. K 41/05, cz. III, pkt 7). Ochrona tajemnicy zawodowej powinna być zatem każdorazowo widziana jako przejaw ochrony wolności i praw jednostki, zwłaszcza jej prywatności (art. 47), autonomii informacyjnej (art. 51 ust. 1), prawa do obrony (art. 42 ust. 2), prawa do sądu (art. 45 ust. 1), wolności sumienia i wyznania (art. 53) czy wolności pozyskiwania informacji, w tym wolności prasy (art. 54 ust. 1 Konstytucji). Z tego powodu Trybunał podkreślał – odnosząc się do tajemnicy radcy prawnego – że prawo do prywatności i poufności informacji przysługuje nie radcom prawnym, ale ich klientom; natomiast na radcach prawnych spoczywa obowiązek respektowania tego prawa (zob. wyrok TK z 22 listopada 2004 r., sygn. SK 64/03, OTK ZU nr 10/A/2004, poz. 107, cz. III, pkt 3). Stanowisko to zachowuje aktualność w odniesieniu do pozostałych tajemnic zawodowych.

11.6. W krajowym, jak i europejskim orzecznictwie istotne znaczenie przypisuje się poufności kontaktów oskarżonego z obrońcą w postępowaniu karnym jako integralnego warunku efektywnego korzystania z prawa do obrony (art. 42 ust. 2 Konstytucji i art. 6 ust. 3 lit. b i c Konwencji) i poufności dziennikarskich źródeł informacji jako warunku istnienia wolności przekazywania informacji, a co za tym idzie – wolności prasy (art. 54 ust. 1 Konstytucji, art. 10 ust. 1 Konwencji).

11.6.1. Doniosłość tajemnicy obrończej jako gwarancji konstytucyjnego prawa do obrony, a zarazem konieczność jej intensywniejszej ochrony, wiąże się – na co trafnie zwróciła uwagę Naczelna Rada Adwokacka – ze szczególną specyfiką procesu karnego, w ramach którego są rozstrzygane kwestie istotne z punktu widzenia statusu jednostki, jak

kwestia pozbawienia wolności osobistej i korzystania z praw publicznych. Mając to na uwadze, w orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka wielokrotnie wskazywano, że dla efektywnego korzystania z pomocy obrońcy niezbędne jest zachowanie poufności komunikatów przekazywanych obrońcy przez oskarżonego (podejrzanego) (zob. wyrok z 11 grudnia 2012 r., sygn. K 37/11, OTK ZU nr 11/A/2012, poz. 133, cz. III, pkt 3 oraz cytowane tam orzecznictwo TK i ETPC). Brak możliwości poufnego porozumiewania się oskarżonego ze swoim obrońcą, również za pośrednictwem technologii teleinformatycznych, oznacza, że pomoc prawna traci dużo ze swej skuteczności. Obawiając się niejawnej kontroli rozmów z obrońcą, oskarżony może wszakże zaniechać korzystania z profesjonalnej pomocy prawnej lub nie przekazywać obrońcy istotnych okoliczności sprawy. Jak trafnie sygnalizuje NRA, w takiej sytuacji, obrońca – nie mogąc pozyskać pełni wiedzy o okolicznościach sprawy – nie jest w stanie udzielić pomocy prawnej w najkorzystniejszej dla klienta formie. W konsekwencji taki stan rzeczy może utrudnić skuteczne konstruowanie linii obrony, prowadząc nawet do niesłusznego skazania. Świadomość niejawnego monitorowania kontaktów oskarżonego z obrońcą osłabia również więź zaufania, która jest niezbędna dla prawidłowego wykonywania funkcji obrońcy oraz efektywnej realizacji prawa do obrony. Zapewnienie poufności rozmów oskarżonego z obrońcą jest konieczne nie tylko na etapie postępowania sądowego, lecz w każdej fazie postępowania, nawet prowadzonej przez organ pozasądowy (prokuratora, policję, służbę ochrony państwa). Naruszenie prawa do obrony w fazie przedsądowej może się bowiem przekładać na nierzetelność postępowania sądowego (zob. P. Hofmański, A. Wróbel [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz do artykułów 1-18, Tom 1*, red. L. Garlicki, Warszawa 2010, s. 407 i przywołane tam orzecznictwo ETPC).

11.6.2. Szczególna ochrona dziennikarskich źródeł informacji wiąże się z uznaniem mediów za strażnika demokracji i pluralizmu (zob. orzeczenia ETPC z: 27 marca 1996 r. w sprawie Goodwin przeciwko Wielkiej Brytanii, skarga nr 17488/90; 22 listopada 2007 r. w sprawie Voskuil przeciwko Holandii, skarga nr 64752/01; 14 września 2010 r. w sprawie Sanoma Uitgevers B.V. przeciwko Holandii, skarga nr 38224/03). Brak szczególnej ochrony źródeł informacyjnych prowadzić może do utraty zaufania informatorów do dziennikarzy, a także do obawy przed nawiązywaniem i utrzymywaniem tego rodzaju współpracy. Będzie to stanowić poważną przeszkodę w prawidłowym funkcjonowaniu prasy oraz innych środków masowego przekazu. W orzecznictwie ETPC wskazywano jednocześnie, że nie w każdym wypadku, gdy władze publiczne wchodzą w posiadanie materiałów stanowiących tajemnicę dziennikarską, nawet obejmujących dziennikarskie źródła informacji, ingerencja w prawo określone w art. 10 ust. 1 Konwencji europejskiej jest nieproporcjonalna. W przywołanym wyżej orzeczeniu w sprawie Weber i Saravia przeciwko Niemcom, w której jedną ze skarżących była dziennikarka, zarzucano również naruszenie art. 10 ust. 1 Konwencji przez to, że w drodze monitoringu strategicznego połączeń telekomunikacyjnych możliwe było pozyskanie informacji identyfikujących jej źródła. Europejski Trybunał Praw Człowieka nie dopatrzył się w niemieckich unormowaniach sprzeczności z art. 10 ust. 1 Konwencji. Po pierwsze, strategiczny monitoring połączeń nie był skierowany bezpośrednio na ustalenie danych, na podstawie których można było zidentyfikować źródła informacji – celem nie było ujawnienie tych źródeł. Nie pozyskiwano danych telekomunikacyjnych dziennikarzy, lecz jedynie osób zaangażowanych w działalność przestępczą. Po drugie, jak wskazał ETPC, niemieckie przepisy nie przewidywały wprawdzie szczególnych gwarancji dotyczących ochrony wolności prasy, w szczególności przed ujawnieniem źródeł informacji, jednak zawierały szereg innych (ogólnych) gwarancji minimalizujących ryzyko arbitralności i ekscesów

(zob. § 151-152 uzasadnienia ww. orzeczenia). Z tego powodu ETPC nie uznał naruszenia art. 10 Konwencji.

Problem ujawniania dziennikarskich źródeł informacji pojawił się również w sprawie Telegraaf Media Nederland Landelijke Media B.V. i inni przeciwko Holandii (wyrok z 22 listopada 2012 r., skarga nr 39315/06). ETPC stwierdził (większością pięć do dwóch głosów) naruszenie art. 10 Konwencji. Motywem sprawy było zobowiązanie dziennikarzy przez holenderskie organy władzy publicznej do ujawnienia, kto przekazał informację o nieuprawnionym wycieku tajnych dokumentów z holenderskich służb specjalnych do osób zaangażowanych w działalność przestępczą. Podstawowym celem podsłuchiwania rozmów dziennikarzy w tej sprawie było ustalenie ich informatorów. Ponadto holenderskie prawo nie przewidywało, by uprzednią zgodę na uchylenie tajemnicy dziennikarskiej wydał sąd. Nie było natomiast dla ETPC wystarczające w tym wypadku zagwarantowanie mechanizmów kontroli następczej sprawowanej przez niezależne organy, gdyż kontrola taka nie pozwala przywrócić naruszonej uprzednio poufności źródeł informacji (§ 100-101 uzasadnienia ww. orzeczenia). Podobne stanowisko co do konieczności istnienia uprzedniej sądowej kontroli nad uchylaniem tajemnicy dziennikarskiej ETPC zajął również w wyroku w sprawie Sanoma Uitgevers B.V. przeciwko Holandii, skarga nr 38224/03.

Problem tajemnicy dziennikarskiej był także rozważany w orzecznictwie Trybunału Konstytucyjnego (zob. wyroki TK z 30 października 2006 r., sygn. P 10/06, OTK ZU nr 9/A/2006, poz. 128; 12 maja 2008 r., sygn. SK 43/05, OTK ZU nr 4/A/2008, poz. 57). W wyroku pełnego składu o sygn. P 10/06, Trybunał wskazał na zasadność rozpatrywania tej tajemnicy w perspektywie art. 14 oraz art. 54 Konstytucji. Pierwszy wyraża zasadę ustrojową, podkreślając doniosłość wolności prasy w społeczeństwie demokratycznym. Drugi dotyczy wyrażania poglądów w każdej formie oraz w każdych okolicznościach. Trybunał szerzej nie wypowiadał się natomiast o konstytucyjnych wymogach ochrony tajemnicy dziennikarskiej w kontekście niejawnego pozyskiwania informacji o osobach w drodze czynności operacyjno-rozpoznawczych.

Na znaczenie tajemnicy dziennikarskiej, jako istotnego komponentu wolności prasy i wolności pozyskiwania i rozpowszechniania informacji, zwraca się uwagę w orzecznictwie Sądu Najwyższego. W uchwale z 19 stycznia 1995 r. (sygn. akt I KZP 15/94, OSNKW nr 1-2/1995, poz. 1) SN zaznaczył: „tajemnica zawodowa dziennikarza stanowi niewątpliwie istotny czynnik niezależności prasy i stwarza korzystne warunki dla uzyskania zaufania społecznego. Pozwala bowiem na własną ocenę różnych przejawów życia społecznego, bez konieczności ujawnienia źródeł informacji lub nazwiska autora materiału prasowego. Chroniąca dziennikarza tajemnica zawodowa eliminuje możliwe wpływy na treść publikacji ze strony czynników politycznych i administracyjnych, w tym także policji, organizacji społecznych i zawodowych, różnych grup interesów czy poszczególnych zainteresowanych osób”.

11.7. Między ochroną prywatności, prawa do obrony, wolności sumienia i wyznania, czy też wolności prasy, których ochronę na płaszczyźnie postępowania karnego gwarantuje tajemnica zawodowa oraz chronią wspomniane zakazy dowodowe, z jednej strony, a efektywnym zwalczaniem zagrożeń, z drugiej, może zachodzić kolizja. Pozyskiwanie informacji w drodze kontroli operacyjnej, a nawet sama dopuszczalność zarządzenia kontroli, stanowi wkroczenie w wymagający szczególnej ochrony stosunek zaufania i dyskrecji. Konsekwencje tego mogą być daleko idące, zarówno w wymiarze indywidualnym, wpływając na rzeczywiste korzystanie z konstytucyjnych wolności i praw przez jednostki komunikujące się z osobami wykonującymi zawody zaufania publicznego i powierzające im w związku z tym w poufności informacje, jak i w wymiarze społecznym.

Kolizja obydwu wartości – wbrew twierdzeniom Prokuratora Generalnego – nie jest jednakże tego rodzaju, że pierwszeństwo ma zawsze zyskiwać ochrona wolności i praw jednostki, a pośrednio sama tajemnica zawodowa. Kilkukrotnie zwracał na to uwagę w swym orzecznictwie Trybunał Konstytucyjny (por. wyroki TK z: 22 listopada 2004 r., sygn. SK 64/03, cz. III, pkt 3; 2 lipca 2007 r., sygn. K 41/05, cz. III, pkt 7; 13 grudnia 2011 r., sygn. K 33/08, OTK ZU nr 10/A/2011, poz. 116, cz. III, pkt 6.4), a w niniejszej sprawie stanowisko takie w pełni podtrzymuje. Skoro ochrona poufności pewnych informacji (chronionych na gruncie postępowania karnego za pośrednictwem tajemnicy zawodowych i zakazów dowodowych) służy nieskrępowanemu korzystaniu z wolności i praw konstytucyjnych, to każdorazowe wkroczenie ustawodawcy w tę sferę powinno być rozpatrywane w perspektywie zasady proporcjonalności oraz zgodności z pozostałymi standardami demokratycznego państwa prawnego. Wśród takich wartości jest między innymi ochrona bezpieczeństwa państwa, porządku publicznego lub ochrona wolności i praw innych osób.

Mając to na uwadze, nie jest wykluczone umożliwienie służbom policyjnym i służbom ochrony państwa pozyskanie informacji o charakterze poufnym, przekazywanym podmiotom wykonującym zawody zaufania publicznego. Zważywszy na znaczenie nowych technologii w efektywnej walce z zagrożeniami (zob. cz. III, pkt 1.5-1.7 uzasadnienia), zdaniem Trybunału Konstytucyjnego, ogólne wyłączenie spod kontroli operacyjnej podmiotów zobowiązanych w ustawie do zachowania tajemnicy zawodowej, a nawet wyłączenie informacji uznawanych za stanowiące tajemnicę zawodową, jako bezwzględnie niedopuszczalnych do pozyskania w tym trybie, prowadziłoby do istotnych utrudnień w gromadzeniu materiału dowodowego niektórych rodzajów przestępstw, popełnianych np. z wykorzystaniem nowych technologii. Należy mieć ponadto na uwadze, że nie da się zazwyczaj abstrakcyjnie określić relacji między dobrem, którego ochronie mają służyć zakazy dowodowe (i tajemnica zawodowa), a dobrem wymiaru sprawiedliwości, bezpieczeństwem państwa i porządkiem publicznym w kategoriach „wyższe – niższe" czy „ważniejsze – mniej ważne" (zob. wyrok TK z 13 grudnia 2011 r., sygn. K 33/08, cz. III, pkt 6.4 uzasadnienia). Takie wartościowanie można przeprowadzić *ad casum,* z uwzględnieniem okoliczności konkretnej sprawy. Może się to dokonać dopiero wówczas, gdy znana jest doniosłość zagrożenia, ze względu na które ma być uchylona tajemnica zawodowa, a także waga informacji stanowiących tajemnicę zawodową, które mają być ujawnione. Nie jest wykluczone, że interes, którym jest np. bezpieczeństwo znacznej liczby ludzi w konkretnej sprawie, może przeważyć nad ochroną stosunku poufności, a co za tym idzie uzasadniać utrwalanie poufnych informacji i ich następcze – nawet jedynie operacyjne – wykorzystanie przez organy państwa. Wreszcie nie wolno abstrahować od specyfiki kontroli operacyjnej, która polega nie tyle na utrwalaniu indywidualnych komunikatów przekazywanych między oznaczonymi imiennie osobami, ile na trwającym pewien czas monitoringu źródła informacji (np. podsłuch, kontrolowanie korespondencji pisemnej i elektronicznej) wobec podmiotu objętego stosowanym zarządzeniem sądowym. Dopiero po zakończeniu kontroli oraz analizie zgromadzonych danych jest możliwe zweryfikowanie, jakich treści dotyczą zebrane informacje, i rozstrzygnięcie, które z nich muszą bezwzględnie podlegać ochronie bez możliwości dalszego ich wykorzystania, a które muszą bezwzględnie zostać unicestwione.

Zdaniem Trybunału, punkt ciężkości przesuwa się więc na zapewnienie stosownych gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne oraz służby ochrony państwa informacji, które – z uwagi na ich treść i okoliczności przekazania – powinny podlegać ochronie prawnej. Modelowym rozwiązaniem tego konfliktu dóbr jest przewidziany w art. 180 § 2 k.p.k. mechanizm zwolnienia z tajemnicy zawodowej przez sąd, jeżeli jest to konieczne dla dobra wymiaru

sprawiedliwości, zaś dana okoliczność nie może zostać wykazana w inny sposób, niełamiący tajemnicy zawodowej. Ów mechanizm został pozytywnie oceniony przez Trybunał Konstytucyjny (zob. wyrok TK z 22 listopada 2004 r., sygn. SK 64/03). W ocenie Trybunału, zbliżone w swej istocie rozwiązania legislacyjne powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym. Przeciwnie, standardy te – z uwagi na niejawność kontroli oraz jej ponadprocesowy charakter – powinny być co najmniej zbieżne ze standardami w postępowaniu karnym.

Niezależnie od ustanowienia mechanizmu prewencyjnej sądowej kontroli i selekcji materiałów, co do których zachodzi prawdopodobieństwo, że stanowią tajemnicę zawodową, koniecznym elementem regulacji kontroli operacyjnej jest ponadto istnienie efektywnego mechanizmu umożliwiającego niezwłoczne, komisyjne i protokolarne niszczenie materiałów objętych tajemnicą zawodową, które nie zawierają informacji pozwalających na wszczęcie bądź prowadzenie postępowania karnego z uwagi na ich zbędność z punktu widzenia dalszego postępowania lub niedopuszczalność (brak prawnej możliwości ich wykorzystania w dalszych czynnościach procesowych).

Trybunał Konstytucyjny dostrzega coraz częściej pojawiający się w orzecznictwie i doktrynie kierunek interpretacji przepisów postępowania karnego dotyczących tajemnicy obrończej, że obrońca pozostaje poza kręgiem podmiotów, wobec których dopuszcza się kontrolę i utrwalanie rozmów (zob. zwłaszcza postanowienie SN z 26 października 2011 r., sygn. akt I KZP 12/11, OSNKW nr 10/2011, poz. 90). Stanowisko takie zostało jednak sformułowane na gruncie przepisów k.p.k. regulujących tzw. podsłuch procesowy. Chodzi o to, że skoro niedopuszczalne jest wykorzystanie – jako dowodów w postępowaniu karnym – informacji stanowiących tajemnicę obrończą, ponieważ byłoby to obejście bezwarunkowego zakazu dowodowego ujętego w art. 178 pkt 1 k.p.k., a zarazem nie istnieją prawne przeszkody wykorzystania tych informacji w celu uzyskania innych dowodów (w polskim prawie nie obowiązuje bowiem koncepcja „owoców z zatrutego drzewa"), to jedynym środkiem gwarantującym rzeczywistą ochroną tajemnicy obrończej jest bezwarunkowy zakaz wkraczania w poufność kontaktów między oskarżonym a obrońcą. Innymi słowy, zakaz kontroli i utrwalania rozmów obrońcy. Zwraca na to uwagę w piśmie z 13 maja 2013 r. Marszałek Sejmu. Wyprowadza on jednakże dalej idące wnioski, wskazując na konieczność rozciągnięcia tego zakazu na pozaprocesową kontrolę operacyjną. W konsekwencji w stosunku do obrońcy nie jest możliwie – zdaniem Marszałka Sejmu – stosowanie kontroli operacyjnej. Pogląd ten wydaje się także rozciągać na niedopuszczalność pozyskiwania informacji umożliwiających identyfikację dziennikarskich źródeł informacji.

Trybunał Konstytucyjny nie neguje przyjmowania takiej interpretacji obowiązujących przepisów przez sądy, które w każdym wypadku przyznają pierwszeństwo ochronie tajemnicy obrończej, a przez to poufności kontaktów oskarżonego z obrońcą, chociaż – czego nie można wykluczyć – może to osłabiać walkę z poważnymi zagrożeniami. Standard przyjęty przez sądy i aprobowany w piśmiennictwie przewyższa jednakże to, czego Konstytucja wymaga, gdyż – jak pokreślono – z Konstytucji trudno byłoby wyprowadzić bezwzględne zakazy podmiotowe tego rodzaju. Trybunał w rozpatrywanej sprawie nie podziela jednocześnie optymistycznego wniosku Marszałka Sejmu, że przyjmowana w orzecznictwie interpretacja przepisów k.p.k. i jej odpowiednie stosowanie na gruncie zakwestionowanych regulacji – rozwiązuje wszystkie problemy konstytucyjne i gwarantuje należytą ochroną osób zobowiązanych do zachowania tajemnicy zawodowej na gruncie kontroli operacyjnej. Potwierdza to także pismo Prezesa SN Izby Wojskowej, który wskazuje na brak należytych gwarancji tajemnicy zawodowej

w toku czynności operacyjno-rozpoznawczych, wynikających z treści przepisów bądź orzecznictwa sądowego. Podobne stanowisko zajęli prezesi sądów okręgowych i apelacyjnych, do których Trybunał Konstytucyjny zwrócił się o wyjaśnienia w sprawie stosowania przepisów regulujących kontrolę operacyjną (zob. cz. I, pkt 3.11 uzasadnienia). Wynika z nich, że nie sposób mówić o wykształceniu się linii orzeczniczej gwarantującej ochronę tajemnicy zawodowej w trakcie kontroli operacyjnej.

Zdaniem Trybunału Konstytucyjnego, nawet jeśli przyjąć sugerowaną przez Marszałka Sejmu prokonstytucyjną wykładnię zaskarżonych unormowań, to potencjalny zakaz kontroli operacyjnej osób zobowiązanych do jej zachowania, a zwłaszcza obrońców i dziennikarzy, nie oznacza braku możliwości wejścia przez służby policyjne i służby ochrony państwa w posiadanie informacji stanowiących tego rodzaju tajemnicę (np. w toku stosowania kontroli wobec oskarżonych czy udzielających dziennikarzom informacji). Ponadto nie rozstrzyga o sposobie postępowania z takimi materiałami ani nie pozwala rozstrzygnąć o zakresie ochrony poufnych informacji przekazywanych osobom wykonującym inne zawody zaufania publicznego i zobowiązanym do zachowania w dyskrecji otrzymanych informacji, objętych na gruncie ustawowym tajemnicą zawodową.

Uwzględniwszy powyższe rozważania, Trybunał Konstytucyjny postanowił przejść do oceny poszczególnych zaskarżonych przepisów z Konstytucją.

11.8. Ocena zgodności art. 19 ustawy o Policji z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.8.1. Trybunał Konstytucyjny podziela wątpliwości wnioskodawcy co do braku w zakwestionowanym przepisie (oraz w pozostałych przepisach powszechnie obowiązujących) dostatecznych gwarancji proceduralnych zapewniających ochronę poufności informacji przekazywanych podmiotom wykonującym zawody zaufania publicznego. Nie przewiduje on – w sposób niebudzący wątpliwości interpretacyjnych – ani obowiązku uprzedniej, sądowej kontroli zgromadzonych danych, ani ewentualnego zwolnienia (uchylenia) z tajemnicy zawodowej w konkretnej sprawie. Nie chodzi bynajmniej o wydanie postanowienia wyrażającego zgodę na zarządzenie kontroli operacyjnej (która i tak jest *de lega lata* wymagana). Mankamentem konstytucyjnym art. 19 ustawy o Policji jest niezagwarantowanie w ustawie, że w sytuacji uzasadnionego podejrzenia, że zgromadzone materiały zawierają informacje objęte tajemnicę zawodową i z tego powodu wymagają szczególnej ochrony, nastąpi dodatkowa weryfikacja tych materiałów przez sąd i ewentualne zwolnienie z tajemnicy zawodowej, zanim zostaną przekazane funkcjonariuszom służb bądź prokuratorowi. Trybunał ma świadomość ryzyka, jakie niesie możliwość zapoznania się przez funkcjonariuszy służb z informacjami stanowiącymi tajemnice zawodowe, zwłaszcza wobec braku jednoznacznego ustawowego zakazu wykorzystywania dowodów pochodzących z „zatrutego drzewa". Ryzyko to jest poważne, aczkolwiek nie na tyle, aby usprawiedliwiać zupełne wyłączenie określonej grupy podmiotów – również obrońców i dziennikarzy – spod kontroli operacyjnej. W tym stanie rzeczy to do ustawodawcy należy wprowadzenie rozwiązań prawnych, które zapobiegną ryzyku wykorzystania informacji wymagających ochrony lub przynajmniej zminimalizują to ryzyko.

Zakwestionowane przepisy nie przewidują również procedury niszczenia zebranych w toku kontroli operacyjnej informacji, stanowiących tajemnicę zawodową. Zdaniem TK, takiej podstawy – bez żadnych wątpliwości interpretacyjnych – nie da się wyprowadzić m.in. z art. 19 ust. 15b i 17 ustawy o Policji oraz odpowiednio stosowanych art. 238 § 3-5 i art. 239 k.p.k. Stosownie do art. 19 ust. 15b ustawy o Policji, na prokuratorze spoczywa obowiązek każdorazowego weryfikowania materiałów zebranych w toku kontroli operacyjnej i podjęcia decyzji o zakresie i sposobie ich wykorzystania. Zgodnie z

odpowiednio stosowanym art. 238 § 3 k.p.k., jeśli materiały zebrane w trakcie owej kontroli w całości nie mają znaczenia dla postępowania karnego, prokurator – po jej zakończeniu – wnosi o ich zniszczenie. Natomiast jeśli nie mają one znaczenia dla postępowania karnego, w którym zarządzono kontrolę i utrwalanie rozmów telefonicznych, oraz nie stanowią dowodu, o którym mowa w art. 237a, to stosownie do art. 238 § 4 k.p.k., prokurator wnosi o zarządzenie ich zniszczenia w tej właśnie części. Sąd orzeka w przedmiocie tego wniosku na posiedzeniu, w którym mogą wziąć udział strony. Z kolei zgodnie z art. 238 § 5 k.p.k., jeśli prokurator nie wniesie o zniszczenie materiałów lub zapisów zebranych w trakcie kontroli operacyjnej, z wnioskiem o to, nie wcześniej jednak niż po zakończeniu postępowania przygotowawczego, może wystąpić do sądu m.in. osoba podsłuchiwana. Ustawodawca w art. 239 k.p.k. wskazał też, że ogłoszenie postanowienia o kontroli oraz utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy, a w postępowaniu przygotowawczym – nie później niż do zakończenia tego postępowania.

Wyjątkowo negatywnie należy ocenić brak stosownych rozwiązań w odniesieniu do tych tajemnic zawodowych, które z uwagi na ich znaczenie dla urzeczywistnienia takich wartości, jak prawo do obrony oraz wolność prasy – powinny podlegać szczególnej ochronie przed ujawnianiem ich treści służbom stosującym kontrolę operacyjną. Jakkolwiek możliwość niejawnego uzyskiwania informacji objętych tajemnicą obrończą, samo w sobie, nie narusza jeszcze istoty prawa do obrony (oskarżony może bowiem korzystać z pomocy prawnej obrońcy, komunikując się z nim osobiście bez wykorzystywania takich kanałów komunikacji, które mogą być objęte kontrolą operacyjną), to jednak, zdaniem Trybunału Konstytucyjnego, ustawodawca nie przeciwdziałał należycie głębokim naruszeniom tego prawa przez służby policyjne i ochrony państwa. Podobne argumenty przemawiają za negatywną oceną zaskarżonych unormowań w odniesieniu do wzorca kontroli w niniejszej sprawie, którym jest art. 54 ust. 1 Konstytucji, gwarantujący ochronę tajemnicy dziennikarskiej. Ustawa nie wyklucza bowiem uzyskania przez funkcjonariuszy Policji materiałów o istotnym znaczeniu dla niezależnego dziennikarstwa, jakimi są np. dane informatorów, i zapoznania się z takimi materiałami. Trybunał przypomina, że minimalnym standardem w odniesieniu do ochrony poufności kontaktów oskarżonego z obrońcą i poufności tożsamości dziennikarskich źródeł informacji jest istnienie kontroli sądowej weryfikującej zebrane przez Policję w toku czynności operacyjno-rozpoznawczych materiały, co do których istnieje uzasadnione prawdopodobieństwo, że zawierają treści stanowiące prawnie chronioną tajemnicę zawodową, oraz zarządzającej wyłączenie z dalszego wykorzystania tych materiałów, które są istotne z punktu widzenia ochrony relacji zaufania.

Mając to na uwadze, Trybunał Konstytucyjny stwierdza, że art. 19 ustawy o Policji w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.8.2. Na marginesie Trybunał zwraca uwagę na trafne spostrzeżenie wnioskodawcy, który wskazuje na daleko idącą rozbieżność unormowań w zakresie uzyskiwania informacji w toku czynności operacyjno-rozpoznawczych, *de lege lata* zezwalających utrwalać takie komunikaty, które nie mogą następnie być wykorzystane w postępowaniu karnym jako dowód w sprawie. Obowiązujące unormowania o charakterze gwarancyjnym, jakie przewidują przepisy k.p.k. w stosunku do tajemnicy zawodowej, stają się tym samym iluzoryczne, skoro pomimo ogólnego zakazu wprowadzania treści stanowiących tajemnicę zawodową do procesu karnego jako dowodów w sprawie,

ustawodawca zezwala – chociażby pośrednio, przez niejednoznaczną regulację ustawową – na ich gromadzenie i przechowywanie przez służby uprawnione do stosowania kontroli operacyjnej. Szczególnie jest to widoczne na gruncie ochrony tajemnicy obrończej i dziennikarskiej (we wspomnianym zakresie), które na gruncie k.p.k. są objęte bezwarunkową ochroną prawną w postaci niepodlegającego uchyleniu zakazu dowodowego.

11.9. Ocena zgodności art. 9e ustawy o SG z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.9.1. Wnioskodawca sformułował wobec art. 9e ustawy o SG takie same zarzuty i argumenty, jak w odniesieniu do art. 19 ustawy o Policji. W ocenie Trybunału ani odmienny kontekst normatywny stosowania kontroli operacyjnej w świetle ustawy o SG, ani żadne inne powody, nie uzasadniają odmiennej oceny zgodności tego przepisu ze wskazanymi wzorcami kontroli.

Mając to na uwadze, art. 9e ustawy o SG w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.10. Ocena zgodności art. 31 ustawy o ŻW z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.10.1. Wnioskodawca sformułował wobec art. 31 ustawy o ŻW takie same zarzuty i argumenty, jak w odniesieniu do art. 19 ustawy o Policji. W ocenie Trybunału ani odmienny kontekst normatywny stosowania kontroli operacyjnej w świetle ustawy o ŻW, ani żadne inne powody, nie uzasadniają odmiennej oceny zgodności tego przepisu ze wskazanymi wzorcami kontroli.

Mając to na uwadze art. 31 ustawy o ŻW w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.11. Ocena zgodności art. 36c ustawy o kontroli skarbowej z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.11.1. Wnioskodawca sformułował wobec art. 36c ustawy o kontroli skarbowej takie same zarzuty i przedstawił jednakową argumentację, jak w odniesieniu do art. 19 ustawy o Policji.

W ocenie Trybunału Konstytucyjnego, ani zakres działania wywiadu skarbowego ani żadne inne okoliczności, nie uzasadniają odmiennej oceny zakwestionowanego przepisu ze wskazanymi wzorcami kontroli.

W tym stanie rzeczy Trybunał Konstytucyjny stwierdza, że art. 36c ustawy o kontroli skarbowej w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił skutecznie tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.12. Ocena zgodności art. 27 ustawy o ABW z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.12.1. Wnioskodawca sformułował wobec art. 27 ustawy o ABW takie same zarzuty i argumenty, jak w odniesieniu do art. 19 ustawy o Policji. W ocenie Trybunału Konstytucyjnego ani specyfika działania ABW, ani ustawowy zakres kontroli operacyjnej, nie uzasadnia odmiennej oceny jego zgodności ze wskazanymi wzorcami kontroli.

Mając to na uwadze Trybunał stwierdza, że art. 27 ustawy o ABW w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.13. Ocena zgodności art. 17 ustawy o CBA z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.13.1. Wnioskodawca sformułował wobec art. 17 ustawy o CBA takie same zarzuty i argumenty, jak w odniesieniu do art. 19 ustawy o Policji. W ocenie Trybunału Konstytucyjnego, ani odmienny kontekst normatywny stosowania kontroli operacyjnej w świetle ustawy o CBA, ani żadne inne powody, nie uzasadniają odmiennej oceny zgodności tego przepisu ze wskazanymi wzorcami kontroli.

Mając to na uwadze Trybunał stwierdza, że art. 17 ustawy o CBA w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.14. Ocena zgodności art. 31 ustawy o SKW z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

11.14.1. Wnioskodawca sformułował wobec art. 31 ustawy o SKW takie same zarzuty i argumenty, jak w odniesieniu do art. 19 ustawy o Policji. W ocenie Trybunału, ani odmienny kontekst normatywny stosowania kontroli operacyjnej w świetle ustawy o SKW, ani żadne inne powody nie uzasadniają odmiennej oceny zgodności tego przepisu ze wskazanymi wzorcami kontroli.

Mając to na uwadze, Trybunał stwierdza, że art. 31 ustawy o SKW w zakresie, w jakim nie przewiduje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji.

12. Niszczenie danych telekomunikacyjnych.

12.1. Piątym problemem konstytucyjnym jest brak unormowania w ustawie przesłanek niszczenia danych telekomunikacyjnych, które są nieprzydatne (zbędne) w postępowaniu, w ramach którego je uzyskano. We wniosku z 1 sierpnia 2011 r. Rzecznik Praw Obywatelskich wniósł o stwierdzenie niezgodności art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW w zakresie, w jakim zezwalając na pozyskiwanie danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, nie przewidują zniszczenia tych spośród uzyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania, z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Z kolei we wniosku z 27 kwietnia 2012 r. wniósł on o stwierdzenie niezgodności art. 75d ust. 5 ustawy o SC z art. 51 ust. 4 Konstytucji.

Zdaniem wnioskodawcy, art. 28 ustawy o ABW, art. 18 ustawy o CBA i art. 32 ustawy o SKW nie przewidują usunięcia zgromadzonych danych telekomunikacyjnych, nawet gdy są one nieprzydatne z punktu widzenia realizacji celu, dla którego zostały uzyskane. Zdaniem RPO, gromadzenie i bezterminowe przechowywanie danych telekomunikacyjnych, które nie są niezbędne dla realizacji celów, dla których je zebrano, narusza art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Wnioskodawca sformułował tutaj dwa szczegółowe zarzuty. Po pierwsze, zaskarżone przepisy nie przewidują w ogóle procedury oceny udostępnionych służbom danych telekomunikacyjnych pod kątem ich przydatności dla realizacji celów, dla których zostały uzyskane. Po drugie, ustawodawca nie przewidział procedury niszczenia danych zbędnych. Pod pojęciem „danych zbędnych" wnioskodawca zdaje się rozumieć dane nieprzydatne dla ustawowego celu ich gromadzenia, określonego odpowiednio w art. 28 ust. 1 ustawy o ABW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW. Odnosząc się do zarzutu niekonstytucyjności art. 36b ust. 1 ustawy o kontroli skarbowej, Rzecznik wyjaśnił, że uregulowana w tym przepisie procedura niszczenia danych telekomunikacyjnych wyłącznie w części odpowiada wymaganiom konstytucyjnym. Ustawodawca przewidział obowiązek niszczenia zebranych danych jedynie wówczas, kiedy minister właściwy do spraw finansów – będący służbowym zwierzchnikiem funkcjonariuszy wywiadu skarbowego – uzna wniosek o udostępnienie danych telekomunikacyjnych za niezasadny. Natomiast w sytuacji zebrania danych na podstawie uzasadnionego wniosku, które to dane okazały się nieprzydatne w prowadzonym postępowaniu, ustawodawca nie przewidział obowiązku ich niezwłocznego unicestwienia.

Nieco inaczej wnioskodawca widzi problem konstytucyjny w odniesieniu do art. 75d ust. 5 ustawy o SC, a tym samym formułuje inaczej zarzut jego niekonstytucyjności. Przepis ten ma być niezgodny z art. 51 ust. 4 Konstytucji, gdyż umożliwia zachowanie przez Służbę Celną danych telekomunikacyjnych zebranych w sposób sprzeczny z ustawą. Takimi są dane umożliwiające wykrywanie i ściganie przestępstw innych niż wymienione w katalogu ujętym w art. 75d ust. 1 ustawy o SC, tj. inne czyny niż przestępstwa skarbowe uregulowane w rozdziale 9 k.k.s. Zaskarżony przepis przewiduje bowiem obowiązek niszczenia danych zebranych na podstawie art. 75d ust. 1 ustawy o SC jedynie wobec danych, które „nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe". Tym samym ustawowy cel gromadzenia danych telekomunikacyjnych jest węższy niż cel ich przechowywania i ewentualnie dalszego wykorzystania.

12.2. Ocena zgodności art. 28 ustawy o ABW, art. 18 ustawy o CBA i art. 32 ustawy o SKW z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

12.2.1. Zakwestionowane przepisy regulują udostępnianie funkcjonariuszom ABW, CBA oraz SKW danych telekomunikacyjnych. Wnioskodawca sformułował zarzut w sposób zakresowy, jakkolwiek w rzeczywistości chodzi mu o brak unormowania, które jest konieczne z punktu widzenia Konstytucji. Innymi słowy, problem konstytucyjny dotyczy pominięcia w zaskarżonych przepisach procedury weryfikacji i niszczenia danych niemających znaczenia (tj. zbędnych) dla dalszego postępowania. W jego ocenie, narusza to art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

12.2.2. 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. Jak wskazywano w orzecznictwie TK, przepis ten ma dwojakie znaczenie. Po pierwsze, legalizuje działania władz publicznych polegające na pozyskiwaniu, gromadzeniu i udostępnianiu informacji o jednostkach w sposób inny niż w

drodze zgłoszenia takich danych przez samego obywatela. A zatem również gromadzonych w sposób niejawny przez te władze bez wiedzy i woli jednostki. Po drugie, do pewnego stopnia autonomicznie określa przesłanki legalności (granice) takich działań, ograniczając swobodę ustawodawcy determinowania zakresu zadań i kompetencji organów państwa polegających na uzyskiwaniu danych o obywatelach (por. wyrok TK z 17 czerwca 2008 r., sygn. K 8/04, cz. III, pkt 2 i powołane tam orzecznictwo).

Ustrojodawca nie definiuje w art. 51 ust. 2 Konstytucji, czym są „informacje niezbędne w demokratycznym państwie prawnym". Trybunał przyjmuje, że ocena niezbędności powinna być przeprowadzona z uwzględnieniem zasady proporcjonalności wynikającej z art. 31 ust. 3 Konstytucji. W rezultacie naruszenie autonomii informacyjnej polegające na pozyskiwaniu, gromadzeniu lub udostępnianiu przez władze publiczne informacji o obywatelach odpowiadać powinno zawsze wymaganiom zdefiniowanym w art. 31 ust. 3 Konstytucji (zob. wyrok TK z 20 listopada 2002 r., sygn. K 41/02, cz. V, pkt 27). Jak wskazał Trybunał w innym wyroku, „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" (wyrok TK z 17 czerwca 2008 r., sygn. K 8/04, cz. III, pkt 2). Ustanowiony w art. 51 ust. 2 Konstytucji dodatkowy zakaz pozyskiwania informacji innych niż niezbędne 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" (wyrok TK z 20 listopada 2002 r., sygn. K 41/02, cz. V, pkt 27).

W orzecznictwie dotyczącym czynności operacyjno-rozpoznawczych Trybunał starał się precyzować pojęcie „danych niezbędnych w demokratycznym państwie". W wyroku o sygn. K 32/04 Trybunał zaznaczył: „w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo

państwa i porządek publiczny" (wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 4.7). Trybunał Konstytucyjny w niniejszej sprawie podziela to stanowisko.

Ustrojodawca w art. 51 ust. 2 Konstytucji wyraźnie odniósł wyrażony w nim zakaz do pozyskiwania informacji o „obywatelach". Mogłoby to sugerować możliwość pozyskiwania, gromadzenia i przechowywania przez władze publiczne informacji o innych podmiotach (np. niemających obywatelstwa polskiego) w znacznie szerszym zakresie niż wobec obywateli, a więc także informacji niekoniecznych w demokratycznym państwie. Konsekwencją przyjęcia tego stanowiska byłoby zróżnicowanie ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski. Trybunał Konstytucyjny nie wyklucza takiego zróżnicowania, jakkolwiek nie może być ono traktowane jako zasada, a w każdym wypadku – nie może prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich. Mając na uwadze przede wszystkim art. 30 i art. 37 ust. 1 Konstytucji trzeba przyjmować – jako założenie wyjściowe – jednakowy standard ingerencji w konstytucyjne wolności oraz prawa, bez względu na to, czy ich podmiot ma obywatelstwo polskie. Każdy znajdujący się pod władzą Rzeczypospolitej, tj. podlegający polskiemu prawu (zob. wyrok TK z 15 listopada 2000 r., sygn. P 12/99, OTK ZU nr 7/2000, poz. 260) – niezależnie od statusu obywatelskiego – może zatem zasadnie oczekiwać ochrony przed nieuzasadnioną ingerencją w przysługujące mu wolności i prawa. Na tle rozpoznawanej sprawy należałoby w efekcie zakładać konieczność ustanowienia takich samych standardów dotyczących pozyskiwania, gromadzenia czy przechowywania danych zgromadzonych przez władze publiczne w toku czynności operacyjno-rozpoznawczych w stosunku do wszystkich podmiotów, które znajdują się pod władzą Rzeczypospolitej Polskiej.

Od tak ujętej zasady jednakowej ochrony dopuszczalne będzie wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, którzy podlegają polskiemu prawu. Przesądza o tym art. 37 ust. 2 Konstytucji. Trybunał ma świadomość doktrynalnych kontrowersji, jakie budzą wzajemne relacje art. 37 ust. 2 i art. 31 ust. 3 Konstytucji (zob. m.in. L. Garlicki, uwaga 8 do art. 37, [w:] *Konstytucja…,* t. III, s. 6 i n.). Przychyla się jednak do poglądu, w myśl którego art. 37 ust. 2 Konstytucji nie może być traktowany jako *lex specialis* wyłączający zastosowanie art. 31 ust. 3 Konstytucji, ponieważ w takim wypadku cudzoziemcy nie mieliby faktycznie żadnych gwarantowanych konstytucyjnie praw (tamże, s. 8-9). Każde ograniczenie wolności lub praw niezarezerwowanych jedynie dla obywateli winno być w związku z tym proporcjonalne w rozumieniu art. 31 ust. 3 Konstytucji, a ponadto nie może naruszać ich istoty. Konsekwencją obowiązywania art. 37 ust. 2 Konstytucji jest natomiast możliwość dokonania bardziej elastycznej interpretacji poszczególnych przesłanek składających się na zasadę proporcjonalności, uzasadniającej większy poziom ingerencji w wolności i prawa cudzoziemców niż obywateli. Za takim właśnie stanowiskiem przemawiać może również brzmienie uczynionego w niniejszej sprawie wzorcem kontroli art. 51 ust. 2 Konstytucji, który wyraźnie kładzie nacisk na istnienie przesłanki niezbędności uzyskiwania, gromadzenia i przechowywania danych o obywatelach.

Powyższe założenie nie wyklucza dopuszczalności odmiennego określenia przesłanek pozyskiwania danych i postępowania z nimi w stosunku do osób niepodlegających polskiemu prawu (np. danych pozyskiwanych przez służby wywiadu o działalności obcych podmiotów zagranicą), chociaż w każdym wypadku takie działania władz publicznych muszą mieścić się w ramach standardów państwa prawnego.

12.2.3. Trybunał Konstytucyjny podziela zarzuty wnioskodawcy wobec art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW. Jak wcześniej wskazano (zob. cz. III, pkt 5.1.3 uzasadnienia), warunkiem niejawnego uzyskiwania

informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów. Jak wcześniej podkreślono, ingerencją w sferę prywatności jednostek będzie nie tylko jednorazowe pozyskanie danych o jednostce (m.in. w trybie określonym w art. 28 ust. 1 ustawy o ABW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW), ale również każde kolejne operacje na tych danych, w tym przechowywanie czy wtórne wykorzystywanie w toku innych postępowań (zob. cz. III, pkt 1.9 uzasadnienia).

Zakwestionowane przepisy nie regulują postępowania z danymi telekomunikacyjnymi, po ich zgromadzeniu na podstawie art. 28 ust.1 ustawy o ABW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW. Kwestia postępowania ze zgromadzonymi w tym trybie danymi została przez ustawodawcę pominięta. Nie ma zarazem prawnych podstaw do odpowiedniego stosowania przepisów regulujących niszczenie danych zgromadzonych w kontroli operacyjnej czy przepisów k.p.k. regulujących kontrolę i utrwalanie treści rozmów (art. 237 i n. k.p.k.). Oznacza to, że na gruncie art. 28 ustawy o ABW, art. 18 ustawy o CBA i art. 32 ustawy o SKW nie ma żadnych regulacji dotyczących weryfikacji oraz niszczenia danych zbędnych. Nie jest wobec tego wykluczone przechowywanie danych nieprzydatnych w prowadzonym postępowaniu, w toku którego wystąpiono o te dane, ani nawet do innych usprawiedliwionych konstytucyjnie celów. Jak ponadto zasadnie zwrócił uwagę Marszałek Sejmu w piśmie z 2 marca 2012 r., zakwestionowane przepisy prowadzą do sytuacji, w której dane o jednostkach mogą być przechowywane wyłącznie z powodu zaniechania ich rzetelnej weryfikacji.

Trybunał Konstytucyjny nie neguje dopuszczalności dalszego przechowywania (to jest po ich analizie i stwierdzeniu ewentualnej nieprzydatności w prowadzonym postępowaniu w konkretnej sprawie) danych telekomunikacyjnych dotyczących cudzoziemców znajdujących się pod władzą Rzeczypospolitej Polskiej, w szczególności jeśli istnieją poważne i uzasadnione podejrzenia co do ich zaangażowania w działalność zagrażającą bezpieczeństwu państwa, w tym w terroryzm i przestępczość zorganizowaną. Takie zróżnicowanie stopnia ochrony ma swe umocowanie przede wszystkim w art. 51 ust. 2 i art. 37 ust. 2 Konstytucji.

Mając powyższe na uwadze, art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

12.3. Ocena zgodności art. 36b ust. 5 ustawy o kontroli skarbowej z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

12.3.1. Zakwestionowany przepis ma następującą treść:

„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”.

12.3.2. Wnioskodawca trafnie w tym kontekście ustalił zakres normowania art. 36b ust. 5. Z przepisu tego wynika bowiem, że zniszczeniu podlegają tylko te dane, które zostały pozyskane od operatora telekomunikacyjnego i pocztowego na podstawie nieuzasadnionego wniosku. Rację ma Rzecznik Praw Obywatelskich, twierdząc, że przepis ten wyjątkowo wąsko określa przesłanki zniszczenia danych. Nie przewiduje bowiem

zniszczenia danych, które zebrano na podstawie uzasadnionego wniosku, lecz nie mają one znaczenia dla prowadzonego postępowania.

Ocena konstytucyjności art. 36b ust. 5 ustawy o kontroli skarbowej w kontekście tak sformułowanego zarzutu nie może odrywać się od całokształtu unormowań uzyskiwania i gromadzenia danych telekomunikacyjnych przez wywiad skarbowy, a zwłaszcza od art. 36d ust. 3 tej ustawy. Zgodnie z art. 36d ust. 3, „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". Mając na uwadze treść tego przepisu, Marszałek Sejmu przyjął, że w systemie prawa są gwarancje niszczenia danych zbędnych, których pominięcie zarzuca wnioskodawca (s. 59-60 pisma z 2 marca 2012 r.). Będący przedmiotem kontroli art. 36b ust. 5 ustawy o kontroli skarbowej stanowi dodatkową przesłankę niszczenia danych telekomunikacyjnych uzyskanych w toku działań wywiadu skarbowego. W konsekwencji Marszałek Sejmu zajął stanowisko, że art. 36b ust. 5 ustawy o kontroli skarbowej jest zgodny ze wskazanymi wzorcami kontroli.

Jak wynika z uzasadnienia wniosku oraz wyjaśnień złożonych na rozprawie, Rzecznik Praw Obywatelskich zakwestionował pominięcie prawodawcze. Wskazuje on, że istnieje przepis gwarantujący niszczenie danych, ale czyni to w niewystarczającym z konstytucyjnego punktu widzenia zakresie. Zdaniem Trybunału, problem w niniejszej sprawie nie polega jednak – jak twierdzi wnioskodawca – na pominięciu prawodawczym w art. 36b ust. 5 ustawy o kontroli skarbowej spowodowanym zbyt wąskim unormowaniem w nim przesłanek zniszczenia danych telekomunikacyjnych zgromadzonych przez wywiad skarbowy. Problem konstytucyjny w tej sprawie polega bowiem na zbyt szerokim zakresie normowania art. 36d ust. 3 ustawy, który umożliwia przechowywanie i wykorzystywanie uzyskanych wcześniej danych telekomunikacyjnych w celach niemających konstytucyjnego uzasadnienia. Innymi słowy, problemem nie jest więc to, czego ustawodawca nie unormował, chociaż postępując w zgodzie z Konstytucją powinien był unormować, lecz to, co uregulował w innym przepisie ustawy, który nie został zaskarżony przez wnioskodawcę.

Trybunał Konstytucyjny stwierdza, że wnioskodawca swoje zarzuty sformułował wobec niewłaściwego przepisu. Orzekając w sprawie wniosku, Trybunał związany jest co prawda – zgodnie z art. 66 ustawy o TK – jego granicami, wyznaczonymi przez przedmiot i wzorzec kontroli. Uwzględniając *petitum* i uzasadnienie wniosku RPO z 1 sierpnia 2011 r., nie sposób – nawet odwołując się do zasady *falsa demonstratio non nocet* (zob. wyrok TK z 15 lipca 2013 r., sygn. K 7/12, OTK ZU nr 6/A/2013, poz. 76, cz. III, pkt 1.3) – przyjąć, że intencją wnioskodawcy było zakwestionowanie innego przepisu, tj. art. 36d ust. 3 ustawy o kontroli skarbowej, czy inaczej – przypisanie postawionych zarzutów oraz ich uzasadnienia do art. 36d ust. 3, a nie – jak uczynił to wnioskodawca – do art. 36b ust. 5 tej ustawy. Cały ciężar argumentacji wnioskodawcy (zresztą lakonicznej) koncentruje się na braku istnienia jakiegokolwiek mechanizmu niszczenia danych zbędnych z punktu widzenia prowadzonego postępowania. Wnioskodawca nie odniósł się do przedmiotowego zakresu przechowywania i dalszego wykorzystywania danych telekomunikacyjnych. Mechanizm, którego brak zarzuca RPO, funkcjonuje w systemie prawa, lecz może budzić konstytucyjne zastrzeżenia. Ta jednak kwestia nie może podlegać ocenie w tym postępowaniu. Biorąc pod uwagę zakres wniosku RPO odczytanego z uwzględnieniem zasady *falsa demonstratio*, a także wyjaśnień złożonych na rozprawie, Trybunał nie ma możliwości rozstrzygnięcia tak ujętego problemu konstytucyjnego. W związku z tym stwierdza, że art. 36b ust. 5 ustawy o kontroli skarbowej jest zgodny z art. 51 ust. 2 w

związku z art. 31 ust. 3 Konstytucji. Przepis ten wyraża bowiem dodatkową gwarancję, której istnienie trudno byłoby uznać za niekonstytucyjne. Przeciwnie, powinno to być traktowane jako rozwiązanie sprzyjające legalizmowi działania wywiadu skarbowego, a w konsekwencji wzmacniające poziom ochrony wolności i praw jednostki.

12.4. Ocena zgodności art. 75d ust. 5 ustawy o SC z art. 51 ust. 4 Konstytucji.

12.4.1. Zakwestionowany przepis na następującą treść:

„Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu".

12.4.2. Zakwestionowany art. 75d ust. 5 ustawy o SC zobowiązuje wprawdzie Służbę Celną do niszczenia danych telekomunikacyjnych, które są nieprzydatne w prowadzonym przez Służbę Celną postępowaniu, jednakże – co kwestionuje Rzecznik – zbyt szeroko określa przesłanki zachowania zgromadzonych materiałów. Zniszczeniu podlegać mają jedynie takie materiały, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe. Jak trafnie uznaje Rzecznik, o ile „Służba Celna może pozyskiwać dane telekomunikacyjne w wąsko zakreślonym celu w postaci zapobiegania lub wykrywania przestępstw skarbowych przeciwko organizacji gier hazardowych, to już nie musi niszczyć materiałów, które co prawda nie mają znaczenia z punktu widzenia tego celu, lecz mają znaczenie dla innych postępowań w sprawach o wszelkie wykroczenia skarbowe lub przestępstwa skarbowe. Innymi słowy inny jest cel pozyskiwania danych telekomunikacyjnych przez Służbę Celną i inny jest cel ich przechowywania" (s. 13 wniosku RPO z 27 kwietnia 2012 r.). Wnioskodawca nie domaga się jednak, aby każda jednostka mogła występować z żądaniem usuwania danych uzyskanych nielegalnie, ale aby istniał ustawowy mechanizm – działający niejako w sposób automatyczny – który urzeczywistniałby prawo podmiotowe przewidziane w art. 51 ust. 4 Konstytucji.

12.4.3. Zgodnie z art. 51 ust. 4 Konstytucji „Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą".

Ustrojodawca wyodrębnił w tym przepisie dwojakiego rodzaju uprawnienia, jakie przysługują jednostce odnośnie do dotyczących jej informacji. Po pierwsze, prawo do żądania sprostowania tych informacji. Po drugie, prawo do żądania usunięcia informacji. Wykładnia językowo-logiczna wskazywałaby, że informacje podlegające sprostowaniu albo usunięciu muszą mieć charakter informacji „nieprawdziwych", „niepełnych" bądź „zebranych w sposób sprzeczny z ustawą". Odwołując się do językowego znaczenia tych wyrażeń, można przyjąć, że nieprawdziwymi będą informacje niezgodne z rzeczywistym stanem rzeczy, a niepełnymi – niekompletne lub zawierające jakieś braki, które zniekształcają rzeczywisty obraz rzeczy. Z kolei w wypadku ostatniej kategorii informacji wymienionej w art. 51 ust. 4 chodzi o sposób zgromadzenia informacji przez podmiot, w posiadaniu którego się znajdują, a nie o ich treść (por. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 5.1). Informacje „zebrane w sposób sprzeczny z ustawą" nie muszą być więc jednocześnie nieprawdziwymi lub niepełnymi. Może się wręcz zdarzyć tak, że będą to informacje oddające całościowo obraz rzeczywistego stanu rzeczy (wiedzy o jednostce), jednak – mimo swej prawdziwości oraz kompletności – zostały pozyskane nielegalnie, przez co muszą być unicestwione w świetle art. 51 ust. 4 Konstytucji. Jakkolwiek ustrojodawca w sposób precyzyjny nie rozstrzygnął, jakiego rodzaju uprawnienia wynikające z art. 51 ust. 4 mają przysługiwać jednostce w odniesieniu do każdego z trzech rodzajów informacji, to należałoby przyjąć, że o sprostowaniu może być

mowa w odniesieniu do informacji nieprawdziwych lub niepełnych, natomiast o usunięciu – przede wszystkim (choć nie wyłącznie) – informacji zebranych nielegalnie.

Trybunał uznaje, że w świetle art. 51 ust. 4 Konstytucji o „informacjach zebranych w sposób sprzeczny z ustawą" można mówić w trojakiego rodzaju sytuacjach. Po pierwsze, gdy uzyskiwanie danego rodzaju informacji jest w ogóle niedopuszczalne w świetle Konstytucji. Po drugie, gdy nie dokonuje się na podstawie i w granicach przewidzianych wyraźnie w ustawie. Po trzecie, gdy uzyskanie informacji – nawet konstytucyjnie lub ustawowo dopuszczalne – nastąpiło niezgodnie z procedurą określoną w prawie.

12.4.4. Problem konstytucyjny postawiony przez Rzecznika Praw Obywatelskich sprowadza się do rozstrzygnięcia jedynie wąskiego problemu, a mianowicie czy dane uzyskane wprawdzie przez organ państwa zgodnie z ustawą, można następnie gromadzić i ewentualnie wykorzystać w innym celu niż pierwotny cel ich uzyskania.

Wnioskodawca nie zaskarżył natomiast przepisu regulującego cel gromadzenia danych w kontekście zasady proporcjonalności, a zwłaszcza nie postawił zarzutu, że wykorzystanie danych telekomunikacyjnych, zebranych w związku z zapobieganiem lub wykrywaniem przestępstw skarbowych określonych w rozdziale 9 k.k.s. do zapobiegania innym przestępstwom skarbowym lub wykroczeniom skarbowym oraz ich wykrywania, nadmiernie ingeruje – z uwzględnieniem masowego charakteru gromadzonych niejawnie danych – w prawo do ochrony prywatności, tajemnicę komunikowania się oraz autonomię informacyjną jednostki.

12.4.5. Trybunał Konstytucyjny podziela zastrzeżenia RPO w odniesieniu do art. 75d ust. 5 ustawy o SC, chociaż postrzega problem konstytucyjny nieco inaczej w perspektywie wskazanego przez wnioskodawcę wzorca kontroli. Wnioskodawca stwierdził, że art. 75d ust. 5 umożliwia zachowanie danych telekomunikacyjnych nie tylko wtedy, gdy mają one znaczenie dla postępowania w sprawach o przestępstwa skarbowe, o których mowa w rozdziale 9 k.k.s., ale również gdy mają znaczenie dla postępowań w sprawie każdego przestępstwa skarbowego lub wykroczenia skarbowego bez wyjątku, nawet wykraczającego poza określone w rozdziale 9 k.k.s. Trybunał zwraca jednak uwagę, że poprawnie dokonywana – w perspektywie konstytucyjnej – wykładnia systemowa art. 75d ust. 5 ustawy o SC nie daje podstaw do nadania mu aż tak szerokiej treści, jak czyni to wnioskodawca. Przepis regulujący przesłanki gromadzenia danych (ust. 5) zawarty jest bowiem w tej samej jednostce redakcyjnej ustawy co przepis regulujący cel ich zbierania (ust. 1). Obydwa te przepisy powinny były być zatem interpretowane łącznie. Wówczas rozumienie zakwestionowanego przepisu ograniczone będzie wyłącznie do przestępstw skarbowych i wykroczeń skarbowych określonych w rozdziale 9 k.k.s, do którego to odsyła art. 75d ust. 1 ustawy o SC. Trybunał przyjmuje jednak, że konstytucyjny organ państwa, jakim jest Rzecznik Praw Obywatelskich, dokonał analizy stosowania zaskarżonego przepisu. Trybunał przyjmuje zatem, że przepis ten jest rozumiany przez właściwe organy państwa tak, jak to wskazał Rzecznik.

Trybunał Konstytucyjny przyjmuje ponadto, że art. 75d ust. 5 ustawy o SC regulujący przesłanki niszczenia materiałów zbędnych dla prowadzonego postępowania nie ma jedynie charakteru proceduralnego, lecz – do pewnego stopnia – również materialny. Określa bowiem ustawowe warunki zgodnego z ustawą gromadzenia informacji o jednostkach, jakimi są dane telekomunikacyjne. Dopiero uwzględniwszy treść art. 75d ust. 1 i 5 można oceniać, czy określone informacje zostały „zebrane w sposób sprzeczny z ustawą", a więc czy znajduje do nich zastosowanie prawo wyrażone w art. 51 ust. 4 Konstytucji. Inaczej mówiąc, ocena legalności zgromadzenia informacji przez Służbę Celną w świetle wskazanego przez wnioskodawcę wzorca kontroli nie może ograniczać się do pierwotnego celu zebrania danych (art. 75d ust. 1). Musi również

uwzględniać ustawowe przesłanki ich przechowywania, które z kolei reguluje art. 75d ust. 5 ustawy o SC.

Należy mieć na uwadze, że ustawodawca relatywnie wąsko wyznaczył dopuszczalny zakres uzyskiwania przez Służbę Celną danych telekomunikacyjnych. W świetle art. 75d ust. 1 ustawy o SC, jest ustawowo dopuszczalne w celu zapobiegania przestępstwom skarbowym określonym tylko i wyłącznie w rozdziale 9 k.k.s., czyli przestępstwom przeciwko organizacji gier hazardowych, a także ich wykrywania. Żądanie dostępu do tych danych jest możliwie w związku z konkretnym postępowaniem, jeżeli istnieje podejrzenie popełnienia przestępstwa skarbowego określonego w konkretnym rozdziale ustawy karnej. A zatem w każdym wypadku, kiedy w momencie zebrania danych telekomunikacyjnych przez Służbę Celną istnieje konstytucyjnie lub ustawowo legitymowany cel uzasadniający ich uzyskanie, i następuje to w przewidzianej ustawowo procedurze, należałoby uznać, że dane takie zostały uzyskane w sposób zgodny z ustawą. Zdaniem Trybunału, jeśli w toku analizy zebranych danych okaże się, że materiały te nie zawierają dowodu popełnienia przestępstwa skarbowego lub nie są przydatne w dalszym postępowaniu w odniesieniu do przestępstwa skarbowego, co do którego było możliwe ich zebranie, lecz będą przydatne do zapobiegania lub wykrywania innych czynów zabronionych określonych w rozdziale 9 k.k.s., należałoby uznać je – w świetle art. 75d ust. 5 ustawy o SC – za zebrane zgodnie z ustawą i dopuścić ich wykorzystanie przez Służbę Celną. Można też uznać je za konieczne w demokratycznym państwie, ponieważ niewątpliwie legitymowanym konstytucyjnie celem jest wykrywanie wypadków popełniania czynów zabronionych oraz zapobieganie im. Trybunał nie przesądza natomiast, czy wykorzystywanie uzyskanych danych telekomunikacyjnych do wykrywania wszelkich przestępstw i wykroczeń skarbowych, które są penalizowane w rozdziale 9 k.k.s. lub zapobiegania im, można uznać za proporcjonalne w perspektywie masowego charakteru zbierania danych telekomunikacyjnych. Wnioskodawca takiego zarzutu nie postawił, poprzestając na problemie proceduralnym. W szczególności nie wskazał jako wzorca kontroli w niniejszej sprawie art. 31 ust. 3 Konstytucji.

W tym stanie rzeczy Trybunał Konstytucyjny stwierdza, że art. 75d ust. 5 ustawy o SC w zakresie, w jakim zezwala na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 k.k.s., jest niezgodny z art. 51 ust. 4 Konstytucji.

13. Umorzenie postępowania.

13.1. Umorzenie postępowania z uwagi na częściowe cofnięcie wniosku.

13.1.1. Na rozprawie 30 lipca 2014 r. Prokurator Generalny cofnął wniosek z 21 czerwca 2012 r. w części dotyczącej wskazanego jako przepis związkowy art. 46 ust. 1 prawa prasowego. Przepis ten został uznany za niezgodny z art. 2 i art. 42 ust. 1 Konstytucji w wyroku TK z 1 grudnia 2010 r., sygn. K 41/07 (Dz. U. Nr 235, poz. 1551), i utracił moc obowiązującą z dniem 14 czerwca 2012 r.

Mając powyższe na uwadze, Trybunał Konstytucyjny na podstawie art. 39 ust. 1 ustawy o TK postanowił umorzyć postępowanie w zakresie wskazanym przez wnioskodawcę.

13.2. Umorzenie postępowania w sprawie zbadania zgodności art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

13.2.1. Zakwestionowany art. 31 ust. 1ustawy o SKW ma następującą treść:

„Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez SKW w celu realizacji zadań określonych w art. 5, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

W myśl art. 5 ust. 1 pkt 1 lit. g ustawy o SKW:

„Do zadań SKW należy 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 (…) 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".

Prokurator Generalny sformułował zarzuty niekonstytucyjności jedynie w zakresie, w jakim zarządzenie kontroli operacyjnej jest dopuszczalne w wypadku przestępstw innych niż wymienione w art. 5 ust. 1 pkt 1 lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych Rzeczypospolitej Polskiej i jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność. Jako wzorce kontroli wskazał art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

13.2.2. Do wymagań formalnym wniosku lub pytania prawnego, o których mowa w art. 32 ust. 1 pkt 3 i 4 ustawy o TK zalicza się m.in. sformułowanie zarzutu niezgodności z Konstytucją, ratyfikowaną umową międzynarodową lub ustawą kwestionowanego aktu normatywnego (pkt 3) oraz uzasadnienie postawionego zarzutu, z przedstawieniem dowodów na jego poparcie (pkt 4).

Trybunał Konstytucyjny stwierdza, że wnioskodawca nie dopełnił w tym wypadku drugiego ze wskazanych wyżej wymagań, to jest nie uzasadnił zarzutu naruszenia przepisów Konstytucji i Konwencji, jak również nie przedstawił dowodów na ich poparcie. Jakkolwiek dokonując kontroli hierarchicznej zgodności norm TK jest zobowiązany zbadać wszystkie istotne okoliczności w celu wszechstronnego wyjaśnienia sprawy, nie będąc związany wnioskami dowodowymi uczestników postępowania, i może z urzędu dopuścić dowody, jakie uzna za celowe dla wyjaśnienia sprawy (art. 19 ustawy o TK), to nie znaczy to, że ciężar dowodu spoczywa na Trybunale.

Prokurator Generalny sformułował zarzut niekonstytucyjności w sposób ogólnikowy, przywołując *de facto* taką samą argumentację jak w odniesieniu do pozostałych przepisów ustaw regulujących kompetencje służb policyjnych w zakresie stosowania kontroli operacyjnej. Na poparcie tego zarzutu odwołał się również do postanowienia sygnalizacyjnego o sygn. S 4/10, dotyczącego ustawy o ABW, które ma zachowywać aktualność na gruncie art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW. Wyjaśnił ponadto, że pojęcia przestępstw godzących w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych RP i jednostek organizacyjnych MON, a także państw zapewniających wzajemność jest niedostatecznie określone i nie sposób ustalić, jaką mają treść. Nie przedstawił jednak żadnych przesłanek, które miałyby uzasadniać adekwatność tej tezy. Za niewystarczającą, z punktu widzenia wymagań formalnych wniosku, należałoby uznać konstatację, że art. 5 ust. 1 pkt 1 lit. g ustawy o SKW jest przepisem niezrozumiałym i pojęcia w nim wymienione nie funkcjonują w języku prawnym. Wnikliwe uzasadnienie zarzutu nieprecyzyjności zakwestionowanego przepisu jest w niniejszej sprawie konieczne, jeżeli wziąć pod uwagę wyrok TK z 27 czerwca 2008 r., sygn. K 51/07 (cz. III, pkt 6.1.), w którym wypowiedział się m.in. w sprawie zgodności z zasadą określoności prawa art. 70a ust. 1 przepisów wprowadzających

ustawę o SKW. Odnosząc się do zarzutu, jakoby zaskarżony przepis naruszał zasadę określoności regulacji prawnych oraz legalizmu działania władz państwowych z uwagi na brak możliwości precyzyjnego określenia zakresu działania WSI przed 2003 r., Trybunał Konstytucyjny w przywołanym wyroku stwierdził: „terminy «obronność państwa» i «bezpieczeństwo Sił Zbrojnych RP» charakteryzują się odpowiednią precyzją dla potrzeb określania zakresu działania organów władzy publicznej. Każda nazwa w języku naturalnym cechuje się pewnym stopniem niedookreśloności, co wiąże się z istotą samego języka. Osiągnięcie wyższego stopnia precyzji przy redagowaniu tekstów aktów normatywnych nie jest możliwe. Ryzyko arbitralnego działania organów władzy publicznej pojawia się przede wszystkim w sytuacjach, w których prawo nie przewiduje sądowej kontroli stosowania prawa przez organy władzy wykonawczej". Z tego powodu TK nie orzekł o naruszeniu zasady określoności prawa (art. 2) oraz zasady legalizmu (art. 7 Konstytucji). Mając na uwadze powyższe tezy uzasadnienia wyroku w sprawie o sygn. K 51/07, Prokurator Generalny winien wyjaśnić, z jakich powodów zaskarżone unormowanie narusza konstytucyjną zasadę określoności prawa i to mimo obowiązujących w tym względzie gwarancji proceduralnych, obejmujących m.in. zarządzanie kontroli operacyjnej przez sąd i istnienie przesłanki subsydiarności.

Prokurator Generalny nie podjął też próby ustalenia, do jakich przestępstw zaskarżony przez niego przepis może się potencjalnie odnosić. W szczególności nie wyjaśnił, czy katalog przestępstw ujęty w art. 5 ust. 1 pkt 1 lit. g ustawy o SKW nie jest w istocie zbiorem pustym, gdyż zakres normowania art. 5 ust. 1 pkt 1 lit. a-f ustawy o SKW wyczerpuje wszystkie ustawowe rodzaje przestępstw zagrażającym takim dobrom, jak bezpieczeństwo potencjału obronnego państwa, bezpieczeństwo Sił Zbrojnych i jednostek organizacyjnych MON czy państw zapewniających wzajemność.

Stawiając zarzut nieproporcjonalnej ingerencji w prawo do ochrony prywatności oraz tajemnicę komunikowania się, Prokurator Generalny w żaden sposób nie uzasadnił, na czym miałoby polegać owo nieproporcjonalne ograniczenie praw konstytucyjnych. Nie jest wobec tego jasne, czy przyczyną niekonstytucyjności jest zbyt szeroki katalog przestępstw, odnośnie do których można stosować – na podstawie art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g – kontrolę operacyjną (trzeba przy tym zaznaczyć, że wnioskodawca w ogóle nie przedstawił, w odniesieniu do jakich przestępstw kontrola operacja jest nadmierna), czy też nieprzydatność kontroli operacyjnej do rozpoznawania i wykrywania niektórych z nich, ewentualnie zapobiegania niektórym z nich.

Trybunał Konstytucyjny zwraca również uwagę na brak uzasadnienia zarzutu niezgodności art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW z art. 8 Konwencji. W tym zakresie wnioskodawca odwołał się do ogólniejszych tez z orzecznictwa ETPC. Nie odniósł ich natomiast do polskich uwarunkowań ani nie wyjaśnił, z jakich powodów wymagane przez orzecznictwo strasburskie formalne i materialne przesłanki dopuszczalności stosowania środków niejawnego uzyskiwania informacji mają naruszać art. 8 Konwencji.

Umorzenie postępowania w powyższym zakresie nie stoi na przeszkodzie – w razie zaskarżenia w przyszłości tego przepisu – merytorycznej kontroli, pod warunkiem spełnienia ustawowych wymagań określonych w art. 32 ustawy o TK.

Mając to na uwadze, Trybunał Konstytucyjny postanowił umorzyć postępowanie w powyższym zakresie, z uwagi na niedopuszczalność wydania wyroku (art. 39 ust. 1 pkt 1 ustawy o TK).

13.3. Umorzenie postępowania w sprawie zbadania zgodności art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

13.3.1. Przepis art. 5 ust. 1 pkt 9 ustawy o SKW ma następujące brzmienie:

„Do zadań SKW należy podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana".

Uwzględniając treść normatywną art. 31 ust. 1, ustawodawca umożliwił zarządzenie kontroli operacyjnej nie tylko w celu walki z przestępczością, ale także w celu wykonywania innych zadań bliżej nieskonkretyzowanych w ustawie o SKW, lecz powierzonych tej formacji przez inne akty normatywne.

13.3.2. Zdaniem Trybunału Konstytucyjnego, również w odniesieniu do tego przepisu, wnioskodawca nie spełnił wymagań wynikających z art. 32 ust. 1 pkt 4 ustawy o TK, tj. nie uzasadnił zarzutu niezgodności tego przepisu z Konstytucją i Konwencją. Całość argumentacji sprowadza się do tezy, że ustawodawca nie określił konkretnych działań SKW, uprawniających ją do stosowania kontroli operacyjnej. Prowadzić ma to do sytuacji, w której powierzenie Służbie Kontrwywiadu Wojskowego nowych zadań w ustawach lub w umowach międzynarodowych każdorazowo prowadzi do rozszerzenia przedmiotowego zakresu kontroli operacyjnej.

Prokurator Generalny oparł swój zarzut na potencjalnym naruszeniu wolności i praw jednostek, w związku z możliwym przyjmowaniem nowych zobowiązań międzynarodowych. Nie wskazał jednak żadnych zadań powierzonych SKW w innych ustawach bądź w umowach międzynarodowych, co do których mogłaby być stosowana kontrola operacyjna na podstawie art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW. Również Trybunał Konstytucyjny nie znalazł takich zadań, które byłyby przypisane tej służbie w innych aktach normatywnych, niż ustawa o SKW. Tym samym zarzut niekonstytucyjności ma charakter tylko hipotetyczny i opiera się na daleko idącym uproszczeniu.

Niezależnie od powyższych spostrzeżeń, Trybunał Konstytucyjny zwraca uwagę, że ustawodawca uchwalając przepisy powierzające SKW nowe zadania, musi mieć na uwadze, że rozszerzy to zakres przedmiotowy kontroli operacyjnej prowadzonej przez tę służbę. Zakwestionowany przepis w sposób automatyczny będzie otwierał możliwość kontroli operacyjnej w odniesieniu do każdego nowego zadania, przypisanego SKW w innej ustawie lub w umowie międzynarodowej. W konsekwencji ustawodawca – powierzając nowe zadania tej służbie – obowiązany będzie przestrzegać wymagań wynikających m.in. z niniejszego wyroku w odniesieniu do przepisów regulujących niejawne pozyskiwanie informacji o jednostkach, w szczególności zaś testu proporcjonalności i określoności regulacji. Umorzenie postępowania w powyższym zakresie nie stoi na przeszkodzie – w razie zaskarżenia w przyszłości przepisów innych ustaw lub umów międzynarodowych powierzających SKW określone zadania – kontroli zarówno takiego przepisu w związku z art. 31 ust. 1 i w związku z art. 5 ust. 1 pkt 9, jak również art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW, pod warunkiem spełnienia wymagań formalnych określonych w art. 32 ustawy o TK.

Mając to na uwadze, Trybunał Konstytucyjny postanowił umorzyć postępowanie w powyższym zakresie, z uwagi na niedopuszczalność wydania wyroku (art. 39 ust. 1 pkt 1 ustawy o TK).

13.4. Umorzenie postępowania z uwagi na zbędność wydania wyroku.

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, jeśli TK stwierdza niekonstytucyjność kwestionowanej regulacji chociażby z jednym ze wskazanych wzorców kontroli, postępowanie w zakresie badania zgodności tej regulacji z pozostałymi wzorcami kontroli może zostać umorzone na podstawie art. 39 ust. 1 pkt 1 ustawy o TK ze względu na zbędność wyrokowania (zob. wyrok TK z 12 stycznia 2012 r., sygn. Kp 10/09, OTK ZU nr 1/A/2012, poz. 4, cz. III, pkt 3.8 oraz powołane tam orzecznictwo). Mając to na uwadze, Trybunał postanowił umorzyć na tej podstawie badanie zgodności niektórych przepisów, co do których orzekł o niekonstytucyjności przynajmniej z jednym ze wskazanych wzorców kontroli. Takie rozstrzygnięcie, uwarunkowane ekonomią postępowania, nie może być jednak odczytywane jako aprobata zakwestionowanych przepisów ingerujących w konstytucyjne prawo do ochrony prywatności, autonomię informacyjną i ochronę tajemnicy komunikowania się z punktu widzenia wzorców, wobec których postępowanie zostało umorzone na podstawie art. 39 ust. 1 pkt 1 ustawy o TK. Ustawodawca zobowiązany jest –konstruując nowe unormowania w zakresie kontroli operacyjnej oraz udostępniania i przetwarzania danych telekomunikacyjnych – uwzględnić standard konstytucyjny dotyczący czynności operacyjno-rozpoznawczych, przedstawiony w niniejszym wyroku (zob. cz. III, pkt 4 uzasadnienia).

14. Odroczenie utraty mocy obowiązującej.

Trybunał postanowił w części II sentencji o odroczeniu terminu utraty mocy obowiązującej niekonstytucyjnych przepisów wskazanych w punktach 2, 5, 6, i 8 sentencji. Chodzi o przepisy dotyczące: kontroli operacyjnej w ustawie o ABW w odniesieniu do „przestępstw godzących w podstawy ekonomiczne państwa" (punkt 2), pozyskiwania danych telekomunikacyjnych (punkt 5), ochrony tajemnicy zawodowej w toku kontroli operacyjnej (punkt 6) i niszczenia zbędnych danych telekomunikacyjnych w ustawach o ABW, SKW i CBA (punkt 8).

W świetle dotychczasowego orzecznictwa Trybunału w okresie odroczenia przepisy te pozostają w dalszym ciągu częścią systemu prawa oraz mogą być właściwie stosowane przez organy władzy publicznej. W dalszym ich stosowaniu trzeba jednak uwzględniać, że przepisy te utraciły domniemanie konstytucyjności.

Rozstrzygnięcie to umotywowane jest koniecznością ograniczenia wystąpienia ryzyka braku efektywnych mechanizmów walki z zagrożeniami, a w efekcie wzrostu przestępczości bądź choćby osłabienia ich wykrywalności.

Trybunał odroczył termin utraty mocy obowiązującej niekonstytucyjnych przepisów na maksymalny, przewidziany w art. 190 ust. 3 Konstytucji, okres 18 miesięcy. Zważywszy na sygnalizowane wątpliwości co do konstytucyjności pewnych unormowań regulujących kontrolę operacyjną, wskazanych w postanowieniu TK o sygn. S 4/10, a ponadto dostatecznie znany ustawodawcy standard konstytucyjny, przypominany wielokrotnie w dotychczasowym orzecznictwie, termin ten Trybunał uznaje za wystarczający na dokonanie odpowiednich zmian legislacyjnych.

Mając powyższe na uwadze, Trybunał Konstytucyjny orzekł jak w sentencji.

Zdanie odrębne
sędziego TK Wojciecha Hermelińskiego
do wyroku Trybunału Konstytucyjnego

z dnia 30 lipca 2014 r., sygn. akt K 23/11

Na podstawie art. 68 ust. 3 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643, ze zm.; dalej: ustawa o TK) zgłaszam zdanie odrębne do cz. I, pkt 3, 5 i 6 wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. K 23/11 oraz do zawartego w tym wyroku postanowienia o umorzeniu postępowania.

Uważam, że Trybunał Konstytucyjny w kwestionowanym przeze mnie zakresie niedostatecznie wnikliwie ocenił konstytucyjność zaskarżonych regulacji, a ponadto w nieuzasadniony sposób określił zakres zaskarżenia.

Moim zdaniem, należało wydać następujące orzeczenie:

Punkt 3 w cz. I sentencji wyroku w zakresie odnoszącym się do ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, ze zm.; dalej: ustawa o ABW) powinien brzmieć:

a) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a (w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa") ustawy o ABW jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności (Dz. U. z 1993 r. Nr 61, poz. 284, ze zm.; dalej: Konwencja), natomiast
b) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW, rozumiany jako odnoszący się do przestępstw wskazanych w art. 228-230a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.; dalej: k.k.), jest zgodny ze wskazanymi wzorcami kontroli.

Kwestionuję więc orzeczenie zawarte w cz. I, pkt 3 lit. a sentencji wyroku, nie mam natomiast zastrzeżeń co do konkluzji zamieszczonej w cz. I, pkt 3 lit. b pod warunkiem jej uzupełnienia w powyższy sposób.

W zakresie odnoszącym się do ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, ze zm.; dalej: ustawa o SKW) punkt 3 w cz. I sentencji wyroku powinien brzmieć:

a) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW (w zakresie, w jakim obejmuje zwrot „a także innych ustawach i umowach międzynarodowych)
b) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW (w zakresie, w jakim obejmuje zwrot „oraz innych [przestępstw] niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność") oraz
c) art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW

– są niezgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji. Mam więc zastrzeżenia co do rozstrzygnięcia o pierwszej z wymienionych norm, zawartego w cz. I, pkt 3 lit. c wyroku, a ponadto kwestionuję umorzenie postępowania odnośnie do kontroli pozostałych norm.

Punkt 5 w cz. I sentencji wyroku powinien mieć następującą treść:

a) art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze zm.; dalej: ustawa o Policji),
b) art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675, ze zm.; dalej: ustawa o SG),
c) art. 36b ust. 1 pkt 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, ze zm.; dalej: ustawa o kontroli skarbowej),
d) art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, ze zm.; dalej: ustawa o ŻW),
e) art. 28 ust. 1 pkt 1 ustawy o ABW,

f) art. 32 ust. 1 pkt 1 ustawy o SKW,
g) art. 18 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, ze zm.; dalej: ustawa o CBA),
h) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, ze zm.; dalej: ustawa o SC)

przez to, że:

– umożliwiają dostęp do danych telekomunikacyjnych w innym celu niż wykrywanie i ściganie najpoważniejszych, ściśle określonych w ustawie przestępstw,
– bez obowiązku wykorzystania wcześniej innych, mniej inwazyjnych metod gromadzenia informacji lub wykazania wysokiego prawdopodobieństwa, że okażą się one nieskuteczne,
– nie przewidują niezależnej kontroli nad udostępnieniem danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, ze zm.; dalej: prawo telekomunikacyjne)

są niezgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji.

Podzielam więc kierunek orzekania zaprezentowany przez większość Trybunału Konstytucyjnego, lecz uważam, że sentencja wyroku nie rozstrzyga wszystkich wątpliwości wnioskodawców i nie wskazuje ustawodawcy kierunków niezbędnych zmian.

Punkt 6 w cz. I sentencji wyroku powinien brzmieć:

a) art. 19 ustawy o Policji,
b) art. 9e ustawy o SG,
c) art. 36c ustawy o kontroli skarbowej,
d) art. 31 ustawy o ŻW,
e) art. 27 ustawy o ABW,
f) art. 31 ustawy o SKW,
g) art. 17 ustawy o CBA

w zakresie, w jakim nie przewidują:

– zakazu pozyskiwania w czasie kontroli operacyjnej materiałów objętych tajemnicą obrończą i dziennikarską oraz
– mechanizmu niezwłocznego, protokolarnego i komisyjnego niszczenia tego typu materiałów uzyskanych wbrew powyższemu zakazowi,

są niezgodne z art. 42 ust. 2 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 6 ust. 3 lit. b i c oraz art. 10 ust. 1 Konwencji. Również w tym wypadku akceptuję ocenę dokonaną przez większość składu orzekającego, lecz uważam, że powinna ona obejmować całość zarzutów podniesionych przez wnioskodawców.

Do złożenia zdania odrębnego skłoniły mnie następujące powody:

1. Zakres przedmiotowy kontroli operacyjnej prowadzonej przez ABW (przestępstwa godzące w „bezpieczeństwo państwa" i „przestępstwa korupcyjne" – cz. I, pkt 3 lit. a i b sentencji i cz. III, pkt 8.7. i 8.8 uzasadnienia wyroku).

1.1. W myśl art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW służba ta jest uprawniona do prowadzenia kontroli operacyjnej w celu rozpoznawania, zapobiegania i wykrywania bliżej niesprecyzowanych (innych niż wymienione wprost w ustawie) przestępstw godzących w „bezpieczeństwo państwa".

Odmiennie niż większość Trybunału Konstytucyjnego uważam, że przepis ten przez swoją nieprecyzyjność nie tylko nie spełnia podstawowych standardów dobrej legislacji (por. art. 2 Konstytucji), ale także tworzy realne niebezpieczeństwo

bezpodstawnego wkraczania w prawa i wolności obywateli (por. art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 ust. 1 Konwencji; zob. także – jeżeli chodzi o możliwość współstosowania wzorców formalnych i merytorycznych – wyrok z 20 kwietnia 2004 r., sygn. K 45/02, OTK ZU nr 4/A/2004, poz. 30).

Wskazany przepis pozwala ABW na prowadzenie kontroli operacyjnej w związku ze wszystkimi przestępstwami (także pozakodeksowymi), pod warunkiem, że służba ta uzna je za „godzące w bezpieczeństwo państwa". Zasady kwalifikacji badanego czynu nie są w żaden sposób wystandaryzowane (np. za pomocą kryterium sfer, w których mogłoby dojść do naruszenia bezpieczeństwa państwa), a więc mają charakter całkowicie ocenny. Nie jest też jasne, czy „przestępstwa godzące w bezpieczeństwo państwa", o których mowa w art. 5 ust. 1 pkt 2 lit. a ustawy o ABW, mogą równocześnie „godzić w podstawy ekonomiczne państwa" (por. art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz cz. I, pkt 2 sentencji wyroku).

Przestępstwa „godzące w bezpieczeństwo państwa" nie nawiązują ani do potocznych, ani do ustawowych nazw poszczególnych czynów zabronionych, nie pasują także do systematyki przestępstw przyjętej w kodeksie karnym. Podobne sformułowanie – „przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej" – pojawia się jedynie w art. 112 pkt 1 k.k. przy określeniu *ratione personae* kodeksu karnego. Przepis ten wymaga jednak dopełnienia przepisami, w których określone są znamiona poszczególnych czynów zabronionych (sam art. 112 pkt 1 k.k. nie daje wystarczających podstaw do sformułowania aktu oskarżenia). Ponadto kodeks karny wyodrębnia jeszcze przestępstwa przeciwko „bezpieczeństwu powszechnemu" i „bezpieczeństwu w komunikacji" – rozdziały XX i XXI, które obejmują m.in. spowodowanie pożaru, katastrofy budowlanej lub wypadku komunikacyjnego (co raczej rzadko mogłoby godzić „w bezpieczeństwo państwa").

Nie przekonuje mnie również próba wykładni art. 5 ust. 1 pkt 2 lit. a ustawy o ABW, zaprezentowana w cz. III, pkt 8.7.3 uzasadnienia wyroku, która odwołuje się do akceptacji przez Trybunał Konstytucyjny pojęcia „bezpieczeństwo państwa" w wyroku z 27 czerwca 2008 r., sygn. K 51/07 (OTK ZU nr 5/A/2008, poz. 87). Pogląd ten był bowiem wyrażony w kontekście zakresu przedmiotowego raportu Przewodniczącego Komisji Weryfikacyjnej m.in. dla Prezydenta i Prezesa Rady Ministrów na temat funkcjonowania wywiadu i kontrwywiadu wojskowego. Nie dotyczył on więc bezpośrednio relacji państwo-obywatel (a zwłaszcza – prawa do prywatności w kontekście uprawnień służb do kontroli operacyjnej), lecz stosunków między różnymi organami państwa (zakresu obowiązku sprawozdawczego; wzorcami kontroli były w tym zakresie jedynie art. 2 i art. 7 Konstytucji). Wpływ raportu z weryfikacji WSI na prawa podmiotowe wymienionych w nim osób został oceniony przez Trybunał Konstytucyjny w innym miejscu tego wyroku nie pod kątem dostatecznej precyzyjności pojęcia „bezpieczeństwo państwa", lecz dostatecznych gwarancji proceduralnych rzetelności raportu z weryfikacji WSI.

Zdecydowanie nie zgadzam się ze stwierdzeniem Trybunału Konstytucyjnego, że użycie niedookreślonego zwrotu „przestępstwa przeciwko bezpieczeństwu państwa" jest konieczne z powodu „bogactwa faktycznego i aksjologicznego przedmiotu regulacji", a postulat zastąpienia go zamkniętym katalogiem przestępstw „ocierałby się o granice legislacyjnej poprawności" (cz. III, pkt 8.7.7.6 uzasadnienia wyroku). Takie rozwiązanie jest bowiem stosowane w wypadku podsłuchu procesowego z art. 237 § 3 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, ze zm.; dalej: k.p.k.), a więc instytucji bardzo podobnej. Brak jego odpowiednika w przepisach dotyczących kontroli operacyjnej, prowadzonej pod zdecydowanie mniejszym nadzorem sądu niż podsłuch procesowy (co wyraża się np. w przedłużeniu terminu sądowego zatwierdzenia decyzji Szefa ABW o kontroli operacyjnej z 3 do 5 dni – por. art. 27 ust. 3 zdanie drugie ustawy o ABW), wydaje się przeczyć założeniu o racjonalności ustawodawcy.

Jest wszak oczywiste, że im bardziej ograniczone są gwarancje proceduralne (a zwłaszcza – mniejszy nadzór sądowy), tym większa powinna być precyzyjność zasad wkraczania w prawa i wolności obywatelskie.

Dodatkowo należy zwrócić uwagę, że uzasadnienie wyroku Trybunału Konstytucyjnego w tym zakresie jest wewnętrznie sprzeczne. Przy okazji oceny problemu braku zamkniętego katalogu przestępstw uzasadniających stosowanie kontroli operacyjnej przez SKW i SWW Trybunał Konstytucyjny stwierdził bowiem, że „ustanowienie statycznego odesłania do konkretnych jednostek redakcyjnych ustawy karnej typizujących przestępstwa wzmacniałoby niewątpliwie poziom ochrony jednostki przed potencjalnym ryzykiem arbitralności organów władzy publicznej". *Implicite* uznał więc nie tylko, że jest to możliwe, ale także, że stanowiłoby realizację najwyższego możliwego standardu konstytucyjnego (por. np. cz. III, pkt 8.9.2 *in fine* uzasadnienia wyroku; podobnie: cz. III, pkt 8.8.2 uzasadnienia wyroku; należy jednak uczciwie zaznaczyć, że Trybunał Konstytucyjny nie uważa tego za wystarczający powód obalenia domniemania konstytucyjności zaskarżonych przepisów).

Istotnym skutkiem niedookreśloności zaskarżonej regulacji jest to, że weryfikacja zasadności wniosku o zastosowanie kontroli operacyjnej przez Szefa ABW, Prokuratora Generalnego oraz sąd (notabene zresztą czasem już *ex post* – por. art. 27 ust. 1-3 ustawy o ABW) jest pozorna, pomimo że do takiego wniosku w każdym wypadku musi być dołączone uzasadnienie (por. art. 27 ust. 1a ustawy o ABW). Pozwala ona podjąć decyzję na podstawie samego zaufania do ABW, w myśl założenia, że służba ta jest odpowiedzialna za zapewnienie bezpieczeństwa państwa, co do zasady działa w sposób profesjonalny i każdy złożony przez nią wniosek o zastosowanie kontroli operacyjnej jest słuszny. W ten sposób brzmienie zaskarżonego przepisu wymusza przyjęcie reguły, że (wobec braku obiektywnych kryteriów uzasadniających odmowę uwzględnienia wniosków o kontrolę operacyjną) należy wnioski te akceptować, podczas gdy ochrona praw i wolności obywatelskich wymagałaby postępowania dokładnie odwrotnego (odmowy z zasady, a zgody na kontrolę operacyjną w drodze wyjątku). W rezultacie nie ma jakichkolwiek gwarancji przewidywalności działań ABW – na podstawie brzmienia zaskarżonego przepisu nie można bowiem jednoznacznie odpowiedzieć na pytanie, w jakich konkretnie sprawach (w odniesieniu do jakich typów przestępstw czy konkretnych czynów) stosowanie kontroli operacyjnej jest dopuszczalne, a w jakich nie.

Tymczasem jest oczywiste, że kontrola operacyjna stanowi bardzo głęboką ingerencję w prywatność osób, wobec których jest stosowana i może doprowadzić do ujawnienia istotnych faktów z ich życia osobistego czy zawodowego. Pozwala ona na uzyskiwanie w trybie niejawnym i pozaprocesowym zarówno informacji pochodzących z tradycyjnej korespondencji, jak i – co współcześnie ważniejsze – treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych (np. poczty elektronicznej – por. art. 27 ust. 6 ustawy o ABW). Wobec tego przesłanki jej stosowania powinny być określone w sposób maksymalnie precyzyjny – przez odesłanie do konkretnych przepisów karnych określających znamiona przestępstw, które mają być przy jej pomocy wykrywane lub ścigane (por. wspomniany podsłuch procesowy z art. 237 § 3 k.p.k.). Tylko taki sposób regulacji spełniałby – moim zdaniem – konstytucyjny wymóg, aby ewentualne ograniczenia praw i wolności obywatelskich (tu: prawa do prywatności i autonomii informacyjnej) były uregulowane (*lege non distiguente*: w całości) w ustawach.

W mojej opinii, nie wystarczy aktualny sposób określenia uprawnień ABW, który sprowadza się do wymogu, że kontrola operacyjna może być prowadzona tylko w celu rozpoznawania, zapobiegania i wykrywania „przestępstw" (w analizowanym wypadku – „godzących w bezpieczeństwo państwa"). Standard demokratycznego państwa prawa nie pozwala bowiem zaakceptować tak szerokiego zakresu kontroli operacyjnej, który w

praktyce obejmuje przecież nie tylko sprawców przestępstw lub ich świadków, ale także osoby postronne. Choć w hierarchii wartości konstytucyjnych bezpieczeństwo państwa (także gospodarcze) jest ważniejsze niż prywatność pojedynczych obywateli, nie może to prowadzić do powszechnej, niekontrolowanej inwigilacji obywateli z uwagi na hipotetyczne i niedoprecyzowane zagrożenia. Kontrola operacyjna może natomiast i powinna być stosowana, jednak tylko w związku z podejrzeniami najpoważniejszych, ściśle określonych przestępstw i pod warunkiem zachowania należytych gwarancji proceduralnych (por. niżej).

1.2. Byłbym skłonny równocześnie uznać, że minimalny standard w tym zakresie spełnia art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW (por. cz. I, pkt 3 lit. b sentencji wyroku i cz. III, pkt 8.8 jego uzasadnienia), pod warunkiem, że „przestępstwa korupcji", o których mowa w tym przepisie, byłyby rozumiane jako czyny penalizowane przez art. 228, art. 229, art. 230 i art. 230a k.k.

Przepis ten też wprawdzie uzależnia dopuszczalność stosowania przez ABW kontroli operacyjnej od działania w celu ochrony „bezpieczeństwa państwa" (co nawiązuje do zadań ABW z art. 1 ustawy o ABW oraz kwestionowanego przeze mnie art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW), ale jedynie w odniesieniu do wyraźnie określonych rodzajowo „przestępstw korupcji". Rolą tej klauzuli jest więc w tym wypadku – jak słusznie zauważa Trybunał Konstytucyjny (por. cz. III, pkt 8.8.2 uzasadnienia wyroku) – zawężenie, a nie poszerzenie uprawnień ABW i to w taki sposób, aby służba ta mogła prowadzić kontrolę operacyjną jedynie w związku z najpoważniejszymi „przestępstwami korupcji", o najwyższym stopniu szkodliwości społecznej.

W sumie więc art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. c ustawy o ABW cechuje się znacznie większym stopniem precyzyjności niż art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a i b tej ustawy, co pozwala uznać jego zgodność ze wskazanymi wzorcami kontroli. Moim zdaniem, warunkiem *sine qua non* takiego rozstrzygnięcia powinno być jednak uzupełnienie tej regulacji o wyraźne odesłanie do art. 228, art. 229, art. 230 i art. 230a k.k., aby nie było wątpliwości, co oznaczają wymienione w tej regulacji „przestępstwa korupcyjne". Dostrzega to zresztą pośrednio także Trybunał Konstytucyjny, stwierdzając, że posłużenie się „kodeksowymi wyrażeniami niewątpliwie wzmacniałoby poziom ochrony jednostek" (cz. III, pkt 8.8 uzasadnienia wyroku). Nie znalazło to jednak odpowiedniego odzwierciedlenia w sentencji wyroku.

1.3. Na zakończenie należy uzupełniająco wskazać, że kwestionowany przeze mnie pkt 3 lit. a i b wyroku Trybunału Konstytucyjnego pozostaje w sprzeczności z dotychczasowym standardem ochrony prawa do prywatności, prezentowanym w orzecznictwie Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka (dalej: ETPCz).

Wypada tu wspomnieć przede wszystkim o postanowieniu z 15 listopada 2010 r., sygn. S 4/10 (OTK ZU nr 9/A/2010, poz. 111), wydanym w związku z postanowieniem Trybunału Konstytucyjnego z 5 października 2010 r., sygn. P 79/08 (OTK ZU nr 8/A/2010, poz. 88). Trybunał Konstytucyjny zasygnalizował w nim Sejmowi m.in. potrzebę zmiany art. 5 ust. 1 pkt 2 lit. b ustawy o ABW z uwagi na nieprecyzyjność zawartego w tym przepisie określenia „przestępstwa godzące w podstawy ekonomiczne państwa". W uzasadnieniu tego postanowienia stwierdzono m.in.: „Sąd Okręgowy w Warszawie, zarządzając kontrolę operacyjną, winien wskazać konkretną osobę oraz typ przestępstwa określonego w ustawie karnej, którego ma dotyczyć kontrola operacyjna. Jednakże w przypadku zarządzenia przez sąd kontroli operacyjnej, w zakresie przestępstw określonych w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, tzn. w zakresie przestępstw «godzących w podstawy ekonomiczne państwa», nie jest to możliwe, gdyż wyrażenie «przestępstwa godzące w podstawy

ekonomiczne państwa» uniemożliwia identyfikację typów przestępstw, określonych przez ustawę karną". Trybunał Konstytucyjny zauważył w tym kontekście, że ustawodawca zidentyfikował typy przestępstw określonych przez ustawę karną, w związku z którymi może zostać zarządzona kontrola operacyjna przez Policję (por. art. 19 ust. 1 ustawy o Policji), *implicite* sugerując w ten sposób kierunek pożądanej nowelizacji art. 5 ust. 1 pkt 2 lit. b ustawy o ABW (moim zdaniem, powinna ona zresztą być nawet dalej idąca, tj. wskazywać konkretne przestępstwa, a nie tylko ich „typy" czy „rodzaje").

Wspomniana wskazówka nie okazała się jednak skuteczna, a omówione postanowienie sygnalizacyjne nadal czeka na realizację. Uważam, że zaprezentowana w nim argumentacja pozostaje aktualna i powinna być odpowiednio zastosowana także do niedookreślonego pojęcia „przestępstw godzących w bezpieczeństwo państwa" (por. art. 5 ust. 1 pkt 2 lit. a ustawy o ABW). Ustawodawca miał bowiem czas na dokonanie odpowiednich zmian w ustawie o ABW (Senat 9 lipca 2012 r. przedłożył nawet propozycję nowelizacji – por. druk sejmowy nr 633/VII kadencja Sejmu, która jednak została negatywnie zaopiniowana przez Biuro Analiz Sejmowych i „utknęła" w pierwszym czytaniu). Wobec jego bezczynności Trybunałowi Konstytucyjnemu nie pozostawało nic innego, jak orzec o niekonstytucyjności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW. Nie widzę bowiem żadnych podstaw, aby odstąpić od poglądu wyrażonego w omówionym postanowieniu – nie zostały one także ujawnione w uzasadnieniu kwestionowanego wyroku (por. zwłaszcza – cz. III, pkt 5.1.3.1 i pkt 8.6.3 uzasadnienia wyroku, w których wprost przyznano, że ustalenia zawarte w sygnalizacji w sprawie o sygn. S 4/10 „zachowują aktualność w niniejszej sprawie").

Jeżeli natomiast chodzi o orzecznictwo ETPCz, to należy przywołać przede wszystkim standardy w zakresie ochrony prawa do prywatności podczas czynności operacyjno-rozpoznawczych podsumowane w decyzji z 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom (skarga nr 54934/00). Stwierdzono w niej, że minimalne ustawowe ramy stosowania niejawnej kontroli operacyjnej powinny obejmować co najmniej:

- określenie rodzaju przestępstw (ang. *the nature of the offences*), w których może być zastosowany podsłuch;
- zdefiniowanie kategorii osób, wobec których można zastosować podsłuch;
- określenie maksymalnego okresu stosowania podsłuchu;
- ustalenie procedury badania, użycia oraz przechowywania zgromadzonych danych;
- wskazanie środków, które należy zastosować przy przekazywaniu danych zgromadzonych w wyniku podsłuchu innym organom;
- określenie okoliczności, w których zgromadzone dane muszą zostać usunięte (§ 95 tej decyzji; por. także wyroki ETPCz z: 24 kwietnia 1990 r. w sprawie Huvig przeciwko Francji, skarga nr 11105/84, § 34; 30 lipca 1998 r. w sprawie Valenzuela Contreras przeciwko Hiszpanii, skarga nr 27671/95, § 46; 16 lutego 2000 r. w sprawie Amann przeciwko Szwajcarii, skarga nr 27798/95, § 76; 18 lutego 2003 r. w sprawie Prado Bugallo przeciwko Hiszpanii, skarga nr 58496/00, § 30). Wytyczne te były przez ETPCz operacjonalizowane m.in. w wyroku z 10 lutego 2009 r. Iordachi i inni przeciwko Mołdawii (skarga nr 25198/02), w którym uznano niedopuszczalność stosowania podsłuchów i kontroli korespondencji w postępowaniach dotyczących bliżej nieokreślonej grupy poważnych przestępstw (ang. *very serious and exceptionally serious crimes*), potencjalnie obejmującej ponad połowę przestępstw wymienionych w tamtejszym kodeksie karnym (por. także wyrok ETPCz w sprawie Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii z 28 czerwca 2007 r., skarga nr 62540/00, § 76). Brak pełnego uregulowania uprawnień służb specjalnych w ustawie, pozostawiający im zbyt szeroką swobodę działania w zakresie kontroli operacyjnej, został także skrytykowany w wyroku ETPCz z 2 sierpnia 1984 r. w

sprawie Malone przeciwko Wielkiej Brytanii (skarga nr 8691/79).

2. Zakres przedmiotowy kontroli operacyjnej prowadzonej przez SKW i SWW (przestępstwa określone w „innych ustawach i umowach międzynarodowych", przestępstwa „godzące w bezpieczeństwo potencjału obronnego państwa", kontrola operacyjna w celu realizacji „działań, przewidzianych dla SKW w innych ustawach, a także umowach międzynarodowych" – cz. I, pkt 3 lit. c sentencji, postanowienie o umorzeniu postępowania oraz cz. III, pkt 8.9, 13.2 i 13.3 uzasadnienia wyroku).

2.1. Analizę zakwestionowanych przepisów dotyczących kontroli operacyjnej prowadzonej przez Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego (dalej: SKW i SWW) także należy rozpocząć od zastrzeżeń formalnych.

Moim zdaniem, Trybunał Konstytucyjny niesłusznie umorzył postępowanie co do kontroli dwóch regulacji zaskarżonych przez Prokuratora Generalnego z 7 marca 2012 r.: art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g (w zakresie wskazanym we wniosku) oraz art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW (por. cz. III, pkt 13.2 i 13.3 uzasadnienia wyroku).

W odniesieniu do pierwszej z tych regulacji podstawą nierozpoznania wniosku Prokuratora Generalnego było niepowołanie dowodów jej niekonstytucyjności, a w szczególności brak „próby ustalenia, do jakich przestępstw [wyżej wymieniony] zaskarżony przez niego przepis może się potencjalnie odnosić" oraz uzasadnienia, na czym może polegać powodowane przez niego nieproporcjonalne ograniczenie praw konstytucyjnych. Jak wskazał Trybunał Konstytucyjny, na podstawie tego pisma nie można było określić, „czy przyczyną niekonstytucyjności jest zbyt szeroki katalog przestępstw, odnośnie do których można stosować (…) kontrolę operacyjną (…), czy też nieprzydatność kontroli operacyjnej do rozpoznawania i wykrywania niektórych z nich, ewentualnie zapobiegania niektórym z nich" (cz. III, pkt 13.2.2 *in fine* uzasadnienia wyroku). Tymczasem należy zauważyć, że podstawowym zastrzeżeniem Prokuratora Generalnego wobec tego przepisu była właśnie jego blankietowość i niedookreśloność, uniemożliwiająca ustalenie regulacji, które na jego mocy mają współkształtować kompetencje SKW i SWW. Trudno wobec tego żądać od niego oceny proporcjonalności zaskarżonego przepisu, skoro nie jest jasny jego zakres przedmiotowy (nie da się więc zrekonstruować „przedmiotu" oceny). Poza tym – moim zdaniem – poziom szczegółowości uzasadnienia tego zarzutu nie odbiega od innych, które Trybunał Konstytucyjny dopuścił do merytorycznego rozpoznania.

Podobne były także powołane w uzasadnieniu wyroku powody umorzenia postępowania co do art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW, z tym że dodatkowo Trybunał Konstytucyjny samodzielnie ustalił, iż poza zaskarżoną ustawą nie ma żadnych innych regulacji krajowych czy międzynarodowych, które określałyby zadania SKW i SWW, wobec czego zastrzeżenia Prokuratora Generalnego mają charakter czysto „hipotetyczny". W mojej opinii, stanowisko to jest nazbyt rygorystyczne z analogicznych przyczyn, jak wymienione wyżej, a ponadto pomija specyfikę postępowania przed Trybunałem Konstytucyjnym zainicjowanego przez Prokuratora Generalnego. Należy bowiem przypomnieć, że ani w Konstytucji, ani w ustawie o TK wnioski pochodzące od Prokuratora Generalnego nie mają charakteru konkretnego. Podejmowana na ich skutek kontrola jest kontrolą abstrakcyjną, a więc niezależną od okoliczności konkretnych stanów faktycznych, w których kwestionowany przepis jest stosowany. Niewystępowanie takich stanów faktycznych (nazwany przez Trybunał Konstytucyjny „hipotetycznością") nie może więc być przesłanką odmowy rozpoznania wniosku Prokuratora Generalnego. Aktualny brak „przepisów odesłania" dla art. 5 ust. 1 pkt 9 ustawy o SKW oznacza tylko, że sygnalizowane przez niego negatywne skutki wskazanej regulacji dla praw i wolności obywatelskich są

odroczone w czasie i mogą zaktualizować się wraz ze zmianą stanu prawnego (przyjęcia bliżej nieokreślonych nowych ustaw lub umów międzynarodowych) – co zresztą jest jednym z ważniejszych zarzutów wniosku.

2.2. Art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. a i g ustawy o SKW uprawniają SKW i SWW do prowadzenia kontroli operacyjnej w związku z przestępstwami przeciwko pokojowi, ludzkości oraz przestępstwami wojennymi określonymi w rozdziale XVI k.k., „a także innych ustawach i umowach międzynarodowych" oraz „innych przestępstw" niż wymienione w art. 5 ust. 1 pkt 1 lit. a-f „godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność". Natomiast art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW umożliwia stosowanie tej kontroli w celu „podejmowania działań przewidzianych dla SKW w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana".

Uważam, że powyższe regulacje są niezgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji.

Pierwsza z nich nie spełnia wymogu, aby zakres przedmiotowy dopuszczalnej kontroli operacyjnej był sformułowany na poziomie ustawowym w sposób konkretny, tj. wymieniał zamknięty katalog czynów zabronionych, w związku z którymi SKW i SWW mogą prowadzić tę kontrolę. Zwrot „a także innych ustawach i umowach międzynarodowych", zamieszczony w art. 5 ust. 1 pkt 1 lit. a ustawy o SKW, odsyła jednak do bliżej nieokreślonej grupy przestępstw penalizowanych przez dowolne ustawy i umowy międzynarodowe. Strona podmiotowa tych przestępstw ogranicza się do wskazania profilu zawodowego sprawców (SKW i SWW mogą działać tylko w celu wykrywania i ścigania przestępstw popełnianych przez wojsko lub administrację wojskową), co przecież nie wyklucza naruszenia przy okazji praw i wolności osób postronnych. Strona przedmiotowa nawiązuje do siatki pojęciowej stosowanej przez kodeks karny, wymieniając chronione dobra (pokój, ludzkość) lub rodzaj przestępstw (przestępstwa wojenne). Choć kategorie te są powszechnie używane w języku prawnym i prawniczym, mogą się one okazać trudne do jednoznacznego przełożenia na inne ustawy lub umowy międzynarodowe. Duża swoboda przysługująca SKW i SWW w tym zakresie w praktyce niweczy jakąkolwiek obiektywną kontrolę stosowania zaskarżonej regulacji (por. art. 31 ust. 1-3 ustawy o SKW). Dodatkowo należy także zauważyć, że nie zabezpiecza ona obywateli przed rozszerzaniem zakresu kompetencji tych służb „tylnymi drzwiami" – poprzez tworzenie nowych regulacji kompetencyjnych poza ustawą o SKW. Może to następować także na mocy umów międzynarodowych, które zostały ratyfikowane w trybie zwykłym (bez uprzedniej zgody na ratyfikację wyrażonej w ustawie). Trybunał Konstytucyjny wydaje się świadomy powyższych problemów, skoro stwierdza w kontekście tej regulacji, że „ustanowienie statycznego odesłania do konkretnych jednostek redakcyjnych ustawy karnej typizujących przestępstwa wzmacniałoby niewątpliwie poziom ochrony jednostki przed potencjalnym ryzykiem arbitralności organów władzy publicznej" (cz. III, pkt 8.9.2 *in fine* uzasadnienia wyroku). Ta słuszna konstatacja nie miała jednak wpływu na ocenę konstytucyjności zaskarżonego przepisu.

Druga zaskarżona regulacja, zawarta w art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW, jest obarczona podobnymi błędami, jak analizowane wyżej przepisy o ABW. Nie powtarzając całości już przytoczonej argumentacji wystarczy wskazać, że niewymienione w ustawie, bliżej nieokreślone „przestępstwa godzące w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność", nie mogą uprawniać do stosowania przez SKW i SWW kontroli operacyjnej, bo nie określają jednoznacznie dozwolonego prawnie zakresu tej

kontroli. Pojęcie „godzenia w potencjał obronny” nie jest pojęciem prawnym i trudno określić, jakie stany faktyczne mogą się na niego składać, zwłaszcza że chodzi tutaj także o potencjał obronny państw, „które zapewniają wzajemność”. Oceny tej regulacji nie zmienia fakt, że zakres działania SKW i SWW jest ograniczony pod względem podmiotowym i obejmuje przede wszystkim żołnierzy i pracowników administracji wojskowej. Choć z racji specyfiki wykonywanych zadań muszą się oni liczyć ze stosunkowo większym ograniczeniem prywatności niż cywile, powinni mieć pewność co do zakresu tych ograniczeń.

Najbardziej kuriozalne rozwiązanie znajduje się w trzeciej zaskarżonej regulacji (art. 31 ust. 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW), z której wynika, że SKW i SWW mogą stosować kontrolę operacyjną w związku z realizacją bliżej nieokreślonych „zadań”, jedynie pod tym warunkiem, że wynikałyby one z ustaw lub umów międzynarodowych. Taki sposób uregulowania kompetencji SKW pozornie respektuje tylko jedną przesłankę dopuszczalności ograniczenia praw i wolności konstytucyjnych, a mianowicie wymóg ich określenia w przepisach o randze ustawowej. Nawet on nie jest jednak zrealizowany w całości – podobnie jak art. 5 ust. 1 pkt 1 lit. a ustawy o SKW nie wyłącza on możliwości upoważnienia SKW i SWW do kontroli operacyjnej na mocy umów międzynarodowych ratyfikowanych w trybie zwykłym (bez zgody wyrażonej w ustawie). Zaskarżona regulacja nie przewiduje natomiast żadnych, nawet najbardziej szczątkowych granic przedmiotowych „zadań” tych służb, które mogą wymagać sięgnięcia po podsłuchy czy kontrolę korespondencji. Stopień jej ogólnikowości jest więc szczególnie duży nawet w kontekście pozostałych, także niedopuszczalnych rozwiązań z ustawy o SKW, o których była mowa wyżej.

2.3. Także w tym wypadku Trybunał Konstytucyjny – moim zdaniem – nie uwzględnił standardów ochrony prawa do prywatności i wolności komunikowania się, wynikających z dotychczasowego orzecznictwa (odpowiednie zastosowanie mają w tym zakresie uwagi do zaskarżonych przepisów ustawy o ABW, zamieszczone w pkt 1.3 niniejszego zdania odrębnego).

3. Zakres przedmiotowy i procedura udostępniania danych telekomunikacyjnych (otwarty katalog przestępstw, subsydiarność, brak niezależnej kontroli – cz. I, pkt 5 sentencji oraz cz. III, pkt 10.4-10.11 uzasadnienia wyroku).

3.1. Na wstępie chcę zaznaczyć, że – moim zdaniem – Trybunał Konstytucyjny dokonał nieuprawnionego zawężenia zakresu rozpoznania wniosków Rzecznika Praw Obywatelskich z 1 sierpnia 2011 r. i 27 kwietnia 2012 r. oraz Prokuratora Generalnego z 21 czerwca 2012 r., dotyczących posługiwania się przez różne służby danymi telekomunikacyjnymi. Moim zdaniem, wyrok Trybunału Konstytucyjnego w powyższym zakresie dotknięty jest dwoma wadami formalnymi.

Po pierwsze, zarzuty wnioskodawców nie zostały rozpoznane w całości, pomimo ich prawidłowego omówienia w uzasadnieniu wyroku (por. cz. III, pkt 10.1).

Z treści wszystkich pism inicjujących postępowanie w analizowanym zakresie wyraźnie wynika, że wnioskodawcy stawiają zaskarżonym przepisom zarzuty w trzech płaszczyznach:

– braku selektywności zarówno na etapie rozpoczęcia pozyskiwania danych telekomunikacyjnych (tj. możliwości uzyskiwania przez służby danych telekomunikacyjnych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną, w tym także danych objętych tajemnicą zawodową – por. wniosek RPO z 1 sierpnia 2011 r., s. 15 i 17-19 oraz prawie cały wniosek PG z 21 czerwca 2012 r.; we wniosku RPO zarzut ten nie dotyczy

pozyskiwania danych przez Służbę Celną), jak i po jej zakończeniu (nieusuwanie danych zbędnych dla postępowania karnego zgromadzonych przez część służb – por. wniosek RPO z 1 sierpnia 2011 r., s. 14, 15 i 23 i z 27 kwietnia 2012 r., s. 13 i 14);

– braku subsydiarności (tj. niezachowania zasady, że uzyskiwanie danych telekomunikacyjnych nie powinno być podstawowym sposobem pracy operacyjnej, lecz środkiem, po który sięga się jedynie w ostateczności, po wyczerpaniu innych możliwości zgromadzenia dowodów lub gdy istnieje wysokie prawdopodobieństwo, że okażą się one nieskuteczne – por. wniosek RPO z 1 sierpnia 2011 r., s. 15 i 22 i z 27 kwietnia 2012 r., s. 6 i 10);
– braku niezależnej, sądowej kontroli udzielania zezwoleń na pozyskiwanie danych telekomunikacyjnych (por. wniosek RPO z 1 sierpnia 2012 r., s. 12, 19-21 i z 27 kwietnia 2012 r., s. 11 i 12).

Tymczasem cz. I, pkt 5, 6, 7 i 8 sentencji wyroku Trybunału Konstytucyjnego, w którym rozpoznane są powyższe wnioski, ogranicza się do oceny konstytucyjności zaskarżonych przepisów jedynie pod względem części powyższych zarzutów, a reszta z nich nie jest objęta zawartym w wyroku postanowieniem co do umorzenia postępowania (por. cz. III, pkt 13 uzasadnienia wyroku). Orzeczenie to nie ocenia mianowicie otwartego katalogu przestępstw uzasadniających dostęp służb do danych telekomunikacyjnych i ich zróżnicowanej społecznej szkodliwości, choć w jego uzasadnieniu można znaleźć wywody na ten temat, potwierdzające zastrzeżenia Prokuratora Generalnego (por. np. jeżeli chodzi o niezachowanie zasady subsydiarności: cz. III, pkt 10.4.4 i pkt 10.11 uzasadnienia; nie miało to niestety odpowiedniego przełożenia na sentencję wyroku). Choć znaczna część rozprawy dotycząca wniosków Rzecznika Praw Obywatelskich z 1 sierpnia 2011 r. i 27 kwietnia 2012 r. oraz Prokuratora Generalnego z 21 czerwca 2012 r. koncentrowała się na innych aspektach zaskarżonej regulacji (kwestii należytych gwarancji proceduralnych), wnioskodawcy nie złożyli oświadczenia o ograniczeniu zakresu zaskarżenia i cofnięciu wniosków w pozostałym zakresie.

Moim zdaniem, kwestie te powinny być ujęte w cz. I, pkt 5 sentencji wyroku – samo zagwarantowanie niezależnej kontroli decyzji o udostępnieniu danych telekomunikacyjnych (nawet sądowej – choć Trybunał Konstytucyjny uznaje to za nadmierne – por. cz. III, pkt 10.4 *in fine* uzasadnienia wyroku) bez ustawowego określenia kryteriów, według których ma ona się dokonywać, zapewniłoby tylko formalną, a nie faktyczną ochronę praw i wolności obywateli (por. szczegółowo niżej).

Po drugie, Trybunał Konstytucyjny w cz. I, pkt 5 sentencji w sposób nieuzasadniony ograniczył także zakres wzorców, pomijając wskazane we wnioskach (z odpowiednim uzasadnieniem) art. 2 Konstytucji i art. 8 Konwencji. Wyjaśnienie tej decyzji ograniczyło się do powołania na ogólne zasady ekonomiki postępowania (zbędność orzekania – por. cz. III, pkt 13.4 uzasadnienia wyroku). Formułowane przez wnioskodawców (zwłaszcza Prokuratora Generalnego) zarzuty naruszenia przez zaskarżone przepisy zasady określoności prawa (a w konsekwencji – zaufania obywateli do państwa i prawa) nie tylko nie zostały „skonsumowane" przez pozostałe uwzględnione przez większość składu orzekającego wzorce kontroli, ale także dostarczają – moim zdaniem – bardzo istotnych argumentów za niekonstytucyjnością badanych przepisów (por. niżej). Natomiast pominięcie art. 8 Konwencji miało wyraźnie negatywny wpływ na wynik sprawy, ponieważ przepis ten jest źródłem wyraźnie wyższego standardu ochrony prawa do prywatności i tajemnicy komunikowania się niż przyjęty w niniejszym wyroku (co widać nawet na tle orzeczeń ETPCz omawianych w uzasadnieniu wyroku – por. cz. III, pkt 2, zob. także orzeczenia ETPCz omówione wyżej). Dziwi mnie też brak konsekwencji Trybunału Konstytucyjnego, jeżeli chodzi o traktowanie tego wzorca kontroli – został on przecież (bez bliższego wyjaśnienia tej rozbieżności) uwzględniony obok art. 47 i art. 49 w związku z art.

31 ust. 3 Konstytucji w cz. I, pkt 3 sentencji wyroku, który także dotyczy zakresu przedmiotowego uprawnień ABW, SKW i SWW do inwigilacji obywateli (lecz za pomocą środków kontroli operacyjnej, a nie analizy danych telekomunikacyjnych).

3.2. Przechodząc do *meritum* sprawy, należy zauważyć, co następuje:

Uważam, że wszystkie zarzuty Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego odnośnie do art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 32 ust. 1 pkt 1 ustawy o SKW, art. 18 ust. 1 pkt 1 ustawy o CBA i art. 75d ust. 1 ustawy o SC zasługują na uwzględnienie. Przepisy te naruszają art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji co najmniej z następujących powodów:

Po pierwsze, brak w nich wyraźnego określenia zakresu przedmiotowego dostępu wymienionych służb do danych telekomunikacyjnych. Zaskarżone regulacje odwołują się jedynie do celu, któremu mają służyć uzyskane informacje, przy czym czynią to nader ogólnikowo, wskazując, że musi to być uzasadnione z uwagi na:

- „zapobieganie lub wykrywanie przestępstw" (tak np. art. 20c ust. 1 ustawy o Policji i art. 10b ust. 1 ustawy o SG), względnie także przestępstw skarbowych (por. art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej i art. 30 ust. 1 ustawy o ŻW, a w wypadku Służby Celnej – przestępstw skarbowych tylko z rozdziału 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy, Dz. U. z 2013 r. poz. 186, ze zm.; dalej: k.k.s.) lub także „naruszeń" innych przepisów (które nie są przestępstwami ani przestępstwami skarbowymi – por. art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej),
- realizację ustawowych „zadań" służb (por. art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA oraz art. 32 ust. 1 pkt 1 ustawy o SKW).

W rezultacie zaskarżone przepisy – z wyjątkiem dostatecznie precyzyjnego art. 75d ust. 1 ustawy o SC – pozwalają na uzyskiwanie przez wymienione służby dostępu do danych telekomunikacyjnych podczas postępowań prowadzonych w sprawach:

- czynów penalizowanych przez kodeks karny i zabronionych na mocy licznych ustaw szczególnych (Prokurator Generalny szacuje w tym kontekście, że do dostępu do danych komunikacyjnych upoważnia co najmniej dwa razy więcej przestępstw niż do podejmowania kontroli operacyjnej – por. wniosek z 21 czerwca 2012 r., s. 52);
- stanowiących przestępstwa lub przestępstwa skarbowe, a także: delikty administracyjne (np. niedopełnienie obowiązku zgłoszeń INTRASAT oraz korekty tych zgłoszeń – por. art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej) lub cywilne (np. niesłuszne uzyskanie korzyści kosztem Skarbu Państwa lub innych państwowych osób prawnych – por. art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o CBA), a nawet przewinienia służbowe (np. naruszenie zasad prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne – por. art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o CBA) albo w ogóle bez związku z naruszeniem jakichkolwiek przepisów (np. w ramach kontroli oświadczeń majątkowych osób pełniących funkcje publiczne – por. art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA);
- ściganych z oskarżenia publicznego i z oskarżenia prywatnego (np. pomówienie – por. art. 212 k.k. czy znieważenie – por. art. 216 k.k.), a ponadto czynów, których ściganie następuje na wniosek pokrzywdzonego (tzw. przestępstwa wnioskowe, np. niepłacenie alimentów – por. art. 209 k.k., kradzież na szkodę osoby najbliższej – por. art. 278 § 4 k.k.);
- niezależnie od stopnia ich szkodliwości społecznej;
- często bez względu na specyfikę danej formacji i jej zadania (np. Policja i Straż Graniczna mogą pozyskiwać i przetwarzać dane telekomunikacyjne także w celu

zapobiegania i wykrywania przestępstw skarbowych, choć powinno to być domeną kontroli skarbowej);

- nie zawsze dla wykrywania, ścigania i zapobiegania przestępstwom, ale także dla realizacji zadań kontrolnych (np. wspomniana kontrola oświadczeń majątkowych – por. art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA) lub działalności analityczno-planistycznej (por. art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 4 ustawy o SKW, art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 4 ustawy o ABW i art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 ustawy o CBA).

Wobec powyższego wydaje się, że przeciętnie obyty z prawem i praktyką działania służb obywatel będzie miał duże trudności z ustaleniem, w jakich sytuacjach musi poważnie liczyć się z korzystaniem przez służby z jego danych telekomunikacyjnych. Wymagałoby to znajomości wielu przepisów z różnych ustaw (tak jest nawet w wypadku stosunkowo najbardziej precyzyjnego art. 75d ust. 1 ustawy o SC), a poza tym często także akceptacji rozwiązań rażąco sprzecznych ze zdrowym rozsądkiem. Na podstawie literalnego brzmienia zaskarżonych przepisów na przykład Policja mogłyby skutecznie żądać dostępu do bilingów telefonicznych w związku z podejrzeniem:

- zniesławienia (por. art. 212 k.k.),
- wyrębu drzewa w lesie o wartości przekraczającej 1/4 minimalnego wynagrodzenia (czyli obecnie 420 zł, por. art. 120 ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń, Dz. U. z 2013 r. poz. 482, ze zm.),
- prowadzenia nielegalnej hodowli chartów rasowych (por. art. 52 pkt 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie, Dz. U. z 2013 r. poz. 1226, ze zm.) czy też
- niezamieszczenia „stopki redakcyjnej" w gazecie (por. art. 49 w związku z art. 27 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe, Dz. U. Nr 5, poz. 24, ze zm.).

Wymienione niedostatki zaskarżonych regulacji (poza wspomnianym art. 75d ust. 1 ustawy o SC) stanowią – w mojej opinii – przede wszystkim naruszenie zasady zaufania obywateli do państwa i prawa oraz zasady określoności prawa (art. 2 Konstytucji), które zabraniają stanowienia przepisów niejasnych, zastawiających „pułapki" na obywatela i absurdalnych. W kategoriach art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji i art. 8 Konwencji ich wadliwość polega natomiast przede wszystkim na tym, że umożliwiają one stosowanie kontroli operacyjnej także w odniesieniu do błahych przestępstw, wobec czego nie da się jednoznacznie ocenić, czy jako całość spełniają one wymogi proporcjonalności.

Po drugie, w zaskarżonych przepisach brak jest zastrzeżenia, że dane telekomunikacyjne mogą być udostępnianie służbom tylko wówczas, gdyby inne środki zdobywania informacji okazały się nieskuteczne albo istniało wysokie ryzyko, że okażą się nieskuteczne lub nieprzydatne (wada ta dotyka także art. 75d ust. 1 ustawy o SC, który – jako jedyny – spełniał warunek dostatecznej precyzyjności). Moim zdaniem, ekwiwalentem takiej klauzuli subsydiarności nie może być zastrzeżenie zawarte w trzech zaskarżonych przepisach, że niektóre służby mogą uzyskiwać w celu realizacji swoich zadań tylko informacje „niezbędne" (por. 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 SKW) – brak jest bowiem dokładnie opisanych kryteriów, według których ta niezbędność miałaby być oceniana. Tymczasem tego typu rozwiązania są znane w polskim systemie prawnym i obowiązują na przykład w zakresie pozaprocesowej kontroli operacyjnej dokonywanej przez te same służby, które są objęte wnioskami w analizowanym zakresie (por. art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA i art. 31 ustawy o SKW).

Wskazany brak subsydiarności zaskarżonych przepisów otwiera możliwość wykorzystywania danych telekomunikacyjnych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy gdy jest to po

prostu najprostsze i najwygodniejsze (por. wyrok z 12 grudnia 2005 r., sygn. K 32/04, OTK ZU nr 11/A/2005, poz. 132). Zważywszy na rozwój technologii informatycznej i telekomunikacyjnej, uzyskiwanie i przetwarzanie takich danych staje się coraz mniej skomplikowane i kosztowne, a poza tym daje dobre wyniki w stosunkowo krótkim czasie. Wobec tego istnieje ryzyko, że sprawdzenie bilingów z rozmów telefonicznych czy odczytów z GPS zamontowanego w telefonie czy samochodzie będzie wkrótce pierwszą czynnością podejmowaną we wszystkich sprawach na przykład w celu wytypowania wstępnego kręgu osób zamieszanych w dane przestępstwo, nawet wtedy gdy – bez szkody dla wyniku postępowania – można ten sam cel osiągnąć tradycyjnymi metodami śledczymi, bez ingerencji w prywatność dużej liczby obywateli.

W swoim aktualnym kształcie zaskarżone przepisy jako całość nie spełniają więc warunku konieczności (niezbędności) ograniczeń. Ponadto niewłaściwie wyważają relacje między wartościami chronionymi i wartościami ograniczanymi, naruszając zasadę proporcjonalności z art. 31 ust. 3 Konstytucji. Ten ostatni aspekt jest szczególnie widoczny wtedy, gdy dane telekomunikacyjne mają służyć innym celom niż wykrywanie czy zapobieganie przestępstwom. Uważam, że działania kontrolne (wobec osób, co do których nie ma najmniejszego podejrzenia popełnienia przestępstwa) czy analityczne nigdy nie uzasadniają pozyskiwania i przetwarzania danych telekomunikacyjnych.

Po trzecie, dostęp wskazanych służb do danych telekomunikacyjnych o obywatelach nie podlega w świetle zaskarżonych przepisów jakiejkolwiek obiektywnej kontroli (ani uprzedniej, ani następczej). Przepisy dotyczące poszczególnych formacji przewidują niekiedy jedynie szczątkową kontrolę wewnętrzną w postaci zatwierdzania wniosków o udostępnianie danych przez przełożonych funkcjonariuszy występujących z wnioskiem o udostępnienie danych (np. w wypadku policjantów – Komendanta Głównego Policji lub komendanta wojewódzkiego Policji – por. art. 20c ust. 2 ustawy o Policji), co jednak nie zapewnia w należyty sposób właściwego korzystania przez te służby z prawa dostępu do danych telekomunikacyjnych (por. ETPCz w wyroku z 26 kwietnia 2007 r. w sprawie Dumitru Popescu przeciwko Rumunii, skarga nr 71525/01, § 71 uznał, że wymóg należytej kontroli legalności podsłuchów nie jest spełniony w wypadku nadzoru prokuratora poddanego wpływowi władzy wykonawczej).

Brak omawianego mechanizmu zewnętrznej kontroli świadczy – moim zdaniem – pośrednio także o naruszeniu zasady proporcjonalności z art. 31 ust. 3 Konstytucji. Nie pozwala on bowiem na rzetelną weryfikację, czy w danym wypadku korzystanie z danych telekomunikacyjnych jest rzeczywiście niezbędne i czy oczekiwane korzyści z tego sposobu pozyskiwania informacji będą tak duże, aby uzasadniało to ingerencję w prawo do prywatności i wolność komunikowania się osoby, której dane te dotyczą, oraz pozostających z nią w kontakcie osób postronnych.

Sądzę, że już każda z powyższych wad zaskarżonych rozwiązań osobno stanowiłaby wystarczający powód do uznania ich sprzeczności z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz art. 8 Konwencji. Łącznie doprowadzają one do sytuacji, w której wymienione służby dysponują (praktycznie rzecz biorąc) nieskrępowaną możliwością dostępu do danych telekomunikacyjnych obywateli. Nie zawierają one ani merytorycznych, ani proceduralnych gwarancji, że uprawnienia te nie będą nadużywane bez rzeczywistej przyczyny i w błahych sprawach (por. minimalne warunki czynności operacyjnych wobec obywateli sformułowane w powołanym wyroku o sygn. K 32/04).

Uważam, że szeroki zakres danych telekomunikacyjnych udostępnianych służbom (por. art. 180c i art. 180d prawa telekomunikacyjnego) i możliwość uzyskania na ich podstawie informacji na temat wszystkich sfer życia osobistego obywateli uzasadniają konieczność pilnej nowelizacji zaskarżonych przepisów. Celowe powinno być osiągnięcie porównywalnego standardu ochrony prawa do prywatności i wolności komunikowania się

jak przy kontroli operacyjnej. Przy obecnym poziomie rozwoju technologii inwazyjność tych dwóch sposobów pozyskiwania informacji o obywatelach jest zbliżona (choć dane telekomunikacyjne – w przeciwieństwie do informacji uzyskiwanych w toku kontroli operacyjnej – nie dostarczają informacji o treści komunikatów, to w zamian za to można na ich podstawie ustalić np. fakt przebywania danej osoby w określonym miejscu lub grono osób, z którymi się ona kontaktuje).

Wybór odpowiednich rozwiązań w tym zakresie należy do ustawodawcy, a standard konstytucyjny mogą – moim zdaniem – spełniać różne rozwiązania szczegółowe. Powinny one dawać pewność, że dane telekomunikacyjne obywateli będą udostępniane służbom jedynie wtedy, gdy jest to niezbędne (a więc tylko w odniesieniu do ściśle określonych, najpoważniejszych przestępstw), przy zachowaniu zasady subsydiarności i zapewnieniu kontroli zewnętrznej przez organ niezależny od władzy wykonawczej (najlepiej – sąd).

3.3. Na marginesie można wspomnieć, że z powyższych względów kwestionowane przepisy nie spełniają także wymogów stawianych pozyskiwaniu i przetwarzaniu danych telekomunikacyjnych przez orzecznictwo ETPCz (w tym zwłaszcza wyroki z: 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79; 25 września 2001 r. w sprawie P. G. i J. H. przeciwko Wielkiej Brytanii, skarga nr 44787/98; 3 kwietnia 2007 r. w sprawie Copland przeciwko Wielkiej Brytanii, skarga nr 62617/00 oraz w zakresie obowiązku zapewnienia odpowiednich gwarancji proceduralnych wyroki z: 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii, skarga nr 28341/95 i 26 kwietnia 2007 r. w sprawie Dumitru Popescu przeciwko Rumunii, skarga nr 71525/01) oraz Trybunału Sprawiedliwości UE (por. zwłaszcza wyrok z 8 kwietnia 2014 r. w połączonych sprawach High Court of Ireland i Verfassungsgerichtshof z Austrii, sygn. C-293/12).

Orzeczenia te są szeroko omawiane w cz. III, pkt 2 i 3 uzasadnienia kwestionowanego wyroku, więc niewątpliwie były znane składowi orzekającemu. Mogę wobec tego jedynie wyrazić ubolewanie, że zawarta w nich wszechstronna i szczegółowa argumentacja nie znalazła odpowiedniego zastosowania w niniejszej sprawie, pomimo że Polska jest zobowiązana także do przestrzegania standardów wynikających z prawa Unii Europejskiej i Konwencji (której art. 8 jest zresztą nieprzypadkowo wzorcem kontroli w niniejszej sprawie).

4. Zakres przedmiotowy kontroli operacyjnej (informacje objęte tajemnicą zawodową – cz. I, pkt 6 sentencji i cz. III, pkt 11 uzasadnienia wyroku).

4.1. Uważam, że Trybunał Konstytucyjny także w odniesieniu do stosowania kontroli operacyjnej w celu gromadzenia informacji objętych tajemnicą zawodową wadliwie zrekonstruował zakres zaskarżenia.

Po pierwsze, przyjęty do rozpoznania wniosek Prokuratora Generalnego z 13 listopada 2012 r. częściowo nie spełnia warunków formalnych, przewidzianych w art. 32 ust. 1 pkt 4 ustawy o TK.

Wnioskodawca w *petitum* swojego pisma wniósł o zbadanie dopuszczalności pozyskiwania za pomocą kontroli operacyjnej informacji zawierających tajemnice: adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego i lekarską. Uzasadnienie wniosku dotyczy jednak szczegółowo wyłącznie tajemnicy obrończej oraz tajemnicy dziennikarskiej, a argumentacja odnośnie do pozostałych rodzajów tajemnicy zawodowej ogranicza się do sformułowania zarzutu, że kontrola operacyjna niewyłączająca informacji chronionych tymi tajemnicami daje służbom „zbyt szeroki zakres swobody" (por. s. 63 wniosku). Na marginesie można zauważyć, że także uzasadnienie wyroku Trybunału Konstytucyjnego koncentruje się na tajemnicy obrończej i dziennikarskiej, nie zawiera

natomiast omówienia np. tajemnicy lekarskiej (por. cz. III, pkt 11.6 uzasadnienia wyroku).

Podobnie jest ze wskazanymi we wniosku wzorcami kontroli. Z wymienionych przez Prokuratora Generalnego sześciu przepisów Konstytucji (nie licząc związkowego art. 31 ust. 3) i trzech przepisów Konwencji, podstawą jego argumentacji były wyłącznie – art. 51 ust. 2 (s. 54-55) oraz art. 42 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także art. 6 ust. 3 lit. b i c (s. 71-74) i art. 10 ust. 1 Konwencji (s. 79-84), co w znacznej części koresponduje z ustalonym wyżej przedmiotem zaskarżenia. Treść art. 54 ust. 1 Konstytucji – pomimo że przepis ten obejmuje materię zbliżoną do art. 10 ust. 1 Konwencji – w ogóle nie została w uzasadnieniu wniosku powołana. Natomiast pozostałe wzorce wskazane w *petitum* wniosku są w uzasadnieniu pisma Prokuratora Generalnego obszernie omówione (z uwzględnieniem orzecznictwa TK oraz ETPCz, nie zawsze jednak trafnie – por. np. zbyt daleko idąca teza, że z art. 8 Konwencji bezpośrednio wypływa nakaz ochrony przed ujawnieniem tajemnic zawodowych – s. 64 wniosku), lecz uzasadnienie wątpliwości na ich tle ogranicza się do sformułowania zarzutów, bez powołania dowodów na ich poparcie (a pisma inicjujące postępowanie przed Trybunałem Konstytucyjnym muszą zawierać obydwa te elementy – por. art. 32 ust. 1 pkt 3 i 4 ustawy o TK). Biorąc pod uwagę, że przedmiotem rozpoznania w tym zakresie powinien być jedynie wpływ kontroli operacyjnej na tajemnicę obrończą i tajemnicę dziennikarską, skuteczne ich powołanie nie miałoby zresztą większego znaczenia, gdyż podstawowym wzorcem kontroli powinny być przepisy konstytucyjne i konwencyjne dotyczące tych zagadnień bezpośrednio (Trybunał Konstytucyjny wszak często w ramach rekonstrukcji wzorców kontroli stosuje zasadę, że odwoływanie się do wzorców o charakterze bardziej ogólnym jest zbędne, jeśli istnieją normy konstytucyjne o większym stopniu szczegółowości, ściślej wiążące się z ocenianą regulacją – por. np. wyrok z 27 lipca 2012 r., sygn. P 8/12, OTK ZU nr 7/A/2012, poz. 85).

Moim zdaniem, należało wobec tego ograniczyć zakres orzekania w niniejszej sprawie do zbadania, czy przepisy wymienione w cz. I, pkt 6 sentencji wyroku są zgodne z art. 42 ust. 2 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji oraz z art. 6 ust. 3 lit. b i c oraz art. 10 ust. 1 Konwencji „z powodu" (tak zakres zaskarżenia jest sformułowany we wniosku) pominięcia w nich ochrony tajemnicy obrończej i tajemnicy dziennikarskiej.

Po drugie, Trybunał Konstytucyjny także tym razem nie rozpoznał całości przedłożonej mu sprawy: cz. I, pkt 6 sentencji orzeka jedynie o braku w zaskarżonych przepisach gwarancji niezwłocznego, protokolarnego i komisyjnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne. Prokurator Generalny we wniosku wyraźnie domaga się zaś orzeczenia w szerszym zakresie – czy tego typu materiały w ogóle mogą być pozyskiwane w toku kontroli operacyjnej. Kwestia niszczenia ewentualnych materiałów objętych tajemnicą zawodową nie wyczerpuje więc całości jego zastrzeżeń. Pominięte w sentencji wyroku elementy wniosku Prokuratora Generalnego nie są równocześnie objęte postanowieniem o umorzeniu postępowania (por. cz. III, pkt 13 uzasadnienia wyroku), a wnioskodawca podczas rozprawy nie złożył oświadczenia o cofnięciu wniosku w ich zakresie (pomimo że rzeczywiście z uwagi na pytania składu orzekającego analiza jego pisma dotyczyła przede wszystkim kwestii procedury postępowania z materiałami zawierającymi tajemnicę zawodową już po ich uzyskaniu, tj. tzw. kontroli następczej).

4.2. Jestem przekonany, że brak zakazu zdobywania za pomocą kontroli operacyjnej materiałów objętych tajemnicą dziennikarską i tajemnicą obrończą jest sprzeczny (odpowiednio) z art. 42 ust. 2 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 6 ust. 3 lit. b i c oraz art. 10 ust. 1 Konwencji.

Trybunał Konstytucyjny w uzasadnieniu wyroku (cz. III, pkt 11.6) obszernie

przeanalizował te dwie instytucje, nie ma więc potrzeby powtarzania tych ustaleń. Wystarczy stwierdzić, że bez tajemnicy obrończej nie mogłoby istnieć prawo do obrony, a bez tajemnicy dziennikarskiej – wolność mediów. Nie należy tych tajemnic w żadnym razie traktować w kategoriach przywilejów dla adwokatów (a w węższym zakresie – także radców prawnych) i dziennikarzy, są one bowiem instrumentem ochrony praw (odpowiednio) ich klientów lub współpracowników (informatorów; por. zwłaszcza wyrok z 22 listopada 2004 r., sygn. SK 64/03, OTK ZU nr 10/A/2004, poz. 107).

W przeciwieństwie do większości składu orzekającego nie uważam, aby wystarczającym rozwiązaniem problemu postawionego przez Prokuratora Generalnego było tylko wprowadzenie gwarancji, że materiały uzyskane pomimo zakazów dowodowych będą odpowiednio niszczone. Mechanizm taki jest oczywiście ważny i potrzebny, lecz jedynie jako instrument uzupełniający – na wypadek gdyby nie zadziałała gwarancja podstawowa w postaci całkowitego zakazu podsłuchiwania obrońców i dziennikarzy w zakresie objętym tajemnicą obrończą i dziennikarską. W świetle zasad doświadczenia życiowego należy bowiem przyjąć, że ujawnienie organom prowadzącym kontrolę operacyjną informacji objętych zakazami dowodowymi jest sytuacją nieodwracalną w tym sensie, że pozyskane w ten sposób dane nigdy nie zostają „wymazane" ze świadomości osób, które się z nimi zapoznały. Ograniczona jest tylko ich użyteczność jako formalnych dowodów w postępowaniu karnym, nie ma jednak (bo jest to prawnie niewykonalne) faktycznych przeszkód, aby były one wykorzystywane w toku postępowania na użytek wewnętrzny (np. przy planowaniu czynności postępowania przygotowawczego).

Wobec tego należy uznać, że zaskarżone przepisy w zakresie, w jakim nie przewidują zakazu pozyskiwania w czasie kontroli operacyjnej materiałów objętych tajemnicą obrończą i dziennikarską oraz mechanizmu niezwłocznego, protokolarnego niszczenia tego typu materiałów uzyskanych wbrew zakazowi, są niezgodne z art. 42 ust. 2 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 6 ust. 3 lit. b i c oraz art. 10 ust. 1 Konwencji.

Moim zdaniem, minimalną gwarancją poszanowania tajemnicy obrończej i dziennikarskiej jest zakaz pozyskiwania informacji objętych tą tajemnicą, a w wypadku ich przypadkowego zdobycia – weryfikacja zgromadzonych materiałów przez niezawisły sąd i albo uchylenie tajemnicy zawodowej, albo zniszczenie zgromadzonych materiałów (por. wyrok z 11 grudnia 2012 r., sygn. K 37/11, OTK ZU nr 11/A/2012, poz. 133 i omówione tam wyroki ETPCz z: 16 października 2001 r. w sprawie Brennan przeciwko Wielkiej Brytanii, skarga nr 39846/98 i 13 stycznia 2009 r. w sprawie Rybacki przeciwko Polsce, skarga nr 52479/99). W praktyce realizacja tych wymogów będzie wymagała wprowadzenia co do zasady całkowitego zakazu kontroli operacyjnej adwokatów i dziennikarzy, który mógłby być uchylany wyłącznie przez sąd i tylko w takim zakresie, w jakim nie dotyczyłby bezwzględnej tajemnicy obrończej i dziennikarskiej.

4.3. Nie ulega dla mnie wątpliwości, że sentencja wyroku Trybunału Konstytucyjnego nie respektuje także standardów traktowania tajemnicy obrończej i tajemnicy dziennikarskiej w kontekście kontroli operacyjnej, które na tle art. 6 ust. 3 lit. b i c oraz art. 10 ust. 1 Konwencji (wzorców kontroli w niniejszej sprawie) sformułował ETPCz.

W jego orzecznictwie podkreślano m.in., że niedopuszczalne jest tolerowanie sytuacji, gdy formalny zakaz podsłuchiwania adwokatów nie jest respektowany, ponieważ informacje z podsłuchów przegląda urzędnik pocztowy (a więc osoba podległa władzy wykonawczej), bez jakiegokolwiek nadzoru sądowego (por. wyrok z 18 maja 2010 r. w sprawie Kennedy przeciwko Wielkiej Brytanii, skarga nr 26839/05, § 73 i 74). Wielokrotnie też zaznaczano, że zagrożeniem dla prawa do obrony jest nie tylko rzeczywiście podejmowana kontrola operacyjna, ale także samo uzasadnione przekonanie, iż rozmowa

obrońcy z klientem może być rejestrowana lub podsłuchiwania. Może to bowiem skłaniać klientów do zatajania istotnych faktów, z negatywnym skutkiem dla obrony (por. m.in. wyroki ETPCZ z: 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom, skarga nr 5029/71; 25 czerwca 1997 r. w sprawie Halford przeciwko Wielkiej Brytanii, skarga nr 20605/92; 10 maja 2007 r. w sprawie Modarca przeciwko Mołdawii, skarga nr 14437/05).

Podobnie w orzecznictwie ETPCz była traktowana kwestia zagrożeń dla poufności kontaktów dziennikarzy z ich informatorami. Wskazywano m.in., że brak ochrony informatorów może zniechęcać ich do udzielania mediom informacji, które dotyczą interesu publicznego, a tym samym uniemożliwiać wykonywanie przez media ich podstawowej funkcji – kontroli społecznej (por. m.in. wyroki ETPCz z: 27 marca 1996 r. w sprawie Goodwin przeciwko Wielkiej Brytanii, skarga nr 17488/90, 22 listopada 2007 r. Voskuil przeciwko Holandii, skarga nr 64752/01).

5. Uwagi końcowe.

Na zakończenie chciałbym podkreślić, że na tle niniejszej sprawy z niepokojem obserwuję tendencję do przyznawania służbom kolejnych kompetencji do pozyskiwania informacji o obywatelach (por. np. art. 7 pkt 4 ustawy z dnia 26 maja 2011 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw, Dz. U. Nr 134, poz. 779, który wszedł w życie 14 lipca 2011 r. i umożliwił Służbie Celnej korzystanie z bilingów).

Moje zastrzeżenia budzi przede wszystkim brak należytej staranności ustawodawcy, jeżeli chodzi o badanie, jaki zakres inwigilacji obywateli przez państwo jest rzeczywiście niezbędny do zapobiegania i wykrywania przestępstw. Obawiam się również, że ustawodawca nie przywiązuje także należytej wagi do konieczności zapewnienia stosownych gwarancji proceduralnych, przeciwdziałających nadużywaniu przez Policję, ABW, CBA i inne służby uprawnień w zakresie kontroli operacyjnej i dostępu do danych telekomunikacyjnych.

Zdanie odrębne
sędziego TK Marka Zubika
do wyroku Trybunału Konstytucyjnego
z dnia 30 lipca 2014 r., sygn. akt K 23/11

Na podstawie art. 68 ust. 3 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643, ze zm.; dalej: ustawa o TK) zgłaszam zdanie odrębne do punktu 3 lit. a sentencji wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. o sygn. K 23/11.

1. Nie podzielam stanowiska Trybunału Konstytucyjnego odnośnie do punktu 3 lit. a sentencji niniejszego wyroku. Trybunał uznał, że art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, ze zm.; dalej ustawa o ABW) w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa", jest zgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz

uzupełnionej Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284, ze zm.; dalej: Konwencja).

2. Bezpieczeństwo państwa jest wartością chronioną konstytucyjnie. Jego ochrona uprawnia ustawodawcę do wprowadzania ograniczeń w korzystaniu z konstytucyjnych wolności i praw (*vide:* art. 5, art. 31 ust. 3 Konstytucji). W niniejszej sprawie żaden z uczestników postępowania nie kwestionował tych okoliczności. Problem konstytucyjny polegał na czymś innym. Chodziło bowiem o odpowiedź na pytanie, czy ustawodawca – w sposób dostatecznie precyzyjny – uregulował kompetencje Agencji Bezpieczeństwa Wewnętrznego do niejawnej ingerencji w prywatność jednostek, a w szczególności czy zakwestionowany przepis pozwala ustalić, jakie przestępstwa odpowiadają ogólnej przesłance „godzących w bezpieczeństwo państwa", a jednocześnie mogą być uznane za poważne w takim stopniu, aby uzasadniona i proporcjonalna w stosunku do nich mogła być kontrola operacyjna.

W przeciwieństwie do Trybunału uważam, że przepisy wskazane w punkcie 3 lit. a sentencji nie spełniają wymogu wysokiego stopnia precyzji, jaka w stosunku do przepisów ingerujących w wolności osobiste człowieka wynika zarówno z art. 2, jak i art. 31 ust. 3 Konstytucji w tej części, w której mowa jest o ustanowieniu „ograniczeń w ustawie".

3. Wyrok Trybunału w tym zakresie stanowi akceptację standardu ochrony wolności i praw jednostek poniżej wymagań stawianych dotychczas ustawodawcy przez sam Trybunał Konstytucyjny i Europejski Trybunał Praw Człowieka. W mojej ocenie orzeczenie to redukuje polski system ochrony praw jednostki poniżej wymagań wynikających nie tylko z Konstytucji, ale również z Konwencji.

4. Jak wielką wartością jest bezpieczeństwo państwa i pokojowe współdziałanie narodów, szczególnie dobitnie widać w doświadczeniach historycznych państwa polskiego. Nie każde jednak zagrożenie funkcjonowania instytucji publicznych uzasadnia ingerencję w wolności i prawa obywateli nawet przez państwo tak bardzo doświadczone wojnami i totalitaryzmem, w którym służby specjalne były wykorzystywane do represji własnych obywateli, w czasach „gdy podstawowe wolności i prawa człowieka były w naszej Ojczyźnie łamane" (wstęp do Konstytucji).

Konieczność orzeczenia o konstytucyjności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW, w części, w jakiej obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa", nie wynikała, w moim przekonaniu, z uzasadnionych potrzeb państwa. Nic nie stało bowiem na przeszkodzie, aby ustawodawca doprecyzował te przepisy przez powiązanie tej przesłanki z konkretnymi przestępstwami.

5. Trudne do zrozumienia jest orzeczenie o zgodności z Konstytucją przepisów, które posługują się niedostatecznie określonym wyrażeniem „przestępstw godzących w bezpieczeństwo państwa" w sytuacji, gdy stwierdzono niekonstytucyjność art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, który odnosił się do „przestępstw godzących w podstawy ekonomiczne państwa".

W mojej ocenie, oba przepisy, w takim samym stopniu nie precyzują przedmiotowego zakresu kontroli operacyjnej. Nie jest bowiem jasne, jakie przestępstwa godzą w „bezpieczeństwo państwa" ani w „podstawy ekonomiczne państwa". Nie było więc żadnych uzasadnionych powodów, by odmiennie traktować obydwa przepisy.

6. Niezrozumiałe jest orzeczenie o zgodności z Konstytucją i Konwencją omawianego tu przepisu jeszcze z jednego powodu. Nawet organy uczestniczące w

procedurze zarządzania kontroli operacyjnej dostrzegają bowiem jego wadliwość. Przedstawiciel Prokuratora Generalnego – organu wyrażającego zgodę na wystąpienie przez Szefa ABW z wnioskiem o zarządzenie takiej kontroli – wprost zaznaczył, że brak rodzajowego określenia przestępstw może prowadzić do rozbieżnych ocen Szefa ABW, Prokuratora Generalnego i Sądu Okręgowego w Warszawie co do kwalifikacji danego przestępstwa jako „godzącego w bezpieczeństwo państwa". Również przedstawiciel ABW wskazywał na pojawiające się w praktyce trudności interpretacyjne tego przepisu, postulując jego doprecyzowanie, aby zakres upoważnienia do prowadzenia kontroli operacyjnej był określony przez wskazanie rodzajów przestępstw. Może to prowadzić do faktycznego ograniczenia skuteczności kontroli operacyjnej, a w konsekwencji sprawności działania służb.

7. W art. 5 ust. 1 pkt 2 ustawy o ABW ustawodawca wymienił szereg przestępstw, które niewątpliwie są wymierzone w bezpieczeństwo państwa. Należą do nich: szpiegostwo, terroryzm i bezprawne ujawnienie lub wykorzystanie informacji niejawnych (art. 5 ust. 1 pkt 2 lit. a); produkcja i obrót towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa (art. 5 ust. 1 pkt 2 lit. d) oraz nielegalne wytwarzanie, posiadanie i obrót bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi w obrocie międzynarodowym (art. 5 ust. 1 pkt 2 lit. e). Przepisy te określają niewątpliwie poważne przestępstwa. Z wykładni wyrażenia zawartego w art. 5 ust. 1 pkt 2 lit. a ustawy o ABW „i innych przestępstw godzących w bezpieczeństwo państwa" wynika, że odnosić ma się do innych przestępstw niż wymienione w art. 5 ust. 1 pkt 2 lit. a-e ustawy o ABW.

8. Trafnie podnosił Rzecznik Praw Obywatelskich we wniosku oraz na rozprawie, że wyrażenie „przestępstwa godzące w bezpieczeństwo państwa" nie spełnia konstytucyjnych wymagań będących konsekwencją zasady dostatecznej określoności prawa. Żaden przepis ustawy o ABW nie posługuje się takim wyrażeniem ani nie rozstrzyga, jakie przestępstwa godzą w bezpieczeństwo państwa. Wprawdzie w art. 112 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.) mowa jest o przestępstwach przeciwko bezpieczeństwu wewnętrznemu i zewnętrznemu Rzeczypospolitej Polskiej, a to nawiązuje do wyrażenia występującego w zaskarżonym przepisie, ale nie ma jednolitego stanowiska, jakie przestępstwa mogą wchodzić także i tu w grę. W doktrynie prawa karnego podnosi się, że przepisy te obejmują przede wszystkim przestępstwa stypizowane w rozdziale XVII („Przestępstwa przeciwko Rzeczypospolitej Polskiej)" oraz rozdziale XVIII kodeksu karnego („Przestępstwa przeciwko obronności"). Nie jest jednak wykluczone, że dobru temu będą zagrażać liczne czyny unormowane w pozostałych rozdziałach kodeksu karnego, a także ustawach szczególnych (zob. m.in. T. Gardocka, uwaga 7 do art. 112, [w:] *Kodeks karny. Komentarz*, red. R. Stefański, Beck online 2014; K. Wiak, uwaga 4 do art. 112, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2013; A. Sakowicz, uwaga 5 do art. 112, [w:] *Kodeks karny. Część ogólna. Tom II. Komentarz do art. 32-116*, red. M. Królikowski, R. Zawłocki, Warszawa 2010). W konsekwencji uważam, że nie ma możliwości ustalenia – bez podejmowania ponadprzeciętnych wysiłków interpretacyjnych i odwoływania się do wykładni z analogii – które czyny zabronione są „przestępstwami godzącymi w bezpieczeństwo państwa", w rozumieniu art. 5 ust. 1 pkt 2 lit. a ustawy o ABW. Nie jest więc wykluczone, co trafnie zarzuca wnioskodawca, że każdy czyn zabroniony przez ustawę karną, który bezpośrednio lub pośrednio może być wymierzony w szeroko rozumiane państwo – w tym np. w osoby piastujące funkcję organów władzy publicznej, ich działalność bądź składniki mienia publicznego – może zostać uznany za godzący w

jego bezpieczeństwo, a więc będzie stanowić podstawę prawną do zastosowania kontroli operacyjnej.

Co więcej, o tym, czy dane przestępstwo spełnia ustawową kwalifikację „godzenia w bezpieczeństwo państwa", nie przesądzi ustawa, ale organ stosujący prawo – wnoszący o zarządzenie kontroli operacyjnej Szef ABW oraz Sąd Okręgowy w Warszawie, który wyraża zgodę na kontrolę operacyjną. Przepis ten może być w związku z tym uznany za blankietowy w rozumieniu dotychczasowego orzecznictwa Trybunału (zob. wyroki TK z: 5 maja 2004 r., sygn. P 2/03, OTK ZU nr 5/A/2004, poz. 39; 17 grudnia 2008 r., sygn. P 16/08, OTK ZU nr 10/A/2008, poz. 181).

Podzielam wobec powyższego zarzut niezgodności art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW w zakresie, w jakim obejmuje zwrot „i innych przestępstw godzących w bezpieczeństwo państwa", z art. 2 Konstytucji.

9. Podzielam także zarzut Rzecznika Praw Obywatelskich co do naruszenia przez ten przepis art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji. Niedostateczna określoność prowadzi do sytuacji, w której art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW może obejmować nie tylko poważne przestępstwa, ale także o relatywnie niskim stopniu szkodliwości. W takich wypadkach stosowanie kontroli operacyjnej – z punktu widzenia dolegliwości ingerencji w prywatność oraz tajemnicę komunikowania się – jest nadmierne, w rozumieniu art. 31 ust. 3 Konstytucji.

Ani na podstawie wypowiedzi uczestników postępowania na rozprawie, ani na podstawie ustaleń własnych Trybunału nie można potwierdzić tezy, że omawiany przepis jest stosowany jako podstawa prowadzenia kontroli operacyjnej tylko w wypadku poważnych przestępstw. Nie można było potwierdzić, że istnieje jednolita i utrwalona linia orzecznicza, która wyrażenie „przestępstwa godzące w bezpieczeństwo państwa" interpretuje w sposób ścisły. Co więcej, nie ma szansy na wykształcenie się linii orzeczniczej, gdyż postanowienia sądowe nie są uzasadniane, a procedura sądowa prowadzona jest z zachowaniem przepisów o ochronie informacji niejawnych. Ponadto Prezes Sądu Okręgowego w Warszawie, który zarządza kontrolę operacyjną na wniosek Szefa ABW, nie dokonuje analizy orzecznictwa pod względem jego jednolitości, o czym stanowi art. 22 pkt 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2013 r. poz. 427, ze zm.).

10. Z punktu widzenia sytuacji jednostki nie ma znaczenia, który z organów państwa narusza jej wolności lub prawa konstytucyjne. Naruszenie takie może nastąpić przez organy władzy zarówno ustawodawczej, jak i wykonawczej, a nawet sądowniczej.

Organ przedstawicielski Narodu, jakim jest parlament, powinien wziąć na siebie ciężar odpowiedzialności politycznej za umożliwienie stosowania kontroli operacyjnej w danych sytuacjach. Ma on obowiązek precyzyjnego wskazania poważnych przestępstw, które godzą w bezpieczeństwo państwa i uzasadniają stosowanie kontroli operacyjnej przez ABW. Skoro tego nie uczynił ustawodawca, naruszając przy tym – w mojej ocenie – Konstytucję, będą o tym rozstrzygać w indywidualnych sprawach organy stosujące prawo. Nie ma zatem gwarancji, że kontrola operacyjna będzie zarządzana jedynie w celu zapobiegania lub ścigania poważnych przestępstw.

11. Brak powiązania konkretnych typów przestępstw z podstawą do zarządzenia kontroli operacyjnej ogranicza sądową kontrolę konstytucyjności prawa. Trybunał nie może, co do zasady, badać sposobu stosowania przepisów. Istnieje zatem ryzyko, że umożliwienia kontroli operacyjnej przy ściganiu tego czy innego przestępstwa Trybunał nie mógłby badać nawet wówczas, gdyby oczywiste było, że danego przestępstwa nie

można zaliczyć do poważnych. Innymi słowy, mamy do czynienia ze swego rodzaju błędnym kołem. Trybunał uznał obecnie zakwestionowane unormowania za konstytucyjne, zakładając ich poprawne stosowanie przez organy państwa. Jeśli jednak nie będą stosowane zgodnie z tym, czego wymaga Konstytucja, Trybunał odmówi zbadania ich konstytucyjności, uznając tego rodzaju zarzuty za dotyczące sposobu stosowania prawa.

12. W orzecznictwie ETPC ugruntowany jest pogląd o konieczności określenia przez prawo „natury przestępstw", jeśli ich ściganie uprawnia do niejawnego pozyskiwania informacji o osobach. Tego wymogu nie spełnia, w mojej ocenie, wyrażenie „przestępstw godzących w bezpieczeństwo państwa". Nawet jeśli uznać, że ustawodawca określił w art. 5 ust. 1 pkt 2 lit. a ustawy o ABW naturę przestępstw przez dobro prawnie chronione, jakim jest bezpieczeństwo państwa, to tak określony zakres przedmiotowy kontroli operacyjnej jest zbyt szeroki.

Jak przyjął ETPC w orzeczeniu w sprawie Iordachi i inni przeciwko Mołdawii, nr skargi 25198/02, mołdawskie przepisy umożliwiały stosowanie podsłuchu m.in. w celu zapobiegania poważnym, bardzo poważnym i wyjątkowo poważnym przestępstwom, a zatem przestępstwom zagrożonym w świetle tamtejszego prawa karą pozbawienia wolności do 15 lat lub surowszą. Oznaczało to, że zarządzenie podsłuchu było możliwe w wypadku aż ok. 60% przestępstw stypizowanych w ustawie karnej. Prawodawstwo nie precyzowało też przesłanek zarządzenia kontroli rozmów, jakimi były wówczas „bezpieczeństwo narodowe", „porządek publiczny", „ochrona zdrowia", „ochrona moralności", „ochrona praw i interesów innych osób", „interes gospodarczy kraju", „utrzymanie porządku prawnego" (§ 46 uzasadnienia wyroku w sprawie Iordachi i inni przeciwko Mołdawii). Europejski Trybunał Praw Człowieka uznał w związku z tym takie rozwiązanie za niewystarczające z punktu widzenia „jakości regulacji prawnej ingerencji", wymaganej przez art. 8 Konwencji.

W mojej ocenie, z analogiczną sytuacją mamy do czynienia na gruncie ustawy o ABW. Trybunał powinien był więc ocenić, czy daje się ustalić zamknięty katalog przestępstw uznanych za „godzące w bezpieczeństwo państwa". Potem należało stwierdzić, czy mieszczą się w nim tylko i wyłącznie takie przestępstwa, których stopień szkodliwości uzasadnia ingerencję w wolności i prawa człowieka w trybie kontroli operacyjnej. Tego jednak nie uczynił.

Mając powyższe na uwadze, uznaję, że zakwestionowany przepis narusza również art. 8 Konwencji, ze wszystkimi wynikającymi z tego konsekwencjami dla ewentualnej skargi indywidualnej do Europejskiego Trybunału Praw Człowieka.

13. Trybunał Konstytucyjny oparł orzeczenie na założeniu dokonywania poprawnej interpretacji przepisów przez sąd. Jak podkreślono w raporcie Wysokiego Komisarza ONZ do spraw Praw Człowieka na temat ochrony prywatności w dobie cyfrowej, niejawne regulacje czy niejawna dla społeczeństwa interpretacja prawa – nawet dokonywana przez sądy – nie pozwalają uznać, że prawo regulujące kontrolę operacyjną spełnia wymagania jakościowe i w sposób odpowiedni określa okoliczności, w jakich dopuszczalne jest niejawne pozyskiwanie informacji (zob. *The right to privacy in the digital age*. *Repport of the Office of the United Nations High Commissioner for Human Rights*, 30 czerwca 2014 r., pkt 29).

W konsekwencji uważam orzeczenie Trybunału co do zakwestionowanego przepisu – w sytuacji braku wymaganej precyzji oraz niejawności rozstrzygnięć sądowych dotyczących zarządzenia na jego podstawie kontroli operacyjnej – za pozostające w opozycji do wymagań stawianych w systemie ochrony praw człowieka Narodów Zjednoczonych, a zwłaszcza przez art. 17 Międzynarodowego Paktu Praw Obywatelskich i

Politycznych, otwartego do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).

Z powyższych powodów uznałem za konieczne złożenie zdania odrębnego.

Zdanie odrębne
sędziego TK Mirosława Granata
do uzasadnienia wyroku Trybunału Konstytucyjnego
z dnia 30 lipca 2014 r., sygn. akt K 23/11

Trybunał Konstytucyjny, wypowiadając się o prywatności jednostki w kontekście prowadzenia kontroli operacyjnej przez służby i organy policyjne, spłycił problem wolności człowieka z art. 31 Konstytucji. Nie zrekonstruował w pełni wolności jednostki na gruncie tego przepisu. W konsekwencji, nie sprecyzował miary, za pomocą której rozstrzyga spory o wolność. Relacja między „wolnością człowieka a ochroną bezpieczeństwa państwa i porządku publicznego w erze cyfrowej" (część III pkt 1 uzasadnienia), która w rozstrzyganej sprawie jest kluczowa, stała się przez to niejasna.

1. Wolność wedle Trybunału jest rekonstrukcją art. 31 ust. 2 Konstytucji. Każda jednostka ma pole swobody (wolność pozytywna), w której nikt nie może jej niczego nakazać (wolność negatywna) [s. 71]. Obie wolności, według Trybunału, to dwie strony jednej i tej samej sytuacji. Są powiązane logicznie i jedna nie może istnieć bez drugiej. Wolność jest „pozytywna" (patrząc od strony tego komu przysługuje) i zarazem „negatywna" (od strony tego kto musi się powstrzymać od ingerencji). Są to, jak określa Trybunał, „aspekty wolności".

Podejście TK prezentowane w uzasadnieniu rodzi paradoksy wyrażania wolności. Pokazuje to część III, pkt 1 uzasadnienia. Jak twierdzi Trybunał, można w całości odstąpić od respektowania „aspektu negatywnego" wolności konstytucyjnych, na określonych warunkach, przewidzianych w ust. 3 art. 31 Konstytucji [s. 71]. Jeśli możliwe jest na gruncie Konstytucji odstąpienie od respektowania wolności, którą Trybunał nazywa „wolnością negatywną", to takie podejście, moim zdaniem, zamazuje sens wolności. Jest to myśl, która wywołuje mój sprzeciw. Oznacza bowiem rodzaj wydrążenia wolności z treści, jaką ma być tutaj pole swobody człowieka. Wydaje się, że paradoksów „pozytywno-negatywnego" wyjaśniania wolności można byłoby pokazać tu więcej.

2. Twierdzę, że podejście Trybunału nie rekonstruuje pełnego sensu wolności z art. 31 Konstytucji. Wspomniana „dwustronność" wolności nie wystarcza dla opisania całości wolności w tym przepisie. Nie sięga rdzenia wolności. Wolność „w pozytywno-negatywnym" ujęciu TK koncentruje się jedynie na sferze braku nakazów wobec jednostki (ust. 2 art. 31), pomija zaś sferę zakazów wobec niej (ust. 3 art. 31). Między wolnością w znaczeniu negatywnym a wolnością w znaczeniu pozytywnym nie ma przejścia, które miałoby charakter bezpośredni (o czym piszę niżej).

W trybunalskim pojęciu wolności brakuje przede wszystkim odniesienia do art. 31 ust. 3 Konstytucji, w którym występuje kategoria korzystania z wolności, i która byłaby składnikiem tej wolności. W rozumowaniu TK, klauzule ograniczające z art. 31 ust. 3 Konstytucji są zewnętrznym naddatkiem wobec *aspektów wolności* jakie się wyróżnia.

Wedle Trybunału, dopiero jednoznaczna regulacja ustawowa może nakładać ograniczenia w zakresie podejmowania określonych zachowań mieszczących się w ramach konkretnej wolności [s. 72]. Moim zdaniem, „korzystanie z wolności" z art. 31 ust. 3 mieści się zaś w samej istocie wolności i jest niezbędne dla jej wyjaśnienia. Sądzę, że przesłanki z art. 31 ust. 3 Konstytucji są integralnym składnikiem wolności człowieka. Art. 31 nie należy odczytywać w taki sposób, że mamy do czynienia z sytuacją, w której „jest wolność" i z sytuacją, w której ma miejsce „korzystanie z wolności". Taka jego interpretacja umożliwiłaby skrajne manipulowanie wolnością. Na gruncie wspomnianego przepisu jest inaczej. W samej wolności mieści się korzystanie z wolności.

3. Pojęcie wolności w Konstytucji jest bogatsze, aniżeli „pozytywno-negatywne" jej rozumienie prezentowane przez TK. Wolność w Konstytucji obejmuje pole swobody człowieka i możliwość korzystania z tego pola. Jest iloczynem swobody człowieka oraz możności (umiejętności, kompetencji) korzystania z niej. W istocie, jest zaś tak, że to nasze możliwości wyznaczają pole korzystania z wolności. Zatem, w wolności wyróżniam swobodę, czyli możliwość kształtowania naszego postępowania i życia (ust. 2 art. 31) i zdolność lub umiejętność korzystania z tej swobody (ust. 3 art. 31). Stąd, przesłanki z ust. 3 pozostają integralnymi składnikami wolności człowieka. W samym braku nakazów co do wolności (o czym stanowi ust. 2) nie zawiera się jeszcze brak zakazów co do korzystania z wolności (o czym stanowi ust. 3). Dopiero te dwie wypadkowe razem, tj. brak nakazów co do postępowania jednostki, o czym stanowi ust. 2 art. 31 oraz możliwość wprowadzenia zakazów (ograniczeń) z ust. 3 art. 31, określają pole naszej swobody, którą rozumiem jako wolność na gruncie Konstytucji. Jej treść można zatem wyrazić w ten sposób, że nic nie jest nam nakazywane, ale pewnych rzeczy nie można robić. „Nie nakazywać ludziom, a zakazywać tylko w określonych sytuacjach", tak wydaje się brzmieć kwintesencja wolności konstytucyjnej. Cechą takiego odczytania przepisów Konstytucji o wolności jest to, iż obejmuje sobą cały art. 31, i wciąga ust. 3 do pojmowania wolności. „Ograniczenia w zakresie korzystania z wolności" (ust. 3) nie są czymś zewnętrznym wobec wolności, ale tkwią w niej samej. Doskonale wiemy, że kluczowe spory o wolność, jakie toczą się przed TK i przed innymi sądami konstytucyjnymi, dotyczą właśnie sfery zakazów i ograniczeń (np. sprawa zakazu uboju rytualnego albo sprawy dotyczące zakazu przerywania ciąży). Art. 31 Konstytucji w całości oznacza więc, iż człowiek ma pole swobody i zarazem, że potrafi z niej korzystać.

Sądzę, że zaletą takiego ujęcia wolności jest to, iż jest ono „operacyjne", tj. może służyć sędziemu do tego aby rozsądzać różne problemy dotyczące wolności. Jest bowiem wręcz oczywiste, że pole swobody jednostki (ust. 2 art. 31) i możliwość korzystania z niej (ust. 3 art. 31), muszą być korelowane ze sobą. Trybunał Konstytucyjny w rozstrzyganiu problemu wyznaczenia granic inwigilacji obywateli powinien sprecyzować miarę, za pomocą której waży wolność jednostki. Moim zdaniem, miarą tą posługujemy się dopasowując pole swobody jednostki, które musi być maksymalnie szerokie (co wynika z ust. 2 art. 31) do pola korzystania przez nią z wolności (co wynika z ust. 3 art. 31). W tym ujęciu, „bezpieczeństwo lub porządek publiczny", „zdrowie" „moralność publiczna" albo „wolności i prawa innych osób" znajdują się w zakresie pola swobody jednostki. Służą wówczas do wyważania ograniczeń i zakazów wolności od strony jednostki i jej wolności. Trybunał nie stawia właściwie problemu narzędzia, jakim mierzy wolność i jej ograniczenia. Podkreśla „szerszy wymiar" obowiązku organów państwa gwarantowania wolności i prawa, itd. [s. 78]. Trybunał akcentuje obowiązek stworzenia przez państwo warunków faktycznych, w których obywatele z zagwarantowanych im wolności i praw mogą swobodnie korzystać. Warunkiem zapewnienia wolności i praw ma być poczucie bezpieczeństwa w państwie i brak zagrożeń dla obywateli [*tamże*]. Zapewne nie sposób

zaprzeczyć tym twierdzeniom. Natomiast nie jest jasne, jak przekładają się one na zapowiedź Trybunału [s. 79] wypracowania podejścia do oceny proporcjonalności badanych przepisów, która miałaby się cechować „zróżnicowaniem" [*tamże*].

4. Trybunał posługując się na gruncie Konstytucji dwoma „aspektami wolności", używa terminologii dotyczącej wolności w sposób, który odchodzi od nazewnictwa klasycznego. Kwestia terminologii jest tu rzecz jasna sprawą drugorzędną. Nie chcę na niej skupiać uwagi, aczkolwiek za nazwami, tak czy inaczej używanymi, kryje się zwykle problem dotarcia do istoty sprawy. Zwrócę jedynie uwagę, że TK, na przekór doktrynie klasycznej, pole swobody człowieka określa mianem wolności pozytywnej. Swoboda ta, od czasów J.S. Milla lub I. Berlina (por. *Dwie koncepcje wolności*, Warszawa 1991, s. 114) nazywana jest „wolnością negatywną" (nie zaś „pozytywną"). Podkreślam jednak raz jeszcze, że nie o terminologię tu chodzi.

Gdy mówimy o „wolności negatywnej" i „wolności pozytywnej", to wypowiadamy się o różnych wolnościach. Pod tym rozróżnieniem nie kryją się trybunalskie „aspekty" wolności. Od wskazanej wyżej wolności (wolności negatywnej) odrębna jest wolność pozytywna. Wolność w znaczeniu pozytywnym odpowiada na inne pytanie aniżeli wolność negatywna. Sprowadza się ona do tego, jaki jest wpływ państwa i jego organów na jednostkę i jej postępowanie (kto mną rządzi). Oznacza z reguły ukierunkowanie przez władzę państwową tego, jak człowiek powinien według niej postępować lub zachowywać się. Władza często bowiem chce ludzi uczyć wolności. Wydaje się, że miał rację J. S. Mill, zauważając, iż niekiedy demokracja może bardziej zamachnąć się na wolność człowieka, niż totalitaryzm. Odróżnianie od siebie obu tych koncepcji wolności sięga istoty mówienia o wolności.

5. Ustalenia trybunalskie dotyczące rozumienia konstytucyjnej wolności człowieka mają fundamentalne znaczenie. Z jednej strony, większość spraw, jakie zawisły przed Trybunałem Konstytucyjnym, są sprawami o wolność i jej rozumienie. Ewentualnie dają się łatwo przeformułować jako spory o wolność lub ściślej, jako spory o pole korzystania z wolności. Z drugiej strony, wolność wydaje się nam tak oczywista, że podkładamy pod nią różne wyjaśnienia i treści. Dlatego dostrzeżonej wątpliwości co do rozumienia wolności w art. 31 Konstytucji, nie sposób było nie zasygnalizować.