

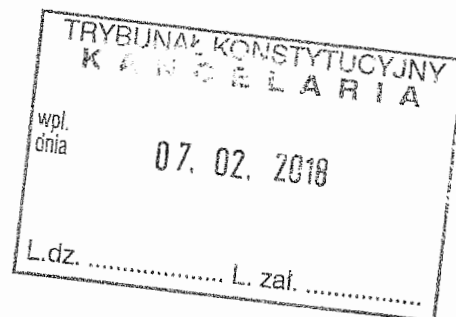


Warszawa, dnia 6 lutego 2018 r.

Rzeczpospolita Polska
PROKURATOR GENERALNY

PK VIII TK 42.2016

K 9/16



TRYBUNAŁ KONSTYTUCYJNY

W związku z wnioskiem Rzecznika Praw Obywatelskich „o stwierdzenie niezgodności:

I.

- art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355 ze zm.),
- art. 9e ust. 10 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r., poz. 1402 ze zm.),
- art. 36c ust. 7 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r., poz. 553 ze zm.),
- art. 31 ust. 10 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r., poz. 568 ze zm.),
- art. 17 ust. 9 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r., poz. 1411 ze zm.)
- w zakresie, w jakim umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy - z art. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP;

II.

- art. 19 ust. 15h ustawy z dnia 6 kwietnia 1990 r. o Policji,
- art. 9e ust. 16h ustawy z dnia 12 października 1990 r. o Straży Granicznej,
- art. 36d ust. 1h ustawy z dnia 28 września 1991 r. o kontroli skarbowej,
- art. 31 ust. 16h ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- art. 31 ust. 14h ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
- art. 17 ust. 15h ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym
- w zakresie, w jakim posługują się nieostrym kryterium <dobra wymiaru sprawiedliwości> i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 Kodeksu postępowania karnego - z art. 2 Konstytucji RP, z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP oraz z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności;

III.

- art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji,
- art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej,
- art. 36b ust. 1 oraz art. 36bb ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej,
- art. 30 ust. 1 oraz art. 30c ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- art. 28 ust. 1 oraz art. 28b ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

- art. 32 ust. 1 oraz art. 32b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
 - art. 18 ust. 1 oraz art. 18b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,
 - art. 75d ust. 1 oraz art. 75db ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej,
- z art. 2, 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE;

IV.

- art. 20c ust. 3 w zw. z art. 20c ust. 2 ustawy o Policji,
 - art. 10b ust. 3 w zw. z art. 10b ust. 2 ustawy o Straży Granicznej,
 - art. 36b ust. 3 w zw. z art. 36b ust. 2 ustawy o kontroli skarbowej,
 - art. 30 ust. 3 w zw. z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
 - art. 28 ust. 3 w zw. z art. 28 ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
 - art. 32 ust. 5 w zw. z art. 32 ust. 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
 - art. 18 ust. 3 w zw. z art. 18 ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym,
 - art. 75d ust. 3 w zw. z art. 75d ust. 2 ustawy o Służbie Celnej
- z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

V.

- art. 20ca ustawy o Policji,
- art. 10ba ustawy o Straży Granicznej,
- art. 36ba ustawy o kontroli skarbowej,
- art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

- art. 28a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
 - art. 32a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
 - art. 18a ustawy o Centralnym Biurze Antykorupcyjnym,
 - art. 75da ustawy o Służbie Celnej
 - w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych - z art. 2, 47, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE;
- VI.
- art. 20c ustawy o Policji,
 - art. 10b ustawy o Straży Granicznej,
 - art. 36b ustawy o kontroli skarbowej,
 - art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,
 - art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
 - art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
 - art. 18 ustawy o Centralnym Biurze Antykorupcyjnym,
 - art. 75d ustawy o Służbie Celnej
 - w zakresie, w jakim przepisy te nie wskazują kategorii osób, których dane mogą być pozyskiwane w sposób określony w ustawach, nie regulują obowiązków informacyjnych wobec osób, których dane były pozyskiwane oraz nie określają czasu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane - z art. 2, 30, 47, 49, 51 ust. 2, 3 i 4 w zw. z art. 31 ust. 3 Konstytucji, z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE;

VII.

- art. 28 ust. 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- art. 32 ust. 9 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego
- w zakresie, w jakim nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych, niemających znaczenia dla prowadzonego postępowania karnego - z art. 51 ust. 2 Konstytucji w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE;

VIII.

Art. 13 oraz art. 16 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147)

- w zakresie, w jakim nakazują stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11 - z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP”

- na podstawie art. 42 pkt 7 oraz art. 63 ust. 1 ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U., poz. 2072) w związku z art. 9 ust. 1 ustawy z dnia 13 grudnia 2016 r. - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego (Dz. U., poz. 2074) -

przedstawiam następujące stanowisko:

- 1) art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity - Dz. U. z 2017 r., poz. 2067 ze zm.), art. 9e ust. 10 ustawy z dnia 12

października 1990 r. o Straży Granicznej (tekst jednolity - Dz. U. z 2016 r., poz. 1643 ze zm.), art. 31 ust. 10 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jednolity - Dz. U. z 2016 r., poz. 1483 ze zm.) oraz art. 17 ust. 9 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jednolity - Dz. U. z 2017 r., poz. 1993 ze zm.) – w zakresie, w jakim przepisy te umożliwiają prowadzenie kontroli operacyjnej przez okres 18 miesięcy – nie są niezgodne z zasadą zaufania obywateli do państwa i stanowionego przez nie prawa, wynikającą z art. 2 Konstytucji Rzeczypospolitej Polskiej;

2) art. 19 ust. 15h powołanej w pkt 1 ustawy o Policji, art. 9e ust. 16h powołanej w pkt 1 ustawy o Straży Granicznej, art. 31 ust. 16h powołanej w pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity - Dz. U. z 2017 r., poz. 1920 ze zm.), art. 31 ust. 14h ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jednolity - Dz. U. z 2017 r., poz. 1978 ze zm.) i art. 17 ust. 15h powołanej w pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym – w zakresie, w jakim posługują się pojęciem „dobro wymiaru sprawiedliwości” i nie zawierają kryteriów podkreślających wagę i istotność dla postępowania karnego okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 180 § 2 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (tekst jednolity - Dz. U. z 2017 r., poz. 1904), nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 tego Kodeksu, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (tekst jednolity - Dz. U. z 2017 r., poz. 2204) – są zgodne z art. 2 Konstytucji RP;

3) przepisy:

a) art. 20c ust. 1 w związku z art. 20ca powołanej w pkt 1 ustawy o Policji, w części odnoszącej się do zapobiegania lub wykrywania przestępstw,

b) art. 10b ust. 1 w związku z art. 10ba powołanej w pkt 1 ustawy o Straży Granicznej,

c) art. 30 ust. 1 w związku z art. 30b powołanej w pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 tej ustawy,

d) art. 28 ust. 1 w związku z art. 28a powołanej w pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

e) art. 32 ust. 1 w związku z art. 32a powołanej w pkt 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

f) art. 18 ust. 1 w związku z art. 18a powołanej w pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym
są zgodne z art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 i z art. 30 Konstytucji RP oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962 oraz z 2003 r. Nr 42, poz. 364), a także z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej (Dz. U. UE. C. 2007.303.1 ze zm.);

4) art. 20c ust. 1 powołanej w pkt 1 ustawy o Policji, art. 10b ust. 1 powołanej w pkt 1 ustawy o Straży Granicznej, art. 30 ust. 1 powołanej w pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 powołanej w pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 powołanej w pkt 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu

Wojskowego i art. 18 ust. 1 powołanej w pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym – w zakresie, w jakim treść tych przepisów zawiera odwołanie do pojęcia „dane internetowe” – są zgodne z art. 2 Konstytucji RP;

5) przepisy:

a) art. 20cb ust. 1 powołanej w pkt 1 ustawy o Policji, w części odnoszącej się do zapobiegania lub wykrywania przestępstw,

b) art. 10bb ust. 1 powołanej w pkt 1 ustawy o Straży Granicznej,

c) art. 30c ust. 1 powołanej w pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 tej ustawy,

d) art. 28b ust. 1 powołanej w pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

e) art. 32b ust. 1 powołanej w pkt 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

f) art. 18b ust. 1 powołanej w pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym

są zgodne z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji RP, a także są zgodne z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE;

6) art. 20c ust. 3 w związku z art. 20c ust. 2 powołanej w pkt 1 ustawy o Policji, art. 10b ust. 3 w związku z art. 10b ust. 2 powołanej w pkt 1 ustawy o Straży Granicznej, art. 30 ust. 3 w związku z art. 30 ust. 2 powołanej w pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 3 w związku z art. 28 ust. 2 powołanej w pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 5 w

związku z art. 32 ust. 2 powołanej w pkt 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego i art. 18 ust. 3 w związku z art. 18 ust. 2 powołanej w pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym są zgodne z art. 20 w związku z art. 31 ust. 3 Konstytucji RP oraz nie są niezgodne z art. 2, art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP;

7) art. 28 ust. 7 powołanej w pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i art. 32 ust. 9 powołanej w pkt 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego – w zakresie, w jakim przepisy te nie przewidują zniszczenia danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, które są istotne dla obronności i bezpieczeństwa państwa – są zgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a także z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE;

8) art. 13 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U., poz. 147) jest zgodny z art. 2 i art. 190 ust. 1 i 3 Konstytucji RP;

9) postępowanie w przedmiocie kontroli zgodności z powołanymi wzorcami art. 36b, art. 36c ust. 7, art. 36d ust. 1h, art. 36ba oraz art. 36bb ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (tekst jednolity - Dz. U. z 2016 r., poz. 720 ze zm.), jak również przepisów art. 75d, art. 75da oraz art. 75db ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (tekst jednolity - Dz. U. z 2016 r., poz. 1799 ze zm.), a także art. 16 powołanej w pkt 9 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw – w zakresie, w jakim przepis ten zezwala na dalsze stosowanie do kontroli operacyjnej, niezakończonych do dnia 7 lutego 2016 r., art. 27 ust. 1 w związku art. 5 ust. 1 pkt 2 lit. b ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, mimo iż moc obowiązująca tego

unormowania, w brzmieniu, którego dotyczy zakwestionowany przepis ustawy zmieniającej z dnia 15 stycznia 2016 r., wygasła przed wejściem w życie tej ustawy zmieniającej na skutek wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11 – podlega umorzeniu na podstawie art. 59 ust. 1 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U., poz. 2072) w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego (Dz. U., poz. 2074), wobec utraty przez zakwestionowane przepisy mocy obowiązującej przed wydaniem orzeczenia przez Trybunał;

10) w pozostałym zakresie postępowanie podlega umorzeniu na podstawie art. 59 ust. 1 pkt 2 ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy z dnia 13 grudnia 2016 r. - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego, wobec niedopuszczalności wydania orzeczenia.

UZASADNIENIE

Rzecznik Praw Obywatelskich (dalej również: Wnioskodawca, Rzecznik lub RPO) wniósł do Trybunału Konstytucyjnego o stwierdzenie niezgodności (w całości albo w określonym zakresie) przepisów:

- art. 19 ust. 9 i ust. 15h, art. 20c, art. 20ca oraz art. 20cb ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity - Dz. U. z 2017 r., poz. 2067 ze zm.) [dalej: ustawa o Policji];

- art. 9e ust. 10 i ust. 16h, art. 10b, art. 10ba oraz art. 10bb ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (tekst jednolity - Dz. U. z 2016 r., poz. 1643 ze zm.) [dalej: ustawa o Straży Granicznej];

- art. 36b, art. 36ba, art. 36bb ust. 1, art. 36c ust. 7 oraz art. 36d ust. 1h ustawy z dnia 28 września 1991 r. o kontroli skarbowej (tekst jednolity - Dz. U. z 2016 r., poz. 720 ze zm.) [dalej: ustawa o kontroli skarbowej];

- art. 30, art. 30b, art. 30c ust. 1 oraz art. 31 ust. 10 i ust. 16h ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jednolity - Dz. U. z 2016 r., poz. 1483 ze zm.) [dalej: ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych];

- art. 17 ust. 9 i ust. 15h, art. 18, art. 18a oraz art. 18b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jednolity - Dz. U. z 2017 r., poz. 1993 ze zm.) [dalej: ustawa o CBA];

- art. 27 ust. 15j, art. 28, art. 28a oraz art. 28b ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity - Dz. U. z 2017 r., poz. 1920 ze zm.) [dalej: ustawa o ABW oraz AW];

- art. 31 ust. 14h, art. 32, art. 32a oraz art. 32b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jednolity - Dz. U. z 2017 r., poz. 1978 ze zm.) [dalej: ustawa o SKW oraz SWW];

- art. 75d, art. 75da oraz art. 75db ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (tekst jednolity - Dz. U. z 2016 r., poz. 1799 ze zm.) [dalej: ustawa o Służbie Celnej];

- art. 13 oraz art. 16 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U., poz. 147)

z powołanymi w *petitum* wniosku wzorcami konstytucyjnej kontroli, a także z art. 6 i art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej protokołem nr 2 (Dz. U. z 1993 r. Nr

61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962 oraz z 2003 r. Nr 42, poz. 364) [dalej: EKPCz lub Konwencja] oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej (Dz. U. UE. C. 2007.303.1 ze zm. (dalej: Karta Praw Podstawowych UE).

Na wstępie należy odnotować, iż w dniu 1 marca 2017 r. ustawa o kontroli skarbowej oraz ustawa o Służbie Celnej utraciły moc obowiązującą i, równocześnie (tego samego dnia), weszła w życie ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2016 r., poz. 1947 ze zm., dalej: ustawa o Krajowej Administracji Skarbowej) [*vide* - art. 1 i art. 159 pkt 1 i 3 w związku z art. 260 ustawy z dnia 16 listopada 2016 r. - Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej, Dz. U. z 2016 r., poz. 1948 ze zm., dalej: ustawa - Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej].

Problematyka utraty mocy obowiązującej aktu normatywnego przed wydaniem orzeczenia przez Trybunał Konstytucyjny była szeroko omawiana w orzecznictwie Trybunału.

W jednym z najnowszych poświęconych tej problematyce orzeczeń - w postanowieniu z dnia 5 kwietnia 2016 r., w sprawie o sygn. akt K 3/15, Trybunał Konstytucyjny stwierdził, że „*[u]morzenie postępowania ze względu na utratę mocy obowiązującej aktu normatywnego stanowi trwałe element kontroli konstytucyjności prawa w Polsce. (...)*

Rozwiązanie to odpowiada ogólnym funkcjom Trybunału i założeniom dotyczącym jego kognicji jako organu powołanego do badania hierarchicznej zgodności aktów normatywnych. Wyznacza też zasadę, wedle której kontroli zgodności z Konstytucją podlegają akty zachowujące moc obowiązującą i wyznaczające określonym podmiotom (adresatom tych norm) odpowiednie reguły postępowania w oznaczonych okolicznościach (...). W aspekcie funkcjonalnym <instytucja «umarzania postępowania» odwołuje się do reguł ekonomii

działania, [które] można przełożyć na ogólne zalecenie (...), aby za pomocą odpowiedniej organizacji pracy (...) organ uwalniał się od merytorycznego rozpatrywania spraw, których kontynuowanie - z uwagi na okoliczności faktyczne lub prawne - a priori i tak nie doprowadzi do zrealizowania celu postępowania> (P. Radziewicz, Umarzanie postępowania przez Trybunał Konstytucyjny ze względu na utratę mocy obowiązującej przepisu przed wydaniem orzeczenia, <Przegląd Sejmowy> nr 2/2006, s. 9 i n. [...]). [...]

*Analiza orzecznictwa Trybunału pozwala wysnuć wniosek, że **ocena - prowadzącej do umorzenia postępowania - utraty mocy obowiązującej aktu normatywnego dokonuje się nie na podstawie formalnego stwierdzenia wyeliminowania kontrolowanego przepisu z systemu prawa, lecz z perspektywy możliwości wywołania przezeń skutków prawnych** (podkr. wł.). Innymi słowy, <wykładnia zwrotu «akt normatywny utracił moc obowiązującą» (...) powinna zmierzać do oceny, czy zaskarżona norma prawna została usunięta z porządku prawnego nie tylko w sensie formalnoprawnym, lecz także w tym zakresie, czy uchylony przepis nadal wywiera określone skutki dla obywateli i czy może być nadal zastosowany w praktyce> (postanowienie z 13 października 1998 r., sygn. SK 3/98; zob. także postanowienia TK z: 18 listopada 1998 r., sygn. SK 1/98, OTK ZU nr 7/1998, poz. 120; 30 grudnia 1999 r., sygn. SK 16/99, OTK ZU nr 7/1999, poz. 173). Trwałości tej linii orzeczniczej nie podważyło ani uchwalenie Konstytucji, ani ustawy o TK.*

Przenosząc powyższe spostrzeżenia na grunt rozpoznawanej sprawy, Trybunał uznał za spełnioną ujemną przesłankę procesową wskazaną w art. 39 ust. 1 pkt 3 ustawy o TK z 1997 r. (obecnie przesłanka ta jest określona w art. 59 ust. 1 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym - przyp. wł.). Zaskarżony art. 18 ust. 1 pkt 3 prawa energetycznego (przepis ten stanowił przedmiot zaskarżenia w skierowanym do Trybunału Konstytucyjnego wniosku Rady Miejskiej w C. - przyp. wł.), wskutek nowelizacji z 2015 r. (chodzi o ustawę z dnia 27 maja 2015 r. o zmianie ustawy -

Prawo energetyczne, Dz. U. z 2015 r., poz. 942 - przyp. wł.), *utracił moc obowiązującą. Mówiąc precyzyjniej, norma prawna, której zgodność z Konstytucją zakwestionowano, została definitywnie usunięta z porządku prawnego i zastąpiona normą o nowej treści (nowym brzmieniu). Przepis w poprzednio obowiązującej wersji nie może być - jako wyłączony z porządku prawnego - przedmiotem oceny Trybunału Konstytucyjnego (...). Oceniając ewentualną możliwość zastosowania zakwestionowanej regulacji do sytuacji z przeszłości, teraźniejszości lub przyszłości, Trybunał przyjął, że nowelizacja z 2015 r. nie przewidywała miarodajnej normy intertemporalnej, która pozwalałaby twierdzić, iż art. 18 ust. 1 pkt 3 prawa energetycznego w poprzednim brzmieniu, zachował moc obowiązującą* (podkr. wł.). Nowa regulacja weszła w życie po 30 dniach od ogłoszenia, tj. 3 sierpnia 2015 r., i od tego dnia jest stosowana jako jedyna, z wyłączeniem art. 18 ust. 1 pkt 3 prawa energetycznego w jego dotychczasowym kształcie, stanowiącym przedmiot wniosku” (OTK ZU seria A z 2016 r., poz. 7).

Podobnie jak w rozpoznanej przez Trybunał Konstytucyjny sprawie, zainicjowanej wnioskiem Rady Miejskiej w C. (sygn. akt K 3/15), także w sprawie wniosku Rzecznika Praw Obywatelskich brak jest miarodajnej normy intertemporalnej, która pozwalałaby twierdzić, iż przepisy: art. 36b, art. 36c ust. 7, art. 36d ust. 1h, art. 36ba oraz art. 36bb ust. 1 ustawy o kontroli skarbowej, jak również przepisy: art. 75d, art. 75da oraz art. 75db ust. 1 ustawy o Służbie Celnej zachowały moc obowiązującą. W tej sytuacji należy przyjąć, że nowa regulacja weszła w życie z dniem 1 marca 2017 r. i od tego dnia jest stosowana jako jedyna, z wyłączeniem art. 36b, art. 36c ust. 7, art. 36d ust. 1h, art. 36ba oraz art. 36bb ust. 1 ustawy o kontroli skarbowej, jak również z wyłączeniem art. 75d, art. 75da oraz art. 75db ust. 1 ustawy o Służbie Celnej w ich kształcie stanowiącym przedmiot wniosku.

Tak więc, wskutek wejścia w życie ustawy o Krajowej Administracji Skarbowej i równoczesnej utraty mocy obowiązującej ustawy o kontroli

skarbowej oraz ustawy o Służbie Celnej, przepisy: art. 36b, art. 36c ust. 7, art. 36d ust. 1h, art. 36ba oraz art. 36bb ust. 1 ustawy o kontroli skarbowej, jak również przepisy: art. 75d, art. 75da oraz art. 75db ust. 1 ustawy o Służbie Celnej utraciły moc obowiązującą (normy prawne, których zgodność z Konstytucją zakwestionowano, zostały definitywnie usunięte z porządku prawnego i zastąpione normami o nowej treści [nowym brzmieniu]).

W związku z powyższym postępowanie w przedmiocie kontroli zgodności z Konstytucją art. 36b, art. 36c ust. 7, art. 36d ust. 1h, art. 36ba oraz art. 36bb ust. 1 ustawy o kontroli skarbowej, jak również przepisów art. 75d, art. 75da oraz art. 75db ust. 1 ustawy o Służbie Celnej, jako przepisów wskazanych w *petitum* wniosku Rzecznika Praw Obywatelskich, na podstawie art. 59 ust. 1 pkt 4 ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U., poz. 2072) [dalej: ustawa o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym] w związku z art. 9 ust. 1 ustawy z dnia 13 grudnia 2016 r. - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego (Dz. U., poz. 2074) [dalej: ustawa - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego] - wobec utraty przez wskazane wyżej zaskarżone przepisy mocy obowiązującej „przed wydaniem orzeczenia przez Trybunał”.

I. Zarzut niezgodności art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o Straży Granicznej, art. 31 ust. 10 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych i art. 17 ust. 9 ustawy o CBA w zakresie, w jakim umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy - z art. 2, art. 47, art. 49, art. 51 ust. 2 w

związku z art. 31 ust. 3 Konstytucji (pkt I *petitum* wniosku Rzecznika Praw Obywatelskich).

Zakwestionowane przepisy, których treść jest podobna, regulują problematykę czasu trwania kontroli operacyjnej i stanowią, że kontrola operacyjna może być przedłużana ponad podstawowy 6 - miesięczny okres jej trwania, jeżeli podczas stosowania kontroli w tym okresie pojawiły się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa. W takich przypadkach sąd może wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, na pisemny wniosek:

- Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego (ustawa o Policji),
- Komendanta Głównego Straży Granicznej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego albo komendanta oddziału Straży Granicznej złożony po uzyskaniu pisemnej zgody właściwego prokuratora okręgowego (ustawa o Straży Granicznej),
- Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej oraz właściwego prokuratora do spraw wojskowych (ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych),
- Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego (ustawa o CBA).

Zaskarżone przepisy stanowią więc, że kontrola operacyjna może być stosowana przez okres nieprzekraczający łącznie 18 miesięcy.

W ocenie Wnioskodawcy, uregulowany w zaskarżonych przepisach czas stosowania kontroli operacyjnej jest nieproporcjonalnie długi, przez co, w pierwszej kolejności, narusza zasadę demokratycznego państwa prawnego, a

przede wszystkim - wynikającą z niej zasadę zaufania obywateli do państwa oraz zasadę praworządności.

W uzasadnieniu tego zarzutu Rzecznik Praw Obywatelskich stwierdził, że „[j]ak się wydaje, zasadę zaufania obywateli do państwa należy pojmować jeszcze szerzej. Składa się na nią nie tylko właściwy formalnie proces stanowienia prawa, wprowadzenie *vacatio legis* i stabilność prowadzonej wykładni. Zasadę lojalności urzeczywistnia się już na etapie kształtowania treści przepisów. Nie sposób utrzymać relację zaufania i lojalności, jeżeli państwo kształtuje swoje kompetencje w sposób poważnie ingerujący w wolności i prawa obywateli, nie wskazując granic korzystania z tych kompetencji, lub wyznaczając granice przekraczające zasadę proporcjonalności. Problem ten jest zauważalny w kontekście wskazywanym w niniejszym wniosku. Przekazanie obywatelom komunikatu, że mogą być inwigilowani przez służby policyjne i służby państwowe przez osiemnaście miesięcy z pewnością nie buduje relacji zaufania między państwem i obywatelami. Zasadniczy wpływ na problemy w tej relacji ma także to, że obywatel nie zostanie, choćby następczo, poinformowany o prowadzonych wobec niego czynnościach kontroli operacyjnej. Informacja nie zostanie przekazana nawet wtedy, gdy nie wykryto żadnych okoliczności mogących uzasadniać pierwotne podejrzenia, które spowodowały złożenie wniosku do sądu i rozpoczęcie kontroli operacyjnej. Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. (w sprawie o sygn. akt K 23/11, OTK ZU seria A nr 7/2014, poz. 80 - przyp. wł.) dopuścił zróżnicowanie standardów przeprowadzania kontroli operacyjnej, zwłaszcza jeżeli prowadzona jest ona przez służby odpowiadające za bezpieczeństwo państwa. Nie oznacza to jednak, że państwo może zupełnie porzucić wynikający ze standardów praw człowieka wymóg określenia maksymalnego okresu prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek. Okres ten mógłby być dłuższy niż w przypadku pozostałych służb, ale powinien być określony.

Biorąc powyższe pod uwagę, w przekonaniu Rzecznika Praw Obywatelskich określony w przepisach czas prowadzenia czynności z zakresu kontroli operacyjnej przekracza ramy konieczne w demokratycznym państwie prawa.

Możliwość stosowania kontroli operacyjnej przez tak długi okres budzi poważne wątpliwości z perspektywy wolności i praw człowieka. Konieczne jest zatem zrekonstruowanie katalogu dóbr, w które ustawodawca ingeruje, a także kolidujących z nimi dóbr mogących uzasadniać wprowadzoną regulację. Ostateczne rozstrzygnięcie tak ukształtowanej kolizji jest możliwe na podstawie art. 31 ust. 3 Konstytucji, a więc z wykorzystaniem zasady proporcjonalności” (uzasadnienie wniosku, s. 19-20).

Wypowiadając się następnie o dopuszczalności ingerencji w prawa i wolności gwarantowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, w świetle kryteriów wynikających z art. 31 ust. 3 ustawy zasadniczej, statuującego wymóg proporcjonalności ograniczenia konstytucyjnych praw i wolności jednostki, Rzecznik, po przedstawieniu bogatego orzecznictwa Trybunału Konstytucyjnego na gruncie art. 31 ust. 3 Konstytucji, stwierdził, że, w Jego ocenie, kwestionowane przepisy „w zakresie, w jakim ustalają czas trwania kontroli operacyjnej łącznie na osiemnaście miesięcy nie spełniają kryterium konieczności. Także zasada proporcjonalności *sensu stricto* będzie zachowana tylko, gdy ingerencja w prawa i wolności będzie odbywała się w rozsądnych ramach czasowych. Trudno jest przyjąć, że służby policyjne i służby specjalne potrzebują aż osiemnastu miesięcy na zebranie materiałów uzasadniających wszczęcie postępowania karnego. Należy pamiętać, że Kodeks postępowania karnego także przewiduje możliwość stosowania środków z zakresu kontroli operacyjnej, prowadzonej już jednak w sposób obudowany gwarancjami procesowymi, w reżimie procedury karnej” (uzasadnienie wniosku, s. 27).

Jako wzorce kontroli zaskarżonych norm Rzecznik wskazał, wynikające z art. 2 Konstytucji, zasadę zaufania obywateli do państwa i stanowionego przez

nie prawa oraz zasadę praworządności, a także gwarantowane w art. 47 Konstytucji prawo do prywatności, wyrażoną w art. 49 ustawy zasadniczej wolność komunikowania się oraz przewidziany w art. 51 ust. 2 Konstytucji zakaz pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym - w związku z art. 31 ust. 3 Konstytucji.

Prawa i wolności jednostki, zadekretowane w art. 2, art. 47, art. 49 i w art. 51 ust. 2 Konstytucji, zostały szczegółowo opisane przez Rzecznika Praw Obywatelskich w uzasadnieniu wniosku, w oparciu o utrwalone, cytowane tamże, orzecznictwo Trybunału Konstytucyjnego, nie ma zatem potrzeby ponownie określać ich treści.

Konieczne wydaje się tylko przypomnienie, wypracowanego w orzecznictwie Sądu Konstytucyjnego na gruncie art. 31 ust. 3 Konstytucji, mechanizmu kontroli konstytucyjności ograniczenia praw i wolności jednostki.

Pośród licznych wypowiedzi Trybunału Konstytucyjnego, odnoszących się do wzorca kontroli z art. 31 ust. 3 Konstytucji, za reprezentatywną uznać można tę, która została zawarta w uzasadnieniu wyroku z dnia 29 września 2008 r., w sprawie o sygn. akt SK 52/05, gdzie Trybunał stwierdził, że *„[z]awarta w art. 31 ust. 3 Konstytucji zasada proporcjonalności w aspekcie formalnym wymaga, aby ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw wprowadzane były w formie ustawy, co wyklucza wprowadzanie ich w aktach niższej rangi. Zasada ta w aspekcie materialnym dopuszcza ustanawianie tylko takich ograniczeń, które nie naruszają istoty danej wolności lub prawa podmiotowego, i tylko wtedy, gdy istnieje konieczność ich wprowadzenia w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia, moralności publicznej, albo wolności i praw innych osób. Zakres wprowadzanych ograniczeń powinien być proporcjonalny, tzn. konieczny dla realizacji określonego celu (...). W związku z tym wprowadza się trzy kryteria: przydatności, konieczności i proporcjonalności*

przyjmowanych ograniczeń (...). Ingerencja taka jest zatem dopuszczalna, jeżeli jest w stanie doprowadzić do zamierzonych przez nią skutków, jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana, a jej efekty pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela” (OTK ZU seria A nr 7/2008, poz. 125).

Podsumowując wywody zawarte w uzasadnieniu wyroku w sprawie o sygn. akt SK 52/05, Trybunał Konstytucyjny stwierdził, że ograniczenia wolności i praw jednostki ze względu na ochronę wartości wyliczonych w art. 31 ust. 3 Konstytucji bądź wskazanych w szczegółowych przepisach ustawy zasadniczej „*muszą (...) czynić zadość zasadzie proporcjonalności. Jak wskazał Trybunał Konstytucyjny we wcześniejszym orzecznictwie <przesłanka «konieczności ograniczenia w demokratycznym państwie» z jednej strony stawia przed prawodawcą każdorazowo wymóg stwierdzenia rzeczywistej potrzeby dokonania ingerencji w danym stanie faktycznym, z drugiej zaś - winna być rozumiana jako wymóg stosowania środków prawnych skutecznych (rzeczywiście służących realizacji zamierzonych celów), ale tylko tych niezbędnych (chroniących określone wartości w sposób bądź w stopniu nieosiągalnym przy zastosowaniu innych środków). Owa niezbędność oznacza również nakaz stosowania środków jak najmniej uciążliwych dla podmiotów, których prawa lub wolności ulegną ograniczeniu, bo ingerencja w sferę statusu jednostki musi pozostawać w racjonalnej i odpowiedniej proporcji do celów, których ochrona uzasadnia dokonane ograniczenie (...). Wprowadzenie ograniczeń wymaga ponadto ich uzasadnienia, przede wszystkim wskazania innej wartości konstytucyjnej, dla której prawo zostało «poświęcone» lub ograniczone (...). Podsumowując, z naruszeniem kryterium «konieczności» zastosowania ograniczenia mamy do czynienia, gdy osiągnięcie danego celu było możliwe poprzez zastosowanie innego środka, nakładającego mniejsze ograniczenia na prawa i wolności jednostki, tymczasem sięgnięto po środek bardziej uciążliwy (...)>” (op. cit.).*

W wyroku z dnia 10 grudnia 2013 r., w sprawie o sygn. akt U 5/13, Sąd Konstytucyjny, formułując ponownie wymogi zasady proporcjonalności, przypomniał, że zasada ta *„jest rozumiana przez Trybunał Konstytucyjny jako suma trzech zasad składowych: zasady przydatności, zasady konieczności oraz zasady proporcjonalności sensu stricto, tzn. zakazu nadmiernej ingerencji (por. wyrok z 11 kwietnia 2000 r., sygn. K. 15/98, OTK ZU nr 3/2000, poz. 86 i wiele innych). Zasada przydatności polega na przeprowadzeniu testu racjonalności instrumentalnej, tzn. ustaleniu, czy według dostępnego stanu wiedzy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków. Zasada konieczności wymaga oceny, czy badane przepisy są niezbędne dla ochrony dóbr wskazanych w art. 31 ust. 3 Konstytucji (pięciu dóbr ogólnospołecznych lub indywidualnych <wolności i praw innych osób>), a ponadto czy spośród środków skutecznie chroniących te wartości zostały wybrane środki najmniej uciążliwe. Zasada proporcjonalności sensu stricto wymaga zaś ustalenia, czy efekty zaskarżonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela”* (OTK ZU seria A nr 9/2013, poz. 136).

Odnosząc się do kwestii naruszenia przez kwestionowane przepisy, w zaskarżonym zakresie, zasady praworządności (art. 2 Konstytucji), i to zarówno w aspekcie formalnym, jak i materialnym (Wnioskodawca nie wyodrębnia żadnego z tych dwóch aspektów), należy zauważyć, iż powołanie art. 2 ustawy zasadniczej jako wzorca kontroli konstytucyjności w takim aspekcie nie jest właściwe.

Zasadę praworządności, ale tylko w jej aspekcie formalnym, rozumianą jako działanie organów władzy publicznej na podstawie i w granicach prawa, wyraża nie art. 2, lecz art. 7 Konstytucji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 13 stycznia 2004 r., w sprawie o sygn. akt SK 10/03, OTK ZU seria A nr 1/2004, poz. 2; uzasadnienie postanowienia TK z dnia 21 czerwca 2012 r., w sprawie o sygn. akt Ts 260/10, OTK ZU seria B nr 6/2012, poz. 504

oraz komentarz W. Sokolewicz do art. 7 Konstytucji, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom V, Wydawnictwo Sejmowe, Warszawa 2007, s. 6).

Z kolei, w uzasadnieniu wyroku z dnia 6 marca 2012 r., w sprawie o sygn. akt K 15/08, Trybunał Konstytucyjny, odnosząc się do kwestii kontroli zgodności przepisu prawa z zasadą praworządności materialnej, przypomniał, że „na tę zasadę powoływano się wielokrotnie przed uchwaleniem Konstytucji z 1997 r. Jak stwierdził Trybunał w orzeczeniu z 30 listopada 1988 r. o sygn. K 1/88, <[z]asada praworządności materialnej wymaga, by prawo wyrażało wartości odpowiadające demokratycznemu charakterowi państwa. Zgodnie z brzmieniem art. 8 ust. 1 Konstytucji prawa Polskiej Rzeczypospolitej Ludowej mają być «wyrazem interesów i woli ludu pracującego». Konstytucja odsyła zatem do najbardziej podstawowych wartości uznawanych przez ustrojodawcę państwa socjalistycznego za godne realizacji i ochrony z punktu widzenia ogólnospołecznego; są nimi interes i wola ludu pracującego> (OTK w 1988 r., poz. 6). Z zasady praworządności materialnej wpisanej do Konstytucji PRL <rozwinęła się> zasada demokratycznego państwa prawnego, która jednocześnie - wyrażając wartości wolnościowe i demokratyczne - stanowi zaprzeczenie tamtej, przynależnej do instrumentarium ideologicznego państwowości socjalistycznej (...). Konsekwentnie klauzula <praworządności materialnej> nie występuje w orzecznictwie Trybunału Konstytucyjnego po wejściu w życie Konstytucji z 1997 r.” (OTK ZU seria A nr 3/2012, poz. 24).

W konsekwencji, postępowanie w sprawie kontroli zgodności zaskarżonych norm z zasadą praworządności (formalnej i materialnej), **jako zasadą wywodzoną z art. 2 Konstytucji**, podlega umorzeniu na podstawie art. 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym

oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Nie wydaje się też prawidłowe uzasadnienie przez Wnioskodawcę zarzutu naruszenia przez zaskarżone normy zasady zaufania obywateli do państwa i stanowionego przez nie prawa, wynikającej z zasady demokratycznego państwa prawnego (art. 2 Konstytucji).

Rzecznik Praw Obywatelskich zarzut, iż art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o Straży Granicznej, art. 31 ust. 10 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 17 ust. 9 ustawy o CBA - w zakresie, w jakim przepisy te umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy - naruszają zasadę zaufania obywateli do państwa i stanowionego przez nie prawa, uzasadnia - cytowanym już wcześniej - stwierdzeniem, że „[n]ie sposób utrzymać relację zaufania i lojalności, jeżeli państwo kształtuje swoje kompetencje w sposób poważnie ingerujący w wolności i prawa obywateli, nie wskazując granic korzystania z tych kompetencji, lub wyznaczając granice przekraczające zasadę proporcjonalności” (uzasadnienie wniosku, s 19).

Niewątpliwie określona w powołanych wyżej przepisach kompetencja organów państwa, polegająca na prowadzeniu kontroli operacyjnej, *per se* poważnie ingeruje w wolności i prawa obywateli. Jednak - wbrew ocenie Rzecznika - przepisy te wyznaczają już granice (w tym przypadku - granice czasowe) korzystania z tych kompetencji.

Zarzut niezgodności owych granic z zasadą proporcjonalności nie może natomiast zostać zbadany z punktu widzenia wynikającej z art. 2 Konstytucji zasady zaufania obywateli do państwa i stanowionego przez nie prawa, skoro wymóg proporcjonalnego (dopuszczalnego) ograniczenia konkretnych, określonych w ustawie zasadniczej, praw i wolności jednostki formułuje inny

przepis Konstytucji - art. 31 ust. 3. Zresztą w tym zakresie (proporcjonalność ograniczeń) sam Wnioskodawca sformułował odrębny zarzut pod adresem zaskarżonych regulacji z uwzględnieniem treści normatywnej art. 31 ust. 3 Konstytucji.

Należy przypomnieć, na co trafnie - w oparciu o utrwalone orzecznictwo Trybunału Konstytucyjnego - zwrócił uwagę Rzecznik Praw Obywatelskich, że zasada zaufania obywateli do państwa i stanowionego przez nie prawa opiera się na wymaganiu pewności prawa, a więc takim zespole cech przysługujących prawu, które zapewniają jednostce bezpieczeństwo prawne; umożliwiają jej decydowanie o swoim postępowaniu na podstawie pełnej znajomości przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie jej działania mogą pociągnąć za sobą (*vide* - uzasadnienie wniosku, s. 19). Zachowanie proporcjonalności, wprowadzonych przez ustawodawcę, ograniczeń w gwarantowanych w Konstytucji prawach i wolnościach jednostki wykracza zatem poza rzeczywistą treść zasady zaufania obywateli do państwa i stanowionego przez nie prawa, co jednocześnie oznacza, że, w zakresie tej zasady, art. 2 Konstytucji nie jest w niniejszej sprawie odpowiednim (adekwatnym) wzorcem kontroli zaskarżonych norm. Na marginesie można jedynie dodać, że zaskarżone przepisy należałoby uznać za zgodne z zasadą ochrony zaufania obywateli do państwa i stanowionego przez nie prawa - w przytoczonym wyżej rozumieniu tej zasady wypracowanym w orzecznictwie Trybunału Konstytucyjnego i w dorobku doktryny. RPO nie sformułował jednak zarzutu dotyczącego naruszenia tego aspektu zasady lojalności państwa wobec obywateli, jak bywa też określana zasada ochrony zaufania obywateli do państwa i stanowionego przez nie prawa (*vide* na przykład - uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 9 marca 2017 r., w sprawie o sygn. akt P 13/14, OTK ZU seria A z 2017 r., poz. 14).

Reasumując tę część rozważań, należy stwierdzić, że art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o Straży Granicznej, art. 31 ust. 10 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 17 ust. 9 ustawy o CBA - w zakresie, w jakim przepisy te umożliwiają prowadzenie kontroli operacyjnej przez okres 18 miesięcy - nie są niezgodne z zasadą zaufania obywateli do państwa i stanowionego przez nie prawa, wynikającą z art. 2 Konstytucji.

Analizę zarzutu naruszenia przez wymienione w tej części wniosku Rzecznika Praw Obywatelskich przepisy, w zaskarżonym zakresie, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji należy rozpocząć od stwierdzenia Rzecznika, iż nie ma On wątpliwości co do tego, że kwestionowane normy stanowią niedopuszczalną ingerencję w prawo rekonstruowane z art. 47, jak również że budzą one poważne wątpliwości w świetle art. 49 i art. 51 ust. 2 Konstytucji (*vide* - uzasadnienie wniosku, s. 24 - 25).

Badając dopuszczalność ingerencji w prawa gwarantowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, w świetle kryteriów wynikających z art. 31 ust. 3 ustawy zasadniczej statuującego wymóg proporcjonalności ograniczenia konstytucyjnych praw i wolności jednostki, Rzecznik stwierdził, że, w Jego ocenie, kwestionowane przepisy w zakresie, w jakim ustalają czas trwania kontroli operacyjnej łącznie na osiemnaście miesięcy, są niezgodne z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, dlatego że:

- „nie spełniają kryterium konieczności” ,
- „zasada proporcjonalności *sensu stricto* będzie zachowana tylko, gdy ingerencja w prawa i wolności będzie odbywała się w rozsądnych ramach czasowych”,
- „[t]rudno jest przyjąć, że służby policyjne i służby specjalne potrzebują aż osiemnastu miesięcy na zebranie materiałów uzasadniających wszczęcie postępowania karnego”,

- „[n]ależy pamiętać, że Kodeks postępowania karnego także przewiduje możliwość stosowania środków z zakresu kontroli operacyjnej, prowadzonej już jednak w sposób obudowany gwarancjami procesowymi, w reżimie procedury karnej” (uzasadnienie wniosku, s. 27).

Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, wniosek inicjujący hierarchiczną kontrolę norm musi spełniać wymogi określone w przepisach o postępowaniu przed Trybunałem Konstytucyjnym. Wnioskodawca powinien określić zarzut niezgodności z Konstytucją, wskazać przedmiot i wzorce kontroli oraz sformułować uzasadnienie. Wymogów tych nie spełniają uwagi nazbyt ogólne, niejasne czy też czynione jedynie na marginesie innych rozważań. Ciężar dowodu spoczywa na podmiocie kwestionującym zgodność ustawy z Konstytucją i dopóki nie powoła on konkretnych i przekonujących argumentów prawnych na rzecz swojej tezy, dopóty Trybunał Konstytucyjny uznawać będzie kontrolowane przepisy za konstytucyjne. W przeciwnym razie Trybunał przekształciłby się w organ orzekający z inicjatywy własnej. Trybunał nie może wyręczać wnioskodawcy w doborze argumentacji właściwej do podnoszonych wątpliwości lub - wychodząc poza granice określone we wniosku - całkowicie modyfikować podstaw kontroli (*vide* na przykład - wyrok Trybunału Konstytucyjnego z dnia 5 czerwca 2014 r., w sprawie o sygn. akt K 35/11, OTK ZU seria A nr 6/2014, poz. 61 oraz postanowienie Trybunału Konstytucyjnego z dnia 15 października 2009 r. w sprawie o sygn. akt P 120/08, OTK ZU seria A nr 9/2009, poz. 143).

W powołanym wyżej postanowieniu z dnia 15 października 2009 r. Trybunał Konstytucyjny przypominał też, iż *„jest związany treścią oraz granicami rozpatrywanego pytania prawnego. Nie może też - wychodząc poza granice określone w pytaniu - wyręczać sądu pytającego w doborze argumentacji adekwatnej do podnoszonych w pytaniu prawnym wątpliwości. Brak adekwatnego uzasadnienia zarzutu niezgodności (...) [przepisu prawa - przyp. wł.] ze wskazanymi w pytaniu wzorcami Konstytucji stanowi o uchybieniu przez pytający*

sąd ustawowej powinności określonej w art. 32 ust. 1 pkt 4 ustawy o TK (chodzi o ustawę z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym, Dz. U. Nr 102, poz. 643 ze zm.; dalej: ustawa o Trybunale Konstytucyjnym z dnia 1 sierpnia 1997 r. - przyp. wł.)” [op. cit.].

Uzupełniając trzeba dodać, że przepis art. 32 ust. 1 pkt 4 ustawy o Trybunale Konstytucyjnym z dnia 1 sierpnia 1997 r. został zastąpiony (w zakresie wniosków) przez art. 47 ust. 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, zaś zasada związania Trybunału przy orzekaniu granicami wniosku, pytania prawnego lub skargi konstytucyjnej została powtórzona w przepisie art. 67 ust. 1 i 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, przy czym obowiązek określenia granic wniosku, pytania prawnego bądź skargi konstytucyjnej zastąpiono obowiązkiem wskazania tamże zakresu zaskarżenia, obejmującego wskazanie kwestionowanego aktu normatywnego lub jego części (określenie przedmiotu kontroli) oraz obowiązkiem sformułowania zarzutu niezgodności z Konstytucją, ratyfikowaną umową międzynarodową lub ustawą (wskazanie wzorca kontroli).

Ponadto, w orzecznictwie Trybunału Konstytucyjnego konsekwentnie przyjmuje się, iż niedochowanie wymogów formalnych wniosku przez Rzecznika Praw Obywatelskich może stanowić przyczynę umorzenia postępowania (*vide* na przykład - postanowienia Trybunału Konstytucyjnego: z dnia 21 stycznia 2015 r., w sprawie o sygn. akt K 13/13, OTK ZU seria A nr 1/2015, poz. 8 oraz z dnia 13 stycznia 2015 r., w sprawie o sygn. akt K 44/13, OTK ZU seria A nr 1/2015, poz. 4).

Powracając na grunt przedmiotowej sprawy należy stwierdzić, że uzasadnienie przez Rzecznika Praw Obywatelskich zarzutu naruszenia przez wymienione w tej części wniosku przepisy, w zaskarżonym zakresie, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji **nie jest wystarczające**.

Uzasadnienie to nie spełnia bowiem określonych w art. 47 ust. 2 pkt 2 i 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym wymogów, jakim powinno odpowiadać uzasadnienie wniosku, kierowanego do Trybunału Konstytucyjnego przez podmiot, wymieniony w art. 191 ust. 1 pkt 1-5 Konstytucji, w tym także przez Rzecznika Praw Obywatelskich (uzasadnienie powinno zawierać przywołanie treści wzorców kontroli wraz z ich wykładnią [pkt 2] oraz wskazanie argumentów lub dowodów na poparcie zarzutu niekonstytucyjności [pkt 4]).

Przed wszystkim Rzecznik, formułując zarzut naruszenia art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, po uprzednim przywołaniu stosownego orzecznictwa Trybunału Konstytucyjnego, **nie przeprowadził prawidłowo testu proporcjonalności**. Należy w związku z tym przypomnieć (*vide* - cytowany wcześniej fragment uzasadnienia wyroku Trybunału Konstytucyjnego z dnia 10 grudnia 2013 r., w sprawie o sygn. akt U 5/13), że test ten wymaga wykazania, iż prawodawca, ograniczając prawa i wolności gwarantowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, uchybił:

- 1) wymogowi przydatności, który polega na przeprowadzeniu testu racjonalności instrumentalnej, tzn. ustaleniu, czy według dostępnego stanu wiedzy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków, albo
- 2) wymogowi konieczności, który oznacza ocenę, czy badane przepisy są niezbędne dla ochrony dóbr wskazanych w art. 31 ust. 3 Konstytucji (pięciu dóbr ogólnospołecznych lub indywidualnych „wolności i praw innych osób”), a ponadto czy spośród środków skutecznie chroniących te wartości zostały wybrane środki najmniej uciążliwe, albo
- 3) wymogowi proporcjonalności *sensu stricto*, który należy rozumieć jako ustalenie, czy efekty zaskarżonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela.

W tym kontekście twierdzenie Wnioskodawcy, że zaskarżone regulacje „nie spełniają kryterium konieczności” należy uznać za przedwczesne.

Ponadto, wydaje się, że Wnioskodawca czerpie przekonanie o niekonstytucyjności zaskarżonych regulacji **z własnej oceny**, iż przewidziane tamże ramy czasowe ingerencji w prawa i wolności konstytucyjne jednostki **nie są rozsądne** (w tym, że owe ramy czasowe nie są rozsądne, Rzecznik upatruje braku respektowania wymogu proporcjonalności *sensu stricto*), ponieważ, w Jego opinii, służby powołane do ochrony bezpieczeństwa państwa i porządku publicznego **nie potrzebują aż osiemnastu miesięcy** na zebranie materiałów uzasadniających wszczęcie postępowania karnego.

Tego rodzaju oceny Wnioskodawca nie poparł jednak żadnym dowodem.

Nie wiadomo więc, jakie ramy czasowe kontroli operacyjnej byłyby dla Wnioskodawcy rozsądne i dlaczego.

W szczególności, wniosek Rzecznika nie zawiera dowodu na to, że efektywne przeprowadzenie kontroli operacyjnej przez służby powołane do ochrony bezpieczeństwa państwa i porządku publicznego (kontroli realizującej cel, dla którego została ona podjęta) jest zawsze (a przynajmniej - w przeważającej zdecydowanie mierze) możliwe w terminie krótszym niż osiemnaście miesięcy.

W związku z powyższym należy stwierdzić, że, wobec konieczności respektowania generalnej zasady, jaką jest domniemanie konstytucyjności aktu normatywnego, samo wskazanie w *petitum* wniosku wzorca kontroli, bez szczegółowego odniesienia się w uzasadnieniu do kwestionowanej regulacji prawnej, lub lakoniczne sformułowanie zarzutu niekonstytucyjności nie może zostać uznane za „uzasadnienie zarzutu niezgodności przedmiotu kontroli ze wskazanym wzorcem kontroli, z powołaniem argumentów lub dowodów na jego poparcie”, w rozumieniu przepisów regulujących postępowanie przez Trybunałem Konstytucyjnym.

Z tych też względów postępowanie w sprawie kontroli zgodności art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o Straży Granicznej, art. 31 ust. 10 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych i art. 17 ust. 9 ustawy o CBA w zakresie, w jakim przepisy te umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy, z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Na marginesie należy zauważyć, iż w uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, zwracając uwagę, że jednym z koniecznych elementów „ustawowej regulacji czynności operacyjno-rozpoznawczych niejawnego pozyskiwania przez władze publiczne informacji o jednostkach” jest sprecyzowanie w ustawie maksymalnego czasu „*prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne*”, stwierdził, iż „*[n]ie jest rolą Trybunału Konstytucyjnego, jako sądu prawa, określanie, jak długi ma być to termin. Termin ten ma określić ustawodawca tak, aby umożliwiał osiągnięcie konstytucyjnie uzasadnionego celu. Nie może być to jednak termin ani nadmiernie długi, ani zbyt krótki, który nie pozwala na efektywną pracę operacyjno-rozpoznawczą* (podkr. wł.). Ustawodawca musi mieć także na uwadze, że w demokratycznym państwie prawa nie jest dopuszczalne - nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw - prowadzenie czynności

operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów” (op. cit.).

II. Zarzut niezgodności art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA w zakresie, w jakim „posługują się nieostrym kryterium <dobra wymiaru sprawiedliwości> i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 Kodeksu postępowania karnego” - z art. 2, art. 42 ust. 2, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji oraz z art. 6 EKPCz (pkt II *petitum* wniosku Rzecznika Praw Obywatelskich).

Zaskarżone, a zawarte w poszczególnych ustawach regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego, przepisy, których treść jest podobna, wprowadzają mechanizm nakładający na sądy obowiązek wydania postanowienia w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k., nieobjęte zakazami określonymi w art. 178a i art. 180 § 3 k.p.k., z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 k.k., zawsze wtedy, gdy jest to niezbędne ze względu na **dobro wymiaru sprawiedliwości**, a okoliczność ta nie może być ustalona na podstawie innego dowodu, na wniosek:

- Prokuratora Generalnego (ustawa o ABW oraz AW, ustawa SKW oraz SWW i ustawa o CBA),
- prokuratora (ustawa o Policji i ustawa o Straży Granicznej),

- prokuratora do spraw wojskowych (ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych) [*vide* - art. 19 ust. 15f pkt 2 w związku z art. 19 ust. 15g pkt 2 i art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16f pkt 2 w związku z art. 9e ust. 16g pkt 2 i art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16f pkt 2 w związku z art. 31 ust. 16g pkt 2 i art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15h pkt 2 w związku z art. 27 ust. 15i pkt 2 i art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14f pkt 2 w związku z art. 31 ust. 14g pkt 2 i art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15f pkt 2 w związku z art. 17 ust. 15g pkt 2 i art. 17 ust. 15h ustawy o CBA].

Jednocześnie we wszystkich zaskarżonych przepisach zobowiązano sąd do zarządzenia niezwłocznego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

W ocenie Rzecznika Praw Obywatelskich, zaskarżone regulacje „zdają się naruszać w sposób rażący” wyrażoną w art. 2 zasadę demokratycznego państwa prawnego.

Wnioskodawca zwrócił uwagę, że „[j]akkolwiek uregulowanie (...) art. 180 § 2 k.p.k. przewiduje pewien mechanizm łagodzący ingerencję w tajemnicę zawodową poprzez uprzednią kontrolę zasadności takiej ingerencji przez sąd, już na gruncie tego przepisu w nauce prawa karnego podniesiono wiele wątpliwości. W literaturze wielokrotnie wskazywano, że znaczenie społeczne tajemnicy, o której mowa w 180 § 2 k.p.k. wymaga wprowadzenia dodatkowych kryteriów podkreślających wagę i istotność informacji ujawnionych w procesie karnym (D. Gruszecka, *Komentarz do art. 180 Kodeksu postępowania karnego* [w:] *Kodeks postępowania karnego. Komentarz*, Warszawa 2015, s. 420).

W tym kontekście decyzja ustawodawcy o wprowadzeniu abstrakcyjnej wartości w postaci dobra wymiaru sprawiedliwości jako kryterium dopuszczalności wykorzystania w postępowaniu karnym informacji uzyskanych za pomocą naruszenia tajemnicy zawodowej powinna budzić duży niepokój.

Zagrożenie dla ochrony praw i wolności jednostki potęguje dodatkowo fakt, że ustawodawca nie zdecydował się na dokładniejsze określenie wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 k.p.k.” (uzasadnienie wniosku, s. 31).

Rzecznik podniósł, że „[o]becny stan prawny zdaje się stwarzać pole do nieskrepowanej ograniczeniami formalnymi dowolności w zakresie ingerencji w informacje objęte tajemnicą zawodową podmiotów obdarzonych wysokim zaufaniem ze strony społeczeństwa. Tymczasem Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (K 23/11) wyraźnie wskazał, że zbieranie informacji niejawnych może być uzasadnione tylko na potrzeby pociągnięcia do odpowiedzialności karnej za poważne przestępstwa i zagrożenia dla bezpieczeństwa państwa”, a następnie stwierdził, iż „[n]iedookreśloność wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje objęte tajemnicą zawodową oraz abstrakcyjność pojęcia <dobro wymiaru sprawiedliwości> naruszają w sposób rażący konstytucyjną zasadę zaufania do państwa. Omawiane uregulowania nie przewidują bowiem żadnych mechanizmów zabezpieczających ich prawa i wolności. Istota czynności operacyjno-rozpoznawczych przekreśla możliwość informowania osób będących obiektem takich działań i właśnie dlatego podstawowym obowiązkiem państwa w tym zakresie jest ustanowienie sprawnego mechanizmu swoistej samokontroli jego organów i ochrony jednostki przed działaniami inwigilacyjnymi. Skoro ingerencja w prawa i wolności jednostki *ex definitione* ma się odbywać bez jej wiedzy, to rolą państwa jako gwaranta przestrzegania jej praw i wolności jest ustanowienie kontrolnego mechanizmu za pomocą organu niezależnego od innych podmiotów państwa zainteresowanych uzyskaniem informacji wskutek inwigilacji” (uzasadnienie wniosku, s. 31-32).

W dalszej części uzasadnienia zarzutu sformułowanego w pkt II *petitum* wniosku Rzecznik Praw Obywatelskich stwierdził, że „[w]ykorzystanie na

potrzeby postępowania karnego informacji objętych tajemnicą zawodową na podstawie wyjątkowo nieostrych kryteriów staje się szczególnie niebezpieczne z punktu widzenia ochrony praw i wolności jednostki w zakresie informacji objętych tajemnicą zawodową niektórych zawodów prawniczych. Mechanizm pozyskiwania takich informacji za pomocą czynności operacyjno-rozpoznawczych prowadzonych w stosunku do adwokatów oraz radców prawnych może prowadzić do rażącego naruszenia jednego z fundamentalnych praw jednostki w państwie prawa, jakim jest prawo do obrony (art. 42 ust. 2 Konstytucji RP). W świetle art. 6 ust. 1 ustawy z dnia 26 maja 1982 r. - Prawo o adwokaturze (t.j. Dz. U. z 2015 r., poz. 615) [aktualny tekst jednolity - Dz. U. z 2016 r., poz. 1999 ze zm., dalej: ustawa - Prawo o adwokaturze - przyp. wł.]: <Adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej>. Z kolei zgodnie z art. 3 ust. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2015 r., poz. 507) [aktualny tekst jednolity - Dz. U. z 2017 r., poz. 1870, dalej: ustawa o radcach prawnych - przyp. wł.]: <Radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej>. **Ze względu na fundamentalne znaczenie tajemnicy adwokackiej oraz radcowskiej dla sytuacji prawnej osób, których bezpośrednio dotyczą informacje objęte tajemnicą, konieczne jest wprowadzenie szczegółowo określonych wymagań co do trybu oraz przesłanek uchylenia obowiązku zachowania takiej tajemnicy (podkr. wł.). Tymczasem procedura przewidziana w art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, (...) art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 14h ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz w art. 17 ust. 15h ustawy o Centralnym Biurze Antykorupcyjnym zdaje się nie spełniać żadnego z wyżej wymienionych wymogów. Sama ingerencja w tajemnicę zawodową odbywa**

się bowiem w warunkach braku jakiegokolwiek mechanizmu kontrolnego. Równie niepokojący jest fakt, że weryfikacja możliwości wykorzystania informacji objętych tajemnicą zawodową na potrzeby postępowania karnego odbywa się na podstawie nieostrego kryterium dobra wymiaru sprawiedliwości (podkr. wł.). Abstrakcyjność tego kryterium sprawia, że sąd, rozstrzygając w przedmiocie dopuszczalności wykorzystania takich informacji zobowiązany jest do każdorazowego ważenia dwóch wartości - jednostkowego prawa do obrony oraz kolektywnego dobra wymiaru sprawiedliwości. Pomijając trafność kolektywistyczno-objektywnego ujęcia dobra wymiaru sprawiedliwości, można przypuszczać, że kolizja ww. dóbr niemalże zawsze powinna być rozstrzygnięta na korzyść dobra ponadindywidualnego mającego znaczenie dla sprawnego funkcjonowania całego aparatu państwowego” (uzasadnienie wniosku, s. 32-34).

W końcowym fragmencie tej części uzasadnienia wniosku Rzecznik stwierdził, że „[n]iedookreśloność przesłanek, spełnienie których powoduje powstanie po stronie sądu obowiązku niezwłocznego dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji stanowi także naruszenie konstytucyjnie zagwarantowanego każdej jednostce prawa do ochrony życia prywatnego (art. 47 Konstytucji RP). Nie ma także wątpliwości, że podnoszona w tym zakresie niedookreśloność przesłanek powoduje naruszenie art. 49 i 51 ust. 2 Konstytucji RP. Trybunał Konstytucyjny wyraźnie podkreślił, że konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 Konstytucji RP objęte są <wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o

wybijanych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń, czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI> (wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11). W tym samym wyroku Trybunał Konstytucyjny podkreślił również wyraźnie, że w ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się również ochrona przed niejawnym monitorowaniem jednostki” (uzasadnienie wniosku, s. 34-35).

Na wstępie rozważań merytorycznych dotyczących przedstawionych zarzutów konieczne wydaje się przypomnienie treści przepisów wskazanych w pkt II *petitum* wniosku Rzecznika Praw Obywatelskich w ich otoczeniu normatywnym. Zarazem, ponieważ przepisy te są zbieżne treściowo, wystarczające będzie przytoczenie art. 19 ust. 15 oraz art. 19 ust. 15f - 15j ustawy o Policji.

Art. 19 ust. 15 ustawy o Policji brzmi:

„15. W przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazuje prokuratorowi, o którym mowa w ust. 1, wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej. W postępowaniu przed sądem, w odniesieniu do tych materiałów, stosuje się odpowiednio art. 393 § 1 zdanie pierwsze Kodeksu postępowania karnego.”.

Przepisy art. 19 ust. 15f-15j cytowanej ustawy mają następujące brzmienie:

„15f. W przypadku, gdy materiały, o których mowa w ust. 15:

1) zawierają informacje, o których mowa w art. 178 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje, o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego, albo informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazuje prokuratorowi te materiały.

15g. W przypadku, o którym mowa w ust. 15f pkt 2, prokurator niezwłocznie po otrzymaniu materiałów kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 3, wraz z wnioskiem o:

- 1) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 15f pkt 2;
- 2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

15h. Sąd, niezwłocznie po złożeniu wniosku przez prokuratora, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 15g pkt 2, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15i. Na postanowienie sądu w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 15g pkt 2, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15j. Organ Policji jest obowiązany do wykonania zarządzenia sądu o zniszczeniu materiałów, o którym mowa w ust. 15h, oraz niezwłocznego, komisyjnego i

protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Policji niezwłocznie informuje prokuratora, o którym mowa w ust. 15g, o zniszczeniu tych materiałów.”.

Treść zarzutu sformułowanego w tej części wniosku wskazuje, iż Rzecznik Praw Obywatelskich uważa, że, określona w art. 19 ust. 15h ustawy o Policji, kompetencja sądu do rozstrzygania w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym materiałów objętych tajemnicami zawodowymi dotyczy także tajemnic, o których mowa w art. 178a k.p.k. i art. 180 § 3 k.p.k.

Tego rodzaju interpretacja art. 19 ust. 15h ustawy o Policji, jak również zaskarżonych w tej części wniosku, odpowiadających mu treściowo, przepisów pozostałych ustaw regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego, **jest jednak nieprawidłowa.**

Wszak w przedmiocie tajemnic zawodowych, które podlegają, określone w art. 19 ust. 15h ustawy o Policji, postępowaniu sądowemu, rozstrzyga ten właśnie przepis, wskazując, że chodzi tu wyłącznie o materiały, o których mowa w art. 15g pkt 2 ustawy o Policji, a więc **materiały zawierające informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k., nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 k.p.k., z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 k.k. (w art. 240 § 1 k.k. spenalizowano karalne niezawiadomienie o przestępstwie).**

Zawarte w art. 19 ust. 15h ustawy o Policji wyrażenie „nieobjęte zakazami określonymi w art. 178a i art. 180 § 3 k.p.k.” wcale nie oznacza uzupełnienia listy tajemnic o jeszcze inne tajemnice oprócz tajemnic wymienionych w art. 180 § 2 k.p.k. Wprost przeciwnie - w ten sposób ograniczono listę materiałów poddanych decyzji sądu, wyłączając z nich te, które zawierają fakty, o których mediator dowiedział się od oskarżonego lub pokrzywdzonego prowadząc postępowanie

mediacyjne (art. 178a k.p.k.), oraz te, które zawierają dane umożliwiające 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 (art. 180 § 3 k.p.k.), oczywiście, w obu przypadkach, z wyłączeniem informacji dotyczących przestępstw, o których mowa w art. 240 § 1 k.k.

Tak więc, zaskarżony przepis nie omija, jak poprzez sposób opisu komentowanego zarzutu zdaje się sugerować Rzecznik Praw Obywatelskich, zakazów dowodowych określonych w art. 178a k.p.k. i art. 180 § 3 k.p.k., a - wprost przeciwnie - eksponuje ich znaczenie i potwierdza ich nienaruszalność.

W orzecznictwie Sądu Najwyższego oraz w doktrynie podkreśla się, że przewidziany w art. 178a k.p.k. zakaz przesłuchania mediatora stanowi zakaz dowodowy niezupełny bezwzględny - to jest zakaz skorzystania z określonego w nim źródła dowodowego odnośnie do określonych okoliczności - funkcjonujący bez możliwości jego uchylecia. Podobnie nie może zostać uchylony (ma bezwzględny charakter) zakaz wskazany w art. 180 § 3 k.p.k. (*vide* - uchwała Sądu Najwyższego z dnia 22 listopada 2002 r., w sprawie o sygn. akt I KZP 26/02, LEX nr 55856 oraz komentarz D. Gruszeckiej do art. 178a k.p.k., [w:] *Kodeks postępowania karnego. Komentarz pod red. J. Skorupki*, Wydawnictwo C. H. BECK, Warszawa 2015, s. 414 i T. Grzegorzczak, *Kodeks postępowania karnego. Komentarz LEX. Tom I. Artykuły 1-467*, Wydawnictwo a Wolters Kluwer business, s. 627).

Skoro wykorzystanie w postępowaniu karnym materiałów zawierających fakty i dane, o których mowa w art. 178a k.p.k. i art. 180 § 3 k.p.k., jest niedopuszczalne, to, jeżeli sąd, na wniosek prokuratora, stwierdzi, że materiały zgromadzone podczas kontroli operacyjnej, w przypadku o którym mowa w art. 19 ust. 15 ustawy o Policji (uzyskania w wyniku tej kontroli dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla

toczącego się postępowania karnego), zawierają tego rodzaju fakty i dane, to wówczas decyzja w przedmiocie ich dopuszczenia do wykorzystania w postępowaniu karnym **nie jest podejmowana** i materiały takie podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu (art. 19 ust. 15j w związku z art. 15, art. 15f pkt 2 i art. 15g ustawy o Policji).

Trzeba dodać, że również prokurator, we wniosku skierowanym w trybie art. 19 ust. 15g ustawy o Policji, nie może domagać się dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 178a k.p.k. i art. 180 § 3 k.p.k. (*vide* - art. 15g pkt 2 ustawy o Policji), ponieważ **tego rodzaju wniosku prokuratora ustawa o Policji po prostu nie przewiduje**.

Mając powyższe na uwadze, należy zmodyfikować treść zarzutu Wnioskodawcy, sformułowanego w pkt II *petitum* wniosku, w części odnoszącej się do zakresu zaskarżenia - z uwagi na konieczność jego dostosowania do rzeczywistej treści normatywnej kwestionowanych w tej grupie przepisów.

Trzeba więc przyjąć, że w pkt II *petitum* wniosku Rzecznik Praw Obywatelskich zarzuca niezgodność z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji oraz z art. 6 EKPCz - **art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA w zakresie, w jakim przepisy te posługują się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 tego Kodeksu, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.**

W następnej kolejności należy zwrócić uwagę, iż wzorzec kontroli z art. 42 ust. 2 Konstytucji (gwarancja prawa do obrony) może dotyczyć tylko niektórych „tajemnic” objętych dyspozycją art. 180 § 2 k.p.k.

Wypada zacząć od tego, że materiały z kontroli operacyjnej (niejawnej), prowadzonej na podstawie ustawy o Policji, ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW, jak również ustawy o CBA, zawierające informacje objęte (ogólnie) tajemnicą zawodową (tajemnicą związaną z wykonywaniem zawodu lub funkcji), mogą być wykorzystane wyłącznie w postępowaniu karnym lub karnym skarbowym w sprawie o przestępstwo lub przestępstwo skarbowe (dalej: postępowanie karne).

W tym kontekście kontrola zgodności zaskarżonych przez Wnioskodawcę: art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w zakresie zawartego w tych przepisach odwołania do treści art. 180 § 2 k.p.k., z **konstytucyjną gwarancją prawa do obrony** (z zastrzeżeniem, o którym poniżej, wskazującym, komu w istocie służy tajemnica zawodowa wiążąca przedstawicieli zawodów prawniczych) może dotyczyć wyłącznie dwóch wymienionych w art. 180 § 2 k.p.k. tajemnic: tajemnicy zawodu adwokata oraz tajemnicy zawodu radcy prawnego. W postępowaniu karnym prawo podejrzanego (oskarżonego, ewentualnie osoby zatrzymanej) do obrony może być bowiem realizowane przez ustanowionego (wyznaczonego) w sprawie obrońcę (ewentualnie adwokata lub radcę prawnego działającego na podstawie art. 245 § 1 k.p.k.), którym może być wyłącznie osoba uprawniona do obrony według przepisów o ustroju adwokatury (ustawy - Prawo o adwokaturze) lub ustawy o radcach prawnych (*vide* - art. 82 k.p.k.).

Tymczasem art. 180 § 2 k.p.k. dotyczy nie dwóch, lecz aż ośmiu tajemnic zawodowych, gdyż, poza tajemnicą adwokacką i radcy prawnego, przepis ten wymienia także tajemnicę lekarską, notarialną, doradcy podatkowego, dziennikarza, tajemnicę statystyczną oraz tajemnicę Prokuraturii Generalnej.

Wnioskodawca nie uzasadnił jednak, w jaki sposób przepisy: art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w zakresie zawartego w tych przepisach odwołania do treści art. 180 § 2 k.p.k., naruszają art. 42 ust. 2 Konstytucji, skoro lekarze, notariusze, doradcy podatkowi, dziennikarze oraz osoby wykonujące czynności w imieniu i na rzecz statystyki publicznej (między innymi: pracownicy służb statystyki publicznej, rachmistrze spisowi i ankieterzy statystyczni, mający bezpośredni dostęp do danych jednostkowych, *vide* - art. 12 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej, tekst jednolity - Dz. U. z 2016 r., poz. 1068 ze zm.), jak również pracownicy Prokuraturii Generalnej, **w postępowaniu karnym nie mogą być obrońcami.**

Dlatego też postępowanie w sprawie zgodności art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w zakresie, w jakim przepisy te posługują się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje objęte tajemnicami zawodowymi: lekarską, notarialną, doradcy podatkowego, dziennikarza, statystyczną oraz tajemnicę Prokuraturii Generalnej, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego, z art. 42 ust. 2 Konstytucji podlega umorzeniu na podstawie

art. 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Jedynie na marginesie wypada zauważyć, że i sam Wnioskodawca rażącego naruszenia „jednego z fundamentalnych praw jednostki w państwie prawa, jakim jest prawo do obrony”, upatruje w mechanizmie pozyskiwania objętych tajemnicą zawodową informacji za pomocą czynności operacyjno-rozpoznawczych **prowadzonych tylko w stosunku do adwokatów oraz radców prawnych** (*vide* - uzasadnienie wniosku, s. 32-33).

Tak więc podstawę do dalszych rozważań może stanowić zarzut Wnioskodawcy o niezgodności z prawem do obrony, gwarantowanym w art. 42 ust. 2 Konstytucji art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w zakresie, w jakim przepisy te posługują się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, **objęte tajemnicami zawodowymi adwokata i radcy prawnego**, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

Jednak przed przejściem do odnoszących się do tego zarzutu rozważań merytorycznych konieczna wydaje się analiza odpowiadającej temu zarzutowi argumentacji Rzecznika Praw Obywatelskich, zawartej w uzasadnieniu wniosku.

Otóż z treści odpowiedniego fragmentu uzasadnienia wniosku wynika, iż za tajemnice związane z wykonywaniem zawodu lub funkcji (art. 180 § 2 k.p.k.)

adwokata lub radcy prawnego, o których mowa w zaskarżonych przepisach, Rzecznik uznaje tajemnice zdefiniowane w art. 6 ust. 1 ustawy - Prawo o adwokaturze oraz w art. 3 ust. 3 ustawy o radcach prawnych.

We fragmencie uzasadnienia wniosku, który wcześniej już cytowano, Rzecznik Praw Obywatelskich, wszak wprost nawiązując do wymienionych wyżej regulacji (art. 6 ust. 1 ustawy - Prawo o adwokaturze oraz art. 3 ust. 3 ustawy o radcach prawnych), podkreślił, że, „[z]e względu na fundamentalne znaczenie tajemnicy adwokackiej oraz radcowskiej dla sytuacji prawnej osób, których bezpośrednio dotyczą informacje objęte tajemnicą, konieczne jest wprowadzenie szczegółowo określonych wymagań co do trybu oraz przesłanek uchylenia obowiązku zachowania takiej tajemnicy” (s. 33).

Tymczasem tajemnice, o których mowa w art. 180 § 2 k.p.k., to nie są te same tajemnice, o których mowa w art. 6 ust. 1 ustawy - Prawo o adwokaturze oraz w art. 3 ust. 3 ustawy o radcach prawnych.

Rzecznik myli określoną w art. 6 ust. 1 ustawy - Prawo o adwokaturze oraz w art. 3 ust. 3 ustawy o radcach prawnych **tajemnicę obrończą** z tajemnicami związanymi z wykonywaniem zawodu lub funkcji, wymienionymi w art. 180 § 2 k.p.k.

Tajemnicę obrończą chroni zakaz sformułowany w art. 178 pkt 1 k.p.k., to jest zakaz korzystania, **bez możliwości uchylenia**, z określonego źródła dowodowego odnośnie do określonych okoliczności.

Zgodnie z art. 178 pkt 1 k.p.k. nie wolno przesłuchiwać jako świadka obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1 k.p.k., co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę (zakaz ten dotyczy również przesłuchania w charakterze świadka duchownego co do faktów, o których dowiedział się przy spowiedzi, *vide* - art. 178 pkt 2 k.p.k.).

T. Grzegorzczak wskazuje, że „[n]a gruncie art. 178 pkt 1 nie chodzi (...) wyłącznie o obrońcę z postępowania karnego, ale o każdego obrońcę, którego nie

wolno tu przesłuchiwać jako świadka co do faktów, o których dowiedział się, udzielając porady prawnej albo prowadząc sprawę. Na równi z obrońcą potraktowano adwokata udzielającego pomocy zatrzymanemu, gdy nie jest on (lub nie może być, gdyż zatrzymany nie jest jeszcze podejrzanym) jego obrońcą. Zakaz odnosi się z założenia - poza wskazanym wyjątkiem - do obrońcy, a nie do adwokata w ogóle (tego ostatniego dotyczy art. 180 § 2). Obejmuje zatem też np. radcę prawnego, jeżeli działał w roli obrońcy, co jest możliwe w postępowaniu w sprawach o wykroczenia (art. 24 § 1 k.p.w.), sędziego działającego w tym charakterze w postępowaniu dyscyplinarnym sędziów (art. 113 p.u.s.p.), czy pracownika wyższej uczelni bądź studenta, gdy był on obrońcą w postępowaniu dyscyplinarnym pracownika lub studenta takiej uczelni (art. 146 ust. 1 i art. 218 ust. 2 ustawy z dnia 27 lipca 2005 r. - Prawo o szkolnictwie wyższym, tekst jedn.: Dz. U. z 2012 r. poz. 572 z późn. zm.) [aktualny tekst jednolity - Dz. U. z 2017 r., poz. 2183 ze zm. - przyp. wł.]. Zakaz **dotyczy tylko okoliczności**, o których obrońca dowiedział się, prowadząc sprawę danego klienta, oraz tych, o których dowiedział się, udzielając porady prawnej (tu aktualizuje się ochrona adwokata działającego na podstawie art. 245 § 1). Nie jest przy tym istotne, czy po udzieleniu porady dana osoba podjęła się roli obrońcy, czy też nie. Nie jest też ważne, z jakiego źródła uzyskała swe informacje, od samego klienta, od członków jego rodziny czy z innego jeszcze źródła. Dopelnieniem zakazu przesłuchania jest zakaz zajmowania pism i innych dokumentów związanych z wykonywaniem obrony (art. 225 § 3).

Nowelizacja z dnia 27 września 2013 r. (chodzi o ustawę z dnia 27 września 2013 r. o zmianie ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw, Dz. U. z 2013 r., poz. 1247 ze zm. - przyp. wł.), modyfikuje zakres podmiotowy zakazu z pkt 1 art. 178 z uwagi na nadanie radcom prawnym prawa do udzielania pomocy prawnej w sprawach karnych także oskarżonym, w tym do występowania w roli obrońcy. Stąd - od 1 lipca 2015 r. (data wejścia w życie nowelizacji z dnia 27 września 2013 r. - przyp. wł.) - przepis

ten będzie zakazywał przesłuchiwania obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę” (T. Grzegorzczuk, *Kodeks postępowania karnego. Komentarz LEX. Tom I. Artykuły 1-467*, op. cit., s. 612-613).

Biorąc powyższe pod uwagę, nie można nie dostrzec, iż, postulowane przez Wnioskodawcę, zwiększenie ochrony tajemnicy obrończej przy czynnościach operacyjnych (niejawnych) nie jest konieczne (niedostatek ochrony tego rodzaju tajemnicy na gruncie zaskarżonych przez Rzecznika przepisów ustaw nie występuje), ponieważ w sposób wystarczający ochronę taką przewidują przepisy art. 19 ust. 15f pkt 1 ustawy o Policji, art. 9e ust. 16f pkt 1 ustawy o Straży Granicznej, art. 31 ust. 16f pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15h pkt 1 ustawy o ABW oraz AW, art. 31 ust. 14f pkt 1 ustawy o SKW oraz SWW i art. 17 ust. 15f pkt 1 ustawy o CBA, które, w sytuacji, gdy materiały zgromadzone podczas kontroli operacyjnej zawierają informacje, o których mowa w art. 178 k.p.k., nakazują właściwemu organowi ich niezwłoczne, komisyjne i protokolarne zniszczenie.

Powyższe wskazuje, że w sytuacji, gdy materiały niejawne zawierają informacje objęte tajemnicami wymienionymi w art. 178 k.p.k., tryb przewidziany w przepisach zaskarżonych przez Rzecznika (pozwalający na dopuszczenie przez sąd do wykorzystania w postępowaniu karnym materiału niejawnego, zgromadzonego podczas stosowania kontroli operacyjnej) **w ogóle nie będzie miał zastosowania.**

Tak więc zarzut opisany w pkt II *petitum* wniosku Rzecznik Praw Obywatelskich oparł na wykładni art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w tym zwłaszcza na wykładni art. 180 § 2 k.p.k. w związku z art. 6 ust. 1 ustawy - Prawo

o adwokaturze oraz w związku z art. 3 ust. 3 ustawy o radcach prawnych, **niezgodnej z rzeczywistą treścią normatywną tych przepisów (w opozycji do wykładni językowej).**

Powyższe oznacza, że postępowanie w sprawie kontroli zgodności art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA, w zakresie, w jakim przepisy te posługują się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, objęte tajemnicami zawodowymi adwokata i radcy prawnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego, **z art. 42 ust. 2 Konstytucji** także podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Przystępując z kolei do oceny zgodności art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA w zakresie, w jakim przepisy te posługują się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określają wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, objęte tajemnicami związanymi z wykonywaniem zawodu lub funkcji, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1

Kodeksu karnego, z art. 2, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji oraz z art. 6 EKPCz należy stwierdzić, że zasadniczym zarzutem Wnioskodawcy pod adresem zaskarżonych norm jest niedookreśloność zawartych w nich przesłanek, „spełnienie których powoduje powstanie po stronie sądu obowiązku niezwłocznego dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji”.

Zdaniem Wnioskodawcy, owa niedookreśloność wynika z braku wymaganej ostrości (precyzji) w sformułowaniu kryterium „dobra wymiaru sprawiedliwości”, a także z braku określenia „wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, objęte tajemnicami związanymi z wykonywaniem zawodu lub funkcji”.

Trzeba w związku z tym przypomnieć, iż w sprawie o sygn. akt SK 64/03 Trybunał Konstytucyjny badał zgodność art. 180 § 2 k.p.k. z art. 2, art. 17, art. 31 ust. 3, art. 42 ust. 1, art. 45 ust. 1, art. 49 oraz art. 51 ust. 2 Konstytucji.

Postępowanie w tej sprawie zostało wszczęte na skutek połączonych czterech skarg konstytucyjnych. Swoją udział w postępowaniu zgłosił Rzecznik Praw Obywatelskich, który przepisowi art. 180 § 2 k.p.k., w zakresie, w jakim zezwala na zwolnienie radców prawnych z obowiązku zachowania tajemnicy zawodowej, ciążącego na nich na podstawie art. 3 ust. 3 i 5 ustawy o radcach prawnych, zarzucił niezgodność z art. 2 i art. 45 ust. 1 Konstytucji.

W uzasadnieniu zapadłego w tej sprawie w dniu 22 listopada 2004 r. wyroku Trybunał Konstytucyjny, na wstępie, zauważył, iż *„[k]ontrola konstytucyjności aktów normatywnych wszczęta na skutek skargi konstytucyjnej charakteryzuje się pewnymi cechami szczególnymi. Ustawodawca, przyjmując koncepcję powszechnej skargi konstytucyjnej, w art. 79 ust. 1 Konstytucji wskazał jednak niezbędne warunki, od których spełnienia zależy możliwość inicjowania kontroli w trybie skargowym. Jednym z nich jest wymaganie, by na podstawie kwestionowanego przepisu zapadło ostateczne orzeczenie dotyczące*

konstytucyjnych wolności lub praw skarżącego. W ocenie Trybunału Konstytucyjnego, kwestią podstawową w rozpatrywanej sprawie jest ustalenie, jaka konstytucyjna wolność lub prawo skarżących zostały naruszone postanowieniem sądu o zwolnieniu ich z obowiązku zachowania tajemnicy służbowej (podkr. wł.). Skarżący mają pełną świadomość tego, iż Konstytucja nie gwarantuje przedstawicielom jakiegokolwiek zawodu prawa do tajemnicy zawodowej. Dlatego proponują, by Trybunał uznał istnienie takiego prawa na podstawie interpretowanych łącznie kilku przepisów Konstytucji powołanych (z wyjątkiem art. 9) w petitum skargi. W konsekwencji, wzorcami kontroli konstytucyjnej skarżący uczynili: art. 2, art. 17, art. 31 ust. 3, art. 42 ust. 1, art. 49 i art. 51 ust. 2 Konstytucji. Dodatkowym wzorcem kontroli w niniejszym postępowaniu jest powołany przez Rzecznika Praw Obywatelskich art. 45 ust. 1 Konstytucji, który - zdaniem Rzecznika - w powiązaniu z art. 78 stanowi element podstawy prawnej dla ochrony tajemnicy zawodowej radcy prawnego.

Jak już wyżej wskazano, między uczestnikami postępowania jest bezsporne, iż Konstytucja nie zawiera przepisu, który wprost stanowiłby o prawie radców prawnych do zachowania w tajemnicy informacji pozyskanych w toku udzielania pomocy prawnej lub przy prowadzeniu sprawy. Zasadniczym problemem teoretycznym, od którego rozwiązania zależy rozstrzygnięcie w niniejszej sprawie, jest ustalenie, czy wolność lub prawo konstytucyjne mogą być zrekonstruowane na podstawie kilku przepisów Konstytucji, i to zarówno zawartych w rozdziale dotyczącym wolności i praw osobistych, jak i w innych rozdziałach, w szczególności poświęconych Rzeczypospolitej (art. 1-29). Dopuszczenie takiej teoretycznej możliwości otwiera dopiero drogę do zbadania, czy powołane przez skarżących przepisy w istocie <składają się> na konstytucyjne prawo do <szczególnej tajemnicy komunikowania się>.

W ocenie Trybunału Konstytucyjnego nie można wykluczyć sytuacji, gdy istnienie prawa lub wolności o charakterze konstytucyjnym zostałyby wyprowadzone z treści kilku przepisów Konstytucji. Za <materiał> niezbędny do

takiej rekonstrukcji należałoby uznać elementy normy, znajdujące się w różnych przepisach, które w sposób spójny mogą tworzyć normę skierowaną do określonego adresata. Rozproszenie wymienionych elementów nie powinno przekreślać możliwości skonstruowania normy. Jeśli reguły logiki nakazywałyby wnioskowanie, iż efektem istnienia pewnych obowiązków konstytucyjnych jest powstanie prawa po stronie innego podmiotu, uzasadnione byłoby przyjęcie istnienia tego prawa (wolności), choćby nie było wyraźnie (wprost) statutowane w Konstytucji.

Przyjmując zatem teoretyczną, ograniczoną pewnymi warunkami, możliwość wywiedzenia prawa konstytucyjnego z treści kilku przepisów Konstytucji, Trybunał przystąpił do badania, czy taka sytuacja zachodzi w przypadku tajemnicy zawodowej radców prawnych (podkr. wł.)” [OTK ZU seria A nr 10/2004, poz. 107].

Następnie Trybunał Konstytucyjny stwierdził, że „nie znajduje podstaw do zaakceptowania tezy o istnieniu konstytucyjnego prawa do zachowania tajemnicy zawodowej (podkr. wł.). Żaden z powołanych w skargach wzorców kontroli, ani sam ani w powiązaniu z innymi, nie zawiera normy, której treść nakazywałaby traktowanie obowiązku zachowania tajemnicy radcowskiej w kategoriach prawa konstytucyjnego przysługującego im z samego tytułu wykonywania zawodu radcy prawnego. Trybunał nie dostrzega też powiązań logicznych między powołanymi przepisami, które pozwalałyby skonstruować takie prawo konstytucyjne. Najbardziej ogólnym argumentem przemawiającym przeciwko niej jest niezwykle celne spostrzeżenie Rzecznika Praw Obywatelskich, iż <tajemnica zawodowa osoby świadczącej pomoc prawną nie jest ustanowiona w interesie samego prawnika, lecz w interesie osoby poszukującej tej pomocy> (podkr. wł.) [s. 11]” (ibidem).

W dalszej części uzasadnienia wyroku w sprawie o sygn. akt SK 64/03, Trybunał Konstytucyjny stwierdził, iż „wyraża przekonanie, że jedynym przepisem Konstytucji, na którym można oprzeć bezwzględny nakaz zachowania

tajemnicy zawodowej przez przedstawiciela zawodu prawniczego jest art. 42 ust. 2, przewidujący prawo do obrony. Z przepisu tego niewątpliwie wynika konstytucyjne prawo każdej osoby, przeciwko której prowadzone jest postępowanie karne, do nieskrępowanego kontaktu z obrońcą. To prawo, jak podkreślił Prokurator Generalny, jest zagwarantowane przez kodeks postępowania karnego w sposób niepodważalny. Trybunał zwraca jednak uwagę, że nawet z art. 42 ust. 2 Konstytucji trudno byłoby wyprowadzić konstytucyjne prawo adwokatów do poszanowania tajemnicy obrończej; przepis statuuje bowiem prawo podejrzanego i oskarżonego, czyli osób korzystających z pomocy prawnej” oraz że „podziela oczywiście wynikające ze skarg i ze stanowiska Rzecznika Praw Obywatelskich przekonanie, iż zachowanie tajemnicy radcowskiej jest elementem prawidłowego funkcjonowania wymiaru sprawiedliwości i - szerzej - całego systemu ochrony prawnej w demokratycznym państwie. Nie oznacza to jednak, by Konstytucja dawała podstawę dla konstruowania prawa podmiotowego radców prawnych w tym zakresie, gdyż - co wypada powtórzyć jeszcze raz - to nie w ich interesie ustawodawca przewidział obowiązek zachowania tajemnicy zawodowej. Te same argumenty, które zadecydowały o istnieniu omawianej instytucji i związaniu radców tajemnicą, tj. prawidłowe funkcjonowanie systemu ochrony prawnej, mogą w pewnych sytuacjach decydować o jej uchyleniu. Tajemnica zawodowa wiążąca przedstawicieli zawodów prawniczych służy bowiem nie samym prawnikom, lecz osobom korzystającym z ich pomocy, a szerzej - skutecznemu funkcjonowaniu wymiaru sprawiedliwości. W ocenie Trybunału Konstytucyjnego wyjątki od zakazu przesłuchiwania w charakterze świadków osób, na których ciąży ustawowy obowiązek zachowania poufności, wprowadzone w art. 180 § 2 k.p.k. służą właśnie temu celowi, co zresztą jednoznacznie wynika z treści przepisu (podkr. wł.)” [ibidem].

W podsumowaniu tej części uzasadnienia wyroku w sprawie o sygn. akt SK 64/03 Trybunał Konstytucyjny wyraził przekonanie, że „istniejące na

poziomie ustaw proceduralnych prawo radców prawnych do zachowania tajemnicy co do pewnych okoliczności jest wyznaczane tymi właśnie ustawami”, po czym, zwracając uwagę na brak konstytucyjnego prawa tajemnicy radcowskiej, uznał, że „w gestii ustawodawcy leży kształtowanie zakresu obowiązku zachowania tajemnicy przez radcę prawnego i odpowiadającego mu prawa odmowy zeznań (udzielenia odpowiedzi na pytanie), przy czym swoboda ustawodawcy jest ograniczona innymi wartościami konstytucyjnymi. Zaskarżony przepis, w ocenie Trybunału Konstytucyjnego, nie narusza jednak żadnej z konstytucyjnych wartości wyrażonych w przepisach powołanych jako wzorce kontroli” oraz że [b]rak konstytucyjnego prawa i wolności skarżącego jest dostatecznym powodem uznania za nieuzasadnioną skargi inicjującej postępowanie, a nawet - stwierdzenia niedopuszczalności wydania orzeczenia. W niniejszej sprawie, ze względu na jej powagę, Trybunał Konstytucyjny uznał za celowe merytoryczne ustosunkowanie się do zarzutów zawartych w skargach. Choć wynik dotychczasowych rozważań wskazuje już jednoznacznie na zgodność z Konstytucją kwestionowanego przepisu, warto zwrócić uwagę na inne aspekty skargi (podkr. wł.)” [ibidem].

Jednym z przedstawionych przez Trybunał Konstytucyjny owych „innych aspektów skargi” jest konieczność „precyzyjnego odróżnienia oceny konstytucyjności przepisu od oceny jego stosowania w praktyce” i - odnosząc się do tego aspektu - Trybunał stwierdził, że „[w] przypadku kwestionowanego art. 180 § 2 k.p.k. <zalecenia> dotyczące stosowania tego przepisu były już formułowane w orzecznictwie Sądu Najwyższego. Zasadniczy kierunek interpretacji wynika z zasady *exceptiones non sunt excendendae*; skoro art. 180 § 2 k.p.k. wprowadza wyjątek od zasady, iż adwokatów, radców prawnych, lekarzy i dziennikarzy (obecnie także notariuszy, doradców podatkowych, osób zobowiązanych do zachowania tajemnicy statystycznej oraz pracowników Prokuraturii Generalnej - przyp. wł.) obowiązuje tajemnica zawodowa, **przesłanki**

zwolnienia z obowiązku jej zachowania muszą być rozumiane ściśle i nie podlegają wykładni rozszerzającej (podkr. wł.).

W praktyce stosowania art. 180 § 2 k.p.k., podobnie jak przy stosowaniu innych przepisów, mogą się oczywiście pojawić nieprawidłowości. Na tle stanu faktycznego niniejszej sprawy Trybunał dostrzega dwie możliwości wadliwego zastosowania przez sąd art. 180 § 2 k.p.k.

Po pierwsze, (...) będzie ono miało miejsce wówczas, gdy sąd odwołuje się do tego przepisu w sytuacji, gdy informacje, które chce uzyskać, w ogóle nie są objęte tajemnicą zawodową radcy prawnego, a zatem nie ma potrzeby stosowania art. 180 § 2 k.p.k. (...)

Po drugie, nieprawidłowość może polegać na tym, że - w zakresie rzeczywiście objętym tajemnicą zawodową - sąd zbyt pochopnie zastosuje zwolnienie z art. 180 § 2 k.p.k., bez dostatecznych podstaw przyjmując ziszczenie się przesłanek w nim przewidzianych. Tymczasem zwolnienie z tajemnicy może nastąpić tylko pod warunkiem stwierdzenia przez sąd, iż w konkretnej sprawie karnej zachodzi rzeczywisty brak możliwości ustalenia danej okoliczności na podstawie innego dowodu niż przesłuchanie radcy prawnego. Przesłanka ta musi być spełniona kumulatywnie z przesłanką ogólną, by przesłuchania wymagało dobro wymiaru sprawiedliwości. Oczywiście warunkiem stosowania art. 180 § 2 k.p.k., niewątpliwie mieszczącym się w przesłance dobra wymiaru sprawiedliwości, jest przekonanie sądu, że okoliczność, którą chce się dowodzić przez przesłuchanie radcy prawnego, ma znaczenie dla ustalenia prawdy o popełnionym czynie i jego sprawcy (podkr. wł.)” [ibidem].

Zanim jednak Trybunał Konstytucyjny, w uzasadnieniu wyroku w sprawie o sygn. akt SK 64/03, doszedł do wniosku, że teza o istnieniu konstytucyjnego prawa do zachowania tajemnicy zawodowej nie znajduje podstaw do zaakceptowania, dokonał analizy zarzutu niedookreśloności art. 180 § 2 k.p.k. oraz niezgodności tego przepisu z art. 49 i art. 51 ust. 2 Konstytucji.

W tym zakresie Trybunał stwierdził, że „zarzut niedookreśloności art. 180 § 2 k.p.k. nie jest uzasadniony. Przepis zawiera dwa kryteria, od których kumulatywnego spełnienia uzależniona jest możliwość zwolnienia z obowiązku zachowania tajemnicy zawodowej: musi tego wymagać dobro wymiaru sprawiedliwości oraz dana okoliczność nie może być ustalona na podstawie innego dowodu. Ponadto przepis wymaga, by przesłuchanie osoby zobowiązanej do zachowania tajemnicy zawodowej było niezbędne dla wskazanych celów. **O ile pojęcie <dobra wymiaru sprawiedliwości> jest bardzo ogólne, o tyle - w ocenie Trybunału Konstytucyjnego - drugie z kryteriów wskazanych w art. 180 § 2 k.p.k., tj. brak innych środków dowodowych jest konkretne, wymierne i sprawdzalne** (podkr. wł.). Ponieważ o zwolnieniu z tajemnicy decyduje sąd, dysponujący już całym materiałem dowodowym zebrany w postępowaniu przygotowawczym, należy przyjąć, że jest on władny ocenić niezbędność dowodu, tj. stwierdzić, że za pomocą innych, realnie dostępnych środków dowodowych (takim środkiem na pewno nie jest zeznanie oskarżonego, który ma prawo zachować milczenie), nie można danej okoliczności udowodnić. Argument braku precyzji art. 180 § 2 k.p.k. na pewno nie wystarcza więc, by podważyć konstytucyjność zaskarżonego przepisu. Przecistawiając się tezie skarżących o naruszeniu zasad prawidłowej legislacji Trybunał Konstytucyjny, w ślad za stanowiskiem Prokuratora Generalnego, uważa za konieczne podkreślenie, iż w prawie polskim istnieje pewna tradycja zwolnień z obowiązku zachowania tajemnicy, a stworzony przez ustawodawcę system zwolnień jest dość jasny i racjonalnie uzasadniony” (ibidem).

Odnośnie natomiast do wskazanego przez skarżących w sprawie o sygn. akt SK 64/03 - jako samodzielnego wzorca kontroli - art. 31 ust. 3 Konstytucji, Sąd Konstytucyjny stwierdził, iż „ustalone orzecznictwo Trybunału Konstytucyjnego przyjmuje, że przepis ten nie może być samodzielnie podstawą skargi, gdyż nie jest źródłem praw ani wolności. Odwołanie się do zasady proporcjonalności wyrażonej w art. 31 ust. 3 Konstytucji może tylko towarzyszyć

innej podstawie prawnej skargi i służyć wykazaniu, że ograniczenie prawa lub wolności poszło za daleko; żeby go stosować trzeba więc najpierw wykazać istnienie takiego konstytucyjnego prawa lub wolności. Jak wskazał Trybunał Konstytucyjny w wyroku z 10 lipca 2000 r. (sygn. SK 2/99, OTK ZU nr 5/2000, poz. 144), art. 31 ust. 3 Konstytucji ma zastosowanie do oceny ograniczenia praw konstytucyjnych, zaś <<konstytucyjnymi> w rozumieniu tego przepisu są prawa podmiotowe, których podstawę stanowi norma rangi konstytucyjnej. Wymagania przewidziane w art. 31 ust. 3 Konstytucji nie dotyczą natomiast praw, których jedynym źródłem jest ustawa>. **Oczywiście Trybunał Konstytucyjny dostrzega, o czym już kilkakrotnie była mowa, konflikt dóbr, jaki rysuje się w niniejszej sprawie; dobru w postaci prywatności, poufności informacji przeciwstawia się dobro wymiaru sprawiedliwości. Trybunał Konstytucyjny podkreśla jednak, że prawo do prywatności i poufności informacji nie przysługuje radcom prawnym, lecz ich klientom** (podkr. wł.). Na radcach ciąży obowiązek respektowania tego prawa. Z ich punktu widzenia należy raczej mówić o konflikcie obowiązków prawnych: obowiązku zachowania tajemnicy zawodowej i obowiązku wystąpienia w roli świadka. <Zwolnienia z obowiązku> zachowania tajemnicy zawodowej, uregulowanego w zaskarżonym art. 180 § 2 k.p.k., nie można traktować jako przypadku <ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw>, do którego odnosi się art. 31 ust. 3 Konstytucji” (ibidem).

Z kolei, odnośnie do wzorców kontroli z art. 49 i art. 51 ust. 2 Konstytucji, Trybunał Konstytucyjny, w uzasadnieniu tego samego wyroku, stwierdził, że „[p]ierwszy z przepisów zapewnia <wolność i tajemnicę komunikowania się>. Drugi - ogranicza władze publiczne w pozyskiwaniu, gromadzeniu i udostępnianiu informacji o obywatelach. Analizując treść tych przepisów pod kątem ich <przydatności> do skonstruowania konstytucyjnego prawa radców prawnych do zachowania tajemnicy zawodowej, Trybunał Konstytucyjny zwraca uwagę na dwie kwestie. Po pierwsze, oba powołane przepisy dopuszczają limitowanie tajemnicy: art. 49 Konstytucji przewiduje możliwość ustawowego

ograniczenia wskazanej w nim wolności, zaś art. 51 ust. 2 już w swej treści zawiera przyzwolenie dla działań władz, jeśli działania te są niezbędne w demokratycznym państwie prawnym. Po drugie, Trybunał Konstytucyjny stoi na stanowisku, że na naruszenie wolności wskazanych w art. 49 i art. 51 ust. 2 Konstytucji - teoretycznie - mogliby powoływać się raczej klienci radców prawnych, aniżeli sami radcowie. Obowiązek zachowania tajemnicy ustanowiono bowiem w interesie klientów, a nie radców. Nie jest on wyrazem uprzywilejowania grupy zawodowej, lecz właśnie obowiązkiem związanym z wykonywaniem zawodu. Nie ulega jednak wątpliwości, że prawa wynikające z analizowanych teraz przepisów ustępują w toku postępowania karnego; świadczy o tym już choćby powszechny obowiązek składania zeznań przez osobę powołaną w charakterze świadka. Jednym z podstawowych zadań demokratycznego państwa prawnego jest niewątpliwie wykrywanie przestępstw, ściganie ich sprawców i wymierzanie im kar. Jeśli do tego celu konieczne okaże się gromadzenie określonych informacji przez policję, prokuraturę i sądy, działania tych organów nie mogą być uznane za niezgodne z Konstytucją. Przewidziane w zaskarżonym art. 180 § 2 k.p.k. kryterium zwolnienia z obowiązku zachowania tajemnicy zawodowej w postaci braku innych środków dowodowych i niezbędności dowodu z zeznań radcy prawnego dostatecznie usprawiedliwiają domaganie się od niego informacji (podkr. wł.)” [ibidem].

Reasumując tę część rozważań, należy stwierdzić, że **wskazania i oceny prawne zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt SK 64/03 zachowują aktualność w zakresie pkt II *petitum* wniosku Rzecznika Praw Obywatelskich.**

Jak już wcześniej podniesiono, zasadniczym zarzutem Wnioskodawcy pod adresem zaskarżonych w tym punkcie *petitum* wniosku norm jest niedookreśloność pojęcia „dobro wymiaru sprawiedliwości”, w połączeniu z niedookreśleniem wagi okoliczności, która ma być ustalona na podstawie

materiałów mogących zawierać informacje, objęte tajemnicami związanymi z wykonywaniem zawodu lub funkcji.

Tymczasem pojęcie „dobro wymiaru sprawiedliwości” nie stanowi jedyne kryterium, od spełnienia którego uzależnione jest wydanie przez sąd (niezwłocznie) postanowienia o dopuszczeniu do wykorzystania w postępowaniu karnym zgromadzonych podczas stosowania kontroli operacyjnej materiałów, zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. (przy uwzględnieniu art. 178a k.p.k. i art. 180 § 3 i 4 k.p.k., to jest pod warunkiem, że informacje te nie są objęte określonymi w tych przepisach zakazami, chyba że chodzi o przestępstwo, o którym mowa w art. 240 § 1 k.k.) [dalej: postanowienie o dopuszczeniu].

Drugim kryterium, od którego spełnienia uzależnione jest wydanie postanowienia o dopuszczeniu, jest wymaganie, aby dana okoliczność nie mogła być ustalona na podstawie innego dowodu.

Trzeba dodać, że oba te kryteria muszą być spełnione kumulatywnie.

Ponadto zaskarżone przepisy wymagają, by dopuszczenie wskazanych wyżej materiałów do wykorzystania w postępowaniu karnym **było niezbędne** dla wskazanych celów.

O ile „dobro wymiaru sprawiedliwości” jest pojęciem bardzo ogólnym, o tyle kryterium braku innych środków dowodowych **jest, na gruncie zaskarżonych przepisów, konkretne, wymierne i sprawdzalne** (podobnie - *vide* - cytowane uprzednio uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt SK 64/03).

Ponieważ o „dopuszczeniu materiałów do wykorzystania w postępowaniu karnym, zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k.”, decyduje sąd dysponujący całym materiałem zgromadzonym podczas stosowania kontroli operacyjnej (*vide* na przykład - art. 15 ustawy o Policji), należy przyjąć,

że sąd jest również władny ocenić niezbędność dowodu z tych materiałów, to jest stwierdzić, że za pomocą innych, realnie dostępnych środków dowodowych nie można danej okoliczności udowodnić.

W tej sytuacji sformułowany przez Wnioskodawcę zarzut braku precyzji zaskarżonych przepisów **nie wystarcza**, by podważyć ich konstytucyjność.

Z tych samych powodów nie jest też trafny sformułowany przez Wnioskodawcę zarzut niedookreślenia wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, objęte tajemnicami związanymi z wykonywaniem zawodu lub funkcji, **czy też trafniej - zarzut braku w zaskarżonych przepisach kryteriów określających wagę i istotność dla postępowania karnego tej okoliczności.**

Waga i istotność „okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, objęte tajemnicami związanymi z wykonywaniem zawodu lub funkcji”, została już bowiem dostatecznie określona poprzez wskazanie funkcji, jakie okoliczność ta ma spełniać w postępowaniu karnym.

Materiały zgromadzone podczas stosowania kontroli operacyjnej, zawierające informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, **muszą być wszak nieodzowne** dla osiągnięcia celów postępowania karnego, które zostały sformułowane w art. 2 § 1 k.p.k., **w sprawie o konkretne przestępstwo**, gdy brak jest innych środków dowodowych, które mogłyby potwierdzić daną okoliczność. „Nieodzowność” oznacza zatem niemożność dokonania ustaleń co do danej okoliczności na podstawie materiałów, które nie zawierają informacji stanowiących wskazane wyżej tajemnice.

Wszak kontrola operacyjna jest traktowana jako **środek ostateczny** (gdy „inne środki okazały się nieskuteczne albo będą nieprzydatne” dla realizacji celów w zakresie zapobiegania przestępstwom i wykrywania ich, ujawniania ich sprawców oraz uzyskiwania i utrwalania dowodów, co należy wykazać we wniosku do sądu o zezwolenie na jej zastosowanie, a wcześniej - przy

uzyskiwaniu aprobaty odpowiedniego prokuratora na wystąpienie z takim wnioskiem, *vide* na przykład - art. 19 ust. 1-2 ustawy o Policji).

Nie można przy tym tracić z pola widzenia tego, że kontrola operacyjna może być stosowana, co do zasady, tylko w sprawach o najpoważniejsze przestępstwa umyślne.

Wszelako należy jednak uczynić zastrzeżenie, iż, w odróżnieniu do stanu prawnego, określonego w sprawie, na tle której Trybunał Konstytucyjny orzekał w dniu 22 listopada 2004 r. (w sprawie o sygn. akt SK 64/03), gdzie wątpliwości konstytucyjne dotyczyły możliwości zwolnienia piastunów funkcji z tajemnicy zawodowej, określonej w art. 180 § 2 k.p.k. w toku **wszczętego i prowadzonego postępowania karnego**, sprawa zainicjowana wnioskiem Rzecznika Praw Obywatelskich dotyczy oceny konstytucyjności mechanizmu dopuszczenia do wykorzystania w postępowaniu karnym materiałów zgromadzonych podczas stosowania kontroli operacyjnej, zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, **którego to postępowania karnego jeszcze nie wszczęto**.

Powyższe powoduje, że, po pierwsze, postanowienie o dopuszczeniu wydaje inny sąd niż sąd właściwy do rozpoznania sprawy (sąd, który wydał postanowienie o zarządzeniu kontroli operacyjnej, czyli sąd okręgowy właściwy miejscowo ze względu na siedzibę składającego wniosek organu), i, po drugie, że wydający to postanowienie sąd ma, z oczywistych względów, możliwość oceny respektowania kryterium niezbędności w ograniczonym zakresie. Dysponuje bowiem wprowadzonymi materiałami, ale tylko tymi, które zostały zgromadzone podczas stosowania kontroli operacyjnej.

Mimo to na etapie sądowej oceny materiałów zgromadzonych podczas stosowania kontroli operacyjnej, a zatem **zanim jeszcze dojdzie do wszczęcia postępowania karnego** (na etapie rozstrzygania o wszczęciu), kryterium braku innych środków dowodowych także **należy uznać za konkretne, wymierne i sprawdzalne**.

Trzeba też mieć na uwadze, że postanowienie o wykorzystaniu, wydawane przez sąd na etapie nadzoru nad czynnościami operacyjnymi, *per se* nie przesądza o tym, czy wskazane w nim materiały istotnie zostaną wykorzystane w konkretnym postępowaniu karnym - o tym bowiem zadecyduje dopiero sąd *meriti*, który, rozstrzygając o zwolnieniu piastuna z tajemnicy zawodowej (art. 180 § 2 k.p.k.), jak również podejmując decyzję o dopuszczeniu do wykorzystania materiałów zawierających informacje objęte tajemnicą zawodową jako dowodów w postępowaniu karnym (art. 226 k.p.k.), zobowiązany będzie uwzględnić kryteria przewidziane w art. 180 § 2 k.p.k.

W tym miejscu należy przytoczyć wypowiedź P. Hofmańskiego i S. Zabłockiego, którzy stwierdzili, że „[u]stawodawca stopniuje poziom ochrony tajemnicy informacji poufnych i zastrzeżonych oraz zawodowej i funkcyjnej w procesie karnym, ograniczając sąd w możliwościach zwolnienia od obowiązku jej zachowania bądź to przez skonstruowanie dodatkowych kryteriów, jakie muszą być wzięte przez sąd pod uwagę, bądź to ograniczając zakres dopuszczalnego zwolnienia. Tak więc, zgodnie z art. 180 § 2 k.p.k., w wypadku tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej lub dziennikarskiej sąd musi skonfrontować treść spodziewanego dowodu z pozostającymi do jego dyspozycji innymi dowodami w sprawie, ponieważ zwolnienie od obowiązku zachowania tajemnicy dopuszczalne jest tylko wtedy, gdy dana okoliczność nie może być ustalona na podstawie innego dowodu. Slogan o <dobru wymiaru sprawiedliwości> ma tu oczywiście zdecydowanie mniejsze znaczenie. **Dokonanie wymaganej prawem oceny może niekiedy okazać się wcale trudne, albowiem wymaga od sądu dokonania apriorycznej oceny dowodów, i to nie tylko tych, które zostały już przeprowadzone, ale także tych, które pozostają do dyspozycji sądu i dopiero mają być przeprowadzone** (podkr. wł.). Na szczęście odstąpienie od zwolnienia świadka z obowiązku zachowania tajemnicy, o której mowa w art. 180 § 2 k.p.k., **nie zamyka drogi do podjęcia takiej decyzji w dalszej fazie postępowania** (podkr. wł.). Jeśli więc na

przykład sąd, przyjmując założenie, że i bez dowodu z zeznań radcy prawnego zasłaniającego się tajemnicą zawodową, da sobie jakoś radę, zaś następnie dowód, na który bardzo liczył, okaże się niedostępny (z powodów prawnych lub faktycznych), może wydać postanowienie o zwolnieniu owego radcy z obowiązku zachowania tajemnicy” (P. Hofmański, S. Zabłocki, *Elementy metodyki pracy sędziego*, http://lex/lex/content.rpc?reqId=1467282661960_1186261608).

Jak wiadomo, uwzględnienie wniosku w przedmiocie zezwolenia na przesłuchanie osoby zobowiązanej do zachowania tajemnicy zawodowej **w toku postępowania przygotowawczego i sądowego** uzależnione jest od tego, czy przesłuchanie tej osoby **jest niezbędne dla dobra wymiaru sprawiedliwości**, oraz od tego, czy **okoliczności, które mają być udowodnione, mogą być ustalone na podstawie innego dowodu**.

Zdaniem P. Hofmańskiego i S. Zabłockiego, „zbadanie tych okoliczności wymaga (...) dokonania wstępnej oceny materiału dowodowego zebranego w sprawie. **Doniosłość społeczna zawodów objętych przepisem art. 180 § 2 k.p.k. sprawia, że zarówno decyzja o zezwoleniu na przesłuchanie takiej osoby w toku postępowania przygotowawczego na okoliczności objęte tajemnicą, jak i decyzja o zwolnieniu następująca w trakcie postępowania jurysdykcyjnego nie mogą być traktowane jako formalność** (podkr. wł.). Zaufanie klienta do notariusza, adwokata, radcy prawnego, doradcy podatkowego, pacjenta do lekarza i informatorów do dziennikarzy warunkuje prawidłowe wykonywanie tych zawodów i stanowi istotną wartość, której ewentualne naruszenie stanowi cenę za osiągnięcie względów sprawiedliwościowych, których bez tego naruszenia nie dałoby się osiągnąć. **Przyjęcie, że spełnione są obie przesłanki wymienione w art. 180 § 2 k.p.k., powinno zatem opierać się na wnikliwej i wszechstronnej ocenie okoliczności faktycznych sprawy, a nie może wynikać z ocen arbitralnych, niedających się instancyjnie skontrolować** (podkr. wł.)” [P. Hofmański, S. Zabłocki, *Elementy metodyki pracy sędziego*, http://lex/lex/content.rpc?reqId=14672829766557_613948371).

W kontekście cytowanych wyżej wypowiedzi P. Hofmańskiego i S. Zabłockiego jest oczywiste, że sąd działający w trybie nadzoru nad czynnościami operacyjnymi, który rozstrzyga w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym zgromadzonych podczas stosowania kontroli operacyjnej materiałów, zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, nie jest w stanie dokonać apriorycznej oceny zwłaszcza tych dowodów, „które pozostają do dyspozycji sądu i dopiero mają być przeprowadzone”.

Można zatem dojść do wniosku, że *ratio legis* zaskarżonych przepisów w istocie nie jest dopuszczenie materiałów zgromadzonych podczas stosowania kontroli operacyjnej, zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, do konkretnego postępowania karnego, **ale zachowanie tychże materiałów na użytek takiego postępowania z pozostawieniem ostatecznej decyzji o ich wykorzystaniu sądowi *meriti*.**

Reasumując, należy stwierdzić, że art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW i art. 17 ust. 15h ustawy o CBA w zakresie, w jakim posługują się pojęciem „dobro wymiaru sprawiedliwości” i nie zawierają kryteriów określających wagę i istotność dla postępowania karnego okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego, są zgodne z art. 2 Konstytucji.

Ponieważ Wnioskodawca źródła naruszenia przez zaskarżone normy pozostałych wzorców konstytucyjnej kontroli upatruje w „niedookreśloności kryterium <dobra wymiaru sprawiedliwości>” oraz w braku określenia „wagi

okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje” objęte tajemnicami, wymienionymi w art. 180 § 2 k.p.k. (nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego), to zgodność zaskarżonych norm z art. 2 Konstytucji oznacza jednocześnie ich zgodność z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

Natomiast postępowanie w przedmiocie kontroli zgodności art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o ABW oraz AW, art. 31 ust. 14h ustawy o SKW oraz SWW oraz art. 17 ust. 15h ustawy o CBA w zakresie, w jakim posługują się nieostrym pojęciem „dobro wymiaru sprawiedliwości” i nie zawierają kryteriów określających wagę i istotność dla postępowania karnego okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 § 3 tego Kodeksu, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego, **z art. 6 EKPCz** podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia. Rzecznik Praw Obywatelskich nie uzasadnił bowiem tego zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonemu w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Warto mimo to w tym miejscu przypomnieć, że art. 6 EKPCz określa prawo do rzetelnego procesu karnego oraz że przepis ten formułuje cały szereg wymogów takiego procesu.

Przepis ten brzmi następująco:

„Art. 6. 1. Każdy ma prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej. Postępowanie przed sądem jest jawne, jednak prasa i publiczność mogą być wyłączone z całości lub części rozprawy sądowej ze względów obyczajowych, z uwagi na porządek publiczny lub bezpieczeństwo państwowe w społeczeństwie demokratycznym, gdy wymaga tego dobro małoletnich lub gdy służy to ochronie życia prywatnego stron albo też w okolicznościach szczególnych, w granicach uznanych przez sąd za bezwzględnie konieczne, kiedy jawność mogłaby przynieść szkodę interesom wymiaru sprawiedliwości.

2. Każdego oskarżonego o popełnienie czynu zagrożonego karą uważa się za niewinnego do czasu udowodnienia mu winy zgodnie z ustawą.

3. Każdy oskarżony o popełnienie czynu zagrożonego karą ma co najmniej prawo do:

- a) niezwłocznego otrzymania szczegółowej informacji w języku dla niego zrozumiałym o istocie i przyczynie skierowanego przeciwko niemu oskarżenia;
- b) posiadania odpowiedniego czasu i możliwości do przygotowania obrony;
- c) bronięcia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony - do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości;

- d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia;
- e) korzystania z bezpłatnej pomocy tłumacza, jeżeli nie rozumie lub nie mówi językiem używanym w sądzie.”.

Jak już podkreślono, Wnioskodawca nie uzasadnił zarzutu naruszenia przez kwestionowane unormowania tak określonych standardów rzetelnego procesu.

III. Zarzut niezgodności:

- art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy o Policji, art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 oraz art. 28b ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 oraz art. 32b ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 oraz art. 18b ust. 1 ustawy o CBA z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE (grupa przepisów wskazana w pkt III *petitum* wniosku Rzecznika Praw Obywatelskich);
- art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o ABW oraz AW, art. 32a ustawy o SKW oraz SWW i art. 18a ustawy o CBA w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych, z art. 2, art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE (grupa przepisów wskazana w pkt V *petitum* wniosku Rzecznika Praw Obywatelskich).

W stosunku do zakwestionowanych w pierwszej ze wskazanych dwóch grup przepisów Wnioskodawca sformułował następujące trzy zarzuty.

Po pierwsze, że przewidują one zbyt szeroki zakres danych, do których upoważnione podmioty mają dostęp. Umożliwiają bowiem Policji, Straży Granicznej, Żandarmerii Wojskowej pozyskiwanie **danych telekomunikacyjnych**, czyli danych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (tekst jednolity - Dz. U. z 2017 r., poz. 1907 ze zm.) [dalej: ustawa - Prawo telekomunikacyjne], **danych pocztowych**, czyli danych, o których mowa w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (tekst jednolity - Dz. U. z 2017 r., poz. 1481) [dalej: ustawa - Prawo pocztowe] oraz **danych internetowych**, czyli danych, o których mowa w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jednolity - Dz. U. z 2017 r., poz. 1219) [dalej: ustawa o świadczeniu usług drogą elektroniczną] w celu zapobiegania **wszelkim czynom stanowiącym przestępstwo** (w przypadku Żandarmerii Wojskowej - także wszelkim czynom stanowiącym przestępstwo skarbowe) oraz ich wykrywania, **bez względu na doniosłość czynu**.

Pozostałym zaskarżonym przepisom Wnioskodawca zarzuca, że upoważniają one funkcjonariuszy:

- ABW - do uzyskiwania danych telekomunikacyjnych, danych pocztowych oraz danych internetowych **niezbędnych do realizacji wszystkich zadań**, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW, w tym również zadania polegającego na rozpoznawaniu, zapobieganiu i wykrywaniu **wszystkich** przestępstw enumeratywnie wymienionych w art. 5 ust. 1 pkt 2 tej ustawy;

- SKW - do uzyskiwania danych telekomunikacyjnych, danych pocztowych oraz danych internetowych **niezbędnych do realizacji wszystkich zadań**, o których mowa w art. 5 ustawy o SKW oraz SWW, w tym również zadania polegającego na rozpoznawaniu, zapobieganiu i wykrywaniu **wszystkich** przestępstw enumeratywnie wymienionych w art. 5 ust. 1 pkt 1 tej ustawy;

- CBA - do uzyskiwania danych telekomunikacyjnych, danych pocztowych oraz danych internetowych **niezbędnych do realizacji wszystkich zadań**, o których mowa w art. 2 ustawy o CBA, w tym również zadania polegającego na rozpoznawaniu, zapobieganiu i wykrywaniu **wszystkich** przestępstw enumeratywnie wymienionych w art. 2 ust. 1 pkt 1 tej ustawy.

Po drugie, że uzyskiwanie, w oparciu o zakwestionowane przepisy, przez wskazane wyżej służby powołane do ochrony bezpieczeństwa państwa i porządku publicznego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych **nie ma wymaganego - w ocenie Wnioskodawcy - charakteru subsydiarnego**, ponieważ jest ono dopuszczalne w każdym wypadku, gdy tylko zwrócić się o to odpowiednie służby. W tej sytuacji, jak argumentuje RPO, warunkiem dostępu do tych danych nie jest wyczerpanie innych środków prawnych, mniej ingerujących w sferę prywatności oraz w tajemnicę komunikowania się.

W tym zakresie Rzecznik Praw Obywatelskich stwierdził, że „[t]ak ujęty cel gromadzenia i przetwarzania danych może (...) oznaczać w istocie brak selektywności zarówno na etapie rozpoczęcia pozyskiwania danych internetowych, czyli możliwości uzyskiwania przez służby danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną. Oznacza ponadto, że nie zagwarantowano, by gromadzenie i przetwarzanie danych internetowych było subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach. Brak subsydiarności proponowanych przepisów otwiera możliwość wykorzystywania danych telekomunikacyjnych, pocztowych i internetowych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy gdy jest to po prostu najprostsze i najwygodniejsze (...). W powiązaniu z przepisami dotyczącymi kontroli sądowej, o czym jeszcze będzie mowa w dalszej części wniosku, należy wyraźnie stwierdzić, że sądy nie będą mogły ocenić, na ile sięgnięcie w określonej sytuacji

po dane było rzeczywiście niezbędne i należyście uzasadnione, co dodatkowo osłabia poziom ochrony prywatności jednostek” [uzasadnienie wniosku, s. 41].

W dalszej części wniosku Rzecznik Praw Obywatelskich, omawiając zarzut odnoszący się do przepisów kwestionowanych w drugiej grupie (art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o ABW oraz AW, art. 32a ustawy o SKW oraz SWW i art. 18a ustawy o CBA), stwierdził, że przewidziany w tych przepisach mechanizm następczej kontroli sądu nad udostępnianiem danych telekomunikacyjnych, danych pocztowych oraz danych internetowych nie jest wystarczający, ponieważ nie zapewnia realnej i niezależnej kontroli pozyskiwania tych danych.

Ponadto Rzecznik zwrócił uwagę, że **wspomnianej następczej kontroli sądu w ogóle nie podlega** uzyskiwanie danych, o których mowa w art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28b ust. 1 ustawy o ABW oraz AW, art. 32b ust. 1 ustawy o SKW oraz SWW i art. 18b ust. 1 ustawy o CBA (chodzi między innymi o pozyskiwanie danych określonych w art. 161 i art. 179 ust. 9 ustawy - Prawo telekomunikacyjne).

Po trzecie, że **odwołanie się** w przepisach art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 ustawy o CBA **do definicji pojęcia „dane internetowe” jest nieprecyzyjne i niejasne.**

Podsumowując, wszystkie zakwestionowane w tych dwóch grupach przepisy, zdaniem Rzecznika Praw Obywatelskich, w sposób nieproporcjonalny ingerują w prywatność jednostki, ochronę tajemnicy komunikowania się i zasadę autonomii informacyjnej, a zatem w wartości chronione, odpowiednio, przez art. 47, art. 49 i art. 51 ust. 2 Konstytucji, a tym samym godzą w prawo do zachowania godności człowieka, gwarantowane w art. 30 Konstytucji, i zarazem - z tych

samych powodów (brak zachowania wymogu proporcjonalności ograniczenia) - naruszają art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Dodatkowo, wymienione w pierwszej grupie przepisy art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 ustawy o CBA w zakresie, w jakim odwołują się do definicji pojęcia „dane internetowe”, w ocenie Wnioskodawcy, naruszają zasadę określoności oraz zasadę ochrony zaufania do państwa i stanowionego przez nie prawa, wynikające z art. 2 Konstytucji.

Zarzut niezgodności ze wskazanymi w tej części wniosku wzorcami konstytucyjnej kontroli przepisów umożliwiającym funkcjonariuszom odpowiednich służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego pozyskiwanie danych określonych w art. 161, art. 179 ust. 9, art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych określonych w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe oraz danych określonych w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, **Rzecznik Praw Obywatelskich łączy, o czym wcześniej była mowa, z zarzutem niewystarczającej kontroli sądowej nad uzyskiwaniem tych danych** (zdaniem Rzecznika, przewidziana przez ustawodawcę kontrola sądowa nie jest w tym przypadku ani niezależna, ani realna).

Odnosnie natomiast do art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o ABW oraz AW, art. 32a ustawy o SKW oraz SWW i art. 18a ustawy o CBA, ich niezgodności z Konstytucją Rzecznik upatruje w braku jakiegokolwiek, w tym także sądowej, niezależnej kontroli uzyskiwania wymienionych w tych przepisach danych.

W przedstawionych wyżej okolicznościach nie sposób rozpatrywać zarzutu określonego w pkt III *petitum* wniosku Rzecznika Praw Obywatelskich, dotyczącego art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 ustawy o CBA, bez odwołania się do treści normatywnej przepisów zaskarżonych w pkt V *petitum* tego wniosku, tym bardziej że w obu przypadkach Wnioskodawca powołał podobne wzorce kontroli.

1. Ocena zarzutu niezgodności art. 20c ust. 1 w związku z art. 20ca ustawy o Policji z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 20c ust. 1 ustawy o Policji ma następującą treść:

„Art. 20c. 1. W celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

- 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,
 - 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2017 r. poz. 1481), zwane dalej <danymi pocztowymi>,
 - 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), zwane dalej <danymi internetowymi>
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Na wstępie należy zauważyć, iż Wnioskodawca, spośród trzech wymienionych w art. 20c ust. 1 ustawy o Policji celów udostępniania danych (zapobieganie lub wykrywanie przestępstw albo ratowanie życia lub zdrowia ludzkiego bądź wsparcie działań poszukiwawczych lub ratowniczych), kwestionuje wyłącznie udostępnianie danych w celu zapobiegania lub wykrywania przestępstw (*vide* - uzasadnienie wniosku, s. 39 i s. 42).

W związku z tym trzeba uznać, że uzyskiwanie przez Policję danych, o których mowa w zaskarżonym przepisie, w innych celach niż zapobieganie lub wykrywanie przestępstw **nie jest objęte zarzutem Wnioskodawcy.**

Z powyższych względów postępowanie w sprawie kontroli zgodności art. 20c ust. 1 w związku z art. 20ca ustawy o Policji w zakresie, w jakim Policja może uzyskiwać dane telekomunikacyjne, pocztowe lub internetowe w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia. Rzecznik Praw Obywatelskich nie uzasadnił bowiem tego zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonemu w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Za uzasadnienie czyniące zadość wspomnianym wymogom nie można bowiem uznać jedynie powtórzenia przez Wnioskodawcę treści tego przepisu i wskazania, że określone w nim prawo przyznane zostało „w celu zapobiegania lub wykrywania przestępstw albo ratowania życia lub zdrowia ludzkiego bądź

wsparcia działań poszukiwawczych lub ratowniczych” (uzasadnienie wniosku, s. 36).

Przepis art. 20c ustawy o Policji - w ust. 1 - upoważnia funkcjonariuszy Policji do gromadzenia oraz przetwarzania bez wiedzy i zgody osoby, której dotyczą, danych telekomunikacyjnych (czyli danych wymienionych w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne), danych pocztowych (czyli danych wymienionych w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe) oraz danych internetowych (czyli danych wymienionych w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną), a także określa przedmiotowe przesłanki oraz warunki udostępniania tych danych na żądanie funkcjonariuszy Policji (ust. 2-7).

Przepisy art. 180c i art. 180d ustawy - Prawo telekomunikacyjne brzmią:

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

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:

- a) inicjującego połączenie,
- b) do którego kierowane jest połączenie;

2) określenia:

- a) daty i godziny połączenia oraz czasu jego trwania,
- b) rodzaju połączenia,
- c) lokalizacji telekomunikacyjnego urządzenia końcowego.

2. Minister właściwy do spraw informatyzacji 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, a także sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 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.”.

Jak wyjaśnia M. Rogalski, „[p]rzepis art. 180c określa, jakie kategorie danych dostępnych operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, podlegają obowiązkowi z art. 180a ust. 1 (obowiązkowi, realizowanemu na własny koszt operatora, zatrzymywania i przechowywania, udostępniania uprawnionym podmiotom oraz ochrony, w określonym w tym przepisie zakresie danych - przyp. wł.). Chodzi o dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest połączenie (art. 180c ust. 1 pkt 1). Będą to więc dane pozwalające na ustalenie zakończenia sieci rozumianego jako fizyczny punkt, w którym abonent otrzymuje dostęp do publicznej sieci telekomunikacyjnej. W przypadku sieci stosujących komutację lub przekierowywanie, zakończenie sieci identyfikuje się za pomocą konkretnego adresu sieciowego, który może być przypisany do numeru lub nazwy abonenta (art. 2 pkt 52). W wypadku danych niezbędnych do ustalenia zakończenia sieci chodzi o wybierany numer odbiorcy połączenia, a w przypadku dodatkowych usług, jak przekierowywanie lub przełączanie połączeń - numer, na który połączenie jest przekierowywane. Kolejne dane muszą pozwolić na ustalenie telekomunikacyjnego urządzenia końcowego, którym jest urządzenie

telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci (art. 2 pkt 43). Niezbędne są również dane pozwalające na ustalenie użytkownika końcowego, czyli podmiotu korzystającego z publicznie dostępnej usługi telekomunikacyjnej lub żądającego świadczenia takiej usługi, dla zaspokojenia własnych potrzeb (art. 2 pkt 50). We wszystkich tych przypadkach chodzi o dane, które pozwolą na jednoznaczną identyfikację urządzeń lub podmiotów. Chodzi o dane urządzeń i podmiotów nie tylko inicjujących połączenie, ale także tych, do których kierowane jest połączenie. W przypadku podmiotów będzie chodziło o dane pozwalające na ustalenie konkretnej osoby, która zainicjowała połączenie lub do której zostało skierowane połączenie, co oczywiście nie oznacza, że osoba ta musi być tożsama z osobą abonenta lub użytkownika danego urządzenia końcowego.

Obowiązkiem określonym w art. 180c objęte są także dane niezbędne do określenia: a) daty i godziny połączenia telefonicznego oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego (art. 180c ust. 1 pkt 2). Przepis art. 180c ust. 1 pkt 2 lit. b mówi ogólnie o rodzaju <połączenia>. W konsekwencji należy przyjąć, że nie chodzi w tym przepisie tylko o rodzaje <połączeń telefonicznych> zdefiniowanych w art. 2 pkt 26. Analogicznie jest w przypadku danych niezbędnych do określenia lokalizacji telekomunikacyjnego urządzenia końcowego, zdefiniowanego w art. 2 pkt 43. Obowiązek ten nie jest ograniczony tylko do lokalizacji telekomunikacyjnych urządzeń końcowych używanych w określonym rodzaju sieci telefonicznej, np. w ruchomej publicznej sieci telefonicznej. Postanowienia art. 179 ust. 3 nie mają obecnie zastosowania do przekazywania sądom i prokuraturom wykazów połączeń. **Przepisy art. 180c i art. 180d (...) obejmują zakresy danych, które w znacznym stopniu się pokrywają. Wszystkie dane objęte art. 180c mieszczą się w zakresie danych określonych w art. 180d (podkr. wł.)**” [komentarz M. Rogalskiego do art. 180c ustawy - Prawo telekomunikacyjne, http://lex/lex/content.rpc?reqId=1461247014567_77562915].

Przepisy art. 159 ust. 1 i art. 161 ustawy - Prawo telekomunikacyjne brzmią:

„Art. 159. 1. Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej <tajemnicą telekomunikacyjną>, obejmuje:

- 1) dane dotyczące użytkownika;
- 2) treść indywidualnych komunikatów;
- 3) 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 lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
- 4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- 5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.”;

Art. 161. 1. Z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej <przetwarzaniem>, dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.

2. Dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną:

- 1) nazwisk i imion;

- 2) imion rodziców;
- 3) miejsca i daty urodzenia;
- 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania;
- 5) numeru ewidencyjnego PESEL - w przypadku obywatela Rzeczypospolitej Polskiej;
- 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego (Unii Europejskiej - przyp. wł.) albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu;
- 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

3. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.”.

Przepis art. 159 ustawy - Prawo telekomunikacyjne znajduje się w Dziale VII tej ustawy poświęconym tajemnicy telekomunikacyjnej oraz ochronie użytkowników końcowych.

K. Kawałek, komentując art. 159 tej ustawy, stwierdził, że „[t]ajemnica telekomunikacyjna jest elementem szerszego pojęcia, którym jest tajemnica komunikowania się. W Rozdziale II Konstytucji RP poświęconym wolnościom, prawom i obowiązkom człowieka i obywatela, w części obejmującej wolności i prawa osobiste zamieszczony jest art. 49, który stanowi: <Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony>. Przepis ten

nie określa, co należy rozumieć przez komunikowanie się, tym samym obejmuje ochronę tajemnicy wszelkich sposobów porozumiewania. Pojęcie <komunikować się> oznacza <wymieniać z kimś informacje, np. w rozmowie lub listownie> (*Słownik wyrazów obcych*, Warszawa 2009, s. 493). Ochrona tajemnicy komunikowania się nie ma charakteru bezwzględnego, jednakże ograniczenie tego dobra osobistego wymaga uregulowania w przepisie o randze ustawy, który to przepis musi określać nie tylko w jakich przypadkach może nastąpić ograniczenie, lecz wskazywać sposób w jaki to ograniczenie może być realizowane. Z kolei art. 51 ust. 1 Konstytucji RP stanowi, że nikt nie może być obowiązany do ujawniania informacji na temat jego osoby inaczej niż na podstawie przepisów ustawy. Zaś ust. 2 tego artykułu stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. (...)

Przedmiot tajemnicy telekomunikacyjnej obejmuje, zgodnie z art. 159 ust. 1:

- 1) dane dotyczące użytkownika;
- 2) treść indywidualnych komunikatów;
- 3) 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;
- 4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- 5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczające połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które

zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

W zakresie tym można wyróżnić dwie kategorie: dane, których dotyczą pkt 1, 3, 4 i 5 oraz treść przekazu, której dotyczy pkt 2” (komentarz K. Kawałka do art. 159 ustawy - Prawo telekomunikacyjne, http://lex/lex/content.rpc?reqId=1467619466398_756898887).

Ten sam Autor, komentując z kolei art. 161 ustawy - Prawo telekomunikacyjne, stwierdził, że „[p]rzepis ust. 1 art. 161 zawiera zestaw czynności, które stanowią przetwarzanie treści i danych objętych tajemnicą telekomunikacyjną. Są nimi: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie, co odpowiada zakazanym przez art. 159 ust. 2 czynnościom przy uwzględnieniu użytego w tym ostatnim przepisie terminu <inne wykorzystywanie>. Jako cel uzasadniający przetwarzanie treści i danych i tym samym wyłączający w tym zakresie naruszenie obowiązku zachowania tajemnicy telekomunikacyjnej art. 161 ust. 1 wskazuje, że treści i dane powinny dotyczyć usługi świadczonej użytkownikowi lub być niezbędne do jej wykonania i w tym zakresie regulacja zamieszczona w art. 161 ust. 1 odpowiada postanowieniom zamieszczonym w art. 159 ust. 2 pkt 1.

Przepis art. 161 ust. 2 dotyczy pierwszego składnika tajemnicy telekomunikacyjnej zamieszczonego w art. 159 ust. 1 pkt 1, tj. danych dotyczących użytkownika. Jest on ograniczony do danych użytkownika będącego osobą fizyczną. Obejmuje on dane, do przetwarzania których uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych. Dostawcą jest, zgodnie z art. 2 pkt 27, przedsiębiorca telekomunikacyjny uprawniony do świadczenia usług telekomunikacyjnych, tj. usług polegających głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej, o czym stanowi art. 2 pkt 28. Przetwarzanie danych wymienionych w art. 160 ust. 2 może być dokonane bez zgody użytkownika. Katalog tych danych jest katalogiem zamkniętym i obejmuje:

- 1) nazwiska i imiona;
- 2) imiona rodziców;
- 3) miejsce i datę urodzenia;
- 4) adres i miejsce zameldowania na pobyt stały;
- 5) numer ewidencyjny PESEL - w przypadku obywatela RP;
- 6) nazwę, serię, i numer dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego (Unii Europejskiej - przyp. wł.) albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu;
- 7) dane zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

Przepis art. 161 ust. 2 pkt 6 nie wskazuje, jakie dokumenty są dokumentami potwierdzającymi tożsamość obywateli państw członkowskich oraz Konfederacji Szwajcarskiej. Jedynie dla innych cudzoziemców stawia wymaganie, by dokumentem tym był paszport lub karta pobytu. Od dostawcy usług zależy jakie dokumenty uzna za potwierdzające tożsamość użytkownika, np. dowód osobisty, prawo jazdy. Również dostawcy usług telekomunikacyjnych pozostawione jest określenie, jakie dokumenty potwierdzają możliwość wykonania zobowiązania użytkownika wobec dostawcy usług telekomunikacyjnych, których to dokumentów dotyczy art. 161 ust. 2 pkt 7.

Przepis art. 161 nie określa danych mogących ulegać przetworzeniu odnośnie do użytkowników niebędących osobami fizycznymi” (komentarz K. Kawałka do art. 161 ustawy - Prawo telekomunikacyjne, http://lex/lex/content.rpc?reqId=1461241667304_709995992).

Wreszcie wymieniony w art. 180d ustawy - Prawo telekomunikacyjne przepis art. 179 ust. 9 tej ustawy brzmi:

„Przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy.”.

Przepis ten nakłada na przedsiębiorcę telekomunikacyjnego obowiązek zapewnienia uprawnionym podmiotom dostępu do elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci. M. Rogalski podnosi, że „[w] wykazie tym znajdują się dane pozyskane przez przedsiębiorcę telekomunikacyjnego przy zawarciu umowy”, oraz wyjaśnia, że „[w] związku z wątpliwościami, które powodowało poprzednie określenie podmiotów uprawnionych, szczególnie w kontekście jednoczesnego i wzajemnie niezależnego dostępu, przyjęto rozwiązanie definiujące jako <uprawnione podmioty>: Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy. Uprawnienia tych podmiotów w zakresie dostępu do danych i ich utrwalania są uregulowane w ustawach dotyczących działalności tych służb” (komentarz M. Rogalskiego do art. 179 ustawy - Prawo telekomunikacyjne, http://lex/lex/content.rpc?reqId=146124113220_435185196).

Rekonstruując rzeczywistą treść normatywną art. 180c i art. 180d ustawy - Prawo telekomunikacyjne należy mieć na uwadze, że, w uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny analizował treść obu tych przepisów i stwierdził, iż „[w] myśl art. 180c ust. 1 prawa telekomunikacyjnego udostępnia się dane dotyczące ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie i do którego kierowane jest połączenie, a także określające datę i godzinę połączenia oraz czas jego trwania, rodzaj połączenia, a także lokalizację telekomunikacyjnego urządzenia końcowego. Doprecyzowanie katalogu danych, o których mowa w art. 180c ust. 1, zawiera wydane na

podstawie art. 180c ust. 2 rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226, poz. 1828; dalej: rozporządzenie Ministra Infrastruktury).

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

Uwzględniając powyższe przepisy, ustawodawca zezwolił na pozyskiwanie przez uprawnione podmioty danych dotyczących użytkownika, danych transmisyjnych (tj. danych przetwarzanych dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług

telekomunikacyjnych), danych o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, danych o próbach uzyskania połączenia między zakończeniami sieci, w tym o nieudanych próbach połączeń oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń. W świetle art. 161 prawa telekomunikacyjnego, dostawca publicznie dostępnych usług telekomunikacyjnych może też gromadzić następujące dane, o które mogą występować uprawnione organy władzy publicznej: dane osobowe abonenta obejmujące nazwisko i imiona; imiona rodziców; miejsce i datę urodzenia; adres miejsca zamieszkania i adres korespondencyjny, jeżeli jest on innym niż adres miejsca zamieszkania; numer PESEL - w wypadku obywatela polskiego; nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w wypadku cudzoziemca niebędącego obywatelem państwa członkowskiego UE albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu; dane zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Jeśli dostawca publicznie dostępnych usług telekomunikacyjnych uzyskał zgodę użytkownika będącego osobą fizyczną na przetwarzanie innych danych tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, adres korespondencyjny użytkownika (jeżeli jest on inny niż adres miejsca zamieszkania), a ponadto adres poczty elektronicznej oraz numery telefonów kontaktowych, również i tego rodzaju dane, znajdujące się w dyspozycji dostawcy publicznie dostępnych usług telekomunikacyjnych, mogą być pozyskiwane i przetwarzane przez służby policyjne i służby ochrony państwa w celach określonych w ustawach. Ponadto służby te mogą otrzymywać dane wskazane w art. 179 ust. 9 prawa telekomunikacyjnego, czyli zawarte w prowadzonym

obligatoryjnie przez każdego przedsiębiorcę telekomunikacyjnego wykazie abonentów, użytkowników lub zakończeń sieci, dane uzyskiwane podczas zawarcia umowy.

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

Przepis art. 82 ust. 1 ustawy - Prawo pocztowe brzmi:

„Art. 82. 1. Operator pocztowy, poczynszy od dnia rozpoczęcia działalności pocztowej, jest obowiązany do nieodpłatnego zapewnienia, w ramach wykonywanej przez siebie działalności pocztowej, technicznych i organizacyjnych możliwości wykonywania przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową, zwane dalej <uprawnionymi podmiotami>, oraz prokuraturę i sądy, ich zadań określonych odrębnymi przepisami, wymagających:

1) **uzyskania danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług** (podkr. wł.),

2) udostępniania przesyłek pocztowych w celu kontroli treści korespondencji lub **zawartości przesyłek** (podkr. wł.),

3) udostępniania zatrzymanej przez operatora przesyłki pocztowej w przypadku podejrzenia, że stanowi przedmiot przestępstwa do oględzin przez uprawnione podmioty,

4) dopuszczenia do dalszego przewozu przesyłki pocztowej zawierającej przedmioty przestępstwa w stanie nienaruszonym lub po ich usunięciu albo zastąpieniu w całości lub w części

- zgodnie z zasadami i trybem określonym w przepisach odrębnych.”.

Treść powołanego wyżej przepisu wskazuje na to, że, na podstawie art. 20c ust. 1 ustawy o Policji, **możliwe jest pozyskanie tylko takich danych przesyłki pocztowej, które dotyczą nadawcy** (czyli podmiotu, który zawarł z operatorem pocztowym umowę o świadczenie usługi pocztowej, której zawarcie może nastąpić przez przyjęcie przez operatora pocztowego przesyłki pocztowej do przemieszczenia i doręczenia, *vide* - art. 3 pkt 10 w związku z art. 15 ust. 1 pkt 1 ustawy - Prawo pocztowe), **adresata** (czyli podmiotu wskazanego przez nadawcę jako odbiorcę przesyłki pocztowej lub kwoty pieniężnej określonej w przekazie pocztowym, *vide* - art. 3 pkt 2 ustawy - Prawo pocztowe), **jak również zawartości przesyłki**. Nie istnieje natomiast prawna możliwość pozyskiwania w tym trybie treści indywidualnej korespondencji przekazywanej przesyłką listową (przesyłka listowa - to przesyłka pocztowa z korespondencją lub druk, z wyłączeniem przesyłki reklamowej, zaś druk - to przesyłka pocztowa zawierająca informację pisemną lub graficzną, zwielokrotnioną za pomocą technik drukarskich lub podobnych, utrwaloną na papierze albo innym materiale używanym w drukarstwie, w tym książkę, dziennik lub czasopismo) [*vide* - art. 3 pkt 5 i pkt 20 ustawy - Prawo pocztowe].

Art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną ma następującą treść:

„Art. 18. 1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:

1) nazwisko i imiona usługobiorcy;

- 2) numer ewidencyjny PESEL lub - gdy ten numer nie został nadany - numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość;
- 3) adres zameldowania na pobyt stały;
- 4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3;
- 5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
- 6) adresy elektroniczne usługobiorcy.

2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.

3. Usługodawca wyróżnia i oznacza te spośród danych, o których mowa w ust. 2, jako dane, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną zgodnie z art. 22 ust. 1.

4. Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów określonych w art. 19 ust. 2 pkt 2, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną.

5. Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):

- 1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;
- 2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;
- 3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;
- 4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.”.

W komentarzu do art. 18 ustawy o świadczeniu usług drogą elektroniczną J. Gołaczyński stwierdził, że „[p]rzepisy dotyczące ochrony danych osobowych

zbieranych w związku ze świadczeniem usług drogą elektroniczną można podzielić na trzy grupy: **pierwszą stanowią zasady zbierania, oznaczenia i dalszego przetwarzania danych niezbędnych do świadczenia usługi** (podkr. wł.), drugą - zasady przetwarzania danych po zakończeniu stosunku prawnego, trzecią - zasady wykorzystywania danych do celów reklamowych. W ramach pierwszej grupy dotyczącej zasad przetwarzania danych można wyróżnić kilka obowiązujących zasad, w zależności od rodzaju danych, które podlegają przetwarzaniu.

Pierwszą grupę danych osobowych wyszczególnionych w ustawie stanowią dane opisane w ust. 1 art. 18. **Wyliczenie to przedstawia podstawowe dane osobowe usługobiorcy, które mogą być przetwarzane. Ich wyliczenie nie stanowi katalogu zamkniętego, ponieważ usługodawca może przetwarzać także inne dane, jeżeli jest to niezbędne ze względu na właściwość danej usługi lub sposób jej rozliczenia (art. 18 ust. 2 u.ś.u.d.e.), nie ma bowiem możliwości stworzenia ustawowego, zamkniętego katalogu informacji o osobie, których przetwarzanie może być niezbędne w celach związanych z zawartą umową** (podkr. wł.). Przepis art. 18 ust. 1 u.ś.u.d.e. zawiera pewne podobieństwa do art. 69 pr. tel., w którym określono katalog zamknięty danych, których przetwarzanie jest dopuszczalne. Jednakże świadczenie usług drogą elektroniczną obejmuje także umowy zawierane i wykonywane on-line. Nie jest przy tym możliwe ustawowe określenie zakresu niezbędnych danych (...). **W związku z tym usługodawca może przetwarzać także numer karty płatniczej, numer rachunku bankowego usługobiorcy, o ile służą one do rozliczenia usługi. Za każdym razem jednak poszerzenie omawianego katalogu danych podlegających przetworzeniu musi mieć uzasadnienie w treści świadczonej usługi** (podkr. wł.) [...].

Przetwarzanie danych osobowych jest dopuszczalne po spełnieniu **łącznie** (podkr. wł.) kilku warunków. I tak, **dane te mogą być przetwarzane jedynie w związku z realizacją celu wymienionego w ust. 1 art. 18 u.ś.u.d.e., czyli dla**

nawiązania stosunku prawnego. Następnie konieczne jest spełnienie przesłanki mówiącej, że uzyskanie danych, na przykład numeru PESEL, NIP, jest niezbędne z uwagi na rodzaj świadczonej usługi. Jeżeli zatem usługodawca będzie, zgodnie z literalnym brzmieniem przepisu, przetwarzał te dane, ale nie zostanie spełniona przesłanka związku z usługą, będzie to niezgodne z prawem.

Do drugiej grupy zalicza się dane, które będą wykorzystywane przez usługodawcę ze względu na rodzaj świadczonej usługi (na przykład dane dotyczące wieku danej osoby) albo też ze względu na sposób rozliczenia z usługobiorcą (czyli na przykład będzie to numer NIP potrzebny do wystawienia faktury) [podkr. wł.]. W tym przypadku należy jednoznacznie wskazać, że dane te będą **potrzebne niezbędnie** (podkr. wł.) do realizacji określonej usługi. W sytuacji odmowy udzielenia tych danych usługodawca ma prawo odmówić świadczenia usługi (art. 22 ust. 1 u.ś.u.d.e.). Chodzi tu o spełnienie warunku niezbędności uzyskania określonych danych ze względu na funkcjonowanie systemu teleinformatycznego. **Do drugiej grupy zaliczane są również dane sprzętu i oprogramowania, z którego korzysta usługobiorca, bądź też dane gromadzone ze względu na obowiązek ich uzyskania wynikający z innych ustaw** (podkr. wł.) - tak będzie w przypadku wspomnianego już numeru NIP (obowiązek jego zamieszczenia na fakturze wystawianej przez świadczącego usługę wynika z ustawy o rachunkowości).

Dane, o których mowa w art. 18 ust. 1-3 u.ś.u.d.e., czyli dane niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego przez usługodawcę i usługobiorcę, są udostępniane przez usługobiorcę świadomie. Natomiast dane, o których mowa w art. 18 ust. 5 u.ś.u.d.e. (dane eksploatacyjne), są **pozyskiwane automatycznie przez działanie systemu teleinformatycznego** (podkr. wł.). Ich przetwarzanie następuje niejako bez wiedzy usługobiorcy i dlatego poddane zostało bardziej rygorystycznym wymogom (...).

Pozyskanie podstawowych danych nie będzie wymagane przez usługodawcę, jeżeli (usługobiorca - przyp. wł.) będzie (...) chciał skorzystać z usługi lub zapłacić za usługę odpłatną anonimowo lub używając pseudonimu. Koniecznym jednak warunkiem braku obowiązku pozyskania danych osobowych będzie techniczna możliwość świadczenia usługi odpłatnie bez tych danych. Może to się jednak okazać trudne. W przypadku usługi świadczonej na rzecz podmiotu anonimowego lub wykorzystującego pseudonim wszelkie aktualne informacje dotyczące skorzystania z takiej możliwości powinny być udostępniane usługobiorcy, który przetwarza dane określonej osoby.

W przypadku danych osobowych, które nie są niezbędne do świadczenia usługi drogą elektroniczną, a jedynie potrzebne do realizacji celów określonych w art. 19 ust. 2 pkt 2 u.ś.u.d.e., których przetwarzanie odbywa się i za zgodą usługobiorcy, ustawa wprowadza odmienne zasady. **Jeżeli nie są niezbędnie potrzebne do świadczenia usługi drogą elektroniczną, dane tego rodzaju mogą być przetwarzane po spełnieniu, po pierwsze, warunku uzyskania zgody usługobiorcy** (podkr. wł.). [...] Po drugie, dane, podobnie jak w przypadku danych z ust. 2 art. 18 u.ś.u.d.e., mogą być przetwarzane jedynie w celu związanym z realizacją umowy lub dokonaniem innej czynności prawnej z usługobiorcą (...).

Przepis art. 18 ust. 5 u.ś.u.d.e. odnosi się do tzw. danych eksploatacyjnych. Jak już wskazano wyżej, dane te są powiązane z konkretną usługą i dlatego **ich celem jest bardziej identyfikowanie konkretnej usługi niż osoby, która z niej korzysta. Można jednak za pomocą tych danych ustalić także osobę korzystającą z usługi** (podkr. wł.), na przykład przez ustalenie końcowego urządzenia, za pomocą którego uzyskano tę usługę.

Wszystkie rodzaje danych wymienione w ust. 1-5 art. 18 u.ś.u.d.e. usługodawca jest obowiązany podać organom państwa dla celów prowadzonych przez nie postępowań. (...)

W doktrynie pojawiły się także wątpliwości interpretacyjne dotyczące art. 18 ust. 3 u.ś.u.d.e., który zwiera między innymi sformułowanie o podaniu danych niezbędnych do świadczenia usług drogą elektroniczną zgodnie z art. 22 u.ś.u.d.e. Przepis art. 18 ust. 3 odnosi się bowiem także do danych osobowych wymienionych w art. 18 ust. 2 u.ś.u.d.e., natomiast między przepisami art. 18 ust. 2 i art. 22 u.ś.u.d.e. istnieją różnice odnośnie do treści podstaw uzasadniających niezbędność przetwarzania danych, a tym samym również różnice w zakresie kategorii danych, których przetwarzanie jest niezbędne. Powstaje zatem pytanie, która spośród kategorii danych, do których odnoszą się przepisy art. 18 ust. 1, ust. 2 i art. 22 ust. 1 u.ś.u.d.e. powinna być wyróżniona zgodnie z obowiązkiem wynikającym z art. 18 ust. 3 u.ś.u.d.e. (...) należy przyjąć bezpieczne rozwiązanie, czyli założyć, że konieczne jest wyróżnienie kategorii, do których odnoszą się wszystkie te trzy przepisy” (J. Gołaczyński, *Komentarz do art. 18 ustawy o świadczeniu usług drogą elektroniczną*, http://lex/lex/content.rpc?reqId=1467641295819_526793878).

Przepis art. 22 ustawy o świadczeniu usług drogą elektroniczną brzmi:

„Art. 22. 1. Odmowa świadczenia usługi drogą elektroniczną z powodu nieudostępnienia przez usługobiorcę danych, o których mowa w art. 18 ust. 1 i 2, jest dopuszczalna tylko wtedy, gdy przetwarzanie tych danych jest niezbędne ze względu na sposób funkcjonowania systemu teleinformatycznego zapewniającego świadczenie usługi drogą elektroniczną lub właściwość usługi albo wynika z odrębnych ustaw.

2. Usługodawca umożliwia usługobiorcy korzystanie z usługi lub uiszczanie opłat za nią, jeżeli usługa świadczona drogą elektroniczną jest odpłatna, w sposób anonimowy albo przy użyciu pseudonimu, o ile jest to technicznie możliwe oraz zwyczajowo przyjęte.”.

W komentarzu do tego przepisu A. Frań-Adamek stwierdziła, że dane wymienione w art. 18 ust. 1 ustawy o świadczeniu usług drogą elektroniczną, jak również dane określone w art. 18 ust. 2 tej ustawy „podlegają przetwarzaniu

przez usługodawcę tylko pod warunkiem ich niezbędności w odniesieniu do konkretnej usługi. **Przepis art. 22 uzupełnia wspomniany art. 18 potwierdzając, że określone dane wtedy są niezbędne do korzystania z danej usługi, gdy bez ich przetworzenia nie może być ona w ogóle świadczona (podkr. wł.).** W przypadku chęci pozyskania przez usługodawcę innego rodzaju danych, zakończenie jego działań w tym kierunku z dobrym czy też złym efektem nie może mieć wpływu na samo świadczenie usługi. Usługodawca nie ma również uprawnienia do odmowy świadczenia usługi w sposób anonimowy lub z użyciem pseudonimu. **Jedynym uzasadnieniem odmowy świadczenia usługi z powodu braku chęci ujawnienia swoich podstawowych danych są wymagania techniczne, oraz, jak się wydaje, brak samej przesłanki <zwyczajowego> przyjęcia występowania anonimowo lub pod pseudonimem w przypadku określonych usług (podkr. wł.)**” [komentarz A. Frań-Adamek do art. 22 ustawy o świadczeniu usług drogą elektroniczną, http://lex/lex/content.rpc?reqId=1467709663243_741791148].

Rzecznik twierdzi, że art. 20c ust. 1 ustawy o Policji w sposób nieproporcjonalny ingeruje w prawo do prywatności, ochronę tajemnicy komunikowania się i zasadę autonomii informacyjnej jednostki, a zatem w wartości chronione, odpowiednio, przez art. 47, art. 49 i art. 51 ust. 2 Konstytucji, a tym samym godzi w prawo do zachowania godności człowieka, gwarantowane w art. 30 Konstytucji, i zarazem - z tych samych powodów (brak zachowania wymogu proporcjonalności ograniczenia) - narusza art. 7 i art. 8 Konwencji oraz art. 52 ust. 1 Karty Praw Podstawowych UE przez to, że upoważnia funkcjonariuszy Policji do uzyskiwania w sposób niejawnny określonych w tym przepisie danych w celu zapobiegania lub wykrywania wszystkich bez wyjątku, a zatem i błahych przestępstw, przy jednoczesnej niewystarczającej, przewidzianej w ustawie, kontroli sądu nad uzyskiwaniem tych danych.

Należy w związku z tym rozstrzygnąć, czy art. 20c ust. 1 ustawy o Policji, który niewątpliwie ingeruje w prawa i wolności jednostki gwarantowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), czyni to z zachowaniem **wymogu proporcjonalności** tej ingerencji.

Dla przypomnienia (wcześniej była już o tym mowa) - tego rodzaju kontrola, zwana testem proporcjonalności, polega na sprawdzeniu, czy ustawodawca, ograniczając prawa i wolności gwarantowane w Konstytucji, sprostą:

- 1) wymogowi przydatności, który polega na przeprowadzeniu testu racjonalności instrumentalnej, tzn. ustaleniu, czy według dostępnego stanu wiedzy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków,
- 2) wymogowi konieczności, który oznacza ocenę, czy badane przepisy są niezbędne dla ochrony dóbr wskazanych w art. 31 ust. 3 Konstytucji (pięciu dóbr ogólnospołecznych lub indywidualnych „wolności i praw innych osób”), a ponadto, czy spośród środków skutecznie chroniących te wartości zostały wybrane środki najmniej uciążliwe,
- 3) wymogowi proporcjonalności *sensu stricto*, który należy rozumieć jako ustalenie, czy efekty zaskarżonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela.

Należy przy tym podkreślić, że niekonstytucyjnością badanego uregulowania skutkuje uchybienie przez ustawodawcę już choćby jednemu spośród wskazanych wyżej wymogów.

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, wskazując, jakim **materialnym** wymaganiom powinny odpowiadać regulacje dopuszczające czynności operacyjno-rozpoznawcze, stwierdził, że „[c]zynności operacyjno-rozpoznawcze są konstytucyjnie usprawiedliwione tylko o tyle, o ile ich celem jest obrona wartości

demokratycznego państwa prawnego. Muszą zatem sprostać wymaganiom <konieczności w demokratycznym państwie prawnym> (vide: art. 31 ust. 3, art. 51 ust. 2 Konstytucji). Nie wystarczy więc ich celowość, użyteczność, taniość bądź łatwość posługiwania się nimi przez organy władzy publicznej. Nie ma także przesądzającego znaczenia, czy podobne środki są wykorzystywane w innych państwach (...). Niejawne pozyskiwanie informacji przez służby policyjne i ochrony państwa ma bowiem służyć wzmocnieniu poziomu ochrony wartości istotnych w państwie demokratycznym w sposób niemożliwy do osiągnięcia z wykorzystaniem innych rozwiązań, mniej ingerujących w sferę wolności lub praw jednostek. Jednocześnie muszą to być środki najmniej uciążliwe dla podmiotów, których wolności lub prawa ulegają ograniczeniu, stosowane absolutnie wyjątkowo, w celu wykrywania i ściganiu poważnych przestępstw. W przeciwnym razie demokratyczne państwo stałoby się w rzeczywistości państwem policyjnym.

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

prowadzą do wzrostu wykrywalności przestępstw, podniesienia stanu bezpieczeństwa państwa lub obywateli, nie spełnią one przesłanki przydatności ograniczenia.

Ograniczenie konstytucyjnych wolności i praw w świetle zasady proporcjonalności wymaga oceny, czy korzyści wprowadzonych ograniczeń pozostają w odpowiedniej proporcji do uszczerbku doznawanego przez jednostki. Innymi słowy, musi występować odpowiednie zbilansowanie konkurujących ze sobą wartości. Oczywiście tego rodzaju ocena jest możliwa do przeprowadzenia wyłącznie w konkretnym wypadku. W tym miejscu Trybunał formułuje więc jedynie ogólne warunki, jakie muszą być każdorazowo brane pod uwagę w toku badania proporcjonalności unormowania” (op. cit.).

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

informacyjną”, oraz zwrócił uwagę „na konieczność nieustannej weryfikacji katalogu takich przestępstw. Z biegiem czasu niektóre przestępstwa - uznawane dotąd za poważne zagrożenia - mogą zmieniać swoją kwalifikację. Katalog poważnych przestępstw, co do których może być dopuszczalne niejawnie pozyskiwanie informacji o osobach przez organy państwa, musi być tym samym ciągle przez ustawodawcę aktualizowany” (op. cit.).

Następnie Trybunał Konstytucyjny wskazał, że „[p]rzepisy regulujące niejawnie pozyskiwanie informacji o jednostkach przez władze publiczne nie mogą ujmować przesłanek ich zarządzenia w sposób abstrakcyjny, w oderwaniu od rzeczywistego stopnia wywoływanego zagrożenia dla określonych dóbr w danej sprawie. Aby unormować przesłanki zarządzenia czynności operacyjno-rozpoznawczych, trzeba zatem precyzyjnie określić katalog poważnych przestępstw, ale także wskazać dodatkowe okoliczności, umożliwiające niuansowanie zasadności tego rodzaju sposobu pozyskiwania informacji i dowodów w konkretnych sprawach, z uwzględnieniem m.in. ciężaru gatunkowego lub rozmiarów wyrządzonej szkody”, a następnie podkreślił, że „nie neguje możliwości pozyskiwania informacji o jednostkach za pomocą czynności operacyjno-rozpoznawczych także w celu zapobiegania poważnym przestępstwom, czyli podejmowania działań przeciwdziałających popełnianiu przestępstw”, oraz że „nie podważa (...) dopuszczalności wykorzystywania tych czynności w celu rozpoznawania zagrożeń, to jest pozyskiwania informacji o sytuacjach sprzyjających popełnieniu przestępstw. Dotyczy to w szczególności podejmowania tych działań przez służby ochrony państwa stojące na straży jego bezpieczeństwa zewnętrznego i wewnętrznego. W świetle standardu konstytucyjnego zarządzenie kontroli operacyjnej lub pozyskanie danych telekomunikacyjnych może nastąpić jednak w takich wypadkach, w których prawdopodobieństwo popełnienia przestępstwa jest realne, a nie tylko hipotetyczne. Ciężar wykazania prawdopodobieństwa zagrożenia przestępstwem ma przy tym spoczywać na organach państwa wnoszących o umożliwienie im

niejawnego gromadzenia informacji i podlegać ocenie sądu lub innego niezależnego organu”, po czym zauważył, iż „[c]hoć inne są cele czynności operacyjno-rozpoznawczych prowadzonych przez służby odpowiedzialne za utrzymanie porządku (np. Policję), inne zaś przez służby informacyjno-wywiadowcze (np. ABW, SKW), to z punktu widzenia naruszenia wolności i praw jednostki nie ma znaczenia, jaki organ władzy publicznej oraz na jakiej podstawie pozyskuje niejawnie informacje na jej temat. Stopień naruszenia prywatności i tajemnicy komunikowania się jest bowiem taki sam, bez względu na to, czy chodzi o ingerencję służb policyjnych, czy służb ochrony państwa”, i zwrócił uwagę, że „specyfika działalności służb informacyjno-wywiadowczych oraz związany z tym relatywnie wąsko określony zakres ich ustawowych zadań, może uzasadniać odmienne ustalenie zasad prowadzenia takich czynności i wykorzystywania zgromadzonych materiałów, od reguł obowiązujących pozostałe organy państwa, a zwłaszcza służby policyjne, mające szeroki zakres działania. Takie różnicowanie zasad prowadzenia czynności operacyjno-rozpoznawczych nie uchyla oczywiście wymogu przestrzegania zasady proporcjonalności” (op. cit.).

Kolejnym, wskazanym przez Trybunał Konstytucyjny, warunkiem dopuszczalności czynności operacyjno-rozpoznawczych jest to, aby niejawne pozyskiwanie w toku tych czynności informacji o jednostkach było środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. Trybunał Konstytucyjny wyjaśnił, że warunek ten oznacza, iż „*niejawna ingerencja w wolności i prawa, ma stanowić ultima ratio*”, oraz podkreślił, że „*[d]otyczy to w takiej samej mierze kontroli operacyjnej, jak i udostępniania danych telekomunikacyjnych czy innych form pracy operacyjno-rozpoznawczej o podobnym skutku dla jednostek*” (uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11, op. cit.).

W kontekście cytowanej wyżej wypowiedzi Trybunału Konstytucyjnego należy stwierdzić, że uzyskiwanie przez Policję danych telekomunikacyjnych,

danych pocztowych i danych internetowych **jest niewątpliwie przydatne** w celu zapobiegania i wykrywania **wszystkich przestępstw**.

Tego rodzaju regulacja zawarta w art. 20c ust. 1 ustawy o Policji jest zatem w stanie doprowadzić do zamierzonych przez nią skutków.

Szczegółowe argumenty potwierdzające tę tezę zostały przedstawione przez Trybunał Konstytucyjny w uzasadnieniu powołanego już wyroku w sprawie o sygn. akt K 23/11 z dnia 30 lipca 2014 r., gdzie Trybunał:

- podniósł, że „[w] obliczu rosnącego znaczenia nowych technologii wzrasta jednocześnie ryzyko wykorzystywania ich do popełniania przestępstw i naruszania prawa. Mogą być one bowiem wykorzystywane do nieuprawnionego pozyskiwania wiedzy o zachowaniach współobywateli, w tym o treściach oraz formach przekazywanych komunikatów, gromadzenia tychże danych na własne potrzeby i ich przetwarzania. Mogą ponadto stanowić narzędzie służące popełnianiu specjalistycznych i wyrafinowanych przestępstw zagrażających rozmaitym dobrom lub służyć komunikowaniu się czy integracji osób naruszających prawo. Zjawisko to jest niebezpieczne, ponieważ komunikowanie się za pomocą nowych technologii i przestępstwa popełniane z ich wykorzystaniem generalnie wymykają się spod kontroli społeczeństwa. Niejednokrotnie utrudnia to ustalenie tożsamości osób naruszających prawo, a w konsekwencji zapobieżenie i wykrycie takich zagrożeń”, oraz że „[r]ozwój technologiczny doprowadził zarazem, z jednej strony, do wykształcenia się nowych form popełniania <tradycyjnych> przestępstw. Internet i środki komunikowania się na odległość są dodatkowym, specjalistycznym narzędziem w rękach przestępców, istniejącym niejako równolegle do dotychczas wykorzystywanych technik. Z drugiej strony, wykształciły się nowe, nieistniejące wcześniej rodzaje przestępstw, możliwe do popełnienia wyłącznie z użyciem nowych technologii (tzw. cyberprzestępczość związana m.in. z nieuprawnionym dostępem do danych komputerowych)”;

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

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

nowych technologii teleinformatycznych w pozyskiwaniu wiedzy o działalności przestępczej, ustawodawca uprawnijący służby policyjne oraz służby ochrony państwa do niejawnego uzyskiwania informacji i dowodów za pomocą nowych technologii nie może ignorować specyfiki naruszeń prawa dokonanych z ich wykorzystaniem ani skali zjawiska w polskich realiach”;

- zwrócił uwagę na okoliczność, że „[c]iążący na organach państwa obowiązek zagwarantowania wolności i praw oznacza nie tylko zakaz nadmiernej ingerencji, w tym polegającej na niejawnym pozyskiwaniu przez organy państwa informacji o osobach, ale ma szerszy wymiar. Zdaniem Trybunału, wynika z niego obowiązek stworzenia przez państwo warunków, w których obywatele z zagwarantowanych im wolności i praw mogą swobodnie korzystać. Warunkiem zapewnienia wolności i praw jest zaś poczucie bezpieczeństwa w państwie i braku zagrożeń obywateli. Osiągnięcie tego stanu możliwe jest m.in. przez zwalczanie przestępczości mogącej zagrażać wolności człowieka, korzystaniu z własności czy podejmowaniu działalności gospodarczej. Z drugiej strony, zdaniem Trybunału, korelatem konstytucyjnego obowiązku państwa, o którym mowa w art. 5 Konstytucji, jest także prawo obywateli do ochrony ich bezpieczeństwa przed zewnętrznymi i wewnętrznymi zagrożeniami, w tym terroryzmem i przestępczością. Nie istnieje zatem niedająca się przezwyciężyć <naturalna antynomia> między zapewnieniem bezpieczeństwa i porządku publicznego a ochroną wolności i praw konstytucyjnych. Niekiedy bowiem wykorzystanie niejawnych metod pracy operacyjnej umożliwia ograniczenie skali przestępczości, a to przekłada się na podniesienie stopnia poczucia bezpieczeństwa obywateli i większą swobodę korzystania z zagwarantowanych im wolności i praw (podkr. wł.)”;

- po czym, w podsumowaniu przedstawionych w tej części uzasadnienia rozważań, stwierdził, że „[j]ednym z powszechnie uznanych instrumentów wykrywania zagrożeń i ścigania naruszeń prawa są czynności operacyjno-rozpoznawcze. Obejmują m.in. kontrolę operacyjną (podkr. wł.) [w

szczegółności z wykorzystaniem środków technicznych umożliwiających uzyskiwanie w sposób niejawnny informacji i dowodów oraz ich utrwalanie, przekazywanych za pomocą sieci telekomunikacyjnych], **a także gromadzenie i przetwarzanie danych telekomunikacyjnych** (podkr. wł.). Najogólniej rzecz ujmując, czynności te mają umożliwiać zapobieganie i zwalczanie zagrożeń w stopniu dotąd niespotykanym i niemożliwym do osiągnięcia za pomocą tradycyjnych metod analizy kryminalnej i pracy wywiadowczej (...).

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

Po drugie, **nowe technologie stanowią w zasadzie jedyne sposoby umożliwiający walkę z szeroko rozumianą tzw. cyberprzestępczością, to znaczy przestępstwami popełnianymi z wykorzystaniem nowych technologii**

teleinformatycznych (podkr. wł.). Zastosowanie czynności operacyjno-rozpoznawczych jest nie tyle udogodnieniem w pracy operacyjnej, lecz stanowi w większości wypadków praktycznie jedyny sposób zapobieżenia przestępstwu lub wykrycia ich sprawców” (op. cit.).

Jednocześnie, w uzasadnieniu wyroku w tej samej sprawie (sygn. akt K 23/11), Trybunał Konstytucyjny podniósł, że „[d]ostrzegając odmienności związane z wykorzystywaniem nowych technologii w celu popełniania tradycyjnych przestępstw i w celu popełniania szeroko rozumianych przestępstw komputerowych, **niezbędne jest, zdaniem Trybunału, wypracowanie zróżnicowanego podejścia do oceny proporcjonalności przepisów uprawniających do stosowania nowych technologii dla zapobiegania naruszeniom prawa, ich zwalczania i wykrywania, w zależności od sposobu użycia nowych technologii w celach niezgodnych z prawem** (podkr. wł.)” oraz zwrócił uwagę, że „[u]możliwienie służbom policyjnym i ochrony państwa pozyskiwania wiedzy o treści, czasie i formach komunikowania się jednostek, a także monitorowania ich aktywności życiowej w inny sposób, **nieuchronnie popada w kolizję z prawem do ochrony prywatności, ochroną tajemnicy komunikowania się, autonomią informacyjną, a w niektórych wypadkach (podśluchu lub monitoringu zainstalowanego w mieszkaniu) z nienaruszalnością mieszkania. Co więcej, samo istnienie przepisów uprawniających organy władzy wykonawczej do takiego rodzaju czynności winno być postrzegane jako ingerencja w konstytucyjnie chroniony status człowieka i obywatela, którego źródłem jest przyrodzona i niezbywalna godność** (podkr. wł.). Prawna dopuszczalność pozyskiwania informacji o jednostkach, niekiedy o sferach istotnych z punktu widzenia ich uczestnictwa w życiu publicznym, negatywnie wpływa na korzystanie przez nie z konstytucyjnych wolności i praw. Niezależnie od konkretnych, niekiedy zróżnicowanych form wkroczenia w sferę życia prywatnego, sama nawet świadomość znajdowania się pod ciągłym nadzorem władz publicznych może zniechęcać jednostki do

swobodnego korzystania z zagwarantowanych im konstytucyjnych wolności i praw. Może to rodzić obawy, że organy władzy publicznej będą w nieuprawniony sposób gromadzić i wykorzystywać informacje o osobach. Obawy te są wyjątkowo silne w polskim społeczeństwie, które przez dziesięciolecia reżimu komunistycznego było inwigilowane przez tajne służby bezpieczeństwa, najczęściej niesłużące dobrze rozumianym interesom własnego państwa i jego współobywateli.

*Z punktu widzenia konstytucyjnych gwarancji prawa do ochrony prywatności, a także ochrony tajemnicy komunikowania się, zdaniem Trybunału, ingerencją władzy publicznej w tę sferę jest nie tylko pozyskanie przez władze publiczne danych o jednostce po raz pierwszy. Ochrona prawa do prywatności i tajemnicy komunikowania się rozciąga się bowiem na cały proces pozyskiwania, gromadzenia, przechowywania oraz przetwarzania (w tym analizowania i porównywania) informacji o jednostkach. Dlatego też **jako odrębne przejawy ingerencji w konstytucyjnie chroniony status jednostki - wymagające każdorazowo odrębnej legitymizacji konstytucyjnej - należałoby traktować pozyskiwanie informacji m.in. o treści komunikatów przekazywanych za pomocą sieci teleinformatycznych w toku kontroli operacyjnej, nałożenie na dostawców usług telekomunikacyjnych obowiązku zatrzymywania danych o ruchu i lokalizacji, dostęp do tych danych, ich następczą weryfikację czy przekazanie innym organom** (podkr. wł.)” [op. cit.].*

Odnośnie natomiast do **wymogu konieczności**, jakiemu muszą sprostać wprowadzone do art. 20c ust. 1 ustawy o Policji ograniczenia praw i wolności konstytucyjnych, określonych w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, polegające na możliwości uzyskiwania (niejawnie) przez Policję danych telekomunikacyjnych, danych pocztowych i danych internetowych w celu zapobiegania lub wykrywania przestępstw, należy podnieść następujące kwestie.

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, kontrolując zgodność z art. 47 i art. 49 w związku

z art. 31 ust. 3 Konstytucji art. 20c ust. 1 ustawy o Policji, w brzmieniu tego przepisu obowiązującym do dnia 6 lutego 2016 r., to jest w brzmieniu sprzed wejścia w życie (7 lutego 2016 r.) ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U., poz. 147, dalej: ustawa zmieniająca z dnia 15 stycznia 2016 r.) [wówczas przepis ten brzmiał: „(w) celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej «danymi telekomunikacyjnymi», oraz może je przetwarzać.”] stwierdził, iż „[z] wykładni językowej art. 20c ust. 1 ustawy o Policji wynika, że funkcjonariuszom Policji mogą być udostępnione dane telekomunikacyjne w celu <zapobiegania lub wykrywania> **każdego czynu uznawanego za przestępstwo** (podkr. wł.), a nawet - co nie jest definitywnie wykluczone - również przestępstwo skarbowe. Jedyne ograniczeniem jest to, by zapobieganie określonemu przestępstwu lub jego wykrywanie mieściło się w ramach ustawowych zadań tej formacji, określonych w art. 1 ustawy o Policji. **Katalog owych zadań jest jednak szeroki** (podkr. wł.). Ustawodawca przewidział, że do zadań Policji należy m.in. ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra (art. 1 ust. 2 pkt 1); ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania (art. 1 ust. 2 pkt 2), czy wreszcie wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców (art. 1 ust. 2 pkt 4). Zwłaszcza z brzmienia art. 1 ust. 2 pkt 4 można wyprowadzić wniosek, zgodnie z którym do zadań Policji należy wykrywanie każdego czynu uznawanego za przestępstwo w świetle prawa polskiego. Odnosząc te ustalenia do wykładni zakwestionowanego art. 20c ust. 1 ustawy o Policji, należałoby w konsekwencji przyjmować, że żądanie udostępnienia danych telekomunikacyjnych będzie również możliwe w celu zapobiegania wszelkim czynom przestępnym lub ich

wykrywania. Tym samym uzasadnione jest stwierdzenie, że ustawodawca określił cel udostępnienia Policji danych telekomunikacyjnych w sposób bardzo ogólny.

Trybunał Konstytucyjny przypomina, że ingerencja w konstytucyjne prawo do ochrony prywatności (art. 47) i tajemnicę komunikowania się (art. 49 Konstytucji) może mieć miejsce nie tylko w wypadku zapoznawania się organów władzy publicznej z samą treścią komunikatów przekazywanych między jednostkami, ale również w sytuacji pozyskania przez władze informacji towarzyszących temu procesowi (podkr. wł.) [...]. Takie stanowisko - jak zwrócono wcześniej uwagę - zajął również TSUE (Trybunał Sprawiedliwości Unii Europejskiej - przyp. wł.) w wyroku z 8 kwietnia 2014 r. (w połączonych sprawach: C-293/12 i C-594/12 - przyp. wł.), stwierdzając nieważność dyrektywy 2006/24/WE (dyrektywy Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE - przyp. wł.). Oznacza to, że udostępnienie Policji danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego stanowi ingerencję w prawo do ochrony prywatności i ochrony tajemnicy komunikowania się. Jakkolwiek tego rodzaju ingerencja jest obecnie nieunikniona, bo Policja musi dysponować instrumentarium pozwalającym jej na efektywną walkę z przestępczością, to jednak dopuszczalność tego środka uzależniona jest od spełnienia wymagań wynikających z zasady proporcjonalności (art. 31 ust. 3 Konstytucji) [podkr. wł.]” (op. cit.).

I wreszcie zasadniczym, wskazywanym przez Trybunał Konstytucyjny, warunkiem dopuszczalności czynności operacyjno-rozpoznawczych jest to, aby niejawnemu pozyskiwaniu w toku tych czynności informacji o jednostkach towarzyszyły odpowiednie gwarancje proceduralne.

W uzasadnieniu wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny, badając konstytucyjność art. 20c ust. 1 ustawy o Policji w

brzmieniu tego przepisu obowiązującym do dnia 6 lutego 2016 r. i stwierdzając, że na jego podstawie „*Policja może pozyskiwać dane telekomunikacyjne nie tylko dla zwalczania poważnych przestępstw, ale także w sprawach mniejszej wagi*” oraz że „*ustawodawca nie uzależniał możliwości żądania danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie - wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji*”, jednocześnie zauważył, iż „*[w] takiej sytuacji tym większe znaczenie ma ustanowienie gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych* (podkr. wł.)” [op. cit.].

Tym samym Trybunał Konstytucyjny nawiązał nie tylko do, cytowanych wyżej, tez uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., ale też do wcześniejszej swojej wypowiedzi, zawartej w uzasadnieniu tego samego wyroku w sprawie o sygn. akt K 23/11, w której przypominał, iż „*[n]iejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. To znaczy, że niejawna ingerencja w wolności i prawa, ma stanowić ultima ratio. Dotyczy to w takiej samej mierze kontroli operacyjnej, jak i udostępniania danych telekomunikacyjnych czy innych form pracy operacyjno-rozpoznawczej o podobnym skutku dla jednostek* (podkr. wł.)”, po czym stwierdził, że „*[z] przesłanką subsydiarności wiąże się wprowadzenie proceduralnego wymogu, którym jest kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa. Pożądane jest powierzenie kompetencji w tym zakresie niezależnym i niezawisłym sądom, dającym rękojmię odpowiednio wysokiego stopnia wiedzy i doświadczenia życiowego. Z punktu widzenia Konstytucji sądowa kontrola nad czynnościami operacyjno-rozpoznawczymi jest rozwiązaniem optymalnym. Nie jest jednak bezwzględnie konieczna. Kompetencje tego rodzaju mogą zostać też powierzone innym organom państwa, których status ustrojowy i zakres*

ustawowych kompetencji gwarantuje efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa.

Ustawowe unormowania kontroli muszą wykluczać jej fasadowość. Ustawodawca jest zatem obowiązany wyposażyć sądy bądź inne organy w kompetencje pozwalające na ocenę celowości i subsydiarności czynności operacyjno-rozpoznawczych, jak również sposobów ich prowadzenia w indywidualnej sprawie względem konkretnych podmiotów (podkr. wł.). Niezbędnym warunkiem rzetelności tej kontroli jest generalny obowiązek uzasadniania decyzji w sprawie wyrażenia zgody na ich podjęcie, a także wskazania podmiotu, czasu prowadzenia kontroli, a także szczegółowego zakresu pozyskiwanych informacji. Trybunał przyjmuje, że podstawową rolę należy przypisać kontroli uprzedniej (ex ante) [podkr. wł.], która powinna być traktowana jako zasada przynajmniej wtedy, gdy organy państwa pozyskują w sposób niejawnny informacje o jednostkach związane z treścią przekazywanych wiadomości. Nie jest jednakże wykluczone wprowadzenie kontroli następczej, czyli legalizującej uprzednio podjęte zgodnie z ustawową procedurą czynności operacyjno-rozpoznawcze (podkr. wł.)” [op. cit.].

Idąc tym tokiem rozumowania, Trybunał Konstytucyjny, badając w sprawie o sygn. akt K 23/11 zgodność art. 20c ust. 1 ustawy o Policji, w brzmieniu tego przepisu obowiązującym do dnia 6 lutego 2016 r., z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, **w pierwszej kolejności odniósł się do zarzutu niedostatecznych gwarancji proceduralnych, związanych z brakiem zewnętrznej kontroli udostępniania danych telekomunikacyjnych.** Zarzut ten pozostawał bowiem wspólny dla wszystkich przepisów, które zostały zakwestionowane w ramach tej grupy (do tej grupy, poza art. 20c ust. 1 ustawy o Policji, należały przepisy 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 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW, art. 18 ust. 1 pkt 1 ustawy o

CBA i art. 75d ust. 1 ustawy o Służbie Celnej)). Jednocześnie Trybunał Konstytucyjny podniósł, że stwierdzenie niekonstytucyjności tych przepisów w omawianym zakresie (niedostateczne gwarancje proceduralne) „*uczyni zbędnym odnoszenie się do pozostałych zarzutów sformułowanych przez wnioskodawców, a związanych z dopuszczalnością pozyskiwania danych również w celu zapobiegania przestępstwom o relatywnie niewielkim stopniu społecznej szkodliwości oraz ich ścigania, czy z brakiem przesłanki subsydiarności*” (podkr. wł.) [op. cit.].

W tej części rozważań, zawartych w uzasadnieniu wyroku z dnia 30 lipca 2014 r., Trybunał Konstytucyjny stwierdzi, że „*[j]ednym z wymagań, które powinny spełniać przepisy ustawowe upoważniające Policję do pozyskiwania danych telekomunikacyjnych, jest wykreowanie mechanizmu niezależnej kontroli. Skoro pozyskiwanie tych danych dokonuje się w sposób niejawnny, bez wiedzy i woli podmiotów, o których informacje są przez Policję gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć* (podkr. wł.). *Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji. Policja może pozyskiwać dane telekomunikacyjne nie tylko dla zwalczania poważnych przestępstw, ale także w sprawach mniejszej wagi, czy wręcz - jak to określił w piśmie z 2 marca 2012 r. Marszałek Sejmu - w sprawach błahych.* (...)”

Zakwestionowany art. 20c ust. 1 ustawy o Policji, ani żaden inny przepis, nie nakłada obowiązku uzyskania zgody sądu (bądź innego organu, który byłby niezależny od organów żądających udostępnienia tych danych lub organów nad nimi nadrzędnych) na udostępnienie Policji danych, o których mowa w art. 180c

i art. 180d prawa telekomunikacyjnego. Procedura ta - jak zresztą wcześniej podkreślono - nie wymaga nawet uzyskania zgody prokuratora. Ustawodawca nie przewidział też zrębowych elementów kontroli ex post legalizującej podjęte działania. Pozyskiwanie danych telekomunikacyjnych przez funkcjonariuszy Policji pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane (podkr. wł.).

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

Trybunał Konstytucyjny nie przesądza w tym miejscu, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału, nie jest wobec tego wykluczone - w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych - wprowadzenie, jako zasady, kontroli następcej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres

zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami (podkr. wł.) [...]

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

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

Trzeba w tym miejscu przypomnieć, że TSUE, odnosząc się do kwestii, czy ingerencja, którą zakładała dyrektywa 2006/24, zobowiązująca do zatrzymywania wszystkich danych o ruchu związanych z telefonią stacjonarną i mobilną, dostępem do Internetu, pocztą elektroniczną oraz telefonią internetową, jest ograniczona do tego, co ściśle niezbędne, w uzasadnieniu wyroku z dnia 8 kwietnia 2014 r. (wyrok ten stanowił podstawę rozważań Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11) stwierdził, że „po pierwsze, (...) dyrektywa 2006/24 obejmuje generalnie wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, **przy czym nie przewidziano**

w niej jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw (podkr. wł.).

Z jednej bowiem strony dyrektywa 2006/24 obejmuje całościowo wszystkie korzystające z usług łączności elektronicznej osoby, których dane zatrzymywane są nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego. **Ma ona zastosowanie nawet wobec tych osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami (podkr. wł.).** Ponadto dyrektywa nie przewiduje żadnych wyjątków, a więc **w rezultacie stosuje się nawet wobec tych osób, których komunikacja na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową (podkr. wł.).**

Z drugiej strony, **mając jednocześnie na celu przyczynienie się do walki z poważną przestępczością, dyrektywa ta nie wymaga istnienia żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego (podkr. wł.);** w szczególności dyrektywa nie ogranicza się do zatrzymywania danych związanych albo z określonym czasem, określonym obszarem geograficznym lub określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, albo osobami, których zatrzymane dane z innych powodów mogłyby przyczynić się do zapobiegania poważnym przestępstwom oraz ich wykrywania lub ścigania.

Po drugie, dyrektywa 2006/24 nie tylko nie wyznacza ogólnych granic swojego zakresu zastosowania, ale także nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw, które z uwagi na zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty (Karty Praw Podstawowych UE - przyp. wł.), **można uznać za wystarczająco poważne, by taką ingerencję uzasadnić (podkr. wł.).** Przeciwnie, dyrektywa 2006/24

ogranicza się do ogólnego odesłania, w art. 1 ust. 1, do pojęcia <poważnych przestępstw> określonych w ustawodawstwie każdego państwa członkowskiego.

Ponadto dyrektywa nie określa żadnych materialnych i proceduralnych przesłanek, w przypadku zaistnienia których właściwe organy krajowe będą mogły uzyskać dostęp do danych i następnie je wykorzystać. Artykuł 4 tej dyrektywy, regulujący kwestię dostępu tych organów do zatrzymanych danych, nie stanowi wyrażnie, że możliwość dostępu do tych danych i ich późniejszego wykorzystania **powinna być ściśle ograniczona celami zapobiegania i wykrywania dokładnie określonych poważnych przestępstw lub ich ścigania** (podkr. wł.), a jedynie wskazuje, że każde państwo członkowskie ma określić procedury i warunki uzyskiwania dostępu do zatrzymanych danych, mając na uwadze wymogi konieczności i proporcjonalności.

W szczególności dyrektywa 2006/24 nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby ograniczyć liczbę osób uprawnionych do uzyskiwania dostępu i późniejszego wykorzystywania zatrzymanych danych do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu. Przede wszystkim to **uzyskanie przez właściwe organy krajowe dostępu do danych nie podlega uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które pilnowałyby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu, oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw** (podkr. wł.). Co więcej, dyrektywa nie nakazuje państwom członkowskim w sposób wyraźny ustanowienia takich mechanizmów” (<http://curia.europa.eu/juris/document/document.jsf?docid=150642>).

Uzupełniając trzeba dodać, że w dniu 5 maja 2016 r. weszła w życie dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE.L.2016.119.132) [dalej dyrektywa 2016/680].

Dyrektywa 2016/680 ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, przy czym „dane osobowe” (na użytek tej dyrektywy) oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), a możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”, zaś „przetwarzanie” - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (*vide* - artykuł 1 ust. 1 i ust. 3 pkt 1 i 2 dyrektywy 2016/680).

We wstępnej części dyrektywy 2016/680 wskazuje się, że:

- „[p]rzetwarzanie danych osobowych musi być zgodne z prawem, rzetelne i przejrzyste względem zainteresowanej osoby fizycznej oraz służyć wyłącznie

konkretnym celom określonym prawem. Nie stanowi to dla organów ścigania przeszkody w prowadzeniu czynności takich jak nadzór niejawni lub monitoring wizyjny. Czynności takie można prowadzić do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jeżeli czynności te są określone prawem i stanowią środek niezbędny i proporcjonalny w społeczeństwie demokratycznym, z należyтым uwzględnieniem uzasadnionych interesów danej osoby fizycznej. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 Karty i w art. 6 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej <EKPC>). Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. Wyraźne, uzasadnione i określone w momencie zbierania danych osobowych powinny być w szczególności konkretne cele ich przetwarzania. Dane osobowe powinny być adekwatne i właściwe w stosunku do celów przetwarzania. Należy w szczególności zapewnić, by zebrane dane osobowe nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania. **Dane osobowe powinny być przetwarzane tylko wtedy, gdy celu przetwarzania nie można rozsądnie osiągnąć innymi sposobami** (podkr. wł.). Aby zapobiec przechowywaniu danych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia dla danych osobowych przechowywanych dłużej w celu archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych” (motyw 26);

- „[z]apobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych wymaga, aby właściwe organy przetwarzały dane osobowe – zebrane w kontekście zapobiegania konkretnym czynom zabronionym, prowadzenia postępowań przygotowawczych w ich sprawie, wykrywania ich lub ścigania – w kontekście szerszym, dla lepszego zrozumienia działalności przestępczej oraz ustalenia powiązań pomiędzy różnymi wykrytymi czynami zabronionymi.” (motyw 27);

- „[d]ane osobowe należy zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach mieszczących się w zakresie zastosowania niniejszej dyrektywy i nie należy ich przetwarzać w celach niezgodnych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych i wykonywaniem kar, w tym z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom. Jeżeli dane osobowe przetwarza ten sam lub inny administrator w celu wchodzącym w zakres stosowania niniejszej dyrektywy, ale innym niż cel, w którym dane zostały zebrane, przetwarzanie takie powinno być dopuszczalne, pod warunkiem że przetwarzanie jest dozwolone na mocy mających zastosowanie przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu” (motyw 29);

oraz, że:

- „[z]asadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, które mają możliwość wykonywania swych funkcji w sposób całkowicie niezależny. Organy nadzorcze powinny monitorować stosowanie niniejszej dyrektywy oraz powinny przyczyniać się do ich spójnego stosowania w całej Unii, po to by chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją” (motyw 75);

- [k]ażda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka prawnego przed sądem zgodnie z art. 47 Karty praw podstawowych, jeżeli uzna, że jej prawa wynikające z przepisów przyjętych na podstawie niniejszej dyrektywy są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, w części lub w całości ją odrzuca lub oddala lub nie podejmuje działania, choć jest ono niezbędne do ochrony praw osoby, której dane dotyczą. Postępowanie wyjaśniające w sprawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiednim do konkretnej sprawy. Właściwy organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien przedsięwziąć takie środki, jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji” (motyw 85).

Warto dodać, że zgodnie z artykułem 63 ust. 1 dyrektywy 2016/680, „[p]aństwa członkowskie przyjmują i publikują do dnia 6 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Tekst tych przepisów niezwłocznie przekazują Komisji. **Państwa członkowskie stosują te przepisy od dnia 6 maja 2018 r.** (podkr. wł.)”. Wyjątkiem jest art. 25 ust. 1 tej dyrektywy dotyczący ewidencjonowania operacji przetwarzania danych w systemach zautomatyzowanych (przepisy artykułu 63 ust. 2 i 3 dyrektywy 2016/680, w wyjątkowych okolicznościach dopuszczają bowiem transpozycję tego przepisu w dłuższym terminie).

Wprawdzie w powołanym wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 20c ust. 1 ustawy o Policji,

którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych i danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału w zakresie pozyskiwania przez Policję danych telekomunikacyjnych można również odnieść do pozyskiwania przez Policję pozostałych danych wymienionych w tym przepisie, jak również do samych danych telekomunikacyjnych, ponieważ w zakresie tych ostatnich danych zarówno treść art. 20c ust. 1 ustawy o Policji jak i jego otoczenie normatywne, jak dotychczas (pomimo krytycznej oceny Trybunału), nie uległy postulowanej zmianie.

Policja nadal bowiem może uzyskiwać dane telekomunikacyjne, a, dodatkowo, także dane pocztowe i dane internetowe, „w sprawach mniejszej wagi, czy wręcz (...) w sprawach błahych”.

Co więcej, ustawodawca **nadal** nie uzależnia możliwości żądania wymienionych w tym przepisie danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie - wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji (zasada subsydiarności) [*vide* też - motyw 26 dyrektywy 2016/680].

Niemniej jednak należy podkreślić – co w niniejszej sprawie jest kluczowe i co wiąże się z przesłanką subsydiarności – że ustawodawca zapewnił kontrolę nad niejawnym pozyskiwaniem przez Policję danych o osobach przez niezależny od rządu organ państwa (sąd okręgowy właściwy dla siedziby składającego wniosek organu Policji), i kontrola ta może zostać uznana za dostateczną.

Ustawa zmieniająca z dnia 15 stycznia 2016 r., której zakładanym celem, co też należy podkreślić, było wykonanie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, wprowadziła do ustawy o Policji art. 20ca, w brzmieniu:

„Art. 20ca. 1. Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.

2. Organ Policji, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd okręgowy informuje organ Policji o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 20cb ust. 1 (przepis ten upoważnia Policję do uzyskiwania, między innymi w celu zapobiegania lub wykrywania przestępstw, danych z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

W uzasadnieniu tej zmiany wskazano, że realizuje ona wyrok „Trybunału Konstytucyjnego w sprawie K 23/11, stwierdzający niezgodność z Konstytucją RP obecnych uregulowań nieprzewidujących niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy - Prawo telekomunikacyjne, w projekcie ustawy zaproponowano, aby podmiotem uprawnionym do kontroli uzyskiwania danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku –

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

Jednocześnie na uprawnione formacje został nałożony obowiązek przekazywania określonemu powyżej sądowi, raz na 6 miesięcy, sprawozdań obejmujących: liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz ich rodzaj; rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe; liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane. W ramach kontroli sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie danych. Sąd informuje szefa służby o wyniku kontroli w terminie 30 dni od jej zakończenia.

Z uwagi na konieczność opracowania kompleksowego ujęcia materii, obok danych telekomunikacyjnych, kontrolą sądową objęto również proces udostępniania uprawnionym służbom danych pocztowych, określonych na podstawie ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2012 r. poz. 1529) oraz tzw. danych internetowych, określonych w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422). Pomimo, że pkt 5 wyroku Trybunału o sygn. K 23/11 nie obejmuje swoim zakresem danych uzyskiwanych na podstawie prawa pocztowego oraz danych uzyskiwanych na podstawie ustawy o świadczeniu usług drogą elektroniczną, powyższe rozszerzenie zakresu przedmiotowego kontroli znajduje uzasadnienie w tym, że działalność służb w tych obszarach w podobnym stopniu ingeruje w prawa i wolności obywatelskie jak proces pozyskiwania danych telekomunikacyjnych. Projekt przewiduje

również takie same przesłanki udostępniania, procedury weryfikacji oraz niszczenia udostępnianych służbom danych pocztowych oraz danych, o których mowa w ustawie o świadczeniu usług drogą elektroniczną, zbędnych dla prowadzonego postępowania. Skorelowanie regulacji prawnych w stosunku do wszystkich obszarów danych dotyczących sfery komunikacji między osobami stanowi rozwiązanie systemowe służące pogłębieniu zaufania obywateli do organów państwowych” (uzasadnienie projektu ustawy zmieniającej z dnia 15 stycznia 2016 r., Sejm VIII kadencji, druk nr 154).

Zdaniem Rzecznika Praw Obywatelskich, procedury kontrolne wprowadzone ustawą zmieniającą z dnia 15 stycznia 2016 r. budzą poważne wątpliwości konstytucyjne.

Rzecznik wskazał, iż „[k]westia zapewnienia realnej uprzedniej kontroli sądowej była przedmiotem rozważań Trybunału Sprawiedliwości UE w połączonych sprawach C-293/12 i C-594/12, gdzie TSUE stwierdził wyraźnie - analizując przepisy dyrektywy 2006/24/WE - że nie przewidywała ona uprzedniej kontroli sądu lub niezależnego organu administracyjnego, który pilnowałby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. Brak uprzedniej kontroli sądu lub niezależnego organu TSUE uznał za nieuzasadnioną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 KPP UE” (uzasadnienie wniosku, s. 48-49).

Wnioskodawca zauważył, iż „[w] przepisach dotyczących poszczególnych służb wskazuje się na właściwość sądu okręgowego (lub odpowiednio innych sądów) [do przeprowadzania kontroli - przyp. wł.] w tzw. trybie następczym. Kontrola ta ma polegać na analizie półrocznych sprawozdań przedkładanych sądom przez służby. Należy podkreślić, że w przypadku zakwestionowanych we wniosku ustaw ustawodawca nie podjął się żadnego

wyważenia potrzeby wprowadzenia uprzedniej kontroli, a ponadto - w odniesieniu do kontroli następczej - skonstruował ją w ten sposób, że w praktyce może mieć ona charakter iluzoryczny. Sprawozdania służb kierowane co pół roku do właściwego sądu w oparciu o przepisy o ochronie informacji niejawnych nie będą stanowiły informacji publicznej, chociaż będą zawierały informacje dotyczące liczby przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, a także kwalifikacji prawnej czynów, w związku z zaistnieniem których wystąpiono o dane. Przeprowadzenie czynności kontrolnych przez sąd będzie mieć charakter fakultatywny, a nie obligatoryjny. Ponadto, sąd po przeprowadzeniu kontroli będzie mógł jedynie poinformować kontrolowaną służbę o wynikach kontroli, ale nie będzie mógł zarządzić zniszczenia zgromadzonych danych” oraz iż „[w]ydaje się, że przy dużej skali pozyskiwanych danych oraz stosunkowo dużym odstępie czasowym, kontrola ta może mieć w istocie charakter iluzoryczny i nie spełniać wymogów wynikających z Konstytucji RP, a także ze wskazanych umów międzynarodowych. Zaproponowana forma kontroli jest zatem niewystarczająca. Kontrola następcza nie powinna być stosowana domyślnie, lecz może być dopuszczalna jedynie wyjątkowo, w sytuacjach, w których zachodzi potrzeba natychmiastowego działania służb. Zakwestionowane przepisy ustaw w żadnym przypadku nie przewidują przeprowadzenia kontroli uprzedniej. Dzięki takiemu mechanizmowi przypadki sięgania po dane mogłyby podlegać rzetelnej ocenie pod względem spełniania kryteriów niezbędności, adekwatności i celowości. Podkreślenia wymaga, że zgodnie z art. 51 ust. 2 Konstytucji RP, władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Przewidziana forma kontroli nie gwarantuje w sposób realny przestrzegania tych zasad, a przede wszystkim nie blokuje możliwości pozyskiwania danych nawet wtedy, gdyby miało ono nastąpić z naruszeniem tychże zasad” (uzasadnienie wniosku, s. 49-50).

Rzecznik dodał, że, zgodnie z art. 20ca ust. 5 ustawy o Policji (i, odpowiednio, w przypadku pozostałych zaskarżonych w tej grupie przepisów regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego), „żadnej kontroli nie podlega uzyskiwanie danych, pozyskiwanych na podstawie art. 20cb ust. 1 ustawy o Policji. Należy w tym miejscu wskazać, że ustawa o Policji i analogicznie pozostałe ustawy spod jakiegokolwiek kontroli wyłączają pozyskiwanie danych nie tylko określonych w art. 179 ust. 9 Prawa telekomunikacyjnego, ale również całego art. 161 Prawa telekomunikacyjnego, co znacząco poszerza zakres dostępu do danych wyłączonych spod jakiegokolwiek kontroli” (uzasadnienie wniosku, s. 51).

Biorąc pod uwagę tezy zawarte w uzasadnieniu wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11 oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 20ca ustawy o Policji **mechanizm kontroli** nad uzyskiwaniem przez Policję danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane, **stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.**

Wprawdzie kontrola dotyczy jedynie zbiorczych danych ujętych przez organ Policji w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to nie można nie dostrzec, iż, zgodnie z art. 20ca ust. 3 ustawy o Policji, „sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie policji danych telekomunikacyjnych, pocztowych lub internetowych”.**

Zapis ten oznacza, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi, posiadanymi przez organ Policji materiałami uzasadniającymi

wniosek o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 20c ust. 1 ustawy o Policji. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 20ca ust. 2 ustawy o Policji, to można zasadnie stwierdzić, że kontroli sądu okręgowego podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 20c ust. 6 i 7 ustawy o Policji).

Należy przy tym zauważyć, iż ocena przez kontrolujący sąd prawidłowości wniosku organu Policji o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Komendanta Głównego Policji, Komendanta Centralnego Biura Śledczego Policji oraz komendantów wojewódzkich Policji (*vide* - art. 20c ust. 5 ustawy o Policji).

Istotnym zapisem gwarancyjnym jest, wprowadzony w art. 20c ust. 7 ustawy o Policji, obowiązek **niezwłocznego**, komisyjnego i protokolarnego zniszczenia danych, które nie mają znaczenia dla postępowania karnego.

Termin „niezwłocznie” oznacza, jak powszechnie wiadomo, **bez zbędnej zwłoki**.

Jest zatem oczywiste, że „**niezwłocznie**” nie oznacza „**natychmiast**”.

Aby mogło nastąpić niezwłoczne zniszczenie danych niemających znaczenia dla postępowania karnego, należy uwzględnić realia konkretnej sprawy, a przede wszystkim możliwości techniczne i uwarunkowania wynikające z obowiązujących regulacji prawnych, w tym regulacji wiążących się z

przetwarzaniem danych telekomunikacyjnych, pocztowych i internetowych (podobna definicja terminu „niezwłocznie” przyjmowana jest, na przykład, na gruncie art. 245 Kodeksu postępowania karnego, *vide* - komentarz do tego przepisu T. Grzegorzcyka, [w:] T. Grzegorzcyk, *Kodeks postępowania karnego. Komentarz. Tom I. Artykuły 1-467*, 6. wydanie, Wydawnictwo a Wolters Kluwer business, Warszawa 2014, s. 874 oraz postanowienie Sądu Najwyższego z dnia 13 października 2011 r., w sprawie o sygn. akt III KK 64/11, LEX nr 1101660).

W konsekwencji, przy konkretyzacji w poszczególnych sprawach użytego w art. 20c ust. 7 ustawy o Policji terminu „niezwłocznie”, należy uwzględnić wymóg przedstawienia kontrolującemu sądowi okręgowemu wszystkich materiałów uzasadniających udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych, zadekretowany w art. 20ca ust. 3 tejże ustawy.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 20ca ustawy o Policji mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Policji w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość**. Wszak sądowi okręgowemu umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu**.

Powyższe przesądza, że art. 20c ust. 1 w związku z art. 20ca ustawy o Policji, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, **jest zgodny z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3, a także zgodny z art. 30 Konstytucji**.

W ocenie Rzecznika, konsekwencją niezgodności art. 20c ust. 1 ustawy o Policji z art. 47, art. 49 i art. 51 ust. 2 Konstytucji jest godzenie w prawo do zachowania godności człowieka, gwarantowane w art. 30 Konstytucji.

Zgodnie z art. 30 ustawy zasadniczej, „[p]rzyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych”.

W uzasadnieniu wyroku z dnia 18 października 2017 r., w sprawie o sygn. akt K 27/15, Trybunał Konstytucyjny stwierdził, że *„Ustrojodawca uczynił z godności człowieka podstawę odniesienia dla systemu wartości, wokół którego zbudowano Konstytucję. Jak wskazał Trybunał w wyroku z 30 września 2008 r. o sygn. K 44/07 (OTK ZU nr 7/A/2008, poz. 126), <Art. 30 Konstytucji jest postanowieniem wiodącym dla wykładni i stosowania wszystkich pozostałych postanowień o prawach, wolnościach i obowiązkach jednostki. Podkreśla to także preambuła do Konstytucji, która wzywa wszystkich stosujących konstytucję do tego, «aby czynili to, dbając o zachowanie przyrodzonej godności człowieka...», a także art. 233 ust. 1 Konstytucji, zakazując w sposób bezwzględny naruszania godności człowieka nawet w razie wprowadzenia nadzwyczajnego stanu państwowego>. Zarówno ustawodawca, jak i organy stosujące prawo mają więc obowiązek respektować treści zawarte w pojęciu godności, które przysługują każdemu człowiekowi. Godność nie jest cechą czy zespołem praw, które mogą być ograniczone przez państwo.*

Z wyrażonej w art. 30 Konstytucji zasady nienaruszalności, poszanowania i ochrony godności człowieka wynikają istotne konsekwencje. Zasada nienaruszalności godności ma charakter powszechny, a jej adresatem jest każdy, także podmioty prawa prywatnego. W piśmiennictwie podkreśla się, że powszechność tego zakazu wynika z absolutnej wartości tego dobra prawnego, szacunku dla życia i bezpieczeństwa człowieka (...).

Zasada poszanowania godności zakłada, że wszelkie działania władzy publicznej powinny uwzględniać istnienie pewnej sfery autonomii, w ramach której człowiek może się realizować społecznie. Chodzi o elementy najważniejsze dla tożsamości jednostki, które dotyczą jej samookreślenia, integralności fizycznej i psychicznej, utrzymania relacji z innymi osobami, a także jej bezpiecznego miejsca w społeczności. Działania władz publicznych nie mogą prowadzić do tworzenia sytuacji prawnych lub faktycznych, które naruszałby tę autonomię, odbierając jednostce poczucie godności. W swoim orzecznictwie Trybunał podkreślał, że człowiek powinien być traktowany jako wolny, autonomiczny podmiot, zdolny do rozwijania swojej osobowości i kształtowania swojego postępowania (...). Takie rozumienie godności powoduje, że niedopuszczalne są wszelkie sytuacje, w których człowiek staje się wyłącznie przedmiotem działań podejmowanych przez władze, a jego rola zostaje sprowadzona do czysto instrumentalnej postaci (...).

Trybunał w swoim orzecznictwie podkreślał, że jedną z przesłanek poszanowania godności człowieka jest <istnienie pewnego minimum materialnego, zapewniającego jednostce możliwość samodzielnego funkcjonowania w społeczeństwie> (wyrok TK z 4 kwietnia 2001 r., sygn. K 11/00). Pogląd ten znalazł potwierdzenie również w piśmiennictwie, gdzie wskazywano, że odmowa udzielenia pomocy materialnej osobie ubogiej w krytycznej sytuacji może być uznana - wedle obiektywnych miar właściwych godności ludzkiej - za wyraz pogardy dla człowieka (...).

Władza publiczna musi nie tylko sama powstrzymać się przed działaniami naruszającymi godność (obowiązek jej poszanowania), ale także ochraniać ją przed zachowaniami osób trzecich. Rodzi to obowiązek władz stworzenia systemu procedur, prawnych nakazów i zakazów zapobiegających wszelkim naruszeniom i zagrożeniom godności. O ile bowiem zakaz naruszania godności ma charakter bezwzględny i dotyczy wszystkich, o tyle to na władze publiczne został nałożony

obowiązek poszanowania i ochrony godności” (OTK ZU seria A z 2017 r., poz. 74).

Niewątpliwie prywatność, tajemnica komunikowania się czy autonomia informacyjna jednostki to jedne z podstawowych potrzeb każdego i dlatego stanowią one konieczne elementy zabezpieczenia poszanowania godności ludzkiej. Stąd trzeba przyjąć, iż naruszenie choćby jednego z tych elementów powoduje jednocześnie naruszenie art. 30 Konstytucji.

Ponadto (w tym przypadku także w konsekwencji wykazanej wyżej zgodności z art. 47, art. 49 i art. 51 ust. 2 Konstytucji), art. 20c ust. 1 w związku z art. 20ca ustawy o Policji, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, **jest również zgodny** z art. 8 Konwencji oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Zgodnie z art. 8 Konwencji, „[k]ażdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji” (ust. 1) oraz „[n]iedopuszczalna 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 i moralności lub ochronę praw i wolności innych osób (ust. 2).

Z kolei art. 7 Karty Praw Podstawowych UE wyraża prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się, zaś art. 8 - prawo każdej osoby do ochrony danych osobowych, które go dotyczą.

Przesłanki dopuszczalnego ograniczenia tych praw zostały natomiast zawarte w art. 52 ust. 1 powołanej wyżej Karty, który to przepis brzmi: „[w]szelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu

ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.”.

Z powyższego wynika, że treść normatywna art. 8 ust. 1 Konwencji, a także art. 7 i art. 8 Karty Praw Podstawowych UE odpowiada treści normatywnej art. 47, art. 49 i art. 51 ust. 2 Konstytucji, zaś treść normatywna art. 8 ust. 2 Konwencji i art. 52 ust. 1 Karty Praw Podstawowych UE odpowiada treści normatywnej art. 31 ust. 3 Konstytucji.

Stąd konsekwencją zgodności zaskarżonej regulacji z wzorcami konstytucyjnymi jest **zgodność** tej regulacji także z art. 8 Konwencji oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Wnioskodawca, już tylko samemu art. 20ca ustawy o Policji (bez powiązania treściwego tego przepisu z art. 20c ust. 1 ustawy o Policji), zarzucił niezgodność także z art. 2 Konstytucji, jednak zarzutu tego nie uzasadnił ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonemu w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Dlatego też postępowanie w zakresie kontroli zgodności art. 20ca ust. 1 ustawy o Policji z art. 2 Konstytucji podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Z tych samych powodów i w tym samym zakresie (brak wymaganego uzasadnienia zarzutu), z uwagi na identyczną treść pozostałych przepisów, zaskarżonych w tej samej grupie co art. 20ca ustawy o Policji, umorzeniu wobec niedopuszczalności wydania orzeczenia przez Trybunał Konstytucyjny podlega postępowanie w sprawie zgodności z art. 2 Konstytucji z art. 10ba ustawy o Straży

Granicznej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o ABW oraz AW, art. 32a ustawy o SKW oraz SWW i art. 18a ustawy o CBA.

Kolejnym zarzutem, który, zgodnie z intencją Wnioskodawcy, należy rozpatrywać, odnosząc go wyłącznie do art. 20c ust. 1 ustawy o Policji (bez związku normatywnego z art. 20ca tej ustawy), jest odwoływanie się w tym przepisie do nieprecyzyjnego i niejasnego, zdaniem Rzecznika, pojęcia „dane internetowe”.

Rzecznik podnosi, że pojęcie to definiowane jest poprzez odwołanie do art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, który wprowadzie wymienia kategorie danych, ale określa je zbyt ogólnie, co, w Jego ocenie, „może powodować niejasności i prowadzić do zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe” (uzasadnienie wniosku, s. 43).

W konkluzji Rzecznik stwierdza, że „[n]iejasności związane z zakresem danych internetowych, które mogą być gromadzone przez służby, powoduje, że nie można uznać, by spełniony był wymóg precyzyjności prawa” (uzasadnienie wniosku, s. 43-44).

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, określając wymagania formalne, jakie muszą spełniać regulacje dopuszczające wykonywanie czynności operacyjno-rozpoznawczych, stwierdził, między innymi, że „[o]graniczenia w korzystaniu z konstytucyjnych wolności i praw muszą być precyzyjne unormowane w ustawie. Chodzi jednak nie tylko o formalne umiejscowienie przepisu ograniczającego w akcie normatywnym o randze co najmniej ustawy, ale również o <jakość> tego unormowania, które **musi zapewniać przewidywalność rozstrzygnięć organów władzy publicznej wobec jednostek** (podkr. wł.). Ustawowa forma ograniczeń prawa do ochrony prywatności (art. 47), wolności i ochrony tajemnicy

komunikowania się (art. 49) oraz autonomii informacyjnej (art. 51 ust. 1 Konstytucji) wynika bezpośrednio z art. 31 ust. 3 Konstytucji, a zapewnienie dostatecznej określoności przepisów także z zasady demokratycznego państwa prawa (art. 2 Konstytucji). Wymóg ustawowego unormowania kwestii gromadzenia i udostępniania informacji został ustanowiony w art. 51 ust. 5 Konstytucji.

Trybunał Konstytucyjny zrekapitulował swoje dotychczasowe orzeczenia dotyczące zasady dostatecznej określoności prawa w wyroku o sygn. Kp 3/09. Stwierdził, że *<norma konstytucyjna nakazująca zachowanie odpowiedniej określoności regulacji prawnych ma charakter zasady prawa. Nakłada to na ustawodawcę obowiązek jej optymalizacji w procesie stanowienia prawa. Ustawodawca powinien dążyć do możliwie maksymalnej realizacji wymogów składających się na tę zasadę. Tym samym stopień określoności konkretnych regulacji podlega każdorazowej relatywizacji w odniesieniu do okoliczności faktycznych i prawnych, jakie towarzyszą podejmowanej regulacji (podkr. wł.). Relatywizacja ta stanowi naturalną konsekwencję nieostrości języka, w którym redagowane są teksty prawne oraz różnorodności materii podlegającej normowaniu>* (wyrok TK z 28 października 2009 r., sygn. Kp 3/09, OTK ZU nr 9/A/2009, poz. 138, cz. III, pkt 6.2). Na ustawodawcy ciąży zatem obowiązek tworzenia przepisów prawa możliwie najbardziej określonych w danym wypadku pod względem zarówno ich treści, jak i formy. W związku z powyższym każde unormowanie regulujące status jednostki w państwie powinno cechować się *<poprawnością>*, *<precyzyjnością>* i *<jasnością>*. Każdy przepis prawny winien być skonstruowany poprawnie z punktu widzenia językowego i logicznego. Dopiero po spełnieniu tego podstawowego warunku można ocenić przepis w aspekcie pozostałych kryteriów wynikających z zasady określoności prawa (...). Przepisy ustawowe ograniczające konstytucyjne wolności lub prawa muszą być zatem sformułowane w sposób pozwalający jednoznacznie ustalić, kto i w jakiej sytuacji podlega ograniczeniom przez organy państwa; muszą być na tyle

precyzyjne, by je stosowano i interpretowano w jednolity sposób; wreszcie muszą być tak ujęte, by zakres ich zastosowania obejmował wyłącznie sytuacje, w których racjonalny ustawodawca zamierzał wprowadzić regulację ograniczającą korzystanie z konstytucyjnych wolności i praw (...).

Jak wskazał Trybunał w (...) wyroku w sprawie o sygn. Kp 3/09, <ocena konstytucyjności aktu normatywnego zawsze musi mieć charakter złożony. W wypadku określoności, złożoność tego procesu dostrzegana jest na dwóch płaszczyznach. Po pierwsze, w odniesieniu do analizy samej określoności uwzględnić należy najpierw wspomniane wyżej aspekty testu określoności (precyzyjność, jasność, poprawność), a następnie we właściwej proporcji odnieść je do charakteru badanej regulacji. Drugą płaszczyznę stanowi kontekst aksjologiczny, w jakim przeprowadzana jest kontrola konstytucyjności norm. Na kontekst ten składa się wykładnia całości reguł, zasad i wartości konstytucyjnych, z którymi skonfrontowana musi zostać badana norma, wyinterpretowana z przepisu poddanego wcześniej kontroli z formalnego punktu widzenia (określoności właśnie)> (wyrok TK z 28 października 2009 r., sygn. Kp 3/09, cz. III, pkt 6.3.1)” [OTK ZU seria A nr 7/2014, poz. 80].

W kolejnym fragmencie tej części uzasadnienia wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny wyjaśnił, że „zakres akceptacji stopnia niejasności przepisów nie jest jednakowy dla całości ustawodawstwa. Im bardziej przepisy oddziałują na wolności i prawa konstytucyjne, zwłaszcza o charakterze osobistym, tym większy rygoryzm towarzyszyć musi ocenie precyzyjności unormowania. Trybunał podkreśla ponadto, że ponieważ wolności osobiste - w świetle systematyki Konstytucji - są wyjątkowo silnie eksponowane, to ustawowe ograniczenia w korzystaniu z nich powinny być możliwe do ustalenia już na podstawie wykładni językowej przepisów ustawy, bez potrzeby odwoływania się do wykładni systemowej czy funkcjonalnej. Zdaniem Trybunału, w wypadku wolności osobistych nie jest dopuszczalne skorygowanie niekonstytucyjnej normy prawnej wyprowadzonej za pomocą wykładni językowej przez odwołanie się do

pozostałych, pozajęzykowych metod wykładni, aby wreszcie odnaleźć - czasami gdzieś na bezdrożach systemu prawnego - rozumienie przepisu ograniczającego konstytucyjne wolności osobiste, które będzie zgodne z Konstytucją”, po czym, przekładając dotychczasowe ustalenia na ustawowe unormowanie ingerencji w wolności i prawa konstytucyjne w związku ze stosowaniem przez służby powołane do ochrony bezpieczeństwa państwa i porządku publicznego czynności operacyjno-rozpoznawczych, stwierdził, że, Jego zdaniem, „jednostka na podstawie przepisu ustawy powinna wiedzieć, kto oraz w jakim zakresie podmiotowym, przedmiotowym i czasowym jest uprawniony do niejawniej ingerencji w szeroko rozumianą sferę prywatności. Kryterium przewidywalności nie oznacza jednakże - na co też kładzie się nacisk w orzecznictwie ETPC - że jednostka będzie mogła dokładnie przewidzieć moment, w którym organy władzy publicznej zarejestrują jej zachowania lub pozyskają o niej inne informacje, a co za tym idzie będzie mogła dostosować do tej sytuacji własne zachowanie (np. unikając prowadzenia rozmów telefonicznych i kontaktowania się z innymi). Prawo musi być natomiast wystarczająco precyzyjne, aby dać odpowiednie wskazania co do okoliczności i warunków, w których organy państwa mogą zastosować któryś z takich środków. Trybunał Konstytucyjny stwierdza, że ustalone w orzecznictwie ETPC standardy w powyższym zakresie zachowują pełną aktualność oraz mają swe odzwierciedlenie w treści zasady demokratycznego państwa prawnego wynikającej z art. 2 Konstytucji, jak i w tej części art. 31 ust. 3 Konstytucji, który dla ograniczeń wolności i praw wymaga ustawowej formy regulacji.

Podstawowym celem precyzyjnego określenia w prawie przesłanek dopuszczalności czynności operacyjno-rozpoznawczych jest wyznaczenie organom władzy wykonawczej możliwie jak najściślejszych ram działania. Zapobiegać ma to arbitralności stosowania prawa, a zwłaszcza przenoszeniu na organy stosujące prawo ciężaru faktycznego wyznaczenia granic wolności człowieka. Trybunał Konstytucyjny zwraca ponadto uwagę, że im większa jest

skala stosowania czynności operacyjno-rozpoznawczych, a więc wzrasta - choćby potencjalnie - częstotliwość ingerencji w konstytucyjne wolności i prawa, tym bardziej unormowanie ustawowe musi cechować się zupełnością i maksymalną precyzją” (ibidem).

Biorąc pod uwagę cytowaną wyżej wypowiedź Trybunału Konstytucyjnego oraz wynik wykładni językowej art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, a także przedstawiony we wcześniejszym fragmencie niniejszego stanowiska (s. 85-88) komentarz J. Gołaczyńskiego do tego przepisu, należy dojść do wniosku, że art. 20c ust. 1 ustawy o Policji w zakresie, w jakim zawarte w jego treści pojęcie „dane internetowe” definiowane jest poprzez odwołanie do art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, **nie narusza nakazu jasności i precyzji** normy upoważniającej Policję do wykonywania czynności operacyjno-rozpoznawczych.

Przede wszystkim, już na podstawie treści komentowanego przepisu jednostka jest w stanie zorientować się, które, wchodzące w zakres „danych internetowych”, dane osobowe jej dotyczące oraz jakie, wchodzące także w zakres „danych internetowych”, tzw. dane eksploatacyjne (skoro za pomocą tych danych także można ustalić osobę korzystającą z usługi Internetu) mogą być uzyskiwane i przetwarzane przez Policję przy wykonywaniu czynności operacyjno-rozpoznawczych, polegających na uzyskiwaniu i przetwarzaniu danych internetowych.

Istotnie, przepis art. 20c ust. 1 ustawy o Policji zawiera odwołanie do art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną i definiuje dane zawarte w tym przepisie jako „dane internetowe”.

Nietrafny jest jednak pogląd Rzecznika, iż wspomniany art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną wymienione w nim kategorie danych określa nazbyt ogólnie (co prowadzić miałyoby do „zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe”).

Przedstawione w art. 18 ust. 1 ustawy o świadczeniu usług drogą elektroniczną wyliczenie danych zawiera **podstawowe dane osobowe usługobiorcy**, które mogą być przetwarzane przez usługodawcę.

Rzeczywiście wyliczenie to **nie stanowi katalogu zamkniętego**, ponieważ **usługodawca może przetwarzać** także inne dane usługobiorcy, jeżeli jest to niezbędne ze względu na właściwość danej usługi lub sposób jej rozliczenia (art. 18 ust. 2 tej ustawy).

Niemniej jednak trzeba mieć świadomość, że stworzony przez ustawodawcę katalog informacji o osobie, których przetwarzanie przez usługodawcę może być niezbędne w celach związanych z zawartą umową na usługę w Internecie, **ma charakter otwarty tylko dlatego**, że, w przypadku wykonywania usług internetowych, ustawowe określenie zakresu niezbędnych danych **w praktyce nie jest możliwe**. Warto w tym miejscu przypomnieć (zwracał na to uwagę J. Gołaczyński), że świadczenie usług drogą elektroniczną obejmuje także umowy zawierane i wykonywane on-line.

W tej sytuacji wydaje się, że wystarczającą gwarancją „przewidywalności” przedmiotowego zakresu ingerencji Policji w szeroko rozumianą sferę prywatności jednostki (usługobiorcy) związanej z uzyskiwaniem w sposób niejawnny danych internetowych i jednocześnie gwarancją odpowiedniego respektu ustawodawcy dla znaczenia tej sfery prawa jest okoliczność, że poszerzenie katalogu danych podlegających przetworzeniu przez usługodawcę **musi mieć zawsze uzasadnienie w treści świadczonej usługi**.

W oparciu o art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną można więc wskazać dwa podstawowe warunki, jakie muszą spełniać dane osobowe, aby dopuszczalne było ich przetwarzanie przez usługodawcę internetowego.

Po pierwsze, dane te mogą być przetwarzane jedynie w związku z realizacją celu wymienionego w art. 18 ust. 1 wspomnianej ustawy, czyli **dla nawiązania stosunku prawnego** (danych niezbędnych do świadczenia usługi).

Po drugie, dla przetwarzania tych danych konieczne jest spełnienie przesłanki **niezbędności z uwagi na:**

- **rodzaj świadczonej usługi** (np. dane dotyczące wieku danej osoby) albo
- **sposób rozliczenia z usługobiorcą** (np. numer NIP potrzebny do wystawienia faktury).

Ponadto obowiązek uzyskania określonych danych **może wynikać z innych ustaw** (np. numer NIP, którego obowiązek zamieszczenia na fakturze wystawionej przez świadczącego usługę wynika z ustawy z dnia 29 września 1994 r. o rachunkowości, tekst jednolity - Dz. U. z 2016 r., poz. 1047 ze zm.).

Wreszcie usługodawca może przetwarzać dane sprzętu i oprogramowania, z którego korzysta usługobiorca.

Należy przy tym podkreślić, że wszystkie wymienione wyżej dane, czyli dane niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego przez usługodawcę i usługobiorcę (art. 18 ust. 1-3 ustawy o świadczeniu usług drogą elektroniczną), **są udostępniane przez usługobiorcę świadomie.**

Również świadomie, bo wszak wyłącznie za własną zgodą, usługobiorca udostępnia też usługodawcy dane, określone w art. 18 ust. 4 ustawy o świadczeniu usług drogą elektroniczną (chodzi tu o dane, które nie są niezbędne do świadczenia usługi drogą elektroniczną).

Jedynie dane określone w art. 18 ust. 5 ustawy o świadczeniu usług drogą elektroniczną, które są pozyskiwane automatycznie przez działanie systemu teleinformatycznego (dane eksploatacyjne), mogą być przetwarzane przez usługodawcę bez wiedzy usługobiorcy. Jednak zakres tych danych jest ściśle określony przez ustawodawcę, co oznacza, że nie istnieją przeszkody uniemożliwiające usługobiorcy zorientowanie się co do przedmiotowego zakresu

tych danych, a - w konsekwencji - także co do głębokości takiej ingerencji Policji w jego konstytucyjne prawa i wolności, która polega na uzyskiwaniu i przetwarzaniu przez Policję danych internetowych, w trybie art. 20c ust. 1 ustawy o Policji.

Biorąc powyższe pod uwagę, należy stwierdzić, że art. 20c ust. 1 ustawy o Policji w zakresie, w jakim jego treść zawiera odwołanie do pojęcia „dane internetowe”, jest **zgodny** z art. 2 Konstytucji.

Z tych samych powodów i w tym samym zakresie (w zakresie, w jakim treść przepisu zawiera odwołanie do pojęcia „dane internetowe”), z uwagi na identyczne brzmienie pozostałych, zaskarżonych w tej grupie, przepisów oraz odpowiadających im zarzutów Wnioskodawcy, za zgodne z art. 2 Konstytucji należy uznać art. 10b ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 ustawy o CBA.

2. Ocena zarzutu niezgodności art. 20cb ust. 1 ustawy o Policji z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 20cb ustawy o Policji ma następującą treść:

„Art. 20cb. 1. W celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,

3) w przypadku użytkownika, który nie jest osobą fizyczną, numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 20c ust. 2-7 stosuje się.”.

Poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, art. 20cb ust. 1 ustawy o Policji umożliwia tej formacji uzyskiwanie danych z elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci, prowadzonego (obligatoryjnie) przez przedsiębiorcę telekomunikacyjnego świadczącego publicznie dostępne usługi telekomunikacyjne, to jest z wykazu zawierającego **dane przekazane przez abonenta przy zawarciu umowy** na te usługi (ust. 1 pkt 1).

Natomiast poprzez odwołane do art. 161 ustawy - Prawo telekomunikacyjne komentowany przepis umożliwia Policji uzyskiwanie, w celach w nim określonych, **tzw. danych abonamentowych**, to znaczy danych dotyczących użytkownika będącego osobą fizyczną w postaci: nazwisk i imion, imion rodziców, miejsca i daty urodzenia, adresu miejsca zamieszkania i adresu korespondencyjnego, jeżeli jest on inny niż adres miejsca zamieszkania, numeru ewidencyjnego PESEL - w przypadku obywatela Rzeczypospolitej Polskiej, nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego UE albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu oraz danych zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług

telekomunikacyjnych, **jak również** danych przekazanych przez użytkownika będącego osobą fizyczną, za jego zgodą, dostawcy publicznie dostępnych usług telekomunikacyjnych, **o ile dane te pozostają w związku ze świadczoną usługą** (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, Policja, w celach określonych w art. 20cb ust. 1 ustawy o Policji, ma dostęp do numeru zakończenia sieci oraz nazwy siedziby lub miejsca wykonywania działalności gospodarczej, nazwy firmy lub nazwy i formy organizacyjnej tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także do nazwy miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Zarzuty Wnioskodawcy pod adresem komentowanego przepisu są podobne do zarzutów sformułowanych wobec art. 20c ust. 1 ustawy o Policji (*vide* - pkt III *petitum* wniosku wraz z odpowiednim fragmentem jego uzasadnienia).

Wnioskodawca wskazał też identyczne wzorce kontroli.

Na wstępie należy zauważyć, iż Wnioskodawca **zarzut nadmiernie szerokiego, w Jego ocenie, katalogu przestępstw**, w odniesieniu do których dopuszczalne jest uzyskiwanie i przetwarzanie przez Policję określonych w tym przepisie danych, między innymi z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne (pkt 1) oraz o których mowa w art. 161 tej ustawy (pkt 2), połączył z zarzutem **braku**, w tym przypadku już nie tylko (jak w odniesieniu do art. 20c ust. 1 ustawy o Policji) wystarczającej (odpowiedniej czy realnej), ale **jakiegokolwiek niezależnej kontroli pozyskiwania tych danych przez Policję** (*vide* - uzasadnienie wniosku, s. 39, 42).

Wnioskodawca stwierdza bowiem, że „**zgodnie z art. 20ca ust. 5 ustawy o Policji (i odpowiednio w przypadku pozostałych służb) żadnej kontroli nie podlega uzyskiwanie danych, pozyskiwanych na podstawie art. 20cb ust. 1 ustawy o Policji** (podkr. wł.). Należy w tym miejscu wskazać, że ustawa o Policji i analogicznie pozostałe ustawy spod jakiegokolwiek kontroli wyłączają

pozyskiwanie danych nie tylko określonych w art. 179 ust. 9 Prawa telekomunikacyjnego, ale również całego art. 161 Prawa telekomunikacyjnego, co znacząco poszerza zakres dostępu do danych wyłączonych spod jakiejkolwiek kontroli. W szczególności art. 161 ust. 3 Prawa telekomunikacyjnego zawiera odniesienie do bliżej nieokreślonych <innych danych>”(uzasadnienie wniosku, s. 51).

Na wstępie trzeba dostrzec, iż, podobnie jak w przypadku art. 20c ust. 1 ustawy o Policji, także w odniesieniu do art. 20cb ust. 1 tej ustawy, uzyskiwanie na podstawie tego przepisu przez Policję danych w innych celach niż zapobieganie lub wykrywanie przestępstw **nie jest objęte zarzutem Wnioskodawcy.**

Z powyższych względów postępowanie w sprawie kontroli zgodności art. 20cb ust. 1 ustawy o Policji w zakresie, w jakim upoważnia Policję do uzyskiwania, określonych w tym przepisie, danych w celu z ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia. Rzecznik Praw Obywatelskich nie uzasadnił bowiem tego zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonemu w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Przechodząc do rozważań merytorycznych należy zwrócić uwagę, iż art. 20cb ust. 1 ustawy o Policji, podobnie jak art. 20c ust. 1 tej ustawy, umożliwia Policji uzyskiwanie określonych w nim danych w celu zapobiegania lub

wykrywania wszystkich przestępstw oraz że przepis ten, podobnie jak art. 20c ust. 1 ustawy o Policji, nie uzależnia uzyskiwania określonych w nim danych od bezskuteczności albo nieprzydatności innych możliwych do zastosowania środków.

Tym, co odróżnia art. 20cb ust. 1 ustawy o Policji od art. 20c ust. 1 tej ustawy, jest, o czym wcześniej była już mowa, brak w art. 20cb ust. 1 wprowadzenia jakiegokolwiek niezależnej kontroli pozyskiwania przez Policję określonych w nim danych (uzyskiwanie danych, o których mowa w art. 20c ust. 1 ustawy o Policji zostało objęte niezależną kontrolą, i to kontrolą sprawowaną przez sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane, *vide* - art. 20ca tej ustawy).

Ani bowiem art. 20cb ust. 1 ustawy o Policji, ani żaden inny przepis tej ustawy nie nakłada obowiązku uzyskania zgody sądu (bądź innego organu, który byłby niezależny od organów żądających udostępnienia tych danych lub organów nad nimi nadrzędnych) na udostępnienie Policji danych, o których mowa w tym przepisie. Procedura ta nie wymaga nawet uzyskania zgody prokuratora. Ustawodawca nie przewidział też choćby zrębowych elementów kontroli *ex post* legalizującej podjęte działania. Pozyskiwanie przez funkcjonariuszy Policji danych telekomunikacyjnych (art. 161 i art. 179 ust. 9 ustawy - Prawo telekomunikacyjne) i innych wymienionych w tym przepisie danych pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane.

Ponadto, ustawodawca **wprost wykluczył kontrolę sądową** uzyskiwania przez Policję danych, określonych w art. 20cb ust. 1 ustawy o Policji - taką kontrolę, jaką przewidział dla uzyskiwania przez Policję danych na podstawie art. 20c ust. 1 ustawy o Policji (*vide* - art. 20ca ust. 5 ustawy o Policji).

Na wstępie należy odnotować, iż przepisy ustawy o Policji zawierają pewne ograniczenia dostępu do danych określonych w art. 20cb ustawy o Policji. Nie każdy bowiem funkcjonariusz Policji może - w ramach wykonywanych przez

siebie czynności - mieć udostępnione te dane. Zgodnie art. 20c ust. 2 ustawy o Policji w związku z art. 20cb ust. 2 tej ustawy, dane, o których mowa w art. 20cb ust. 1 ustawy o Policji, mogą być udostępniane tylko tym funkcjonariuszom, którzy otrzymali stosowne upoważnienie Komendanta Głównego Policji lub komendanta wojewódzkiego Policji.

O ile jednak w art. 20c ust. 1 pkt 1 ustawy o Policji mamy do czynienia z danymi telekomunikacyjnymi określonymi w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, o tyle przepis art. 20cb ust. 1 ustawy o Policji odnosi się do danych z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne (ust. 1 pkt 1) oraz do danych, o których mowa w art. 161 tejże ustawy (ust. 1 pkt 2).

Trzeba w tym miejscu przypomnieć, że art. 180c ustawy - Prawo telekomunikacyjne wymienia dane „niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:

- a) inicjującego połączenie,
- b) do którego kierowane jest połączenie;

2) określenia:

- a) daty i godziny połączenia oraz czasu jego trwania,
- b) rodzaju połączenia,
- c) lokalizacji telekomunikacyjnego urządzenia końcowego.”, zaś art. 180d ustawy - Prawo telekomunikacyjne wymienia dane, o których mowa w art. 159 ust. 1 pkt 1 i 3-5, art. 161 oraz w art. 179 ust. 8 tejże ustawy.

Powyższe oznacza, że zakres danych telekomunikacyjnych z art. 20c ust. 1 pkt 1 ustawy o Policji jest znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 20cb ust. 1 ustawy o Policji, a, w konsekwencji, że dane z art. 20c ust. 1 pkt 1 ustawy o Policji **zawierają nieporównanie więcej informacji o osobie** niż dane, o których mowa w art. 20cb ust. 1 ustawy o Policji.

O ile w oparciu o art. 20c ust. 1 pkt 1 ustawy o Policji możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 20cb ust. 1 ustawy o Policji możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

Dane z art. 161 ustawy - Prawo telekomunikacyjne to wszak dane o usłudze świadczonej użytkownikowi oraz dane niezbędne do wykonywania tej usługi, a zatem takie dane jak, przykładowo: imię i nazwisko abonenta, miejsce i data jego urodzenia czy nazwa, seria i numer dokumentów potwierdzających tożsamość abonenta (w przypadku obywatela RP - numer ewidencyjny PESEL), jak również inne dane abonenta (osoby fizycznej) pod warunkiem, że abonent na przetwarzanie przez przedsiębiorcę telekomunikacyjnego owych innych danych wyrazi zgodę (dane dotyczące abonamentu).

Z kolei wykaz, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, obejmuje dane o abonencie uzyskane przez przedsiębiorcę telekomunikacyjnego od samego zainteresowanego przy zawieraniu z nim umowy na konkretną usługę (dane o abonencie).

O ile w przypadku pozyskiwania danych na podstawie art. 20c ust. 1 pkt 1 ustawy o Policji zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej wykazano, odnośnie do tej procedury zostały przewidziane w art. 20ca ustawy o Policji), o tyle w przypadku pozyskiwania danych na podstawie art. 20cb ust. 1 ustawy o Policji **konieczność taka nie zachodzi.**

Należy bowiem zauważyć, iż niektóre dane, określone w art. 20cb ust. 1 ustawy o Policji, przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Natomiast pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego za zgodą abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji można zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 20cb ust. 1 ustawy o Policji ingerencja w prawa i wolności jednostki zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Wprowadzone w art. 20cb ust. 1 ustawy o Policji ograniczenie konstytucyjnych praw i wolności jednostki jest przy tym usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując tę część rozważań, należy stwierdzić, że art. 20cb ust. 1 ustawy o Policji, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Natomiast umorzeniu - wobec niedopuszczalności wydania orzeczenia - na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego

podlega postępowanie w sprawie kontroli zgodności art. 20cb ust. 1 ustawy o Policji z art. 2 Konstytucji.

W tej bowiem sprawie Rzecznik Praw Obywatelskich nie zadośćuczynił, określone w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, wymogowi uzasadnienia zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie.

Wszak art. 20cb ust. 1 ustawy o Policji oraz posiadające analogiczną treść przepisy pozostałych ustaw regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego nie zawierają odwołania do pojęcia „dane internetowe”, a tylko do tego rodzaju danych Rzecznik odnosił się, formułując zarzut niezgodności powołanych przepisów z art. 2 Konstytucji.

Tak więc - z tych samych powodów (z uwagi na wskazaną identyczność treści normatywnej wszystkich zaskarżonych w tej grupie przepisów) - umorzeniu wobec niedopuszczalności wydania orzeczenia przez Trybunał Konstytucyjny podlega również postępowanie w zakresie badania zgodności z art. 2 Konstytucji art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28b ust. 1 ustawy o ABW oraz AW, art. 32b ust. 1 ustawy o SKW oraz SWW i art. 18b ust. 1 ustawy o CBA.

3. Ocena zarzutu niezgodności art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 10b ust. 1 ustawy o Straży Granicznej ma następującą treść:

„Art. 10b. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,

2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2016 r. poz. 1113 i 1250), zwane dalej <danymi pocztowymi>,

3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030), zwane dalej <danymi internetowymi>

- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Z kolei art. 10ba ustawy o Straży Granicznej brzmi:

„Art. 10ba. 1. Kontrolę nad uzyskiwaniem przez Straż Graniczną danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby składającego wniosek organu Straży Granicznej.

2. Organ Straży Granicznej, który wystąpił z wnioskiem, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Straży Granicznej danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd okręgowy informuje organ Straży Granicznej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 10bb ust. 1 (przepis ten upoważnia Straż Graniczną do uzyskiwania w celu zapobiegania lub wykrywania przestępstw danych z wykazu, o którym mowa w

art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

Przepis art. 10b ustawy o Straży Granicznej upoważnia zatem funkcjonariuszy Straży Granicznej do gromadzenia oraz przetwarzania - bez wiedzy i zgody osoby, której dotyczą - danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych pocztowych, o których mowa w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe, oraz danych internetowych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną (ust. 1) [podobne upoważnienie, tyle że odnoszące się do funkcjonariuszy Policji, zawiera przepis art. 20c ust. 1 ustawy o Policji]. Ponadto przepis ten (podobnie jak art. 20c ust. 2-7 ustawy o Policji w odniesieniu do funkcjonariuszy Policji) określa przedmiotowe przesłanki oraz warunki udostępniania tych danych na żądanie funkcjonariuszy Straży Granicznej (ust. 2-7).

Z kolei przepis art. 10ba ustawy o Straży Granicznej wprowadza procedurę kontroli następcej sądu nad uzyskiwaniem danych, o których mowa w art. 10b ust. 1 ustawy o Straży Granicznej (w tym wypadku kontrolę przeprowadza sąd okręgowy właściwy dla siedziby składającego wniosek o udostępnienie danych organu Straży Granicznej), identyczną jak procedura kontroli uzyskiwania takich samych danych przez funkcjonariuszy Policji (*vide* - art. 20c ust. 1 w związku z art. 20ca ustawy o Policji).

Wnioskodawca sformułował wobec art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej takie same zarzuty i argumenty za niezgodnością tej regulacji z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także z art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE jak w odniesieniu do art. 20c ust. 1 w związku z art. 20ca ustawy o Policji.

Należy tylko zauważyć, iż art. 10b ust. 1 ustawy o Straży Granicznej od art. 20c ust. 1 ustawy o Policji różni ograniczenie możliwości uzyskiwania danych

telekomunikacyjnych, danych pocztowych oraz danych internetowych przez funkcjonariuszy Straży Granicznej **tylko do jednego celu - do zapobiegania lub wykrywania przestępstw**, przy czym katalog tych przestępstw jest mniej obszerny niż w przypadku Policji, obejmuje bowiem tylko te przestępstwa, których zapobieganie i wykrywanie należy do ustawowych zadań Straży Granicznej. Trzeba bowiem pamiętać, że identyfikacja katalogu przestępstw, o których mowa w art. 10b ust. 1 ustawy o Straży Granicznej, musi się odbywać poprzez art. 1 ust. 2 ustawy o Straży Granicznej, regulujący zadania tej formacji, w szczególności z uwzględnieniem treści pkt. 4 tego przepisu, który definiuje rodzaje przestępstw, jakich rozpoznawanie oraz wykrywanie (zapobieganie), a także ściganie ich sprawców należy do właściwości Straży Granicznej, a brzmi on następująco:

„2. Do zadań Straży Granicznej należy:

(...)

4) rozpoznawanie, zapobieganie i wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, w zakresie właściwości Straży Granicznej, a w szczególności:

a) przestępstw i wykroczeń dotyczących zgodności przekraczania granicy państwowej z przepisami, związanych z jej oznakowaniem, wykonywaniem pracy przez cudzoziemców, prowadzeniem działalności gospodarczej przez cudzoziemców oraz powierzaniem wykonywania pracy cudzoziemcom, a także przestępstw określonych w art. 270-276 Kodeksu karnego dotyczących wiarygodności dokumentów uprawniających do przekraczania granicy państwowej, dokumentów uprawniających do pobytu na terytorium Rzeczypospolitej Polskiej lub dokumentów wymaganych do ich wydania,

b) przestępstw skarbowych i wykroczeń skarbowych wymienionych w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego,

c) przestępstw i wykroczeń pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów

oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni i amunicji, o materiałach wybuchowych, o prekursorach materiałów wybuchowych podlegających ograniczeniom, o bibliotekach, o ochronie zabytków i opiece nad zabytkami, o narodowym zasobie archiwalnym, o przeciwdziałaniu narkomanii oraz o ewidencji ludności i dowodach osobistych,

d) przestępstw i wykroczeń określonych w ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach oraz w ustawie z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 680, z 2013 r. poz. 1650, z 2014 r. poz. 1004, z 2015 r. poz. 1607 oraz z 2016 r. poz. 783),

e) przestępstw przeciwko bezpieczeństwu powszechnemu oraz przestępstw i wykroczeń przeciwko bezpieczeństwu w komunikacji, pozostających w związku z wykonywaniem komunikacji lotniczej,

f) przestępstw określonych w art. 228, 229 i 231 Kodeksu karnego, popełnionych przez pracowników Straży Granicznej w związku z wykonywaniem czynności służbowych,

g) przestępstw 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,

h) przestępstw określonych w art. 190, 222, 223 i 226 Kodeksu karnego skierowanych przeciwko funkcjonariuszom Straży Granicznej podczas lub w związku z pełnieniem obowiązków służbowych,

i) przestępstw określonych w art. 264a Kodeksu karnego, przestępstw i wykroczeń określonych w ustawie z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769) oraz wykroczeń określonych w ustawie z dnia 20 kwietnia 2004 r. o promocji

zatrudnienia i instytucjach rynku pracy (Dz. U. z 2016 r. poz. 645, 691, 868 i 1265),

j) przestępstw określonych w art. 189a Kodeksu karnego i w art. 8 ustawy z dnia 6 czerwca 1997 r. - Przepisy wprowadzające Kodeks karny (Dz. U. poz. 554 i 1083, z 1998 r. poz. 715, z 2009 r. poz. 1149 i 1589 oraz z 2010 r. poz. 626);”.

Wprawdzie w powołanym uprzednio wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 10b ust.1 ustawy o Straży Granicznej, którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych i danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału w zakresie pozyskiwania przez Straż Graniczną danych telekomunikacyjnych można również odnieść do pozyskiwania przez tę formację pozostałych danych wymienionych w tym przepisie.

Biorąc pod uwagę tezy zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 10ba ustawy o Straży Granicznej **mechanizm kontroli** nad uzyskiwaniem przez Straż Graniczną danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez sąd okręgowy właściwy dla siedziby składającego wniosek organu Straży Granicznej, z powodów **o których była mowa w pkt III ppkt 1 niniejszego stanowiska, stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.**

Podobnie bowiem jak w przypadku Policji, wprawdzie kontrola dotyczy jedynie zbiorczych danych ujętych przez organ Straży Granicznej w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to nie można jednak nie dostrzec, iż, zgodnie z art. 10ba ust. 3 ustawy o Policji, „sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie**

Straży Granicznej danych telekomunikacyjnych, pocztowych lub internetowych”.

Formuła ta oznacza to samo, co identyczna w swej treści norma zawarta w art. 20ca ust. 3 ustawy o Policji, a mianowicie, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi posiadanymi przez organ Straży Granicznej materiałami uzasadniającymi wnioski o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 10b ust. 1 ustawy o Straży Granicznej. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 10ba ust. 2 ustawy o Straży Granicznej, to można zasadnie stwierdzić, że kontroli sądu okręgowego podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 10b ust. 6 i 7 ustawy o Straży Granicznej).

Podobnie też jak w przypadku Policji, ocena przez kontrolujący sąd prawidłowości wniosku organu Straży Granicznej o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Komendanta Głównego Straży Granicznej i komendantów oddziałów Straży Granicznej (*vide* - art. 10b ust. 5 ustawy o Straży Granicznej).

Ponadto do Straży Granicznej mają odpowiednie zastosowanie uwagi zawarte w pkt III ppkt 1 niniejszego stanowiska odnoszące się do sposobu rozumienia sformułowania „niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu”, użytego w art. 10b ust. 7 ustawy o Straży Granicznej.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 10ba ustawy o Straży Granicznej mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Straży Granicznej w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość.** Wszak sądowi okręgowemu umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu.**

Powyższe przesądza, że art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, co jednocześnie oznacza **zgodność** tej regulacji także z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a także z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej.

4. Ocena zarzutu niezgodności art. 10bb ust. 1 ustawy o Straży Granicznej z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 10bb ustawy o Straży Granicznej ma następującą treść:

„Art. 10bb. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,

- 3) w przypadku użytkownika, który nie jest osobą fizyczną, numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 10b ust. 2-7 stosuje się.”.

Analizowany przepis, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, umożliwia Straży Granicznej uzyskiwanie danych przekazywanych przez użytkownika przy zawieraniu umowy na usługi telekomunikacyjne (ust. 1 pkt 1).

Z kolei, poprzez odwołanie do art. 161 ustawy - Prawo telekomunikacyjne, art. 10bb ust. 1 ustawy o Straży Granicznej umożliwia tej formacji uzyskiwanie, w celach w nim określonych, tzw. danych abonamentowych oraz danych przekazanych operatorowi przez użytkownika będącego osobą fizyczną za jego zgodą, o ile dane te pozostają w związku ze świadczoną usługą (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, Straż Graniczna, w celach określonych w art. 10bb ust. 1 ustawy o Straży Granicznej, może uzyskiwać numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Zarzuty Wnioskodawcy pod adresem komentowanego przepisu są tożsame z zarzutami sformułowanymi pod adresem art. 20cb ust. 1 ustawy o Policji.

Wnioskodawca wskazał też identyczne wzorce kontroli.

W tej sytuacji oceny i wnioski przedstawione w pkt III ppkt 2 niniejszego stanowiska pozostają aktualne także w odniesieniu do art. 10bb ust. 1 ustawy o Straży Granicznej, co jednocześnie oznacza, że konstytucyjność tego przepisu, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, **determinuje zakres** uzyskiwanych przez Straż Graniczną, a określonych w tym przepisie danych, jak również **zasady przekazywania tych danych operatorowi telekomunikacyjnemu przez użytkownika.**

Podobnie bowiem jak w - odpowiadających w tym przypadku treściowo i wzajemnie porównywanych - przepisach art. 20c ust. 1 pkt 1 i art. 20cb ust. 1 ustawy o Policji, określony w art. 10b ust. 1 pkt 1 ustawy o Straży Granicznej zakres danych telekomunikacyjnych jest znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 10bb ust. 1 ustawy o Straży Granicznej, co, w konsekwencji, prowadzi do wniosku, że dane z art. 10b ust. 1 pkt 1 ustawy o Straży Granicznej **zawierają nieporównanie więcej informacji o osobie** niż dane, o których mowa w art. 10bb ust. 1 ustawy o Straży Granicznej.

O ile w oparciu o art. 10b ust. 1 pkt 1 ustawy o Straży Granicznej możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 10bb ust. 1 ustawy o Straży Granicznej możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

W przedstawionych warunkach, o ile w przypadku pozyskiwania danych na podstawie art. 10b ust. 1 pkt 1 ustawy o Straży Granicznej zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej wykazano, zostały przewidziane w art. 10ba ustawy o Straży Granicznej), o tyle w przypadku pozyskiwania danych na podstawie art. 10bb ust. 1 ustawy o Straży Granicznej **konieczność taka nie zachodzi.**

Należy bowiem zauważyć, iż, tak jak dane z art. 20cb ust. 1 ustawy o Policji, niektóre dane, określone w art. 10bb ust. 1 ustawy o Straży Granicznej, przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Z kolei pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego także **za zgodą** abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji, podobnie jak w przypadku danych z 20cb ust. 1 ustawy o Policji, można zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 10bb ust. 1 ustawy o Straży Granicznej ingerencja w prawa i wolności jednostki, zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Przy tym, podobnie jak ograniczenia konstytucyjnych praw i wolności jednostki wprowadzone w art. 20cb ust. 1 ustawy o Policji, tego samego rodzaju ograniczenie ustanowione w art. 10bb ust. 1 ustawy o Straży Granicznej jest usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując tę część rozważań, należy stwierdzić, że art. 10bb ust. 1 ustawy o Straży Granicznej **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku

z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

5. Ocena zarzutu niezgodności art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych ma następującą treść:

„Art. 30. 1. W celu zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Żandarmeria Wojskowa może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

- 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,
- 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2016 r. poz. 1113 i 1250), zwane dalej <danymi pocztowymi>,
- 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030), zwane dalej <danymi internetowymi> – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Przepis art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych brzmi:

„Art. 30b. 1. Kontrolę nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych, pocztowych lub internetowych sprawuje

wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane.

2. Organ Żandarmerii Wojskowej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych.

3. W ramach kontroli, o której mowa w ust. 1, wojskowy sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych, pocztowych lub internetowych.

4. Wojskowy sąd okręgowy informuje organ Żandarmerii Wojskowej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 30c ust. 1 (przepis ten upoważnia Straż Graniczną do uzyskiwania, między innymi w celu zapobiegania lub wykrywania przestępstw - w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych - danych z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

Przepis art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych upoważnia zatem żołnierzy Żandarmerii Wojskowej do gromadzenia oraz przetwarzania - bez wiedzy i zgody osoby, której dotyczą - danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych pocztowych, o których mowa w art. 82 ust. 1

pkt 1 ustawy - Prawo pocztowe, oraz danych internetowych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną (ust. 1), a także określa przedmiotowe przesłanki udostępniania tych danych na żądanie żołnierzy Żandarmerii Wojskowej (ust. 2-7).

Z kolei art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych wprowadza kontrolę następczą wojskowego sądu okręgowego właściwego dla siedziby organu Żandarmerii Wojskowej nad uzyskiwaniem przez tę formację danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, określonych w art. 30 tej ustawy. Co do zasady, procedura kontrolna została określona w tym przepisie w sposób identyczny, jak w art. 20ca ustawy o Policji oraz w art. 10ba ustawy o Straży Granicznej (różnice dotyczą określenia sądu właściwego do przeprowadzenia tej kontroli).

Natomiast treść normatywną art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych od treści normatywnej art. 20c ust. 1 ustawy o Policji oraz art. 10b ust. 1 ustawy o Straży Granicznej różni odmienny cel udostępniania danych. W art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych celem tym jest bowiem **zapobieganie lub wykrywanie przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 tej ustawy, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.**

Na wstępie należy zauważyć, iż Wnioskodawca, spośród trzech wymienionych w zaskarżonym przepisie celów udostępniania danych (zapobieganie lub wykrywanie przestępstw, w tym przestępstw skarbowych, albo ratowanie życia lub zdrowia ludzkiego bądź wsparcie działań poszukiwawczych lub ratowniczych), podobnie jak w przypadku art. 20c ust. 1 ustawy o Policji, kwestionuje wyłącznie udostępnianie danych w celu zapobiegania lub wykrywania przestępstw (w tym przestępstw skarbowych).

W związku z tym trzeba uznać, że uzyskiwanie przez Żandarmerię Wojskową danych, o których mowa w zaskarżonym przepisie, w innych celach niż zapobieganie lub wykrywanie przestępstw, w tym przestępstw skarbowych, **nie jest objęte zarzutem Wnioskodawcy.**

Z powyższych względów postępowanie w przedmiocie kontroli zgodności art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych - w zakresie, w jakim Żandarmeria Wojskowa może uzyskiwać dane telekomunikacyjne, dane pocztowe oraz dane internetowe w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych - z art. 2, art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia. Rzecznik Praw Obywatelskich nie uzasadnił bowiem tego zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonego w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Wnioskodawca wobec art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych sformułował takie same zarzuty i argumenty za niezgodnością tego unormowania z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także z art. 8 Konwencji i art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE jak w odniesieniu do art. 20c ust. 1 w związku z art. 20ca ustawy o Policji i art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej.

Wprawdzie w powołanym wcześniej wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych i danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału w zakresie pozyskiwania przez żołnierzy Żandarmerii Wojskowej danych telekomunikacyjnych można również odnieść do pozyskiwania przez żołnierzy tej formacji pozostałych danych wymienionych w tym przepisie.

Biorąc pod uwagę tezy zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych **mechanizm kontroli** nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane, z powodów, **o których była mowa w pkt III ppkt 1 i 3 niniejszego stanowiska, stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.**

Podobnie bowiem jak w przypadku Policji i Straży Granicznej, wprawdzie kontrola dotyczy jedynie zbiorczych danych ujętych przez organ Żandarmerii Wojskowej w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to jednak nie można nie dostrzec, iż, zgodnie z art. 30b ust. 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, „wojskowy sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych, pocztowych lub internetowych”.**

Formuła ta oznacza to samo, co identyczne w swej treści sformułowania w art. 20ca ust. 3 ustawy o Policji i art. 10ba ust. 3 ustawy o Straży Granicznej, a mianowicie, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi posiadanymi przez organ Żandarmerii Wojskowej materiałami uzasadniającymi wniosek o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 30b ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, to można zasadnie stwierdzić, że kontroli wojskowego sądu okręgowego podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 30 ust. 6 i 7 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych).

Podobnie też jak w przypadku Policji i Straży Granicznej, ocena przez kontrolujący sąd prawidłowości wniosku organu Żandarmerii Wojskowej o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Komendanta Głównego Żandarmerii Wojskowej i komendantów oddziałów Żandarmerii Wojskowej (*vide* - art. 30 ust. 5 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych).

Ponadto do Żandarmerii Wojskowej mają odpowiednie zastosowanie uwagi zawarte w pkt III ppkt 1 niniejszego stanowiska odnoszące się do sposobu

rozumienia sformułowania „niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu”, użytego w art. 30 ust. 7 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Żandarmerii Wojskowej w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość**. Wszak wojskowemu sądowi okręgowemu umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu**.

Powyższe przesądza, że art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, co jednocześnie oznacza zgodność tej regulacji także z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a także z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej.

6. Ocena zarzutu niezgodności art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 30c ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych brzmi:

„Art. 30c. 1. W celu zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Żandarmeria Wojskowa może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
 - 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
 - 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 30 ust. 2-7 stosuje się.”.

Oceniany przepis, podobnie jak w przypadku art. 20cb ustawy o Policji i art. 10bb ustawy o Straży Granicznej, poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, umożliwia Żandarmerii Wojskowej pozyskiwanie danych uzyskiwanych przez operatora przy zawieraniu umowy na usługi telekomunikacyjne (ust. 1 pkt 1).

Z kolei, poprzez odwołanie do art. 161 ustawy - Prawo telekomunikacyjne, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych umożliwia tej formacji uzyskiwanie, w celach w nim określonych, nie tylko tzw. danych abonamentowych, ale również danych przekazanych operatorowi przez użytkownika będącego osobą fizyczną

za jego zgodą, o ile dane te pozostają w związku ze świadczoną usługą (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, Żandarmeria Wojskowa, w celach określonych w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, może uzyskiwać numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Na wstępie należy zauważyć, iż Wnioskodawca, podobnie jak w przypadku art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych (*vide* też - uwagi do art. 20c i art. 20cb ust. 1 ustawy o Policji), **kwestionuje nadmiernie szeroki, w Jego ocenie, katalog przestępstw i przestępstw skarbowych**, w odniesieniu do których dopuszczalne jest uzyskiwanie i przetwarzanie przez Żandarmerię Wojskową danych.

W związku z tym, podobnie jak w przypadku art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych (oraz art. 20c ust. 1 i art. 20cb ust. 1 ustawy o Policji), w odniesieniu do art. 30c ust. 1 omawianej tutaj ustawy także trzeba uznać, że uzyskiwanie na podstawie tego przepisu przez Żandarmerię Wojskową danych w celach innych niż rozpoznawanie, zapobieganie i wykrywanie przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 tej ustawy, **nie jest objęte zarzutem Wnioskodawcy.**

Z powyższych względów postępowanie w przedmiocie kontroli zgodności art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych - w zakresie, w jakim odnosi się do zadań Żandarmerii Wojskowej związanych z ratowaniem życia lub zdrowia ludzkiego bądź wsparciem działań poszukiwawczych lub ratowniczych - z art. 2, art. 30, art. 47, art. 49 i art. 51 ust.

2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE podlega umorzeniu na podstawie art. 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia. Rzecznik Praw Obywatelskich nie uzasadnił bowiem tego zarzutu ze wskazaniem argumentów lub dowodów na jego poparcie, przez co nie zadośćuczynił wymogowi, określonego w art. 47 ust. 2 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

Przechodząc do rozważań merytorycznych, należy stwierdzić, iż zarzuty Wnioskodawcy pod adresem komentowanego przepisu są tożsame z zarzutami sformułowanymi pod adresem art. 20cb ust. 1 ustawy o Policji oraz art. 10bb ust. 1 ustawy o Straży Granicznej.

Wnioskodawca wskazał też identyczne wzorce kontroli.

W tej sytuacji oceny i wnioski przedstawione w pkt III ppkt 2 i 4 niniejszego stanowiska pozostają aktualne także w odniesieniu do art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, co jednocześnie oznacza, że konstytucyjność tego przepisu, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji i art. 10bb ust. 1 ustawy o Straży Granicznej, **determinuje zakres** uzyskiwanych przez Żandarmerię Wojskową, a określonych w tym przepisie danych, jak również **zasady przekazywania tych danych operatorowi telekomunikacyjnemu przez użytkownika**.

Podobnie bowiem jak w - odpowiadających w tym przypadku treściowo i wzajemnie porównywanych - przepisach art. 20c ust. 1 pkt 1 i art. 20cb ust. 1 ustawy o Policji oraz art. 10b ust. 1 pkt 1 i art. 10bb ust. 1 ustawy o Straży Granicznej, określony w art. 30 ust. 1 pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zakres danych telekomunikacyjnych jest

znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, co, w konsekwencji, prowadzi do wniosku, że dane z art. 30 ust. 1 pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych **zawierają nieporównanie więcej informacji o osobie** niż dane, o których mowa w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

O ile w oparciu o art. 30 ust. 1 pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

W przedstawionych warunkach, o ile w przypadku pozyskiwania danych na podstawie art. 30 ust. 1 pkt 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej wykazano, zostały przewidziane w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych), o tyle w przypadku pozyskiwania danych na podstawie art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych **konieczność taka nie zachodzi**.

Należy bowiem zauważyć, iż, tak jak dane z art. 20cb ust. 1 ustawy o Policji oraz dane z art. 10bb ust. 1 ustawy o Straży Granicznej, niektóre dane, określone w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego także **za zgodą** abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji, podobnie jak w przypadku danych z art. 20cb ust. 1 ustawy o Policji oraz danych z art. 10bb ust. 1 ustawy o Straży Granicznej, można zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych ingerencja w prawa i wolności jednostki, zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Przy tym, podobnie do jak ograniczenia konstytucyjnych praw i wolności jednostki wprowadzone w art. 20cb ust. 1 ustawy o Policji oraz w art. 10bb ust. 1 ustawy o Straży Granicznej, tego samego rodzaju ograniczenie wynikające z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych jest usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w części odnoszącej się do zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 tej ustawy, **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji,

a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

7. Ocena zarzutu niezgodności art. 28 ust. 1 w związku z art. 28a ustawy o ABW oraz AW z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Zakwestionowany przepis art. 28 ust. 1 ustawy o ABW oraz AW ma następujące brzmienie:

„Art. 28. 1. ABW może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1, dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

- 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489 z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,
- 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2016 r. poz. 1113 i 1250), zwane dalej <danymi pocztowymi>,
- 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), zwane dalej <danymi internetowymi> - oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Z kolei art. 5 ust. 1 ustawy o ABW oraz AW, do którego odwołuje się art. 28 ust. 1 tej ustawy, brzmi:

„Art. 5. 1. Do zadań ABW należy:

- 1) rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa;
- 2) rozpoznawanie, zapobieganie i wykrywanie przestępstw:

- a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa,
 - b) godzących w podstawy ekonomiczne państwa,
 - c) korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2017 r. poz. 1393), jeśli może to godzić w bezpieczeństwo państwa,
 - d) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
 - e) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym,
 - f) przeciwko wymiarowi sprawiedliwości, określonych w art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2016 r. poz. 1137, z późn. zm.), jeżeli pozostają w związku z przestępstwami, o których mowa w lit. a-e
- oraz ściganie ich sprawców;
- 2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566);
 - 2b) ujawnianie mienia zagrożonego przepadkiem w związku z przestępstwami, o których mowa w pkt 2;

- 3) realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;
- 4) uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego;
- 5) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.”.

Natomiast art. 28a ustawy o ABW oraz AW brzmi:

„Art. 28a. 1. Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie.

2. Szef ABW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa ABW o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28b ust. 1 (przepis ten upoważnia ABW do uzyskiwania - w celu realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW - danych z wykazu,

o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

Dla przypomnienia, przepis art. 28 ustawy o ABW oraz AW upoważnia ABW do gromadzenia oraz przetwarzania - bez wiedzy i zgody osoby, której dotyczą - danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych pocztowych, o których mowa w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe, oraz danych internetowych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną (ust. 1), a także określa przedmiotowe przesłanki udostępniania tych danych na żądanie funkcjonariuszy ABW (ust. 2-7).

Z kolei art. 28a ustawy o ABW oraz AW wprowadza kontrolę następczą Sądu Okręgowego w Warszawie nad uzyskiwaniem przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, określonych w art. 28 tej ustawy. Co do zasady, procedura kontrolna została określona w tym przepisie w sposób identyczny jak w art. 20ca ustawy o Policji, w art. 10ba ustawy o Straży Granicznej oraz w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

Wobec art. 28 ust. 1 w związku z art. 28a ustawy o ABW oraz AW Wnioskodawca sformułował, jak się wydaje, odmienne zarzuty i argumenty za niezgodnością tego unormowania z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także z art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, niż w odniesieniu do art. 20c ust. 1 w związku z art. 20ca ustawy o Policji, art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej oraz art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Wskazał bowiem, że konstytucyjną wadą zaskarżonej normy jest uniemożliwienie sądowi sprawowania rzeczywistej kontroli udostępniania funkcjonariuszom Agencji Bezpieczeństwa Wewnętrznego danych

telekomunikacyjnych, danych pocztowych oraz danych internetowych, wymienionych w art. 28 ust. 1 ustawy o ABW oraz AW, **niezbędnych do realizacji zadań, o których mowa w art. 5 ust. 1 tej ustawy**, przy czym rozpoznawanie, zapobieganie i wykrywanie niektórych przestępstw (*vide* - art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW) jest tylko jednym z, określonych w tym przepisie, zadań wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego.

Do wykonywanych przez funkcjonariuszy tej Agencji zadań innych niż rozpoznawanie, zapobieganie i wykrywanie przestępstw ustawa o ABW oraz AW - co należy przypomnieć - zalicza: 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 (art. 1 ust. 1 pkt 1), rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jednolity - Dz. U. z 2013 r., poz. 1166 ze zm.) [art. 1 ust. 1 pkt 2a], 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 (art. 1 ust. 1 pkt 3), uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (art. 1 ust. 1 pkt 4) oraz podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 1 ust. 1 pkt 5).

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, kontrolując zgodność z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW, który w chwili kontroli brzmiał:

„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.);”,
zaś art. 5 ust. 1 pkt 2 tej samej ustawy, w chwili kontroli, zawierał treść:

„2) rozpoznawanie, zapobieganie i wykrywanie przestępstw:

a) szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa,

b) godzących w podstawy ekonomiczne państwa,

c) korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584, z 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375), jeśli może to godzić w bezpieczeństwo państwa,

d) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,

e) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców;”,

stwierdził, że *„niektóre zadania w postaci rozpoznawania i wykrywania przestępstw wymienionych w art. 5 ust. 1 pkt 2 ustawy o ABW i zapobiegania takim przestępstwom zostały sformułowane w sposób na tyle ogólny, że nie można*

na ich podstawie zdefiniować konkretnych okoliczności, w których mogą być udostępniane funkcjonariuszom ABW dane telekomunikacyjne”, po czym „raz jeszcze” podkreślił, że „relatywnie ogólne wskazanie zadań organu władzy publicznej (...) samo w sobie nie jest niezgodne z Konstytucją. Problem powstaje natomiast wtedy, gdy w ramach takich zadań, organy władzy publicznej mogą podejmować działania ingerujące w wolności i prawa jednostek polegające na niejawnym pozyskiwaniu informacji. Ilekroć organ władzy publicznej jest uprawniony do pozyskiwania informacji o życiu prywatnym jednostek, w tym danych telekomunikacyjnych, konieczne jest bardzo precyzyjne określenie w ustawie przedmiotowego zakresu, w jakich te działania mogą być realizowane”, zaś, odnosząc tę uwagę bezpośrednio do Agencji Bezpieczeństwa Wewnętrznego, stwierdził, że, „[m]ając na uwadze wyjątkowo szeroki zakres okoliczności, w jakich ABW może mieć udostępnione dane telekomunikacyjne, a zarazem jednoznaczne wyłączenie obowiązku uzyskania zgody sądu oraz braku obowiązku uzyskania zgody jakiegokolwiek niezależnego organu na ich pozyskanie, Trybunał stwierdza, że zakwestionowany przepis nie zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia Konstytucji. Jest to wystarczające do stwierdzenia niezgodności art. 28 ust. 1 pkt 1 ustawy o ABW przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji” (op. cit.).

Wprawdzie w powołanym wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 28 ust. 1 (pkt 1) ustawy o ABW oraz AW, którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych i danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału co do pozyskiwania przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego danych

telekomunikacyjnych można również odnieść do pozyskiwania przez tychże funkcjonariuszy pozostałych danych wymienionych we wskazanym przepisie.

Biorąc pod uwagę tezy zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 28a ustawy o ABW oraz AW **mechanizm kontroli** nad uzyskiwaniem przez Agencję Bezpieczeństwa Wewnętrznego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez Sąd Okręgowy w Warszawie, z powodów, **o których była mowa w pkt III ppkt 1, 3 i 5 niniejszego stanowiska, stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.**

Podobnie bowiem jak w przypadku Policji, Straży Granicznej i Żandarmerii Wojskowej, wprawdzie kontrola dotyczy jedynie zbiorczych danych ujętych przez Szefa Agencji Bezpieczeństwa Wewnętrznego w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to jednak nie można pominąć tego, iż, zgodnie z art. 28a ust. 3 ustawy o ABW oraz AW, „sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych”.**

Formuła ta oznacza to samo, co identyczne w swej treści sformułowania w art. 20ca ust. 3 ustawy o Policji, art. 10ba ust. 3 ustawy o Straży Granicznej i art. 30b ust. 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych a mianowicie, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi posiadanymi przez Szefa Agencji Bezpieczeństwa Wewnętrznego materiałami uzasadniającymi wnioski o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 28 ust. 1 ustawy o ABW oraz AW. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 28a ust. 2 ustawy

o ABW oraz AW, to można zasadnie stwierdzić, że kontroli Sądu Okręgowego w Warszawie podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 28 ust. 6 i 7 ustawy o ABW oraz AW).

Podobnie też jak w przypadku Policji, Straży Granicznej i Żandarmerii Wojskowej, ocena przez kontrolujący sąd prawidłowości wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Szefa Agencji Bezpieczeństwa Wewnętrznego (*vide* - art. 28 ust. 5 ustawy o ABW oraz AW).

Ponadto do Agencji Bezpieczeństwa Wewnętrznego mają odpowiednie zastosowanie uwagi zawarte w pkt III ppkt 1 niniejszego stanowiska odnoszące się do sposobu rozumienia określenia „niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu”, użytego w art. 28 ust. 7 ustawy o ABW oraz AW.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 28a ustawy o ABW oraz AW mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Agencji Bezpieczeństwa Wewnętrznego w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość**. Wszak Sądowi Okręgowemu w Warszawie umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego

pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu.**

Wszystko to powoduje, że art. 28 ust. 1 w związku z art. 28a ustawy o ABW oraz AW **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

8. Ocena zarzutu niezgodności art. 28b ust. 1 ustawy o ABW oraz AW z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Art. 28b ustawy o ABW oraz AW brzmi:

„Art. 28b. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1, ABW może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 3) w przypadku użytkownika, który nie jest osobą fizyczną, numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
- 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 28 ust. 2-7 stosuje się.”.

Analizowany przepis, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o

Żandarmerii Wojskowej i wojskowych organach porządkowych, poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, umożliwia Agencji Bezpieczeństwa Wewnętrznego uzyskiwanie danych przekazywanych przez użytkownika przy zawieraniu umowy na usługi telekomunikacyjne (ust. 1 pkt 1).

Z kolei, poprzez odwołanie do art. 161 ustawy - Prawo telekomunikacyjne, art. 28b ustawy o ABW oraz AW umożliwia Agencji Bezpieczeństwa Wewnętrznego uzyskiwanie, w celach w nim określonych, tzw. danych abonamentowych oraz danych przekazanych operatorowi przez użytkownika będącego osobą fizyczną za jego zgodą, o ile dane te pozostają w związku ze świadczoną usługą (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, w celach określonych w art. 28b ustawy o ABW oraz AW, będą mogli uzyskiwać numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Należy stwierdzić, iż pomiędzy zarzutami Wnioskodawcy sformułowanymi pod adresem analizowanego przepisu a zarzutami sformułowanymi pod adresem art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zachodzi podobieństwo.

Wnioskodawca wskazał też identyczne wzorce kontroli.

O ile jednak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zarzut braku jakiejkolwiek niezależnej kontroli uzyskiwania przez wskazane w tych przepisach służby

powołane do ochrony porządku publicznego wymienionych tamże danych Wnioskodawca połączył z zarzutem nadmiernie szerokiego, w Jego ocenie, katalogu przestępstw lub przestępstw skarbowych, w odniesieniu do których dopuszczalne jest uzyskiwanie i przetwarzanie przez te służby danych, o tyle, w przypadku art. 28b ust. 1 ustawy o ABW oraz AW, podobnie jak w przypadku art. 28 ust. 1 tejże ustawy, Wnioskodawca zarzut braku jakiegokolwiek niezależnej kontroli uzyskiwania danych łączy z zarzutem braku precyzyjnego określenia w ustawie przedmiotowego zakresu, w jakim w omawianej sferze mogą być realizowane działania Agencji Bezpieczeństwa Wewnętrznego, w związku z przewidzianym w art. 28b ust. 1 ustawy o ABW oraz AW ogólnym odesłaniem do przepisu tejże ustawy (art. 5 ust. 1), który zawiera szeroki katalog zadań wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego.

Niemniej oceny i wnioski przedstawione w pkt III ppkt 2, 4 i 6 niniejszego stanowiska, pomimo (o czym wcześniej była mowa) częściowo odmiennego zarzutu Wnioskodawcy, pozostają aktualne także w odniesieniu do art. 28b ust. 1 ustawy o ABW oraz AW, ponieważ konstytucyjność tego przepisu, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, **determinuje zakres** uzyskiwanych przez Agencję Bezpieczeństwa Wewnętrznego, a określonych w tym przepisie danych, jak również **zasady przekazywania tych danych operatorowi telekomunikacyjnemu przez użytkownika.**

Podobnie bowiem jak w - odpowiadających w tym przypadku treściowo i wzajemnie porównywanych - przepisach art. 20c ust. 1 pkt 1 i art. 20cb ust. 1 ustawy o Policji, art. 10b ust. 1 pkt 1 i art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30 ust. 1 pkt 1 i art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, określony w art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW zakres danych telekomunikacyjnych jest znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 28b ust. 1 ustawy o

ABW oraz AW, co, w konsekwencji, prowadzi do wniosku, że dane z 28 ust. 1 pkt 1 ustawy o ABW oraz AW **zawierają nieporównanie więcej informacji o osobie** niż dane, o których mowa w art. 28b ust. 1 ustawy o ABW oraz AW.

O ile w oparciu o art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 28b ust. 1 ustawy o ABW oraz AW możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

W przedstawionych warunkach, o ile w przypadku pozyskiwania danych na podstawie art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej wykazano, zostały przewidziane w art. 28a ustawy o ABW oraz AW), o tyle w przypadku pozyskiwania danych na podstawie art. 28b ust. 1 ustawy o ABW oraz AW **konieczność taka nie zachodzi**.

Należy bowiem zauważyć, iż, tak jak dane z art. 20cb ust. 1 ustawy o Policji, dane z art. 10bb ust. 1 ustawy o Straży Granicznej oraz dane z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, niektóre dane, określone w art. 28b ust. 1 ustawy o ABW oraz AW, przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Z kolei pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego także **za zgodą** abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji, podobnie jak w przypadku danych z art. 20cb ust. 1 ustawy o Policji, z art. 10bb ust. 1 ustawy o Straży Granicznej oraz z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, można

zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 28b ust. 1 ustawy o ABW oraz AW ingerencja w prawa i wolności jednostki, zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji, nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Przy tym, podobnie jak ograniczenia konstytucyjnych praw i wolności jednostki wprowadzone w art. 20cb ust. 1 ustawy o Policji, w art. 10bb ust. 1 ustawy o Straży Granicznej oraz w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, tego samego rodzaju ograniczenie wprowadzone w art. 28b ust. 1 ustawy o ABW oraz AW jest usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując, art. 28b ust. 1 ustawy o ABW oraz AW **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

9. Ocena zarzutu niezgodności art. 32 ust. 1 w związku z art. 32a ustawy o SKW oraz SWW z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Zakwestionowany przepis art. 32 ust. 1 ustawy o SKW oraz SWW ma następującą treść:

„Art. 32. 1. SKW może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 5, dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

- 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,
 - 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2017 r. poz. 1481), zwane dalej <danymi pocztowymi>,
 - 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), zwane dalej <danymi internetowymi>
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Z kolei art. 5 ustawy o SKW oraz SWW, do którego odwołuje się art. 32 ust. 1 tej ustawy, brzmi:

„Art. 5. 1. Do zadań SKW należy:

- 1) rozpoznawanie, zapobieganie oraz wykrywanie, popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, przestępstw:
 - a) przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w rozdziale XVI ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2016 r. poz. 1137, z późn. zm.), a także innych ustawach i umowach międzynarodowych,
 - b) przeciwko Rzeczypospolitej Polskiej określonych w rozdziale XVII ustawy z dnia 6 czerwca 1997 r. - Kodeks karny oraz takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność,
 - c) określonych w art. 140 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,
 - d) określonych w art. 228-230 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON,

e) przeciwko ochronie informacji określonych w rozdziale XXXIII ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, a także takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność,

f) określonych w art. 33 ust. 1, 2 i 3 ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2017 r. poz. 1050),

g) innych niż określone w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność,

h) określonych w art. 232, art. 233 § 1, 1a, 4 i 6, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, jeżeli dotyczą przestępstw, o których mowa w lit. a-g,

jak również ujawnianie mienia zagrożonego przypadkiem w związku z tymi przestępstwami;

2) współdziałanie z Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania przestępstw wymienionych w pkt 1;

2a) rozpoznawanie, zapobieganie oraz wykrywanie zdarzeń oraz przestępstw o charakterze terrorystycznym godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON;

3) realizowanie, w granicach swojej właściwości, zadań określonych w przepisach ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948 oraz z 2017 r. poz. 935);

4) uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej SZ RP lub innych jednostek

organizacyjnych MON, w zakresie określonym w pkt 1, oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń;

5) prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy;

6) uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia;

7) ochrona bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa;

8) ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez SZ RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez SZ RP i inne jednostki organizacyjne MON, w zakresie określonym w pkt 1;

9) podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana.

2. Zadania SKW obejmują również rozpoznawanie oraz wykrywanie przestępstw, o których mowa w ust. 1, popełnionych we współdziałaniu z żołnierzami pełniącymi czynną służbę wojskową, funkcjonariuszami SKW i SWW lub pracownikami SZ RP i innych jednostek organizacyjnych MON.

3. Działalność SKW poza granicami Rzeczypospolitej Polskiej może być prowadzona w związku z jej działalnością na terytorium państwa wyłącznie w zakresie realizacji zadań określonych w ust. 1 i 2.”.

Natomiast art. 32a ustawy o SKW oraz SWW brzmi:

„Art. 32a. 1. Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Wojskowy Sąd Okręgowy w Warszawie.

2. Szef SKW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa SKW o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 32b ust. 1 (przepis ten upoważnia SKW do uzyskiwania w celu realizacji zadań, o których mowa w art. 5 ustawy o SKW oraz SWW, danych z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

Przepis art. 32 ustawy o SKW oraz SWW upoważnia zatem Służbę Kontrwywiadu Wojskowego do gromadzenia oraz przetwarzania - bez wiedzy i zgody osoby, której dotyczą - danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych pocztowych, o których mowa w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe, oraz danych internetowych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną (ust. 1), a także określa przedmiotowe przesłanki udostępniania tych danych na żądanie funkcjonariuszy SKW (ust. 2-9).

Z kolei art. 32a ustawy o SKW oraz SWW wprowadza kontrolę następczą Wojskowego Sądu Okręgowego w Warszawie nad uzyskiwaniem przez funkcjonariuszy Służby Kontrwywiadu Wojskowego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych,

określonych w art. 32 tej ustawy. Co do zasady, procedura kontrolna została określona w tym przepisie w sposób identyczny, jak w art. 20ca ustawy o Policji, w art. 10ba ustawy o Straży Granicznej, w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz w art. 28a ustawy o ABW oraz AW.

Wobec art. 32 ust. 1 w związku z art. 32a ustawy o SKW oraz SWW, podobnie jak w przypadku art. 28 ust. 1 w związku z art. 28a ustawy o ABW oraz AW, Wnioskodawca sformułował, jak się wydaje, odmienne zarzuty i argumenty za jego niezgodnością z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także z art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, niż w odniesieniu do art. 20c ust. 1 w związku z art. 20ca ustawy o Policji, art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej oraz art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Wskazał bowiem, że konstytucyjną wadą zaskarżonej normy jest uniemożliwienie sądowi sprawowania rzeczywistej kontroli udostępniania funkcjonariuszom Służby Kontrwywiadu Wojskowego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, wymienionych w art. 32 ust. 1 ustawy o SKW oraz SWW, **niezbędnych do realizacji zadań, o których mowa w art. 5 tej ustawy**, przy czym rozpoznawanie, zapobieganie i wykrywanie niektórych przestępstw (*vide* - art. 5 ust. 1 pkt 1 ustawy o SKW oraz SWW) jest tylko jednym z zadań wykonywanych przez tę Służbę.

Do wykonywanych przez funkcjonariuszy Służby Kontrwywiadu Wojskowego zadań innych niż rozpoznawanie, zapobieganie i wykrywanie przestępstw ustawa o SKW oraz SWW zalicza - co należy przypomnieć - między innymi, prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy (art. 5 ust. 1 pkt 5), ochronę bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa (art. 5

ust. 1 pkt 7) czy też podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana (art. 5 ust. 1 pkt 9).

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, kontrolując zgodność z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW, który w chwili kontroli brzmiał:

„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. z 2014 r. poz. 243), zwanych dalej <danymi telekomunikacyjnymi>;”

zwrócił uwagę na bardzo szeroki zakres zadań, dla realizacji których Służba Kontrwywiadu Wojskowego może pozyskiwać dane telekomunikacyjne (ówczesne brzmienie art. 5 ustawy o SKW oraz SWW nie odbiegało znacznie od obecnego brzmienia tego przepisu), stwierdzając, że „[n]ie zawężają się (one - przyp. wł.) *do rozpoznawania oraz wykrywania przestępstw wymienionych w art. 5 ust. 1 pkt 1, popełnionych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych i innych jednostek organizacyjnych MON, czy zapobiegania takim przestępstwom. Obejmują też zadania polegające m.in. na uzyskiwaniu, gromadzeniu, analizowaniu, przetwarzaniu i przekazywaniu właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych lub innych jednostek organizacyjnych MON, w zakresie przestępstw określonych w art. 5 ust. 1 pkt 1, a ponadto podejmowanie działań w celu eliminowania ustalonych zagrożeń (art. 5 ust. 1 pkt 6), uczestnictwa w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia (art. 5 ust. 1 pkt 4), czy rozpoznawanie i wykrywanie*

przestępstw, o których mowa w art. 5 ust. 1, popełnionych we współdziałaniu z żołnierzami pełniącymi czynną służbę wojskową, funkcjonariuszami SKW i SWW lub pracownikami Sił Zbrojnych i innych jednostek organizacyjnych MON” oraz że „[j]akkolwiek specyfika wojskowej służby kontrwywiadowczej, właściwej w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej, może uzasadniać - do pewnego stopnia - szerszy zakres kompetencji w zakresie pozyskiwania danych telekomunikacyjnych, to jednak zdaniem Trybunału Konstytucyjnego niezbędne jest istnienie gwarancji proceduralnych, które zapobiegą nadużywaniu prawa” (op. cit.).

Wprawdzie w powołanym wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 32 ust. 1 (pkt 1) ustawy o SKW oraz SWW, którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych oraz danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału odnośnie do pozyskiwania przez funkcjonariuszy Służby Kontrwywiadu Wojskowego danych telekomunikacyjnych można również odnieść do pozyskiwania przez tych funkcjonariuszy pozostałych danych wymienionych obecnie w tym przepisie.

Biorąc pod uwagę tezy zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 32a ustawy o SKW oraz SWW **mechanizm kontroli** nad uzyskiwaniem przez Służbę Kontrwywiadu Wojskowego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez Wojskowy Sąd Okręgowy w Warszawie, z powodów, o których była mowa w pkt III ppkt 1, 3, 5 i 7 niniejszego stanowiska, stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.

Podobnie bowiem jak w przypadku Policji, Straży Granicznej, Żandarmerii Wojskowej i Agencji Bezpieczeństwa Wewnętrznego, wprowadzie kontrola dotyczy jedynie zbiorczych danych ujętych przez Szefa Służby Kontrwywiadu Wojskowego w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to nie można jednak nie dostrzegać, iż, zgodnie z art. 32a ust. 3 ustawy o SKW oraz SWW, „sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych”.**

Sformułowanie to oznacza to samo, co identyczne w swej treści formuły w art. 20ca ust. 3 ustawy o Policji, art. 10ba ust. 3 ustawy o Straży Granicznej, art. 30b ust. 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych i art. 28a ust. 3 ustawy o ABW oraz AW, a mianowicie, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi posiadanymi przez Szefa Kontrwywiadu Wojskowego materiałami uzasadniającymi wniosek o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 32 ust. 1 ustawy o SKW oraz SWW. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 32a ust. 2 ustawy o SKW oraz SWW, to można zasadnie stwierdzić, że kontroli Wojskowego Sądu Okręgowego w Warszawie podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 32 ust. 8 i 9 ustawy o SKW oraz SWW).

Podobnie też jak w przypadku Policji, Straży Granicznej, Żandarmerii Wojskowej i Agencji Bezpieczeństwa Wewnętrznego, ocena przez kontrolujący sąd prawidłowości wniosku Szefa Służby Kontrwywiadu Wojskowego o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Szefa Służby Kontrwywiadu Wojskowego (*vide* - art. 32 ust. 7 ustawy o SKW oraz SWW).

Ponadto do Służby Kontrwywiadu Wojskowego mają odpowiednie zastosowanie uwagi zawarte w pkt III ppkt 1 niniejszego stanowiska, odnoszące się do sposobu rozumienia określenia „niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu”, użytego w art. 32 ust. 9 ustawy o SKW oraz SWW.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 32a ustawy o SKW oraz SWW mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Służby Kontrwywiadu Wojskowego w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość.** Wszak Wojskowemu Sądowi Okręgowemu w Warszawie umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu.**

Wszystko to powoduje, że art. 32 ust. 1 w związku z art. 32a ustawy o SKW oraz SWW **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

10. Ocena zarzutu niezgodności art. 32b ust. 1 ustawy o SKW oraz SWW z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 32b ustawy o SKW oraz SWW brzmi:

„Art. 32b. 1. W celu realizacji zadań, o których mowa w art. 5, SKW może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
- 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 32 ust. 2-9 stosuje się.”.

Oceniany przepis, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 28b ustawy o ABW oraz AW, poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, umożliwia Służbie Kontrwywiadu Wojskowego uzyskiwanie danych przekazywanych przez użytkownika przy zawieraniu umowy na usługi telekomunikacyjne (ust. 1 pkt 1).

Z kolei, poprzez odwołanie do art. 161 ustawy - Prawo telekomunikacyjne, art. 32b ustawy o SKW oraz SWW umożliwia Służbie

Kontrwywiadu Wojskowego uzyskiwanie, w celach w nim określonych, tzw. danych abonamentowych oraz danych przekazanych operatorowi przez użytkownika będącego osobą fizyczną za jego zgodą, o ile dane te pozostają w związku ze świadczoną usługą (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, funkcjonariusze Służby Kontrwywiadu Wojskowego, w celach określonych w art. 32b ustawy o SKW oraz SWW, mogą uzyskiwać numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Należy odnotować, iż pomiędzy zarzutami Wnioskodawcy, sformułowanymi pod adresem wskazanego przepisu ustawy o SKW oraz SWW, a zarzutami, sformułowanymi pod adresem art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 28b ust. 1 ustawy o ABW oraz AW, zachodzi podobieństwo.

Wnioskodawca wskazał też identyczne wzorce kontroli.

O ile jednak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zarzut braku jakiegokolwiek niezależnej kontroli uzyskiwania przez wskazane w tych przepisach służby powołane do ochrony porządku publicznego wymienionych tamże danych Wnioskodawca połączył z zarzutem nadmiernie szerokiego, w Jego ocenie, katalogu przestępstw lub przestępstw skarbowych, w odniesieniu do których dopuszczalne jest uzyskiwanie i przetwarzanie przez te służby danych, o tyle, w przypadku art. 32b ust. 1 ustawy o SKW oraz SWW, podobnie jak w przypadku art. 32 ust. 1 tejże ustawy, Wnioskodawca zarzut braku jakiegokolwiek niezależnej kontroli uzyskiwania danych łączy z zarzutem braku precyzyjnego określenia w

ustawie przedmiotowego zakresu, w jakim w omawianej sferze mogą być realizowane działania Służby Kontrwywiadu Wojskowego, w związku z przewidzianym w art. 32b ust. 1 ustawy o SKW oraz SWW ogólnym odesłaniem do przepisu tejże ustawy (art. 5), który zawiera szeroki katalog zadań wykonywanych przez Służbę Kontrwywiadu Wojskowego.

Niemniej jednak oceny i wnioski przedstawione w pkt III ppkt 2, 4, 6 i 8 niniejszego stanowiska pozostają aktualne także w odniesieniu do art. 32b ust. 1 ustawy o SKW oraz SWW, co jednocześnie oznacza, że konstytucyjność tego przepisu, podobnie jak w przypadku art. 20cb ust 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 28b ust. 1 ustawy o ABW oraz AW, **determinuje zakres** uzyskiwanych przez Służbę Kontrwywiadu Wojskowego, a określonych w tym przepisie danych, jak również **zasady przekazywania tych danych operatorowi telekomunikacyjnemu przez użytkownika**.

Podobnie bowiem jak w - odpowiadających w tym przypadku treściowo i wzajemnie porównywanych - przepisach art. 20c ust. 1 pkt 1 i art. 20cb ust. 1 ustawy o Policji, art. 10b ust. 1 pkt 1 i art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 pkt 1 i art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz art. 28 ust. 1 pkt 1 i art. 28b ust. 1 ustawy o ABW oraz AW, określony w art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW zakres danych telekomunikacyjnych jest znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 32b ust. 1 ustawy o SKW oraz SWW, co, w konsekwencji, prowadzi do wniosku, że dane z art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW **zawierają nieporównanie więcej informacji o osobie niż dane**, o których mowa w art. 32b ust. 1 ustawy o SKW oraz SWW.

O ile w oparciu o art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału

Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 32b ust. 1 ustawy o SKW oraz SWW możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

W przedstawionych warunkach, o ile w przypadku pozyskiwania danych na podstawie art. 32 ust. 1 pkt 1 ustawy o SKW oraz SWW zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej wykazano, zostały przewidziane w art. 32a ustawy o SKW oraz SWW), o tyle w przypadku pozyskiwania danych na podstawie art. 32b ust. 1 ustawy o SKW oraz SWW **konieczność taka nie zachodzi**.

Należy bowiem zauważyć, iż, tak jak dane z art. 20cb ust. 1 ustawy o Policji, dane z art. 10bb ust. 1 ustawy o Straży Granicznej, dane z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz dane z art. 28b ust. 1 ustawy o ABW oraz AW, niektóre dane, określone w art. 32b ust. 1 ustawy o SKW oraz SWW przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego także **za zgodą** abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji, podobnie jak w przypadku danych z art. 20cb ust. 1 ustawy o Policji, z art. 10bb ustawy o Straży Granicznej, z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz z art. 28b ust. 1 ustawy o ABW oraz AW, można zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 32b

ust. 1 ustawy o SKW oraz SWW ingerencja w prawa i wolności jednostki zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Przy tym, podobnie jak ograniczenie konstytucyjnych praw i wolności jednostki wprowadzone w art. 20cb ust. 1 ustawy o Policji, w art. 10bb ust. 1 ustawy o Straży Granicznej, w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz w art. 28b ust. 1 ustawy o ABW oraz AW, tego samego rodzaju ograniczenie wprowadzone w art. 32b ust. 1 ustawy o SKW oraz SWW jest usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując, art. 32b ust. 1 ustawy o SKW oraz SWW **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

11. Ocena zarzutu niezgodności art. 18 ust. 1 w związku z art. 18a ustawy o CBA z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Zakwestionowany przepis art. 18 ust. 1 ustawy o CBA ma następującą treść:

„Art. 18. 1. CBA może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 2, dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

- 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.), zwane dalej <danymi telekomunikacyjnymi>,
- 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2017 r. poz. 1481), zwane dalej <danymi pocztowymi>,
- 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), zwane dalej <danymi internetowymi> - oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”.

Z kolei art. 2 ustawy o CBA, do którego przepis art. 18 ust. 1 tej ustawy się odwołuje, brzmi:

„Art. 2. 1. Do zadań CBA, w zakresie właściwości określonej w art. 1 ust. 1, należy:

- 1) rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko:
 - a) działalności instytucji państwowych oraz samorządu terytorialnego, określonych w art. 228-231 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, a także o którym mowa w art. 14 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2017 r. poz. 1393),
 - b) wymiarowi sprawiedliwości, określonych w art. 232, art. 233, art. 234, art. 235, art. 236 § 1 i art. 239 § 1, wyborom i referendum, określonych w art. 250a, porządkowi publicznemu, określonych w art. 258, wiarygodności dokumentów, określonych w art. 270-273 i art. 277a § 1, mieniu, określonych w art. 286, obrotowi gospodarczemu, określonych w art. 296-297, art. 299 i art. 305, obrotowi pieniędzmi i papierami wartościowymi, określonych w art. 310 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, a także o których mowa w art. 585-592 ustawy z dnia 15 września 2000 r. - Kodeks spółek handlowych (Dz. U. z 2017 r. poz. 1577) oraz określonych w art. 179-183 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2017 r. poz. 1768), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa,

- c) finansowaniu partii politycznych, określonych w art. 49d i 49f ustawy z dnia 27 czerwca 1997 r. o partiach politycznych (Dz. U. z 2017 r. poz. 876 i 1089), jeżeli pozostają w związku z korupcją,
 - d) obowiązkom podatkowym i rozliczeniom z tytułu dotacji i subwencji, określonych w rozdziale 6 ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy (Dz. U. z 2016 r. poz. 2137, z późn. zm.), jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa,
 - e) zasadom rywalizacji sportowej, określonych w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2017 r. poz. 1463 i 1600),
 - f) obrotowi lekami, środkami spożywczymi specjalnego przeznaczenia żywieniowego, wyrobami medycznymi określonymi w art. 54 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2016 r. poz. 1536 i 1579 oraz z 2017 r. poz. 1200 i 1458)
- oraz ściganie ich sprawców;
- 1a) ujawnianie mienia zagrożonego przepadkiem w związku z przestępstwami, o których mowa w pkt 1;
 - 2) ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne;
 - 3) dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy z dnia 21 czerwca 1990 r. o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych (Dz. U. poz. 255, z późn. zm.);
 - 4) ujawnianie przypadków nieprzestrzegania określonych przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem jednostek lub przedsiębiorców, o których mowa w art. 1 ust. 4 oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i

przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych;

5) kontrola prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, o których mowa w art. 115 § 19 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, składanych na podstawie odrębnych przepisów;

6) prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi,

7) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

2. Szef Centralnego Biura Antykorupcyjnego w celu realizacji zadań CBA może podejmować współpracę z właściwymi organami i służbami innych państw oraz z organizacjami międzynarodowymi.

2a. Podjęcie współpracy, o której mowa w ust. 2, może nastąpić po uzyskaniu zgody Prezesa Rady Ministrów.

3. CBA może prowadzić postępowanie przygotowawcze obejmując wszystkie czyny ujawnione w jego przebiegu, jeżeli pozostają w związku podmiotowym lub przedmiotowym z czynem stanowiącym podstawę jego wszczęcia.

4. Działalność CBA poza granicami Rzeczypospolitej Polskiej może być prowadzona w związku z jego działalnością na terytorium państwa wyłącznie w zakresie realizacji zadań określonych w ust. 1 pkt 1.”.

Natomiast art. 18a ustawy o CBA brzmi:

„Art. 18a. 1. Kontrolę nad uzyskiwaniem przez CBA danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie.

2. Szef CBA przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa CBA o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 18b ust. 1 (przepis ten upoważnia CBA do uzyskiwania w celu realizacji zadań, o których mowa w art. 2 ustawy o CBA, danych z wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, oraz danych, o których mowa w art. 161 tejże ustawy - przyp. wł.).”.

Przepis art. 18 ustawy o CBA upoważnia więc funkcjonariuszy CBA do gromadzenia oraz przetwarzania - bez wiedzy i zgody osoby, której dotyczą - danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy - Prawo telekomunikacyjne, danych pocztowych, o których mowa w art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe, oraz danych internetowych, o których mowa w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną (ust. 1), a także określa przedmiotowe przesłanki udostępniania tych danych na żądanie funkcjonariuszy CBA (ust. 2-7).

Z kolei art. 18a ustawy o CBA wprowadza kontrolę następczą Sądu Okręgowego w Warszawie nad uzyskiwaniem przez funkcjonariuszy CBA danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, określonych w art. 18 ust. 1 tej ustawy. Co do zasady, procedura kontrolna została

określona w tym przepisie w sposób identyczny jak w art. 20ca ustawy o Policji, w art. 10ba ustawy o Straży Granicznej, w art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w art. 28a ustawy o ABW oraz AW i w art. 32a ustawy o SKW oraz SWW.

Wobec art. 18 ust. 1 w związku z art. 18a ustawy o CBA, podobnie jak w przypadku art. 28 ust. 1 w związku z art. 28a ustawy o ABW oraz AW i art. 32 ust. 1 w związku z art. 32a ustawy o SKW oraz SWW, Wnioskodawca sformułował, jak się wydaje, odmienne zarzuty i argumenty za jego niezgodnością z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także z art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, niż w odniesieniu do art. 20c ust. 1 w związku z art. 20ca ustawy o Policji, art. 10b ust. 1 w związku z art. 10ba ustawy o Straży Granicznej oraz art. 30 ust. 1 w związku z art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Wskazał bowiem, że konstytucyjną wadą zaskarżonej normy jest uniemożliwienie sądowi sprawowania rzeczywistej kontroli udostępniania funkcjonariuszom Centralnego Biura Antykorupcyjnego danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, wymienionych w art. 18 ust. 1 ustawy o CBA, **niezbędnych do realizacji zadań, o których mowa w art. 2 tej ustawy**, przy czym rozpoznawanie, zapobieganie i wykrywanie niektórych przestępstw (*vide* - art. 2 ust. 1 pkt 1 ustawy o CBA) jest tylko jednym z zadań wykonywanych przez funkcjonariuszy tego Biura.

Do wykonywanych przez funkcjonariuszy Centralnego Biura Antykorupcyjnego zadań innych niż rozpoznawanie, zapobieganie i wykrywanie przestępstw ustawa o CBA zalicza, między innymi, prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi (art. 2 ust. 1 pkt

6) czy podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 2 ust. 1 pkt 7).

W uzasadnieniu wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, Trybunał Konstytucyjny, kontrolując zgodność z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji art. 18 ust. 1 pkt 1 ustawy o CBA, który w chwili kontroli brzmiał:

„[o]bowiązek 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>>”

zwrócił uwagę na bardzo szeroki zakres zadań, w wypadku których funkcjonariusze CBA mogą mieć udostępnione dane telekomunikacyjne, i stwierdził, że *„[z]adania te (...) nie obejmują wyłącznie rozpoznawania i ścigania poważnych przestępstw oraz zapobiegania im, ale również wykonywanie innych zadań, w tym ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (art. 2 ust. 1 pkt 2 ustawy o CBA), dokumentowanie podstaw i inicjowanie realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych (art. 2 ust. 1 pkt 3 ustawy o CBA), czy wreszcie - prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi (art. 2 ust. 1 pkt 6 ustawy o CBA)”* oraz że, *„[m]ając na uwadze wyjątkowo szeroki zakres okoliczności, w jakich CBA może mieć udostępnione dane telekomunikacyjne, a zarazem jednoznaczne wyłączenie obowiązku uzyskania zgody sądu oraz brak obowiązku uzyskania zgody jakiegokolwiek niezależnego organu na ich pozyskanie, (...) zakwestionowany przepis nie*

zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia Konstytucji. Jest to wystarczające do orzeczenia o niezgodności art. 18 ust. 1 pkt 1 ustawy o CBA przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji” (op. cit.).

Wprawdzie w powołanym wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny badał konstytucyjność art. 18 ust. 1 (pkt 1) ustawy o CBA, którego treść, w chwili orzekania, nie obejmowała (tak jak obecnie) danych pocztowych oraz danych internetowych, jednak zawarte w uzasadnieniu tego wyroku uwagi Trybunału co do pozyskiwania przez funkcjonariuszy Centralnego Biura Antykorupcyjnego danych telekomunikacyjnych można odnieść także do pozyskiwania przez tych funkcjonariuszy pozostałych danych wymienionych w tym przepisie.

Biorąc pod uwagę tezy zawarte w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego oraz treść uzasadnienia wyroku TSUE z dnia 8 kwietnia 2014 r., należy stwierdzić, że przewidziany w art. 18a ustawy o CBA **mechanizm kontroli** nad uzyskiwaniem przez Centralne Biuro Antykorupcyjne danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, sprawowanej przez Sąd Okręgowy w Warszawie, z powodów, **o których była mowa w pkt III ppkt 1, 3, 5, 7 i 9 niniejszego stanowiska, stanowi dostateczną gwarancję należytej kontroli udostępniania tych danych.**

Podobnie bowiem jak w przypadku Policji, Straży Granicznej, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego kontrola dotyczy wprawdzie jedynie zbiorczych danych ujętych przez Szefa Centralnego Biura Antykorupcyjnego w formę sprawozdania, obejmującego liczbę przypadków pozyskania danych, ich rodzaj oraz kwalifikację prawną czynów, w związku z zaistnieniem których o dane te wystąpiono, **przekazywanego sądowi w okresach półrocznych, to jednak nie**

można zapominać o tym, iż, zgodnie z art. 18a ust. 3 ustawy o CBA, „sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych, pocztowych lub internetowych”.

Ta formuła oznacza to samo, co identyczne w swej treści sformułowania użyte w art. 20ca ust. 3 ustawy o Policji, art. 10ba ust. 3 ustawy o Straży Granicznej, art. 30b ust. 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ust. 3 ustawy o ABW oraz AW i 32a ust. 3 ustawy o SKW oraz SWW, a mianowicie, że kontrolujący sąd ma możliwość zapoznać się ze wszystkimi posiadanymi przez Szefa Centralnego Biura Antykorupcyjnego materiałami uzasadniającymi wnioski o udostępnienie danych, co jednocześnie oznacza, iż sąd może ocenić prawidłowość każdego wniosku o udostępnienie danych w kontekście przesłanek określonych w art. 18 ust. 1 ustawy o CBA. Jeżeli tego rodzaju kontrolę połączy się z kontrolą przypadków pozyskania danych, w oparciu o treść sprawozdania, o którym mowa w art. 18a ust. 2 ustawy o CBA, to można zasadnie stwierdzić, że kontroli Sądu Okręgowego w Warszawie podlegają wszystkie etapy przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych, począwszy od złożenia wniosku o ich udostępnienie, a skończywszy na przekazaniu uzyskanych danych mających znaczenie dla postępowania karnego prokuratorowi, ewentualnie ich zniszczeniu, jeżeli okaże się, że nie mają znaczenia dla postępowania karnego (art. 18 ust. 6 i 7 ustawy o CBA).

Podobnie też jak w przypadku Policji, Straży Granicznej, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego, ocena przez kontrolujący sąd prawidłowości wniosku Szefa Centralnego Biura Antykorupcyjnego o udostępnienie danych jest nie tylko dopuszczalna, ale też faktycznie możliwa. Niezbędne do przeprowadzenia takiej kontroli dane zawierają bowiem rejestry wystąpień o udostępnienie danych telekomunikacyjnych, pocztowych i internetowych, obligatoryjnie prowadzone przez Szefa CBA (*vide* - art. 18 ust. 5 ustawy o CBA).

Ponadto do Centralnego Biura Antykorupcyjnego mają odpowiednie zastosowanie uwagi zawarte w pkt III ppkt 1 niniejszego stanowiska odnoszące się do sposobu rozumienia określenia „niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu”, użytego w art. 18 ust. 7 ustawy o CBA.

Reasumując tę część rozważań, należy zatem stwierdzić, iż przewidziany w art. 18a ustawy o CBA mechanizm kontrolny umożliwia kompleksowe zweryfikowanie przez sąd prawidłowości działania Centralnego Biura Antykorupcyjnego w obszarze niejawnego pozyskiwania informacji o osobach, co jednocześnie oznacza, że **przepis ten realizuje, zawarty w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11, nakaz Trybunału Konstytucyjnego, aby ustawowe unormowania niejawnej kontroli wykluczały jej fasadowość.** Wszak Sądowi Okręgowemu w Warszawie umożliwiono dokonanie oceny celowości i subsydiarności czynności niejawnego pozyskiwania informacji o osobach, jak również sposobu ich uzyskania **w każdej indywidualnej sprawie względem każdego indywidualnego podmiotu.**

Wszystko to powoduje, że art. 18 ust. 1 w związku z art. 18a ustawy o CBA **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

12. Ocena zarzutu niezgodności art. 18b ust. 1 ustawy o CBA z art. 30, art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

Przepis art. 18b ustawy o CBA brzmi:

„Art. 18b. 1. W celu realizacji zadań, o których mowa w art. 2, CBA może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne,
- 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
- 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 18 ust. 2-7 stosuje się.”.

Oceniany przepis, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28b ustawy o ABW oraz AW i art. 32b ust. 1 ustawy o SKW oraz SWW, poprzez odwołanie do wykazu, o którym mowa w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, umożliwia funkcjonariuszom CBA uzyskiwanie danych przekazywanych przez użytkownika przy zawieraniu umowy na usługi telekomunikacyjne (ust. 1 pkt 1).

Z kolei, poprzez odwołanie do art. 161 ustawy - Prawo telekomunikacyjne, art. 18b ust. 1 ustawy o CBA umożliwia funkcjonariuszom tej służby uzyskiwanie, w celach w nim określonych, tzw. danych abonamentowych oraz danych przekazanych operatorowi przez użytkownika będącego osobą fizyczną za jego zgodą, o ile dane te pozostają w związku ze świadczoną usługą (ust. 1 pkt 2).

Ponadto, w przypadku użytkownika, który nie jest osobą fizyczną, funkcjonariusze Centralnego Biura Antykorupcyjnego, w celach określonych w art. 18b ust. 1 ustawy o CBA, będą mogli uzyskiwać numer zakończenia sieci

oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, a w przypadku stacjonarnej publicznej sieci telekomunikacyjnej - także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi (ust. 1 pkt 3 i 4).

Należy stwierdzić, iż pomiędzy zarzutami Wnioskodawcy sformułowanymi pod adresem analizowanego przepisu ustawy o CBA a zarzutami sformułowanymi pod adresem art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28b ust. 1 ustawy o ABW oraz AW i art. 32b ust. 1 ustawy o SKW oraz SWW zachodzi podobieństwo.

Wnioskodawca wskazał też identyczne wzorce kontroli.

O ile jednak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej oraz art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych zarzut braku jakiegokolwiek niezależnej kontroli uzyskiwania przez wskazane w tych przepisach służby powołane do ochrony porządku publicznego wymienionych tamże danych Wnioskodawca połączył z zarzutem nadmiernie szerokiego, w Jego ocenie, katalogu przestępstw i przestępstw skarbowych, w odniesieniu do których dopuszczalne jest uzyskiwanie i przetwarzanie przez te służby danych, o tyle, w przypadku art. 18b ust. 1 ustawy o CBA, podobnie jak w przypadku art. 18 ust. 1 tej ustawy, Wnioskodawca zarzut braku jakiegokolwiek niezależnej kontroli uzyskiwania danych łączy z zarzutem braku precyzyjnego określenia w ustawie przedmiotowego zakresu, w jakim w omawianej sferze mogą być realizowane działania Centralnego Biura Antykorupcyjnego w związku z przewidzianym w art. 18b ust. 1 ustawy o CBA ogólnym odesłaniem do przepisu tejże ustawy (art. 2), który zawiera szeroki katalog zadań wykonywanych przez CBA.

Tym niemniej oceny i wnioski przedstawione w pkt III ppkt 2, 4, 6, 8 i 10 niniejszego stanowiska pozostają aktualne także w odniesieniu do art. 18b ust. 1

ustawy o CBA, co jednocześnie oznacza, że konstytucyjność tego przepisu, podobnie jak w przypadku art. 20cb ust. 1 ustawy o Policji, art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28b ust. 1 ustawy o ABW oraz AW i art. 32b ust. 1 ustawy o SKW oraz SWW, **determinuje zakres** uzyskiwanych przez Centralne Biuro Antykorupcyjne, a określonych w tym przepisie danych, jak również **zasady przekazywania tych danych operatorowi telekomunikacyjnemu przez użytkownika**.

Podobnie bowiem jak w - odpowiadających w tym przypadku treściowo i wzajemnie porównywanych - przepisach art. 20c ust. 1 pkt 1 i art. 20cb ust. 1 ustawy o Policji, art. 10b ust. 1 pkt 1 i art. 10bb ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 pkt 1 i art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 i art. 28b ust. 1 ustawy o ABW oraz AW, a także art. 32 ust. 1 pkt 1 i art. 32b ust. 1 ustawy o SKW oraz SWW, określony w art. 18 ust. 1 pkt 1 ustawy o CBA zakres danych telekomunikacyjnych jest znacznie szerszy od zakresu danych telekomunikacyjnych wymienionych w art. 18b ust. 1 ustawy o CBA, co, w konsekwencji, prowadzi do wniosku, że dane z art. 18 ust. 1 pkt 1 ustawy o CBA **zawierają nieporównanie więcej informacji o osobie** niż dane, o których mowa w art. 18b ust. 1 ustawy o CBA.

O ile w oparciu o art. 18 ust. 1 pkt 1 ustawy o CBA możliwe jest pozyskiwanie takich danych jak: dane o abonencie, dane o ruchu (tzw. dane bilingowe), a także dane o lokalizacji (*vide* - uzasadnienie wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11), o tyle w oparciu o art. 18b ust. 1 ustawy o CBA możliwe jest pozyskanie wyłącznie danych dotyczących abonamentu oraz abonenta.

W przedstawionych warunkach, o ile w przypadku pozyskiwania danych na podstawie art. 18 ust. 1 pkt 1 ustawy o CBA zachodzi konieczność zapewnienia odpowiednich gwarancji proceduralnych (i tego rodzaju gwarancje, co wcześniej

wykazano, zostały przewidziane w art. 18a ustawy o CBA), o tyle w przypadku pozyskiwania danych na podstawie art. 18b ust. 1 ustawy o CBA **konieczność taka nie zachodzi**.

Należy bowiem zauważyć, iż, tak jak dane z art. 20cb ust. 1 ustawy o Policji, dane z art. 10bb ust. 1 ustawy o Straży Granicznej, dane z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, dane z art. 28b ust. 1 ustawy o ABW oraz AW, jak również dane z art. 32b ust. 1 ustawy o SKW oraz SWW, niektóre dane, określone w art. 18b ust. 1 ustawy o CBA, przedsiębiorca telekomunikacyjny uzyskuje bezpośrednio od (przyszłego) abonenta **dobrowolnie**, jako że dane te stanowią niezbędne elementy umowy na wykonywanie konkretnej usługi telekomunikacyjnej.

Z kolei pozostałe dane to dane gromadzone przez przedsiębiorcę telekomunikacyjnego także **za zgodą** abonenta i są to dane, bez których wykonywanie konkretnej (przewidzianej w umowie) usługi telekomunikacyjnej w ogóle nie byłoby możliwe.

W tej sytuacji, podobnie jak w przypadku danych z art. 20cb ust. 1 ustawy o Policji, z art. 10bb ustawy o Straży Granicznej, z art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, z art. 28b ust. 1 ustawy o ABW oraz AW, jak również z art. 32b ust. 1 ustawy o SKW oraz SWW, można zasadnie stwierdzić, że każdy abonent usługi telekomunikacyjnej, który z przedsiębiorcą telekomunikacyjnym zawarł umowę na wykonywanie tej usługi, ma świadomość, że dane o nim, które sam dobrowolnie przekazał, mogą być przez tego przedsiębiorcę przetwarzane w ramach świadczonej usługi, co jednocześnie oznacza, iż przewidziana w art. 18b ust. 1 ustawy o CBA ingerencja w prawa i wolności jednostki zadekretowane w art. 47, art. 49 i art. 51 ust. 2 Konstytucji nie jest na tyle głęboka (poważna), aby wymagała gwarancji proceduralnych, i to w postaci kontroli procedury uzyskiwania danych sprawowanej przez niezależny organ.

Przy tym, podobnie jak ograniczenie konstytucyjnych praw i wolności jednostki wprowadzone w art. 20cb ust. 1 ustawy o Policji, w art. 10bb ust. 1 ustawy o Straży Granicznej, w art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w art. 28b ust. 1 ustawy o ABW oraz AW, a także w art. 32b ust. 1 ustawy o SKW oraz SWW, tego samego rodzaju ograniczenie wprowadzone w art. 18b ust. 1 ustawy o CBA jest usprawiedliwione koniecznością zapewnienia bezpieczeństwa i porządku publicznego, która stanowi jedną z wartości wymienionych w art. 31 ust. 3 Konstytucji.

Reasumując, art. 18b ustawy o CBA **jest zgodny** z art. 47, art. 49 i art. 51 ust. 2 w związku z art. 31 ust. 3 oraz z art. 30 Konstytucji, a także **jest zgodny** z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

IV. Zarzut niezgodności art. 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji, art. 10b ust. 3 w związku z art. 10b ust. 2 ustawy o Straży Granicznej, art. 30 ust. 3 w związku z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 3 w związku z art. 28 ust. 2 ustawy o ABW oraz AW, art. 32 ust. 5 w związku z art. 32 ust. 2 ustawy o SKW oraz SWW i art. 18 ust. 3 w związku z art. 18 ust. 2 ustawy o CBA z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji (pkt IV *petitum* wniosku Rzecznika Praw Obywatelskich).

Zakwestionowane przepisy, których treść jest podobna, regulują problematykę udostępniania nieodpłatnie przez przedsiębiorcę telekomunikacyjnego, operatora pocztowego oraz usługodawcę świadczącego usługi drogą elektroniczną danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, o których mowa w art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 30 ust. 1 ustawy o Żandarmerii

Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o ABW oraz AW, art. 32 ust. 1 ustawy o SKW oraz SWW i art. 18 ust. 1 ustawy o CBA:

1) w ustawie o Policji:

- a) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej,
- b) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w ppkt a,
- c) za pośrednictwem sieci telekomunikacyjnej - policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w ppkt a;

2) w ustawie o Straży Granicznej:

- a) funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
- b) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w ppkt a,
- c) za pośrednictwem sieci telekomunikacyjnej - funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w ppkt a;

3) w ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych:

- a) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej,
- b) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w ppkt a,
- c) za pośrednictwem sieci telekomunikacyjnej - żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w ppkt a;

5) w ustawie o ABW oraz AW:

- a) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ,
 - b) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW,
 - c) za pośrednictwem sieci telekomunikacyjnej - funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w ppkt b;
- 6) w ustawie o SKW oraz SWW:
- a) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej,
 - b) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW,
 - c) za pośrednictwem sieci telekomunikacyjnej - funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW;
- 7) w ustawie o CBA:
- a) na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej,
 - b) na ustne żądanie funkcjonariusza CBA, posiadającego pisemne upoważnienie Szefa CBA lub osoby przez niego upoważnionej,
 - c) za pośrednictwem sieci telekomunikacyjnej - funkcjonariuszowi CBA posiadającemu pisemne upoważnienie osób, o których mowa w ppkt a,
- jak również regulują** warunki, w jakich odbywa się udostępnianie tych danych za pośrednictwem sieci telekomunikacyjnej (bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego oraz usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy, odpowiednio, Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Komendantem Głównym Żandarmerii Wojskowej, Szefem ABW, Szefem SKW oraz Szefem CBA a tym podmiotem.

Ponieważ przepisy zaskarżone w tej części wniosku Rzecznika Praw Obywatelskich są zbieżne treściowo, wystarczające będzie przytoczenie art. 20c ust. 2 i 3 ustawy o Policji, które mają następujące brzmienie:

„2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1 (dane telekomunikacyjne, dane pocztowe oraz dane internetowe - przyp. wł.):

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

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.”.

Zdaniem Rzecznika, przepisy art. 20c ust. 2 i 3 ustawy o Policji (i odpowiadające im treściowo przepisy: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA) mogą prowadzić do ingerencji w zasadę swobody działalności gospodarczej, wyrażoną w art. 20 Konstytucji, dlatego że nie określają „przesłanek zawarcia porozumienia, co może oznaczać w praktyce ograniczenie swobody przedsiębiorcy co do odmowy zawarcia porozumienia” (uzasadnienie wniosku, s. 45), jak również przez to, że ograniczają przedsiębiorcy możliwość podejmowania działań faktycznych i prawnych, mieszczących się w ramach prowadzonej działalności gospodarczej, „wyraźnie” wskazując, że udostępnianie danych odbywa się nieodpłatnie.

Wynikająca z art. 20 (oraz z art. 22) Konstytucji zasada wolności działalności gospodarczej stanowiła przedmiot licznych wypowiedzi Trybunału Konstytucyjnego.

W uzasadnieniu powołanego także przez Rzecznika wyroku z dnia 21 kwietnia 2004 r., w sprawie o sygn. akt K 33/03, Trybunał stwierdził, iż „[w] odniesieniu do zasady wolności gospodarczej, wynikającej z art. 20 i 22 Konstytucji, Trybunał Konstytucyjny wielokrotnie wyrażał pogląd, że obejmuje ona wolność wyboru działalności gospodarczej oraz wolność jej wykonywania. Jak stwierdzono w wyroku z 10 kwietnia 2001 r., U 7/00 (OTK ZU nr 3/2001, poz. 56) <art. 22 konstytucji pełni dwojaką funkcję. Z jednej strony traktować go należy jako wyrażenie jednej z zasad ustroju gospodarczego Rzeczypospolitej (i w tym zakresie stanowi on konkretyzację ogólniejszych zasad, wyrażonych w art. 20), z drugiej strony - może on stanowić podstawę do konstruowania prawa podmiotowego, przysługującego każdemu, kto podejmuje działalność gospodarczą>. (...)

Z przepisów Konstytucji i ugruntowanego orzecznictwa Trybunału Konstytucyjnego wynika, że wolność działalności gospodarczej nie ma charakteru absolutnego i może zostać w pewnych sytuacjach ograniczona, co może jednakże nastąpić wyłącznie w formie ustawowej i tylko ze względu na ważny interes publiczny (podkr. wł.). Jednocześnie <ustawodawca nie może ustanawiać ograniczeń przekraczających pewien stopień uciążliwości, a zwłaszcza zapoznających proporcje pomiędzy stopniem naruszenia uprawnień jednostki a rangą interesu publicznego, który ma w ten sposób podlegać ochronie> (orzeczenie z 26 kwietnia 1995 r., K. 11/94, OTK w 1995 r., cz. I, poz. 12). Ponadto Trybunał Konstytucyjny wskazał na <konieczność uwzględnienia przy ograniczaniu praw jednostki zasady wymagającej odpowiedniego wyważenia wagi interesu publicznego, któremu służy ograniczenie danego prawa i wagi interesów naruszonych przez takie ograniczenie> (wyrok z 26 kwietnia 1999 r., K. 33/98, OTK ZU nr 4/1999, poz. 71). Wcześniej, w orzeczeniu z 9

sierpnia 1998 r., K. 28/97, OTK ZU nr 4/1998, poz. 50) Trybunał Konstytucyjny stwierdził, iż *<wymóg konieczności jest spełniony, jeżeli ustanowione ograniczenia są zgodne z zasadą proporcjonalności>*, to znaczy, że:

- <1) środki zastosowane przez prawodawcę muszą być w stanie doprowadzić do zamierzonych celów,*
- 2) muszą być one niezbędne do ochrony interesu, z którym są powiązane,*
- 3) ich efekty muszą pozostawać w proporcji do ciężarów nakładanych na obywatela>*” (OTK ZU seria A nr 4/2004, poz. 31).

Już na wstępie trzeba zwrócić uwagę, że przepisów zaskarżonych w tej części wniosku RPO nie można rozpatrywać, tak jak czyni to Wnioskodawca, wyłącznie w oparciu o ich treść zawartą w poszczególnych ustawach regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego, ale w ich otoczeniu normatywnym, do którego zaliczają się odpowiednie przepisy ustawy - Prawo telekomunikacyjne, ustawy - Prawo pocztowe oraz ustawy o świadczeniu usług drogą elektroniczną. Wszak „porozumienia”, o których mowa w art. 20c ust. 3 ustawy o Policji (i w odpowiadających temu przepisowi regulacjach przewidzianych w ustawie o Straży Granicznej, ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawie o ABW oraz AW, ustawie o SKW oraz SWW i ustawie o CBA), zawierane są pomiędzy odpowiednim organem danej Służby a **przedsiębiorcami** telekomunikacyjnymi, **operatorami** pocztowymi oraz **usługodawcami** świadczącymi usługi drogą elektroniczną, którzy prowadzą tego rodzaju działalność na zasadach określonych w, odpowiednio, ustawie - Prawo telekomunikacyjne, ustawie - Prawo pocztowe oraz ustawie o świadczeniu usług drogą elektroniczną.

Już w przepisach ogólnych wspomnianych ustaw wskazuje się, że określają one, między innymi:

- prawa i obowiązki przedsiębiorców telekomunikacyjnych (art. 1 pkt 2 ustawy - Prawo telekomunikacyjne),
- zasady wykonywania działalności gospodarczej polegającej na świadczeniu usług pocztowych w obrocie krajowym lub zagranicznym (art. 1 ustawy - Prawo pocztowe),
- obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną (art. 1 pkt 1 ustawy o świadczeniu usług drogą elektroniczną).

Jednym z zadekretowanych w przepisach powołanych ustaw **obowiązków** nałożonych na podmioty wykonujące uregulowaną w nich działalność gospodarczą jest wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (*vide* - art. 176 ustawy - Prawo telekomunikacyjne, art. 81 ustawy - Prawo pocztowe i art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną).

Zakres i sposób wykonywania tych obowiązków określają:

- 1) art. 176a - 182 ustawy - Prawo telekomunikacyjne oraz przepisy aktów wykonawczych wydanych na podstawie art. 176a ust. 5, art. 177 ust. 6, art. 180a ust. 4, art. 180c ust. 2, art. 180f ust. 3 i art. 182 tej ustawy,
- 2) art. 81-86 ustawy - Prawo pocztowe oraz przepisy aktów wykonawczych wydanych na podstawie art. 82 ust. 3, art. 83 ust. 4, art. 85 ust. 4 i art. 86 ust. 3 tej ustawy,
- 3) art. 18 ustawy o świadczeniu usług drogą elektroniczną.

W szczególności, przepisy art. 179 ust. 3-4b ustawy - Prawo telekomunikacyjne brzmią:

„3. Przedsiębiorca telekomunikacyjny, z zastrzeżeniem ust. 12 pkt 2, jest obowiązany do:

- 1) zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, zwanych dalej <warunkami dostępu i utrwalania>, umożliwiających jednocześnie i wzajemnie niezależne:

a) uzyskiwanie przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową, zwane dalej <uprawnionymi podmiotami>, w sposób określony w ust. 4b, dostępu do:

- przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe,
- posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi, o których mowa w ust. 9, art. 159 ust. 1 pkt 1 i pkt 3-5,

b) uzyskiwanie przez uprawnione podmioty danych związanych ze świadczoną usługą telekomunikacyjną i danych, o których mowa w art. 161,

c) utrwalanie przez uprawnione podmioty przekazów telekomunikacyjnych i danych, o których mowa w lit. a i b;

2) utrwalania na rzecz sądu i prokuratora przekazów telekomunikacyjnych i danych, o których mowa w pkt 1 lit. a i b.

3a. Przedsiębiorca telekomunikacyjny zapewnia, na własny koszt, warunki dostępu i utrwalania w zakresie wszystkich świadczonych usług telekomunikacyjnych, począwszy od dnia rozpoczęcia działalności telekomunikacyjnej, a w przypadku rozpoczęcia świadczenia nowej usługi telekomunikacyjnej od dnia jej uruchomienia.

3b. Przedsiębiorca telekomunikacyjny zapewnia, na własny koszt, utrwalanie na rzecz sądu lub prokuratora przekazów telekomunikacyjnych i danych, o których mowa w ust. 3 pkt 1 lit. a i b.

4. Przedsiębiorca telekomunikacyjny zapewnia warunki dostępu i utrwalania z zachowaniem wymagań określonych w rozporządzeniu, o którym mowa w ust. 12.

4a. Warunki dostępu i utrwalania mogą być zapewniane za pomocą interfejsów zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy telekomunikacyjnego na zasadach określonych w umowach zawartych przez uprawnione podmioty z przedsiębiorcą telekomunikacyjnym.

Umowa może określać współdział stron w kosztach zastosowania interfejsów. W przypadku braku uzgodnień w zakresie lokalizacji interfejsu uprawnione podmioty wskazują miejsce lokalizacji pozostające w obrębie sieci telekomunikacyjnej przedsiębiorcy telekomunikacyjnego, umożliwiające: techniczną realizację interfejsu, niezbędną ochronę tego miejsca wynikającą z przepisów odrębnych oraz minimalizację nakładów ponoszonych przez przedsiębiorcę telekomunikacyjnego i podmioty uprawnione.

4b. Zapewnienie warunków dostępu i utrwalania powinno umożliwiać uprawnionym podmiotom dostęp do przekazów telekomunikacyjnych i danych bez udziału pracowników przedsiębiorcy telekomunikacyjnego. Za zgodą uprawnionego podmiotu warunki dostępu i utrwalania mogą być zapewnione przy niezbędnym współdziale upoważnionych pracowników przedsiębiorcy telekomunikacyjnego gwarantujących prawidłową realizację przedmiotowych czynności w zakresie określonym przez uprawniony podmiot.”.

Art. 82 ust. 1 ustawy - Prawo pocztowe był już cytowany wcześniej, niemniej warto przypomnieć zdanie wstępne tego przepisu, które brzmi:

„1. Operator pocztowy, poczynszy od dnia rozpoczęcia działalności pocztowej, jest obowiązany do nieodpłatnego zapewnienia, w ramach wykonywanej przez siebie działalności pocztowej, technicznych i organizacyjnych możliwości wykonywania przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową, zwane dalej <uprawnionymi podmiotami>, oraz prokuraturę i sądy, ich zadań określonych odrębnymi przepisami, wymagających: (...)”.

Natomiast przepis art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną (ust. 1-5 tego przepisu cytowano wcześniej, *vide* - s. 85-86 niniejszego stanowiska) ma następujące brzmienie:

„6. Usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań.”.

Biorąc pod uwagę treść zaskarżonych w tym punkcie *petitum* wniosku Rzecznika Praw Obywatelskich przepisów ustawy o Policji oraz odpowiadających im treściowo przepisów pozostałych ustaw w ich otoczeniu normatywnym, należy stwierdzić, że ograniczenia zasady swobody działalności gospodarczej „ze względu na ważny interes publiczny” (*vide* - cytowany wcześniej wyrok Trybunału Konstytucyjnego w sprawie o sygn. akt K 33/03) polegające, między innymi, na obowiązku nieodpłatnego udostępniania danych, jest dostatecznie uzasadnione koniecznością wykonywania zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Wspomniane ograniczenia zasady swobody działalności gospodarczej spełniają zatem kryterium konieczności z art. 31 ust. 3 Konstytucji.

Jednocześnie Wnioskodawca nie zarzuca nierespektowania przez zaskarżone przepisy wymogu zachowania proporcjonalności ograniczenia zasady swobody działalności gospodarczej (kwestionuje sam fakt wprowadzenie takiego ograniczenia), w związku z tym przeprowadzenie testu proporcjonalności jest w tym przypadku bezprzedmiotowe.

Z kolei wspomniane w art. 20c ust. 3 ustawy o Policji (i w odpowiadających im treściowo przepisach: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA) „porozumienie”, **które może, ale nie musi zostać zawarte** pomiędzy odpowiednim organem konkretnej Służby a przedsiębiorcą telekomunikacyjnym, operatorem pocztowym albo usługodawcą świadczącym usługi drogą elektroniczną, dotyczy jedynie kwestii „organizacyjno-technicznych”, to jest sposobu realizacji przez tego przedsiębiorcę, operatora czy usługodawcę obowiązku przekazywania danych,

nie zaś samego obowiązku ich przekazywania. Oznacza to, że brak zgody przedsiębiorcy telekomunikacyjnego, operatora pocztowego czy usługodawcy świadczącego usługi drogą elektroniczną na zawarcie takiego porozumienia (brak zainteresowania zawarciem porozumienia) nie uchyla ciążącego na tym podmiocie (z mocy ustawy) obowiązku przekazywania danych, o których mowa w art. 20c ustawy o Policji (i w odpowiadających im treściowo przepisach wyżej wymienionych ustaw).

Z drugiej strony, brak zgody na zawarcie wspomnianego porozumienia nie rodzi po stronie przedsiębiorcy telekomunikacyjnego, operatora pocztowego czy usługodawcy świadczącego usługi drogą elektroniczną żadnych konsekwencji w sferze gwarantowanej im konstytucyjnie swobody działalności gospodarczej. Pomimo braku takiego porozumienia dalej bowiem podmioty te muszą wykonywać, ingerując w tę swobodę, obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, choć w tej sytuacji już w inny sposób i na innych warunkach niż te, które mogłyby zostać objęte porozumieniem (wynegocjowane).

Drugi zarzut Wnioskodawcy, sformułowany pod adresem zaskarżonych w tej grupie przepisów, związany jest z faktem utrzymywania stałej infrastruktury prowadzącej do permanentnego zbierania danych telekomunikacyjnych, danych pocztowych i danych internetowych.

Zdaniem Wnioskodawcy, „[p]rzepisy pozwalające na nieograniczone zbieranie danych internetowych, bez następczego informowania osoby, których zbierane dane dotyczyły, stanowią naruszenie tak fundamentalnych zasad, jak zasada demokratycznego państwa prawnego, godność człowieka i wynikające z niej prawo do prywatności, wolność i ochrona tajemnicy komunikowania się czy w końcu ochrona informacji o sobie” (uzasadnienie wniosku, s. 45).

Problem jednak w tym, że art. 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji (i odpowiadające im treściowo przepisy: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy

o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA) *per se* nie stanowią podstawy do pobierania z wykorzystaniem owej stałej infrastruktury konkretnych danych przez funkcjonariuszy służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego.

Wspomniane przepisy, o czym wcześniej była mowa, mają bowiem charakter organizacyjno-techniczny, wskazując tylko sposoby, w jakich przez przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną **może, ale wcale nie musi być** wykonywany obowiązek (ustawowy) realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Natomiast przesłanki, jakie muszą zostać spełnione do tego, aby funkcjonariusze odpowiednich Służb z wykorzystaniem owej stałej infrastruktury mogli sięgnąć po konkretne dane telekomunikacyjne, dane pocztowe oraz dane internetowe, zawarte zostały w art. 20c ust. 1 ustawy o Policji (i odpowiadających im treściowo przepisach: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA) **i w tym zakresie (niewystarczające przesłanki uzyskiwania danych oraz brak realnej kontroli ich uzyskiwania) przepisy te stanowią przedmiot zarzutu Rzecznika Praw Obywatelskich w pkt III i V wniosku.**

Z kolei brak obowiązku informacyjnego wobec osób, których dane były pozyskiwane w oparciu o przepis art. 20c ust. 1 ustawy o Policji (i odpowiadające im treściowo przepisy: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA) **stanowi przedmiot zarzutu Rzecznika Praw Obywatelskich w pkt VI wniosku.**

Przepisy rozpatrywane obecnie stwarzają, co Wnioskodawca wszak sam przyznaje, **jedynie potencjalną możliwość dostępu** funkcjonariuszy służb

powołanych do ochrony bezpieczeństwa państwa i porządku publicznego do systemów, w których przetwarzane są dane podlegające przekazywaniu poszczególnym tym służbom.

Jednocześnie trzeba pamiętać, że podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące są obowiązane do zachowania tajemnicy telekomunikacyjnej (szerzej o tajemnicy telekomunikacyjnej była mowa wcześniej) oraz do zachowania należytej staranności, w zakresie uzasadnionym względami technicznymi lub ekonomicznymi, przy zabezpieczaniu urządzeń telekomunikacyjnych, sieci telekomunikacyjnych oraz zbiorów danych przed ujawnieniem tajemnicy telekomunikacyjnej (*vide* - art. 160 ust. 1 i 2 ustawy - Prawo telekomunikacyjne).

K. Kawałek wskazuje, że „[p]rzepis art. 160 określa krąg podmiotów zobowiązanych do zachowania tajemnicy telekomunikacyjnej. W przepisie ust. 1 obowiązek ten nakłada na podmioty uczestniczące w działalności telekomunikacyjnej, którą to działalnością, zgodnie z art. 1 ust. 1 pkt 1, jest świadczenie usług telekomunikacyjnych, dostarczanie sieci telekomunikacyjnych lub udogodnień towarzyszących. Obowiązek zachowania tajemnicy telekomunikacyjnej dotyczy tylko podmiotów wykonujących działalność telekomunikacyjną w sieciach publicznych. Tym samym wyłączone zostały spod regulacji art. 160 podmioty określone w art. 4. Obowiązek zachowania tajemnicy telekomunikacyjnej dotyczy również podmiotów współpracujących z podmiotami uczestniczącymi w wykonywaniu działalności telekomunikacyjnej. Ustawa nie zawiera bliższego określenia tych podmiotów i tym samym należy przyjąć, że będą to podmioty, bez względu na przedmiot współpracy oraz stosunek prawny łączący je z podmiotem wykonującym działalność telekomunikacyjną” oraz że „[p]rzepis ust. 2 nakłada na podmioty uczestniczące w wykonywaniu działalności telekomunikacyjnej i podmioty z nimi współpracujące obowiązek zachowania należytej staranności przy zabezpieczaniu

urządzeń telekomunikacyjnych, zdefiniowanych w art. 2 pkt 46, sieci telekomunikacyjnych, których definicje zawiera art. 2 pkt 35 oraz zbiorów danych przed ujawnieniem tajemnicy telekomunikacyjnej. Wydaje się, że obowiązek nałożony w ust. 2 stanowi środek służący realizacji obowiązku określonego w ust. 1. Przepis art. 160 ust. 2 nie zawiera określenia co należy rozumieć przez należytą staranność. Celowe wydaje się sięgnięcie do regulacji zamieszczonej w kodeksie cywilnym, dotyczącej wykonania zobowiązania, przy uwzględnieniu, że działalność telekomunikacyjna wykonywana jest przez podmioty jako działalność gospodarcza. Tym samym, zgodnie z art. 355 § 2 k.c., należytą staranność należy określać przy uwzględnieniu zawodowego charakteru tej działalności. Jest to tym samym podwyższona staranność” (K. Kawałek, *Komentarz do art. 160 ustawy - Prawo telekomunikacyjne*, http://lex/lex/content.rpc?reqId=1490009608666_745892779).

Podobne zasady stosuje się przy przetwarzaniu danych pocztowych i danych internetowych.

Przepisy art. 41 i art. 42 ustawy - Prawo pocztowe brzmią:

„Art. 41. 1. Tajemnica pocztowa obejmuje informacje przekazywane w przesyłkach pocztowych, informacje dotyczące realizowania przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Do zachowania tajemnicy pocztowej są obowiązani:

- 1) operator pocztowy;
- 2) osoby, które z racji wykonywanej działalności mają dostęp do tajemnicy pocztowej.

3. Naruszeniem obowiązku zachowania tajemnicy pocztowej jest w szczególności:

- 1) ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową;

- 2) otwieranie zamkniętych przesyłek pocztowych lub zapoznawanie się z ich treścią;
- 3) umożliwianie osobom nieuprawnionym podejmowania działań mających na celu wykonywanie czynności, o których mowa w pkt 1 i 2.
4. Nie stanowi naruszenia obowiązku zachowania tajemnicy pocztowej:
 - 1) podejmowanie działań, o których mowa w ust. 3 pkt 1 i 2, w przypadkach przewidzianych przepisami prawa lub w umowie o świadczenie usługi pocztowej;
 - 2) posługiwanie się przez operatora pocztowego referencjami obejmującymi dane dotyczące podmiotów korzystających z jego usług pocztowych oraz rodzajów tych usług, w przypadku gdy dane te są publikowane za zgodą podmiotów, których one dotyczą.
5. Obowiązek zachowania tajemnicy pocztowej jest nieograniczony w czasie.
6. Operator pocztowy jest obowiązany do zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi przy zabezpieczaniu urządzeń i obiektów wykorzystywanych przy świadczeniu usług pocztowych oraz zbiorów danych przed ujawnieniem tajemnicy pocztowej.

Art. 42. Informacje lub dane objęte tajemnicą pocztową mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te dotyczą świadczonej usługi pocztowej albo są niezbędne do jej wykonania lub jeżeli przepisy odrębne stanowią inaczej.”.

Z kolei art. 16 ustawy o świadczeniu usług drogą elektroniczną ma następujące brzmienie:

„Art. 16. 1. Do przetwarzania danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), w związku ze świadczeniem usług drogą elektroniczną, stosuje się przepisy tej ustawy, o ile przepisy niniejszego rozdziału nie stanowią inaczej.

2. Dane osobowe podlegają ochronie przewidzianej w niniejszym rozdziale w zakresie ich przetwarzania niezależnie od tego, czy jest ono dokonywane w zbiorach danych.”.

Reasumując tę część rozważań, należy stwierdzić, że art. 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji, art. 10b ust. 3 w związku z art. 10b ust. 2 ustawy o Straży Granicznej, art. 30 ust. 3 w związku z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 3 w związku z art. 28 ust. 2 ustawy o ABW oraz AW, art. 32 ust. 5 w związku z art. 32 ust. 2 ustawy o SKW oraz SWW i art. 18 ust. 3 w związku z art. 18 ust. 2 ustawy o CBA wprowadzie ingerują w zasadę swobody działalności gospodarczej przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną, ale czynią to na podstawie zawartego pomiędzy tymi podmiotami a państwem porozumienia, którego warunki precyzuje ustawa, zaś wprowadzone ograniczenia w swobodzie działalności gospodarczej są uzasadnione ważnym interesem publicznym (względ na obronność, bezpieczeństwo państwa oraz bezpieczeństwo i porządek publiczny), co powoduje, że zaskarżone przepisy są zgodne z art. 20 w związku z art. 31 ust. 3 Konstytucji.

Odnosnie natomiast do art. 2, art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, to - w odniesieniu do zaskarżonych przepisów - nie są one adekwatnymi wzorcami kontroli.

Zaskarżony w tej części wniosku Rzecznika art. 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji i odpowiadające im treściowo przepisy: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA nie stanowią bowiem normatywnej podstawy do uzyskiwania przez Policję i pozostałe uprawnione podmioty konkretnych danych telekomunikacyjnych,

pocztowych czy internetowych. Wyrażają jedynie normę o charakterze technicznym adresowaną do przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną.

Trzeba też pamiętać, iż w innych częściach wniosku (*vide* - pkt III, V i VI *petitum* i uzasadnienia) Rzecznik sformułował zarzuty identyczne jak w pkt IV *petitum* i uzasadnienia wniosku, tyle że pod adresem art. 20c *in toto* ustawy o Policji i odpowiadających jemu treściowo przepisów: ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o ABW oraz AW, ustawy o SKW oraz SWW i ustawy o CBA.

Reasumując tę część rozważań należy stwierdzić, że art. 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji, art. 10b ust. 3 w związku z art. 10b ust. 2 ustawy o Straży Granicznej, art. 30 ust. 3 w związku z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 3 w związku z art. 28 ust. 2 ustawy o ABW oraz AW, art. 32 ust. 5 w związku z art. 32 ust. 2 ustawy o SKW oraz SWW i art. 18 ust. 3 w związku z art. 18 ust. 2 ustawy o CBA nie są niezgodne z art. 2, art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

W tym miejscu jedynie na marginesie należy odnieść się do sformułowanej w końcowym fragmencie omówienia zarzutu z punktu IV *petitum* wniosku oceny Rzecznika, która bezpośrednio nie odnosi się do zaskarżonych w tej grupie przepisów, iż „obowiązki nałożone na przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną, będą w praktyce dotyczyć wyłącznie przedsiębiorców mających siedzibę na terenie Rzeczypospolitej Polskiej (art. 3 ustawy o świadczeniu usług drogą elektroniczną)”, co, w ocenie Rzecznika, „pozwala na stwierdzenie, że taka regulacja może prowadzić do sytuacji, w której niemożliwe będzie w ogóle sięgnięcie po dane posiadane przez przedsiębiorców

z siedzibą poza terytorium RP lub będzie się odbywać w ogóle bez żadnej podstawy prawnej”.

Przedstawiona wyżej ocena Rzecznika nie jest trafna.

Przepis art. 3 ustawy o świadczeniu usług drogą elektroniczną brzmi:

„Przepisów ustawy nie stosuje się do:

- 1) rozpowszechniania lub rozprowadzania programów radiowych lub programów telewizyjnych i związanych z nimi przekazów tekstowych w rozumieniu ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji (Dz. U. z 2016 r. poz. 639, 929 i 2260), z wyłączeniem programów rozpowszechnianych wyłącznie w systemie teleinformatycznym;
- 2) używania poczty elektronicznej lub innego równorzędnego środka komunikacji elektronicznej między osobami fizycznymi, w celach osobistych niezwiązanych z prowadzoną przez te osoby, chociażby ubocznie, działalnością zarobkową lub wykonywanym przez nie zawodem;
- 3) świadczenia przez przedsiębiorcę telekomunikacyjnego usług telekomunikacyjnych, z wyłączeniem art. 12-15;
- 4) (uchylony);
- 5) (uchylony);
- 6) świadczenia usług drogą elektroniczną, jeżeli odbywa się ono w ramach struktury organizacyjnej usługodawcy, przy czym usługa świadczona drogą elektroniczną służy wyłącznie do kierowania pracą lub procesami gospodarczymi tego podmiotu.”.

Należy zauważyć, iż powołany przepis art. 3 ustawy o świadczeniu usług drogą elektroniczną zawiera listę czynności, **a nie podmiotów**, w odniesieniu do których ustawa o świadczeniu usług drogą elektroniczną nie znajduje w całości zastosowania.

Prawdopodobnie Wnioskodawca opinie, że obowiązki nałożone na przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną będą w praktyce

dotyczyć wyłącznie przedsiębiorców mających siedzibę na terenie Rzeczypospolitej Polskiej, oparł na treści art. 3a ustawy o świadczeniu usług drogą elektroniczną, który brzmi:

„Świadczenie usług drogą elektroniczną podlega prawu państwa członkowskiego Unii Europejskiej oraz Europejskiego Porozumienia o Wolnym Handlu (EFTA) - strony umowy o Europejskim Obszarze Gospodarczym, **na którego terytorium usługodawca ma miejsce zamieszkania lub siedzibę** (podkr. wł.)”.

Tymczasem, zgodnie art. 3b tej samej ustawy, „[n]a zasadach określonych przez przepisy odrębne swoboda świadczenia usług drogą elektroniczną **może zostać ograniczona, jeżeli jest to niezbędne ze względu na ochronę zdrowia, obronność, bezpieczeństwo państwa lub bezpieczeństwo publiczne** (podkr. wł.)”.

Jak podnosi M. Świerczyński, „[f]undamentem świadczenia usług drogą elektroniczną na terytorium Unii Europejskiej jest zasada państwa pochodzenia (...). Wynika z niej poddanie usług społeczeństwa informacyjnego prawu państwa członkowskiego UE (...), w którym znajduje się siedziba usługodawcy, o ile strony nie wybiorą innego prawa bądź zastosowania nie znajdzie jeden z wyjątków przewidzianych przez dyrektywę (dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego [dyrektywa o handlu elektronicznym], Dz. U.UE.L.2000.178.1; dalej: dyrektywa 2000/31/WE - przyp. wł.). [...]

Zasada państwa pochodzenia w ujęciu dyrektywy 2000/31/WE składa się z dwóch elementów: 1) skierowanego do władz państwa pochodzenia usługodawcy obowiązku kontroli jego działań. Kontrola ta dotyczy zgodności usług społeczeństwa informacyjnego z przepisami prawa krajowego i wspólnotowego. Wniosek ten wynika także z pkt 22 preambuły do dyrektywy,

który wskazuje, że usługi społeczeństwa informacyjnego winny być nadzorowane w taki sposób, aby zapewniona była skuteczna ochrona interesu publicznego; 2) skierowanego do państwa odbioru zakazu dyskryminacji zagranicznych usług (...). W ten też sposób należy interpretować art. 3a ust. 1 u.ś.u.d.e (ustawy o świadczeniu usług drogą elektroniczną - przyp. wł.).

W celu uniknięcia wątpliwości dyrektywa definiuje pojęcie siedziby przedsiębiorcy (...). W odniesieniu do usługodawców będących osobami fizycznymi przepis posługuje się pojęciem <miejsce zamieszkania> (trafniejsze byłoby posłużenie się pojęciem <miejsce zwykłego pobytu>)" [M. Świerczyński, *Komentarz do art. 3(a) ustawy o świadczeniu usług drogą elektroniczną*, http://lex/lex?content.rpc?reqId=1490017895335_66521026).

W tym miejscu należy przypomnieć, że definicja pojęcia „siedziba” została określona w art. 2 pkt 8 ustawy o świadczeniu usług drogą elektroniczną, który brzmi następująco: „siedziba - siedziba przedsiębiorstwa lub siedziba oddziału przedsiębiorcy zagranicznego wykonującego działalność gospodarczą na terytorium Rzeczypospolitej Polskiej”.

W komentarzu do tej definicji M. Świerczyński stwierdził, że „[d]odanie w art. 2 pkt 8 ustawy definicji siedziby (...) jest wzorowane na art. 2 lit. c dyrektywy 2000/31/WE. Zgodnie z definicją dyrektywy siedziba znajduje się tam, gdzie usługodawca faktycznie prowadzi działalność, wykorzystując stałe przedsiębiorstwo założone na czas nieokreślony. Pojęcie to jest istotne ze względu na wykorzystanie go jako łącznika w art. 3a, ustanawiającym zasadę państwa pochodzenia. Początkowo w projekcie nowelizacji z 2008 r. odniesiono to pojęcie do kodeksu cywilnego oraz ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jedn. Dz. U. z 2007 r. Nr 155, poz. 1095 z późn. zm.). Rozwiązanie takie byłoby błędne, albowiem definicja ta odnosi się do działalności międzynarodowej (transgranicznej), dlatego pojęcie to powinno zostać zdefiniowane w sposób autonomiczny, zgodnie z intencją dyrektywy, w oderwaniu od definicji wykorzystywanych na potrzeby

prawa materialnego. Senat w uchwale z dnia 2 listopada 2008 r. stanął z kolei na stanowisku (druk nr 1242), iż w definicji siedziby należy odwołać się również do siedziby oddziału przedsiębiorcy zagranicznego wykonującego działalność gospodarczą na terytorium Rzeczypospolitej Polskiej. Należy przyjąć, że pojęcie to (jak i termin <miejsce zamieszkania> występujący w art. 3a) powinny być interpretowane autonomicznie, zgodnie z metodą kwalifikacyjną przyjętą w prawie międzynarodowym” (M. Świerczyński, *Komentarz do art. 2 ustawy o świadczeniu usług drogą elektroniczną*, http://lex/lex/content.rpc?reqId=1490019887993_527418888).

Komentując z kolei art. 3b ustawy o świadczeniu usług drogą elektroniczną, M. Świerczyński na wstępie zauważył, że przepis ten „błędnie odnosi się do ograniczenia swobody świadczenia usług drogą elektroniczną, gdyż powinien dotyczyć jedynie ograniczenia skutków zastosowania zasady państwa pochodzenia z art. 3a ust. 1”, po czym stwierdził, iż „[w] konsekwencji należy uznać, że **zasada państwa pochodzenia może zostać wyłączona tylko przez działania właściwych organów w stosunku do danej usługi w oparciu o przepisy odrębne, gdy jest to niezbędne ze względu na ochronę zdrowia, obronność, bezpieczeństwo państwa lub bezpieczeństwo publiczne** (podkr. wł.)” [http://lex/lex/content.rpc?reqId=1490018204623_1962751149].

Biorąc powyższe pod uwagę, należy dojść do wniosku, że przedsiębiorca zagraniczny mający siedzibę poza terytorium Rzeczypospolitej Polskiej, a świadczący na terenie Rzeczypospolitej Polskiej usługi drogą elektroniczną, wbrew ocenie Wnioskodawcy, **nie jest wyłączony z wykonywania obowiązków** na rzecz obronności, bezpieczeństwa oraz bezpieczeństwa i porządku publicznego RP, o których mowa w art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną.

Podobnie nie są wyłączeni z wykonywania obowiązków na rzecz obronności, bezpieczeństwa oraz bezpieczeństwa i porządku publicznego RP

zagraniczni przedsiębiorcy i operatorzy pocztowi świadczący na terenie RP usługi telekomunikacyjne oraz pocztowe.

Zgodnie z art. 10 ust. 1 ustawy - Prawo telekomunikacyjne, „[d]ziałalność telekomunikacyjna będąca działalnością gospodarczą jest działalnością regulowaną i podlega wpisowi do rejestru przedsiębiorców telekomunikacyjnych, zwanego dalej <rejestrem>. Wpisowi do rejestru podlega również działalność telekomunikacyjna prowadzona przez przedsiębiorcę telekomunikacyjnego z państwa członkowskiego albo państwa, które zawarło ze Wspólnotą Europejską i jej państwami członkowskimi umowę regulującą swobodę świadczenia usług, **który czasowo świadczy na terytorium Rzeczypospolitej Polskiej** (podkr. wł.) usługi na zasadach określonych odpowiednio w przepisach Traktatu ustanawiającego Wspólnotę Europejską, umowy o Europejskim Obszarze Gospodarczym albo w przepisach innej umowy regulującej swobodę świadczenia usług.”.

Podobnie działalność pocztowa jest „działalnością regulowaną w rozumieniu przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2016 r. poz. 1829, 1948, 1997 i 2255 oraz z 2017 r. poz. 460 i 819) i wymaga wpisu do rejestru operatorów pocztowych, zwanego dalej <rejestrem>” (art. 6 ust. 1 ustawy - Prawo pocztowe).

Zgodnie z art. 7 ustawy - Prawo pocztowe, „[d]ziałalność pocztową w zakresie objętym obowiązkiem wpisu do rejestru (organem właściwym w sprawach wpisu do rejestru jest Prezes Urzędu Komunikacji Elektronicznej - przyp. wł.), może wykonywać przedsiębiorca, który:

- 1) zapewnia warunki do przestrzegania tajemnicy pocztowej, o której mowa w art. 41;
- 2) zapewnia warunki techniczne i organizacyjne świadczenia usług pocztowych niezbędne dla zachowania bezpieczeństwa obrotu pocztowego;
- 3) posiada regulamin świadczenia usług pocztowych oraz cennik usług pocztowych;

- 4) nie był prawomocnie skazany za umyślne przestępstwo przeciwko ochronie informacji, wiarygodności dokumentów, mieniu, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi lub umyślne przestępstwo skarbowe - dotyczy to osób fizycznych wykonujących we własnym imieniu działalność gospodarczą lub osób kierujących działalnością osób prawnych lub jednostek organizacyjnych niebędących osobami prawnymi, którym odrębna ustawa przyznaje zdolność prawną;
- 5) zapewnia, że wykonywanie działalności objętej wpisem do rejestru nie zagraża obronności, bezpieczeństwu państwa lub bezpieczeństwu i porządkowi publicznemu.”.

Biorąc powyższe pod uwagę należy stwierdzić, że wykonywanie przez zagranicznego przedsiębiorcę telekomunikacyjnego czy też zagranicznego operatora pocztowego obowiązków na rzecz obronności, bezpieczeństwa oraz bezpieczeństwa i porządku publicznego RP nie wynika, tak jak w przypadku usługodawcy zagranicznego świadczącego usługi drogą elektroniczną, z przepisu szczególnego, wyłączającego w tym zakresie skutki działania zasady państwa pochodzenia, lecz z faktu prowadzenia na terytorium Rzeczypospolitej Polskiej działalności gospodarczej (telekomunikacyjnej, pocztowej), która to działalność *per se* podlega regulacji. Działalność ta, poza wpisaniem jej do odpowiedniego rejestru, wymaga spełnienia określonych, restrykcyjnych warunków związanych z ochroną tajemnicy telekomunikacyjnej oraz tajemnicy pocztowej.

V. Zarzut niezgodności art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA w zakresie, w jakim przepisy te nie wskazują kategorii osób, których dane mogą być pozyskiwane w sposób określony w ustawach, nie regulują obowiązków informacyjnych wobec osób, których dane były pozyskiwane, oraz nie określają czasu, przez który

uprawnione podmioty mogą przetwarzać pozyskane dane, z art. 2, art. 30, art. 47, art. 49, art. 51 ust. 2, 3 i 4 w związku z art. 31 ust. 3 Konstytucji, z art. 8 Konwencji oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE (pkt VI *petitum* wniosku Rzecznika Praw Obywatelskich).

Zakwestionowane przepisy, których treść jest podobna, **regulują tryb uzyskiwania** przez Policję, Straż Graniczną, Żandarmerię Wojskową, ABW, SKW oraz CBA danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, jak również - sposób postępowania z uzyskanymi w tym trybie danymi, przy czym:

- według ustaw: o Policji, o Straży Granicznej oraz o Żandarmerii Wojskowej i wojskowych organach porządkowych uzyskane dane właściwy organ tych Służb przekazuje prokuratorowi właściwemu miejscowo lub rzeczowo, który podejmuje decyzję o zakresie i sposobie wykorzystania uzyskanych danych, zaś dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu (art. 20c ust. 6 i 7 ustawy o Policji, art. 10b ust. 6 i 7 ustawy o Straży Granicznej i art. 30 ust. 6 i 7 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych);

- zgodnie z ustawami: o ABW oraz AW i o SKW oraz SWW uzyskane dane, które mają znaczenie dla postępowania karnego, odpowiednio, Szef ABW/Szef SKW przekazuje Prokuratorowi Generalnemu, który podejmuje decyzję o zakresie i sposobie wykorzystania uzyskanych danych, zaś dane, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla, odpowiednio, bezpieczeństwa/obronności Państwa, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu (art. 28 ust. 6 i 7 ustawy o ABW oraz AW i art. 32 ust. 8 i 9 ustawy o SKW oraz SWW);

- zgodnie z ustawą o CBA, uzyskane dane, które mają znaczenie dla postępowania karnego, Szef CBA przekazuje Prokuratorowi Generalnemu, który podejmuje decyzję o zakresie i sposobie wykorzystania uzyskanych danych, zaś

dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu (art. 18 ust. 6 i 7 ustawy o CBA).

Argumentowanie niezgodności z ustawą zasadniczą tej grupy przepisów Rzecznik Praw Obywatelskich rozpoczął od ponownego przywołania wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11 i przypomnienia, że w jego uzasadnieniu Trybunał podkreślił, iż „niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych - przede wszystkim ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Ma to szczególne znaczenie w odniesieniu do osób, wobec których nie zapadł wyrok lub którym nie zostały oficjalnie postawione zarzuty, jak również osób trzecich, których pozyskanie danych dotyczyło bezpośrednio” oraz wskazał, iż „ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie, gdyż powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji narażałoby te działania na nieskuteczność”, a następnie zauważył, że „[n]a konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r. o sygn. S 2/06”, w którym stwierdził, iż „pominięcie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji, nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji” (uzasadnienie wniosku, s. 52).

Tymczasem, jak dalej podniósł RPO, „[z]akwestionowane ustawy nie zakładają istnienia żadnej procedury, w wyniku której o pozyskiwaniu danych

retencyjnych, pocztowych czy internetowych kiedykolwiek dowiedziałby się podmiot, którego dane były przetwarzane. W przekonaniu Rzecznika Praw Obywatelskich, obywatel powinien mieć prawo do podjęcia stosownych środków prawnych w zakresie działań prowadzonych względem niego, również w odniesieniu do informacji gromadzonych przez właściwe służby. Jest to również wymóg jasno określony przez Trybunał Konstytucyjny (postanowienie z 25 stycznia 2006 r. o sygn. akt S 2/06)” [uzasadnienie wniosku, s. 52-53].

W kolejnym fragmencie uzasadnienia wniosku Rzecznik stwierdził, że „[c]o więcej, projektodawca nie przewidział żadnych przepisów określających szczegółowo kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze”, oraz że „[w]reszcie, ustawy nie określają okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane telekomunikacyjne, pocztowe i internetowe. Stoi to w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego, zgodnie z którą dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Ustawa przewiduje jedynie, że dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi, które dla określonego postępowania miały znaczenie i zostały w nim wykorzystane, a tym kwestia weryfikacji potrzeby ich dalszego przetwarzania. O ile do czasu przechowywania danych włączonych w akta postępowania odnosić się będą przepisy szczególne, o tyle brak jest regulacji określających okres retencji danych przetwarzanych w systemach prowadzonych przez Policję i poszczególne służby. W praktyce może prowadzić to do nieuzasadnionego, bezterminowego przechowywania danych. Okres przetwarzania danych telekomunikacyjnych, pocztowych i internetowych powinien zatem być określony w sposób precyzyjny tak, aby wyeliminować ryzyko nadużyć, istniejące wobec faktu, że nie przewidziano zewnętrznej kontroli

niezbędności dalszego przetwarzania danych do realizacji ustawowych zadań” (s. 53).

Na wstępie należy zauważyć, iż o ile w przypadku zarzutu braku w zaskarżonych przepisach zadekretowania obowiązku poinformowania osób o zebraniu w sposób niejawnny dotyczących ich danych telekomunikacyjnych, danych pocztowych oraz danych internetowych Rzecznik Praw Obywatelskich w uzasadnieniu wniosku wskazał konkretne zasady konstytucyjne, które ów brak ma naruszać (art. 51 ust. 3 i 4 Konstytucji), oraz określił, w jaki sposób do naruszenia tych zasad – Jego zdaniem – dochodzi, o tyle w przypadku zarzutu nieokreślenia kategorii podmiotów, wobec których mogą być podejmowane wymienione w zaskarżonych przepisach czynności operacyjno - rozpoznawcze, oraz w przypadku zarzutu nieokreślenia okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane, Rzecznik poprzestał jedynie na ogólnym wskazaniu w *petitum* wniosku szeregu wzorców konstytucyjnej kontroli oraz wzorców kontroli z art. 8 Konwencji i art. 7 oraz art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

W związku z tym, po raz kolejny należy przypomnieć, że wniosek inicjujący hierarchiczną kontrolę norm musi spełniać wymogi określone w przepisach o postępowaniu przed Trybunałem Konstytucyjnym. **Wnioskodawca powinien określić zarzut niezgodności z Konstytucją, wskazać przedmiot i wzorce kontroli oraz sformułować uzasadnienie.** Ciężar dowodu spoczywa na podmiocie kwestionującym zgodność ustawy z Konstytucją.

W tym kontekście należy stwierdzić, że uzasadnienie przez Rzecznika Praw Obywatelskich zarzutu naruszenia przez wymienione w tej części wniosku przepisy art. 2, art. 30, art. 47, art. 49, art. 51 ust. 2, 3 i 4 w związku z art. 31 ust. 3 Konstytucji, a także art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, przez to, że owe zaskarżone unormowania nie określają kategorii podmiotów, wobec których mogą być podejmowane wymienione w

zaskarżonych przepisach czynności operacyjno - rozpoznawcze, oraz nie wskazują okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane, **nie jest prawidłowe.**

Uzasadnienie to nie spełnia bowiem określonych w art. 47 ust. 2 pkt 2 i 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym wymogów, jakim powinno odpowiadać uzasadnienie wniosku, kierowanego do Trybunału Konstytucyjnego przez podmiot, wymieniony w art. 191 ust. 1 pkt 1-5 Konstytucji, w tym także przez Rzecznika Praw Obywatelskich (uzasadnienie powinno zawierać przywołanie treści wzorców kontroli wraz z ich wykładnią [pkt 2] oraz wskazanie argumentów lub dowodów na poparcie zarzutu niekonstytucyjności [pkt 4]).

Przede wszystkim Rzecznik, formułując zarzut nadmiernego (nieproporcjonalnego) ograniczenia praw i wolności jednostki, określonych w art. 47, art. 49 i art. 51 ust. 2, 3 i 4 ustawy zasadniczej, jednocześnie **nie przeprowadził testu proporcjonalności**, mimo iż jako związkowy wzorzec kontroli zaskarżonych przepisów wskazał art. 31 ust. 3 Konstytucji.

W związku z powyższym należy stwierdzić, że, wobec konieczności respektowania generalnej zasady, jaką jest domniemanie konstytucyjności aktu normatywnego, samo wskazanie w *petitum* wniosku wzorca kontroli, bez szczegółowego odniesienia się w uzasadnieniu do kwestionowanej regulacji prawnej (lub lakoniczne sformułowanie zarzutu niekonstytucyjności), nie może zostać uznane za „uzasadnienie zarzutu niezgodności przedmiotu kontroli ze wskazanym wzorcem kontroli, z powołaniem argumentów lub dowodów na jego poparcie”, w rozumieniu przepisów regulujących postępowanie przez Trybunałem Konstytucyjnym.

Z tych też względów postępowanie w przedmiocie kontroli zgodności art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA, w

zakresie, w jakim nie określają kategorii podmiotów, wobec których mogą być podejmowane wymienione w tych przepisach czynności operacyjno - rozpoznawcze, oraz w zakresie, w jakim nie wskazują okresu, przez który uprawnione podmioty mogą przetwarzać uzyskane dane, z art. 2, art. 30, art. 47, art. 49, art. 51 ust. 2, 3 i 4 w związku z art. 31 ust. 3 Konstytucji, jak również z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE podlega umorzeniu na podstawie 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy - Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego - wobec niedopuszczalności wydania orzeczenia.

Jedynie na marginesie należy wskazać, że **podmiotowy** zakres kontroli operacyjnej **jest, co do zasady, nieograniczony**.

Wyłącznie w ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych wprost przewidziano, że kontrolę operacyjną, o której mowa w art. 30 tej ustawy, można zarządzić w stosunku do osób wskazanych w jej art. 3 ust. 2 pkt 1, pkt 3, pkt 4, pkt 5 i pkt 6. Chodzi o żołnierzy pełniących czynną służbę wojskową, pracowników zatrudnionych w jednostkach wojskowych w związku z ich zachowaniem się podczas pracy w tych jednostkach albo w związku z popełnieniem przez nich czynu zabronionego przez ustawę pod groźbą kary, wiążącego się z tym zatrudnieniem, osób przebywających na terenach lub w obiektach jednostek wojskowych, innych osób niż określone w art. 3 ust. 2 pkt 1-4, podlegających orzecznictwu sądów wojskowych albo jeśli wynika to z odrębnych przepisów, a także osób niebędących żołnierzami, jeżeli współdziałają z osobami, o których mowa w pkt 1-5, w popełnieniu czynu zabronionego przez ustawę pod groźbą kary albo też jeżeli dokonują czynów zagrażających dyscyplinie wojskowej albo czynów przeciwko życiu lub zdrowiu żołnierza albo mieniu wojskowemu. Natomiast pośrednio ograniczony jest podmiotowy zakres

kontroli operacyjnej określony w przepisach ustawy o SKW oraz SWW, gdyż w świetle art. 5 ust. 1 pkt 1 oraz ust. 2 tej ustawy Służba Kontrwywiadu Wojskowego może prowadzić czynności operacyjno-rozpoznawcze w sprawach o przestępstwa popełniane przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych Rzeczypospolitej Polskiej i innych jednostek organizacyjnych MON (lub we współdziałaniu z tymi osobami). Trzeba dodać, że do zadań SKW należy również rozpoznawanie, zapobieganie oraz wykrywanie zdarzeń oraz przestępstw o charakterze terrorystycznym godzących w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych RP oraz jednostek organizacyjnych MON (art. 5 ust. 1 pkt 2 ustawy o SKW oraz SWW). To ostatnie zadanie poszerza zakres podmiotowy kontroli operacyjnej przewidzianej w ustawie o SKW oraz SWW o osoby związane ze zdarzeniami oraz przestępstwami o charakterze terrorystycznym godzącymi w wyżej wymienione dobra chronione.

Odnośnie zaś do problematyki związanej z czasem (okresem) przetwarzania pozyskanych danych telekomunikacyjnych, danych pocztowych oraz danych internetowych należy zauważyć, iż czas ten, co do zasady, jest tożsamy z czasem trwania postępowania karnego, w którym dane te są wykorzystywane. Wszak zostały one uzyskane w większości w celu zapobiegania lub wykrywania przestępstw lub przestępstw skarbowych i jeżeli dane te nie mają znaczenia dla postępowania karnego (postępowania karnego skarbowego), „podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu”.

Jedynie w przypadku ABW i SKW czas przetwarzania (wykorzystywania) wspomnianych danych nie jest ograniczony wyłącznie czasem trwania postępowania karnego. Dane te mogą być bowiem przetwarzane (nie podlegają zniszczeniu) także wtedy, gdy są one istotne dla, odpowiednio, bezpieczeństwa/obronności państwa, co ma swoje uzasadnienie w specyfice wykonywanych przez te Służby zadań (szerzej na ten temat w dalszej części niniejszego stanowiska).

Przy tym należy podkreślić, że dopuszczalność wykorzystania danych telekomunikacyjnych, danych pocztowych oraz danych internetowych w postępowaniu sądowym nie może budzić kontrowersji. Wprawdzie, definiując cele pozyskiwania oraz przetwarzania danych telekomunikacyjnych przez służby powołane do ochrony bezpieczeństwa państwa i porządku publicznego, ustawodawca pominął cel dowodowy i ograniczył się tylko do wskazania, że dane te mogą być udostępniane tym służbom w celu zapobiegania przestępstwom bądź ich wykrywania, a także wykonywania przez te służby ustawowo określonych zadań, to jednak wskazuje się, że *„na podstawie wykładni funkcjonalnej przepisów regulujących pozyskiwanie danych telekomunikacyjnych można uznać wykorzystanie danych pozyskanych na etapie przedprocesowym, jako dowodów w postępowaniu karnym (...)”* [uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11, *op. cit.*].

Na tej samej podstawie i z tych samych powodów (brak uzasadnienia zarzutu niezgodności przedmiotu kontroli **ze wskazanymi wzorcami kontroli**, z powołaniem argumentów lub dowodów na jego poparcie, w tym brak przeprowadzenia testu proporcjonalności) umorzeniu - wobec niedopuszczalności wydania orzeczenia - podlega postępowanie w przedmiocie kontroli zgodności art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA, w zakresie, w jakim przepisy te nie przewidują obowiązku poinformowania osoby o posiadaniu na jej temat informacji w wyniku podjętych wobec niej i zakończonych działań polegających na uzyskiwaniu w sposób niejawnny danych teleinformatycznych, danych pocztowych oraz danych internetowych, z art. 2, art. 30, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE, co oznacza, iż umorzeniu podlega postępowanie w sprawie kontroli zgodności powołanych

wyżej przepisów, w zaskarżonym zakresie, **z innymi wzorcami niż wymienione w art. 51 ust. 3 i 4 Konstytucji.**

Na wstępie dalszych rozważań należy podnieść, iż przepisom art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA, Rzecznik Praw Obywatelskich w istocie zarzuca **niedostatek treściowy**, co oznacza, iż w tym przypadku niezgodności z Konstytucją Rzecznik upatruje **nie w wynikającym z wykładni autentycznej (treści ustawowej) rzeczywistym brzmieniu tych przepisów, ale w treści, której te przepisy nie zawierają a, w ocenie Wnioskodawcy, zawierać powinny.**

Przed podjęciem merytorycznej analizy zarzutów Rzecznika konieczne jest zatem rozstrzygnięcie, czy w tym przypadku mamy do czynienia – jak twierdzi Wnioskodawca – z „pominięciem”, czy też z, niepodlegającym kognicji Trybunału Konstytucyjnego, „zaniechaniem” ustawodawczym.

W uzasadnieniu postanowienia z dnia 2 grudnia 2014 r., w sprawie o sygn. akt SK 7/14, Trybunał Konstytucyjny stwierdził, że, aby dopuszczalna była merytoryczna ocena konkretnego zarzutu jako pominięcia ustawodawczego, należy w tym celu „*co najmniej ustalić występowanie:*

- *jakościowej tożsamości (a przynajmniej - daleko idącego podobieństwa) materii pominiętej w zaskarżonym przepisie i materii w nim uwzględnionej i (równocześnie)*
- *konstytucyjnego nakazu uregulowania kwestii pominiętych konkretnie w sposób wskazany przez (autora wniosku, pytania prawnego bądź skargi konstytucyjnej - przyp. wł.) [...], a dodatkowo ewentualnie także*
- *przypadkowości (bezrefleksyjności) decyzji ustawodawcy co do pominięcia w zaskarżonym przepisie materii wskazanej (...) [ta ostatnia okoliczność nie może*

jednak samoistnie przesądzać o dopuszczalności wydania wyroku]” (OTK ZU seria A nr 11/2014, poz. 123).

W jednym z późniejszych orzeczeń poświęconych charakterowi kontroli konstytucyjności pominięć prawodawczych - w postanowieniu z dnia 1 marca 2017 r., w sprawie o sygn. akt K 13/14, Trybunał Konstytucyjny przypomniał, że *„specyfika zarzutów dotyczących pominięcia prawodawczego wiąże się z wyjątkowym charakterem orzekania o pominięciach prawodawczych, a także z trudnościami w wyznaczeniu granicy między pominięciem a zaniechaniem prawodawczym. Zgodnie bowiem z art. 188 Konstytucji w kompetencji Trybunału jest orzekanie o wskazanych w nim przepisach prawa stanowionego, natomiast ocenianie konstytucyjności aktów prawnych pod względem zupełności regulacji dopuszcza się zarówno w doktrynie, jak i w samym orzecznictwie TK - na zasadzie wyjątku. Trybunał musi podchodzić z ostrożnością do tego rodzaju zarzutów, aby działalnością orzeczniczą nie wkraczać w sferę tworzenia prawa, zastrzeżoną, co do zasady, dla władzy ustawodawczej. Możliwość oceny konstytucyjności pominięć prawodawczych winna zatem podlegać regule exceptiones non sunt extendendae. Charakter kontroli konstytucyjności pominięć legislacyjnych Trybunał określał wielokrotnie. Na szczególną uwagę zasługuje w tym kontekście postanowienie z 18 czerwca 2013 r., sygn. SK 1/12, OTK ZU nr 5/A/2013, poz. 70, w którym wskazano, że: <[o]kreślona regulacja może być uznana za zawierającą unormowanie niepełne w sytuacji, gdy z punktu widzenia zasad konstytucyjnych ma zbyt wąski zakres zastosowania albo pomija treści istotne z punktu widzenia przedmiotu i celu tej regulacji. Ocena, czy ustawodawca dopuścił się pominięcia prawodawczego, wymaga więc a casu ad casum zbadania danego unormowania w kontekście wzorców i wartości konstytucyjnych, które ze względu na naturę tej regulacji muszą zostać poszerzone o daną kategorię podmiotów lub zachowań. To znaczy, że z norm konstytucyjnych da się odtworzyć wzorzec instytucji prawnej kształtowanej w akcie normatywnym, lecz instytucja w akcie tym ukształtowana konstytucyjnemu wzorcowi nie odpowiada (...).*

Niezbędnym warunkiem tej analizy jest ustalenie, że w określonej sytuacji zachodzi jakościowa tożsamość materii unormowanych w danym przepisie i tych pozostawionych poza jego zakresem, gdyż zbyt pochopne «upodobnienie» materii nieuregulowanych z materiałami, które znalazły swój wyraz w treści kwestionowanego przepisu, może spowodować wykroczenie przez Trybunał poza sferę kontroli prawa>” (OTK ZU seria A z 2017 r., poz. 10).

Wprawdzie w uzasadnieniu zarzutu niekonstytucyjności zaskarżonych w tej grupie przepisów poszczególnych ustaw regulujących ustrój i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego przez to, że nie zawierają one treści, którą – zdaniem Wnioskodawcy – zawierać powinny (powinny nakazywać poinformowanie jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych, po zakończeniu tych działań) Rzecznik Praw Obywatelskich nie odniósł się do, opisanych wyżej, ugruntowanych w orzecznictwie konstytucyjnym kryteriów rozróżnienia pominięcia od zaniechania prawodawczego i niejako „z góry” przyjął, iż określonej (niezbędnej z punktu widzenia wymogów konstytucyjnych) treści brakuje właśnie w tych przepisach, które wskazał, to należy przyjąć, że materia uregulowana w zaskarżonych przepisach: art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA **jest jedynie zbliżona do** materii, którą Rzecznik ocenił jako w tych przepisach pominiętą.

Treść powołanych przepisów dotyczy bowiem **materii trybu uzyskiwania** przez Policję, Straż Graniczną, Żandarmerię Wojskową, ABW, SKW oraz CBA danych telekomunikacyjnych, danych pocztowych lub danych internetowych, jak również - sposobu postępowania z uzyskanymi w tym trybie danymi. Postulowane przez Rzecznika wprowadzenie obowiązku informacyjnego to materia, która nie wchodzi w zakres procedury związanej z uzyskiwaniem, a następnie wykorzystywaniem danych, o których mowa w zaskarżonych

przepisach, do celów, dla których zostały pozyskane, jako że dotyczy postępowania, ze zbiorami danych już zgromadzonych, w ramach ewentualnych działań kontrolnych i interwencyjnych podejmowanych lub inicjowanych przez osobę, której określony zbiór danych dotyczy. Trzeba przy tym uwzględnić fakt, że ewentualne uzupełnienie kwestionowanych w tym punkcie wniosku RPO przepisów o regulacje postulowane przez Wnioskodawcę doprowadziłoby do stworzenia unormowań niepełnych, a wręcz pozornych – wobec braku instrumentarium prawnego do podjęcia przez zainteresowanego dalszych działań w stosunku do zebranych przez daną służbę danych na jego temat, to zaś oznaczałoby stan wtórnej niekonstytucyjności. Brak takiej kompleksowej regulacji dodatkowo świadczy o tym, że zamiarem ustawodawcy było zaniechanie wprowadzenia do tekstu nie tylko zakwestionowanych unormowań, ale mieszczących je aktów normatywnych w ogólności, przepisów dotyczących powiadamiania zainteresowanych osób o zebraniu dotyczących ich danych telekomunikacyjnych, internetowych czy pocztowych. Może to też świadczyć o przekonaniu ustawodawcy, że wprowadzona sądowa kontrola pozyskiwania przez poszczególne służby owych danych, w połączeniu z faktem, że dane te nie obejmują treści przekazów ani zawartości przesyłek, jest wystarczająca dla zagwarantowania przestrzegania ustawowych zasad pozyskiwania przedmiotowych danych, wszak pozyskiwania uzasadnionego interesem publicznym i dobrem innych osób, pokrzywdzonych zachowaniami, których zwalczaniu (zapobieganiu, wykrywaniu sprawców, pozyskiwaniu dowodów dla potrzeb postępowania w sprawach owych zachowań) służy pozyskiwanie danych.

W niniejszej sprawie problem jawi się zatem jako zaniechanie ustawodawcze, które nie może być przedmiotem kontroli Trybunału Konstytucyjnego.

Należy jednak przypomnieć, że w uzasadnieniu wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny stwierdził, iż „*[n]iejawne pozyskiwanie*

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

Przede wszystkim ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie. (...) Trybunał ma świadomość, że w pewnych sytuacjach może być również uzasadnione odstępnie od wspomnianego obowiązku informacyjnego (podkr. wł.), zaś w podsumowaniu swoich wywodów, pośród wymogów, jakie łącznie muszą spełniać przepisy ograniczające konstytucyjne prawa i wolności (przepisy regulujące niejawnie uzyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach), Trybunał Konstytucyjny wymienił, między innymi, „unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo (zob. np. postanowienie TK z 25 stycznia 2006 r., sygn. S 2/06)”, wskazując jednocześnie, że „nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne” (op. cit.).

To, że prawo podmiotu objętego kontrolą operacyjną (kontrolą niejawną) do bycia powiadomionym o takiej kontroli nie ma charakteru absolutnego i może zostać ograniczone, a nawet, że dopuszczalne jest odstępnie od faktu

powiadomienia, w szeregu swoich orzeczeniach potwierdza też Europejski Trybunał Praw Człowieka (dalej: ETPCz).

Na przykład, w uzasadnieniu wyroku z dnia 4 grudnia 2015 r. w sprawie *Zakharov v. Rosja* (47143/06), ETPCz stwierdził, że „[w] praktyce może nie być możliwym wymaganie późniejszego powiadomienia o wszystkich przypadkach kontroli. Działalność lub niebezpieczeństwo, w odniesieniu do którego stosowano konkretny zestaw środków niejawnnej kontroli, może utrzymywać się przez lata, a nawet dekady, po zawieszeniu stosowania takich środków. Późniejsze powiadomienie każdej osoby dotkniętej zawieszonym środkiem może również zniweczyć długoterminowy cel, dla którego pierwotnie zarządzono kontrolę. Dalej, takie powiadomienie może służyć ujawnieniu metod pracy i pól działania służb wywiadowczych, a nawet ujawnić ich agentów. A zatem fakt, iż osoby, których dotyczyły niejawne środki kontroli, nie są później powiadamiane o stosowaniu tychże środków po zakończeniu kontroli niejawnnej, nie może sam w sobie uzasadniać konkluzji, iż ingerencja nie była <konieczna w demokratycznym społeczeństwie>, gdyż to właśnie brak wiedzy o takiej kontroli zapewnia skuteczność przedmiotowej ingerencji. Z chwilą, w której można powiadomić osobę zainteresowaną bez narażenia na szwank celu odnośnej ingerencji po zakończeniu stosowania środka kontroli niejawnnej, osoba zainteresowana powinna jednakże otrzymywać taką informację” (LEX nr 1929190).

Obowiązek powiadomienia podmiotu objętego kontrolą operacyjną (kontrolą niejawną) o takiej kontroli – z ograniczeniami tego obowiązku, o jakich mowa była wyżej – wynika z dyrektywy 2016/680.

W części wstępnej powołanej dyrektywy, w motywach 43-48, wskazuje się, że:

- „[k]ażda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania danych i móc zweryfikować jego zgodność z prawem. Dlatego każda osoba, której dane

dotyczą, powinna mieć prawo do poznania i uzyskania informacji na temat celów przetwarzania danych, okresu ich przetwarzania oraz odbiorców danych, także w państwach trzecich. Jeśli takie informacje obejmują informacje o pochodzeniu danych osobowych, nie powinny one ujawniać tożsamości osób fizycznych, w szczególności poufnych źródeł informacji. Dla realizacji tego prawa wystarczy przekazać osobie, której dane dotyczą, pełne podsumowanie tych danych w zrozumiałej formie, czyli w formie pozwalającej jej poznać te dane, sprawdzić ich prawidłowość oraz zweryfikować zgodność ich przetwarzania z niniejszą dyrektywą, tak by mogła ona wykonywać prawa przysługujące jej na mocy niniejszej dyrektywy. Takie podsumowanie może mieć formę kopii przetwarzanych danych osobowych.”;

- „[p]aństwa członkowskie powinny mieć możliwość przyjmowania aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym (podkr. wl.) - przy należyтым uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej - tak aby uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić prawa i wolności innych osób. Administrator powinien dokonywać oceny – badając konkretnie i indywidualnie każdy przypadek – czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone.”;

- „[c]o do zasady o każdej odmowie lub każdym ograniczeniu dostępu należy powiadomić pisemnie osobę, której dane dotyczą, z podaniem faktycznych lub prawnych podstaw decyzji.”;

- „[k]ażde ograniczenie praw osoby, której dane dotyczą, musi być zgodne z Kartą i EKPC, w myśl wykładni zawartej, odpowiednio, w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka, a zwłaszcza musi odbywać się z poszanowaniem istoty tych praw i wolności.”;
- „[k]ażda osoba fizyczna powinna mieć prawo do uzyskania sprostowania dotyczących jej nieprawidłowych danych osobowych, zwłaszcza danych dotyczących faktów, oraz prawo do usunięcia danych, jeżeli przetwarzanie takich danych narusza niniejszą dyrektywę. Niemniej prawo do sprostowania danych nie powinno dotyczyć, na przykład, treści zeznania świadka. Każda osoba fizyczna powinna mieć również prawo do ograniczenia przetwarzania danych osobowych, gdy kwestionuje ona ich prawidłowość, której nie da się potwierdzić, lub gdy dane osobowe muszą zostać zachowane do celów dowodowych. W szczególności należy ograniczyć przetwarzanie danych osobowych zamiast ich usuwania, jeżeli w konkretnym przypadku uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą. W takim przypadku ograniczone dane należy przetwarzać tylko w celu, który zapobiegł ich usunięciu. Metody ograniczonego przetwarzania danych osobowych obejmują między innymi przeniesienie wybranych danych do innego systemu przetwarzania – np. do celów archiwizacyjnych – lub uniemożliwienie użytkownikom dostępu do wybranych danych. W zautomatyzowanych zbiorach danych ograniczenie przetwarzania danych osobowych należy zasadniczo zapewnić środkami technicznymi. Fakt ograniczenia przetwarzania danych osobowych należy zaznaczyć w systemie w sposób jasno wskazujący, że przetwarzanie tych danych jest ograniczone. O takim sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania należy poinformować odbiorców, którym dane zostały ujawnione, oraz właściwe organy, od których pochodzą nieprawidłowe dane. Administratorzy powinni również powstrzymać się od dalszego rozpowszechniania tych danych.”;

- „[j]eżeli administrator odmawia osobie, której dane dotyczą, prawa do informacji, dostępu lub sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, osoba, której dane dotyczą, powinna mieć prawo wystąpienia do krajowego organu nadzorczego o weryfikację zgodności przetwarzania z prawem. O prawie tym należy poinformować osobę, której dane dotyczą. Jeżeli organ nadzorczy podejmie działanie w imieniu osoby, której dane dotyczą, spoczywa na nim obowiązek poinformowania tej osoby co najmniej o fakcie przeprowadzenia wszelkich niezbędnych przeglądów lub kontroli. Organ nadzorczy powinien także poinformować osobę, której dane dotyczą, o przysługującym jej prawie do środka prawnego przed sądem.”.

Konkretyzację wspomnianych zasad przewidują przepisy zawarte w rozdziale III dyrektywy 2016/680, zatytułowanym „Prawa osoby, której dane dotyczą”.

Przykładowo, przepisy, zawartych w tym rozdziale, artykułów 13-15 brzmią następująco:

„Artykuł 13

Informacje udostępniane lub przekazywane osobie, której dane dotyczą

1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:

- a) tożsamość i dane kontaktowe administratora;
- b) dane kontaktowe inspektora ochrony danych, w razie potrzeby;
- c) cele przetwarzania, do których mają posłużyć dane osobowe;
- d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
- e) informacje o prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych odnoszącego się do osoby, której dane dotyczą.

2. Państwa członkowskie zapewniają, by oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach administrator przekazywał osobie, której dane dotyczą, następujące dalsze informacje umożliwiające wykonywanie przysługujących jej praw:

- a) podstawa prawna przetwarzania;
- b) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
- c) w stosownym przypadku kategoria odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
- d) w razie potrzeby dalsze informacje, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dotyczą.

3. Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należyтым uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

- a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
- b) uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar;
- c) chronić bezpieczeństwo publiczne;
- d) chronić bezpieczeństwo narodowe;
- e) chronić prawa i wolności innych osób (podkr. wł.).

4. Państwa członkowskie mogą przyjąć akty prawne dla określenia kategorii przetwarzania, które w całości lub części wchodzą w zakres stosowania środków wskazanych w którejkolwiek z liter ust. 3 (podkr. wł.).

Prawo dostępu przysługujące osobie, której dane dotyczą

Z zastrzeżeniem art. 15 państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli takie dane są przetwarzane, prawo dostępu do danych osobowych i do następujących informacji:

- a) cele i podstawa prawna przetwarzania;
- b) kategorie odnośnych danych osobowych;
- c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- d) w miarę możliwości planowany okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
- e) informacje o prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby;
- f) informacje o prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
- g) wskazanie, jakie dane osobowe są przetwarzane, oraz wszelkie dostępne informacje o ich pochodzeniu.

Artykuł 15

Ograniczenia prawa dostępu

1. Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należyтым uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

- a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
- b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;
- c) chronić bezpieczeństwo publiczne;
- d) chronić bezpieczeństwo narodowe;
- e) chronić prawa i wolności innych osób (podkr. wł.).

2. Państwa członkowskie mogą przyjąć akty prawne, aby ustalić kategorie przetwarzania, które w całości lub części wchodzą w zakres stosowania ust. 1 lit. a)–e) (podkr. wł.).

3. W przypadkach, o których mowa w ust. 1 i 2, państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia. **Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa w ust. 1** (podkr. wł.). Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

4. Państwa członkowskie zapewniają, by administrator dokumentował faktyczne lub prawne powody, na jakich opiera się decyzja. Informacje te udostępnia się organom nadzorczym.”.

Należy przy tym pamiętać, że, **począwszy od dnia 6 maja 2018 r., państwa członkowskie UE będą zobowiązane stosować przepisy art. 13-15 dyrektywy 2016/680.**

Wszystko to powoduje, że w niniejszej sprawie postępowanie w przedmiocie badania zgodności art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach

porządkowych, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW i art. 18 ustawy o CBA – w zakresie, w jakim przepisy te nie przewidują obowiązku poinformowania osoby o posiadaniu na jej temat informacji zebranych w wyniku podjętych wobec niej i zakończonych działań polegających na uzyskiwaniu w sposób niejawni danych telekomunikacyjnych, danych pocztowych oraz danych internetowych – z art. 51 ust. 3 i 4 Konstytucji podlega umorzeniu na podstawie art. 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy – Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym oraz ustawę o statusie sędziów Trybunału Konstytucyjnego, wobec niedopuszczalności wydania orzeczenia dotyczącego zaniechania ustawodawczego. Zarazem jednak aktualne unormowania winny zostać przeanalizowane przez ustawodawcę pod kątem realizacji wymogów wprowadzonych dyrektywą 2016/680.

VI. Zarzut niezgodności art. 28 ust. 7 ustawy o ABW oraz AW i art. 32 ust. 9 ustawy o SKW oraz SWW w zakresie, w jakim przepisy te nie przewidują zniszczenia wszelkich danych telekomunikacyjnych, danych pocztowych oraz danych internetowych innych niż tylko tych, które nie mają znaczenia dla prowadzonego postępowania karnego, z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, a także z art. 8 Konwencji oraz art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE (pkt VII *petitum* wniosku Rzecznika Praw Obywatelskich).

Wprawdzie treść zaskarżonych w tej grupie przepisów została omówiona w pkt V niniejszego stanowiska, tym niemniej dla przeprowadzenia prawidłowej analizy zgodności konieczne wydaje się przypomnienie, że:

- art. 28 ust. 7 ustawy o ABW oraz AW brzmi:

„Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu.”;

- art. 32 ust. 9 ustawy o SKW oraz SWW ma następujące brzmienie:

„Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla obronności państwa, podlegają niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu.”.

Z powyższego wynika, że „ustawa” zezwala na zachowanie danych, określonych jako „istotne dla bezpieczeństwa państwa” (w przypadku Agencji Bezpieczeństwa Wewnętrznego) oraz „istotne dla obronności państwa” (w przypadku Służby Kontrwywiadu Wojskowego).

W uzasadnieniu tego zarzutu Rzecznik Praw Obywatelskich przypomniał, iż „Trybunał Konstytucyjny w wyroku w sprawie K 23/11 w punkcie I ppkt 8 wyraźnie stwierdził, że art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, a także art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji. Przyjęta ustawa nie usunęła tego zastrzeżenia. W tym świetle Rzecznik Praw Obywatelskich nie ma wątpliwości, że wykazane tutaj pominięcie jest niezgodne z Konstytucją” (uzasadnienie wniosku, s. 54-55).

Na wstępie należy zauważyć, iż przedmiotem kontroli Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11 były przepisy:

- art. 28 ustawy o ABW oraz AW w brzmieniu:

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

1) możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane;

2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych.”

oraz

- art. 32 ustawy o SKW oraz SWW w następującym brzmieniu:

„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. z 2014 r. poz. 243), 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.”.

Przepisy: ust. 7 w art. 28 ustawy o ABW oraz AW i ust. 9 w art. 32 ustawy o SKW oraz AW zostały wprowadzone dopiero ustawą zmieniającą z dnia 15 stycznia 2016 r. i **obowiązują od dnia 7 lutego 2016 r.**

Trzeba dodać, że w wyroku w sprawie o sygn. akt K 23/11 Trybunał Konstytucyjny odroczył utratę mocy obowiązującej art. 28 ustawy o ABW oraz AW i art. 32 ustawy o SKW oraz SWW, w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, o 18 miesięcy i **termin ten upływał z dniem 6 lutego 2016 r.**

W uzasadnieniu rozstrzygnięcia w sprawie o sygn. akt K 23/11 dotyczącego art. 28 ustawy o ABW oraz AW i art. 32 ustawy o SKW oraz SWW (uzasadnienie to dotyczyło także art. 18 ustawy o CBA w brzmieniu obowiązującym w chwili wydania wyroku przez Trybunał Konstytucyjny, którego to przepisu po jego nowelizacji ustawą zmieniającą z dnia 15 stycznia 2016 r. Rzecznik nie zaskarżył), w określonym zakresie, Trybunał stwierdził, że *„problem konstytucyjny dotyczy pominięcia w zaskarżonych przepisach procedury weryfikacji i niszczenia danych niemających znaczenia (tj. zbędnych) dla dalszego postępowania* (podkr. wł.). *W jego ocenie, (w ocenie Wnioskodawcy - przyp. wł.) narusza to art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.*

Zgodnie z art. 51 ust. 2 Konstytucji władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Jak wskazywano w orzecznictwie TK, przepis ten ma dwojakie znaczenie. Po pierwsze, legalizuje działania władz publicznych polegające na pozyskiwaniu, gromadzeniu i udostępnianiu informacji o jednostkach w sposób inny niż w drodze zgłoszenia takich danych przez samego obywatela. A zatem również gromadzonych w sposób

niejawny przez te władze bez wiedzy i woli jednostki. Po drugie, do pewnego stopnia autonomicznie określa przesłanki legalności (granice) takich działań, ograniczając swobodę ustawodawcy determinowania zakresu zadań i kompetencji organów państwa polegających na uzyskiwaniu danych o obywatelach (...).

Ustrojodawca nie definiuje w art. 51 ust. 2 Konstytucji, czym są <informacje niezbędne w demokratycznym państwie prawnym>. Trybunał przyjmuje, że ocena niezbędności powinna być przeprowadzona z uwzględnieniem zasady proporcjonalności wynikającej z art. 31 ust. 3 Konstytucji. W rezultacie naruszenie autonomii informacyjnej polegające na pozyskiwaniu, gromadzeniu lub udostępnianiu przez władze publiczne informacji o obywatelach odpowiadać powinno zawsze wymaganiom zdefiniowanym w art. 31 ust. 3 Konstytucji (...). Jak wskazał Trybunał w innym wyroku, <norma wysłowniona w art. 51 ust. 2 Konstytucji nie ma charakteru całkowicie samodzielnego. Wprawdzie ustrojodawca wskazał w powołanym przepisie expressis verbis na ograniczenie możliwości arbitralnego kształtowania zakresu informacji o obywatelach pozyskiwanych przez władze publiczne w ustawodawstwie zwykłym i podkreślił wymóg niezbędności takiego ograniczenia, oceniany wedle standardów obowiązujących w demokratycznym państwie prawnym, nie określił jednak katalogu interesów (wartości) konstytucyjnie chronionych, które - jego zdaniem - mogą być stawiane na szali w procesie oceny dopuszczalności takiego rozwiązania. W tym zakresie konieczne jest odwołanie się do ogólnej regulacji art. 31 ust. 3 Konstytucji, zgodnie z którym ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw> (wyrok TK z 17 czerwca 2008 r., sygn. K 8/04, cz. III, pkt 2). Ustanowiony w art. 51 ust. 2 Konstytucji dodatkowy

zakaz pozyskiwania informacji innych niż niezbędne należy tłumaczyć tym, że <naruszenia autonomii informacyjnej poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki. Autonomia informacyjna, której wyodrębnienie normatywne z całości ochrony prywatności przewiduje art. 51, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Normatywne wyodrębnienie, ustanowienie w art. 51 ust. 2 Konstytucji odrębnego zakazu - ułatwia dostrzeżenie takiego wkroczenia i upraszcza przedmiot dowodu, iż takie wkroczenie nastąpiło. Przedmiotem dowodu staje się wtedy bowiem tylko to, czy pozyskiwanie informacji było konieczne, czy tylko «wygodne» lub «użyteczne» dla władzy. Dowodu wymaga, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym> (wyrok TK z 20 listopada 2002 r., sygn. K 41/02, cz. V, pkt 27).

W orzecznictwie trybunalskim dotyczącym czynności operacyjno-rozpoznawczych Trybunał starał się precyzować pojęcie <danych niezbędnych w demokratycznym państwie>. W wyroku o sygn. K 32/04 Trybunał zaznaczył: <w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny> (wyrok TK z 12 grudnia 2005 r., sygn. K 32/04, cz. III, pkt 4.7). Trybunał Konstytucyjny w niniejszej sprawie podziela to stanowisko (podkr. wł.).

Ustrojodawca w art. 51 ust. 2 Konstytucji wyraźnie odniósł wyrażony w nim zakaz do pozyskiwania informacji o <obywatelach>. Mogłoby to sugerować możliwość pozyskiwania, gromadzenia i przechowywania przez władze publiczne

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

Od tak ujętej zasady jednakowej ochrony dopuszczalne będzie wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, którzy podlegają polskiemu prawu. Przesądza o tym art. 37 ust. 2 Konstytucji. Trybunał ma świadomość doktrynalnych kontrowersji, jakie budzą wzajemne relacje art. 37 ust. 2 i art. 31 ust. 3 Konstytucji (...). Przychyliła się jednak do poglądu, w myśl którego art. 37 ust. 2 Konstytucji nie może być traktowany jako *lex specialis* wyłączający zastosowanie art. 31 ust. 3 Konstytucji, ponieważ w takim wypadku cudzoziemcy nie mieliby faktycznie żadnych gwarantowanych konstytucyjnie praw (...). Każde ograniczenie wolności lub praw niezarezerwowanych jedynie

dla obywateli winno być w związku z tym proporcjonalne w rozumieniu art. 31 ust. 3 Konstytucji, a ponadto nie może naruszać ich istoty. Konsekwencją obowiązywania art. 37 ust. 2 Konstytucji jest natomiast możliwość dokonania bardziej elastycznej interpretacji poszczególnych przesłanek składających się na zasadę proporcjonalności, uzasadniającej większy poziom ingerencji w wolności i prawa cudzoziemców niż obywateli. Za takim właśnie stanowiskiem przemawiać może również brzmienie uczynionego w niniejszej sprawie wzorcem kontroli art. 51 ust. 2 Konstytucji, który wyraźnie kładzie nacisk na istnienie przesłanki niezbędności uzyskiwania, gromadzenia i przechowywania danych o obywatelach.

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

Trybunał Konstytucyjny podziela zarzuty wnioskodawcy wobec art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW. Jak wcześniej wskazano (...), warunkiem niejawnego uzyskiwania informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów (podkr. wł.). Jak wcześniej podkreślono, ingerencją w sferę prywatności jednostek będzie nie tylko jednorazowe pozyskanie danych o jednostce (m.in. w trybie określonym w art. 28 ust. 1 ustawy o ABW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW), ale również każde kolejne operacje

na tych danych, w tym przechowywanie czy wtórne wykorzystywanie w toku innych postępowań (...).

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

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

Przede wszystkim należy zwrócić uwagę na odmienne cele prowadzenia czynności operacyjno-rozpoznawczych przez służby powołane do ochrony

bezpieczeństwa państwa, jakimi są ABW i SKW, w porównaniu do celów prowadzenia takich samych czynności przez służby powołane do ochrony porządku publicznego, a więc przez, przykładowo, Policję, Straż Graniczną czy Żandarmerię Wojskową.

Rozpoznawanie, zapobieganie i wykrywanie przestępstw, o których mowa w art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW i w art. 5 ust 1 pkt 1 ustawy o SKW oraz SWW **to nie jedyne zadania ABW i SKW**, dla realizacji których służby te zostały wyposażone w kompetencję do uzyskiwania, w sposób niejawni, danych telekomunikacyjnych, danych pocztowych oraz danych internetowych.

ABW może uzyskiwać wspomniane dane **także w celu**, między innymi, rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny (art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW), zaś SKW **także w celu**, między innymi, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych RP, prowadzenia kontrwywiadu radioelektronicznego czy też ochrony bezpieczeństwa jednostek wojskowych (art. 5 ust. 1 pkt 4, 5 i 7 ustawy o SKW oraz SWW).

Powyższe wskazuje, że zakładanym przez ustawodawcę celem, który ma zapewnić niejawnie uzyskiwanie przez ABW i SKW danych telekomunikacyjnych, danych pocztowych oraz danych internetowych **nie jest tylko zebranie dowodów przydatnych dla postępowania karnego** (prowadzenie postępowania karnego w sprawie o szpiegostwo może być czasem uznawane za porażkę służb powołanych do ochrony bezpieczeństwa państwa), ale **również, a może przede wszystkim, pozyskiwanie wiedzy o potencjalnych zagrożeniach bezpieczeństwa i obronności państwa**, w tym także wiedzy o obcej agenturze - po to, aby móc skutecznie wszystkim tym zagrożeniom **przeciwdziałać**, choćby przez kontrolę takich działań.

W związku z tym „konkretne postępowanie, prowadzone na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny”, o którym jest mowa w uzasadnieniu powołanego wyżej wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11, to nie tylko **postępowanie karne**.

Przez pojęcie „konkretne postępowanie” należy bowiem rozumieć także inne postępowanie prowadzone przez służby powołane do ochrony bezpieczeństwa państwa w ramach ustawowych zadań tych służb, a więc niejawnie postępowanie prowadzone niekoniecznie „na użytek” postępowania karnego (chodzi tu głównie o przeciwdziałanie ingerencjom obcych służb wymierzonym w bezpieczeństwo i obronność czy też w inne interesy państwa polskiego).

Rzeczywiście przepisy art. 28 ust. 7 ustawy o ABW oraz AW i art. 32 ust. 9 ustawy o SKW oraz SWW nie zawierają jakiegokolwiek, wyrażonej wprost, normy, która wskazywałaby na respektowanie obowiązku niszczenia „danych nieprzydatnych” dla prowadzonego postępowania, w tym także danych nieprzydatnych dla innego postępowania niż postępowanie karne.

Wiadomo tylko, że niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu podlegają tylko te dane, które **nie mają znaczenia** dla postępowania karnego, oraz te dane, które **nie są istotne** dla obronności i bezpieczeństwa państwa.

Dane **istotne** dla obronności i bezpieczeństwa państwa zniszczeniu więc nie podlegają.

W tej sytuacji można przyjąć interpretację, że te dane telekomunikacyjne, dane pocztowe oraz dane internetowe, które nie są istotne dla obronności i bezpieczeństwa państwa, nie są również istotne dla tego postępowania, w którym zostały one uzyskane.

W konsekwencji nie ulegają zniszczeniu tylko te dane, które mają znaczenie (uznano je wszak za istotne) dla podjętego i prowadzonego

postępowania w przedmiocie wykrycia i przeciwdziałania zagrożeniom dla obronności i bezpieczeństwa państwa.

Powyższe oznacza, że przepisy art. 28 ust. 7 ustawy o ABW oraz AW i art. 32 ust. 9 ustawy o SKW oraz SWW **w istocie nakładają obowiązek niszczenia uzyskanych przez te służby w trybie niejawnym danych telekomunikacyjnych, danych pocztowych oraz danych internetowych w każdym przypadku, gdy dane te nie mają znaczenia dla prowadzonego przez te służby postępowania.**

Tak więc zaskarżone przepisy, wbrew ocenie Wnioskodawcy, gwarantują zniszczenie danych telekomunikacyjnych, danych pocztowych oraz danych internetowych nie tylko tych, które nie mają znaczenia dla prowadzonego postępowania karnego, ale też danych, które nie mają znaczenia (nie są rzeczywiście przydatne) dla innego postępowania (innego niż postępowanie karne), prowadzonego przez daną służbę dla przeciwdziałania zagrożeniom bezpieczeństwa czy obronności państwa.

Biorąc pod uwagę, że w demokratycznym państwie prawnym za **konieczne może zostać uznane** przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych **wyłącznie ze względu na rzeczywistą (a nie potencjalną) przydatność** tych informacji, należy stwierdzić, że art. 28 ust. 7 ustawy o ABW oraz AW i art. 32 ust. 9 ustawy o SKW oraz SWW w zakresie, w jakim przepisy te nie przewidują zniszczenia danych telekomunikacyjnych, danych pocztowych oraz danych internetowych, które są istotne dla obronności i bezpieczeństwa państwa, są zgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji, a także art. 7 i art. 8 w związku z art. 52 ust. 1 Karty Praw Podstawowych UE.

VII. Zarzut niezgodności art. 13 oraz art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r. w zakresie, w jakim nakazują stosować przepisy, które

przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP (pkt VIII *petitum* wniosku Rzecznika Praw Obywatelskich).

Przepis art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r. brzmi:

„Do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu, stosuje się przepisy dotychczasowe.”.

Z kolei przepis art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r. ma następującą treść:

„Do kontroli operacyjnej prowadzonej na podstawie art. 27 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w brzmieniu dotychczasowym, w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2 lit. b tej ustawy, niezakończonych do dnia wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.”.

Niezgodności wskazanych przepisów z art. 2 oraz z art. 190 ust. 2 i 3 Konstytucji Rzecznik upatruje w tym, że nakazują one stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11.

Wskazuje na to, zdaniem Rzecznika, zakres ustawy zmieniającej z dnia 15 stycznia 2016 r., bowiem jej przepisy - jak wskazywano w uzasadnieniu do projektu ustawy - mają na celu wykonanie powołanego wyżej wyroku Trybunału Konstytucyjnego.

Tym samym, jak dowodzi Wnioskodawca, „należy uznać, że wprowadzając odwołanie do <przepisów dotychczasowych> ustawodawca ma na myśli przepisy uznane przez Trybunał za niezgodne z Konstytucją RP. Wnioskowanie to znajduje pokrycie w uzasadnieniu do projektu ustawy (Uzasadnienie do projektu ustawy, druk sejmowy nr 154, s. 15-16). W ocenie Rzecznika Praw Obywatelskich przepisy te są niezgodne z art. 2 oraz z art. 190 ust. 2 i 3 Konstytucji RP” (uzasadnienie wniosku, s. 56).

W dalszej części uzasadnienia tego zarzutu Rzecznik Praw Obywatelskich podnosi, że „[j]ak się wydaje skutki wyroku Trybunału Konstytucyjnego o niezgodności przepisu z Konstytucją RP są dwojakie. Po pierwsze, przepis ten formalnie jest usuwany z obrotu prawnego, niezwłocznie po ogłoszeniu wyroku lub - w razie odroczenia utraty mocy obowiązującej - w terminie wskazanym w orzeczeniu Trybunału Konstytucyjnego. Po drugie, ogłaszając niezgodność przepisu z Konstytucją RP, Trybunał jednocześnie orzeka niejako o niezgodności danej normy prawnej z ustawą zasadniczą. Nie tylko przepis jest niekonstytucyjny, ale także normy, które są z niego interpretowane. Tak rozumiany skutek orzeczenia prowadzi do ograniczenia kompetencji ustawodawcy w zakresie prawodawstwa w obszarze objętym wyrokiem Trybunału Konstytucyjnego. Oczywiście jest, że ustawodawca nie może uchwalić przepisu o tej samej treści, która została uznana za niezgodną z ustawą zasadniczą. Ustawodawca jednak nie tylko nie może uchwalić przepisu o tej samej treści, ale także przepisu o innej treści, z którego można wyinterpretować tylko normę o treści uznanej wcześniej za niekonstytucyjną. Innymi słowy, efektem jest derogacja nie tylko przepisu, ale także norm prawnych. W świetle zasady przyzwoitej legislacji należy zatem pamiętać, że uchwalanie norm - nawet przy zmianie językowego brzmienia przepisów - wcześniej uznanych za niezgodne z Konstytucją, narusza zasadę demokratycznego państwa prawnego. W kontekście art. 13 i 16 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, naruszenie zasady przyzwoitej legislacji jest bardziej oczywiste. Nie próbując nawet zmieniać brzmienia przepisów uznanych za niezgodne z ustawą zasadniczą, utrzymuje się je w mocy, uchybiając w ten sposób wyrokowi Trybunału Konstytucyjnego. W świetle tej zasady, przepis uznany za niezgodny z Konstytucją RP nie tylko formalnie, ale nawet materialnie nie może funkcjonować w obrocie prawnym” (uzasadnienie wniosku, s. 56-57).

Zdaniem Rzecznika, „[n]iewątpliwie uprawnione jest przekonanie obywatela o możliwości uznania za nieobowiązujące tych przepisów, które

Trybunał Konstytucyjny uznał za niezgodne z Konstytucją RP i jednocześnie upłynął termin odraczający utratę ich mocy. Decyzja ustawodawcy o utrzymaniu takich przepisów w mocy powoduje zachwianie bezpieczeństwa prawnego. Uderza ona także w zasadę zaufania obywateli do państwa, zwłaszcza w kontekście art. 190 ust. 1 i 3 Konstytucji RP” (uzasadnienie wniosku, s. 57).

Rzecznik wskazuje, iż zabieg ustawodawcy prowadzący do utrzymania w mocy przepisów obowiązujących przed wejściem w życie ustawy zmieniającej z dnia 15 stycznia 2016 r., a uznanych przez Trybunał Konstytucyjny za niezgodne z Konstytucją, „narusza zasadę ostateczności i powszechnej mocy obowiązującej wyroków Trybunału Konstytucyjnego”, co znajduje potwierdzenie w „wyroku Naczelnego Sądu Administracyjnego z 31 stycznia 2014 r., w którym zauważono, że: <Z art. 190 ust. 3 Konstytucji można wyprowadzić wniosek, że skoro Konstytucja wyjątkowo tylko zezwala na obowiązywanie niezgodnego z nią aktu prawnego, to regułą jest jego nieobowiązywanie, a więc niestosowanie> (wyrok NSA z 31 stycznia 2014 r., sygn. II FSK 2752/13) [LEX nr 1450203 - przyp. wł.]” (uzasadnienie wniosku, s. 57-58).

Jako wzorce kontroli art. 13 oraz art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r., w zaskarżonym zakresie, Rzecznik Praw Obywatelskich wskazał, wynikające z art. 2 Konstytucji, zasady: zaufania obywatela do państwa i stanowionego przez nie prawa oraz pewności i jednoznaczności prawa, a także art. 190 ust. 1 i 3 Konstytucji, statuujące zasadę ostateczności i powszechnej mocy obowiązującej orzeczeń Trybunału Konstytucyjnego.

Zadekretowana w art. 2 Konstytucji zasada zaufania obywateli do państwa i stanowionego przez nie prawa została szczegółowo opisana przez Rzecznika Praw Obywatelskich w uzasadnieniu wniosku, w oparciu o utrwalone, cytowane tamże, orzecznictwo Trybunału Konstytucyjnego, nie ma zatem potrzeby ponownie określać jej treści.

Uzupełniając należy stwierdzić, że, w ocenie P. Tulei, koniecznym wymogiem realizacji zasady zaufania obywateli do państwa i stanowionego przez nie prawa „jest zagwarantowanie bezpieczeństwa prawnego. Bezpieczeństwo prawne jednostki związane z pewnością prawa umożliwia więc przewidywalność działań organów państwa, a także prognozowanie działań własnych (...). Chodzi przy tym o pewność prawa nie tyle w rozumieniu stabilności przepisów, co **w aspekcie pewności tego, że na podstawie obowiązującego prawa obywatel może kształtować swoje stosunki życiowe** (podkr. wł.). W tym kontekście zasada ta wykazuje pewne podobieństwo do znanej z prawa prywatnego i międzynarodowego zasady *pacta sunt servanda*, nakazującej dotrzymywania zawartych umów (...).

Z zasady zaufania wynika zasada jednoznaczności prawa, rozumiana jako dyrektywa poprawnej legislacji (podkr. wł.). Odnosnie do nakazu respektowania przez ustawodawcę zasad przyzwoitej legislacji, stanowiących element zasady demokratycznego państwa prawnego, TK stwierdził, że zasady te obejmują m.in. <wymaganie określoności przepisów, które muszą być formułowane w sposób poprawny, precyzyjny i jasny>, a <standard ten wymagany jest zwłaszcza, gdy chodzi o ochronę praw i wolności> (wyr. z 11.1.2000 r., K 7/99, OTK 2000, Nr 1, poz. 2). Z tak ujętej zasady określoności wynika, że każdy przepis prawny powinien być skonstruowany poprawnie z punktu widzenia językowego i logicznego - dopiero spełnienie tego warunku podstawowego pozwala na jego ocenę w aspekcie pozostałych kryteriów. Wymóg jasności oznacza nakaz tworzenia przepisów klarownych i zrozumiałych dla ich adresatów, którzy od racjonalnego ustawodawcy oczekiwać mogą stanowienia norm prawnych niebudzących wątpliwości co do treści nakładanych obowiązków i przyznawanych praw. Związana z jasnością precyzja przepisu powinna przejawiać się w konkretności nakładanych obowiązków i przyznawanych praw, tak by ich treść była oczywista i pozwalała na wyegzekwowanie (...). Trybunał Konstytucyjny wielokrotnie podkreślał, że zasady przyzwoitej legislacji są

przejawem ogólnej zasady ochrony zaufania do państwa i stanowionego przez nie prawa, a w konsekwencji jedną z cech państwa prawnego. Brak precyzji przepisów powoduje bowiem stworzenie nazbyt szerokich ram dla organów stosujących prawo, które muszą zastępować ustawodawcę w zakresie tych zagadnień, które uregulował on w sposób nieprecyzyjny. Jak podkreślił TK, <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> (wyr. z 22.5.2002 r., K 6/02, OTK-A 2002, Nr 3, poz. 33 [...]). [...]

Z zasady zaufania TK wywodzi zakazy adresowane do organów władzy publicznej, w szczególności do ustawodawcy: „W demokratycznym państwie prawnym stanowienie i stosowanie prawa nie może być pułapką dla obywatela, a obywatel powinien mieć możliwość układania swoich spraw w zaufaniu, iż nie naraża się na niekorzystne skutki prawne swoich decyzji i działań niemożliwe do przewidzenia w chwili podejmowania tych decyzji i działań> (wyr. TK z 25.11.1997 r., K 26/97, OTK 1997, Nr 5-6, poz. 64 [...]). Takim zakazem jest też zakaz tworzenia uprawnień pozornych. Naruszeniem zasady ochrony zaufania do państwa i stanowionego przez nie prawa jest sytuacja, w której określone rozwiązanie prawne ma charakter iluzoryczny i pozorny. W wyr. z 8.1.2013 r. (K 18/10, OTK-A 2013, Nr 1, poz. 2) TK stwierdził, że ustawodawca nie może tworzyć konstrukcji normatywnych, które są niewykonalne, stanowią złudzenie prawa i w konsekwencji dają jedynie pozór ochrony interesów jednostki. Ustawodawca, co do zasady, nie może więc doprowadzać do istotnego zawężenia możliwości realizacji formalnie przyznanego jednostce prawa podmiotowego, tak że w istocie prowadzi to do powstania swoistego *nudum ius*, które wskutek tego staje się prawem bezprzedmiotowym” (komentarz P. Tulei do art. 2 Konstytucji, [w:] *Konstytucja RP, Komentarz. Art. 1-86*, Tom I, pod red. M. Safjana i L. Boska, Wydawnictwo C. H. BECK, Warszawa 2016, s. 224-225).

Z kolei, w przedmiocie skutków orzeczeń Trybunału Konstytucyjnego w sferze obowiązywania i stosowania prawa, A. Mączyński i J. Podkowiak stwierdzili, że „[s]kutków orzeczeń TK dotyczą wprost tylko dwa przepisy, a mianowicie art. 190 ust. 3, wskazujący, że następstwem uznania kontrolowanego aktu normatywnego za niezgodny z aktem wyższej rangi jest utrata mocy obowiązującej, oraz art. 190 ust. 4 Konstytucji RP, przewidujący możliwość ponownego rozpoznania sprawy, w której prawomocne orzeczenie sądowe, ostateczną decyzję administracyjną lub inne rozstrzygnięcie wydano na podstawie aktu normatywnego uznanego przez TK za niezgodny z normą hierarchicznie wyższą”, oraz że skutki stwierdzenia przez Trybunał Konstytucyjny, że dany przepis jest niezgodny z przepisem wyższej rangi „polegają na **całkowitym wyłączeniu możliwości stosowania tego przepisu nawet do stanów faktycznych powstałych w okresie przed ogłoszeniem wyroku TK, czyli w okresie, gdy przysługiwała mu moc obowiązująca** (podkr. wł.). Jak wyraził to TK, <orzeczenie przez Trybunał Konstytucyjny o niezgodności z konstytucją aktu normatywnego lub jego części powoduje bezwzględne, bezwarunkowe i bezpośrednie zniesienie (kasację) przepisów (norm) w nim wskazanych. Następuje to niezależnie od działań innych organów państwowych>” (zob. np. post. TK z 21.3.2000 r., K 4/99, OTK 2000, Nr 2, poz. 65; wyr. TK z: 21.2.2006 r., K 1/05, OTK-A 2006, Nr 2, poz. 18; 24.3.2009 r., K 53/07, OTK-A 2009, Nr 3, poz. 27). O ile więc <derogacja prawodawcza> ma charakter ograniczony, o tyle <derogacja trybunalska> - **całkowity, prowadząc do zupełnego usunięcia danej normy z systemu prawnego. Przyjmuje się, że wyrok uznający określony przepis za niezgodny z przepisem wyższej rangi ustanawia bezwzględny zakaz jego stosowania do jakichkolwiek sytuacji. Zakaz ten ma pierwszeństwo przed normą prawa międzyczasowego, nakazującą ocenę konkretnego stanu faktycznego na podstawie przepisów obowiązujących w czasie, gdy stan ten został zrealizowany**(podkr. wł.). Tezę tę uzasadnia w szczególności konstytucyjna regulacja tzw. kontroli konkretnej, czyli

realizowanej w postępowaniu wszczętym na podstawie pytania prawnego lub skargi konstytucyjnej. W tych sytuacjach zajęcie innego stanowiska przekreślałoby rację ustanowienia w Konstytucji RP obu tych instytucji. Sąd przedstawia pytanie prawne, aby zapobiec zastosowaniu przepisu, który ocenia jako niezgodny. Gdyby przyjąć, że wyrok uznający dany przepis za niezgodny ze wskazanym wzorcem kontroli nie uchyla obowiązku jego stosowania do wcześniejszych stanów faktycznych (a taki *ex thesi* jest stan faktyczny sprawy, w której przedstawiono pytanie prawne), to przedstawianie pytania prawnego nie miałoby sensu. Podobnie skarga konstytucyjna dotyczy sytuacji, w której zakwestionowany przepis obowiązywał w dacie ostatecznego rozstrzygnięcia, co więcej - został wówczas zastosowany jako podstawa rozstrzygnięcia o konstytucyjnych wolnościach, prawach lub obowiązkach przysługujących skarżącemu. Wprawdzie wyrok TK nie uchyla sam przez się skutków tego rozstrzygnięcia, ale skarżący (a także każdy inny podmiot, w którego sprawie wydane zostało rozstrzygnięcie oparte na zakwestionowanym przepisie) na podstawie art. 190 ust. 4 Konstytucji RP ma prawo żądać ponownego rozpoznania sprawy, w której ono zapadło. Podkreślić trzeba, że art. 190 ust. 4 dotyczy nie tylko wyroków TK wydanych w sprawach wszczętych przez wniesienie skargi konstytucyjnej. Skoro art. 190 ust. 4 dopuszcza, aby sprawy z okresu poprzedzającego wejście w życie wyroku TK mogły być ponownie rozpoznane, to jest oczywiste, że chodzi tu o ich rozpoznanie na podstawie nowego stanu prawnego, zmienionego w następstwie wyroku TK. Tym bardziej uzasadnione jest poddanie temu stanowi prawnemu spraw dotyczących stanów faktycznych, które wprawdzie miały miejsce przed zmianą stanu prawnego, lecz jeszcze nie stały się przedmiotem rozstrzygnięcia wydanego przez właściwy organ władzy publicznej. W konsekwencji, jak przyjmuje się w orzecznictwie i w literaturze, **z art. 79 ust. 1, art. 190 ust. 4 i art. 193 Konstytucji RP wynika mająca rangę konstytucyjną norma prawa międzyczasowego, zgodnie z którą stan prawny powstały w wyniku wejścia w życie wyroku TK stwierdzającego niezgodność**

jest adekwatny zarówno do oceny stanów faktycznych zrealizowanych po zmianie, jak i przed nią, nawet gdy sprawy te zostały ostatecznie rozstrzygnięte. Zakaz stosowania normy uznanej przez TK za niekonstytucyjną obowiązuje od dnia utraty mocy obowiązującej wynikającej z orzeczenia TK (podkr. wł.). Dotyczy to też sytuacji, w których na podstawie <zwykłych> reguł prawa międzyczasowego, miarodajnych dla danej dziedziny stosunków prawnych, należałoby zastosować tę normę (...). Uzasadnieniem aksjologicznym obowiązywania tej normy, która jako norma rangi konstytucyjnej ma pierwszeństwo przed normami rangi ustawowej, jest teza, iż przepis niezgodny nie powinien być znaleźć się w systemie prawnym (...).

Podsumowując, zgodzić się należy z poglądem, w myśl którego orzeczenia negatoryjne działają prospektywnie w sferze obowiązywania prawa, a retrospektywnie - w sferze stosowania prawa (...), a zatem ich skutki prawne wymykają się prostemu podziałowi na skuteczne *ex nunc* lub *ex tunc* (...).

Z perspektywy systemu prawa norma uznana za niekonstytucyjną przestaje być jego częścią od dnia ogłoszenia w organie urzędowym orzeczenia TK. **Po wydaniu orzeczenia nie jest konstytucyjnie dopuszczalne stanowienie norm mających treść lub ustanowionych w sposób oceniony przez TK jako naruszający normy wyższego rzędu** (podkr. wł.). Zdaniem TK <powtórzenie zrębów uznanej już raz za niekonstytucyjną konstrukcji prawnej stanowi wyraz lekceważenia przez Sejm rozstrzygnięć Trybunału oraz dowodzi ignorowania nałożonego na wszystkie organy państwa obowiązku wykonywania orzeczeń sądu konstytucyjnego> (zob. wyr. TK z 11.7.2012 r., K 8/10, OTK-A 2012, Nr 7, poz. 78). Ponadto niedopuszczalne jest wprowadzanie norm intertemporalnych nakazujących stosowanie normy prawnej uznanej za niekonstytucyjną do jakichkolwiek stanów faktycznych. Zakaz stanowienia norm, które faktycznie przedłużają obowiązywanie przepisów uznanych przez TK za niekonstytucyjne, ma znaczenie w szczególności w razie skorzystania przez TK z kompetencji określonej w art. 190 ust. 3 Konstytucji RP i określenia innego terminu utraty

mocy obowiązującej niekonstytucyjnego przepisu. Wskazany przez TK termin odroczenia jest nieprzekraczalną barierą, poza którą przepisy uznane za niekonstytucyjne mają utracić moc obowiązującą w rozumieniu tego przepisu. **Nowelizacja lub uchylene przepisu, którego dotyczył wyrok TK, w okresie odroczenia wyznaczonym na podstawie art. 190 ust. 3, przy jednoczesnym wprowadzeniu zasady dalszego stosowania uchylonego przepisu do określonych stanów faktycznych (np. faktów prawnych mających miejsce przed wejściem w życie nowego prawa) oznaczałaby *de facto* obejście zasady - mającej rangę konstytucyjną - powszechnie obowiązującej mocy orzeczeń TK (podkr. wł.).**

Z punktu widzenia sądów utrata mocy obowiązującej aktu normatywnego na skutek wyroku TK wyłącza możliwość jego zastosowania do jakichkolwiek stanów faktycznych sprzed daty wejścia w życie orzeczenia TK oraz stanów zaistniałych po tej dacie. Sądy muszą uwzględniać zmieniony stan prawny z urzędu” (komentarz A. Mączyńskiego i J. Podkowika do art. 190 Konstytucji, [w:] *Konstytucja RP, Komentarz. Art. 87-243*, Tom II, pod red. M. Safjana i L. Boska, Wydawnictwo C. H. BECK, Warszawa 2016, s. 1206 -1210).

Mając powyższe na względzie, należy zauważyć, iż przepis art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r., wprowadzie - do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie tej ustawy i do tego czasu nie została zakończona - nakazuje stosować, co do zasady, **przepisy dotychczasowe**, ale jednocześnie nie określa, czy pośród owych przepisów mają czy też nie mają się znajdować przepisy, które Trybunał Konstytucyjny uznał za niezgodne z Konstytucją w wyroku z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11.

Jest natomiast oczywiste, że pojęciem „przepisy dotychczasowe” nie mogą być objęte przepisy, które z dniem 7 lutego 2016 r. (data wejścia w życie ustawy zmieniającej z dnia 15 stycznia 2016 r.) utraciły moc obowiązującą w

związku z wejściem w życie powołanego wyżej wyroku Trybunału Konstytucyjnego.

Wszak skutki stwierdzenia przez Trybunał Konstytucyjny, że dany przepis jest niezgodny z przepisem wyższej rangi, polegają na całkowitym wyłączeniu możliwości stosowania tego przepisu nawet do stanów faktycznych powstałych w okresie przed ogłoszeniem wyroku Trybunału, czyli w okresie, gdy przysługiwała mu moc obowiązująca, a nowelizacja lub uchylenie przepisu, którego dotyczył ten wyrok, dokonane przez prawodawcę w okresie odroczenia utraty mocy obowiązującej wyznaczonym przez Trybunał Konstytucyjny na podstawie art. 190 ust. 3 Konstytucji, przy jednoczesnym wprowadzeniu zasady dalszego stosowania uchylonego lub zmienionego przepisu w jego dotychczasowym brzmieniu, zakwestionowanym orzeczeniem Trybunału, do określonych stanów faktycznych (np. mających miejsce przed wejściem w życie nowego prawa), **oznaczałoby *de facto* – co należy przypomnieć i podkreślić – obejście, mającej rangę konstytucyjną, zasady powszechnie obowiązującej mocy orzeczeń Trybunału Konstytucyjnego.**

Wszystko to powoduje konieczność takiej (zgodnej z Konstytucją) interpretacji art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r., że przepis ten – do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie tej ustawy i do tego czasu nie została zakończona – nakazuje stosować tylko te „dotychczasowe” przepisy, które od dnia 7 lutego 2016 r. korzystają z domniemania zgodności z Konstytucją.

Dlatego też odmienna, przedstawiona przez Wnioskodawcę, interpretacja art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r., jako niezgodna z Konstytucją, musi zostać uznana za niedopuszczalną.

W tym stanie rzeczy należy stwierdzić, że art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r. jest zgodny z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji.

Inaczej rzecz przedstawiałaby się w przypadku art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r., który – do konkretnej kontroli operacyjnej, a mianowicie kontroli prowadzonej na podstawie art. 27 ust. 1 ustawy o ABW oraz AW w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2 lit. b tej ustawy, niezakończony do dnia wejścia w życie ustawy zmieniającej – nakazuje stosować przepisy dotychczasowe (art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b. ustawy o ABW oraz AW).

Wynik wykładni językowej nie pozostawia wątpliwości, że w tym przypadku ustawodawca **zezwoił na dalsze (od dnia 7 lutego 2016 r.) stosowanie konkretnego przepisu (normy)**, którego moc obowiązująca, na skutek wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11 (*vide* - pkt I ppkt 2 w związku z pkt II sentencji wyroku, który brzmi: „art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu <Dz. U. z 2010 r. Nr 29, poz. 154, Nr 182, poz. 1228 i Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273, Nr 84, poz. 455, Nr 117, poz. 677 i Nr 230, poz. 1371, z 2012 r. poz. 627 i 908, z 2013 r. poz. 628, 675 i 1351 oraz z 2014 r. poz. 502, 544 i 616> jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji”), „wygasła” z końcem dnia 6 lutego w 2016 r., czym doprowadził do obejścia, mającej rangę konstytucyjną, zasady powszechnie obowiązującej mocy orzeczeń Trybunału Konstytucyjnego.

Oczywiście za pozostałe przepisy objęte użytym w art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r. terminem „przepisy obowiązujące” (poza normą wynikającą z art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW), mogą być uznane wyłącznie te przepisy, które nie utraciły mocy obowiązującej na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11 (*vide* - wcześniejsze uwagi dotyczące art. 13 ustawy zmieniającej z dnia 15 stycznia 2016 r.).

Powstaje jednak problem, czy – w zaskarżonym przez Rzecznika Praw Obywatelskich zakresie – ów art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r. istotnie obowiązuje, to znaczy, czy wywołuje jakiekolwiek skutki prawne w odniesieniu do jakichkolwiek podmiotów prawa.

Jak wiadomo, tego rodzaju kontrola operacyjna, której oceniany tu przepis dotyczy, prowadzona jest pod nadzorem Prokuratora Generalnego. Stwierdzam wobec tego kategorycznie, iż nie odnotowano przypadków prowadzenia (kontynuowania) przez Agencję Bezpieczeństwa Wewnętrznego kontroli operacyjnej na podstawie art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW oraz AW w brzmieniu tych przepisów sprzed wejścia w życie ustawy zmieniającej z dnia 15 stycznia 2016 r. Oznacza to, że art. 16 tejże ustawy – w zakresie zakwestionowanym przez RPO – nie może już wywierać żadnych skutków prawnych, jako że nie stanowi on podstawy prawnej ani do wszczęcia nowej, ani do podjęcia na nowo już zakończonej kontroli operacyjnej. Tym samym należy ową zakwestionowaną regulację uznać za *de facto* pozbawioną aktualnej treści normatywnej, mimo formalnego pozostawania tej regulacji w tekście obowiązującego aktu normatywnego. W tym stanie rzeczy kontrola konstytucyjności art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r., w trybie zainicjowanym wnioskiem uprawnionego podmiotu, nie jest dopuszczalna, gdyż oznaczałaby kontrolę przepisu, który – w zakwestionowanym zakresie – utracił moc obowiązującą przed wydaniem orzeczenia przez Trybunał Konstytucyjny w niniejszej sprawie.

W tym stanie rzeczy postępowanie w przedmiocie badania zgodności art. 16 ustawy zmieniającej z dnia 15 stycznia 2016 r., w określonym wyżej zakresie, z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP podlega umorzeniu na podstawie art. 59 ust. 1 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym w związku z art. 9 ust. 1 ustawy – Przepisy wprowadzające ustawę o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym

oraz ustawę o statusie sędziów Trybunału Konstytucyjnego, wobec utraty mocy obowiązującej przez zakwestionowany przepis przed wydaniem orzeczenia przez Trybunał Konstytucyjny.

Z tych wszystkich względów, wnoszę jak na wstępie.

Prokurator Generalny
Robert Heronim
Zastępca Prokuratora Generalnego