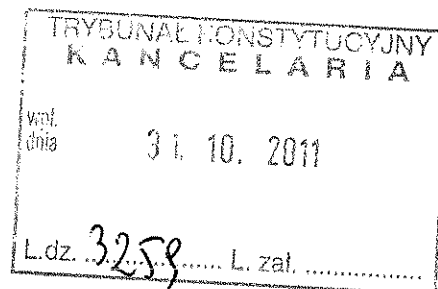




RZECZPOSPOLITA POLSKA
PROKURATOR GENERALNY

Warszawa, dnia 28 października 2011 r.

PG VIII TK 62/11
(K 23/11)



TRYBUNAŁ KONSTYTUCYJNY

W związku z wnioskami Rzecznika Praw Obywatelskich z dnia 25 czerwca 2011 r. oraz z dnia 1 sierpnia 2011 r. o stwierdzenie niezgodności przepisów:

I.

- 1) art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- 2) 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 ze zmianami),
- 3) 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 ze zmianami),
- 4) art. 31 ust. 7 pkt 3 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),

- 5) art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
- 6) art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
- 7) art. 31 ust. 4 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)

- z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej;

II.

- 1) art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- 2) art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675 ze zmianami),
- 3) 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 zmianami),
- 4) art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),
- 5) art. 28 ust. 1 pkt 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
- 6) art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),

7) art. 32 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)

- z art. 49 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (Dz. U. z 1993 r. Nr 61, poz. 284);

III.

- 1) art. 36b ust. 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214 ze zmianami),
- 2) art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
- 3) art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
- 4) art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)

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 zmianami), 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 Rzeczypospolitej Polskiej

– na podstawie art. 33 w związku z art. 27 pkt 5 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643 ze zmianami) –

przedstawiam następujące stanowisko:

I.:

- 1) art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 ze zmianami),
- 2) 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 ze zmianami),
- 3) 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 ze zmianami),
- 4) art. 31 ust. 7 pkt 3 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zmianami),
- 5) art. 27 ust. 6 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zmianami),
- 6) art. 17 ust. 5 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zmianami),
- 7) art. 31 ust. 4 pkt 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zmianami)

- są niezgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej;

II.:

- 1) art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji,
- 2) art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej,
- 3) art. 36b ust. 1 pkt 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej,
- 4) art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- 5) art. 28 ust. 1 pkt 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- 6) art. 18 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,
- 7) art. 32 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego

- są niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (Dz. U. z 1993 r. Nr 61, poz. 284);

III.:

- 1) art. 36b ust. 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej,
- 2) art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- 3) art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,
- 4) art. 32 ustawy z dnia 9 czerwca 2006 r. 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 zmianami), 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 Rzeczypospolitej Polskiej.

UZASADNIENIE

W dniach: 25 czerwca 2011 r. oraz 1 sierpnia 2011 r. Rzecznik Praw Obywatelskich wystąpił do Trybunału Konstytucyjnego z dwoma wnioskami o zbadanie zgodności wymienionych przepisów ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawy o Centralnym Biurze Antykorupcyjnym, jak również ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego z szeregiem wzorców kontroli zawartych w Konstytucji RP oraz w Konwencji o ochronie praw człowieka i podstawowych wolności.

Zarządzeniem Prezesa Trybunału Konstytucyjnego oba wnioski zostały połączone celem ich łącznego rozpoznania – z uwagi na tożsamość przedmiotu sprawy.

Skierowanie do Trybunału Konstytucyjnego wspomnianych wyżej wniosków nastąpiło w wyniku wystąpienia do Rzecznika Praw Obywatelskich Helsińskiej Fundacji Praw Człowieka w sprawie stosowania przez poszczególne służby mundurowe oraz specjalne kontroli operacyjnej, jak również własnej analizy przez Rzecznika przepisów normujących ową kontrolę, w tym

dotyczących pozyskiwania przez służby informacji objętych tajemnicą komunikowania się.

Zdaniem Wnioskodawcy, przepisy: art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym, jak również art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego godzą w art. 2 oraz art. 47 w związku z art. 31 ust. 3 Konstytucji RP, nie wskazując, jakich konkretnie środków mogą używać poszczególne służby podczas stosowania kontroli operacyjnej oraz jakie konkretnie informacje mogą te służby pozyskiwać. Tym samym, ustawodawca dopuścił stosowanie przez służby podczas kontroli operacyjnej wszelkich dostępnych, w tym bliżej niezidentyfikowanych, środków technicznych, w celu pozyskania każdego dowodu i każdej informacji o jednostce, bez żadnych ustawowych ograniczeń w omawianym zakresie.

Rzecznik Praw Obywatelskich podniósł również, że zakwestionowane unormowania, z analogicznych przyczyn, ingerują także w inne prawa i wolności jednostki (których w *petitum* wniosku nie wymieniono), takie jak nienaruszalność mieszkania (art. 50 Konstytucji RP), wolność poruszania się (art. 52 ustawy zasadniczej), autonomię informacyjną jednostki (art. 51 Konstytucji RP), jak również odwołują się do takich kategorii, jak „treści rozmów telefonicznych” oraz „informacje przekazywane za pomocą sieci telekomunikacyjnej” czy też „obraz”, a więc do pojęć pozostających w ścisłym związku z wolnością i ochroną tajemnicy komunikowania się (art. 49 ustawy zasadniczej).

Uzasadnienie analizowanego wniosku zawiera pogląd, że zaskarżone przepisy naruszają zasadę demokratycznego państwa prawnego (art. 2 ustawy

zasadniczej, wskazany w *petitum* wniosku), godząc w zaufanie obywateli do państwa i do tworzonego przez to państwo prawa, poprzez brak precyzji i niedookreśloność regulacji mających wyznaczać granice ingerencji w prawa i wolności jednostki. Z tych samych powodów, wspomniane przepisy kolidują z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (którego to wzorca kontroli w *petitum* wniosku jednak nie wymieniono).

Zgodnie ze stanowiskiem Rzecznika Praw Obywatelskich, przepisy: art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW, art. 18 ust. 1 pkt 1 ustawy o CBA, jak również art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW godzą w art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, pomijając wymóg subsydiarności pozyskiwania danych telekomunikacyjnych i dopuszczając zarządzenie pozyskania tych danych nie tylko, gdy inne środki pozyskania informacji okazały się bezskuteczne albo gdy zachodzi wysokie prawdopodobieństwo ich nieskuteczności, ale również w każdej innej sytuacji, kiedy tylko stosowne służby zwrócą się do podmiotów prowadzących działalność telekomunikacyjną o udostępnienie takich danych.

Wnioskodawca wyraził ponadto pogląd, że zakwestionowane wyżej przepisy są niezgodne z powołanymi wzorcami kontroli również z tego powodu, iż ustawodawca nie wyłączył żadnej kategorii użytkowników z kręgu podmiotów, których dane mogą być pozyskiwane przez służby w omawianym trybie, choć dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską.

Zdaniem Rzecznika Praw Obywatelskich, zakwestionowane przez Niego przepisy naruszają wolność komunikowania się, zezwalając służbom na pozyskiwanie danych telekomunikacyjnych bez uzyskania zgody sądu na

wkroczenie w tę sferę wolności konstytucyjnych i konwencyjnych jednostki, jak również nie przewidując kontroli korzystania przez służby z omawianych uprawnień sprawowanej przez sąd ani przez jakikolwiek inny organ zewnętrzny. Konstatacji o braku kontroli sądowej (zarówno uprzedniej, jak i następczej) pozyskiwania przez służby danych telekomunikacyjnych nie towarzyszy jednak propozycja podjęcia kontroli omawianych przepisów w kontekście wzorca zawartego w art. 45 ust. 1 Konstytucji RP.

Zgodnie ze stanowiskiem Rzecznika Praw Obywatelskich, omawiane regulacje naruszają wspomniane prawa i wolności jednostki, pozostawiając służbom możliwość pozyskiwania danych telekomunikacyjnych poza jakąkolwiek kontrolą, a nawet wiedzą samego zainteresowanego (choćby odsuniętą w czasie na okres po zakończeniu postępowania, jak ma to miejsce w toku procesu karnego).

Wnioskodawca podniósł również, iż wymienione wyżej unormowania kolidują ze wskazanymi przepisami Konstytucji RP oraz Konwencji o ochronie praw człowieka i podstawowych wolności, nie regulują bowiem w sposób precyzyjny celu pozyskiwania danych telekomunikacyjnych, odwołując się jedynie do zakresu zadań poszczególnych służb bądź ogólnego stwierdzenia, iż dane te są pozyskiwane w celu zapobiegania lub wykrywania przestępstw.

Nadto, uzasadnienie analizowanego wniosku zawiera pogląd, że przepisy: art. 36b ust. 5 ustawy o kontroli skarbowej, art. 28 ustawy o ABW oraz AW, art. 18 ustawy o CBA, jak również art. 32 ustawy o SKW oraz SWW, w zakresie, w jakim – 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, godzą w art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP, upoważniając służby do pozyskiwania, gromadzenia i udostępniania informacji o obywatelach innych niż niezbędne w demokratycznym państwie prawnym.

Ocena poglądów prawnych oraz zarzutów, przedstawionych przez Rzecznika Praw Obywatelskich w omawianych wnioskach, jest następująca.

I.

Przed przystąpieniem do analizy zakwestionowanych przez Wnioskodawcę przepisów ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawy o Centralnym Biurze Antykorupcyjnym, jak również ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, należałoby, jak się wydaje, zasygnalizować, w jakich sytuacjach poszczególne służby mogą podejmować kontrolę operacyjną.

Policja może podejmować taką kontrolę przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: przeciwko życiu i zdrowiu, określonych w art. 148 – 150 Kodeksu karnego, określonych w art. 134, art. 135 § 1, art. 136 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 211a, art. 223, art. 228 § 1 i 3 – 5, art. 229 § 1 i 3 – 5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1 – 3, art. 258, art. 269, art. 280 – 282, art. 285 § 1, art. 286 § 1, art. 196 § 1 – 3, art. 296a § 1, 2 i 4, art. 299 § 1 – 6 oraz art. 310 § 1, 2 i 4 Kodeksu karnego, określonych w art. 46 ust. 1, 2 i 4, art. 47 oraz art. 48 ust. 1 i 2 ustawy o sporcie, przeciwko obrotowi gospodarczemu, określonych w art. 297 – 306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów, skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają

pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów, skarbowych, o których mowa w art. 107 § 1 Kodeksu karnego skarbowego, nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi, określonych w art. 8 ustawy – Przepisy wprowadzające Kodeks karny, określonych w art. 43 – 46 ustawy o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, jak również ściganych na mocy umów i porozumień międzynarodowych (art. 19 ust. 1 ustawy o Policji).

Straż Graniczna może podejmować kontrolę operacyjną przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: określonych w art. 163 § 1, art. 164 § 1, art. 165 § 1, art. 166 § 1 i 2, art. 167, art. 168, art. 171, art. 172, art. 173 § 1, art. 258, art. 264 § 2 i 3 oraz art. 299 § 1 Kodeksu karnego, określonych w art. 270 – 275 Kodeksu karnego w zakresie dokumentów uprawniających do przekraczania granicy państwowej, skarbowych, o których mowa w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów, pozostających w związku z przekroczeniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczenia znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz materiałach wybuchowych, a także o przeciwdziałaniu narkomanii, określonego w art. 147 ustawy o cudzoziemcach, określonych w art. 228, 229 i 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej

w związku z wykonywaniem obowiązków służbowych, określonych w art. 229 Kodeksu karnego, popełnionych przez osoby niebędące funkcjonariuszami lub pracownikami Straży Granicznej w związku z wykonywaniem czynności służbowych przez funkcjonariuszy lub pracowników Straży Granicznej, jak również ściganych na mocy umów międzynarodowych (art. 9e ust. 1 ustawy o Straży Granicznej).

Wywiad skarbowy może podejmować kontrolę operacyjną w ramach czynności operacyjno – rozpoznawczych, w celu wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów przestępstw: skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów, skarbowych, o których mowa w art. 107 Kodeksu karnego skarbowego, przeciwko obrotowi gospodarczemu, powodujących szkodę majątkową, jeżeli wysokość szkody przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę, określonego na podstawie odrębnych przepisów, przeciwko mieniu, jeżeli wartość mienia przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów, przyjmowania lub wręczania korzyści majątkowej w związku z pełnioną funkcją publiczną lub funkcją związaną ze szczególną odpowiedzialnością, jak również ściganych na mocy umów i porozumień międzynarodowych (art. 36c ust. 1 ustawy o kontroli skarbowej).

Żandarmeria Wojskowa może podejmować kontrolą operacyjną przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: przeciwko pokojowi i ludzkości, przeciwko Rzeczypospolitej Polskiej, z wyjątkiem przestępstw

określonych w art. 127 – 132 Kodeksu karnego, zamachu na jednostki i komórki organizacyjne Sił Zbrojnych, zabójstwa, uprowadzenia statku powietrznego lub wodnego, użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym, przyjęcia lub udzielenia korzyści majątkowej lub jej obietnicy w związku z pełnieniem funkcji publicznej, uprowadzenia osoby, handlu ludźmi, wymuszenia okupu, udziału w zorganizowanej grupie przestępczej, nielegalnego wyrabiania, posiadania lub handlu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub psychotropowymi albo materiałami jądrowymi lub substancjami trującymi, bezprawnego ujawnienia lub wykorzystania informacji niejawnych o klauzuli tajności „tajne” i „ściśle tajne”, rozboju i kradzieży rozbójniczej, dezercji z bronią lub dezercji wspólnie z innymi żołnierzami, zaboru środków walki, jak również przestępstw ściganych na mocy umów i porozumień międzynarodowych (art. 31 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych).

Agencja Bezpieczeństwa Wewnętrznego może podejmować kontrolę operacyjną przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2 (art. 27 ust. 1 ustawy o ABW oraz AW). Do zadań ABW, o których mowa we wspomnianym wyżej przepisie, należy: rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, bezprawnego ujawniania lub wykorzystywania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa, godzących w podstawy ekonomiczne państwa, korupcji osób pełniących funkcje publiczne, jeśli może to godzić w bezpieczeństwo państwa; w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców.

Centralne Biuro Antykorupcyjne może podejmować kontrolę operacyjną przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu rozpoznawania, zapobiegania i wykrywania przestępstw, a także uzyskania i utrwalenia dowodów przestępstw: określonych w art. 228 – 231, 250a, 258, 286, 296 – 297, 299, 310 § 1, 2 i 4 Kodeksu karnego oraz skarbowych przeciwko obowiązkowi podatkowemu i rozliczeniom z tytułu dotacji i subwencji, określonych w rozdziale 6 Kodeksu karnego skarbowego, jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa i jeżeli wartość przedmiotu czynu lub uszczuplenia należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie przepisów ustawy o minimalnym wynagrodzeniu za pracę (art. 17 ust. 1 w związku z art. 2 ust. 1 pkt 1 lit. d ustawy o CBA).

Służba Kontrwywiadu Wojskowego może podejmować kontrolę operacyjną przy wykonywaniu czynności operacyjno – rozpoznawczych, w celu realizacji zadań określonych w art. 5 (art. 31 ust. 1 ustawy o SKW oraz SWW). Do zadań, o których mowa we wspomnianym wyżej przepisie, należy: rozpoznawanie, zapobieganie oraz wykrywanie popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych RP i innych jednostek organizacyjnych MON, przestępstw: przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w rozdziale XVI Kodeksu karnego, a także innych ustawach i umowach międzynarodowych, przeciwko Rzeczypospolitej Polskiej określonych w rozdziale XVII Kodeksu karnego oraz takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność, określonych w art. 140 Kodeksu karnego, określonych w art. 228 – 230 Kodeksu karnego, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej Sił Zbrojnych RP lub innych jednostek organizacyjnych MON, przeciwko ochronie informacji określonych w rozdziale XXXIII Kodeksu

karnego, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej Sił Zbrojnych RP lub innych jednostek organizacyjnych MON, a także takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność, określonych w art. 33 ustawy o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa, jak również przestępstw związanych z działalnością terrorystyczną oraz innych niż wymienione wyżej, godzących w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność; współdziałanie z Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania wymienionych wyżej przestępstw; realizowanie, w granicach swojej właściwości, zadań określonych w przepisach ustawy o ochronie informacji niejawnych; uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych RP lub innych jednostek organizacyjnych MON oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń; prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy; uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia; ochrona bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa; ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez Siły Zbrojne RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez Siły Zbrojne i inne jednostki organizacyjne MON, podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana.

Analiza przytoczonych wyżej katalogów sytuacji, w których poszczególne służby mundurowe oraz specjalne mogą podejmować kontrolę operacyjną, wskazuje, że katalogi te obejmują łącznie blisko 200 pozycji. Nadto, wypada odnotować, że zakres sytuacji, w których służbom przyznano uprawnienia do podejmowania tego rodzaju czynności operacyjno – rozpoznawczych, z biegiem czasu ulega sukcesywnemu poszerzaniu przez ustawodawcę. Ustawy normujące działalność poszczególnych służb przewidują podejmowanie przez te służby kontroli operacyjnej nie tylko w celu zapobieżenia, wykrycia, ustalenia sprawców czy uzyskania i utrwalenia dowodów określonych przestępstw, ale również w wypadkach prowadzenia przez służby działań kontrolnych, planistycznych bądź analitycznych (jak w przypadku SKW). W końcu, wymagałoby podkreślenia, że wszystkie omawiane katalogi mają charakter otwarty, odwołując się, w omawianym zakresie, do zobowiązań Polski wynikających z umów i porozumień międzynarodowych (a w przypadku Służby Kontrwywiadu Wojskowego także z bliżej nieokreślonych, innych niż ustawa o SKW oraz SWW, aktów normatywnych rangi ustawy).

Tak szerokie zakreślenie ram, w których poszczególne służby uzyskały możliwość wkraczania w sferę konstytucyjnie chronionych wolności i praw jednostki, niewątpliwie nakłada na ustawodawcę obowiązek szczególnie precyzyjnego określenia procedur stosowania kontroli operacyjnej, w tym, jak się wydaje, zapewnienia osobom poddawanych takiej kontroli niezbędnych gwarancji, powstrzymujących służby przed nadmiernym lub nieuprawnionym naruszaniem tychże wolności i praw.

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 19 ust. 6 pkt 3 ustawy o Policji ma następujące brzmienie:

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

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

Objęty wnioskiem Rzecznika Praw Obywatelskich przepis art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej ma następującą treść:

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

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

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej ma następujące brzmienie:

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

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

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

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

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

Objęty wnioskiem Rzecznika Praw Obywatelskich przepis art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu ma poniższą treść:

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

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

Zakwestionowany przepis art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym brzmi następująco:

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

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

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ma następujące brzmienie:

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

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

Wstępna analiza brzmienia przytoczonych wyżej przepisów wskazuje, że – nie licząc drobnych zmian stylistycznych – różnią się one merytorycznie jedynie w zakresie dotyczącym Straży Granicznej, Żandarmerii Wojskowej

i wywiadu skarbowego, opis środków technicznych, umożliwiających uzyskanie przez te trzy służby informacji i dowodów, obejmuje bowiem również „obraz”, podczas gdy w pozostałych przepisach mowa jedynie o „treści rozmów telefonicznych” oraz o „innych informacjach przekazywanych za pomocą sieci telekomunikacyjnych” („przez sieci telekomunikacyjne”).

Przechodząc do oceny kwestionowanych przez Wnioskodawcę przepisów w kontekście powołanych w *petitum* wniosku wzorców kontroli, należy odnotować, że, zgodnie z art. 2 ustawy zasadniczej, Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej. Z kolei, art. 47 Konstytucji RP stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W końcu, art. 31 ust. 3 Konstytucji RP stanowi, że ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia moralności publicznej, albo wolności i praw innych osób, a ograniczenia te nie mogą naruszać istoty wolności i praw.

Nadto, jak się wydaje, nie można w tym miejscu pominąć wzorca kontroli przywołanego przez Rzecznika Praw Obywatelskich w uzasadnieniu wniosku, a zawartego w art. 49 ustawy zasadniczej. Zgodnie ze wspomnianym unormowaniem Konstytucji RP, zapewnia się wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

W doktrynie przyjmuje się, że wolność komunikowania się, ze swej istoty, jako porozumiewanie się określonych osób, związana jest z poufnością, co tradycyjnie obejmuje się określeniem „tajemnica”. Polega ona zarówno na zakazie zmuszania adresatów do ujawniania treści otrzymywanych przekazów,

jak i na zakazie, adresowanym do wszystkich innych podmiotów, łącznie z organami władzy publicznej, podejmowania prób poinformowania się o tych treściach bez zgody adresata. Co więcej, obejmuje również poufność co do faktu, że jest się w ogóle adresatem określonych przekazów. Jako wolność o charakterze osobistym, także ona potwierdza w szczególny sposób godność osoby ludzkiej. Również na adresatach korespondencji, w wielu sytuacjach, spoczywać będzie obowiązek zachowania poufności, zwłaszcza gdyby ujawnienie treści tej korespondencji stanowiło naruszenie prawnie chronionych interesów nadawców, a w szczególności ich prawa do prywatności (por. Paweł Sarnecki, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Tom III, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 49, s. 3).

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

W nauce prawa konstytucyjnego podkreśla się również wymóg kompletności ustawowej regulacji ograniczeń praw jednostki. Nakaz kompletności unormowania ustawowego wymaga, aby ustawa samodzielnie określała wszystkie podstawowe elementy ograniczenia danego prawa i wolności (kompletny zarys ograniczenia), bez przekazywania swobody w tym

zakresie organom administracji rządowej i samorządowej (por. Jerzy Oniszczyk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Zakamycze 2004, s. 419).

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, doniosłość prawa do prywatności (art. 47 Konstytucji) w systemie konstytucyjnej ochrony praw i wolności uwidacznia m. in. okoliczność, że prawo to jest – zgodnie z art. 233 ust. 1 Konstytucji – nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanie wojennym i wyjątkowym. Oznacza to, że nawet warunki tak wyjątkowe i ekstremalne nie zezwalają ustawodawcy na złagodzenie przesłanek, przy spełnieniu których można wkroczyć w sferę życia prywatnego nie narażając się na zarzut niekonstytucyjnej arbitralności (por. wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, OTK ZU Nr 6/A/2005, poz. 64, s. 813 oraz powołane tam orzecznictwo). Przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe – art. 49 Konstytucji (*vide – ibidem*).

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

W szczególności, Trybunał Konstytucyjny, delegalizując między innymi niektóre regulacje zawarte w art. 19 ustawy o Policji, podkreślił, iż „doświadczenia współczesnych państw demokratycznych wskazują, że władza wykonawcza odpowiedzialna za bezpieczeństwo i porządek publiczny, w tym podległe jej podmioty prowadzące czynności operacyjno – rozpoznawcze, dysponują środkami, których zastosowanie – w imię obrony porządku

publicznego – może doprowadzić do zniszczenia instytucji demokratycznych i redukcji praw obywatelskich. Dzieje się tak zarówno dlatego, że poufność i brak zewnętrznej kontroli może prowadzić do nadmiernej autonomizacji czy subiektywizacji samego celu działalności operacyjnej oraz niezachowania w niej należytej wstrzemięźliwości przy wkraczaniu w prawa i wolności obywatelskie. Niekiedy zaś sytuacja taka może wynikać z nadmiernie eksponowanych względów ideologicznych czy politycznych w działaniu egzekutywy. Inaczej mówiąc, cecha niejawności kontroli operacyjnej czyni ją podatną na nadużycia. Bezpieczeństwo publiczne, jako dobro co do zasady usprawiedliwiające ograniczenie przez legislatora korzystania z wolności obywatelskich, wymaga więc zachowania proporcjonalności dopuszczalnego wkroczenia w imię ochrony bezpieczeństwa oraz sprawnego systemu kontroli zachowania tej proporcjonalności w praktyce. W przeciwnym razie środki ochrony tego bezpieczeństwa, w postaci legalnie dopuszczalnej działalności operacyjnej, same w sobie stwarzają zagrożenie dla wolności. Będzie tak wtedy, gdy – po pierwsze – wprowadzane ograniczenia będą arbitralne, nieproporcjonalne do ewentualnych zagrożeń i – po drugie – gdy będą one wyłączone (czy to prawnie, czy faktycznie) spod kontroli sprawowanej przez instytucje demokratyczne. Konflikt między koniecznością istnienia legalnej, prawnie umocowanej działalności operacyjnej i zagrożeniem dla konstytucyjnych wolności i praw jednostki wymaga więc przede wszystkim wyważenia właściwej proporcji w prawnej ochronie obu sfer, pozostających w konflikcie (...). Instrumentarium prawne, umożliwiające wyważenie stosownego kompromisu obejmuje:

- z jednej strony, regulację materialnoprawną (określającą granice stawiane przez system prawa wkroczeniu przez władzę w poszczególne sfery prywatności jednostki);
- z drugiej zaś – gwarancje proceduralne, towarzyszące temu wkroczeniu, tj. konieczność zgłoszenia kontroli organowi pozapolicyjnemu i jej legalizacji przez ten organ, przesłanki i procedury legalizacji – przez organ zewnętrzny i poprzez udostępnienie zainteresowanemu (choćby w pewnym

zakresie i od pewnego momentu czasowego) wiedzy o kontroli i jej rezultatach, środki kontroli na wypadek ekscesu organu przeprowadzającego kontrolę” (wyrok z dnia 12 grudnia 2005 r., sygn. K 32/04, OTK ZU Nr 11/A/2005, poz. 132, s. 1494).

W świetle orzecznictwa Trybunału Konstytucyjnego, zasada proporcjonalności pozostaje w immanentnej więzi z zakazem nadmiernej ingerencji w sferę praw i wolności konstytucyjnych jednostki. Przy ocenie, czy ingerencja była wyrazem konieczności i została przeprowadzona tylko w niezbędnym wymiarze, uwzględnia się specyfikę poszczególnych praw i wolności. Surowsze standardy dotyczą praw osobistych i politycznych niż ekonomicznych i socjalnych. W przypadku konkurencyjności chronionych konstytucyjnie dóbr – jaka występuje jako konflikt pomiędzy konstytucyjnym prawem do prywatności, tajemnicą porozumiewania się oraz ochroną autonomii informacyjnej a względami bezpieczeństwa publicznego – konieczne jest zachowanie przez ustawodawcę czytelnej równowagi między interesami pozostającymi w kolizji. W ocenie Trybunału Konstytucyjnego, występuje nadto ścisły związek między zagrożeniami dla godności człowieka stanowiącej podstawę konstytucyjnych wolności i praw jednostki, a wszelkimi czynnościami, które wkraczają w prywatność jednostki. W odniesieniu do prywatności (która na poziomie konstytucyjnym jest chroniona wieloaspektowo i obejmuje kilka praw oraz wolności – określonych w art. 47 – 51 Konstytucji) związek ten jest szczególnie (jakkolwiek nie taki sam w wypadku każdej z tych konstytucyjnych wolności i praw). Zachowanie godności człowieka wymaga poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność „bycia z innymi” czy dzielenia się z innymi przeżyciami bądź doznaniem o intymnym charakterze (por. wyrok z dnia 23 czerwca 2009 r., sygn. K 54/07, OTK ZU Nr 6/A/2009, poz. 86, s. 910 oraz powołane tam orzecznictwo).

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

W końcu, zgodnie z orzecznictwem Trybunału Konstytucyjnego, ustawodawca, ograniczając wskazane prawa i wolności konstytucyjne, winien jednocześnie stworzyć gwarancje prawne i instytucjonalne, pozwalające stosować określone działania tylko w zakresie koniecznym dla realizacji konstytucyjnych celów i w sposób charakteryzujący się jak najmniejszym stopniem dolegliwości dla obywateli i z zastosowaniem określonych procedur. Nakaz ten jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa. Zgodnie z art. 31 ust. 3 Konstytucji, ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności mogą być ustanawiane „tylko w ustawie”. Oznacza to nie tylko konieczność wskazania w akcie normatywnym tej rangi zakresu, w jakim konstytucyjne wolności lub prawa doznają ograniczenia. Z tych samych względów, dla których niedopuszczalne jest odsyłanie w tej materii do aktów wykonawczych, jako naruszenie wymagań konstytucyjnych oceniać należy tak niejasne i nieprecyzyjne formułowanie przepisu, które powoduje niepewność jego adresatów co do ich praw i obowiązków. Powoduje to bowiem stworzenie

nazbyt szerokich ram dla organów stosujących ten przepis, które w istocie muszą zastępować prawodawcę w zakresie tych zagadnień, które uregulował on w sposób niejasny i nieprecyzyjny. Ustawodawca nie może poprzez niejasne formułowanie tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki. Założenie to można określić ogólnie jako zasadę określoności ustawowej ingerencji w sferę konstytucyjnych wolności i praw jednostki. Kierując się tą zasadą Trybunał Konstytucyjny reprezentuje stanowisko, iż przekroczenie pewnego poziomu niejasności przepisów prawnych stanowić może samoistną przesłankę stwierdzenia ich niezgodności zarówno z przepisem wymagającym regulacji ustawowej określonej dziedziny (np. ograniczeń w korzystaniu z konstytucyjnych wolności i praw, art. 31 ust. 3 zdanie 1 Konstytucji), jak z wyrażoną w art. 2 Konstytucji zasadą państwa prawnego (por. wyrok z dnia 20 kwietnia 2004 r., sygn. K 45/02, OTK ZU Nr 4/A/2004, poz. 30, s. 401 oraz powołane tam orzecznictwo).

Stosowanie kontroli operacyjnej przez służby mundurowe oraz specjalne zawsze stanowi głęboką ingerencję w konstytucyjne prawa i wolności jednostki, w tym w prawo do prywatności, prawo do komunikowania się, a także w autonomię informacyjną i nienaruszalność mieszkania (problematyka ingerencji w dwa ostatnie z wymienionych praw obywateli, chronionych przez ustawę zasadniczą, będzie jeszcze przedmiotem odrębnego wywodu w dalszej części uzasadnienia niniejszego stanowiska). Tym samym, w świetle przytoczonych wyżej poglądów doktryny i orzecznictwa Trybunału Konstytucyjnego, regulacje prawne, dotyczące wkraczania w powyższe prawa osobiste jednostki, muszą odpowiadać szczególnie surowym standardom, tym bardziej że czynności operacyjno – rozpoznawcze, z natury swojej, mają charakter niejawnny, a tym samym, w przeciwieństwie, przykładowo, do czynności procesowych, nieporównanie trudniej zapewnić stosowną kontrolę ich

stosowania. Przede wszystkim, regulacje dotyczące kontroli operacyjnej mogą być zawarte wyłącznie w aktach normatywnych rangi ustawy, przy czym muszą spełniać wymóg kompletności unormowania ustawowego, a więc muszą samodzielnie określać wszystkie podstawowe elementy ograniczenia danego prawa.

Zakwestionowane przez Rzecznika Praw Obywatelskich przepisy ustawowe, niezależnie od wykazanych wyżej różnic między nimi, wszystkie zawierają otwarte katalogi środków technicznych, umożliwiających prowadzenie kontroli operacyjnej polegającej na uzyskiwaniu w sposób niejawnym informacji i dowodów oraz ich utrwalaniu, jak również pozwalają na pozyskiwanie niczym, w praktyce, nie ograniczonego zakresu informacji. Użycie przez ustawodawcę, w każdym z zaskarżonych unormowań, takich określeń, jak „w szczególności” czy też „i innych informacji” pozostawia organom stosującym omawiane przepisy (w praktyce – służbom mundurowym oraz specjalnym) zdecydowanie zbyt szerokie ramy interpretacyjne. W konsekwencji sprzyja to – choćby potencjalnie – arbitralności decyzji podejmowanych przez te organy, tak w zakresie użycia poszczególnych rodzajów środków technicznych, jak i charakteru pozyskiwanych informacji, przekazywanych przy pomocy sieci telekomunikacyjnych.

Ustanawiając otwarte katalogi środków technicznych, pozwalających na stosowanie kontroli operacyjnej, ustawodawca posłużył się w analizowanych regulacjach nieostrą aparaturą pojęciową dotyczącą informacji pozyskiwanych. W szczególności, formułując zakwestionowane przepisy, prawodawca posłużył się nieostрым pojęciem „środki techniczne umożliwiające uzyskiwanie w sposób niejawnym informacji i dowodów oraz ich utrwalanie”, co może prowadzić do legalizacji posługiwania się przez stosowne służby praktycznie każdym środkiem pozyskiwania informacji, bez żadnych ograniczeń natury technicznej. Ustawodawca nie sprecyzował, jakie informacje i dowody służby mogą pozyskiwać, wymieniając jedynie przykładowo treści rozmów telefonicznych

oraz posługując się nieostrym pojęciem „inne” w odniesieniu do informacji przekazywanych za pomocą sieci telekomunikacyjnych. Nadto, Straży Granicznej, Żandarmerii Wojskowej oraz wywiadowi skarbowemu ustawodawca przyznał dodatkowo prawo pozyskiwania „obrazu”, nie precyzując jednak, jaki „obraz” ma na myśli, i nie wprowadzając żadnych ograniczeń w tym zakresie. Powyższa konstatacja zdaje się skłaniać do pogłębienia wątpliwości odnośnie pozostawienia służbom przez prawodawcę zbyt szerokich ram interpretacyjnych.

Wspomniana wyżej, nadmierna swoboda interpretacyjna, pozostawiona stosownym służbom przy podejmowaniu decyzji odnośnie rodzajów stosowanych środków technicznych oraz charakteru pozyskiwanych informacji, może, w konsekwencji, rodzić daleko posuniętą niepewność adresatów omawianych norm prawnych co do zakresu przysługujących im praw i obowiązków. W szczególności, obywatele nie mają możliwości uzyskania informacji, na podstawie przepisów ustawowych, za pomocą jakich konkretnie środków stosowne służby mogą, w sposób niejawnny, wkraczać w sferę konstytucyjnie chronionej ich prywatności oraz sferę swobody komunikowania się bądź innych wymienianych przez Rzecznika Praw Obywatelskich praw i wolności jednostki.

Posłużenie się przez prawodawcę, w ocenianych ustawach, otwartym i nieostro sformułowanym katalogiem środków umożliwiających uzyskiwanie informacji i dowodów oraz ich utrwalanie, przy faktycznym braku ograniczeń odnośnie rodzajów pozyskiwanych informacji przekazywanych za pomocą sieci telekomunikacyjnych, prowadzi do sytuacji, gdy praktycznym ograniczeniem służb w zakresie kontroli operacyjnej stają się nie uwarunkowania prawne, ale aktualne możliwości finansowe służb i ich dostęp do najnowocześniejszych zdobyczy technologicznych. Tym samym, omawiane rozwiązania prawne godzą w wymóg określoności prawa oraz nakaz dochowania przyzwoitej legislacji, wywodzone z zasady demokratycznego państwa prawnego, jak również

w prawo do prywatności, prawo do komunikowania się oraz konstytucyjne gwarancje dopuszczalności ograniczeń w zakresie korzystania przez jednostkę z konstytucyjnych wolności i praw.

Przechodząc do oceny kwestionowanych przez Rzecznika Praw Obywatelskich przepisów w kontekście powołanego w uzasadnieniu wniosku wzorca kontroli, zawartego w art. 50 Konstytucji RP, należy odnotować, że, zgodnie z tym przepisem ustawy zasadniczej, zapewnia się nienaruszalność mieszkania, a przeszukanie mieszkania, pomieszczenia lub pojazdu może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

W doktrynie przyjmuje się, że nienaruszalność mieszkania, która może być określona jako niezakłócone korzystanie ze swego mieszkania (tzw. mir domowy), jest klasyczną wolnością jednostki o charakterze osobistym, służącą zwłaszcza jej psychicznej integralności, posiadającą wyraźny związek z jej deklarowaną godnością. Posiada również oczywisty związek z prawem do prywatności i może być także traktowana jako jeden z jej przejawów. Nienaruszalność mieszkania nie może być rozumiana jako jedynie zakaz przeszukiwania (bez dostatecznych podstaw), ale również jako zakaz wszelkiego nieuprawnionego wkraczania doń i przebywania. Nie tylko więc przeszukanie następować może jedynie w przypadkach określonych przez ustawę i w sposób w niej określony, lecz wymagają tego również wszelkie inne wkroczenia do cudzych mieszkań, w szczególności przez funkcjonariuszy publicznych lub pracowników służb publicznych (por. Paweł Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Tom III, Wydawnictwo Sejmowe, Warszawa 2003 r., tezy do art. 50, s. 1).

W literaturze przedmiotu dominuje również pogląd, że treść art. 50 jest tak zbudowana, iż daje podstawę do przyjęcia, że nienaruszalność, o której mówi się w zdaniu pierwszym, rozciąga się nie tylko na mieszkanie, ale także na

służące konkretnej osobie każde pomieszczenie oraz pojazd rozumiany tu szeroko, jako każdy możliwy środek lokomocji (por. Bogusław Banaszak i Mariusz Jabłoński [w:] *Konstytucje Rzeczypospolitej oraz Komentarz do Konstytucji RP z 1997 roku*, Wrocław 1998, s. 98).

Zgodnie z orzecnictwem Trybunału Konstytucyjnego, związek między zagrożeniem godności człowieka, spoczywającej u podstaw wszystkich konstytucyjnych wolności i praw jednostki, a czynnościami operacyjnymi, które wkraczają w prywatność jednostki – jest powszechnie podkreślany, zarówno w piśmiennictwie, jak w europejskim (w tym polskim) *acquis constitutionnel*. Wszystkie prawa i wolności konstytucyjne jednostki wywodzą się z godności. W wypadku prywatności (która – co należy przypomnieć – na poziomie konstytucyjnym jest chroniona wieloaspektowo, poprzez kilka praw i wolności – por. art. 47 – 51) związek ten jest szczególny, jakkolwiek nie taki sam w wypadku każdej z tych konstytucyjnych wolności i praw. Zachowanie przez człowieka godności wymaga bowiem – co także należy przypomnieć – poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność „bycia z innymi” czy „dzielenia się z innymi” swoimi przeżyciami bądź doznaniem o intymnym charakterze. Dlatego sfera prywatna jest zbudowana z różnych kręgów, w mniejszym lub większym stopniu otwartych (prawnie) na oddziaływanie zewnętrzne, gdzie konstytucyjna aprobata dla władczego wkroczenia przez władzę nie jest jednakowa. Dzieje się tak dlatego, że konieczna w demokratycznym państwie potrzeba wkroczenia w różne kręgi prywatności nie jest dla każdego kręgu taka sama. Nie bez przyczyny np. poszanowanie prywatności mieszkania stawia wyższe wymagania legalności ingerencji władzy stosującej podsłuchy, niż wkroczenie w tajemnicę korespondencji (por wyroki: z dnia 12 grudnia 2005 r., sygn. K 32/04, *op. cit.*, s. 1498 oraz powołane tam orzecznictwo, jak również wyrok z dnia 23 czerwca 2009 r., sygn. K 54/07, *op. cit.*, s. 910 oraz powołane tam orzecznictwo).

W uzasadnieniu wniosku Rzecznik Praw Obywatelskich podniósł, iż w treści kwestionowanych przepisów ustawodawca w ogóle nie wziął pod uwagę, że istnieją uwarunkowane konstytucyjnie, zróżnicowane wymagania w zakresie ochrony poszczególnych kręgów prywatności, poprzestając na przykładowym wskazaniu, iż niejawna ingerencja służb w prawa jednostki może dotyczyć tych elementów prawa do prywatności, które obejmują wolność i ochronę tajemnicy komunikowania się czy też wizerunku jednostki.

Podzielając zastrzeżenia Wnioskodawcy, należałoby w tym miejscu odnotować, iż w pełni zachowują aktualność, zawarte we wcześniejszej części uzasadnienia niniejszego stanowiska, stwierdzenia dotyczące zakreslenia przez ustawodawcę nadmiernie poszerzonych katalogów sytuacji uprawniających służby do podejmowania kontroli operacyjnej, jak również użycia przez prawodawcę, w zakwestionowanych regulacjach, nieostrej aparatury pojęciowej oraz otwartych katalogów środków technicznych, służących do prowadzenia takiej kontroli. Tym samym, można bronić poglądu, że ustawodawca pozostawił stosowanie kontroli operacyjnej, w zakresie odnoszącym się do ewentualnego naruszenia zasady nienaruszalności mieszkania, swobodnemu uznaniu służb mundurowych oraz specjalnych, rezygnując nie tylko z regulacji gwarancyjnych (porównywalnych, przykładowo, do unormowań przepisów art. 219 – 236 Kodeksu postępowania karnego w przypadku procesowej instytucji przeszukania), ale w ogóle z jakichkolwiek ograniczeń w porównaniu z kontrolą operacyjną stosowaną w innych wypadkach. Innymi słowy, przyjmując oceniane regulacje, ustawodawca uchybił zarówno zasadzie nienaruszalności mieszkania, jak i zasadzie określoności ustawowej ingerencji w wolności i prawa jednostki.

Przechodząc do oceny kwestionowanych przez Rzecznika Praw Obywatelskich przepisów w kontekście, powołanej w uzasadnieniu wniosku, konstytucyjnie chronionej autonomii informacyjnej jednostki, należy odnotować, że, zgodnie z art. 51 ust. 1 ustawy zasadniczej, nikt nie może być

obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Przepis art. 51 ust. 2 Konstytucji RP stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Zgodnie z art. 51 ust. 3 ustawy zasadniczej, każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a ograniczenie tego prawa może określić ustawa. Z kolei, art. 51 ust. 4 Konstytucji RP stanowi, że każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. W końcu, art. 51 ust. 5 ustawy zasadniczej przesądza, że zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

W doktrynie przyjmuje się, że, gwarantując prawo do prywatności, nie może Konstytucja – w sposób generalny – pozwalać organom władzy publicznej ani na dokumentowanie dla własnych celów tzw. danych osobowych, czyli informacji o osobowych właściwościach (indywidualnych cechach) konkretnych jednostek, ani też zezwalać tym organom na penetrowanie i dokumentowanie zachowań osób prywatnych, ani też w końcu zmuszać tych osób do ujawniania swych cech, właściwości oraz swego osobistego postępowania, i tu już nie tylko wobec wspomnianych organów, ale wobec kogokolwiek. Z kolei, gdy, w dopuszczalnych granicach ustawowych, zbiory danych osobowych wytworzone przez uprawnione podmioty (organy władzy publicznej, i to tylko we wskazanym zakresie) już funkcjonują – prawo do prywatności, ale również wymóg ochrony godności ludzkiej, sama natura praw osobistych, do których i one należą, oraz zasada demokratycznego państwa prawnego – wymagają zagwarantowania dostępu do takich danych, wnoszenia sprostowań oraz ewentualnie żądania usunięcia pewnych z nich (por. Paweł Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Tom III, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 51, s. 3).

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

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, ochrona życia prywatnego, gwarantowana konstytucyjnie co do zasady w art. 47, obejmuje sobą także autonomię informacyjną (art. 51 Konstytucji RP), oznaczającą prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów (por. wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, OTK ZU Nr 6/A/2005, poz. 64, s. 813 oraz powołane tam orzecznictwo).

W świetle orzecznictwa Trybunału Konstytucyjnego, istnienie w art. 51 ust. 2 Konstytucji odrębnej regulacji, dotyczącej proporcjonalności wkraczania w prywatność jednostki, należy tłumaczyć tym, że naruszenie autonomii informacyjnej poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki. Autonomia informacyjna, której wyodrębnienie normatywne z całości ochrony prywatności przewiduje art. 51, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Normatywne wyodrębnienie, ustanowione w art. 52 ust. 2 Konstytucji, odrębnego zakazu – ułatwia dostrzeżenie takiego wkroczenia i upraszcza przedmiot dowodu, iż takie wkroczenie nastąpiło. Przedmiotem dowodu staje się wtedy bowiem tylko to, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne” lub „użyteczne” dla władzy. Dowodu wymaga, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym. Analiza relacji przepisów art. 31 ust. 3 i art. 51 ust. 2 Konstytucji uzasadnia stwierdzenie, że naruszenie autonomii informacyjnej, przez dozwolone pozyskiwanie informacji o obywatelach, powinno odpowiadać wymaganiom określonym w art. 31 ust. 3 Konstytucji (por. wyroki: z dnia 20 listopada 2002 r., sygn. K 41/02, OTK ZU Nr 6/A/ 2002 r., poz. 83, s. 1112 oraz z dnia 17 czerwca 2008 r., sygn. K 8/04, OTK ZU Nr 5/A/2008, poz. 81, s. 812 – 813).

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

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

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

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

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

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

Rzecznik Praw Obywatelskich podniósł w uzasadnieniu swego wniosku, iż nieograniczony katalog możliwych do zastosowania przez służby środków technicznych powoduje, że mogą one za pomocą tych bliżej niezidentyfikowanych środków ingerować także w autonomię informacyjną jednostki (art. 51 Konstytucji RP).

Jak wspomniano, czynności operacyjno – rozpoznawcze, ze swej istoty, mają charakter niejawny. Kontrola sądowa tych czynności jest ograniczona, bowiem, zgodnie z przepisami: art. 19 ust. 20 ustawy o Policji, art. 9e ust. 19 ustawy o Straży Granicznej, art. 36c ust. 14 ustawy o kontroli skarbowej, art. 31 ust. 19 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 11a ustawy o ABW oraz AW, jak również art. 17 ust. 17 ustawy o CBA, na postanowienie sądu w przedmiocie kontroli operacyjnej zażalenie przysługuje jedynie szefowi lub organowi służby, który złożył wniosek o zastosowanie, zalegalizowanie bądź przedłużenie czasu trwania kontroli operacyjnej, nie przysługuje natomiast osobie, wobec której kontrolę operacyjną stosowano (nawet po zakończeniu tej kontroli). Jedyny wyjątek od opisanej wyżej reguły, przyjętej przez prawodawcę, zawiera ustawa o SKW oraz SWW, która w art. 31 ust. 10 stanowi, że na postanowienia sądu w omawianym przedmiocie przysługuje zażalenie, nie ograniczając jednocześnie kręgu podmiotów, którym to zażalenie przysługuje.

Nadto, ustawodawca nie wprowadził do zakwestionowanych przez Wnioskodawcę ustaw żadnych przepisów zobowiązujących służby do powstrzymania się od pozyskiwania danych objętych tak zwanymi zakazami dowodowymi (co będzie jeszcze przedmiotem rozważań w dalszej części uzasadnienia niniejszego stanowiska). Innymi słowy, rodzą się pytania, czy

zbieranie takich danych rzeczywiście jest niezbędne w demokratycznym państwie i czy w ogóle zbieranie ich można uznać za dozwolone przez Konstytucję RP.

Przytoczone wyżej cechy charakterystyczne modelu czynności operacyjno – rozpoznawczych, przyjętego przez ustawodawcę, jak również, wspomniany we wcześniejszej części uzasadnienia niniejszego stanowiska, nadzwyczaj szeroki katalog sytuacji, w których może być stosowana kontrola operacyjna, wskazują na bezwzględną konieczność zachowania szczególnej precyzji i jednoznaczności przepisów określających granice ingerencji służb w sferę autonomii informacyjnej jednostki, form tego wkraczania, jak również procedur, w jakich owo wkraczanie jest dopuszczalne. Tym samym, użycie w kwestionowanych przepisach nieostrej aparatury pojęciowej i ustanowienie otwartego katalogu środków technicznych, umożliwiających prowadzenie kontroli operacyjnej, przy równoczesnym braku ograniczeń odnośnie rodzaju informacji pozyskiwanych przez służby, należy ocenić zdecydowanie negatywnie. W tym stanie rzeczy wspomniane wyżej zastrzeżenia Wnioskodawcy są zasadne.

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

i zapobieganie przestępstwom, ochronę zdrowia, moralności lub ochronę praw i wolności innych osób.

W doktrynie przyjmuje się, że prawo określone w art. 8 Konwencji ma przede wszystkim chronić jednostkę przed arbitralną ingerencją ze strony władz publicznych. Artykuł 8 nie tylko jednak zmusza państwa do powstrzymania się od niej. W uzupełnieniu tego negatywnego zobowiązania mogą również ciążyć na nich pozytywne obowiązki potrzebne dla skutecznego poszanowania życia prywatnego, rodzinnego, podobnie jak domu i korespondencji (por. Marek Nowicki, *Komentarz do art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, System Informacji Prawnej Lex – Lex Omega – 39/2011).

W literaturze przedmiotu podnosi się również, że ustęp 2 art. 8 Konwencji szczegółowo wylicza sytuacje, w których dopuszczalna jest ingerencja w prawo do prywatności, dodając przy tym zastrzeżenie, że musi być ona legalna, a więc przewidziana w prawie krajowym. Tak więc ingerencja w prawo do poszanowania prywatności, mimo iż dokonana w jednej z sytuacji przewidzianych wprost w ust. 2, uznana być może za naruszającą Konwencję, jeżeli nie ma wyraźnej podstawy ustawowej. I odwrotnie: pomimo oparcia ingerencji na prawie krajowym, może być ona uznana za pogwałcenie Konwencji, jeżeli nie jest np. konieczna w społeczeństwie demokratycznym (por. Piotr Hofmański, *Komentarz do wybranych przepisów Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności* [w:] *Standardy Prawne Rady Europy, Teksty i komentarze*, Tom III, Prawo Karne, Oficyna Naukowa, Warszawa 1997, s. 99).

Zgodnie z wyrokiem Europejskiego Trybunału Praw Człowieka w sprawie *Uzun v. Niemcy*, życie prywatne jest szerokim terminem, niepodlegającym wyczerpującemu zdefiniowaniu. Art. 8 chroni między innymi prawo do tożsamości i do rozwoju osobistego oraz prawo do nawiązywania i rozwijania związków z innymi ludźmi oraz ze światem zewnętrznym. Istnieje

więc sfera interakcji osoby z innymi ludźmi, nawet w kontekście publicznym, która może wejść w zakres stosowania „życia prywatnego” (por. wyrok z dnia 2 września 2010 r., 35623/05, System Informacji Prawnej Lex – lex Omega – 39/2011, Lex Nr 599284).

W sprawie *Malone v. Wielka Brytania*, ETPC orzekł między innymi, że:

„1. Ponieważ rozmowy telefoniczne są objęte pojęciami „życia prywatnego” i „korespondencji” w rozumieniu art. 8 Konwencji, środki podsłuchu stanowią „ingerencję władzy publicznej” w wykonywanie prawa zagwarantowanego w ust. 1 art. 8.

2. Sformułowanie „przypadki przewidziane prawem” nie odnosi się jedynie do samego prawa krajowego, lecz również do jakości tego prawa, wymagając od niego, by było zgodne z Konwencją. W ten sposób wyrażenie to zakłada, a wynika to z przedmiotu i celu art. 8, iż musi istnieć środek ochrony prawnej w prawie krajowym, chroniący przed arbitralną ingerencją władz publicznych w prawa zagwarantowane w ust. 1 art. 8. Zwłaszcza gdy działania władz są realizowane w tajemnicy, ryzyko arbitralności jest oczywiste. Wymóg „przewidywalności” zwłaszcza nie może oznaczać, że jednostka jest w stanie przewidzieć, kiedy władze mogą zastosować względem niej podsłuch, tak by odpowiednio dostosować swoje zachowanie. Tym niemniej, prawo musi być dostatecznie jasne w swych sformułowaniach, by dać obywatelom odpowiednie wskazówki odnośnie do okoliczności i warunków, w jakich władze publiczne są uprawnione do działania w tajemnicy i do potencjalnie niebezpiecznej ingerencji w prawo do życia prywatnego i tajemnicy korespondencji.

3. Jako że wykorzystanie w praktyce środków tajnego podsłuchu nie stanowi przedmiotu kontroli przez zainteresowane jednostki ani przez opinię społeczną jako taką, byłoby niezgodne z zasadą prawa dopuszczenie do tego, by margines swobody przyznany władzy wykonawczej w tym względzie, był nieograniczony. W efekcie, prawo krajowe musi w sposób dostatecznie jasny określać zakres takiego uznania, przyznany właściwej władzy oraz sposób jego

wykonania, uznając uzasadniony cel przyjętego środka, tak by zapewnić jednostce właściwą ochronę przeciwko arbitralnej ingerencji.

(...)

5. Ingerencja w prawa wynikające z ust. 1 art. 8 może być uznana za „konieczną w demokratycznym społeczeństwie” wtedy, gdy przyjęty szczególny system kontroli rozmów telefonicznych przez policję zawiera odpowiednie gwarancje uniemożliwiające nadużycia.”

(wyrok z dnia 2 sierpnia 1984 r., 8691/79, System Informacji Prawnej Lex – Lex Omega – 39/2011, Lex nr 80974).

Z kolei, zgodnie z wyrokiem ETPC w sprawie Bykov v. Rosja, „[j]eżeli chodzi o przechwytywanie komunikacji pomiędzy osobami dla celów dochodzenia prowadzonego przez policję, postanowienia ustawy muszą być wystarczająco jasne, aby dawać obywatelom odpowiednie wskazówki co do okoliczności i warunków, na jakich organy władzy krajowej są uprawnione do odwoływania się do tej tajnej i potencjalnie niebezpiecznej ingerencji w prawo do poszanowania życia prywatnego i korespondencji. W szczególności, ażeby spełnić wymóg „jakości prawa”, przepisy prawa przyznające [organom władzy krajowej] swobodę decyzyjną w tej dziedzinie muszą wskazywać na zakres tej swobody, mimo iż szczegółowe procedury i warunki, które należy zachować, niekoniecznie muszą się znajdować w przepisach materialnoprawnych. Stopień szczegółowości „ustawy” w tym kontekście będzie zależeć od konkretnego jej przedmiotu. Jako że stosowanie w praktyce środków niejawnnej inwigilacji komunikacji [pomiędzy osobami] nie podlega kontroli ani ze strony zainteresowanych osób, ani ze strony całego społeczeństwa, wyrażenie swobody decyzyjnej w tym zakresie w postaci nieograniczonego uprawnienia przyznanego organowi władzy wykonawczej – lub sądowej – byłoby sprzeczne z zasadą praworządności. W konsekwencji ustawa musi wskazywać w sposób wystarczająco wyraźny zakres takiej swobody decyzyjnej przyznawanej właściwym organom władzy oraz sposób jej wykorzystania, tak, aby jednostka

uzyskała odpowiednią ochronę przed arbitralną ingerencją.” (wyrok z dnia 10 marca 2009 r., 4378/02, System Informacji Prawnej Lex – Lex Omega – 39/2011, Lex nr 486978).

W cytowanym wyżej wyroku ETPC orzekł również, iż „wobec braku konkretnych i szczegółowych regulacji, stosowaniu techniki [w postaci podsłuchu przy wykorzystaniu urządzeń radiowych] jako części „eksperymentu operacyjnego” nie towarzyszyły odpowiednie gwarancje przeciwko różnym możliwym nadużyciom. W związku z tym stosowanie tego środka było podatne na arbitralność i było niezgodne z wymogami zgodności z prawem. Należy przyjąć, iż przedmiotowa ingerencja w prawo skarżącego do poszanowania życia prywatnego nie była „przewidziana przez ustawę”, czego wymaga art. 8 Konwencji.”(wyrok z dnia 10 marca 2009 r. 4378/02, *ibidem*).

Orzekając w sprawie Kvasnica v. Słowacja, Europejski Trybunał stanął, między innymi, na stanowisku, że sformułowanie „przewidziane przez ustawę” z art. 8 Konwencji wymaga, po pierwsze, by niejawni środek inwigilacji miał jakąś podstawę w prawie krajowym; odnosi się ono także do jakości danej ustawy, wymagając, by ustawa taka była zgodna z zasadą praworządności oraz dostępna osobie zainteresowanej, która to osoba, ponadto, musi mieć możliwość przewidzenia jej konsekwencji dla siebie, a także zgodna z zasadą praworządności (por. wyrok z dnia 9 czerwca 2009 r., 72094/01, System Informacji Prawnej Lex – Lex Omega – 39/2011, Lex nr 504371).

W końcu, w sprawie Rotaru v. Rumunia, Wielka Izba Europejskiego Trybunału Praw Człowieka orzekła między innymi: „Aby systemy niejawnej inwigilacji były zgodne z art. 8 Konwencji, muszą one zawierać gwarancje prawne stosowane do kontroli działań właściwych służb. Procedury kontrolne muszą odpowiadać wartościom demokratycznego społeczeństwa tak wiernie, jak to możliwe, a w szczególności zasadzie praworządności, która jest w sposób wyraźny przywołana w preambule do Konwencji. Zasada rządów prawa zakłada, między innymi, iż ingerencja ze strony organów władzy wykonawczej

w prawa jednostki powinna być przedmiotem skutecznej kontroli, która w normalnych warunkach powinna być przeprowadzona przynajmniej przez organy sądowe, jako że kontrola sądowa zapewnia najlepszą gwarancję niezależności, bezstronności oraz stosowania właściwej procedury (wyrok z dnia 4 maja 2000 r., 28341/95, System Informacji Prawnej Lex – Lex Omega 30/2011, Lex nr 76775).

Również Trybunał Konstytucyjny dokonywał kontroli szeregu unormowań określających uprawnienia służb mundurowych oraz specjalnych podczas podejmowania czynności operacyjno – rozpoznawczych.

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

- a) dostatecznie precyzyjnej, a zarazem konkretnej podstawy prawnej wkroczenia w sferę wolności (praw) w drodze ustawy; nie jest dopuszczalne wprowadzanie ograniczeń (tu: prywatności) aktami innej rangi,
- b) konieczności tego wkroczenia, rozważanej z punktu widzenia wymogów demokratycznego państwa prawa; niewystarczające jest odwołanie się li tylko do czynnika celowości; niezbędne jest wykazanie konieczności, i to co do konkretnego (opisanego co do zakresu i sposobu) ograniczenia

wprowadzonego w ustawie zwykłej, respektującej standard państwa oświeconego, otwartego, tolerancyjnego, dysponującego fachowym aparatem policyjnym zdolnym działać w sposób rzetelny, profesjonalny i niemałostkowy, traktujący wkroczenie w sferę chronionych praw jednostki jako zło konieczne, a nie jako czynnik usprawniający pracę policji,

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

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

Trybunał Konstytucyjny przypominał również, że w orzecznictwie Europejskiego Trybunału Praw Człowieka podkreśla się konieczność zbadania, czy w konkretnym przypadku ingerencji w sferę prywatności istniały podstawy uprawniające działania państwa. Działania można uznać za usprawiedliwione, gdy służą celom wymienionym w klauzulach ograniczających (art. 8 ust. 2 Konwencji). Ingerencja musi być przewidziana przez prawo, co oznacza, że stosowane środki mają mieć podstawę w prawie krajowym, przy czym prawo to ma być dostępne osobom zainteresowanym oraz przewidywalne co do swoich skutków. Prawo musi być dostatecznie jasne w swych sformułowaniach, by dać obywatelom odpowiednie wskazówki odnośnie okoliczności i warunków,

w jakich władze publiczne są uprawnione do działania w tajemnicy i do potencjalnie niebezpiecznej ingerencji w prawo do życia prywatnego i tajemnicę korespondencji (por. wyrok z dnia 20 czerwca 2005 r., sygn. K 4/04, *op. cit.*, s. 821, jak również powołane tam orzecznictwo Europejskiego Trybunału Praw Człowieka).

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

W szczególności, zasada poszanowania praworządności (w rozumieniu orzecznictwa ETPC) obliguje strony Konwencji do ograniczenia działań policji (jak się wydaje, również innych służb) tylko do sytuacji dozwolonych i dostatecznie uzasadnionych przez prawo krajowe. Wypełnienie takiego obowiązku powinno polegać na tym, że stosowne przepisy powinny być dostępne dla obywateli i być jasne w swoim zakresie, tak aby jednostka wiedziała, w jakich okolicznościach i na jakich warunkach władze publiczne są uprawnione do uciekania się do działań niejawnnych, ingerujących w życie prywatne obywateli.

Możliwości posłużenia się przez służby mundurowe oraz specjalne określonymi środkami, pozwalającymi na pozyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie, są determinowane w obowiązującym stanie prawnym – co zostało już skonstatowane – nie tyle unormowaniami ustawowymi (ze względu na niedoskonałość regulacji), co możliwościami finansowymi tych służb oraz dostępem do najnowszych technologii. Tym

samym, możliwość wkraczania w życie prywatne i swobodę komunikowania się nie została w prawie polskim, na szczeblu ustawy, zdefiniowana w sposób wystarczająco jasny i precyzyjny. Innymi słowy, dostępne dla obywateli przepisy prawne nie pozwalają tymże obywatelom na wystarczająco pełne rozeznanie, w jakich okolicznościach i na jakich warunkach władze publiczne są uprawnione do uciekania się do działań niejawnych, ingerujących w życie prywatne jednostki. Powyższy zarzut nabiera szczególnej ostrości, jeżeli się zważy, jak szeroko określił ustawodawca katalogi sytuacji, w których służby uzyskały prawo wkraczania w sferę konstytucyjnie chronionych praw i wolności jednostki. W tej sytuacji, zarzuty Wnioskodawcy, w omawianym zakresie, sformułowane odnośnie analizowanych przepisów, należy uznać za w pełni zasadne.

Reasumując powyższe wywody, należy przypomnieć, iż Rzecznik Praw Obywatelskich zaproponował w *petitum* swego wniosku ocenę zakwestionowanych przez siebie przepisów jedynie w kontekście wzorców kontroli zawartych w art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji RP. Powyższą propozycją Wnioskodawca nie objął natomiast oceny tychże przepisów w kontekście wskazanych w uzasadnieniu wniosku unormowań art. 49, art. 50 i art. 51 ustawy zasadniczej ani art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

Biorąc powyższe pod uwagę, należy uznać, że przepisy: art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego godzą w zasadę demokratycznego państwa prawnego,

prawo do prywatności oraz konstytucyjne gwarancje dopuszczalności ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw. Tym samym, zakwestionowane przez Wnioskodawcę przepisy ustawowe są niezgodne z art. 2 oraz z art. 47 w związku z art. 31 ust. 3 ustawy zasadniczej.

II.

Zakwestionowany przez Rzecznika Praw Obywatelskich przepis art. 20c ust. 1 ustawy o Policji ma następujące brzmienie:

„Art. 20c. 1. W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”, oraz może je przetwarzać.”.

Zakwestionowany przez Wnioskodawcę przepis art. 10b ust. 1 ustawy o Straży Granicznej brzmi następująco:

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

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

Przepis art. 36b ust. 1 ustawy o kontroli skarbowej ma następującą treść:

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

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

2) identyfikujące podmiot korzystający z usług pocztowych oraz dotyczące faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług

- oraz może je przetwarzać.”,

przy czym RPO kwestionuje tylko pkt 1 w tym przepisie.

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych ma następujące brzmienie:

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

Przepis art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Wnioskodawca kwestionuje jedynie pkt 1 w tym ustępie) brzmi następująco:

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

1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);

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

Przepis art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym ma następujące brzmienie:

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

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

przy czym RPO kwestionuje tylko pkt 1.

Przepis art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ma następującą treść:

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

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

przy czym także w przypadku tego przepisu Rzecznik Praw Obywatelskich kwestionuje jedynie pkt 1.

Przepisy art. 180a ust. 1, art. 180c oraz art. 180d Prawa telekomunikacyjnego mają następujące brzmienie:

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

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

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

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

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

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

„Art. 180d. Przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom na własny koszt, a także sądowi i prokuratorowi, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i pkt 3 – 5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.”.

Przed przystąpieniem do oceny zakwestionowanych przepisów w kontekście wskazanych przez Wnioskodawcę wzorców kontroli, jak się wydaje, należałoby dokonać porównania niektórych regulacji zawartych w unormowaniach dotyczących prowadzenia kontroli operacyjnej przez poszczególne służby mundurowe i specjalne. Już wstępna analiza brzmienia wspomnianych unormowań pozwala na wysnucie wniosku, że regulacje w nich zawarte, w sposób istotny, różnią się merytorycznie między sobą w zakresie stanowiącym przedmiot wniosku Rzecznika Praw Obywatelskich (pomijając uprawnienia niektórych służb odnośnie pozyskiwania informacji od operatorów

świadczących usługi pocztowe, jak również pomijając liczne różnice stylistyczno - językowe).

Policja, Straż Graniczna i Żandarmeria Wojskowa mogą mieć udostępniane dane telekomunikacyjne, jak również mogą je przetwarzać w celu zapobiegania lub wykrywania przestępstw (art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej oraz art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych). Innymi słowy, ustawodawca nadał wspomnianym wyżej służbom uprawnienie pozyskiwania danych telekomunikacyjnych w związku ze zwalczaniem wszelkich przestępstw, a nie tylko określonych przestępstw ściganych z oskarżenia publicznego, jak miało to miejsce w odniesieniu do zarządzania kontroli operacyjnej (co zostało omówione w poprzedniej części uzasadnienia niniejszego stanowiska). Zakres uprawnień tychże służb w odniesieniu do pozyskiwania danych telekomunikacyjnych będzie jeszcze przedmiotem dalszych rozważań. W tym miejscu wypadałoby jedynie odnotować, że katalog sytuacji, w których służby posiadają prawo wkraczania w sferę wolności i praw jednostki w omawianej formie czynności operacyjno – rozpoznawczych, jest wielokrotnie szerszy niż w przypadku podejmowania kontroli operacyjnej.

Również analogiczne kompetencje wywiadu skarbowego zostały dopuszczone przez ustawodawcę w znacznie większej liczbie sytuacji niż miało to miejsce w przypadku kontroli operacyjnej. Katalog sytuacji uprawniających omawianą służbę do pozyskiwania danych telekomunikacyjnych obejmuje zapobieganie lub wykrywanie wszystkich przestępstw skarbowych (a nie tylko takich, w których wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza określoną wartość), jak również przestępstw określonych w art. 228 – 231 Kodeksu karnego, popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów. Nadto, omawiany katalog został poszerzony o zapobieganie i wykrywanie naruszeń krajowych przepisów

celnych oraz ściganie naruszeń krajowych lub wspólnotowych przepisów celnych przez wykonywanie nadzoru transgranicznego osób, miejsc, środków transportu i towarów oraz dostawy kontrolowanej, w rozumieniu Konwencji sporządzonej na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi, sporządzonej w Brukseli dnia 18 grudnia 1997 r. (art. 36b ust. 1 w związku z art. 2 ust. 1 pkt 12 i pkt 14b ustawy o kontroli skarbowej).

Szersze kompetencje w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych niż wymienionym wyżej służbom, przyznał ustawodawca Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu oraz Służbie Kontrwywiadu Wojskowego. Ostatnie trzy wymienione służby uzyskały bowiem omawiane kompetencje odnośnie wszelkich informacji niezbędnych do realizacji ich zadań ustawowych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA oraz art. 32 ust. 1 ustawy o SKW oraz SWW). Kompetencje te nie ograniczają się do rozpoznawania, zapobiegania oraz wykrywania przestępstw, jak w przypadku Policji, Straży Granicznej oraz Żandarmerii Wojskowej.

Zgodnie z przepisem art. 5 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, do zadań ABW należy: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa; rozpoznawanie, zapobieganie i wykrywanie przestępstw (wymienionych we wcześniejszej części uzasadnienia niniejszego stanowiska); 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; uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony

bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego; podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

Z kolei, przepis art. 2 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym stanowi, że do zadań CBA należy: rozpoznawanie, zapobieganie i wykrywanie przestępstw (wymienionych we wcześniejszej części uzasadnienia niniejszego stanowiska); ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne; dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych; ujawnianie przypadków nieprzestrzegania procedur podejmowania i realizacji decyzji w przedmiocie prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych; kontrola prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne; jak również prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości Centralnego Biura Antykorupcyjnego oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi.

Przepis art. 5 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, normujący zadania SKW, został przytoczony we wcześniejszej części uzasadnienia niniejszego stanowiska, podczas omawiania katalogu sytuacji uprawniających tę służbę do podejmowania kontroli operacyjnej. Innymi słowy, SKW jest jedyną służbą, która z woli ustawodawcy może wdrażać zarówno kontrolę operacyjną, jak i pozyskiwać

oraz przetwarzać dane telekomunikacyjne we wszystkich przypadkach, których mogą dotyczyć jakiekolwiek zadania tej służby.

Porównując zakresy zadań ostatnich trzech z omawianych służb, należałoby odnotować, że ustawodawca wyraźnie zróżnicował uprawnienia tych służb odnośnie pozyskiwania i przetwarzania danych telekomunikacyjnych, odmiennie określając przypadki upoważniające do podejmowania tego rodzaju czynności operacyjno - rozpoznawczych (nawiązujące do ustawowych zadań tychże służb) i przyznając zdecydowanie najszersze uprawnienia w omawianym zakresie – w sferze wykraczającej poza zwalczanie przestępczości – funkcjonariuszom CBA.

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

Z kolei, unormowania dotyczące prowadzenia kontroli operacyjnej przez Policję, Straż Graniczną i Żandarmerię Wojskową zawierają (dość syntetyczne skądinąd) regulacje przewidujące zniszczenie materiałów, które nie zawierają informacji mających znaczenie dla postępowania karnego (art. 20c ust. 7 ustawy o Policji, art. 10b ust. 6 ustawy o Straży Granicznej oraz art. 30 ust. 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Przepis art. 36b ust. 5 ustawy o kontroli skarbowej przewiduje dyskrecyjne

uprawnienie ministra właściwego do spraw finansów, który nakazuje zniszczenie takich materiałów, o ile uzna za niezasadne wcześniejsze wystąpienie z wnioskiem przez Generalnego Inspektora Kontroli Skarbowej lub pracownika wywiadu skarbowego o udostępnienie tychże danych. Natomiast analizowane przepisy ustaw o ABW oraz AW, o CBA ani o SKW oraz SWW stosownych regulacji, dotyczących ewentualnego niszczenia materiałów nieprzydatnych do dalszego prowadzenia postępowania, nie zawierają. W tym miejscu należy zasygnalizować, że powyższa problematyka będzie jeszcze przedmiotem rozważań w dalszej części uzasadnienia niniejszego stanowiska.

W końcu, należałoby zauważyć, iż żaden z omawianych przepisów, normujących uzyskiwanie danych telekomunikacyjnych przez stosowne służby, nie zawiera regulacji przewidujących obowiązek poinformowania jednostki o pozyskiwaniu wspomnianych wyżej danych, dotyczących tej osoby, chociażby po zakończeniu postępowania, ani regulacji ograniczających możliwość pozyskiwania danych, które nie mogą być wykorzystywane dla potrzeb postępowania karnego (to jest informacji chronionych na podstawie tajemnicy lekarskiej, obrończej, dziennikarskiej itp.). Również i ta problematyka będzie jeszcze przedmiotem rozważań w dalszej części uzasadnienia niniejszego stanowiska.

Reasumując tę część rozważań, należałoby odnotować, że część zarzutów, podniesionych przez Wnioskodawcę w odniesieniu do unormowań dotyczących poszczególnych służb prowadzących kontrolę operacyjną, dotyczy regulacji zawartych w zaskarżonych przepisach, jednak wiele z tych zarzutów dotyczy materii, które w analizowanych przepisach nie zostały unormowane. W tej sytuacji istotnego znaczenia nabiera kwestia dopuszczalnego kształtu zarzutów formułowanych w stosunku do norm prawnych w postępowaniu przed Trybunałem Konstytucyjnym, a zwłaszcza rozróżnienia pomiędzy zaniechaniem prawodawczym a pominięciem prawodawczym.

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

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

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

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

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

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

Przechodząc do oceny zakwestionowanych przez Rzecznika Praw Obywatelskich regulacji w kontekście zasady wolności i ochrony komunikowania się, określonej w art. 49 w związku z art. 31 ust. 3 Konstytucji

RP, oraz prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji jednostki, określonych w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, należałoby podkreślić, że w pełni zachowują tu aktualność wywody, zawarte we wcześniejszej części uzasadnienia niniejszego stanowiska, dotyczące konstytucyjnych i konwencyjnych standardów wiążących ustawodawcę przyjmującego regulacje określające podejmowanie przez służby czynności operacyjno – rozpoznawczych.

Tytułem uzupełnienia wypadałoby odnotować, że w doktrynie, na gruncie Konwencji, dominuje pogląd, iż potrzeba zapewnienia odpowiednich zabezpieczeń chroniących dane osobowe jest tym większa, jeśli są one poddawane automatycznemu przetwarzaniu, w tym do celów policyjnych. Prawo krajowe musi zapewnić, aby były one zbierane w celach wyłącznie istotnych; aby nie były przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, i nie dłużej, niż przez okres wymagany ze względu na taki cel; prawo krajowe musi również zapewnić odpowiednie gwarancje skutecznej ich ochrony przed niewłaściwym użyciem lub nadużyciem. Jest to ważne zwłaszcza przy ochronie specjalnych kategorii danych bardziej wrażliwych (por. Marek Nowicki, *Komentarz do art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, op. cit.).

Zgodnie z wyrokiem Europejskiego Trybunału Praw Człowieka we wspomianej już sprawie *Malone v. Wielka Brytania*, z samej swej natury billing musi być rozróżniany od podsłuchu, który jest zjawiskiem niepożądanym i bezprawnym w społeczeństwie demokratycznym, chyba że istnieją po niemu uzasadnione powody. Ale użycie danych wynikających z billingu może, w niektórych okolicznościach, stanowić naruszenie art. 8. Dane bilingowe, zawierające informacje, szczególnie o wybieranych numerach, stanowią integralny składnik komunikacji telefonicznej. W efekcie, ujawnienie tej informacji policji, bez zgody abonenta, również stanowi ingerencję w prawa

zagwarantowane w art. 8 (por. wyrok z dnia 2 sierpnia 1984 r., 8691/79, *op. cit.*).

Orzekając w sprawie *Leander v. Szwecja*, ETPC stanął na stanowisku, że zarówno przechowywanie, jak i udostępnianie informacji zawartych w tajnym rejestrze policyjnym, które było połączone z odmową przyznania skarżącemu możliwości zakwestionowania tych informacji, stanowiło ingerencję w jego prawo do poszanowania życia prywatnego, zagwarantowane w art. 8 Konwencji. Wyrażenie „przewidziane przez ustawę”, zawarte w art. 8 ust. 2, wymaga na początek, by ingerencja miała podstawę w prawie krajowym. Zgodność z prawem krajowym sama w sobie jednak nie wystarcza: przedmiotowa ustawa musi być dostępna dla zainteresowanej jednostki, a skutki jej muszą być dla niej przewidywalne. Jednakże wymóg przewidywalności w specyficznym kontekście tajnych kontroli personelu w sektorach dotyczących bezpieczeństwa narodowego nie może być taki sam w wielu innych dziedzinach. Dlatego nie może on oznaczać, że jednostka powinna umieć precyzyjnie przewidzieć, jakie kontrole zostaną przeprowadzone w odniesieniu do niej przez specjalne służby policyjne, podejmujące wysiłki w celu ochrony bezpieczeństwa narodowego. Niemniej jednak, w systemie stosowanym powszechnie do wszystkich obywateli, sformułowania ustawy muszą być wystarczająco jasne, by dawały wystarczające wskazówki co do okoliczności oraz warunków, w jakich władze publiczne są upoważnione do odwołania się do tego rodzaju tajnej i potencjalnie niebezpiecznej ingerencji w życie prywatne (por. wyrok z dnia 26 marca 1987 r., 9248/81, System Informacji Prawnej Lex – Lex Omega – 39/2011, Lex nr 81034).

Policja, Straż Graniczna i Żandarmeria Wojskowa, jak zostało to wspomniane we wcześniejszej części uzasadnienia niniejszego stanowiska, mogą mieć udostępniane dane telekomunikacyjne, jak również mogą je przetwarzać w celu zapobiegania lub wykrywania wszelkich przestępstw, a więc zarówno przestępstw ściganych z oskarżenia publicznego, jak i ściganych

z oskarżenia prywatnego. Innymi słowy, nie ma przeszkód prawnych, by omawiane służby pozyskiwały dane telekomunikacyjne w celu zapobiegania lub wykrywania takich przestępstw, jak, przykładowo: zniesławienie (art. 212 Kodeksu karnego), znieważenie (art. 216), naruszenie nietykalności cielesnej (art. 217), niezawiadomienie o wypadku przy pracy (art. 222), kradzież lub przywłaszczenie cudzej rzeczy ruchomej o wartości 251 zł (art. 278 lub art. 284), zniszczenie mienia ruchomego o wartości 251 zł (art. 288), wyrąb drzewa w lesie, gdy wartość tego drzewa wynosi 76 zł (art. 290).

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, ustawodawca, konstruując przepis, który ingeruje głęboko w sferę prywatności jednostki, musi uwzględnić nie tylko zasady przyzwoitej legislacji (w tym zasadę dookreśloności i konkretności), ale także rozważyć proporcjonalność zastosowanego środka. Nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, ułatwiały ich osiągnięcie albo były wygodne dla władzy, która ma je wykorzystać do osiągnięcia tych celów. Środki te powinny być godne państwa określanego jako demokratyczne i prawne. Pamiętać przy tym należy, że wskazane środki (czynności operacyjne) o tyle tylko mogą być uznane za usprawiedliwione, o ile ich własnym celem jest właśnie obrona wartości demokratycznego państwa prawnego. Minimalnym wymogiem konstytucyjnym jest to, aby przeszły one test „konieczności w demokratycznym państwie prawnym”. Nie wystarczy zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę – w odniesieniu do użytego środka. Bez znaczenia jest też argument porównawczy, że podobne środki w ogóle bywają stosowane w innych państwach. Tylko bowiem odwołanie się geograficzne i historyczne do środków koniecznych w demokratycznym państwie prawnym może mieć wartość perswazyjną. Chodzi zatem o zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak

najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają ograniczeniu (por. wyrok z dnia 12 grudnia 2005 r., sygn. K 32/04, *op. cit.*, s. 1497 – 1498 oraz powołane tam orzecznictwo).

Niezależnie od wątpliwości co do racjonalności decyzji ustawodawcy, który zezwolił służbom na pozyskiwanie i przetwarzanie danych telekomunikacyjnych w celu zapobiegania lub wykrywania wymienionych wyżej przestępstw, jak również niezależnie od wątpliwości co do proporcjonalności wkroczenia w sferę wolności i praw jednostki w celu ochrony dóbr, przeciwko którym kierowane są te przestępstwa, należałoby wyrazić pogląd, że tak skonstruowane regulacje wydają się nadzwyczaj odległe od spełnienia testu „konieczności w demokratycznym państwie prawnym”, w rozumieniu orzecznictwa Trybunału Konstytucyjnego, jak również nie spełniają wymogu przewidywalności dla jednostki, w rozumieniu orzecznictwa Europejskiego Trybunału Praw Człowieka.

Omawiane służby zostały upoważnione przez ustawodawcę do pozyskiwania i przetwarzania danych telekomunikacyjnych nie tylko w celu zapobiegania i wykrywania przestępstw określonych w Kodeksie karnym i Kodeksie karnym skarbowym, ale również wszelkich innych przestępstw określonych w ustawach szczególnych, których to aktów normatywnych nawet nie wymieniono w ustawach normujących działalność konkretnych służb. Szacunkowo można byłoby przyjąć, że katalogi przestępstw, których zwalczanie upoważnia służby do pozyskiwania danych telekomunikacyjnych, obejmują co najmniej dwukrotnie więcej pozycji, niż katalogi przestępstw zawarte w regulacjach uprawniających służby do podejmowania kontroli operacyjnej. Nadto, nie wydaje się, by katalogi te spełniały wymogi dostatecznej precyzji i określoności, skoro jednostka nie otrzymuje w żadnej z omawianych tu ustaw, dotyczących poszczególnych służb, nawet ogólnej wskazówki, w którym akcie normatywnym ma poszukiwać określenia sytuacji prawnej, w jakiej służby będą

uprawnione do wkroczenia w konstytucyjnie chronioną sferę praw i wolności tejże jednostki.

Wydaje się, że, tytułem przykładu, można byłoby w tym miejscu wymienić kilka przestępstw określonych w ustawach szczególnych, których zwalczanie, teoretycznie rzecz ujmując, może upoważniać służby do pozyskiwania lub przetwarzania danych telekomunikacyjnych, co skądinąd nasuwa analogiczne wątpliwości. Do takich przestępstw należą: umieszczenie oznakowania CE albo znaku budowlanego na wyrobie budowlanym, który nie spełnia wymagań określonych w ustawie, umieszczenie na wyrobie budowlanym znaku podobnego do oznakowania CE albo znaku budowlanego, mogących wprowadzić w błąd użytkownika, konsumenta lub sprzedawcę tego wyrobu oraz umieszczenie znaku budowlanego na wyrobie, niebędącym wyrobem budowlanym (art. 34 pkt 2, 3 i 4 ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz. U. Nr 92, poz. 881), niezgłoszenie, w określonym terminie, Inspektorowi do Spraw Substancji Chemicznych wywozu chemikaliów wymienionych w załączniku I części 1 rozporządzenia nr 689/2008 (art. 33 ustawy z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach, Dz. U. Nr 63, poz. 322), dokonywanie przewozu zwierząt, niejadalnych produktów pochodzenia zwierzęcego lub ubocznych produktów zwierzęcych wbrew zakazowi przywozu lub bez zachowania bądź z naruszeniem wymagań weterynaryjnych obowiązujących w tym zakresie, przewożenie, wbrew zakazowi, produktów pochodzenia zwierzęcego, o których mowa w przepisach o produktach pochodzenia zwierzęcego, dokonywanie handlu lub umieszczanie na rynku zwierząt, niejadalnych produktów pochodzenia zwierzęcego lub ubocznych produktów zwierzęcych bez zachowania lub z naruszeniem wymagań weterynaryjnych obowiązujących w tym zakresie, dokonywanie przemieszczania koniowatych bez zachowania lub z naruszeniem wymagań weterynaryjnych obowiązujących w tym zakresie oraz umieszczanie zwierząt w gospodarstwie lub

transportowanie ich bez zachowania lub z naruszeniem wymagań weterynaryjnych obowiązujących w tym zakresie (art. 77 pkt 2, 2a, 3, 4 i 5 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 zmianami), wchodzenie w posiadanie bezprawnie pozyskanej tuszy lub trofeów zwierząt łownych, jak również hodowanie lub utrzymywanie bez zezwolenia chartów rasowych lub ich mieszańców (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 zmianami).

Przyjęcie przez ustawodawcę przytoczonych regulacji, podobnie jak w przypadku wskazanych wyżej przestępstw określonych w Kodeksie karnym, o wyrażnie mniejszym ładunku społecznej szkodliwości czynu, nasuwa poważne wątpliwości w zakresie proporcjonalności ograniczeń w korzystaniu przez jednostkę z jej konstytucyjnych praw i wolności, wprowadzonych w celu ochrony dóbr, przeciwko którym kierowane są te przestępstwa, odnośnie spełniania przez te regulacje testu „konieczności w demokratycznym państwie prawnym” w rozumieniu orzecznictwa Trybunału Konstytucyjnego, jak również – szerzej – wątpliwości co do racjonalności prawodawcy przyjmującego omawiane unormowania.

Jak wspomniano we wcześniejszej części uzasadnienia niniejszego stanowiska, wywiad skarbowy może pozyskiwać i przetwarzać dane telekomunikacyjne między innymi w celu zapobiegania lub wykrywania wszelkich przestępstw skarbowych. Brak jakichkolwiek ograniczeń w tym zakresie, nawet obejmujących przestępstwa skarbowe o relatywnie niskim ładunku społecznej szkodliwości, nasuwa analogiczne wątpliwości i zastrzeżenia, jak w przypadku zezwolenia ustawodawcy na pozyskiwanie przez Policję, Straż Graniczną oraz Żandarmerię Wojskową danych telekomunikacyjnych dotyczących przestępstw o niższym ciężarze gatunkowym.

Odrębnego omówienia, jak się wydaje, wymaga problematyka zezwolenia przez ustawodawcę na pozyskiwanie przez wywiad skarbowy informacji telekomunikacyjnych w celu zapobiegania i wykrywania naruszeń krajowych przepisów celnych oraz ścigania naruszeń krajowych lub wspólnotowych przepisów celnych przez wykonywanie nadzoru transgranicznego osób, miejsc, środków transportu i towarów oraz dostawy kontrolowanej.

Zgodnie z art. 1 ustawy z dnia 19 marca 2004 r. – Prawo celne (Dz. U. z 2004 r. Nr 68, poz. 622 ze zmianami), ustawa reguluje w zakresie uzupełniającym przepisy prawa wspólnotowego:

- 1) zasady przywozu towarów na obszar celny Wspólnoty Europejskiej, zwanej dalej „Wspólnotą”, i wywozu towarów z tego obszaru,
- 2) zasady postępowania z towarami objętymi Wspólną Polityką Rolną,
- 3) sposób przekazywania informacji do celów ewidencji i statystyki dotyczącej obrotu towarowego z państwami członkowskimi Wspólnoty - oraz związane z tym prawa i obowiązki osób, a także uprawnienia i obowiązki organów celnych.

Z kolei, art. 2 tejże ustawy stanowi, że wprowadzenie towaru na obszar celny Wspólnoty lub jego wyprowadzenie z tego obszaru powoduje z mocy prawa powstanie obowiązków i uprawnień przewidzianych w przepisach prawa celnego, jeżeli przepisy prawa, w tym umowy międzynarodowe, nie stanowią inaczej.

Powołana w art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej Konwencja sporządzona na podstawie artykułu K. 3 Traktatu o Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi, sporządzona w Brukseli dnia 18 grudnia 1997 r. (Dz. U. z 2008 r. Nr 6, poz. 31) przesądza, że „krajowe przepisy celne” w rozumieniu Konwencji to wszystkie przepisy ustawowe, wykonawcze i administracyjne Państwa Członkowskiego, których zastosowanie podlega, w całości lub częściowo, jurysdykcji celnej tego Państwa

Członkowskiego w odniesieniu do przepływu transgranicznego towarów podlegającego zakazom, ograniczeniom lub kontroli, w szczególności na podstawie art. 36 i 223 Traktatu ustanawiającego Wspólnotę Europejską, jak również niezharmonizowanej akcyzy (art. 4 ust. 1). Nadto, „wspólnotowe przepisy celne”, w rozumieniu Konwencji, to ogół przepisów prawa wspólnotowego i powiązanych przepisów wykonawczych, regulujących przywóz, wywóz, tranzyt i obecność towarów będących przedmiotem handlu między Państwami Członkowskim a państwami trzecimi, jak również między Państwami Członkowskimi w przypadku towarów nieposiadających statusu wspólnotowego w rozumieniu art. 9 ust. 2 Traktatu ustanawiającego Wspólnotę Europejską lub towarów podlegających dodatkowym kontrolom lub badaniom dla uzyskania statusu wspólnotowego; ogół przepisów przyjętych na szczeblu Wspólnoty w ramach wspólnej polityki rolnej i przepisów szczególnych przyjętych w odniesieniu do towarów uzyskanych w wyniku przetworzenia produktów rolnych; ogół przepisów przyjętych na szczeblu Wspólnoty w odniesieniu do zharmonizowanej akcyzy i podatków importowych od wartości dodanej wraz z wykonawczymi dla nich przepisami prawa krajowego (art. 4 ust. 2 Konwencji). W końcu przez „naruszenia” rozumie się, na gruncie Konwencji, działania sprzeczne z krajowymi lub wspólnotowymi przepisami celnymi, w tym *inter alia*: udział w popełnianiu takich naruszeń lub próbę ich popełnienia, udział w organizacji przestępczej, która dokonuje takich naruszeń, pranie pieniędzy pochodzących z naruszeń określonych w niniejszym ustępie (art. 4 ust. 3 Konwencji).

Oceniany przepis art. 36b ust. 1 ustawy o kontroli skarbowej zezwala wywiadowi skarbowemu na pozyskiwanie i przetwarzanie danych telekomunikacyjnych między innymi w celu zapobiegania lub wykrywania naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12 tejże ustawy. Ów art. 2 ust. 1 pkt 12 posługuje się zaś pojęciami: „naruszenia krajowych przepisów celnych” oraz „naruszenia krajowych lub wspólnotowych przepisów

celnych”. Ustawa – Prawo celne reguluje – jak już zaznaczono – określone materie „w zakresie uzupełniającym przepisy prawa wspólnotowego”. Z kolei, unormowania Konwencji w sprawie wzajemnej pomocy i współpracy między administracjami celnymi zredagowano w sposób bardzo ogólny, a zawarte w nich katalogi „krajowych przepisów celnych” oraz „wspólnotowych przepisów celnych” cechuje stosunkowo niewielka precyzja, a co ważniejsze, zdecydowanie otwarty charakter. W tej sytuacji, nie tylko zdekodowanie zawartości normatywnej użytych w prawie polskim przytoczonych wyżej sformułowań, odnoszących się do owych „naruszeń”, ale nawet odszukanie stosownych przepisów przesądzających, co należy traktować jako „naruszenie” (zwłaszcza w prawie unijnym), zdaje się wymagać głębokiej wiedzy specjalistycznej. Tym samym, tworzenie przez polskiego ustawodawcę regulacji o takim stopniu niedookreśloności należałoby uznać za niedopuszczalne.

Porównując zadania Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego oraz Służby Kontrwywiadu Wojskowego, których realizacja, z woli ustawodawcy, uprawnia te służby do pozyskiwania i przetwarzania danych telekomunikacyjnych, należałoby odnotować, że w odniesieniu do ABW i SKW obejmują one również zadania związane z ochroną informacji niejawnych, w odniesieniu do ABW – rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa, natomiast w odniesieniu do SKW – uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej jednostek organizacyjnych MON, uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia, ochronę bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez jednostki organizacyjne MON

oraz produkcji i obrotu towarami, technologiami o przeznaczeniu wojskowym. Z kolei, zdecydowanie odmienny zakres zadań ustawodawca wyznaczył CBA, zlecając tej służbie kontrolę prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych, ujawnianie przypadków nieprzestrzegania określonych przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych. W końcu, katalogi zadań wszystkich trzech omawianych tu służb mają charakter katalogów otwartych, zawierają bowiem klauzule o „podejmowaniu innych działań” określonych (przewidzianych) w odrębnych ustawach i umowach międzynarodowych (art. 5 ust. 1 ustawy o ABW oraz AW, art. 2 ust. 1 ustawy o CBA oraz art. 5 ust. 1 ustawy o SKW oraz SSW).

Kolejnym problemem, wymagającym, jak się wydaje, omówienia w tej części uzasadnienia niniejszego stanowiska, pozostaje kwestia dookreśloności i konkretności zakwestionowanych przez Rzecznika Praw Obywatelskich unormowań. Ustawodawca, jak wspomiano, upoważnił Policję, Straż Graniczną oraz Żandarmerię Wojskową do pozyskiwania i przetwarzania danych telekomunikacyjnych w celu zapobiegania lub wykrywania przestępstw (art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej oraz art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych). Analogiczne uprawnienia wywiadu skarbowego (ograniczone

do przestępstw skarbowych) zostały poszerzone o zapobieganie i wykrywanie naruszeń przepisów celnych (art. 36b ust. 1 w związku z art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej). W końcu – ABW, CBA i SKW uzyskały kompetencje do pozyskiwania i przetwarzania informacji niezbędnych do realizacji ich zadań ustawowych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA oraz art. 32 ust. 1 ustawy o SKW oraz SWW).

Określenie przez ustawodawcę celu pozyskiwania i przetwarzania danych telekomunikacyjnych jako „zapobieganie lub wykrywanie przestępstw” bądź „zapobieganie i wykrywanie naruszeń przepisów celnych” wydaje się nadzwyczaj lakoniczne w kontekście wymogu dookreśloności i konkretności unormowań ograniczających prawa i wolności konstytucyjne. Znacznie poważniejsze zastrzeżenia nasuwa analiza przepisów określających wspomniane zadania ustawowe ABW, CBA oraz SKW (art. 5 ust. 1 ustawy o ABW oraz AW, art. 2 ust. 1 ustawy o CBA oraz art. 5 ust. 1 ustawy o SKW oraz SWW). Użycie przez ustawodawcę, we wspomnianych przepisach, takich pojęć jak: „informacje mogące mieć znaczenie”, „informacje mogące mieć istotne znaczenie” czy „przeciwdziałanie przypadkom nieprzestrzegania przepisów” w zestawieniu z otwartym katalogiem ustawowych zadań omawianych służb zdają się wykluczać możliwość uznania, że analizowane unormowania dostarczają obywatelom wystarczających wskazówek, w jakiej sytuacji służby uzyskują prawo wkraczania w sferę objętą konstytucyjną ochroną prawa do prywatności, swobody komunikowania się oraz autonomii informacyjnej.

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

przypadków, uprawniających służby do pozyskiwania i przetwarzania danych telekomunikacyjnych, należałoby uznać za zdecydowanie wadliwy.

Reasumując tę część rozważań, należy stwierdzić, że przyjęte przez ustawodawcę katalogi sytuacji, upoważniających służby mundurowe oraz specjalne, są nieracjonalnie obszerne. Katalogi te obejmują wszystkie, bez wyjątku, przestępstwa i przestępstwa skarbowe, liczne i często niedookreślone lub niedoprecyzowane przypadki przekraczania przepisów prawa, tak krajowego, jak wspólnotowego, które przestępstwami nie są, liczne działania kontrolne, podejmowane w przypadkach, gdy nie wiadomo, czy jakiegokolwiek przekroczenie prawa w ogóle mogło nastąpić, a także działalność analityczną bądź planistyczną służb. Nadto, szereg omawianych katalogów ma charakter otwarty. W tej sytuacji nie sposób precyzyjnie określić liczby sytuacji, w których służby zostały uprawnione przez ustawodawcę do pozyskiwania i przetwarzania danych telekomunikacyjnych. Szacunkowo, liczba ta może obejmować kilkaset sytuacji, co już samo w sobie budzi poważne zastrzeżenia. Nadto, przepisy regulujące materię dostępu poszczególnych służb do danych telekomunikacyjnych – a więc sferę takich wolności konstytucyjnych i konwencyjnych jednostki, jak prawo do prywatności, tajemnica komunikowania się i autonomia informacyjna – zostały zredagowane w sposób nie dość precyzyjny i niewystarczająco konkretny. Innymi słowy, negatywną ocenę Rzecznika Praw Obywatelskich, sformułowaną odnośnie sposobu unormowania przez ustawodawcę celu gromadzenia przez służby danych telekomunikacyjnych, należy uznać za zasadną.

Obowiązek operatora publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych udostępniania danych telekomunikacyjnych wskazanym w uzasadnieniu niniejszego stanowiska służbom stanowi wyjątek od zasady zobowiązującej wspomniane wyżej podmioty do zachowania tajemnicy telekomunikacyjnej i szerszej zasady

ochrony danych osobowych. Zgodnie z art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami), za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Z kolei, art. 160 ust. 1 Prawa telekomunikacyjnego stanowi, że podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące są obowiązane do zachowania tajemnicy telekomunikacyjnej. Nadto, zgodnie z art. 159 ust. 1 Prawa telekomunikacyjnego, tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana „tajemnicą telekomunikacyjną”, obejmuje: dane dotyczące użytkownika; treści indywidualnych komunikatów; dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku; dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwania zestawianych połączeń. W końcu, art. 159 ust. 4 Prawa telekomunikacyjnego stanowi, że, z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej.

Wspomniane wyżej unormowania prawne przesądzają, że tajemnica telekomunikacyjna obejmuje nie tylko samą treść przekazu (komunikatu,

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

Analiza zakwestionowanych przez Rzecznika Praw Obywatelskich przepisów pozwala na wysnucie wniosku, że decyzja o pozyskaniu danych telekomunikacyjnych pozostaje w gestii stosownych służb mundurowych bądź specjalnych. W praktyce dane takie udostępniane są funkcjonariuszowi (żołnierzowi, pracownikowi) wskazanemu w pisemnym wniosku jego przełożonego odpowiedniej rangi lub posiadającemu pisemne upoważnienie takiego przełożonego bądź takiemu funkcjonariuszowi – za pośrednictwem sieci telekomunikacyjnej (art. 20c ust. 2 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 2 ustawy o kontroli skarbowej, art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 2 ustawy o ABW oraz AW, art. 18 ust. 2 ustawy o CBA oraz art. 32 ust. 2 ustawy o SKW oraz SWW). Obowiązek udostępnienia danych telekomunikacyjnych przez operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych zachodzi w każdym przypadku, gdy zwrócić się o to uprawnione służby (art. 180a ust. 1 pkt 2 w związku z art. 180c ust. 1 Prawa telekomunikacyjnego).

W przeciwieństwie do przepisów normujących kontrolę operacyjną w postaci, przykładowo, podsłuchu (art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o Straży Granicznej, art. 36c ust. 1 ustawy o kontroli skarbowej, art. 31 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA, jak również art. 31 ust. 1 ustawy o SKW oraz SWW), omawiane regulacje nie przyjmują subsydiarnego charakteru pozyskiwania danych telekomunikacyjnych. Tym samym, uprawnione służby zawsze mogą domagać się udostępnienia danych telekomunikacyjnych lub pobierać je samodzielnie, a nie tylko wtedy, gdy inne środki pozyskania informacji okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne. Z kolei, obowiązek udostępnienia omawianych danych aktualizuje się po stronie podmiotu wykonującego działalność telekomunikacyjną w każdym przypadku, gdy zwrócić się o to odpowiednie służby, a nie tylko wówczas, gdy inne środki podejmowane w celu realizacji ustawowego celu okazały się bezskuteczne. Innymi słowy, oceniane unormowania, ze względów oczywistych, nie są w stanie sprostać testowi „konieczności w demokratycznym państwie prawnym” w rozumieniu, przytoczonego we wcześniejszej części uzasadnienia niniejszego stanowiska, orzecznictwa Trybunału Konstytucyjnego.

Zarzut braku ustanowienia przez ustawodawcę warunku subsydiarności pozyskiwania przez służby danych telekomunikacyjnych nabiera szczególnej ostrości w przypadku, gdy służby te realizują swe uprawnienia w omawianym zakresie nie tylko w celu zapobiegania lub wykrywania przestępstw (zwłaszcza tych najgroźniejszych), ale w celu realizacji innych zadań ustawowych. Tytułem przykładu można by tu wymienić chociażby potencjalną możliwość pozyskiwania przez funkcjonariuszy Centralnego Biura Antykorupcyjnego danych telekomunikacyjnych w celu przeprowadzenia kontroli prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, przy

wcześniejszym pominięciu jakichkolwiek innych czynności, które mogłyby doprowadzić do uzyskania koniecznych informacji (art. 2 ust. 1 pkt 5 ustawy o CBA).

Reasumując tę część wywodów, należałoby odnotować, że pominięcie przez ustawodawcę regulacji statuujących zasadę subsydiarności przy pozyskiwaniu danych telekomunikacyjnych przez stosowne służby budzi zasadnicze zastrzeżenia. Tym samym, zarzuty, sformułowane w omawianym zakresie przez Rzecznika Praw Obywatelskich wobec zakwestionowanych przepisów, wydają się uzasadnione.

Jak wspomniano we wcześniejszej części uzasadnienia niniejszego stanowiska, ustawodawca wprost zwolnił funkcjonariuszy ABW, CBA oraz SKW z obowiązku uzyskania zgody sądu na pozyskiwanie danych telekomunikacyjnych (art. 28 ust. 1 ustawy o ABW oraz AW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW oraz SWW). Na pozostałe, wymienione we wniosku Rzecznika Praw Obywatelskich, służby ustawodawca nie nałożył obowiązku uzyskiwania takiej zgody podczas wykonywania omawianych czynności operacyjno - rozpoznawczych. Oznacza to, że działania służb w tym zakresie nie zostały poddane żadnej kontroli ze strony sądu (ani wstępnej, ani nawet następczej), pomimo że ustawodawca wprowadził taką kontrolę w przypadku podejmowania przez służby kontroli operacyjnej, ograniczającej te same prawa i wolności konstytucyjnie chronione, to jest w przypadku podsłuchu (art. 19 ust. 1 ustawy o Policji, art. 9e ust. 1 ustawy o Straży Granicznej, art. 36c ust. 1 ustawy o kontroli skarbowej, art. 31 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 1 ustawy o ABW oraz AW, art. 17 ust. 1 ustawy o CBA, jak również art. 31 ust. 1 ustawy o SKW oraz SWW).

Rezygnując z sądowej kontroli omawianego pozyskiwania i przetwarzania danych telekomunikacyjnych, ustawodawca usunął podstawowy

czynnik gwarancyjny, mający chronić obywateli przed nieuprawnionym wkraczaniem służb w sferę prywatności, swobody komunikowania się i autonomii informacyjnej jednostki. Innymi słowy, jak się wydaje, należałoby podzielić pogląd Rzecznika Praw Obywatelskich, który można wywieść z analizowanego wniosku, iż brak sądowej kontroli pozyskiwania przez służby danych telekomunikacyjnych przesądza o deficycie regulacji gwarancyjnych w zakresie kontroli zewnętrznej omawianej działalności tychże służb.

W tym miejscu wypadałoby odnotować, iż w polskiej rzeczywistości konstytucyjnej ramy kontroli zewnętrznej wyznacza przede wszystkim art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP. Treść art. 77 ust. 2 Konstytucji RP przesądza w zasadzie o tym, że w sprawach dotyczących konstytucyjnych wolności i praw (a więc także w sprawie objętej zakresem art. 49 Konstytucji RP) takim zewnętrznym organem kontroli powinien być sąd.

Wnioskodawca nie zaproponował jednak kontroli zakwestionowanych unormowań w kontekście wzorców zawartych w art. 45 ust. 1 i art. 77 ust. 2 ustawy zasadniczej. Jednakże całkowita rezygnacja z przedstawienia chociażby kilku związanych uwag, dotyczących tego aspektu kwestionowanych we wniosku Rzecznika Praw Obywatelskich unormowań, jak się wydaje, nie byłaby zasadna.

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

W doktrynie przyjmuje się, że zawarte w art. 45 ust. 1 Konstytucji RP „prawo do sądu” oznacza uznanie znaczenia sądu dla ostatecznego określenia statusu prawnego jednostki. Uzasadnieniem dla tego uznania jest – nawiązujący do wykształconego w europejskiej kulturze prawnej – wymóg niezależności, bezstronności i niezawisłości tego organu. Funkcją sądu jest wymierzanie sprawiedliwości (art. 175 ust. 1, art. 177 Konstytucji RP; por. też art. 182

Konstytucji). W kontekście art. 45 ust. 1 Konstytucji RP oznacza to możliwość zwrócenia się w każdej sytuacji (sprawie) do sądu z żądaniem określenia (ustalenia) statusu prawnego jednostki, w sytuacjach nie tylko zakwestionowania lub naruszenia jej praw i wolności, lecz również w sytuacjach odczuwanych przez nią niejasności, niepewności, a zwłaszcza obawy wystąpienia takiego naruszenia. Brak wyszczególnienia w komentowanym artykule sytuacji, w których jednostka mogłaby zaangażować sąd w swojej sprawie, oznacza oczywiście zezwolenie na takie zaangażowanie w każdej sytuacji, według swobodnej jej oceny (por. Paweł Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, III Tom, Wydawnictwo Sejmowe, Warszawa 2003, tezy do art. 45, s. 1 – 2).

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

Z kolei, zakres podmiotowy prawa do sądu został wyznaczony przez konstytucyjne pojęcie „sprawy”. Ustalając znaczenie tego terminu, Trybunał Konstytucyjny wielokrotnie wyrażał pogląd, że urzeczywistnienie konstytucyjnych gwarancji prawa do sądu obejmuje wszystkie sytuacje – bez względu na szczegółowe regulacje proceduralne, w których pojawia się konieczność rozstrzygnięcia o prawach danego podmiotu (w relacji do innych

równorzędnych podmiotów lub relacji do władzy publicznej), a jednocześnie natura danych stosunków prawnych wyklucza arbitralność rozstrzygnięcia o sytuacji prawnej podmiotu przez drugą stronę tego stosunku (por. wyroki: z dnia 10 maja 2000 r., sygn. K 21/99, OTK ZU Nr 4/2000, poz. 109, s. 555, z dnia 18 maja 2004 r., sygn. SK 28/03, OTK ZU Nr 5/A/2004, poz. 45, s. 629 oraz z dnia 11 czerwca 2002 r., sygn. SK 5/02, OTK ZU Nr 4/A/2002, poz. 41, s. 554).

Nadto, wypada odnotować, że w literaturze przedmiotu przyjmuje się, iż natura prawna art. 77 ust. 2 Konstytucji RP jest dwojaka. Z jednej strony, przepis ten wyraża (podmiotowe) „prawo do sądu”, stanowiąc dopełnienie postanowień zawartych w art. 45 ust. 1. Z drugiej strony, zarówno usytuowanie redakcyjne art. 77 ust. 2, jak i jego orientacja na sytuację „naruszenia wolności lub praw” (podobnie zorientowane zostały art. 79 ust. 1 i art. 80), sugerują postrzeganie go jako przepisu gwarancyjnego wobec materialnego prawa do sądu wyrażonego w art. 45 ust. 1. Oba te elementy współistnieją w treści art. 77 ust. 2 (por. Leszek Garlicki, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, V Tom, Wydawnictwo Sejmowe, Warszawa 2007, tezy do art. 77, s. 23 – 24).

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

Problematyka ochrony prywatności, swobody komunikowania się oraz autonomii informacyjnej przed ograniczaniem tych praw konstytucyjnych przez służby mundurowe oraz specjalne poprzez nieuprawnione pozyskiwanie danych

telekomunikacyjnych niewątpliwie stanowi „sprawę” w rozumieniu przytoczonego orzecznictwa Trybunału Konstytucyjnego. W konsekwencji, wszelkie unormowania prawne i pominięcia legislacyjne ze strony ustawodawcy, zmierzające do wyeliminowania sądu z procedury ograniczania wymienionych praw konstytucyjnych, należałoby ocenić zdecydowanie negatywnie.

Regulacje wyłączające konieczność uzyskania zgody sądu na pozyskiwanie danych telekomunikacyjnych, podobnie jak brak regulacji wprowadzających obowiązek uzyskania takiej zgody przez stosowne służby, eliminują podstawowy czynnik gwarancyjny, chroniący jednostkę przed nieuprawnionym wkraczaniem w sferę jej wolności i praw konstytucyjnych. Jak słusznie podniósł w swym wniosku Rzecznik Praw Obywatelskich, analizowane przepisy w sposób wyraźny bądź w sposób wynikający z ich kontekstu normatywnego (udostępnianie danych na pisemny wniosek szefa danej służby, ustne żądanie funkcjonariusza) wyłączają zarówno uprzednią, jak też następczą zgodę sądu na ingerencję służb w konstytucyjną wolność i ochronę tajemnicy komunikowania się.

Wypadałoby nadto zauważyć, że zakwestionowane przepisy, normujące wykonywanie czynności operacyjno – rozpoznawczych, w ogóle pomijają możliwość dokonania przez sąd oceny, czy pozyskiwanie i przetwarzanie przez poszczególne służby danych telekomunikacyjnych spełnia bądź spełniało wymogi legalności, prawidłowości i rzetelności, jak również czy służby, podejmując takie działania, dochowały obowiązujących procedur.

W tym miejscu należy podkreślić, że Europejski Trybunał Praw Człowieka, rozstrzygając sprawę *Klass i inni v. Niemcy*, orzekł między innymi, że, w przypadku gdy państwo ustanawia niejawną kontrolę, której istnienie pozostaje nieznane dla osoby będącej pod taką kontrolą (także po jej zakończeniu), co skutkuje niemożnością odwołania się od jej zarządzenia, stosowanie art. 8 Konwencji może zostać w dużej mierze ograniczone do zera.

Możliwe jest w takiej sytuacji, iż jednostka będzie traktowana w sposób przeciwny do art. 8 lub nawet w ogóle pozbawiona praw gwarantowanych przez art. 8, będąc nieświadomą tego faktu, a co za tym idzie niemającą możliwości zaradzenia temu zarówno na poziomie krajowym, jak i przed instytucjami powołanymi do życia Konwencją (por. wyrok z dnia 6 września 1978 r., 5029/71, System Informacji Prawnej Lex – Lex Omega – 39/2011, Lex nr 80801).

W powołanym wyżej wyroku Europejski Trybunał orzekł również: „Potencjalne pole do nadużyć (przy stosowaniu kontroli niejawnej) w indywidualnych przypadkach jest tak duże i mogłoby przynieść tak dojmujące skutki dla demokratycznego społeczeństwa jako całości, że co do zasady pożądanym jest, aby poddać jej stosowanie nadzorowi sędziego”.

Niezależnie od braku kontroli sądu omawianej sfery działalności służb, należy zdecydowanie zakwestionować brak jakiejkolwiek kontroli zewnętrznej tej działalności. W szczególności, ustawodawca pominął w kwestionowanych unormowaniach jakiejkolwiek regulacje nakładające obowiązek powiadamiania obywatela o pozyskiwaniu dotyczących go danych (choćby po zakończeniu kontroli operacyjnej). Niewątpliwie uniemożliwia to temuż obywatelowi podjęcie jakichkolwiek działań zmierzających do ochrony wspomnianych wolności i praw. Tym samym, czynności operacyjno - rozpoznawcze, w omawianym zakresie, wyłączone zostały również spod jakiejkolwiek kontroli osoby, wobec której są stosowane, a więc podmiotu najbardziej zainteresowanego.

Brak wiedzy o samym fakcie pozyskiwania danych telekomunikacyjnych przez stosowne służby, nawet w przypadku podejrzeń lub wątpliwości co do prawidłowości postępowania tych służb, uniemożliwia samemu zainteresowanemu nie tylko poszukiwanie pomocy u czynników zewnętrznych (sąd, prokurator, Rzecznik Praw Obywatelskich, Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu itp.), ale nawet zwrócenie się

do przełożonych funkcjonariuszy dokonujących czynności operacyjno - rozpoznawczych o zbadanie prawidłowości postępowania ich podwładnych.

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

W końcu, niejako na marginesie, należałoby odnotować, że, pozyskując i przetwarzając dane telekomunikacyjne, służby są wyłączone również spod nadzoru czy choćby kontroli ze strony prokuratora. Ani zakwestionowane przepisy, normujące funkcjonowanie poszczególnych służb, ani żadne inne regulacje ustawowe nie dają prokuraturze żadnych uprawnień w omawianym zakresie, jak również nie nakładają na służby stosownych obowiązków. Przepis § 1 rozporządzenia Ministra Sprawiedliwości z dnia 9 czerwca 2011 r. w sprawie sposobu realizacji kompetencji prokuratora w zakresie nadzoru nad czynnościami operacyjno – rozpoznawczymi (Dz. U. Nr 121, poz. 692) nie przewiduje podejmowania przez prokuratora żadnych czynności kontrolnych lub nadzorczych wobec służb odnośnie pozyskiwania przez nie i przetwarzania danych telekomunikacyjnych. Rzecz jasna, samo ewentualne uzupełnienie przez rozporządzeniodawcę wspomnianego aktu normatywnego, w omawianym zakresie, byłoby wątpliwe wobec brzmienia regulacji ustawowej.

Reasumując tę część rozważań, należy stwierdzić, że ustawodawca, mimo nieracjonalnie szeroko zakreślonych, otwartych, nieprecyzyjnych i często

niedookreślonych katalogów sytuacji, w których służby uzyskały prawo pozyskiwania i przetwarzania danych telekomunikacyjnych, wyłączył – wprost lub na skutek pominięcia prawodawczego – kontrolę sądową, jak również nie przewidział żadnej innej zewnętrznej kontroli ocenianej działalności służb (a nawet poinformowania, choćby po zakończeniu czynności, samego zainteresowanego). Tym samym, brak w zakwestionowanych przepisach jakiegokolwiek regulacji gwarancyjnej, mogącej chronić jednostkę przed ewentualną, potencjalną dowolnością lub arbitralnością decyzji podejmowanych przez służby w zakresie wkraczania w konstytucyjne i konwencyjne prawa i wolności jednostki, co – w kontekście orzecznictwa Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka – należy uznać za niedopuszczalne.

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

Zgodnie z przepisem art. 180 § 1 Kodeksu postępowania karnego, osoby obowiązane do zachowania tajemnicy służbowej lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania tajemnicy. Z kolei § 2 wspomnianego art. 180 stanowi, że osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, lekarskiej lub dziennikarskiej mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być

ustalona na podstawie innego dowodu. W końcu, zgodnie z § 3 tegoż art. 180, zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.

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

W doktrynie przyjmuje się, że zakaz przewidziany w ostatnim przytoczonym wyżej przepisie ma charakter bezwzględny; nie może być uchylony przez organ procesowy, jak również osoby te nie mogą być przesłuchiwane, chociażby chciały lub domagał się tego oskarżony. W ogóle wyłączona jest możliwość przesłuchania tych osób w charakterze świadka. Zakaz trwa także po ustaniu wykonywania obowiązków obrońcy lub duchownego. Zakaz jest skierowany do wszystkich organów procesowych, tj. prowadzących dochodzenie lub śledztwo, jak i do sądu (por. Ryszard Stefański [w:] *Kodeks Postępowania Karnego, Komentarz*, Tom I, Dom Wydawniczy ABC, 2003, s. 786 oraz powołane tam poglądy doktryny).

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

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

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

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

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, konstytucyjne prawo do obrony należy rozumieć szeroko, jest ono bowiem nie

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

Trybunał Konstytucyjny podkreślał również, że proces karny jest ze swej istoty kontradyktoryjny, stanowi on spór równouprawnionych stron przed bezstronnym sądem. W postępowaniu przygotowawczym, którym kieruje prokurator, owa kontradyktoryjność jest w pewnym zakresie ograniczona, co nie oznacza jednak, iż ograniczenia mogą naruszać istotę prawa do obrony. Stąd też zachowane są pewne uprawnienia obrońcy, takie jak: prawo składania wniosków o dokonanie czynności śledztwa lub dochodzenia (art. 315 § 1 Kodeksu postępowania karnego), prawo do udziału w czynnościach niepowtarzalnych (art. 316 § 1 k.p.k.) oraz w innych czynnościach postępowania (art. 317 § 1 k.p.k.), a także prawo udziału w czynnościach zapoznawania podejrzanego z materiałami postępowania przygotowawczego (art. 321 § 3 k.p.k.). Uprawnienia obrońcy to nie tylko możliwość przeglądania akt postępowania karnego – zapoznawania się z materiałem dowodowym, ale przede wszystkim kontakt z jego mocodawcą. To na podstawie osobistego kontaktu obrońca pozyskuje faktyczną wiedzę o czynie sprawcy oraz okolicznościach zdarzenia będącego przedmiotem postępowania, buduje strategię obrony, zgłasza wnioski dowodowe i współdziała z innymi obrońcami

występującymi w sprawie (por. wyrok z dnia 17 lutego 2004 r., sygn. SK 39/02, OTK ZU Nr 2/A/2004, poz. 7, s. 115).

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

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

W szczególności, pominięcie przez ustawodawcę regulacji wyłączających pozyskiwanie przez służby danych telekomunikacyjnych, dotyczących obrońcy podejrzanego lub oskarżonego, może zostać

zinterpretowane – ewentualnie – jako pozostawienie owym służbom możliwości swojego rodzaju „obejścia prawa”, gwarantującego poufność kontaktów tegoż podejrzanego lub oskarżonego z jego obrońcą.

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

Reasumując, należałoby przyjąć, że pominięcie przez ustawodawcę regulacji wyłączających z kręgu podmiotów, których dane telekomunikacyjne mogą być pozyskiwane przez służby, takich kategorii użytkowników telekomunikacyjnych urządzeń końcowych, wobec których niezbędne jest respektowanie tajemnicy notarialnej, adwokackiej, radcy prawnego, lekarskiej lub dziennikarskiej, godzi w powołane w *petitum* wniosku wzorce kontroli. Tym samym, zarzuty sformułowane w omawianym zakresie przez Rzecznika Praw Obywatelskich pod adresem ocenianych unormowań należy uznać za uzasadnione.

Pełna ocena zakwestionowanych przez Wnioskodawcę przepisów ustaw: o Policji, o Straży Granicznej, o kontroli skarbowej, o Żandarmerii Wojskowej i wojskowych organach porządkowych, o ABW oraz AW, o CBA, jak również o SKW oraz SWW nie wydaje się możliwa bez odniesienia się do niektórych – powołanych w tych przepisach, jak również wspomnianych w uzasadnieniu wniosku Rzecznika Praw Obywatelskich – unormowań Prawa telekomunikacyjnego.

W pierwszej kolejności należałoby odnotować, że zastrzeżenia nasuwa nieprecyzyjne sformułowanie zakresu danych telekomunikacyjnych w przepisie art. 180c ust. 1 pkt 1 Prawa telekomunikacyjnego. Jak już wspomniano, zgodnie

ze wspomnianą regulacją, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani, między innymi, zatrzymywać, przechowywać i udostępniać dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest to połączenie. Ustawodawca nie określił jednak w omawianym przepisie wszystkich konkretnych danych użytkownika końcowego podlegających zatrzymaniu, przechowywaniu i udostępnianiu.

Wydaje się, że uprawnione byłoby przypuszczenie, iż ustawodawca zdawał sobie sprawę z niekompletności powyższej regulacji, skoro w art. 180c ust. 2 Prawa telekomunikacyjnego upoważnił ministra właściwego do spraw łączności, by ten, w porozumieniu z ministrem właściwym do spraw wewnętrznych, określił, w drodze rozporządzenia, między innymi szczegółowy wykaz omawianych danych.

Odniesienie się do wspomnianego przepisu art. 180c ust. 2 wymaga, jak się wydaje, przywołania wzorca kontroli zawartego w art. 92 ust. 1 Konstytucji RP. Wprawdzie ocena unormowania byłaby możliwa przy ograniczeniu się do regulacji zawartych w art. 49 w związku z art. 31 ust. 3 zdanie pierwsze ustawy zasadniczej, a także art. 8 ust. 2 Konwencji o ochronie praw człowieka i podstawowych wolności, nakazujących kompletne unormowanie w ustawie wszelkich przejawów ograniczania konstytucyjnych (a w określonym zakresie również chronionych przez Konwencję) praw i wolności jednostki oraz zakazujących wkraczania w sferę tychże praw i wolności w drodze podustawowego aktu normatywnego, jednakże wydaje się, że ocena wspomnianego art. 180c ust. 2 Prawa telekomunikacyjnego byłaby pełniejsza przy uwzględnieniu również art. 92 ust. 1 ustawy zasadniczej.

Zgodnie ze wspomnianym przepisem ustawy zasadniczej, rozporządzenia są wydawane przez organy wskazane w Konstytucji, na podstawie szczegółowego upoważnienia zawartego w ustawie i w celu jej

wykonania. Upoważnienie powinno określać organ właściwy do wydania rozporządzenia i zakres spraw przekazanych do uregulowania oraz wytyczne dotyczące treści aktu.

W literaturze przedmiotu podnosi się, że powiązanie unormowań art. 87 ust. 1 i art. 92 Konstytucji z ogólnymi konsekwencjami zasady demokratycznego państwa prawnego (art. 2 Konstytucji) prowadzi do wniosku, iż nie może obecnie, w systemie prawa powszechnie obowiązującego, pojawiać się żadna regulacja podustawowa, która nie służy wykonaniu ustawy. W tym sensie wyłączność ustawy nabrała pełnego charakteru, bo nie ma takich materii, w których mogłyby być stanowione regulacje podustawowe (o charakterze powszechnie obowiązującym), bez uprzedniego ustawowego unormowania tych materii (por. Jerzy Oniszczyk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Zakamycze 2004, s. 796).

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

Trybunał Konstytucyjny podkreślał również niejednokrotnie, że ustawodawca nie może udzielać upoważnienia do wydania aktu normatywnego, dotyczącego materii zastrzeżonych dla ustawy, które nie zostały uregulowane w danej ustawie. Materie uregulowane w rozporządzeniu muszą być jednorodne

z tymi, które są uregulowane w ustawie. Należy pamiętać, że sprawy przekazane do uregulowania w akcie wykonawczym nie powinny mieć zasadniczego znaczenia z punktu widzenia konstrukcji całej ustawy (por. wyrok z dnia 12 lipca 2007 r., sygn. U 7/06, OTK ZU Nr 7/A/2007, poz. 76, s. 1029 – 1030 oraz powołane tam orzecznictwo).

W świetle utrwalonego orzecznictwa Trybunału Konstytucyjnego, wykonawczy charakter rozporządzenia determinuje treść upoważnienia do jego wydania. Upoważnienie to musi być sformułowane w taki sposób, aby odsyłało do unormowania tylko takich spraw, które są przedmiotem ustawy i które służą realizacji tych samych celów, jakie znajdują wyraz w przepisach ustawy. Dlatego przepisy ustawy upoważniającej, a w szczególności przepis upoważniający, powinny wyznaczać co najmniej w sposób ogólny, lecz jednocześnie dostatecznie wyraźny, kierunek unormowań, które mają nastąpić w drodze rozporządzenia. Nie można bowiem wykonywać w drodze rozporządzenia tego, co nie zostało uregulowane w ustawie (por. wyrok z dnia 31 marca 2009 r., sygn. K 28/08, OTK ZU Nr 3/A/2009, poz. 28, s. 300 oraz powołane tam orzecznictwo).

W końcu, Trybunał Konstytucyjny, w swoich orzeczeniach, zwracał szczególną uwagę na to, że nakaz zamieszczania wszystkich zasadniczych elementów regulacji prawnej bezpośrednio w ustawie, połączony z zakazem regulowania ich w rozporządzeniu, jako akcie podustawowym, dotyczy zwłaszcza materii odnoszącej się do praw i wolności jednostki lub do władczych form działania władzy publicznej wobec obywateli. Wymaganie umieszczenia bezpośrednio w tekście ustawy wszystkich zasadniczych elementów regulacji prawnej musi być stosowane ze szczególnym rygoryzmem, gdy regulacja ta dotyczy władczych form działania organów administracji publicznej wobec obywateli, praw i obowiązków organu administracji i obywatela w ramach stosunku publicznoprawnego lub korzystania przez obywateli z ich praw i wolności (por. wyrok, wydany w pełnym składzie Trybunału, z dnia 10 marca

2010 r., sygn. U 5/07, OTK ZU Nr 3/A/2010, poz. 20, s. 347 oraz powołane tam orzecznictwo).

Wydane na podstawie upoważnienia ustawowego, zawartego w art. 180c ust. 2 Prawa telekomunikacyjnego, rozporządzenie Ministra Infrastruktury w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, deklaruje w § 1, że określa, między innymi, szczegółowy wykaz danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, jak również ustalenie zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie. Pozostałe dane wymienione w przepisie (określenie daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, jak również lokalizacji telekomunikacyjnego urządzenia końcowego) stanowią powtórzenie regulacji zawartych w art. 180c ust. 1 pkt 2 Prawa telekomunikacyjnego.

Wspomniane wyżej wykazy danych, odrębnie dla stacjonarnej publicznej sieci telekomunikacyjnej, ruchomej publicznej sieci telekomunikacyjnej, usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej, zostały określone, odpowiednio, w przepisach § 3 – 7 omawianego rozporządzenia. Powyższe dane dotyczą nie tylko parametrów technicznych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, w postaci numeru zakończenia stacjonarnej publicznej sieci telefonicznej, z którego inicjowane jest połączenie lub do którego kierowane jest połączenie (§ 3 pkt 1 lit. a oraz pkt 2 lit. a), numeru przydzielonego użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej, użytkownika końcowego inicjującego połączenie lub do którego kierowane jest połączenie (§ 4 pkt 1 lit. a oraz pkt 2 lit. a), międzynarodowego numeru przydzielonego karcie identyfikacyjnej użytkownika w ruchomej

publicznej sieci telefonicznej, użytkownika końcowego, inicjującego połączenie lub do którego kierowane jest połączenie (§ 4 pkt 1 lit. c oraz pkt 2 lit. c), pierwsze 14 cyfr indywidualnego międzynarodowego numeru identyfikującego telekomunikacyjne urządzenie końcowe, używane w ruchomej publicznej sieci telefonicznej lub międzynarodowego numeru przydzielonego karcie identyfikującej użytkownika w ruchomej sieci telefonicznej, urządzenia końcowego, inicjującego połączenie lub do którego kierowane jest połączenie (§ 4 pkt 1 lit. d oraz pkt 2 lit. d), numeru przydzielonego użytkownikowi końcowemu, korzystającemu z dostępu do sieci Internet za pośrednictwem publicznej sieci telefonicznej (§ 6 pkt 1 lit. b), numeru przydzielonego użytkownikowi końcowemu, do którego jest kierowane połączenie w telefonii internetowej (§ 7 pkt 1 lit. a) itp. Omawiane dane obejmują również imię i nazwisko albo nazwę oraz adres użytkownika końcowego (§ 3 pkt 1 lit. b oraz pkt 2 lit. b, § 4 pkt 1 lit. b oraz pkt 2 lit. b, § 5, § 6 pkt 1 lit. e, § 7 pkt 1 lit. b).

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

Zgodnie z wyrokiem Naczelnego Sądu Administracyjnego z dnia 18 listopada 2009 r., sygn. I OSK 667/09, dane osobowe to zespół wiadomości (komunikatów) o konkretnym człowieku na tyle zintegrowany, że pozwala na jego zindywidualizowanie. Obejmuje co najmniej informacje niezbędne do

identyfikacji (imię, nazwisko, miejsce zamieszkania), jednakże do tego się nie ogranicza, bowiem mieszczą się w nim również dalsze informacje, wzmacniające stopień identyfikacji (por. LEX nr 588798, System Informacji Prawnej Lex – Lex Omega – 20/2011).

Omawiany we wcześniejszej części uzasadnienia niniejszego stanowiska przepis art. 180c ust. 1 pkt 1 Prawa telekomunikacyjnego nakazuje operatorom publicznej sieci telekomunikacyjnej oraz dostawcom publicznie dostępnych usług telekomunikacyjnych udostępnianie uprawnionym służbom, między innymi, danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest połączenie. Regulacja ta nie wymienia wprost, wśród wspomnianych danych, ani imienia i nazwiska, ani adresu użytkownika końcowego. Skoro powyższe dane objęte są tajemnicą telekomunikacyjną, to obowiązek udostępniania imienia i nazwiska oraz adresu użytkownika końcowego nie może być dorozumiany, ale winien wynikać wprost z ustawy. Tym samym, upoważnienia zawartego w art. 180c ust. 2 Prawa telekomunikacyjnego, jak się wydaje, nie należy traktować jako upoważnienia do uzupełnienia (poprawienia) ustawy poprzez zobowiązanie operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych do dostarczania stosownym służbom danych obejmujących imię i nazwisko oraz adres użytkownika końcowego korzystającego ze wspomnianych sieci lub usług, skoro ustawodawca nie był uprawniony przez ustrojodawcę do cedowania swoich uprawnień prawotwórczych w omawianym zakresie.

Tym samym, należałoby odnotować, że sam sposób unormowania zakresu danych telekomunikacyjnych, pozyskiwanych i przetwarzanych przez służby mundurowe oraz specjalne, zdaje się budzić wątpliwości, tak na gruncie ustawy zasadniczej, jak i na gruncie art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

Reasumując, należałoby stwierdzić, że zakwestionowane przez Wnioskodawcę przepisy godzą w prawo do prywatności, swobodę komunikowania się, autonomię informacyjną oraz prawo do sądu poprzez brak precyzji, niedookreśloność i niepełność przyjętych regulacji, brak zasady subsydiarności wkraczania przez właściwe służby w sferę konstytucyjnych praw i wolności jednostki, brak sądowej kontroli pozyskiwania danych telekomunikacyjnych przez służby, brak regulacji o powiadamianiu zainteresowanych o prowadzonej wobec nich kontroli operacyjnej (choćby po zakończeniu tej kontroli), jak również brak respektowania tajemnicy zawodowej wskazanych kategorii osób oraz związanych z tym zakazów dowodowych.

Rzecznik Praw Obywatelskich ograniczył propozycję kontroli kwestionowanych unormowań przez Trybunał Konstytucyjny do wzorców podanych w *petitum* swego wniosku. Tym samym, należy stwierdzić, że przepisy: art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, jak również art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego są niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

III.

Zakwestionowany przez Rzecznika Praw Obywatelskich przepis art. 36b ust. 5 ustawy o kontroli skarbowej ma następujące brzmienie:

„Art. 36b. 5. Minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych

od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, o którym mowa w ust. 2, za nieuzasadnione.”.

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu brzmi następująco:

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

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

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

- 1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ;
- 2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW;
- 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2.

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

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

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

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

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

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

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

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

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich

współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem.

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

1) sieć ta zapewnia:

- a) możliwość ustalenia funkcjonariusza CBA uzyskującego te dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
- b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do uzyskanych danych;

2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne CBA albo prowadzonych przez nie czynności.”.

Zakwestionowany we wniosku Rzecznika Praw Obywatelskich przepis art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ma następujące brzmienie:

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

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

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

- 1) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej;
- 2) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW;

3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW.

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

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

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

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

1) wykorzystywane sieci i system teleinformatyczny zapewniają:

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

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

Przechodząc do oceny zakwestionowanych przez Rzecznika Praw Obywatelskich unormowań w kontekście zasady autonomii informacyjnej, określonej w art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP, należałoby podkreślić, że w pełni zachowują tu aktualność wywody zawarte we wcześniejszej części uzasadnienia niniejszego stanowiska, odnośnie konstytucyjnych i konwencyjnych standardów wiążących ustawodawcę

przyjmującego regulacje określające podejmowanie przez służby czynności operacyjno – rozpoznawczych. Podobnie zachowują aktualność wywody dotyczące rozróżnienia zaniechania ustawodawczego i pominięcia prawodawczego.

Problemem związanym z brakiem ograniczeń w zakresie pozyskiwania przez służby danych telekomunikacyjnych jest kwestia usuwania przez te służby danych, o których mowa w art. 180c, jak również w art. 180d Prawa telekomunikacyjnego. Szczątkowe regulacje, w omawianym zakresie, zawierają ustawy: o Policji (art. 20c ust. 7), o Straży Granicznej (art. 10b ust. 6), o kontroli skarbowej (art. 36b ust. 5) oraz o Żandarmerii Wojskowej i wojskowych organach porządkowych (art. 30 ust. 6). Natomiast Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne ani Służba Kontrwywiadu Wojskowego nie zostały zobligowane przez ustawodawcę do niszczenia, w jakiegokolwiek sytuacji, pozyskanych danych telekomunikacyjnych.

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

Z kolei, w myśl art. 36b ust. 5 ustawy o kontroli skarbowej – co należy przypomnieć – minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną, w przypadku, gdy uzna wystąpienie z wnioskiem o przekazanie tych danych za nieuzasadnione. Wspomniana regulacja nie przewiduje więc zniszczenia danych, jeżeli nie

zawierają one informacji mających znaczenie dla prowadzonego przez organ skarbowy postępowania (nie mówiąc już o danych pozyskanych nieprawidłowo), lecz tylko wtedy, gdy sam wniosek o ich udostępnienie został uznany przez ministra za niezasadny. Tym samym, ustawodawca dopuścił sytuację, gdy sam wniosek o udostępnienie danych był uzasadniony, zaś zgromadzone w wyniku jego realizacji dane nie zostaną zniszczone, mimo że nie mają one znaczenia dla prowadzonego postępowania.

W końcu brak jakichkolwiek regulacji, dotyczących niszczenia materiałów, zgromadzonych przez funkcjonariuszy ABW, CBA lub SKW w toku kontroli operacyjnej, w zakresie pozyskiwania danych telekomunikacyjnych, należałoby uznać za możliwość – przynajmniej potencjalną – ukształtowania się zakwestionowanej przez Trybunał Konstytucyjny w przytoczonym we wcześniejszej części uzasadnienia niniejszego stanowiska orzecznictwie, praktyki zbierania i przetrzymywania przez służby mundurowe i specjalne najrozmaitszych informacji nie tylko „koniecznych w demokratycznym państwie” dla ochrony wykazanych w ustawie zasadniczej wartości, ale również „wygodnych” lub „użytecznych” dla tychże służb. Powyższy stan prawny narusza więc literę Konstytucji RP, która, w art. 51 ust. 2, wyraźnie zakazuje wszelkim władzom publicznym pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach, niż niezbędne w demokratycznym państwie prawnym.

W tym miejscu, niejako na marginesie, wypadałoby odnotować, że w powołanej już sprawie *Rotaru v. Rumunia*, Europejski Trybunał Praw Człowieka stanął na stanowisku, iż zarówno przechowywanie danych związanych z życiem prywatnym osoby fizycznej, jak i używanie ich, a także odmowa przyznania możliwości sprostowania spowodzają się do ingerencji w prawo poszanowania życia prywatnego chronionego w art. 8 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności (*vide* – wyrok z dnia 4 maja 2000 r., 28341/95, *op. cit.*). Podobne stanowisko zajął Trybunał również

we wspominatej wyżej sprawie *Leander v. Szwecja* (*vide* – wyrok z dnia 26 marca 1987 r., 9248/81, *op. cit.*).

Należy zatem uznać, że zakwestionowane przez Rzecznika Praw Obywatelskich unormowania: 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, jak również 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 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 RP.

Z tych wszystkich względów, wnoszę jak na wstępie.

z upoważnienia
Prokuratora Generalnego
Robert Hermand
Zastępcę Prokuratora Generalnego