



SEJM
RZECZYPOSPOLITEJ POLSKIEJ
Sygn. akt K 9/16
BAS-WPTK-744/16

Warszawa, 26 stycznia 2018 r.

TRYBUNAŁ KONSTYTUCYJNY KANCLARIA	
wpl. dnia	26. 01. 2018
L.dz. L. zał.	

Trybunał Konstytucyjny

Na podstawie art. 69 ust. 2 w związku z art. 42 pkt 3 ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U. z 2016 r., poz. 2072), w imieniu Sejmu Rzeczypospolitej Polskiej przedkładam wyjaśnienia w sprawie wniosku Rzecznika Praw Obywatelskich z 18 lutego 2016 r. (sygn. akt K 9/16), jednocześnie wnosząc o stwierdzenie, że art. 19 ust. 15h ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2017 r., poz. 2067), art. 9e ust. 16h ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2017 r., poz. 2365), art. 31 ust. 16h ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organizacjach porządkowych (t.j. Dz. U. z 2016 r., poz. 1483), art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. 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 (t.j. Dz. U. z 2017 r., poz. 861), art. 17 ust. 15h ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz. U. z 2017 r., poz. 1993) w zakresie, w jakim posługują się 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 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2017 r., poz. 1904) **są zgodne** z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

Ponadto wnoszę o **umorzenie postępowania**:

1) w przedmiocie 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), art. 36b ust. 1 oraz art. 36bb ust. 1, art. 36d ust. 1h ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2016 r., poz. 720 ze zm.) z uwagi na utratę mocy obowiązującej przez przepisy do których odsyłały wyżej wymienione artykuły przed wydaniem orzeczenia przez Trybunał Konstytucyjny na podstawie art. 59 ust. 1 pkt 4 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

2) w przedmiocie art. 28 ust.1, art. 28 ust. 7, art. 28b ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2017 r., poz. 1920 ze zm.) oraz art. 32 ust. 1, art. 32 ust. 9, art. 32b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz. U. z 2017 r., poz. 861); art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2017 r., poz. 2067), art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2017 r., poz. 2365), art. 30 ust. 1 oraz art. 30c ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organizacjach porządkowych (t.j. Dz. U. z 2016 r., poz. 1483), art. 18 ust. 1 oraz art. 18b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz. U. z 2017 r., poz. 1993) na podstawie art. 59 ust. 1 pkt 3 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym ze względu na zbędność orzekania.

3) w pozostałej części na podstawie art. 59 ust. 1 pkt 2 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym ze względu na niedopuszczalność orzekania.

Uzasadnienie

I. Uwagi ogólne

1. W dniu 6 kwietnia 2016 r. do Kancelarii Sejmu wpłynęło zawiadomienie Prezesa Trybunału Konstytucyjnego o wszczęciu postępowania przed Trybunałem Konstytucyjnym w sprawie wniosku Rzecznika Praw Obywatelskich (dalej również: RPO, Rzecznik, wnioskodawca) z 18 lutego 2016 r. (sygn. akt K 9/16). Wnioskodawca zakwestionował zgodność :

1) art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2017 r., poz. 2067; dalej: ustawa o Policji), art. 9e ust. 10 ustawy z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2017 r., poz. 2365; dalej: ustawa o SG), art. 36c ust. 7 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (t.j. Dz. U. z 2016 r., poz. 720 ze zm.; dalej: ustawa o k.s.), art. 31 ust. 10 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz. U. z 2016 r., poz. 1483; dalej: ustawa o ŻW), art. 17 ust. 9 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz. U. z 2016 r., poz. 1310; dalej: ustawa 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;

2) art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o SG, art. 36d ust. 1h ustawy o k.s., art. 31 ust. 16h ustawy o ŻW, art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2017 r., poz. 1920 ze zm.; dalej: ustawa o ABW), art. 31 ust. 14h ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz. U. z 2017 r., poz. 861; dalej: ustawa o SKW), 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 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2017 r., poz. 1904; dalej: k.p.k.) – z art. 2 Konstytucji, z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3

Konstytucji oraz z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.; dalej: EKPCz);

3) art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy o Policji, art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy o SG, art. 36b ust. 1 oraz art. 36bb ust. 1 ustawy o k.s., art. 30 ust. 1 oraz art. 30c ust. 1 ustawy o ŻW, art. 28 ust. 1 oraz art. 28b ust. 1 ustawy o ABW, art. 32 ust. 1 oraz art. 32b ust. 1 ustawy o SKW, art. 18 ust. 1 oraz art. 18b ust. 1 ustawy o CBA, art. 75d ust. 1 oraz art. 75db ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (t.j. Dz. U. z 2016 r., poz. 1799; dalej: ustawa o SC) z art. 2, 30, art. 47, art. 49, 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 Unii Europejskiej (Dz. Urz. UE C 2012 Nr 326, s. 391; dalej: KPP);

4) 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 SG, art. 36b ust. 3 w związku z art. 36b ust. 2 ustawy o k.s., art. 30 ust. 3 w związku z art. 30 ust. 2 ustawy o ŻW, art. 28 ust. 3 w związku z art. 28 ust. 2 ustawy o ABW, art. 32 ust. 5 w związku z art. 32 ust. 2 ustawy o SKW, art. 18 ust. 3 w związku z art. 18 ust. 2 ustawy o CBA, art. 75d ust. 3 w związku z art. 75d ust. 2 ustawy o SC z art. 2, art. 20 oraz art. 47 i art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji;

5) art. 20ca ustawy o Policji, art. 10ba ustawy o SG, art. 36ba ustawy o k.s., art. 30b ustawy o ŻW, art. 28a ustawy o ABW, art. 32a ustawy o SKW, art. 18a ustawy o CBA, art. 75da ustawy o SC – w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych – z art. 2, art. 47, 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 KPP;

6) art. 20c ustawy o Policji, art. 10b ustawy o SG, art. 36b ustawy o k.s., art. 30 ustawy o ŻW, art. 28 ustawy o ABW, art. 32 ustawy o SKW, art. 18 ustawy o CBA, art. 75d ustawy o SC – 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, ust. 3 i ust. 4 w związku z art. 31 ust. 3 Konstytucji, z art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 KPP;

7) art. 28 ust. 7 ustawy o ABW, art. 32 ust. 9 ustawy o SKW – 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 w związku z art. 31 ust. 3 Konstytucji, art. 8 EKPCz oraz art. 7 i art. 8 w związku z art. 52 ust. 1 KPP;

8) 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; dalej: ustawa zmieniająca; u.z.) – w zakresie, w jakim nakazują stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. akt K 23/11 – z art. 2 oraz z art. 190 ust. 1 i ust. 3 Konstytucji.

2. Zarzuty Rzecznika Praw Obywatelskich koncertują się wokół zagadnień związanych ze stosowaniem kontroli operacyjnej (pkt I, II, VIII *petitum* wniosku RPO) oraz trybu pozyskiwania i przetwarzania danych telekomunikacyjnych, pocztowych i internetowych przez służby policyjne i służby specjalne oraz zewnętrznej kontroli nad tymi czynnościami (pkt III, IV, V, VI, VII *petitum* wniosku RPO). Przed przystąpieniem do oceny dopuszczalności rozpoznania, a następnie merytorycznej analizy poszczególnych zarzutów warto zaprezentować ogólne uwagi dotyczące wspomnianych instytucji.

3. Charakter czynności operacyjno-rozpoznawczych w perspektywie konstytucyjnej był przedmiotem obszernych rozważań Trybunału w wyroku z 12 grudnia 2005 r. (sygn. akt K 32/04).

Jak zauważył sąd konstytucyjny: „Czynności operacyjno-rozpoznawcze mają charakter nieprocesowy [na temat relacji zachodzących pomiędzy czynnościami operacyjno-rozpoznawczymi a procesowymi oraz ujawnianymi na tym tle kontrowersjami zob. np. D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 320 i n. – uwaga własna]. To ogranicza kontrolę sądową nad ich przebiegiem. Czynności operacyjno-rozpoznawcze «praktyka służby śledczej ukształtowała jako czynności uzupełniające lub wykonawcze w stosunku do czynności procesowych i zadań postępowania przygotowawczego» (tak L. Szaff, *O niektórych problemach dotyczących zakresu postępowania przygotowawczego*, „Nowe Prawo” nr 12/1957). Pozapprocesowy charakter jest ich cechą istotną (B. Hołyst, *Kryminalistyka*, Warszawa 1983, s. 23). Czynności operacyjnorozpoznawcze spełniają funkcje: rozpoznawcze, wykrywcze,

kierunkujące późniejsze udowodnienie, weryfikujące uprzednie ustalenia, zapobiegawcze (profilaktyczne), ochronne, zabezpieczające (T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1998, s. 131). [...] Czynności te są z natury rzeczy niejawne (także wobec zainteresowanego), prowadzone w warunkach dających policji szeroki margines uznaniowości, przy ograniczonych gwarancjach dla praw osoby poddanej tym czynnościom, a także okrojonej kontroli zewnętrznej, w tym sądowej. Ten sposób działania [...] jest we współczesnym państwie nieodzowny. Przejrzystość czynności operacyjnych powodowałaby ich nieskuteczność. Współczesne państwo, zobowiązane do zapewnienia bezpieczeństwa (co także jest powinnością konstytucyjną), staje przed trudnym zadaniem, ze względu na zagrożenia terroryzmem, przestępczością (w tym także zorganizowaną). Techniczne udogodnienia, wpływające na szybkość komunikowania się i przemieszczania, w równym stopniu mogą być wykorzystywane w celu ochrony bezpieczeństwa państwa, jak i przez przestępców. [...] Czynności operacyjno-rozpoznawcze jako zespół prawnie określonych w oparciu o wiedzę kryminalistyczną niejawnych działań prowadzonych poza procesem karnym i administracyjnym celem wykrycia, rozpoznawania i utrwalania przestępczej działalności (A. Żebrowski, *op.cit.*, s. 16 [Czynności operacyjno-rozpoznawcze. Regulacje prawne, Kraków 2000 – uwaga własna]) są konieczną koncesją na rzecz skutecznego zwalczania przestępczości, wiążącą się jednakowoż z ograniczeniem gwarancji dla jednostki, korzystającej z prawa do prywatności i autonomii informacyjnej. Wynika to z pozaprocesowego (pozbawionego wpływu sądu) oraz tajnego i nieformalnego charakteru czynności operacyjno-rozpoznawczych. Wszelkie ograniczenia konstytucyjnych wolności i praw jednostki, nawet te, na które zezwalają ustawy, muszą jednak odpowiadać zakresowo, przedmiotowo i co do sposobu – temu, co mówi sama Konstytucja określająca margines regulacyjny ustawodawcy zwykłego – w momencie gdy zezwala mu poprzez czynności operacyjno-rozpoznawcze na wkroczenie w sferę praw i wolności regulowanych konstytucyjnie. Margines ten określają z jednej strony wspomniane już szczególne regulacje konstrukcyjnie wmontowane w regulacje dotyczące poszczególnych konstytucyjnych praw podmiotowych (np. we wspomnianych już art. 49 i art. 51 Konstytucji), a nadto ogólna klauzula proporcjonalności, wskazana w art. 31 ust. 3 Konstytucji”.

4. Wniosek RPO w części dotyczy specyficznej instytucji zaliczanej do czynności operacyjno-rozpoznawczych, a mianowicie kontroli operacyjnej. Kontrola

operacyjna jest instytucją do pewnego stopnia zunifikowaną, tzn. uregulowaną analogicznie we wszystkich aktach prawnych przyznających kompetencję do jej prowadzenia służbom i organom policyjnym. Jednym z przejawów takiego ujednolicenia jest katalog czynności podejmowanych w ramach owej kontroli, która polega na niejawnym: 1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; 4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; 5) uzyskiwaniu dostępu i kontroli zawartości przesyłek. Pojęcie kontroli operacyjnej jest więc bardzo pojemne. Taka kontrola umożliwia pozyskiwanie różnego rodzaju informacji o jednostce, przede wszystkim związanych z komunikowaniem się (treść korespondencji lub rozmów, zawartość przesyłek) i innymi formami przekazywania wiadomości. Mając powyższe na uwadze, Trybunał przyjął w wyroku z 30 lipca 2014 r. (sygn. akt K 23/11), że przepisy regulujące kontrolę operacyjną umożliwiają m.in. podsłuch osób i pomieszczeń, w tym rozmów za pośrednictwem telefonii stacjonarnej, bezprzewodowej (komórkowej) i internetowej, pozyskiwanie treści wiadomości tekstowych i multimedialnych przesyłanych za pomocą urządzeń telefonicznych oraz innych urządzeń służących do komunikowania się na odległość, stosowanie urządzeń rejestrujących położenie osób i rzeczy wykorzystujących nawigację satelitarną lub przechwytywanie ulotu elektromagnetycznego (zob. J. Kudła, *Wybrana problematyka czynności operacyjno-rozpoznawczych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 533-534; J. Widacki, *Kryminalistyka*, Warszawa 2012, s. 135-137).

Kontrola operacyjna ma charakter subsydiarny. Może być zatem zarządzana tylko wtedy, gdy inne środki okazały się bezskuteczne lub są nieprzydatne. Przez pojęcie „innych środków” należy rozumieć pozostałe formy czynności operacyjno-rozpoznawczych, niebędące kontrolą operacyjną. Można w tym miejscu przykładowo wskazać na: pozyskiwanie danych bankowych, danych osobowych, posługiwanie się tajnym współpracownikiem, obserwację miejsc publicznie dostępnych.

„Bezskuteczność” oznacza nieprzynoszenie spodziewanych rezultatów, zaś „nieprzydatność” – brak możliwości osiągnięcia zamierzonych celów za pomocą określonego środka. Jak przyjmuje się w piśmiennictwie, wnosząc o zarządzenie kontroli operacyjnej, właściwy organ ma wykazać bezskuteczność dotychczasowych działań lub uprawdopodobnić nieprzydatność tradycyjnych metod analizy kryminalnej (zob. W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [w:] *Praktyczne elementy...*, s. 511).

5. Drugim, obok kontroli operacyjnej, obszarem zainteresowania RPO jest pozyskiwanie danych niestanowiących treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną. Są to tzw. dane: telekomunikacyjne (m.in. dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest połączenie; dane niezbędne do określenia: daty i godziny połączenia telefonicznego oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego), pocztowe (dane o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług) oraz internetowe.

Nie ulega wątpliwości, że także i opisane wyżej środki stanowią skuteczne narzędzie walki z przestępczością, zarówno w jej tradycyjnym rozumieniu, jak i przybierającą na skutek postępu technologicznego nowe kształty i przejawy (tzw. cyberprzestępczość). Słusznie zwraca uwagę Trybunał Konstytucyjny, iż metadane dotyczące nawiązywanego połączenia (dane o ruchu i lokalizacji) pozwalają na rekonstrukcję społecznych zachowań jednostek objętych obserwacją, bez potrzeby osobistego prowadzenia działań operacyjnych wymagających zaangażowania wielu osób, długiego czasu oraz ponadprzeciętnej ostrożności przed dekonspiracją. Analiza 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 (zob szerzej. wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11).

6. Obszerne podsumowanie dorobku doktryny prawa oraz orzecznictwa sądów międzynarodowych, a także podtrzymania i rozwinięcia trybunalskiego *acquis* w zakresie regulacji dotyczących czynności operacyjno-rozpoznawczych Trybunał Konstytucyjny dokonał w, wydanym w pełnym składzie, wyroku z 30 lipca 2014 r. (sygn. akt K 23/11). W pierwszej kolejności należy zatem odwołać się do poczynionych tam ustaleń, które będą stanowić płaszczyznę odniesienia dla szczegółowych rozważań prowadzonych w dalszej części niniejszego stanowiska.

Na tle swoich dotychczasowych wypowiedzi Trybunał skatalogował konieczne elementy ustawowej regulacji czynności operacyjno-rozpoznawczych (niejawnego pozyskiwania przez władze publiczne informacji o jednostkach).

Po pierwsze, to ustawa ma precyzować przedmiotowe przesłanki zarządzenia takich czynności. Ustawodawca zobowiązany jest wobec tego zdefiniować zamknięty i możliwie wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki.

Po drugie, niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Mając na uwadze ogromną liczbę środków stosowanych przez organy państwa, przydatnych w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie, norma prawna musiałaby być kazuistyczna. Według Trybunału, najbardziej pożądanym rozwiązaniem z konstytucyjnego punktu widzenia jest uregulowanie rodzajów środków służących niejawnemu pozyskiwaniu informacji o jednostkach w ustawie.

Po trzecie, ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. Nie jest rolą Trybunału Konstytucyjnego, jako sądu prawa, określanie, jak długi ma być to termin.

Po czwarte, w ustawie ma być uregulowana procedura zarządzania czynności operacyjno-rozpoznawczych, włączając w to powierzenie kompetencji do zarządzania tych czynności, a także badanie ich legalności przez zewnętrznego i niezależnego od organów władzy wykonawczej podmiot, najlepiej przez sąd. Ustawa ma wskazywać podstawowe elementy proceduralne, zasady wykorzystywania zgromadzonych materiałów oraz przesłanki czy tryb ich niszczenia.

Po piąte, ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza

wykorzystanie ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisijnemu zniszczeniu, z uwagi na ich zbędność lub nieprzydatność.

7. Przed zaprezentowaniem właściwej analizy formalnoprawnej i merytorycznej zarzutów wysuniętych przez RPO Sejm zwraca uwagę na przyjęty układ tekstu. Tam gdzie zarzuty wnioskodawcy zostaną zestawione z wzorcami kontroli już wcześniej – w tożsamym zakresie – powołanymi, Sejm w celu uniknięcia powtórzenia odeśle do odpowiedniej części niniejszego pisma zawierającej analizę normatywnej podstawy kontroli.

II. Maksymalny czas trwania kontroli operacyjnej

II.1. Przedmiot kontroli

1. Przepisy zakwestionowane przez wnioskodawcę w ramach pierwszego zarzutu stanowią następująco.

Artykuł 19 ust. 9 ustawy o Policji: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawiają się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, również po upływie okresów, o których mowa w ust. 8, wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy”.

Artykuł 9e ust. 10 ustawy o SG: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawiają się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, złożony po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 1, może, również po upływie okresów, o których mowa w ust. 9, wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy”.

Artykuł 36c ust. 7 ustawy o kontroli skarbowej: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla wykrycia przestępstwa lub przestępstwa skarbowego albo ustalenia sprawców i uzyskania dowodów takich przestępstw, Sąd, na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, również po upływie okresów, o których mowa w ust. 6, wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy”.

Artykuł 31 ust. 10 ustawy o ŻW: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, wojskowy sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu Żandarmerii Wojskowej, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej oraz właściwego prokuratora do spraw wojskowych, może, również po upływie okresów, o których mowa w ust. 9, wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy”.

Artykuł 17 ust. 9 ustawy o CBA: „W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie okresów, o których mowa w ust. 8, kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy”.

2. Jak już była o tym mowa, RPO domaga się kontroli wymienionych wyżej przepisów 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.

II.2. Zarzuty wnioskodawcy

Zdaniem Rzecznika Praw Obywatelskich przewidziany przez ustawodawcę w zaskarżonych przepisach maksymalny czas prowadzenia kontroli operacyjnej jest nieproporcjonalnie długi i „przekracza ramy konieczne w demokratycznie państwie prawnym”. W ocenie RPO: „Trudno jest przyjąć, że służby policyjne i służby specjalne potrzebują aż osiemnastu miesięcy na zebranie materiałów uzasadniających wszczęcie postępowania karnego”.

II.3. Analiza formalnoprawna

1. Zgodnie z art. 47 ust. 1 pkt 6 ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U. z 2016 r., poz. 2072; dalej: ustawa o TK) wniosek złożony przez podmiot, o którym mowa w art. 191 ust. 1 pkt 1-5 Konstytucji (a zatem także przez RPO) powinien zawierać uzasadnienie. Wśród warunków, jakie winno spełniać uzasadnienie – sprecyzowanych w art. 47 ust. 2 pkt 1-4 ustawy o TK – ustawodawca wymienił określenie problemu konstytucyjnego i zarzutu niekonstytucyjności (pkt 3) oraz wskazanie argumentów lub dowodów na poparcie zarzutu niekonstytucyjności (pkt 4). Zbliżone wymogi w tym zakresie przewidywały poprzednie ustawy regulujące tryb postępowania przed Trybunałem w związku z czym wydane na ich podstawie dotychczasowe orzecznictwo sądu konstytucyjnego może być miarodajne dla oceny wywiązania się z powyższego obowiązku przez RPO w niniejszym postępowaniu.

Konieczność uzasadnienia zarzutu sformułowanego w pytaniu prawnym związana jest z domniemaniem konstytucyjności norm prawnych oraz z zasadą kontrydiktoryjności. Zgodnie z wypowiedziami Trybunału Konstytucyjnego: „Kontrola konstytucyjności ustaw przebiega w oparciu o domniemanie, że badane normy są zgodne z konstytucją. 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 naruszeniu uległaby zasada kontrydiktoryjności postępowania przed Trybunałem Konstytucyjnym, a Trybunał przekształciłby się w organ orzekający z inicjatywy własnej (zob. np. orzeczenia TK z: 26 kwietnia 1995 r., sygn. akt K 11/94; 31 stycznia 1996 r., sygn. akt K 9/95; wyroki TK z: 27 czerwca

2008 r., sygn. akt K 51/07; 15 kwietnia 2014 r., sygn. SK 48/13). Jak wskazuje się w literaturze, wymóg uzasadnienia powołanych zarzutów oznacza konieczność przedstawienia argumentów, które przemawiają za stwierdzeniem niezgodności zaskarżonych norm prawnych z normami powołanymi jako podstawa kontroli. Wymóg ten odnosi się do każdego z podniesionych zarzutów niezgodności danej normy (zob. K. Wojtyczek, *Ciężar dowodu i argumentacji w procedurze kontroli norm przez Trybunał Konstytucyjny*, „Przegląd Sejmowy” 2004, nr 1, s. 17).

W wyroku z wyrok TK z 8 września 2005 r., sygn. akt P 17/04 Trybunał Konstytucyjny stwierdził: „Zarzut niezgodności przepisu stanowiącego przedmiot zaskarżenia z Konstytucją, ratyfikowaną umową międzynarodową lub ustawą powinien być poparty przytoczeniem argumentów podważających domniemanie konstytucyjności przepisu. Pytanie prawne [takie same wymogi formalne odnoszą się do wniosku – uwaga własna], w którym przedstawiający je sąd ograniczyłby się do wyrażenia przekonania o niezgodności zaskarżonego przepisu z Konstytucją, a tym bardziej tylko ogólnie powołał się na istniejące w tej kwestii wątpliwości, nie mogłoby być rozpoznane przez Trybunał Konstytucyjny”. Wnioskodawca powinien wskazać precyzyjnie co najmniej jeden argument za naruszeniem określonych wzorców kontroli, który ma znaczenie konstytucyjne, to znaczy może być uwzględniony w toku kontroli konstytucyjności prawa (zob. wyrok TK z 31 lipca 2015 r.). Trybunał wyjaśniał, że „nie realizują omawianych wymagań uwagi nazbyt ogólne, niejasne czy też czynione jedynie na marginesie innych rozważań” (wyrok TK z 5 czerwca 2014 r., sygn. akt K 35/11).

2. Rzecznik Praw Obywatelskich poprzestał na sformułowaniu tezy o niezgodności zaskarżonych przepisów z wzorcami kontroli. Natomiast nie opatrzył sformułowanego zarzutu szczegółowym uzasadnieniem, które wykraczając poza ogólną konstatację o sprzeczności z normami wyższego rzędu pozwoliłoby na merytoryczne odniesienie się przez Sejm.

Argumenty przedstawione przez wnioskodawcę nie wykraczają bowiem poza stanowisko o „nieproporcjonalnie długotrwałym stosowaniu kontroli operacyjnej” prowadzącym do naruszenia zasady demokratycznego państwa prawnego, w tym w szczególności wynikającej z niej zasady zaufania obywateli do państwa oraz zasady praworządności. W odniesieniu do tej ostatniej zasady za nazbyt lakoniczne należy uznać stwierdzenie RPO, że: „Przekazanie obywatelom komunikatu, że mogą być inwigilowani przez służby policyjne i służby państwowe przez osiemnaście miesięcy z pewnością nie buduje relacji zaufania między państwem a obywatelami”.

Równie ogólny jest pogląd, iż „czas prowadzenia czynności z zakresu kontroli operacyjnej przekracza ramy konieczne w demokratycznym państwie prawa”.

Także w stosunkowo obszernej części uzasadnienia wniosku odnoszącej się do poszczególnych praw i wolności konstytucyjnych (wynikających z aktów prawa międzynarodowego) próżno szukać argumentów spełniających standardy wynikające z orzecznictwa Trybunału Konstytucyjnego. Rzecznik Praw Obywatelskich nie idzie bowiem w swojej analizie dalej niż poza ogólne twierdzenia, że m.in.: „długie osiemnastomiesięczne okresy prowadzenia kontroli przez ww. służby stanowią naruszenie art. 49 Konstytucji”; „kryterium rozsądnych granic czasowych, wynikającego z art. 51 ust. 2 Konstytucji nie spełniają przepisy ustaw wskazanych w petitum wniosku”; „przepisy kwestionowane w tej części wniosku, w zakresie, w jakim ustalają czas trwania kontroli operacyjnej łącznie na osiemnaście miesięcy nie spełniają kryterium konieczności”; „trudno jest przyjąć, że służby policyjne i służby specjalne potrzebują aż osiemnastu miesięcy na zebranie materiałów uzasadniających wszczęcie postępowania karnego”.

W kontekście postawionego zarzutu za niedostateczne należy uznać także poprzestanie na odwołaniu się do orzecznictwa ETPCz, w którym Trybunał „*expressis verbis* wskazał, że przepisy muszą określać czas trwania inwigilacji”. Skoro bowiem ustawodawca unormował w zaskarżonych przepisach maksymalny czas trwania kontroli operacyjnej, to prowadzona argumentacja nie może poprzestać na zrekonstruowaniu konstytucyjnego (konwencyjnego) wymogu zakreślenia owych ram czasowych.

3. Trzeba zatem przypomnieć, że ustanowienie przepisów regulujących prowadzenie kontroli operacyjnej można ujmować jako obowiązek ustawodawcy znajdującym konstytucyjne zakotwiczenie przede wszystkim w art. 5 Konstytucji, który stanowi że: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju”. Jest zatem oczywiste, że prawodawca musi wyposażyć służby powołane do realizowania zadań w zakresie szeroko rozumianego bezpieczeństwa publicznego w określone kompetencje realizowane w adekwatnym otoczeniu normatywnym. Jak trafnie zauważył Trybunał Konstytucyjny, „brak wyposażenia służb policyjnych oraz służb ochrony państwa w możliwość korzystania ze zdobyczy nowoczesnej techniki, a nawet wyposażenie

ich w taką możliwość, lecz w niewystarczającym zakresie, może oznaczać niewywiązanie się państwa z jego konstytucyjnego zadania strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli (art. 5 Konstytucji), czy naruszać zasadę sprawności działania instytucji publicznych (wstęp do Konstytucji). Niekiedy może powodować naruszenie obowiązków wiążących Polskę umów międzynarodowych zobowiązujących do współdziałania w walce z międzynarodową przestępczością i terroryzmem” (wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11).

Z drugiej zaś strony ustawodawca dysponuje w omawianym zakresie swobodą kształtowania i doboru środków służących realizacji wspomnianych wartości konstytucyjnych. W odniesieniu do czasu trwania niejawnego pozyskiwania informacji o jednostce, w tym za pomocą środków kontroli operacyjnej w orzecznictwie Trybunału zwraca się uwagę na wymóg określenia maksymalnego terminu po upływie którego takie pozyskiwanie danych jest niedopuszczalne – „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” (*ibidem*).

W ocenie Sejmu wnioskodawca powinien zatem przedstawić uzasadnienie krytycznej oceny czasowych ograniczeń prowadzenia kontroli operacyjnej, uwzględniając z jednej strony konieczność stworzenia systemu uprawnień służb pozwalającego na efektywne osiąganie konstytucyjnych celów z drugiej zaś nie tracąc z pola widzenia swobody ustawodawcy w tym zakresie. Poza rolę uczestnika postępowania zajmowaną przez Sejm wykracza wskazywanie wnioskodawcy obszarów analiz i zagadnień, które winny zostać uwzględnione przy formułowaniu postawionego zarzutu. Nie można jednak nie zauważyć, że Rzecznik zaniechał przedstawienia jakiegokolwiek argumentacji rozwijającej i uprawdopodobniającej sygnalizowaną niekonstytucyjność. W szczególności nie odniósł się do zadań realizowanych przez poszczególne służby – w tym do specyfiki popełniania przestępstw, których rozpoznawaniu i zapobieganiu służyć mają czynności operacyjne, zróżnicowanego charakteru dowodów, rozciągnięcia w czasie działań sprawczych – wykazując tym samym ogólną albo tylko częściową nieproporcjonalność regulacji ustawowych.

Uwagę zwraca również pominięcie roli sądu w przedłużaniu prowadzonej kontroli, która jest wszak zarządzana na krótsze okresy a każdorazowe jej

przedłużenie wymaga należytego uzasadnienia. Dalsze prowadzenie kontroli operacyjnej może być uzasadnione wyłącznie pojawieniem się nowych okoliczności istotnych dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa. *A contrario*, jeżeli organ wnioskujący nie wskaże takiej okoliczności, sąd nie będzie mógł uwzględnić wniosku. W grę nie wchodzi zatem niejako „profilaktyczne” stosowanie kontroli operacyjnej, nakierowane na zarejestrowanie okoliczności, które nie były znane w momencie jej zarządzania i wystąpienia z wnioskiem o przedłużenie kontroli, a które mogą wystąpić w bliżej nieokreślonej przyszłości. W tym kontekście należy przypomnieć o subsydiarnym charakterze tej metody pozyskiwania informacji oraz podkreślić, że w przypadku przepisów, które ograniczają prawa i wolności obywatelskie, należy dokonywać ich wykładni w sposób ścisły, a w przypadku wątpliwości co do treści normy w nich zawartej stosować – konstytucyjnie zakotwiczoną – regułę *in dubio pro libertate* (zob. np. wyrok TK z 27 czerwca 2008 r., sygn. akt K 52/07; postanowienie TK z 25 stycznia 2005 r., sygn. akt Ts 109/04; wyrok SN z 3 lipca 2013 r., sygn. akt V KK 412/12; L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 163-164)

Wreszcie Rzecznik Praw Obywatelskich w żaden sposób nie odniósł się do uzasadnienia projektu ustawy zmieniającej, w którym wskazano, że „projektowane określenie maksymalnego czasu prowadzenia kontroli operacyjnej pozostaje w zbieżności z regulacją art. 180a ust.1 pkt 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, przewidującą obowiązek operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych zatrzymywania i przechowywania, na własny koszt, danych, o których mowa w art. 180c ustawy, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Oceny zasadności przechowywania przez okres 12 miesięcy danych telekomunikacyjnych należy dokonać przez pryzmat możliwości ich skutecznego wykorzystania w realizowanych działaniach operacyjno-rozpoznawczych. Należy podkreślić, iż w ramach rozpoznawania, zapobiegania i wykrywania przestępstw, w tym w szczególności o charakterze szpiegowskim, terrorystycznym, czy udziału w zorganizowanej grupie lub związku przestępczym, ważną rolę odgrywa praca analityczna. Uzyskanie informacji o określonej, niezgodnej z prawem działalności, uruchamia proces analityczny, którego jednym z ważnych celów jest wykazanie genezy rozpoznawanych powiązań przestępczych. Powyższe pozwala (np. w przypadku przestępstwa szpiegostwa) na określenie potencjalnych szkód wyrządzonych taką działalnością. Priorytetową rolę w tym zakresie odgrywają

dane telekomunikacyjne, pozwalające niejednokrotnie na wychwycenie okresu nawiązania współpracy w ramach niezgodnej z prawem działalności. Dane telekomunikacyjne pozwalają również we właściwy sposób zaplanować kolejne – niejednokrotnie złożone – czynności operacyjno-rozpoznawcze w celu neutralizacji istniejących zagrożeń”.

5. Mając powyższe na uwadze, Sejm stwierdza, że wnioskodawca nie uzasadnił postawionego zarzutu w sposób zgodny z wymogami postępowania przed Trybunałem Konstytucyjnym. Jak już wspomniano, ustawa o TK wymaga spełnienia przez podmiot inicjujący postępowanie przed Trybunałem dwóch odrębnie wyrażonych wymogów. Po pierwsze, określenia problemu konstytucyjnego i zarzutu niekonstytucyjności. Po drugie, wskazania argumentów lub dowodów na poparcie zarzutu niekonstytucyjności. W ocenie Sejmu poglądy i przekonania wyrażone w uzasadnieniu wniosku RPO nie mogą zostać uznane za relewantne procesowo argumenty, co uniemożliwia merytoryczną ocenę postawionego zarzutu. Z powyższych względów postępowanie w części obejmującej zarzut postawiony w pkt I petitum wniosku RPO powinno zostać **umorzone** na podstawie art. 59 ust. 1 pkt ustawy o TK ze względu na niedopuszczalność wydania wyroku.

III. Wykorzystywanie materiałów kontroli operacyjnej zawierających prawnie chronione tajemnice

III.1. Przedmiot kontroli

1. Rzecznik Praw Obywatelskich zakwestionował przepisy ustaw o służbach policyjnych i bezpieczeństwa, które stanowią odpowiednio.

Artykuł 19 ust. 15h ustawy o Policji: „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 [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 – uwaga własna], 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”.

Artykuł 9 ust. 16h ustawy o SG: „Sąd, niezwłocznie po złożeniu wniosku przez prokuratora, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 16g pkt 2 [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 – uwaga własna], 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”.

Artykuł 36d ust. 1h ustawy o kontroli skarbowej: „Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe materiałów, o których mowa w ust. 1g pkt 2 [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 – uwaga własna], 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 w sprawie o przestępstwo lub przestępstwo skarbowe jest niedopuszczalne”.

Artykuł 31 ust. 16h ustawy o ŻW: „Sąd, niezwłocznie po złożeniu wniosku przez prokuratora do spraw wojskowych, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 16g pkt 2 [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 – uwaga własna], 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”.

Artykuł 27 ust. 15j ustawy o ABW: „Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 15i pkt 2 [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 – uwaga własna], 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”.

Artykuł 31 ust. 14h ustawy o SKW: „Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 14g pkt 2 [materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, nieobjęte zakazami określonymi w art. 178a i art. 180 § 3 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny – uwaga własna], 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.

Artykuł 17 ust. 15h ustawy o CBA: „Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 15g pkt 2 [materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego, nieobjęte zakazami określonymi w art. 178a i art. 180 § 3 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny – uwaga własna], 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”.

2. Wnioskodawca zakwestionował konstytucyjność wspomnianych przepisów 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 k.p.k..

III.2. Zarzuty wnioskodawcy

W ocenie Rzecznika Praw Obywatelskich standardom konstytucyjnym uchybiają zasady wykorzystywania – uzyskanych w toku kontroli operacyjnej – materiałów, zawierających dowody pozwalające na wszczęcie postępowania karnego lub mających znaczenie dla już toczącego się postępowania. Jeżeli materiały zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. (chodzi tu o tajemnice: notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną), 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 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2016 r., poz. 1137), decyzję o ich dopuszczeniu do wykorzystania w postępowaniu karnym podejmuje sąd na wniosek prokuratora. Sąd może podjąć owo rozstrzygnięcie tylko, „gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu”.

Zdaniem wnioskodawcy wymienione przesłanki są nieprecyzyjne i przez to uchybiają przywołanym wzorcom kontroli. Niepokój RPO wzbudza w szczególności wprowadzenie „abstrakcyjnej wartości w postaci dobra wymiaru sprawiedliwości jako kryterium dopuszczalności wykorzystania w postępowaniu karnym informacji uzyskanych za pomocą naruszenia tajemnicy zawodowej”.

III.3. Analiza formalnoprawna

1. Wskazany jako wzorzec kontroli art. 6 EKPCz nie został opatrzony jakimkolwiek komentarzem w części wniosku RPO zawierającej uzasadnienie

omawianego w zarzutu. Nie można zatem przyjąć, że w zakresie wspomnianego wzorca konwencyjnego wnioskodawca prawidłowo zrealizował nakaz przedstawienia argumentów na poparcie wysuwanego zarzutu. Wobec powyższego Sejm wnosi o **umorzenie postępowania** na podstawie 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku w części obejmującej badanie zgodności przepisów wymienionych w pkt II petitum wniosku RPO z art. 6 EKPCz.

Nawet gdyby przyjąć, że wnioskodawca dąży do wykazania naruszenia wzorców konstytucyjnych i konwencyjnych tym samym uzasadnieniem bez wyraźnego ustosunkowania się do każdego z nich, zajęcie względem art. 6 EKPCz nie jest, zdaniem Sejmu, celowe. Wnioskodawca nie wywiódł z przepisu EKPCz treści szerszych niż z przywołanego jako wzorzec art. 42 ust. 2 Konstytucji. W takiej sytuacji – jak wskazuje dotychczasowy dorobek Trybunału Konstytucyjnego (por. wyroki TK z: 17 grudnia 2008 r., sygn. akt P 16/08; 10 lipca 2008 r., sygn. akt P 15/08; 27 maja 2008 r., sygn. akt P 59/07; 18 października 2004 r., sygn. akt P 8/04, a także odnoszący się w tym względzie do Konwencji o prawach osób niepełnosprawnych wyrok TK z 23 stycznia 2014 r., sygn. akt K 51/12) – należy uznać, że oddzielne orzekanie o zgodności zaskarżonej regulacji z prawem międzynarodowym jest zbędne, co również nakazywałoby umorzenie postępowania w tym zakresie na.

2. Wnioskodawca uczynił wzorcem kontroli także art. 2 Konstytucji. Uzasadnienie naruszenia wymienionego przepisu ustawy zasadniczej jest jednak lakoniczne. Rzecznik Praw Obywatelskich odwołał się do niego dwukrotnie. Po pierwsze, stwierdzając że zaskarżone przepisy zdają się „naruszać w sposób rażący wyrażoną w art. 2 zasadę demokratycznego państwa prawnego”. Po drugie, wskazując, że „niedookreśloność 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”.

Mając zatem na uwadze, że w orzecznictwie Trybunału Konstytucyjnego zasada demokratycznego państwa prawnego jest traktowana jako zbiorcze ujęcie reguł, które wprawdzie nie zostały *expressis verbis* wyrażone w tekście Konstytucji, ale w sposób immanentny wynikają z aksjologii oraz istoty demokratycznego państwa prawnego (zob. wyrok TK z 26 lutego 2003 r., sygn. akt K 1/01; postanowienie TK z 14 grudnia 2004 r., sygn. akt SK 29/03), Sejm uznaje, że

wskazanie przez RPO na zasadę ochrony zaufania do państwa i stanowionego przez nie prawa stanowi konkretyzację zarzutu naruszenia ogólnie ujmowanej zasady demokratycznego państwa prawnego. W orzecznictwie Trybunału nie budzi bowiem wątpliwości, że zasada ta, choć niewystawiona w tekście Konstytucji niewątpliwie należy do kanonu zasad składających się na pojęcie państwa prawnego w znaczeniu, w jakim pojęcie to występuje w art. 2 Konstytucji (zob. np. wyroki TK z: 20 grudnia 1999 r., sygn. akt K 4/99; 24 lutego 2010 r., sygn. akt K 6/09; 18 października 2015 r., sygn. akt K 21/14).

3. Na marginesie należy zaznaczyć, że Sejm zmodyfikuje zaproponowany przez RPO zakres zaskarżenia przepisów ujętych w pkt II jego wniosku. Nie ma bowiem potrzeby, aby Trybunał orzekał co do konstytucyjności zaskarżonych przepisów w zakresie, w jakim posługują się one „nieostrym kryterium” dobra wymiaru sprawiedliwości. Owa nieostrość stanowi bowiem podstawę ewentualnego stwierdzenia przez Trybunał, że ustawodawca, posługując się pojęciem „dobra wymiaru sprawiedliwości” uchybił przepisom Konstytucji. Dlatego też Sejm w odnośnej części wniosku Sejm formułowanego w niniejszym postępowaniu Sejm – bez uszczerbku dla intencji RPO – pominie tę część pierwotnego zakresu zaskarżenia.

III.4. Wzorce kontroli

III.4.2. Zasada ochrony zaufania do państwa i stanowionego przez nie prawa (art. 2 Konstytucji)

1. Zgodnie z art. 2 Konstytucji: „Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej”. Zasada ochrony zaufania do państwa i stanowionego przez nie prawa określana jest w orzecznictwie Trybunału także jako zasada lojalności państwa wobec adresata norm prawnych. W wyroku z 15 lutego 2005 r. (sygn. akt K 48/04) Trybunał Konstytucyjny wskazał m.in., że zasada ta wyraża się: „[...] w stanowieniu i stosowaniu prawa w taki sposób, by nie stawało się ono swoistą pułapką dla obywatela, który powinien móc układać swoje sprawy w zaufaniu, że nie naraża się na prawne skutki niedające się przewidzieć w momencie podejmowania decyzji i że jego działania są zgodne z obowiązującym prawem oraz także w przyszłości będą

uznawane przez porządek prawny. Przyjmowane przez ustawodawcę nowe unormowania nie mogą zaskakiwać ich adresatów, którzy powinni mieć czas na dostosowanie się do zmienionych regulacji i spokojne podjęcie decyzji co do dalszego postępowania” (por. także m.in. wyrok TK z 25 listopada 1997 r., sygn. akt K 26/97).

Podobnie Trybunał wypowiedział się w wyroku z 25 kwietnia 2001 r. (sygn. akt K 13/01), w którym – podtrzymując swoje wcześniejsze stanowisko – stwierdził, że analizowana zasada opiera się na pewności prawa, a więc „takim zespole cech przysługujących prawu, które zapewniają jednostce bezpieczeństwo prawne; umożliwiają jej decydowanie o swoim postępowaniu w oparciu o pełną znajomość przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie ich działania mogą pociągnąć za sobą. Jednostka winna mieć możliwość określenia zarówno konsekwencji poszczególnych zachowań i zdarzeń na gruncie obowiązującego w danym momencie stanu prawnego jak też oczekiwać, że prawodawca nie zmieni ich w sposób arbitralny. Bezpieczeństwo prawne jednostki związane z pewnością prawa umożliwia więc przewidywalność działań organów państwa, a także prognozowanie działań własnych. W ten sposób urzeczywistniana jest wolność jednostki, która według swoich preferencji układa swoje sprawy i przyjmuje odpowiedzialność za swoje decyzje, a także jej godność, poprzez szacunek porządku prawnego dla jednostki, jako autonomicznej, racjonalnej istoty [...]. Wartości te, przy zmianie prawa, prawodawca narusza wtedy, gdy jego rozstrzygnięcie jest dla jednostki zaskoczeniem, bo w danych okolicznościach nie mogła go przewidzieć, szczególnie zaś wtedy, gdy przy jego podejmowaniu prawodawca mógł przypuszczać, że gdyby jednostka przewidywała zmianę prawa, byłaby inaczej zdecydowała o swoich sprawach” (zob. także np. wyroki TK z: 14 czerwca 2000 r., sygn. akt P 3/00; 7 lutego 2001 r., sygn. akt K 27/00; 19 grudnia 2002 r., sygn. akt K 33/02; 19 listopada 2008 r., sygn. akt Kp 2/08; 10 lutego 2015 r., sygn. akt P 10/11).

2. Zarzuty wysunięte przez RPO dotyczą nie tyle – powszechniejszej w kontekście uchybień zasadzie ochrony zaufania do państwa i stanowionego przez nie prawa – kwestii zaskakującej dla adresata zmiany stanu prawnego, ile poprawności i jasności sformułowania przepisów. Wymóg określoności regulacji prawnej także znajduje swą konstytucyjną podstawę w zasadzie demokratycznego państwa prawnego. Odnosi się on do wszelkich regulacji (pośrednio czy

bezpośrednio) kształtujących pozycję prawną obywatela. Zasada określoności prawa jest bowiem jedną z dyrektyw prawidłowej legislacji. Stanowi ona także element zasady ochrony zaufania obywatela do państwa i tworzonego przez nie prawa, wynikający z art. 2 Konstytucji (zob. wyroki z TK z: 15 września 1999 r., sygn. akt K 11/99; 11 stycznia 2000 r., sygn. akt K 7/99; 21 marca 2001 r., sygn. akt K 24/00; 30 października 2001 r., sygn. akt K 33/00, 22 maja 2002 r., K 6/02, 20 listopada 2002 r., K 41/02; 3 grudnia 2002 r., sygn. akt P 13/02, 29 października 2003 r., sygn. akt K 53/02; 9 października 2007 r., sygn. akt SK 70/06; 28 października 2009 r.; sygn. akt K 32/08; 29 maja 2012 r., sygn. akt SK 17/09; 29 lipca 2014 r., sygn. akt P 49/13).

Zgodnie z zasadą określoności przepisy prawa powinny być formułowane w sposób precyzyjny i jasny oraz poprawny pod względem językowym. Wymóg jasności oznacza obowiązek tworzenia przepisów 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 ich wyegzekwowanie. Jak stwierdził Trybunał, z zasady określoności „[...] wynika nakaz stanowienia przepisów prawa w sposób dostatecznie precyzyjny i jasny, umożliwiający jednoznaczną ich wykładnię oraz konstruowanie na gruncie tych przepisów dostatecznie precyzyjnych norm prawnych, jeśli przepisy te mają za zadanie taką funkcję normotwórczą spełniać” (zob. wyrok TK z 7 kwietnia 2011 r., sygn. akt K 4/09, a także wyroki TK z: 15 września 1999 r., sygn. akt K 11/99; 11 stycznia 2000 r., sygn. akt K 7/99; 20 listopada 2002 r., sygn. akt K 41/02).

III.4.2. Prawo do obrony (art. 42 ust. 2 Konstytucji)

Artykuł 42 ust. 2 Konstytucji stanowi: „Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu”.

Jak wskazuje się w doktrynie prawa, prawo do obrony, występujące w postępowaniu karnym, oznacza możliwość podejmowania wszelkich działań niesprzecznych z prawem, które w przekonaniu osoby poddanej temu postępowaniu potwierdzają jej wersję zdarzeń (w trakcie których dojść miało do popełnienia

zarzucanego czynu) oraz jej niewinność lub występowanie określonego charakteru winy (zob. P. Sarnecki, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. III, Warszawa 2003, komentarz do art. 42, s. 8). Użyte przez ustrojodawcę wyrażenie „we wszystkich stadiach postępowania” oznacza, że prawo do obrony powinno występować „zarówno w stadiach przedjudykacyjnych, jak i przed organami orzekającymi, w tym i przed sądami wszystkich instancji. We wszystkich tych stadiach występuje ono w takim samym pełnym zakresie, niezależnie od tego, że nie wszystkie z tych stadiów mogą kończyć się takim czy innym orzeczeniem” (*ibidem*).

Prawo do obrony było również przedmiotem licznych orzeczeń Trybunału Konstytucyjnego.

W wyroku z 9 lipca 2009 r. (sygn. akt K 31/08) sąd konstytucyjny wskazał, że „konstytucyjne prawo do obrony należy rozumieć szeroko, jest ono bowiem nie tylko fundamentalną zasadą procesu karnego, ale także elementarnym standardem demokratycznego państwa prawnego. Prawo to przysługuje każdemu od chwili wszczęcia przeciwko niemu postępowania karnego (w praktyce od chwili przedstawienia zarzutów) aż do wydania prawomocnego wyroku, obejmuje również etap postępowania wykonawczego [...]”.

Prawo do obrony może być rozpatrywane w dwóch aspektach: materialnym i formalnym. Obrona materialna to możliwość bronięcia przez oskarżonego jego interesów osobiście (np. możliwość odmowy składania wyjaśnień, prawo wglądu w akta i składania wniosków dowodowych) – zob. przykładowo wyrok TK z 9 lipca 2009 r. (sygn. akt K 31/08). Natomiast w wyroku z 8 listopada 2004 r. (sygn. akt K 38/03) sąd konstytucyjny stwierdził za przedstawicielami doktryny prawa, że istota prawa do obrony w aspekcie materialnym przejawia się w możliwości „podejmowania wszelkich niesprzecznych z prawem działań (czynności procesowych) w celu obrony oskarżonego bądź podejrzanego przed stawianymi zarzutami oraz grożącymi konsekwencjami prawnymi (por. A. Murzynowski, *Istota i zasady procesu karnego*, Warszawa 1994, s. 272 [...])”.

Z kolei przez obronę w aspekcie formalnym należy rozumieć prawo do korzystania z obrońcy z wyboru lub z urzędu (zob. przykładowo wyrok TK z 9 lipca 2009 r., sygn. akt K 31/08). Jak wskazał Trybunał Konstytucyjny w wyroku z 17 lutego 2004 r. (sygn. akt SK 39/02): „Obrońca jest pełnomocnikiem oskarżonego, jego procesowym przedstawicielem, a jego głównym zadaniem jest ochrona oskarżonego w taki sposób, by cel procesu karnego osiągnięty został

z zagwarantowaniem prawa do obrony. Charakter działań obrońcy determinowany jest interesem prawnym oskarżonego, dla którego ochrony przepisy procedury karnej przewidują szereg koniecznych uprawnień. [...] Proces karny jest ze swej istoty kontradiktoryjny, stanowi on spór równouprawnionych stron przed bezstronnym sądem. W postępowaniu przygotowawczym, którym kieruje prokurator, owa kontradiktoryjność jest w pewnym zakresie ograniczona, co nie oznacza jednak, iż owe ograniczenia mogą naruszać istotę prawa do obrony” (por. też m.in. wyrok TK z 19 marca 2007 r., sygn. akt K 47/05).

W ramach konstytucyjnego prawa do obrony wyróżnić można szereg uprawnień, przysługujących zarówno oskarżonemu (podejrzanemu), jak i jego obrońcy (nie ulega wątpliwości, że beneficjentami stosownych uprawnień wynikających z prawa do obrony jest zarówno sam oskarżony, jak i jego obrońca, a ich uprawnienia pozostają w ścisłym związku. W realiach niniejszej sprawy należy zwrócić szczególną uwagę na jedno z nich, a mianowicie prawo do kontaktu oskarżonego (podejzranego) ze swoim obrońcą. Jest ono dostrzegane w orzecznictwie Trybunału Konstytucyjnego, który z perspektywy uprawnień obrońcy stwierdza: „Uprawnienia obrońcy to nie tylko możliwość przeglądania akt postępowania karnego – zapoznawania się z materiałem dowodowym, ale przede wszystkim kontakt z jego mocodawcą. To na podstawie osobistego kontaktu, obrońca pozyskuje faktyczną wiedzę o czynie sprawcy oraz okolicznościach zdarzenia będącego przedmiotem postępowania, buduje strategię obrony, zgłasza wnioski dowodowe i współdziała z innymi obrońcami występującymi w sprawie” (wyrok TK z 17 lutego 2004 r., sygn. akt SK 39/02).

Należy podkreślić, że standard konstytucyjny wymaga, aby kontakt oskarżonego (podejzranego) ze swoim obrońcą był co do zasady kontaktem swobodnym (zob. wyrok TK z 17 lutego 2004 r., sygn. akt SK 39/02). Oznacza to, że porozumiewanie się obrońcy i jego klienta powinno być nieskrępowane, wolne od kontroli i innych, nadmiernych utrudnień.

W wyroku z 30 lipca 2014 r. (sygn. akt K 23/11) Trybunał, podkreślając wagę poufnego charakteru kontaktów oskarżonego z obrońcą stwierdził: „Doniosłość tajemnicy obrończej jako gwarancji konstytucyjnego prawa do obrony, a zarazem konieczność jej intensywniejszej ochrony, wiąże się [...] ze szczególną specyfiką procesu karnego, w ramach którego są rozstrzygane kwestie istotne z punktu widzenia statusu jednostki, jak kwestia pozbawienia wolności osobistej i korzystania z praw publicznych. Mając to na uwadze, w orzecznictwie Trybunału

Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka wielokrotnie wskazywano, że dla efektywnego korzystania z pomocy obrońcy niezbędne jest zachowanie poufności komunikatów przekazywanych obrońcy przez oskarżonego (podejrzanego) [...] Brak możliwości poufnego porozumiewania się oskarżonego ze swoim obrońcą, również za pośrednictwem technologii teleinformatycznych, oznacza, że pomoc prawna traci dużo ze swej skuteczności. Obawiając się niejawnego kontroli rozmów z obrońcą, oskarżony może wszakże zaniechać korzystania z profesjonalnej pomocy prawnej lub nie przekazywać obrońcy istotnych okoliczności sprawy. [...] w takiej sytuacji, obrońca – nie mogąc pozyskać pełni wiedzy o okolicznościach sprawy – nie jest w stanie udzielić pomocy prawnej w najkorzystniejszej dla klienta formie. W konsekwencji taki stan rzeczy może utrudnić skuteczne konstruowanie linii obrony, prowadząc nawet do niesłusznego skazania. Świadomość niejawnego monitorowania kontaktów oskarżonego z obrońcą osłabia również więź zaufania, która jest niezbędna dla prawidłowego wykonywania funkcji obrońcy oraz efektywnej realizacji prawa do obrony. Zapewnienie poufności rozmów oskarżonego z obrońcą jest konieczne nie tylko na etapie postępowania sądowego, lecz w każdej fazie postępowania, nawet prowadzonej przez organ pozasądowy (prokuratora, policję, służbę ochrony państwa). Naruszenie prawa do obrony w fazie przedsądowej może się bowiem przekładać na nierzetelność postępowania sądowego.

2. Wyrażone w art. 42 ust. 2 Konstytucji prawo do obrony nie ma charakteru absolutnego (zob. np. wyroki TK z: 3 czerwca 2008 r., sygn. akt K 42/07; 9 lipca 2009 r., sygn. akt K 31/08). Tym samym podlega ono limitowaniu, jednakże na warunkach określonych w art. 31 ust. 3 ustawy zasadniczej.

Przepis art. 31 ust. 3 Konstytucji formułuje następujące, kumulatywnie ujęte, przesłanki dopuszczalności ograniczeń w korzystaniu z konstytucyjnych praw i wolności: 1) ustawowa forma ograniczenia; 2) istnienie w państwie demokratycznym konieczności wprowadzenia ograniczenia; 3) funkcjonalny związek ograniczenia z realizacją wskazanych w art. 31 ust. 3 wartości (bezpieczeństwo państwa, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, wolności i praw innych osób); 4) zakaz naruszania istoty danego prawa lub wolności (zob. np. L. Garlicki [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. III, Warszawa 2003, komentarz do art. 31, s. 14 i n.).

W kontekście zakazu naruszania istoty konstytucyjnego prawa do obrony trzeba podkreślić, że „możliwość niejawnego uzyskiwania informacji objętych

tajemnicą obrończą, samo w sobie, nie narusza jeszcze istoty prawa do obrony (oskarżony może bowiem korzystać z pomocy prawnej obrońcy, komunikując się z nim osobiście bez wykorzystywania takich kanałów komunikacji, które mogą być objęte kontrolą operacyjną)”, a „minimalnym standardem w odniesieniu do ochrony poufności kontaktów oskarżonego z obrońcą i poufności tożsamości dziennikarskich źródeł informacji jest istnienie kontroli sądowej weryfikującej zebrane przez Policję w toku czynności operacyjno-rozpoznawczych materiały, co do których istnieje uzasadnione prawdopodobieństwo, że zawierają treści stanowiące prawnie chronioną tajemnicę zawodową, oraz zarządzającej wyłączenie z dalszego wykorzystania tych materiałów, które są istotne z punktu widzenia ochrony relacji zaufania” (wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11).

III.4.3. Prawo do prywatności, wolność komunikowania się, autonomia informacyjna jednostki

1. Artykuł 47 Konstytucji stanowi: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”.

Jak zauważył Trybunał Konstytucyjny: „Art. 47 konstytucji określa prawo każdego do ochrony życia prywatnego i rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Oznacza, iż państwo zobowiązuje się z jednej strony do nieingerencji w konstytucyjnie określony zakres życia jednostek, a z drugiej strony zapewnia stosowną ochronę w przypadku, gdy działania takie zostały już podjęte” (wyrok TK z 2 kwietnia 2001 r., sygn. akt SK 10/00; por. wyrok TK z 9 lipca 2009 r., sygn. akt SK 48/05). „Koncepcja prawa do prywatności zaczęła stosunkowo niedawno odgrywać poważniejszą rolę w regulacjach konstytucyjnych i orzecznictwie sądowym. Zdołała już jednak zyskać sobie trwałe miejsce we współczesnych państwach demokratycznych. Stanowią ją zasady i reguły odnoszące się do różnych sfer życia jednostki, a ich wspólnym mianownikiem jest przyznanie jednostce prawa «do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej» (A. Kopff, *Koncepcje prawa do intymności i do prywatności życia. Zagadnienia konstrukcyjne*, Studia Cywilistyczne, t. XX/1972). Tak rozumiana prywatność odnosi się przede wszystkim do życia osobistego, rodzinnego, towarzyskiego i czasem jest określana jako «prawo do pozostawienia w spokoju» (zob. W. Sokolewicz, *Prawo do*

prywatności [w:] *Prawa człowieka w Stanach Zjednoczonych*, Warszawa 1985, s. 252). Na ogół przyjmuje się, że prywatność odnosi się też do ochrony informacji dotyczących danej osoby i gwarantuje m.in. pewien stan niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu” (orzeczenie TK z 24 czerwca 1997 r., sygn. akt K 21/96). Konstytucyjną ochroną wynikającą z art. 47 Konstytucji objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej (wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11).

Niewątpliwie posługiwanie się niejawnymi sposobami pozyskiwania informacji o jednostce stanowi jedną z najgłębszych ingerencji w konstytucyjne prawo do prywatności, którego źródłem jest godność człowieka: „Związek między zagrożeniem godności człowieka, spoczywającej u podstaw wszystkich konstytucyjnych wolności i praw jednostki a czynnościami operacyjnymi, które wkraczają w prywatność jednostki – jest powszechnie podkreślany, zarówno w piśmiennictwie, jak i w europejskim (w tym polskim) *acquis constitutionnel*. Wszelkie prawa i wolności konstytucyjne jednostki wywodzą się z godności. W wypadku prywatności (która – na poziomie konstytucyjnym – jest chroniona wieloaspektowo, poprzez kilka praw i wolności – por. art. 47-51) związek ten jest szczególnie, jakkolwiek nie taki sam w wypadku każdej z tych konstytucyjnych wolności i praw. Zachowanie przez człowieka godności wymaga bowiem poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność «bycia z innymi» czy «dzielenia się z innymi»

swoimi przeżyciami czy doznaniem o intymnym charakterze” (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04).

2. Zgodnie z 49 Konstytucji: „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony”.

W piśmiennictwie wskazuje się niekiedy, że wolność komunikowania się dotyczy raczej porozumiewania się za pomocą pewnego środka przekazu, nie zaś bezpośredniej rozmowy osób w jakimś miejscu, albowiem to ostatnie jest raczej wyrazem prawa do prywatności (zob. P. Sarnecki, [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz, t. III, red. L. Garlicki, Warszawa 2007, komentarz do art. 49, s. 3). Trybunał Konstytucyjny przyjmuje jednak szersze rozumienie wolności komunikowania się, nie przeciwstawiając jej tak kategorycznie prawu do ochrony prywatności (zob. wyroki TK z: 12 grudnia 2005 r., sygn. akt K 32/04, 30 lipca 2014 r., sygn. akt K 23/11). Konstytucyjną ochroną wynikającą z art. 49 Konstytucji objęta jest tym samym treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania się na odległość. Według Trybunału, „przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzysobowe” (wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04). Z punktu widzenia prawa do ochrony tajemnicy komunikowania się (art. 49 Konstytucji) „sposób porozumiewania się istotny jest tylko o tyle, o ile jego zastosowanie w danych warunkach (okolicznościach) pozbawia osoby trzecie, które nie są adresatami danych treści, możliwości zapoznania się z nimi. Tylko wtedy bowiem można sensownie mówić o istnieniu jakiejś «tajemnicy», którą można byłoby objąć ochroną. W konsekwencji, w tym jedynie znaczeniu forma komunikacji może mieć in casu wpływ na zakres prawa do ochrony tajemnicy komunikowania się” (wyrok TK z 2 lipca 2007 r., sygn. akt K 41/05).

Podsumowując trzeba zatem podkreślić, że wszelkie sposoby komunikowania się, bez względu na sposób przekazywania informacji, podobnie jak okoliczności procesu porozumiewania się, objęte są konstytucyjną ochroną. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której ochrona ta byłaby samoistnie ograniczona (zob. np. wyrok TK z 30 lipca 2014 r., sygn. K 23/11).

3. Artykuł 51 ust. 2 Konstytucji stanowi: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym”.

Autonomia informacyjna, wskazana w art. 51 Konstytucji, jest jednym z komponentów prawa do prywatności w szerokim znaczeniu, przyjętym w art. 47 Konstytucji (zob. wyroki TK z: 20 marca 2006 r., sygn. akt K 17/05; 22 lipca 2014 r., sygn. akt K 25/13; 18 grudnia 2014 r., sygn. akt K 33/13; 11 października 2016 r., sygn. akt SK 28/15). Obejmuje ona prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących siebie, jak również prawo do kontrolowania tych informacji, jeżeli znajdują się w dyspozycji innych podmiotów. W konsekwencji art. 47 i art. 51 Konstytucji pozostają w określonej relacji wzajemnej: prawo do prywatności, statutowane w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności – *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 – stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych (zob. wyroki TK z: 19 maja 1998 r., sygn. U 5/97; 11 października 2016 r., sygn. akt SK 28/15).

W związku z powyższym Trybunał Konstytucyjny przyjmuje w swoim orzecznictwie, że art. 51 Konstytucji stanowi szczególny środek ochrony tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji. Prywatność dotyczy bowiem także ochrony informacji dotyczących określonej jednostki, w tym ochrony danych osobowych (zob. wyroki TK z: 12 listopada 2002 r., sygn. akt SK 40/01; 13 grudnia 2011 r., sygn. akt K 33/08; 22 lipca 2014 r., sygn. akt K 25/13 oraz 30 lipca 2014 r., sygn. akt K 23/11). Konstytucja w art. 51 ust. 2 realizuje zasadnicze elementy składające się na treść prawa do ochrony życia prywatnego: respekt dla autonomii informacyjnej jednostki, a więc sam obowiązek udostępnienia danych ograniczony do ściśle określonych ustawowo sytuacji; ograniczenie arbitralności ustawodawcy – ustawa nie może zakresu obowiązku kształtować dowolnie (zob. wyroki TK z: 20 czerwca 2005 r., sygn. K 4/04; 11 października 2016 r., sygn. akt SK 28/15).

W wyroku z 11 października 2016 r. (sygn. akt SK 28/15) sąd konstytucyjny stwierdził, że: „Istotą autonomii informacyjnej jest pozostawienie każdej osobie swobody określenia sfery dostępności dla innych wiedzy o sobie. Zasadą powszechnie przyjmowaną wedle takiego ujęcia jest ochrona każdej informacji

osobowej i przyznanie podstawowego znaczenia przesłance zgody osoby zainteresowanej na udostępnienie informacji [...]"

4. Podsumowując należy podkreślić, że: „Konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI. W ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się nadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnie dostępnych. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej” (wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11).

5. Prawo do ochrony życia prywatnego, podobnie jak autonomia informacyjna, nie mają charakteru absolutnego i mogą podlegać ograniczeniom zgodnie z zasadą proporcjonalności (zob. np. wyroki TK z: 11 kwietnia 2000 r., sygn. akt K 15/98; 20 marca 2006 r., sygn. akt K 17/05; 2 lipca 2009 r., sygn. akt K 1/07; 26 lutego 2014 r., sygn. akt K 22/10; 4 listopada 2014 r., sygn. akt SK 55/13).

Już z samej treści art. 51 ust. 2 Konstytucji wynika, że władze publiczne mogą pozyskiwać i udostępniać informacje o obywatelach „niezbędne w demokratycznym państwie prawnym”. Trybunał Konstytucyjna zwraca uwagę, że: „Ustanowienie w art. 51 ust. 2 Konstytucji odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki należy tłumaczyć tym, że naruszenia autonomii informacyjnej w postaci żądania niekoniecznych, lecz wygodnych dla władzy

publicznej, informacji o jednostce, są typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki”, zaś: „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” (wyrok TK z 11 października 2016 r., sygn. akt SK 28/15; por. wyroki TK z: 20 listopada 2002 r., sygn. akt K 41/02; 20 czerwca 2005 r., sygn. akt K 4/04; 17 czerwca 2008 r., sygn. akt K 8/04).

Zawarta art. 51 ust. 2 Konstytucji przesłanka niezbędności gromadzenia informacji o jednostce w demokratycznym państwie prawnym nie jest przesłanką wyłączną, zaś dopuszczalność ograniczenia autonomii informacyjnej zależy również od spełnienia przesłanek wynikających z art. 31 ust. 3 Konstytucji (zob. wyroki TK z: 17 czerwca 2008 r., sygn. akt K 8/04; 22 lipca 2014 r., sygn. akt K 25/13; 18 grudnia 2014 r., sygn. akt K 33/13). „Norma wysłowiona w art. 51 ust. 2 Konstytucji nie ma charakteru całkowicie samodzielnej. 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” (wyrok TK z 17 czerwca 2008 r., sygn. akt K 8/04).

Artykuł 31 ust. 3 Konstytucji („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”) formułuje kumulatywnie ujęte przesłanki dopuszczalności ograniczeń w korzystaniu z konstytucyjnych praw i wolności. Są to: 1) ustawowa forma ograniczenia; 2) istnienie w państwie demokratycznym konieczności wprowadzenia ograniczenia; 3) funkcjonalny związek ograniczenia z realizacją

wskazanych w art. 31 ust. 3 Konstytucji wartości (bezpieczeństwo państwa, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, wolności i praw innych osób); 4) zakaz naruszania istoty danego prawa lub wolności (zob. np. wyrok TK z 30 maja 2007 r., sygn. akt SK 68/06; por. również L. Garlicki [w:] *Konstytucja...*, komentarz do art. 31, s. 14 i n.; J. Zakolska, *Zasada proporcjonalności w orzecznictwie Trybunału Konstytucyjnego*, Warszawa 2008, s. 115-141).

III.5. Analiza merytoryczna

1. W pierwszej kolejności należy zauważyć, że wszystkie zaskarżone przepisy przewidują jednolite zasady włączania do postępowania karnego materiałów kontroli operacyjnej zawierających szczególne informacje. Wymaga przy tym podkreślenia, że RPO doprecyzował zakres kontroli konstytucyjności zakwestionowanych przepisów, dopatrując się ich konstytucyjnej wadliwości w posłużeniu się przez ustawodawcę pojęciem „dobra wymiaru sprawiedliwości” oraz pominięciu wagi okoliczności, które mają być ustalone z pomocą informacji pozyskanych w drodze kontroli operacyjnej. Analiza tak postawionego zarzutu nie wymaga – jak się wydaje – odwoływania się do różnic w uregulowaniach dotyczących poszczególnych służb np. w zakresie przesłanek zarządzania kontroli operacyjnej. Z tego powodu Sejm zaprezentuje konstrukcję owego ustawowego mechanizmu odwołując się *expressis verbis* do postanowień ustawy o Policji.

2. Wszystkie zakwestionowane przepisy regulują zasady wykorzystywania w postępowaniu karnym materiałów, o których mowa w innych jednostkach redakcyjnych zaskarżonych artykułów. I tak w wypadku ustawy o Policji zaskarżony art. 15 ust. 15h odsyła do ust. 15g pkt 2 tej ustawy. Chodzi zatem o materiały zawierające 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.

W celu zdekodowania zawartości normatywnej zakwestionowanych przepisów należy zatem odwołać się do odpowiednich przepisów k.p.k. Jak wspomniano materiały te mają zawierać informacje, które jednocześnie należy traktować jako

tajemnice związane z wykonywaniem określonych zawodów (funkcji), o których mowa w art. 180 § 2 k.p.k.

Artykuł 180 § 2 k.p.k. wylicza natomiast podmioty zobowiązane do zachowania tajemnicy: „notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej”. Spośród wymienionych wyżej należy wyłączyć informacje objęte zakazami dowodowymi określonymi w art. 178a i 180 § 3 k.p.k. Chodzi tu o informacje, które pozyskał mediator od oskarżonego lub pokrzywdzonego prowadząc postępowanie mediacyjne (art. 178a) oraz informacje posiadane przez dziennikarza dotyczące danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych (art. 180 § 3 k.p.k.). Zakazy te nie rozciągają się jednak na dane służące badaniu przestępstwa z art. 240 § 1 k.k. tzn. karalnego niezawiadomienia o karalnym usiłowaniu lub przygotowaniu przestępstw enumeratywnie wymienionych w tym przepisie (poprzez odesłanie do stosownych artykułów k.k.) lub przestępstwa o charakterze terrorystycznym.

Podsumowując można stwierdzić, że zaskarżone przepisy normują zasady wykorzystania w postępowaniu karnym materiałów zawierających tajemnice: notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną z wyłączeniem danych objętych tajemnicą mediacji oraz dziennikarską ochroną źródeł informacji.

Trzeba przy tym zauważyć, że zakwestionowane przepisy wymieniają wyłącznie informacje objęte tajemnicami, o których mowa w art. 180 § 2 k.p.k. Nie zezwalają tym samym na wykorzystanie w postępowaniu karnym danych objętych bezwzględными zakazami dowodowymi z art. 178 k.p.k. a zatem tajemnicą obrończą (*scil.* faktów, o których obrońca albo adwokat lub radca prawny, z którym skontaktował się zatrzymany, dowiedział się udzielając porady prawnej lub prowadząc sprawę) oraz spowiedzi.

3. Wykorzystanie omawianych materiałów w postępowaniu karnym wymaga wystąpienia przez prokuratora z odpowiednim wnioskiem oraz wydania postanowienia przez sąd. Sąd nie jest jednak związany wspomnianym żądaniem i każdorazowo musi ocenić jego merytoryczną zasadność. Ustawodawca wymaga bowiem, by wykorzystanie w postępowaniu karnym materiałów zawierających

omawiane dane było niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

Kwestionowane przez wnioskodawcę sformułowanie „dobra wymiaru sprawiedliwości” nie zostało użyte przez ustawodawcę przypadkowo. Jest to bowiem – na co zwraca uwagę także RPO – kryterium występujące w art. 180 § 1 i § 2 k.p.k. I tak w oparciu o powyższe sąd lub prokurator może zwolnić od obowiązku zachowania tajemnicy względem informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” lub tajemnicy związanej z wykonywaniem zawodu lub funkcji (art. 180 § 1 k.p.k.). Podobnie prezentuje się mechanizm przesłuchiwania osób obowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej, co do faktów objętych tą tajemnicą (180 § 2 k.p.k.). W tym ostatnim wypadku, podobnie jak w świetle zaskarżonych przepisów, z obowiązku zachowania tajemnicy może zwolnić tylko sąd po stwierdzeniu, że dana okoliczność nie może być ustalona na podstawie innego dowodu.

4. Warto zauważyć, że elementy normatywne art. 180 § 2 k.p.k. relewantne w perspektywie zarzutów RPO obowiązują od dłuższego czasu. Fraza „tylko wtedy, gdy to jest niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu” znalazła się już w tekście pierwotnym art. 180 § 2 k.p.k.

Z kolei do art. 181 § 1 k.p.k. kryterium „dobra wymiaru sprawiedliwości” wprowadzono ustawą z dnia 27 września 2013 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 1247). Co szczególnie istotne owa zmiana miała na celu wykonanie wyroku TK z 13 grudnia 2011 r. (sygn. akt K 33/08), w którym stwierdzono, że m.in. art. 180 § 1 k.p.k. jest niezgodny z art. 47 oraz z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej, przez to że nie określa przesłanek zwolnienia od obowiązku zachowania tajemnicy statystycznej. Wymaga odnotowania, że badając konstytucyjność art. 180 § 1 k.p.k. Trybunał analizował również możliwość takiej jego wykładni, która uwzględniałaby kryteria wymienione w art. 180 § 2 k.p.k.: „W obecnym kodeksie postępowania karnego z 1997 r. znajduje się bowiem art. 180 § 2 KPK, który zawiera wyraźnie określone warunki zwolnienia z obowiązku zachowania wymienionych w nim tajemnic zawodowych. Może to mianowicie nastąpić «tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości,

a okoliczność nie może być ustalona na podstawie innego dowodu». Taki kształt omawianej regulacji mógłby sugerować, że jedynie w przypadku tajemnic zawodowych wymienionych w art. 180 § 2 KPK konieczne jest spełnienie warunku konieczności zwolnienia z obowiązku przestrzegania tych tajemnic, natomiast decyzja o zwolnieniu z obowiązku przestrzegania pozostałych tajemnic zawodowych mogłaby być podjęta także w innych, niesprecyzowanych sytuacjach”. Także przeprowadzona analiza praktyki wydawania postanowień o zwolnieniu z obowiązku przestrzegania tajemnicy statystycznej „ani wykładnia art. 180 § 1 KPK, ani dotychczasowa sposób stosowania tego przepisu nie zapewniają tego, że zwolnienie z obowiązku zachowania tajemnicy statystycznej będzie następować tylko wtedy, gdy jest to konieczne dla postępowania karnego”. Poczynienie tych ustaleń sprawiło, że w dalszej kolejności sąd konstytucyjny ustalił, czy decyzja o zwolnieniu z obowiązku zachowania tajemnicy statystycznej jest zaskarżalna, stwierdzając ostatecznie, że „mechanizm zwalniania z obowiązku przestrzegania tajemnicy statystycznej uregulowany w art. 180 § 1 KPK nie stwarza gwarancji, iż informacje statystyczne będą przekazywane na cele postępowania karnego tylko wtedy, gdy jest to niezbędne i konieczne. Brak określenia w zaskarżonym przepisie przesłanek zwolnienia z obowiązku przestrzegania tajemnicy statystycznej nie wyklucza żądania przekazania na cele postępowania karnego informacji udzielonych przez jednostki na cele statystyczne także w sytuacjach, gdy istnieje możliwość pozyskania tych informacji z innych źródeł. Z kolei brak procedury kontrolnej wobec postanowień wydanych na podstawie art. 180 § 1 KPK uniemożliwia następczą weryfikację trafności decyzji o zwolnieniu z tajemnicy statystycznej co do określonych informacji”.

W świetle zarzutów postawionych przez RPO trzeba zatem podkreślić, że uzasadnienie cytowanego wyroku pośrednie wskazuje, iż Trybunał Konstytucyjny pozytywnie odniósł się do gwarancyjnego charakteru przesłanek z 180 § 2 k.p.k. powtórzonych w zaskarżonych przepisach.

5. W świetle zarzutu sformułowanego przez Rzecznika Praw Obywatelskich istotniejsza wydaje się jednak ocena konstytucyjności art. 180 § 2 k.p.k. dokonana w wyroku z 22 listopada 2004 r. (sygn. akt K 64/03). Trybunał stwierdził tam mianowicie, że „zarzut niedookreśloności art. 180 § 2 KPK [...] 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 [...] drugie z kryteriów wskazanych w art. 180 § 2 KPK, tj. brak innych środków dowodowych jest konkretne, wymierne i sprawdzalne. 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 KPK na pewno nie wystarcza więc, by podważyć konstytucyjność zaskarżonego przepisu”.

Sejm dostrzega, że powyższe poglądy Trybunału nie mogą stanowić bezpośredniego odniesienia dla oceny przepisów zakwestionowanych przez RPO. Z istoty rzeczy, na etapie decydowania o dopuszczalności procesowego wykorzystania materiałów zgromadzonych w wyniku stosowania kontroli operacyjnej sąd nie dysponuje tak obszernym materiałem porównawczym, pozwalającym ustalić rzeczywistą konieczność wykorzystania materiałów zawierających prawnie chronione tajemnice. Niemniej jednak także i w tym wypadku można wskazać na okoliczności minimalizujące ryzyko pochopnego uznania, że w danej sprawie ziściły się przesłanki zezwalające na pozostawienie owych materiałów w dyspozycji prokuratora. Decyzję podejmuje bowiem sąd, który zarządził kontrolę operacyjną albo wyraził na nią następczą zgodę. Mamy zatem do czynienia z organem, który dysponuje wiedzą o materiale dowodowym zebrany przed przeprowadzeniem kontroli operacyjnej – wniosek o zarządzenie kontroli operacyjnej przedstawia się wraz z materiałami uzasadniającymi potrzebę jej zastosowania. Co bardziej istotne, sąd wraz z wnioskiem prokuratora otrzymuje materiały zgromadzone w czasie kontroli operacyjnej (*verba legis*: „prokurator niezwłocznie po otrzymaniu materiałów kieruje je do sądu” – art. 19 ust. 15 g ustawy o Policji). Chodzi w tym wypadku o wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej (zob. art. 19 ust. 15 w związku z ust. 15g ustawy o Policji).

Ponadto, jak już wspomniano, sąd nie jest związany wnioskiem prokuratora, na którym spoczywa obowiązek należytego umotywowania wysuniętego żądania.

6. Potwierdzeniem zgodności ze standardem konstytucyjnym rozwiązania przewidzianego w art. 180 § 2 k.p.k. są uwagi Trybunału Konstytucyjnego zawarte w uzasadnieniu wyroku 30 lipca 2014 r. (sygn. akt K 23/11). W ocenie sądu konstytucyjnego ów mechanizm zwolnienia z tajemnicy zawodowej przez sąd jest modelowym rozwiązaniem konfliktu pomiędzy wymogami ochrony tajemnic zawodowych i respektowania zakazów dowodowych z jednej strony a dobrem wymiaru sprawiedliwości, bezpieczeństwem państwa i porządkiem publicznym z drugiej. Co szczególnie istotne Trybunał Konstytucyjny zwrócił uwagę, że „zbliżone w swej istocie rozwiązania legislacyjne powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej”. Tak też uczynił ustawodawca posługując się w zaskarżonych przepisach analogicznymi przesłankami uzasadniającymi wykorzystanie materiałów zawierających informacje objęte tajemnicami zawodowymi.

7. Sposób ujęcia przez wnioskodawcę zarzutu omawianego w tej części stanowiska Sejmu nakazuje odwołanie się do praktyki orzeczniczej organów stosujących zakwestionowane regulacje. Krótki czas obowiązywania zaskarżonych przepisów oraz wynikające z istoty kontroli operacyjnej wymogi zachowania warunków właściwych dla przekazywania, przechowywania i przetwarzania informacji niejawnych wymuszają sięgnięcie do dorobku judykatury wypracowanego na gruncie art. 180 § 2 k.p.k. Zabieg taki wydaje się jednak usprawiedliwiony, ponieważ wątpliwości konstytucyjne Rzecznika Praw Obywatelskich budzi w tym zakresie precyzja wykorzystanych przez ustawodawcę pojęć konstytuujących przesłankę wykorzystania w postępowaniu karnym materiałów zawierających informacje objęte tajemnicą zawodową. Też zaś, jak wielokrotnie to już podkreślano, są analogiczne.

Po pierwsze w orzecznictwie sądowym wskazuje się jednolicie, że przepisy przewidujące odstępstwo od poszanowania prawnie chronionej tajemnicy zawodowej muszą być wykładane ściśle (zakaz wykładni rozszerzającej) z uwzględnieniem wyjątkowego charakteru takiej regulacji. Zasadniczy kierunek interpretacji art. 180 § 2 k.p.k., jednolity zarówno w orzecznictwie wynika zatem z kategorycznego respektowania zasady *exceptiones non sunt excendendae* – wyjątków nie należy interpretować rozszerzająco (zob. m.in. postanowienie SN z dnia 26 października 2011 r., sygn. akt I KZP12/11; postanowienia SA w Krakowie z: 13 stycznia 2009 r., sygn. akt II AKZ 651/08, 19 marca 2009 r., sygn. akt II AKZ 64/09; postanowienia SA we Wrocławiu z 18 września 2009 r., sygn. akt II AKZ 472/09, 4 listopada 2010 r.,

sygn. akt II AKZ 588/10; postanowienie SA w Katowicach z dnia 13 kwietnia 2011 r., II AKZ 232/11; wyrok TK z 22 listopada 2004 r., sygn. akt SK 64/03; postanowienie SA w Szczecinie z 29 października 2013 r., sygn. akt II AKZ 330/13).

Po drugie, obie przesłanki wskazane w art. 180 § 2 k.p.k. (i przeniesione do treści zaskarżonych przepisów) muszą być spełnione łącznie. Innymi słowy zwolnienie z obowiązku zachowania tajemnicy zawodowej może być orzeczone jedynie, gdy stwierdzi się zachodzące w koniunkcji przesłanki takiego orzeczenia, a to niezbędność zeznań dla dobra wymiaru sprawiedliwości, więc istotny charakter okoliczności, która ma być wykazana zeznaniami oraz niemożność stwierdzenia jej na podstawie innego dowodu (zob. m.in. postanowienie SA w Krakowie z 1 kwietnia 2015 r., sygn. akt II AKZ 111/15; postanowienie SA w Warszawie z 15 maja 2008 r., sygn. akt II AKZ 294/08).

Po trzecie, nie ulega wątpliwości, że prokurator występując do sądu z przedmiotowym wnioskiem jest obowiązany do jego szczegółowego uzasadnienia. Na gruncie art. 180 § 2 k.p.k. podkreśla się, że: „Bezwzględny obowiązek prokuratora składającego wniosek w przedmiocie zwolnienia z tajemnicy radcy prawnego jest wnikliwe wykazanie w nim istnienia wskazanych wyżej dwóch przesłanek. Obowiązek zachowania tajemnicy zawodowej przez radcę prawnego, czy adwokata ma charakter bezwzględny, stąd wniosek prokuratora mający na celu uczynienie wyłomu w tej zasadzie nie może być traktowany jak zwykła formalność i ograniczać się, w większości do powtórzenia wyrażen ustawowych i to jeszcze niekompletnych. Uzasadnienie takiego wniosku musi być wnikliwie uargumentowane, z właściwym odniesieniem do materiału dowodowego akt sprawy. Dopiero taki wniosek może być przedmiotem ocen ze strony sądu orzekającego, tak by wydana decyzja miała pełne oparcie zarówno w obowiązujących przepisach, jak i materiale dowodowym sprawy” (postanowienie SA w Katowicach z 17 lutego 2016 r., sygn. akt II AKZ 64/16). W ocenie Sejmu zaprezentowane stanowisko jest trafne także w stosunku do zaskarżonych przepisów.

Po czwarte, mimo krytycznej oceny sformułowania „dobro wymiaru sprawiedliwości” w orzecznictwie sądowym nie są formułowane tezy o kwalifikowanym stopniu niedookreślenia tego wyrażenia, uniemożliwiającej stosowanie przepisów, w których nim się posłużono. Nie jest również tak, że owa niedookreśloność uniemożliwia wykładnię tych przepisów bądź też prowadzi do rezultatów, nieakceptowalnych z punktu widzenia gwarancyjnego charakteru norm prawa karnego oraz zasad spójności systemu prawa. W orzecznictwie przyjmuje się,

że pod pojęciem dobra wymiaru sprawiedliwości należy przede wszystkim rozumieć potrzebę ustalenia prawdy obiektywnej (postanowienie SN z dnia 15 grudnia 2004 r., III KK 278/04; postanowienie SA w Szczecinie z 29 października 2013 r., sygn. akt II AKz 330/13; wyrok TK z 22 listopada 2004 r., sygn. akt SK 64/03, w którym sąd konstytucyjny ujmuje dobro wymiaru sprawiedliwości, relatywizowane do postępowania karnego, jako „poszukiwanie prawdy o popełnionym czynie i jego sprawcy”).

Należy również przypomnieć, że w wyroku z 22 listopada 2004 r. (sygn. akt SK 64/03) Trybunał Konstytucyjny nie zakwestionował zgodności brzmienia art. 180 § 2 k.p.k. z konstytucyjnym standardem określoności prawa.

8. Należy wreszcie przypomnieć, iż w orzecznictwie konstytucyjnym przyjmuje się że nie każde użycie klauzuli generalnej albo wyrażenia niedookreślonego stanowi naruszenie wymogów poprawnej legislacji. Trybunał podkreśla, że prawodawca powinien z dużą ostrożnością posługiwać się wszelkiego rodzaju zwrotami niedookreślonymi, choć nie da się nigdy całkowicie wyeliminować tych zwrotów z przepisów prawa obowiązującego (zob. np. wyrok pełnego składu TK z 25 maja 2016 r., sygn. akt Kp 2/15). Toteż z samego faktu użycia przez ustawodawcę danego zwrotu niedookreślonego nie można wysnuwać wniosku o niekonstytucyjności przepisu prawa (zob. np. wyrok TK z 23 listopada 2016 r., sygn. akt K 6/14).

9. Mając na uwadze wszystkie poczynione wyżej ustalenia Sejm wnosi o stwierdzenie, że zakwestionowane przepisy w zakresie, w jakim posługują się 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 k.p.k. **są zgodne** z art. 2, art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

IV. Podstawy dostępu do danych telekomunikacyjnych, pocztowych i internetowych

IV.1. Przedmiot kontroli

Artykuł 20c ust. 1 ustawy o Policji: „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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe ((t.j. Dz. U. z 2016 r., poz. 1113 ze zm.)), zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 20cb ust. 1 ustawy o Policji: „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”.

Artykuł 10b ust. 1 ustawy o SG: „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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2016 r., poz. 1113 ze zm.), zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 10bb ust. 1 ustawy o SG: „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”.

Artykuł 36b ust. 1 ustawy o kontroli skarbowej: „W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy 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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2016 r., poz. 1113 ze zm.), zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 36bb ust. 1 ustawy o kontroli skarbowej: „W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy 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”.

Artykuł 30 ust. 1 ustawy o ŻW: „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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2016 r., poz. 1113 ze zm.), zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 30c ust. 1 ustawy o ŻW: „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”.

Artykuł 28 ust. 1 ustawy o ABW: „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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2016 r., poz. 1113 ze zm.), zwane dalej «danymi pocztowymi», 3) art. 18

ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 28b ust. 1 ustawy o ABW: „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”.

Artykuł 32 ust. 1 ustawy o SKW: „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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2016 r., poz. 1113 ze zm.), zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 32b ust. 1 ustawy o SKW: „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”.

Artykuł 18 ust. 1 ustawy o CBA: „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 2014 r. poz. 243, z późn. zm.9)), zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz.U. poz. 1529 oraz z 2015 r. poz. 1830), 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”.

Artykuł 18b ust. 1 ustawy o CBA: „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”.

Artykuł 75d ust. 1 ustawy o SC: „W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celną może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego 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 (t.j. Dz. U. z 2016 r., poz. 1489 ze zm.), zwane dalej «danymi telekomunikacyjnymi», 2) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r., poz. 1030 ze zm.), zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą”.

Artykuł 75db ust. 1 ustawy o SC: „W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celną 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 dotyczy”.

IV.2. Zarzuty wnioskodawcy

Zdaniem RPO za niekonstytucyjne należy uznać uregulowanie pozyskiwania i przetwarzania przez służby danych niestanowiących treści przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną. Są to tzw. dane: telekomunikacyjne, pocztowe oraz internetowe.

Rzecznik Praw Obywatelskich stwierdza, że: „Analizując katalog przestępstw, w przypadku których dopuszczalne jest uzyskiwanie i przetwarzanie tych danych w odniesieniu do poszczególnych służb wyraźnie widać, że jest on zbyt szeroki, co wskazuje na przekroczenie granic, o których mowa w art. 31 ust. 3 Konstytucji, art. 8 ust. 2 EKPCz oraz art. 52 ust. 1 KPP UE”. Posłużenie się przez ustawodawcę w zaskarżonych przepisach ogólnymi pojęciami takimi jak „przestępstwa”, czy „przestępstwa skarbowe” powoduje w ocenie RPO, że „co najmniej część z tych przestępstw nie spełnia kryterium «wystarczająco poważnych»”. Innymi słowy „nie zagwarantowano, by gromadzenie i przetwarzanie danych internetowych było subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach”.

Rzecznik Praw Obywatelskich wskazuje ponadto, że zakwestionowane przepisy naruszają również „art. 30, 47, 49, 51 ust. 2 Konstytucji w zw. z art. 2 Konstytucji statuującym zasadę ochrony zaufania do państwa i stanowionego przez nie prawa, a także zasadę określoności przepisów prawa poprzez odwołanie się do definicji pojęcia «dane internetowe», które nie jest jasne i precyzyjne”. W ocenie wnioskodawcy art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną, do którego odsyłają zaskarżone przepisy, wymieniane kategorie danych określone są w sposób nazbyt ogólny, „co może powodować niejasności i prowadzić do zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe”.

IV.3. Analiza formalnoprawna

1. Zarzuty postawione przez Rzecznika Praw Obywatelskich ograniczają się do nieprawidłowego wyznaczenia katalogu przestępstw, uzasadniających pozyskiwanie i przetwarzanie danych abonenckich. Analizując przepisy ustawy o Policji RPO podkreśla, że użyte w art. 20c te same ogólne pojęcia „przestępstw” jest nadmiernie szerokie i przekreśla subsydiarny charakter niejawnego pozyskiwania danych o jednostkach. „Z podobnych względów” za niezgodne z powołanymi wzorcami kontroli należy, zdaniem RPO, uznać pozostałe zaskarżone przepisy. Tak sformułowany i uzasadniony zarzut rzutuje na ewentualny zakres trybunalskiej derogacji w przypadku uznania wątpliwości konstytucyjnych wnioskodawcy za zasadne. Trzeba bowiem przypomnieć, że niektóre ze służb są uprawnione do pozyskiwania danych abonenckich z innych niż kryminalno-prewencyjne powodów. Policja oraz Żandarmeria Wojskowa mogą pozyskiwać owe dane także w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Wymaga zauważenia, że uzasadnienie wniosku RPO nie zawiera konstytucyjnej oceny wymienionych przesłanek, a co za tym idzie muszą one pozostać poza granicami zaskarżenia, mimo że w *petitum* wniosku nie zniuansowano tej kwestii.

Lektura części uzasadnienia wniosku RPO zawierającej argumenty na poparcie omawianego zarzutu przekonuje, że wątpliwości wnioskodawcy nie dotyczą dopuszczalności pozyskiwania danych abonenckich przez wybrane formacje do celów ratowniczych i poszukiwawczych. Rzecznik Praw Obywatelskich nie odnosi się w żaden sposób do tej podstawy niejawnego dostępu do informacji, poprzestając na analizie zbyt szerokiego katalogu przestępstw (przestępstw skarbowych) zawartego w każdym z zakwestionowanych przepisów.

Uzasadnienie wniosku nie zawiera ponadto argumentów na rzecz naruszenia art. 30 Konstytucji i w tym zakresie nie może zostać za podstawę rozpoznania omawianego zarzutu niekonstytucyjności. W tym zakresie postępowanie winno zostać **umorzone** na podstawie art. 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku.

2. W przedmiocie drugiego ze sformułowanych przez Rzecznika zarzutów, dotyczącego niedostatecznej precyzji pojęcia danych internetowych, odnotowania wymaga lakoniczność jego uzasadnienia. Jak już była o tym mowa uzasadnienie

zarzutu niekonstytucyjności powinno wykraczać poza przytoczenie literalnego brzmienia przepisów, ich omówienie oraz ogólną konstatację o niezgodności z określonym wzorcem kontroli. W orzecznictwie Trybunał Konstytucyjny przywiązuje szczególną wagę do należytego uargumentowania zarzutu naruszenia wymogu określoności przepisów prawa, wskazując na konieczność wyjaśnienia przez podmiot inicjujący postępowanie, dlaczego uważa, że zaskarżone wyrażenie jest nieostre i nieprecyzyjne. Sąd konstytucyjny podkreśla także powinność przedstawienia wykładni kwestionowanego wyrażenia oraz przedstawienia argumentów – czy to teoretycznoprawnych, czy to z zakresu stosowania prawa – na poparcie twierdzenia, że zakwestionowane wyrażenie może być rozumiane niejednolicie. W ocenie Trybunału, ograniczenie argumentację do apriorycznych stwierdzeń nie jest wystarczające do spełnienia wymagania należytego uzasadnienia postawionego zarzutu (zob. postanowienie TK z 8 lipca 2013 r., sygn. akt P 11/11; por. wyrok TK z 7 lipca 2015 r., sygn. akt K 47/12).

W ocenie Sejmu wywody Rzecznika w omawianym zakresie nie spełniają warunków należytego uzasadnienia postawionego zarzutu. Wnioskodawca jedynie zasygnalizował brak jasności i precyzji oraz nadmierną ogólność pojęcia „danych internetowych” i przyjętej metody jego zdefiniowania poprzez odesłanie do przepisów ustawy o świadczeniu usług drogą elektroniczną. Mając powyższe na uwadze należy wniesć o **umorzenie postępowania** w wymienionym zakresie na podstawie art. 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku.

3. Powołane we wniosku międzynarodowe wzorce kontroli nie wyrażają treści szerszych niż wynikające z odpowiadających im przepisów ustawy zasadniczej. Jak już była o tym mowa, w takiej sytuacji – jak wskazuje dotychczasowy dorobek Trybunału Konstytucyjnego (por. wyroki TK z: 17 grudnia 2008 r., sygn. akt P 16/08; 10 lipca 2008 r., sygn. akt P 15/08; 27 maja 2008 r., sygn. akt P 59/07; 18 października 2004 r., sygn. akt P 8/04, a także odnoszący się w tym względzie do Konwencji o prawach osób niepełnosprawnych wyrok TK z 23 stycznia 2014 r., sygn. akt K 51/12) – należy uznać, że oddzielne orzekanie o zgodności zaskarżonej regulacji z prawem międzynarodowym jest zbędne, co nakazywałoby **umorzenie postępowania** w tym zakresie na podstawie art. 59 ust. 1 pkt 3 ustawy o TK. W przedmiocie art. 36b ust. 1 oraz art. 36bb ust. 1 ustawy o kontroli skarbowej postępowanie **podlega umorzeniu** z uwagi na utratę mocy obowiązującej przed wydaniem orzeczenia przez Trybunał Konstytucyjny" art. 59 ust. 1 pkt 4 ustawy o TK.

V. Zasady dostępu do danych telekomunikacyjnych, pocztowych i internetowych

V.1. Przedmiot kontroli

Prezentację przedmiotu zaskarżenia należy poprzedzić odnotowaniem błędnego określenia przez wnioskodawcę zakwestionowanych przepisów ustawy o SKW. Jak bowiem jednoznacznie wynika z uzasadnienia postawionego zarzutu oraz treści przepisów pozostałych zaskarżonych ustaw, Rzecznik Praw Obywatelskich domaga się kontroli art. 32 ust 5 w związku z art. 32 ust. 2 ustawy o SKW. W treści wniosku zamiast art. 32 ust. 5 kwestionowanej ustawy konsekwentnie wspomina się jednak o art. 32 ust. 3 tejże, co Sejm traktuje jako oczywistą omyłkę – sprostowaną pismem RPO z 25 lutego 2016 r. – i stosownie skoryguje w dalszej części rozważań.

Artykuł 20c ust. 3 w związku z art. 20c ust. 2 ustawy o Policji: „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” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:

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” (ust. 2).

Artykuł 10b ust. 3 w związku z art. 10b ustawy o SG: „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 Straży Granicznej a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca

świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej; 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2).

Artykuł 36b ust. 3 w związku z art. 36b ust. 2 ustawy o kontroli skarbowej: „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 taką przewiduje porozumienie zawarte pomiędzy Generalnym Inspektorem Kontroli Skarbowej a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej; 2) na pisemny wniosek pracownika wywiadu skarbowego posiadającego pisemne upoważnienie Generalnego Inspektora Kontroli Skarbowej do występowania w jego imieniu o udostępnienie danych, o których mowa w ust. 1” (ust. 2).

Artykuł 30 ust. 3 w związku z art. 30 ust. 2 ustawy o ŻW: „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 ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej; 2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2).

Artykuł 28 ust. 3 w związku z art. 28 ust. 2 ustawy o ABW: „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 ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio: 1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ; 2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2” (ust. 2).

Artykuł 32 ust. 5 w związku z art. 32 ust. 2 ustawy o SKW: „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 współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem SKW a tym podmiotem” (ust. 5); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej; 2) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW” (ust. 2).

Artykuł 18 ust. 3 w związku z art. 18 ust. 2 ustawy o CBA: „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 współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej; 2) na ustne żądanie funkcjonariusza CBA, posiadającego pisemne upoważnienie Szefa CBA lub osoby

przez niego upoważnionej; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi CBA posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2)”.

Artykuł 75d ust. 3 w związku z art. 75d ust. 2 ustawy o SC: „W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub internetowych odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym między Szefem Służby Celnej a tym podmiotem” (ust. 3); „Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane telekomunikacyjne lub internetowe: 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Szefa Służby Celnej lub dyrektora izby celnej albo osoby przez nich upoważnionej; 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2).

V.2. Zarzuty wnioskodawcy

Wątpliwości RPO budzą przepisy regulujące zawieranie porozumień przez przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną z właściwymi organami służb (m.in. Komendantem Głównym Policji). Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia odpowiednie dane nieodpłatnie. Jednym z prawem przewidzianych sposobów jest udostępnienie danych funkcjonariuszowi danej służby posiadającemu pisemne upoważnienie odpowiedniego organu za pośrednictwem sieci telekomunikacyjnej. W takim wypadku dane udostępnia się bez udziału pracowników podmiotu udostępniającego lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy organem danej służby a tym podmiotem. Zaskarżone przepisy nie określają przesłanek zawarcia wspomnianego porozumienia, „co może oznaczać w praktyce ograniczenie swobody przedsiębiorcy co do odmowy zawarcia porozumienia”. Także zasada nieodpłatnego udostępniania danych „może prowadzić do ingerencji w swobodę działalności gospodarczej”. Wreszcie stały dostęp służb do wspomnianych danych narusza – zdaniem RPO

– „zasadę demokratycznego państwa prawnego, godność człowieka i wynikające z niej prawo do prywatności, wolność i ochronę tajemnicy komunikowania się czy w końcu ochronę informacji o samym sobie”. Jak zauważa wnioskodawca: „Trudno bowiem twierdzić, że prywatność i dane osobowe są chronione w sytuacji, gdy bez ściśle określonych przesłanek i bez realnej kontroli mogą być pobierane przez funkcjonariuszy służb. Niemożliwe jest wykazanie konieczności i proporcjonalności takich regulacji”.

V.3. Analiza formalnoprawna

1. W ocenie Sejmu dopuszczalność merytorycznego rozpoznania zarzutu wyrażonego w pkt V petitum wniosku RPO budzi poważne wątpliwości. W pierwszej kolejności należy podkreślić lakoniczność argumentów przedstawionych przez wnioskodawcę. Co więcej część wypowiedzi RPO zdaje się odnosić do innych niż ujęte jako przedmiot zaskarżenia regulacji i powielać krytyczne oceny wyrażone w ramach innych zarzutów niekonstytucyjności zawartych we wniosku Rzecznika.

Spośród zarzutów odnoszących się do zawartości normatywnej zaskarżonych przepisów należy wskazać dwa podstawowe. Po pierwsze, Rzecznik podnosi, że zaskarżone przepisy nie określają przesłanek zawarcia porozumienia, „co może oznaczać w praktyce ograniczenie swobody przedsiębiorcy co do odmowy zawarcia porozumienia”. Po drugie, zarzuca brak konstytucyjności obowiązku nieodpłatnego udostępniania danych. W ocenie RPO może to bowiem prowadzić do ingerencji w zasadę swobody działalności gospodarczej poprzez ograniczenie możliwości swobodnego podejmowania działań faktycznych i prawnych w ramach prowadzonej działalności. Po trzecie wskazuje, że „porozumienia spowodują budowę stałej infrastruktury tzw. stałych łącz, dzięki którym funkcjonariusze służb bez udziału pracowników usługodawcy lub przy niezbędnym ich udziale będą mogli w dowolnym czasie pozyskiwać dane [...]”. Ten zarzut wydaje się natomiast mieć charakter pochodny wobec dostrzeganych przez Rzecznika niedostatków zaskarżonych ustaw w zakresie ścisłego określenia przesłanek dostępu do danych oraz mechanizmu realnej kontroli ich pozyskiwania. W takim bowiem kontekście Rzecznik wskazuje na nadmierność ingerencji w prawo do prywatności i autonomii informacyjnej opisanego modelu dostępu służb do danych telekomunikacyjnych, internetowych i pocztowych.

Jak widać, argumenty Rzecznika ograniczają się do zasygnalizowania potencjalnej ingerencji w swobodę prowadzenia działalności gospodarczej.

Wnioskodawca poprzestaje jednak na powyższej konstatacji nie rozwijając tych wątków. Nie wskazuje przy tym konkretnych argumentów uzasadniających wadliwość konstytucyjną zaskarżonych przepisów. Ponadto w żaden sposób nie odnosi się do wyrażonej w art. 22 Konstytucji dopuszczalności wprowadzania ograniczeń wolności działalności gospodarczej ze względu na ważny interes publiczny. Skrótność wyводу wnioskodawcy zdaje się wręcz sugerować niedopuszczalność wprowadzenia jakichkolwiek ograniczeń (nawet potencjalnych) w tej sferze. Nie ulega przy tym wątpliwości, że wnioskodawca dostrzega wagę okoliczności, które stoją za potrzebą przyznania służbom uprawnień do niejawnego pozyskiwania informacji o jednostkach. We wstępnej części wniosku, zawierającej uwagi ogólne, nieprzypisane poszczególnym zarzutom RPO uznaje oczywistą przydatność stosowania technik niejawnego pozyskiwania informacji. W tym kontekście tym wyraźniej rysują się niedostatki argumentacyjne omawianego zarzutu. Zaprezentowana argumentacja pomija bowiem nieodłączny udział podmiotów zatrzymujących i udostępniających określone dane, a ten wymusza – zdaniem Sejmu – odpowiednie zniuansowanie zarzutów niekonstytucyjności wymierzonych w przepisy regulujące praktyczne aspekty wykonywania obowiązków nałożonych na dostawców usług i odpowiadających im kompetencji służb.

Wobec powyższego Sejm wnosi o umorzenie postępowania w zakresie badania przepisów zaskarżonych przepisów ze względu na uchybienie przez wnioskodawcę obowiązkowi przedstawienia argumentów na poparcie postawionego zarzutu.

VI. Kontrola udostępniania danych telekomunikacyjnych, pocztowych i internetowych

VI.1. Przedmiot kontroli

1. Artykuł 20ca ustawy o Policji: „Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane” (ust. 1); „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” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych” (ust. 3); „Sąd okręgowy informuje organ Policji o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 20cb ust. 1” (ust. 5).

Artykuł 10ba ustawy o SG: „Kontrolę nad uzyskiwaniem przez Straż Graniczną danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby składającego wniosek organu Straży Granicznej” (ust. 1); „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” (ust. 2); „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” (ust. 3); „Sąd okręgowy informuje organ Straży Granicznej o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 10bb ust. 1” (ust. 5).

Artykuł 36ba ustawy o kontroli skarbowej: „Kontrolę nad uzyskiwaniem przez wywiad skarbowy danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie, zwany dalej «Sądem»” (ust. 1); „Generalny Inspektor Kontroli Skarbowej przekazuje Sądowi, 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” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych, pocztowych lub internetowych” (ust. 3); „Sąd informuje

Generalnego Inspektora Kontroli Skarbowej o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 36bb ust. 1” (ust. 5).

Artykuł 30b ustawy o ŻW: „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” (ust. 1); „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” (ust. 2); „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” (ust. 3); „Wojskowy sąd okręgowy informuje organ Żandarmerii Wojskowej o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 30c ust. 1” (ust. 5).

Artykuł 28a ustawy o ABW: „Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie” (ust. 1); „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” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych” (ust. 3); „Sąd, o którym mowa w ust. 1, informuje Szefa ABW o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28b ust. 1” (ust. 5).

Artykuł 32a ustawy o SKW: „Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Wojskowy Sąd Okręgowy w Warszawie” (ust. 1); „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” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych” (ust. 3); „Sąd, o którym mowa w ust. 1, informuje Szefa SKW o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 32b ust. 1” (ust. 5).

Artykuł 18a ustawy o CBA: „Kontrolę nad uzyskiwaniem przez CBA danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie” (ust. 1); „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” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych, pocztowych lub internetowych” (ust. 3); „Sąd, o którym mowa w ust. 1, informuje Szefa CBA o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 18b ust. 1” (ust. 5).

Artykuł 75da ustawy o SC: „Kontrolę nad uzyskiwaniem przez Służbę Celną danych telekomunikacyjnych i internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Służby Celnej, któremu udostępniono te dane” (ust. 1); „Organ Służby Celnej, 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 lub internetowych oraz rodzaj tych danych; 2) kwalifikacje prawne czynów, w związku

z zaistnieniem których wystąpiono o dane telekomunikacyjne lub internetowe” (ust. 2); „W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Służbie Celnej danych telekomunikacyjnych lub internetowych” (ust. 3); „Sąd, o którym mowa w ust. 1, informuje Szefa Służby Celnej o wyniku kontroli w terminie 30 dni od jej zakończenia” (ust. 4); „Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 75db ust. 1” (ust. 5).

2. Rzecznik Praw Obywatelskich wnosi o stwierdzenie niezgodności wymienionych przepisów ze wskazanymi wzorcami kontroli w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych.

VI.2. Zarzuty wnioskodawcy

Rzecznik kwestionuje konstytucyjność sądowej kontroli udostępniania danych telekomunikacyjnych, pocztowych i internetowych. Kontrolę tę sprawuje właściwy miejscowo sąd okręgowy, któremu w okresach półrocznych, wskazany ustawowo organ danej służby przekazuje sprawozdanie obejmujące: liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych; 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.

Wnioskodawca zwraca uwagę, że w wypadku zaskarżonych przepisów, „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 [...] 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”. Podsumowując ten wątek swoich rozważań wnioskodawca stwierdza: „Kontrola następcza nie powinna być stosowana domyślnie, lecz może być dopuszczalna jedynie wyjątkowo, w sytuacjach, w których zachodzi potrzeba natychmiastowego działania służb”.

Zastrzeżenia RPO budzi ponadto zbyt szeroki katalog danych, których uzyskiwanie nie podlega omówionym mechanizmom kontrolnym: „[U]stawa 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. W szczególności art. 161 ust. 3 Prawa telekomunikacyjnego zawiera odniesienie do bliżej nieokreślonych «innych danych»”.

VI.3. Analiza formalnoprawna

Wymaga odnotowania, że w części wniosku zawierającej uzasadnienie omawianego zarzutu wnioskodawca nie rozwija odrębnej argumentacji wykraczającej poza uwagi odnośnie do zgodności zaskarżonych przepisów z konstytucyjnymi wzorcami kontroli. Co prawda odwołuje się, do rozważań i ocen dokonanych przez TSUE w wyroku z 8 kwietnia 2014 r. (sygn. akt C-293/12), jednakże nie zestawia ich w sposób analityczny i konkluzywny ze standardem konstytucyjnym rekonstruowanym na potrzeby niniejszego postępowania w oparciu o wyrok TK z 30 lipca 2014 r. (sygn. akt K 23/11).

Argumentacja przedstawiana przez Rzecznika na poparcie niezgodności z powoływanymi konstytucyjnymi wzorcami kontroli ma charakter postulatów *de lege ferenda*, nieukierunkowanych na wykazanie niezgodności z Konstytucją regulacji już obowiązujących – w związku z czym nie może być przedmiotem merytorycznego rozpoznania przez Trybunał Konstytucyjny.

Biorąc powyższe pod uwagę, Sejm wnosi o **umorzenie postępowania** na podstawie 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku w części obejmującej zaskarżonych we wniosku przepisów.

VII. Obowiązek poinformowania jednostki o pozyskaniu i przetwarzaniu dotyczących jej danych telekomunikacyjnych, pocztowych i internetowych; określenie katalogu podmiotów, których dane dotyczą oraz czasu przetwarzania danych

VII.1. Przedmiot kontroli

1. Artykuł 20c ustawy o Policji: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [...], zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 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” (ust. 2); „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” (ust. 3); „Udostępnienie Policji danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) wykorzystywane sieci telekomunikacyjne zapewniają: a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych; 2) jest to

uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności” (ust. 4); „Komendant Główny Policji, Komendant CBŚP i komendant wojewódzki Policji prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Policji i funkcjonariusza Policji uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 5); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 6); „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu” (ust. 7).

Artykuł 10b ustawy o SG: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [...], zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej; 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2); „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 Straży Granicznej a tym podmiotem” (ust. 3); „Udostępnienie Straży Granicznej danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) wykorzystywane sieci telekomunikacyjne zapewniają: a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych; 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Straży Granicznej albo prowadzonych przez nie czynności” (ust. 4); „Komendant Główny Straży Granicznej i komendant oddziału Straży Granicznej prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Straży Granicznej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 5); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 6); „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu” (ust. 7).

Artykuł 36b ustawy o kontroli skarbowej: „W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy 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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek

Generalnego Inspektora Kontroli Skarbowej; 2) na pisemny wniosek pracownika wywiadu skarbowego posiadającego pisemne upoważnienie Generalnego Inspektora Kontroli Skarbowej do występowania w jego imieniu o udostępnienie danych, o których mowa w ust. 1; 3) za pośrednictwem sieci telekomunikacyjnej pracownikowi wywiadu skarbowego posiadającemu pisemne upoważnienie, o którym mowa w pkt 2” (ust. 2); „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 taką przewiduje porozumienie zawarte pomiędzy Generalnym Inspektorem Kontroli Skarbowej a tym podmiotem” (ust. 3); „(uchylony)” (ust. 4); „(uchylony)” (ust. 5); „Udostępnienie wywiadowi skarbowemu danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia: 1) możliwość ustalenia pracownika wywiadu skarbowego uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane; 2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych” (ust. 6); „Udostępnianie wywiadowi skarbowemu danych, o których mowa w ust. 1, następuje na koszt przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną” (ust. 7); „Generalny Inspektor Kontroli Skarbowej prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną wywiadu skarbowego i pracownika wywiadu skarbowego uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 8).

Artykuł 30 ustawy o ŻW: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług

drogą elektroniczną [...], zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej; 2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2); „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 ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem” (ust. 3); „Udostępnienie Żandarmerii Wojskowej danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) wykorzystywane sieci i system teleinformatyczny zapewniają: a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych; 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności” (ust. 4); „Komendant Główny Żandarmerii Wojskowej i komendant oddziału Żandarmerii Wojskowej prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Żandarmerii Wojskowej i żołnierza Żandarmerii Wojskowej uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 5); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 6); „Dane, o których mowa w ust. 1, które nie mają znaczenia dla

postępowania karnego, podlegają niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu” (ust. 7).

Artykuł 28 ustawy o ABW: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [...], zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio: 1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ; 2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2” (ust. 2); „W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem” (ust. 3); „Udostępnienie ABW danych, o których mowa w ust. 1 pkt 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia: 1) możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane; 2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych” (ust. 4); „Szef ABW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną ABW i funkcjonariusza ABW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 5); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Szef ABW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie

wykorzystania przekazanych danych” (ust. 6); „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” (ust. 7).

Artykuł 32 ustawy o SKW: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe [...], zwane dalej «danymi pocztowymi», 3) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [...], zwane dalej «danymi internetowymi» – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej; 2) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW” (ust. 2); „O udostępnieniu danych w trybie określonym w ust. 2 pkt 2 przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną informuje niezwłocznie Szefa SKW” (ust. 3); „Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną są obowiązani udostępnić dane, o których mowa w ust. 1, funkcjonariuszom wskazanym we wniosku” (ust. 4); „W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, 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 współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem SKW a tym podmiotem” (ust. 5); „Udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) wykorzystywane sieci i system teleinformatyczny zapewniają: a) możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych; 2) jest

to uzasadnione specyfiką lub zakresem zadań wykonywanych przez SKW albo prowadzonych przez nią czynności” (ust. 6); „Szef SKW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną SKW i funkcjonariusza SKW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 7); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Szef SKW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 8); „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla obronności Państwa, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu” (ust. 9).

Artykuł 18 ustawy o CBA: „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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz.U. poz. 1529 oraz z 2015 r. poz. 1830), 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” (ust. 1); „Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1: 1) na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej; 2) na ustne żądanie funkcjonariusza CBA, posiadającego pisemne upoważnienie Szefa CBA lub osoby przez niego upoważnionej; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi CBA posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2); „W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, 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 współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem” (ust. 3); „Udostępnienie CBA danych, o których mowa

w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) sieć ta zapewnia: a) możliwość ustalenia funkcjonariusza CBA uzyskującego te dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do uzyskiwanych danych; 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne CBA albo prowadzonych przez nie czynności” (ust. 4); „Szef CBA prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną CBA i funkcjonariusza CBA uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 5); „Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Szef CBA przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 6); „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu” (ust. 7).

Artykuł 75d ustawy o SC: „W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego 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 [...], zwane dalej «danymi telekomunikacyjnymi», 2) art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [...], zwane dalej «danymi internetowymi» –oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą” (ust. 1); „Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane telekomunikacyjne lub internetowe: 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Szefa Służby Celnej lub dyrektora izby celnej albo osoby przez nich upoważnionej; 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1; 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1” (ust. 2); „W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub internetowych odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli

możliwość taka jest przewidziana w porozumieniu zawartym między Szefem Służby Celnej a tym podmiotem” (ust. 3); „Udostępnienie danych telekomunikacyjnych lub internetowych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli: 1) wykorzystywane sieci telekomunikacyjne zapewniają: a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane, b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych; 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Służby Celnej albo prowadzonych przez nie czynności” (ust. 4); „Dane telekomunikacyjne lub internetowe, które mają znaczenie dla postępowania karnego lub postępowania karnego skarbowego, Szef Służby Celnej albo dyrektor izby celnej przekazuje prokuratorowi właściwemu ze względu na siedzibę organu przekazującego. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych” (ust. 5); „Dane telekomunikacyjne lub internetowe, które nie mają znaczenia dla postępowania karnego lub postępowania karnego skarbowego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu” (ust. 6); „Szef Służby Celnej i dyrektor izby celnej prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Służby Celnej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych” (ust. 7).

2. Wymienione przepisy zaskarżono w zakresie, w jakim 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.

VII.2. Zarzuty wnioskodawcy

W ocenie Rzecznika Praw Obywatelskich ustawodawca pominął uregulowanie materii, która z uwagi na standard konstytucyjny oraz wynikający z powołanych jako wzorce kontroli aktów prawa międzynarodowego i wspólnotowego powinna się znaleźć w zaskarżonych przepisach. Chodzi tu o uzupełnienie regulacji dotyczących uzyskiwania i przetwarzania danych telekomunikacyjnych, pocztowych oraz

internetowych o: obowiązek poinformowania jednostki o podjętych wobec niej działaniach, tj. o pozyskaniu i przetwarzaniu danych, szczegółowe określenie kategorii podmiotów, wobec których mogą być podejmowane „czynności operacyjno-rozpoznawcze”, wreszcie o wyznaczenie okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane. W odniesieniu do ostatniej wymienionej kwestii RPO podnosi, że: „Ustawa przewiduje jedynie, że dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi, które dla określonego postępowania miały znaczenie i zostały w nim wykorzystane, w 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 przetwarzania danych. Okres przetwarzania danych [...] 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”.

VII.3. Analiza formalnoprawna

1. Rzecznik Praw Obywatelskich sformułował trzy zarzuty pod adresem przepisów ujętych w pkt VII petitum swojego wniosku. W pierwszej kolejności należy zatem odnieść się do dopuszczalności merytorycznego rozpoznania każdego z nich.

2. W ocenie Sejmu zarzut braku określenia przez ustawodawcę kategorii podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze nie może zostać merytorycznie rozpoznany przez Trybunał Konstytucyjny. Jak już to wielokrotnie wspomniano na wnioskodawcy ciąży procesowy obowiązek poparcia wysuniętego zarzutu. Sygnalizowane przez Rzecznika pominięcie nie znajduje natomiast należytego rozwinięcia w warstwie argumentacyjnej wniosku, RPO poprzestał bowiem na jednozdaniowej konstatacji zbieżnej treściowo z zakresem zaskarżenia zawartym w petitum wniosku. Nie można zatem przyjąć, że w omawianym wypadku mamy do czynienia z dochowaniem przez

wnioskodawcę formalnych wymogów postępowania przed Trybunałem Konstytucyjnym.

Warto w tym miejscu przypomnieć, że podobny zarzut został wysunięty przez Rzecznika w postępowaniu o sygn. K 23/11. Jak zreferował Trybunał Konstytucyjny: „Rzecznik Praw Obywatelskich we wniosku z 1 sierpnia 2011 r., kwestionując przepisy o gromadzeniu i przetwarzaniu danych telekomunikacyjnych, również wskazał na niepełność regulacji. W jego ocenie, ustawodawca nie wyłączył w zakwestionowanych przepisach żadnej kategorii osób korzystających z sieci teleinformatycznych z kręgu podmiotów, których dane mogą być pozyskane. W szczególności nie są, zdaniem Rzecznika, uwzględnione szczególne rygory ochrony informacji objętych tajemnicami zawodowymi (adwokacką, notarialną, radcy prawnego, dziennikarską, lekarską – *vide*: art. 180 § 2 k.p.k.), których zniesienie jest możliwe wyłącznie wówczas, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a określonej okoliczności nie można ustalić na podstawie innych dowodów”. Argumentacja przedstawiona przez Rzecznika nie została jednak uznana przez sąd konstytucyjny za wystarczającą do merytorycznego rozpoznania wniosku w tym zakresie: „Poza ogólnie sformułowanym zarzutem, Rzecznik nie przywołał żadnych argumentów na jego poparcie. Wniosek Rzecznika Praw Obywatelskich nie spełnia w powyższym zakresie wymagań formalnych wynikających z art. 32 ust. 1 pkt 4 ustawy o TK, czyli nie zawiera uzasadnienia z powołaniem dowodów na poparcie postawionego zarzutu. Tym samym postępowanie w powyższym zakresie także podlega umorzeniu”.

Mając na uwadze powyższe Sejm wnosi o **umorzenie postępowania** na podstawie art. 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku w części obejmującej kontrolę tych przepisów w zakresie, „w jakim nie wskazują kategorii osób, których dane mogą być pozyskane w sposób określony w ustawach”.

3. Wątpliwości Rzecznika wiążą się także z nieuregulowaniem przez ustawodawcę obowiązków informacyjnych wobec osób, których dane były pozyskiwane.

W pierwszej kolejności należy odnieść się do dopuszczalności merytorycznego rozpoznania przez sąd konstytucyjny wniosku RPO. Trybunał Konstytucyjny dopuszcza bowiem w swoim orzecznictwie orzekanie odnośnie do tak

zwanego pominięcia prawodawczego, odróżniając je od zaniechania ustawodawczego, które nie podlega jego kognicji.

Zaniechaniem jest całkowity brak regulacji danej kwestii (jej jakościowa odmienność od materii unormowanych w zaskarżonym przepisie). Jej uregulowanie w sposób niepełny (niewystarczający, niekompletny, przy założeniu jakościowej tożsamości brakujących elementów z elementami ujętymi w zaskarżonym przepisie) stanowi zaś pominięcie prawodawcze (zwane także zaniechaniem względnym albo częściowym). Może ono być badane przez Trybunał – jednak tylko wtedy, gdy na poziomie Konstytucji istnieje „norma o treści odpowiadającej normie pominiętej w ustawie kontrolowanej” (postanowienie TK z 1 marca 2010 r., sygn. akt SK 29/08), czyli w danym obszarze obowiązuje konstytucyjny nakaz uregulowania kwestii pominiętych w określony sposób. W celu ustalenia, że w danym wypadku występuje pominięcie legislacyjne, a więc że regulacja prawna jest fragmentaryczna, konieczna jest jakościowa tożsamość (albo przynajmniej daleko idące podobieństwo) materii unormowanych w danym przepisie i tych, które pozostawiono poza jego zakresem (zob. m.in. wyroki TK z: 15 kwietnia 2014 r., sygn. akt SK 48/13; 3 czerwca 2014 r., sygn. akt K 19/11; 2 grudnia 2014 r., sygn. akt SK 7/14). W przypadku pominięcia regulacja prawna została wydana i obowiązuje, ale jej zakres jest niepełny lub zbyt wąski. Wtedy Trybunał może orzekać nie tylko o treści aktu prawnego, ale również o tym, co ustawodawca pominął, a powinien był uregulować, by zostały spełnione wymogi konstytucyjne (por. m.in. postanowienia TK z: 2 grudnia 2014 r., sygn. akt SK 7/14; 13 stycznia 2015 r., sygn. akt SK 17/13). 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” (wyrok TK z 18 czerwca 2013 r., sygn. akt SK 1/12). W ocenie sądu konstytucyjnego wystąpienie pominięć prawodawczych jest prawdopodobne zwłaszcza w wypadku regulacji sprawiających wrażenie przypadkowych (np. pozostawionych z poprzedniej wersji przepisu), absurdalnych albo oczywiście dysfunkcyjnych (zob. np. wyrok TK z 13 listopada 2007 r., sygn. akt P 42/06).

Skuteczne zakwestionowanie pominięcia prawodawczego wymaga od podmiotu inicjującego postępowanie przed Trybunałem Konstytucyjnym także wyjątkowej staranności i zaangażowania: „[P]ostawione zarzuty muszą być precyzyjne i nie mogą polegać na wskazaniu, że przepis nie zawiera konkretnej regulacji, której istnienie zadowalałoby wnioskodawcę. Gdyby istniała możliwość zaskarżenia przepisu pod zarzutem, iż nie zawiera on regulacji, które w przekonaniu wnioskodawcy winny się w nim znaleźć, każdą ustawę lub dowolny jej przepis można byłoby zaskarżyć w oparciu o tego rodzaju przesłankę negatywną. Gdyby ustawodawca uznał za celowe takie ukształtowanie kompetencji Trybunału Konstytucyjnego, zawarłby stosowną normę w Ustawie Zasadniczej [...]” – wyrok TK z 19 listopada 2001 r., sygn. akt K 3/00.

W tym miejscu należy odwołać się do postępowania przed Trybunałem Konstytucyjnym w sprawie o sygn. akt K 3/04, zainicjowanego wnioskiem Rzecznika Praw Obywatelskich.

Jednym z przepisów wówczas zakwestionowanych przez RPO był art. 19 ust. 16 ustawy o Policji. Wnioskodawca domagał się kontroli tego przepisu w zakresie, w jakim regulując dostęp do materiałów zgromadzonych podczas kontroli operacyjnej, nie przewiduje po jej zakończeniu oraz ustaniu zagrożeń dla realizacji celów postępowania powiadomienia o kontroli innej osoby niż podejrzany oraz jego obrońca – wskazując jako wzorce kontroli art. 49 w związku z art. 31 ust. 3 oraz z art. 45 ust. 1 i art. 77 ust. 2 Konstytucji. W uzasadnieniu swojego wniosku RPO podkreślał, że ograniczenie podmiotowe wyrażone w art. 19 ust. 16 ustawy o Policji jest nazbyt wąskie, a przez to sprzeczne z ustawą zasadniczą.

Zdaniem Sejmu wyraźnie rysuje się podobieństwo pomiędzy zarzutami przedstawionymi w niżej rozpatrywanym oraz przywołanym wniosku RPO, co nakazuje odwołać się do ustaleń Trybunału poczynionych w wyroku z 12 grudnia 2005 r. (sygn. akt K 32/04).

Trybunał Konstytucyjny w pierwszej kolejności ustalił, że: „Zaskarżony przepis rzeczywiście wyklucza możliwość informowania zainteresowanego o kontroli operacyjnej «w czasie jej trwania». Zdaniem Trybunału Konstytucyjnego nie jest to jednak tożsame z zakazem udzielania takiej informacji w sytuacji, gdy czynności operacyjne nie są już prowadzone, a aktu oskarżenia nie wniesiono. Problem leży w tym, czy występujący w zaskarżonym przepisie człon «podczas trwania tej kontroli» odnosi się do czasu, w którym nie może nastąpić zawiadomienie, czy też do przedmiotu udostępnienia informacji. Samo brzmienie kontrolowanego przepisu bynajmniej nie wyklucza pierwszej możliwości. Natomiast odwołanie się do art. 321 k.p.k. dotyczy obowiązku poinformowania zainteresowanego – już jako podejrzanego, w ramach postępowania przygotowawczego, o materiałach operacyjnych, przekształconych w materiał procesowy. W tej sytuacji wniosek Rzecznika kwestionuje tylko jedną z hipotez interpretacyjnych rysujących się na tle zaskarżonej normy, i to hipotezę niekonstytucyjną. Zdaniem Trybunału Konstytucyjnego nie zostało natomiast udowodnione, że taka właśnie interpretacja stanowi powszechnie panującą praktykę. Brzmienie zaskarżonego przepisu bynajmniej nie wyklucza trafnego wniosku, że po odpadnięciu celu kontroli operacyjnej otwiera się dla inwigilowanego, zgodnie z art. 51 ust. 3 Konstytucji, możliwość wglądu w zebrane o nim materiały. Taka właśnie możliwość stanowi logiczną operacjonalizację art. 51 ust. 4 Konstytucji. Nic też nie wskazuje – w wypadku takiej hipotezy interpretacyjnej, jaką w tym miejscu przedstawiono – aby zawierała ona, w rozważanym zakresie, ograniczenie prawa do sądu”.

Następnie Trybunał Konstytucyjny podkreślił, że czym innym jest brak przeszkody w zaskarżonym przepisie do udostępnienia materiałów, na żądane zainteresowanego, co – w ocenie Trybunału – zapewnia już obecny stan prawny, a czym innym pozytywny obowiązek informowania osoby poddanej działaniom operacyjnym, przez Policję, z jej własnej inicjatywy, o prowadzeniu kontroli operacyjnej. Mając na uwadze powyższe rozróżnienie, sąd konstytucyjny skonstatował, że wniosek RPO zmierza w rzeczywistości do zakwestionowania braku wyrażenia w zaskarżonym przepisie pozytywnego obowiązku informowania przez Policję o bezskutecznej, zakończonej kontroli operacyjnej, wobec osoby poddanej takiej kontroli, jeśli w stosunku do tej osoby nie są prowadzone dalsze czynności procesowe. Tak ujęty zarzut RPO jawi się jako zbliżony do postawionego przez wnioskodawcę w niniejszym postępowaniu.

W odniesieniu do konstytucyjności braku regulacji przewidującej obowiązek informowania osoby inwigilowanej o zakończeniu prowadzenia kontroli operacyjnej Trybunał stwierdził natomiast, iż omawiany problem ujawnia się jako „wskazanie luki legislacyjnej, która nie może być przedmiotem zaskarżenia przed Trybunałem Konstytucyjnym. Struktura zaś zaskarżonego art. 19 ust. 16 ustawy o Policji oraz wskazane we wniosku wzorce konstytucyjnej kontroli (dotyczące prawa do sądu oraz tajemnicy korespondencji, pomijające [...] wzorzec z art. 51 ust. 3 i 4 Konstytucji) nie dają – zdaniem Trybunału – podstaw do dopatrzenia się na tle tego przepisu legislacyjnego pominięcia [...], co mogłoby uzasadniać wydanie wyroku zakresowego, o co wnosi Rzecznik. W związku z tym należy przypomnieć, że «legislacyjne pominięcie» uzasadniające skuteczną kontrolę konstytucyjności wymaga, aby na poziomie Konstytucji istniała norma o treści odpowiadającej normie pominiętej w ustawie kontrolowanej. Taka sytuacja w niniejszej sprawie jednak nie zachodzi”.

4. Zdaniem Sejmu pogląd prawny zaprezentowany przez Trybunał w wyroku z 12 grudnia 2005 r. zachowuje aktualność na gruncie niniejszego postępowania. Należy bowiem zwrócić uwagę, że zarzut RPO polega właśnie na dostrzeżeniu braku obligatoryjnego informowania osoby operacyjnie rozpracowywanej o pozyskaniu danych telekomunikacyjnych, pocztowych oraz internetowych. Brak uregulowania tej ostatniej kwestii, jak stwierdził sąd konstytucyjny, nie ma charakteru pominięcia w zakresie materii regulowanej i wymaganej konstytucyjnie, a stanowi lukę prawną (zaniechanie ustawodawcze), które nie podlega kognicji Trybunału.

5. Powyższe uwagi nie wyczerpują argumentacji na rzecz niedopuszczalności merytorycznego rozpoznania zarzutu pod adresem przepisów ujętych w ramach pkt 3 petitum wniosku RPO. Przekonuje o tym również analiza kryteriów rozpoznawania pominięcia prawodawczego (oraz występujących w tej kwestii domniemań) wypracowanych w dotychczasowym orzecznictwie Trybunału.

Czynności operacyjno-rozpoznawcze nie stanowią wyodrębnionej materii regulowanej konstytucyjnie. Na poziomie konstytucyjnym brak zatem normy bezpośrednio odpowiadającej normie pominiętej w kwestionowanej regulacji. Innymi słowy, „w polskim systemie prawnym ocena zgodności czynności operacyjnych z Konstytucją wymaga analizy z punktu widzenia samego sposobu konstytucjonalizacji chronionej wolności/prawa, zagrożonej przez czynności

operacyjne, jak również analizy proporcjonalności działania ustawodawcy zwykłego, w obu wyżej wskazanych aspektach (materialnoprawnym i proceduralnym)” – wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04. Powyższe nie oznacza oczywiście niedopuszczalności kontroli konstytucyjnej przepisów dotyczących czynności operacyjno-rozpoznawczych, jednak wymaga od podmiotu formułującego zarzut postępowaniu przed Trybunałem wykazania konstytucyjnego zakotwiczenia normy prawnej, której brak w systemie prawa stanowi podstawę formułowanego zarzutu.

Jak już wspomniano, przyjęcie, że badany brak normatywny ma charakter pominięcia prawodawczego, wymaga ustalenia jakościowej tożsamości elementów brakujących z elementami ujętymi w zaskarżonym przepisie. Zdaniem Sejmu, Rzecznik Praw Obywatelskich nie sprostął powyższemu warunkowi. Uzasadnienie postawionego zarzutu nie zawiera bowiem pogłębionej analizy podstaw podmiotowego różnicowania zakresu dostępu (aż do jego wyłączenia) do informacji o prowadzonej kontroli operacyjnej. Te zaś ujawniają się już na poziomie *ratio* stosowania samych czynności operacyjno-rozpoznawczych, jako działań o charakterze niejawnym zmierzających do pozyskania informacji bądź utrwalenia dowodów enumeratywnie wyliczonych przestępstw..

Ponadto analiza otoczenia normatywnego kwestionowanych przepisów nie pozwala na przyjęcie, że mamy w tym wypadku do czynienia z pomyłką legislacyjną, czyniącą daną regulację dysfunkcjonalną bądź absurdalną. Kwestie związane z informowaniem osób, których dotyczą pozyskane dane zostały na gruncie kwestionowanych ustaw uregulowane jednolicie.

Należy wreszcie przypomnieć, że zbyt pochopne „upodobnienie” materii nieuregulowanych z materiałami, które znalazły swój wyraz w treści kwestionowanego przepisu, może spowodować wykroczenie przez Trybunał poza sferę kontroli prawa, a tym samym postawienie Trybunałowi zarzutu uzurpowania sobie uprawnień prawotwórczych (zob. postanowienia TK z 11 grudnia 2002 r., sygn. akt SK 17/02; 10 października 2012 r., sygn. akt Ts 38/12).

6. Formułując powyższe uwagi, Sejm nie zaprzecza wypowiedziom Trybunału dotyczącym modelowego sposobu uregulowania omawianych kwestii.

W wyroku z 12 grudnia 2005 r. (sygn. akt K 32/04) sąd konstytucyjny stwierdził, że: „Charakter czynności operacyjnych uzasadnia ich podejmowanie i prowadzenie w sposób tajny, a zatem bez wiedzy i zgody poddanego tym czynnościom, jednakże w warunkach zapewnienia kontroli sądowej dla zapobieżenia

wszelkiego rodzaju nadużyciom [...] Nic natomiast nie stoi na przeszkodzie, aby daną jednostkę poinformować *ex post* o dokonywanych wobec niej czynnościach kontrolnych, gdy nie byłoby to szkodliwe dla celu ingerencji [...]". Nie przeszkodziło to Trybunałowi w sformułowaniu jednoznacznego poglądu, iż „trudno jest uznać, że brak regulacji zawiadamiania o prowadzonych w przeszłości czynnościach operacyjnych jest pominięciem legislacyjnym możliwym do usunięcia w ramach kontroli konstytucyjności zaskarżonego przepisu”.

W następstwie wydania cytowanego wyżej orzeczenia, Trybunał Konstytucyjny zdecydował się na zasygnalizowanie Sejmowi potrzeby podjęcia inicjatywy ustawodawczej dotyczącej zagwarantowania w ustawie o Policji konstytucyjnych praw osób poddanych kontroli operacyjnej, wskazując, że istnienie obowiązku informowania przez Policję o bezskutecznej, zakończonej kontroli operacyjnej wobec osoby poddanej takiej kontroli, jeśli w stosunku do tej osoby nie są prowadzone dalsze czynności procesowe, „byłoby zapewne wskazane i odpowiadałoby potrzebie efektywnej instrumentalizacji proceduralnej konstytucyjnego prawa określonego w art. 51 ust. 4 Konstytucji” („Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą”).

Z kolei w wyroku z 30 lipca 2014 r. (sygn. akt K 23/11) Trybunał przyjął, że „ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie. Tego wymagania nie uchyla wprowadzenie innych, zastępczych rozwiązań, jak choćby pełnomocnika osoby kontrolowanej. [...] Zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji – ponieważ dokonało się to w sposób niejawnny, bez jej wiedzy i zgody – nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji. Obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla

postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności”.

7. W kontekście obowiązku stworzenia przez ustawodawcę takiego oprządkowania prawnego, które pozwoli na realizację przez jednostkę jej praw wynikających z art. 51 Konstytucji, należy podkreślić następujące okoliczności.

Obowiązujące uregulowania przewidują obowiązek niezwłocznego protokolarnego i komisijnego zniszczenia danych, które nie mają znaczenia dla postępowania karnego (zob. art. 20c ust. 7 ustawy o Policji oraz odpowiednie przepisy pozostałych ustaw pragmatycznych zakwestionowanych przez RPO). Natomiast jeżeli uzyskane materiały mają znaczenie dla postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazuje zebrane dane prokuratorowi właściwemu miejscowo lub rzeczowo; prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych (zob. art. 20c ust. 6 ustawy o Policji oraz stosowne przepisy pozostałych zakwestionowanych ustaw). Szczegółowe przepisy ustaw pragmatycznych regulują tryb postępowania z materiałami, o których mowa w art. 178, art. 178a, art. 180 § 2 i § 3 k.p.k., a zatem zawierającymi (mogącymi zawierać) dane stanowiące określone tajemnice, np. tzw. tajemnicę adwokacką, jednak zawsze zasadą jest albo zniszczenie zebranych materiałów, albo ich przekazanie prokuratorowi w celu wszczęcia (dalszego prowadzenia) postępowania karnego.

W świetle powyższego, wypowiedzi Trybunału dotyczące art. 51 Konstytucji nie dają się wprost aplikować do oceny przepisów zakwestionowanych przez RPO. Pozyskane dane są bowiem albo niszczone (co w sposób oczywisty wyklucza potrzebę uregulowania na poziomie ustaw pragmatycznych dostępu do nich oraz żądania sprostowania zawartych tam informacji), albo włączane jako materiał dowodowy w postępowaniu karnym udostępniany na zasadach przyjętych w k.p.k. W takim wypadku zarzuty niedostatecznego urzeczywistnienia prawa wyrażonego w art. 51 ust. 3 Konstytucji mogłyby być kierowane nie pod adresem ustaw pragmatycznych, a przepisów procedury karnej, co dodatkowo przekonuje, że w niniejszej sprawie mamy do czynienia z niepodlegającym kognicji Trybunału zaniechaniem ustawodawczym.

8. Na marginesie prowadzonych rozważań wypada wskazać, że kwestia wykonania sygnalizacji zawartej w postanowieniu TK o sygn. akt S 2/06, do której

wprost odwołuje się RPO, była przedmiotem interpelacji poselskiej nr 1559/VIII kad. Z 7 marca 2016 r. W przekazanej odpowiedzi z 27 kwietnia 2016 r. Sekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji stwierdził, że z uwagi na postępowanie przed Trybunałem wszczęte wnioskami PG i RPO [chodzi o postępowanie o sygn. akt K 32/15 – uwaga własna] „zasadnym jest wstrzymanie się z podejmowaniem decyzji dotyczących inicjatyw legislacyjnych w omawianym zakresie do czasu wydania orzeczenia TK w powyższej sprawie”. Niezależnie od powyższego, w odpowiedzi na interpelację stwierdzono wprost, że „zakończenie kontroli operacyjnej, w wyniku której nie uzyskano bezpośrednich dowodów pozwalających na wszczęcie postępowania karnego, jakkolwiek skutkować będzie niezwłocznym zniszczeniem materiałów zgromadzonych w jej trakcie, to jednakże w wielu przypadkach może nie kończyć zainteresowania operacyjnego daną osobą lub grupą osób. Może się bowiem zdarzyć, iż pomimo negatywnego wyniku stosowania kontroli operacyjnej, nadal prowadzone będą dalsze czynności operacyjne zmierzające do zebrania dowodów pozwalających na przedstawienie zarzutów. Czynności te trwają niekiedy wiele miesięcy. W tym czasie stosowane będą inne metody pracy operacyjnej. Ponadto w przypadku zorganizowanych grup przestępczych kontrola operacyjna często stosowana jest równolegle w stosunku do wielu osób i często terminy zakończenia kontroli wobec poszczególnych osób z danej grupy mogą być różne. Z tych względów umożliwienie osobie wglądu w zbiór informacji zgromadzonych na jej temat w związku z wykonywanymi działaniami operacyjno-rozpoznawczymi należy poprzedzić szczegółową analizą ewentualnych skutków, jakie ww. uprawnienie może nieść za sobą, aby wprowadzone przepisy prawa nie uniemożliwiły skutecznego zapobiegania niektórym rodzajom przestępstw, w szczególności np. przestępstw o charakterze terrorystycznym. Reasumując, ustawodawca wprowadzając uprawnienie do niejawnego realizowania zadań przez funkcjonariuszy Policji wyważył interes dobra państwa, ochrony życia i zdrowia ludzkiego oraz bezpieczeństwa publicznego i prawo jednostki do korzystania z praw i wolności obywatelskich, uznając o konieczności przyjęcia takich rozwiązań”.

Powyższa wypowiedź, adekwatna także w odniesieniu do pozyskiwania danych abonenckich, wspiera zdaniem Sejmu tezę, że w niniejszej sprawie mamy do czynienia z niepodlegającymi kontroli Trybunału zaniechaniem ustawodawczym.

Wobec powyższego zasadny jest wniosek u **umorzenie postępowania** na podstawie art. 59 ust. 1 pkt 2 ustawy o TK ze względu na niedopuszczalność wydania wyroku w części obejmującej kontrolę tych przepisów w zakresie, w jakim

nie regulują obowiązków informacyjnych wobec osób, których dane były pozyskiwane.

3. Trzecie zagadnienie przedstawione przez Rzecznika wiąże się z określeniem czasu przez, który uprawnione podmioty mogą przetwarzać pozyskane dane.

W tym miejscu należy doprecyzować zakres zaskarżenia oraz ocenić trafność oraz poprawność określenia wzorców kontroli. Lektura uzasadnienia wniosku RPO prowadzi do wniosku, że kwestionuje on brak stosownej regulacji określającej czas przechowywania przez służby pozyskanych danych telekomunikacyjnych, pocztowych, internetowych, które okazały się przydatne z punktu widzenia postępowania karnego i które zostały przekazane prokuratorowi (Prokuratorowi Generalnemu). Brak stosownej regulacji w tym zakresie powoduje w ocenie Rzecznika, że w praktyce służby po przekazaniu danych prokuratorowi (Prokuratorowi Generalnemu) mogą je w dalszym ciągu przechowywać w swoich systemach i czynić z nich użytek. Zaprezentowana argumentacja uprawdopodobnia – zdaniem Sejmu – że w niniejszym przypadku mamy do czynienia z podlegającym kognicji Trybunału pominięciem prawodawczym. Istotnie jest bowiem tak, że w zakwestionowanych przepisach nie określono okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane.

Rzecznik nie przedstawił argumentacji bezpośrednio wiążącej opisany wyżej zarzut z powołanymi wzorcami kontroli. Wskazał jednak, że kwestionowane pominięcie stoi w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922; dalej: u.o.d.o.) „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”. Artykuł 26 ust. 1 pkt 4 u.o.d.o. stanowi, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Wydaje się, że odwołanie się przez Rzecznika do owej zasady można uznać za argument na rzecz uchybienia przez zaskarżony przepis art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji., z których to przepisów wynika m.in. zakaz gromadzenia informacji

o obywatelach innych niż niezbędne w demokratycznym państwie prawnym. Nie ulega wątpliwości, że owa niezbędność powinna być oceniana także w aspekcie czasowym. Innymi słowy gromadzenie danych jest dopuszczalne tak długo, jak jest to niezbędne dla realizacji konstytucyjnie legitymowanego celu, w którym je pozyskano. W odniesieniu do pozostałych wzorców kontroli uzasadnienie nie może zostać uznane za spełniające formalne wymagania wyrażone w ustawie o TK, toteż zasadny jest wniosek o **umorzenie postępowania** w tym zakresie ze względu niedopuszczalność wydania wyroku.

VIII. Zasady niszczenia danych telekomunikacyjnych, pocztowych i internetowych pozyskanych przez ABW i SKW.

VIII.1. Przedmiot kontroli

1. Artykuł 28 ust. 7 ustawy o ABW: „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu”.

Artykuł 32 ust. 9 ustawy o SKW: „Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla obronności Państwa, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu”.

2. Wnioskodawca zaskarżył cytowane przepisy w zakresie, w jakim nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych, niemających znaczenia dla prowadzonego postępowania karnego.

VIII.2. Zarzuty wnioskodawcy

Rzecznik wskazuje na niekonstytucyjność przepisów dotyczących pozyskiwania przez Agencję Bezpieczeństwa Wewnętrznego oraz Służbę Kontrwywiadu Wojskowego danych telekomunikacyjnych, pocztowych i internetowych. Zakwestionowane regulacje zezwalają na zachowanie (wyłączają obowiązek zniszczenia) materiałów zawierających nie tylko dane, które mają znaczenia dla postępowania karnego, ale również takich, które są istotne dla bezpieczeństwa (ABW) albo obronności (SKW) państwa. W tej części uzasadnienia

wnioskodawca odwołuje się do wyroku TK z 30 lipca 2014 r. (sygn. akt K 23/11), w którym stwierdzono niekonstytucyjność odnośnych przepisów ustaw ABW i SKW w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania karnego.

VIII.3. Analiza formalnoprawna

1. Analogicznie jak miało to miejsce w poprzednio ocenionych zarzutach Rzecznik nie wywodzi odmiennych treści normatywnych z międzynarodowych wzorców kontroli. Brak również w tym zakresie odrębnej argumentacji.

W petitum swojego wniosku, precyzując zakres zaskarżenia, Rzecznik wspomina o „prowadzonym postępowaniu karnym”. Sejm pragnie podkreślić, że w obowiązującym stanie prawnym ABW oraz SKW nie prowadzą postępowania karnego. W związku z tym argumentacja Rzecznika odnosząca się do niezgodności prowadzenia przez nie tego postępowania, co uzasadniałoby w ocenie wnioskodawcy niezgodność kwestionowanych artykułów z Konstytucją, jest zawieszona w próżni. Do wniosku Rzecznika znajdują zastosowanie przepisy ustawy o TK, a w szczególności art. 46 oraz art. 47. Zgodnie z art. 46 ustawy o TK: „Pismami procesowymi są wnioski, pytania prawne i skargi konstytucyjne, a także inne wnioski i oświadczenia uczestników postępowania, wnoszone do Trybunału w toku postępowania poza rozprawą”. Art. 47 ustawy o TK stanowi: „1. Wniosek złożony przez podmiot, o którym mowa w art. 191 ust. 1 pkt 1-5 Konstytucji, zawiera: 1) oznaczenie podmiotu uprawnionego do złożenia wniosku; 2) podanie podstawy prawnej działania podmiotu uprawnionego do złożenia wniosku; 3) oznaczenie rodzaju pisma procesowego; 4) określenie kwestionowanego aktu normatywnego lub jego części; 5) wskazanie wzorca kontroli; 6) uzasadnienie. 2. Uzasadnienie, o którym mowa w ust. 1 pkt 6, zawiera: 1) przywołanie treści kwestionowanego wnioskiem przepisu wraz z jego wykładnią; 2) przywołanie treści wzorców kontroli wraz z ich wykładnią; 3) określenie problemu konstytucyjnego i zarzutu niekonstytucyjności; 4) wskazanie argumentów lub dowodów na poparcie zarzutu niekonstytucyjności. [...]”. Należy ponadto przypomnieć, że Trybunał Konstytucyjny związany jest zarzutami sformułowanymi w piśmie procesowym (wniosku, pytaniu prawnym, skardze konstytucyjnej), pochodzącym od podmiotu uprawnionego do inicjowania postępowania. Niemniej jednak zarzuty te mogą podlegać rozpatrzeniu tylko wtedy, jeżeli zostały należycie uzasadnione. Jak podkreślił Trybunał

Konstytucyjny: „Przesłanka odpowiedniego uzasadnienia zarzutów nie powinna być traktowana powierzchownie i instrumentalnie. Przytaczane w piśmie procesowym argumenty mogą być mniej lub bardziej przekonujące [...], lecz zawsze muszą być argumentami «nadającymi się» do rozpoznania przez Trybunał Konstytucyjny” (wyrok TK z 19 października 2010 r., sygn. akt P 10/10). Konieczność uzasadnienia zarzutu sformułowanego w piśmie inicjującym postępowanie przed Trybunałem Konstytucyjnym wynika z domniemania konstytucyjności norm prawnych oraz z zasady kontrydiktoryjności.

2. Zgodnie z wypowiedziami Trybunału Konstytucyjnego: „Kontrola konstytucyjności ustaw przebiega w oparciu o domniemanie, że badane normy są zgodne z konstytucją. 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 naruszeniu uległaby zasada kontrydiktoryjności postępowania przed Trybunałem Konstytucyjnym, a Trybunał przekształciłby się w organ orzekający z inicjatywy własnej” (zob. orzeczenie TK z 24 lutego 1997 r., sygn. akt K 19/96 oraz orzeczenia TK z: 26 kwietnia 1995 r., sygn. akt K 11/94; 31 stycznia 1996 r., sygn. akt K 9/95; wyroki TK z: 27 czerwca 2008 r., sygn. akt K 51/07; 15 lipca 2009 r., sygn. akt K 64/07; 12 stycznia 2012 r., sygn. akt Kp 10/09). Jak wskazuje się w literaturze, wymóg uzasadnienia powołanych zarzutów oznacza konieczność przedstawienia argumentów, które przemawiają za stwierdzeniem niezgodności zaskarżonych norm prawnych z normami powołanymi jako podstawa kontroli. Wymóg ten odnosi się do każdego z podniesionych zarzutów niezgodności danej normy (zob. K. Wojtyczek, *Ciężar dowodu i argumentacji w procedurze kontroli norm przez Trybunał Konstytucyjny*, „Przegląd Sejmowy” 2004, nr 1, s. 17; L. Jamróz, *Skarga konstytucyjna. Wstępne rozpoznanie*, Białystok 2011, s. 191).

3. Zgodnie z orzecznictwem TK „przesłanka odpowiedniego uzasadnienia zarzutów w kontekście każdego wzorca kontroli nie powinna być traktowana powierzchownie i instrumentalnie” (wyrok TK z 23 października 2012 r., sygn. akt SK 11/12). Powyższe oznacza, że nie wystarczy sformułowanie samej tezy o niekonstytucyjności zaskarżonego przepisu. Uzasadnienie musi wskazywać precyzyjnie co najmniej jeden argument przemawiający za naruszeniem danego

wzorca kontroli. Wymogu tego nie spełniają uwagi nazbyt ogólne, niejasne czy też czynione jedynie na marginesie innych rozważań (zob. np. wyrok TK z 5 czerwca 2014 r., sygn. akt K 35/11; postanowienie TK z 13 stycznia 2015 r., sygn. akt K 44/13). W opinii Trybunału: „Wobec respektowania generalnej zasady, jaką jest domniemanie konstytucyjności aktu normatywnego, samo wskazanie w petitum wzorca kontroli, bez szczegółowego odniesienia się w uzasadnieniu do kwestionowanej regulacji prawnej lub lakoniczne sformułowanie zarzutu niekonstytucyjności nie może zostać uznane za «uzasadnienie postawionego zarzutu, z powołaniem dowodów na jego poparcie» w rozumieniu przepisów regulujących postępowanie przed Trybunałem Konstytucyjnym. W świetle utrwalonej praktyki orzeczniczej wymóg ten należy rozumieć jako nakaz odpowiedniego udowodnienia zarzutów stawianych w kontekście każdego wskazanego wzorca kontroli” (postanowienie TK z 21 stycznia 2015 r., sygn. akt K 13/13)”. W związku z niedopełnieniem przez Rzecznika obowiązku należytego uzasadnienia podnoszonych zarzutów oraz umiejscowienia ich w obowiązującym stanie prawnym Sejm wnosi o **umorzenie postępowania** w przedmiocie art. 28 ust. 7 ustawy o ABW oraz art. 32 ust. 9 ustawy o SKW na podstawie art. 59 ust. 1 pkt 3 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym ze względu na zbędność orzekania.

IX. Stosowanie przepisów zakwestionowanych przez Trybunał Konstytucyjny

IX.1. Przedmiot kontroli

1. Zgodnie z art. 13 ustawy zmieniającej: „Do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu, stosuje się przepisy dotychczasowe”. Natomiast art. 16 u.z. stanowi: „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”.

2. Rzecznik Praw Obywatelskich zaskarżył wskazane wyżej regulacje w zakresie, w jakim nakazują stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

IX.2. Zarzuty wnioskodawcy

Rzecznik Praw Obywatelskich zakwestionował konstytucyjność dwóch przepisów przejściowych (art. 13, art. 16) zawartych w ustawie zmieniającej. Przepisy te nakazują stosowanie – do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu – regulacji dotychczasowych, w tym tych, które zostały uznane za niezgodne z Konstytucją wyrokiem Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11).

Przyjęta przez ustawodawcę technika legislacyjna prowadzi – zdaniem RPO – do naruszenia konstytucyjnych zasad: przyzwoitej legislacji, zaufania obywatela do państwa, pewności prawa, a także ostateczności i powszechnej mocy obowiązującej wyroków Trybunału Konstytucyjnego.

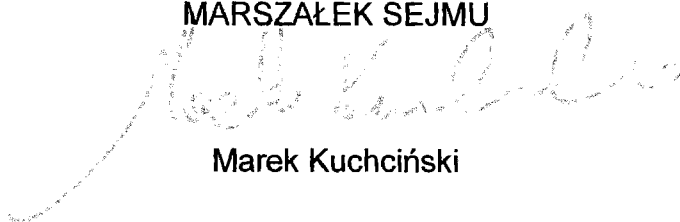
IX.3. Analiza formalnoprawna

1. W pierwszej kolejności należy ustosunkować się do przyjętego przez Rzecznika zakresu zaskarżenia. Rzecznik Praw Obywatelskich kwestionuje bowiem zaskarżone przepisy w zakresie, w jakim przestały obowiązywać na mocy wyroku TK wydanego w sprawie o sygn. akt K 23/11. Należy mieć jednak na uwadze, że 18-miesięczny termin odroczenia utraty mocy obowiązującej przez przepisy wobec których Trybunał zastosował we wspomnianym wyroku art. 190 ust. 3 Konstytucji upływał z dniem 6 lutego 2016 r. Natomiast ustawa zmieniająca, którą dokonano nowelizacji przepisów zakwestionowanych przez Trybunał, weszła w życie 7 lutego 2016 r.

Zgodnie z art. 59 ust. 3 ustawy o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym nie ma możliwości dokonania przez Trybunał Konstytucyjny kontroli norm, które utraciły moc obowiązującą, w innym postępowaniu niż wszczęte w drodze skargi konstytucyjnej. W związku z tym Sejm wnosi o umorzenie postępowania w zakresie 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 uwagi na utratę mocy obowiązującej przez przepisy do których

odsyłały wyżej wymienione artykuły przed wydaniem orzeczenia przez Trybunał Konstytucyjny" na podstawie art. 59 ust. 1 pkt 4 ustawy o TK.

MARSZAŁEK SEJMU

A handwritten signature in dark ink, appearing to read 'Marek Kuchciński', written over the printed name.

Marek Kuchciński