RZĄDOWE CENTRUM LEGISLACJI
DEPARTAMENT PRAWNY
I ORZECZNICTWA

Warszawa, dnia 8 grudnia 2014 r.

RCL.DPiO 5604-99/14

ANALIZA
WYROKU TRYBUNAŁU KONSTYTUCYJNEGO
Z DNIA 30 LIPCA 2014 R., SYGN. AKT K 23/11

I. INFORMACJE O ORZECZENIU:

1. Metryka orzeczenia:

Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11. Sentencja orzeczenia została ogłoszona w Dzienniku Ustaw Rzeczypospolitej Polskiej z dnia 6 sierpnia 2014 r., pod poz. 1055.

2. Sentencja orzeczenia:

1) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.) jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji;

2) Przepisy:

a) art. 20c ust. 1 ustawy 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, z późn. zm.),

b) art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675, z późn. zm.),

c) art. 36b ust. 1 pkt 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, z późn. zm.),

d) art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych Dz. U. z 2013 r. poz. 568, z późn. zm.),

e) art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

f) art. 32 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.),

g) art. 18 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, z późn. zm.),

h) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.)

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

3) Przepisy:

a) art. 19 ustawy o Policji,

b) art. 9e ustawy o Straży Granicznej,

c) art. 36c ustawy o kontroli skarbowej,

d) art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

e) art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

f) art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

g) art. 17 ustawy o Centralnym Biurze Antykorupcyjnym

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

4) Przepisy:

a) art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

b) art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

c) art. 18 ustawy o Centralnym Biurze Antykorupcyjnym

– w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji,

5) art. 75d ust. 5 ustawy o Służbie Celnej w zakresie, w jakim zezwala na zachowanie

materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, ze zm.), jest niezgodny z art. 51 ust. 4 Konstytucji.

3. Utrata mocy obowiązującej niekonstytucyjnej regulacji:

Przepisy wymienione w pkt 1-4, uznane przez Trybunał za niezgodne z Konstytucją utracą moc obowiązującą z upływem 18 miesięcy od dnia ogłoszenia wyroku w Dzienniku Ustaw RP, tj. z dniem 7 lutego 2016 r. W przypadku art. 75d ust. 5 ustawy o Służbie Celnej, z uwagi na zakresowy charakter sentencji wyroku, w której Trybunał wskazał na brak ograniczeń ustawodawczych w kwestii zachowywania materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 Kodeksu karnego skarbowego, przepis ten nie traci mocy obowiązującej z dniem ogłoszenia sentencji wyroku. Natomiast z ww. dniem zostało obalone domniemanie konstytucyjności wskazanej w sentencji treści normatywnej wywodzonej z tej regulacji.

4. Stan prawny (na gruncie którego wydano orzeczenie):

Przedmiotem kontroli Trybunału Konstytucyjnego były przepisy ustaw zawierających regulacje dotyczące kontroli operacyjnej w odniesieniu do „przestępstw godzących w podstawy ekonomiczne państwa", pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych w ustawach: o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (dalej: ustawa o ABW), Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (dalej ustawa o SKW) i o Centralnym Biurze Antykorupcyjnym (dalej: ustawa o CBA).

W pierwszej grupie kontrolowanych zagadnień znalazła się norma wyrażona w art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW, zgodnie z którą przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez ABW w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną. Zadania, o których mowa w art. 5 ust. 1 pkt 2 dotyczą rozpoznawania, zapobiegania

i wykrywania przestępstw godzących w podstawy ekonomiczne państwa.

Następną grupę zakwestionowanych przez Trybunał rozwiązań stanowią przepisy regulujące procedurę udostępniania służbom danych telekomunikacyjnych, o których mowa w art. 180c oraz w art. 180d ustawy z dnia 10 lipca 2004 r. - Prawo telekomunikacyjne, tj. art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej (dalej: ustawa o SG), art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych (dalej: ustawa o ŻW), art. 28 ust. 1 pkt 1 ustawy o ABW, art. 18 ust. 1 pkt 1 ustawy o CBA, art. 32 ust. 1 pkt 1 ustawy o SKW i art. 75d ust. 1 ustawy o Służbie Celnej (dalej: ustawa o S.C.).

Wspólną cechą wymienionych powyżej regulacji jest możliwość dostępu podmiotów uprawnionych, wskazanych w ww. ustawach, do danych telekomunikacyjnych dotyczących ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz użytkownika, do którego kierowane jest połączenie, a także określających daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego. Przywołane regulacje wprost wyłączają kontrolę sądową zarówno wstępną, jak i następczą uzyskania tych danych, jak również udział pracownika podmiotu prowadzącego działalność telekomunikacyjną, gdyż ustawa – w jednym ze sposobów pozyskiwania danych – dopuszcza ich nieodpłatne udostępnienie za pośrednictwem sieci telekomunikacyjnej. Przykładowa treść zakwestionowanych regulacji, wspólna dla ustawy o Policji, ustawy o SG, ustawy o kontroli skarbowej, ustawy o ŻW oraz ustawy o SC ma następujące brzmienie: *„W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 i 827), zwane dalej "danymi telekomunikacyjnymi" oraz może je przetwarzać.".* Natomiast przedmiotowa regulacja przewidziana dla Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego stanowi, iż: *„Obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez ABW zadań, o których mowa w art. 5 ust. 1, w postaci danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).".*

Kolejna grupa przepisów poddana ocenie Trybunału dotyczy braku regulacji wyłączających stosowanie czynności operacyjno-rozpoznawczych (tj. kontroli operacyjnej i pozyskiwania wzmiankowanych powyżej danych telekomunikacyjnych) wobec podmiotów zobowiązanych do zachowania tajemnicy zawodowej oraz braku procedury niszczenia

zebranych w toku tychże czynności danych, które stanowią przedmiotową tajemnicę. Zarzuty takiego pominięcia prawodawczego sformułowane zostały wobec treści art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 17 ustawy o CBA oraz art. 31 ustawy o SKW. W ocenie wnioskodawców, przepisy te, uprawniające określone podmioty do stosowania czynności operacyjno-rozpoznawczych, winny uwzględniać konieczność ochrony tajemnicy zawodowej, której zniesienie jest dopuszczalne jedynie, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a określonej okoliczności nie można ustalić na podstawie innych dowodów. Tajemnica zawodowa, która podlega szczególnej ochronie obejmuje tajemnicę adwokacką, dziennikarską, notarialną, radcy prawnego, doradcy podatkowego oraz lekarską.

Problemem, który również poddany został krytycznej ocenie Trybunału Konstytucyjnego jest brak unormowania w ustawie obowiązku zniszczenia danych telekomunikacyjnych, które są nieprzydatne (zbędne) w postępowaniu, w ramach którego je uzyskano. Zarzuty dotyczące wskazanego powyżej braku sformułowane zostały wobec art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW, które to przepisy umożliwiając pozyskiwanie określonych danych, nie przewidują obowiązku zniszczenia tych spośród nich, które zawierają informacje nieistotne dla prowadzonego postępowania. Problem konstytucyjny dotyczy więc pominięcia ustawodawczego.

Kontrolą Trybunału w podobnym zakresie objęty został również art. 75d ustawy o SC, który ma następujące brzmienie: „Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu". Przepis ten zobowiązuje wprawdzie Służbę Celną do zniszczenia nieprzydatnych w postępowaniu danych telekomunikacyjnych, jednakże zniszczeniu podlegają materiały, które nie mają znaczenia dla postępowania w sprawach o przestępstwa skarbowe, co dopuszcza przedstawioną wykładnię, iż uzyskane materiały mogą być przechowywane na potrzeby postępowań w sprawach innych niż o przestępstwa skarbowe, o których mowa w rozdziale 9 Kodeksu karnego skarbowego.

Powołany wzorzec konstytucyjny:

Regulacja wskazana w pierwszej grupie, dotycząca dopuszczalności prowadzenia kontroli operacyjnej w celu rozpoznawania, zapobiegania i wykrywania przestępstw godzących w podstawy ekonomiczne państwa została przez Trybunał oceniona krytycznie względem art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji. Przyczyną takiej oceny Trybunału było

uznanie, iż wyrażenie „przestępstwa godzące w podstawy ekonomiczne państwa" uniemożliwia identyfikację typów przestępstw, określonych przez ustawę karną.

Wzorzec konstytucyjny, jaki został powołany w ramach kontroli powyżej wskazanej regulacji odnosił się do art. 47 Konstytucji, który gwarantuje każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym oraz wyrażonych w treści art. 49 Konstytucji, gwarancji wolności i ochrony tajemnicy komunikowania się. Jak przyjmuje się w orzecznictwie, art. 47 i art. 51 Konstytucji chronią tę samą wartość konstytucyjną – sferę prywatności. Autonomia informacyjna stanowi istotny element składowy prawa do ochrony prywatności, a polega na samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi informacjami, nawet jeśli znajdują się w posiadaniu innych osób.

Z ochroną prywatności i autonomii informacyjnej koresponduje też prawo do ochrony tajemnicy komunikowania się, ustanowione w art. 49 Konstytucji. Konstytucyjną ochroną wynikającą z art. 49 Konstytucji objęta jest tym samym treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania się na odległość. Według Trybunału, przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe. Z punktu widzenia prawa do ochrony tajemnicy komunikowania się, 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 w sposób uzasadniony 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.

Mając powyższe na uwadze, Trybunał Konstytucyjny stwierdził, 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.

Przepisy te zrelacjonowane zostały do - mieszczącej się w treści klauzuli demokratycznego państwa prawnego wyrażonej w art. 2 Konstytucji – zasady określoności prawa, która definiowana jest przez Trybunał, jako obowiązek ustawodawcy zapewnienia regulacjom określającym status jednostki maksymalnego stopnia określoności. Na ustawodawcy ciąży zatem obowiązek tworzenia przepisów prawa możliwie najbardziej określonych w danym wypadku pod względem zarówno ich treści, jak i formy. W związku z powyższym każde unormowanie regulujące status jednostki w państwie powinno cechować się „poprawnością", „precyzyjnością" i „jasnością".

Każdy przepis prawny winien być skonstruowany poprawnie z punktu widzenia językowego i logicznego. Dopiero po spełnieniu tego podstawowego warunku można ocenić przepis w aspekcie pozostałych kryteriów wynikających z zasady określoności prawa. W ocenie Trybunału przepisy ustawowe ograniczające konstytucyjne wolności lub prawa muszą być zatem sformułowane w sposób pozwalający jednoznacznie ustalić, kto i w jakiej sytuacji podlega ograniczeniom przez organy państwa. Przepisy te muszą być na tyle precyzyjne, by je stosowano i interpretowano w jednolity sposób. Wreszcie muszą być one tak ujęte, by zakres ich zastosowania obejmował wyłącznie sytuacje, w których racjonalny ustawodawca zamierzał wprowadzić regulację ograniczającą korzystanie z konstytucyjnych wolności i praw. Przekładając powyższe ustalenia na unormowanie ingerencji w wolności i prawa konstytucyjne w związku ze stosowaniem przez służby policyjne lub służby ochrony państwa czynności operacyjno-rozpoznawczych, zdaniem Trybunału, jednostka na podstawie przepisu ustawy powinna wiedzieć, kto oraz w jakim zakresie podmiotowym, przedmiotowym i czasowym jest uprawniony do niejawnej ingerencji w szeroko rozumianą sferę prywatności.

Precyzyjne określenie tej kwestii przez ustawodawcę nie tylko wiąże się z realizacją zasady określoności prawa wynikającą z art. 2 Konstytucji, ale przede wszystkim z tą częścią art. 31 ust. 3 Konstytucji, która przewiduje obowiązek unormowania ustawowego ograniczenia w korzystaniu z wolności i praw konstytucyjnych. W świetle wyrażonej w tym ostatnim przepisie zasady proporcjonalności, niejawne pozyskiwanie informacji przez służby policyjne

i ochrony państwa ma bowiem służyć wzmocnieniu poziomu ochrony wartości istotnych w państwie demokratycznym, co byłoby niemożliwe do osiągnięcia z wykorzystaniem innych rozwiązań, mniej ingerujących w sferę wolności lub praw jednostek. Jednocześnie muszą to być środki najmniej uciążliwe dla podmiotów, których wolności lub prawa ulegają ograniczeniu, stosowane absolutnie wyjątkowo, w celu wykrywania i ścigania poważnych przestępstw.

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

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

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

Zważywszy, że Kodeks karny ani inne ustawy nie posługują się wyrażeniem „przestępstwa godzące w podstawy ekonomiczne państwa", zarówno gdy chodzi o nazwy

rodzajowe poszczególnych czynów zabronionych, ich elementy definicyjne, czy tytuły rozdziałów ustaw karnych, w których zebrane są przestępstwa danego rodzaju, brak jest podstawy do ustalenia możliwego zakresu normowania obowiązującej regulacji. Ustalenie tego zakresu normowania nie dokonało się również na gruncie praktyki orzeczniczej. Jako, że nie udało się usunąć niejasności tego przepisu w ramach sądowej wykładni, jednostka nie jest świadoma rzeczywistego zakresu ograniczeń prywatności oraz granic legalnej ingerencji w tajemnicę komunikowania się.

W ocenie Trybunału Konstytucyjnego, co do zasady, nie jest niezgodne z Konstytucją zdefiniowanie ustawowych zadań organu państwa – w tym wypadku służby ochrony państwa właściwej w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego - w sposób ogólny, z wykorzystaniem pojęć nieostrych. Jeżeli jednak ustawodawca określa kompetencje powierzone danej formacji, w następstwie których dochodzić może do niejawnej ingerencji w wolności osobiste, powinien on wykazać się daleko idącą precyzją, tak by ustawowe przesłanki niejawnej ingerencji możliwe były do ustalenia na podstawie wykładni językowej przepisów ustawy, bez odwoływania się do wykładni systemowej czy funkcjonalnej.

Zakwestionowany przepis, przez zastosowanie nieostrego pojęcia oraz nieuwzględnienie elementów normy karnej takich jak szkodliwości popełnionego czynu, czy rozmiar wyrządzonej szkody, stanowi głęboką ingerencję w sferę prywatności i tajemnicę komunikowania się. Brak możliwości ustalenia w jakich dokładnie sytuacjach ABW może stosować kontrolę operacyjną, powołując się na przesłankę zawartą w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, uniemożliwia również stwierdzenie, iż środek pozyskiwania informacji o osobach jest przydatny i konieczny, w rozumieniu art. 31 ust. 3 Konstytucji, w każdym ustawowo dopuszczalnym wypadku.

Powyższe względy przesądzają za uznaniem, iż art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji

Następną kwestią ocenianą przez Trybunał w ramach kontroli zgodności regulacji ustawowych z konstytucyjnym wzorcem, określonym w art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, były wskazane w piątym punkcie sentencji wyroku, przepisy regulujące procedurę udostępniania służbom danych telekomunikacyjnych, o których mowa w art. 180c oraz w art. 180d Prawa telekomunikacyjnego. Przyjmując, iż również do tych regulacji aktualność zachowuje przedstawiony powyżej wzorzec konstytucyjny, Trybunał stwierdził, iż regulacje te upoważniają określone w nich podmioty do gromadzenia oraz przetwarzania

danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, a także określają przedmiotowe przesłanki udostępniania tych danych. Przypominając, iż ingerencja w konstytucyjne prawo do ochrony prywatności (art. 47) i tajemnicę komunikowania się (art. 49 Konstytucji) może mieć miejsce nie tylko w wypadku zapoznawania się organów władzy publicznej z samą treścią komunikatów przekazywanych między jednostkami, ale również w sytuacji pozyskania przez władze informacji towarzyszących temu procesowi, Trybunał stwierdził, iż jednym z wymagań, które powinny spełniać przepisy ustawowe upoważniające do pozyskiwania danych telekomunikacyjnych, jest wykreowanie mechanizmu niezależnej kontroli takich działań. Brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji. Zauważyć ponadto należy, iż ustawodawca nie uzależnił możliwości żądania danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia lub wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji, w wyniku czego większe znaczenie ma ustanowienie gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych.

Żaden z zakwestionowanych przepisów nie nakłada obowiązku uzyskania zgody sądu (bądź innego organu, który byłby niezależny od organów żądających udostępnienia tych danych lub organów nad nimi nadrzędnych) na udostępnienie uprawnionym podmiotom danych telekomunikacyjnych. Procedura ta nie wymaga nawet uzyskania zgody prokuratora. Ustawodawca nie przewidział też zrębowych elementów kontroli *ex post,* legalizującej podjęte działania. Pozyskiwanie danych telekomunikacyjnych przez uprawnione organy pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane.

Mając powyższe na uwadze, zakwestionowane przepisy ustaw (wymienione w pkt 5 sentencji wyroku) przez to, że nie przewidują niezależnej kontroli nad udostępnieniem danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

Kolejnym konstytucyjnym problemem poddanym ocenie Trybunału był brak określonej treści normatywnej (gwarancji niezwłocznego i protokolarnego zniszczenia

materiałów objętych zakazami dowodowymi), która w świetle art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji, winna zostać zawarta w art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 31 ustawy o ŻW, art. 36c ustawy o kontroli skarbowej, art. 27 ustawy o ABW, art. 17 ustawy o CBA oraz art. 31 ustawy o SKW.

Uzupełniając przedstawiony powyżej wzorzec o gwarancję wynikającą z art. 42 ust. 2 Konstytucji, który wyraża podmiotowe prawo do obrony we wszystkich stadiach postępowania karnego, w ocenie Trybunału, w kontrolowanych przepisach brak jest dostatecznych gwarancji proceduralnych zapewniających ochronę poufności informacji przekazywanych podmiotom wykonującym zawody zaufania publicznego. Zarówno ze względu na wątpliwości interpretacyjne co do obowiązku uprzedniej, sądowej kontroli zgromadzonych danych, jak i ewentualnego zwolnienia (uchylenia) z tajemnicy zawodowej w konkretnej sprawie, brak jest gwarancji ustawowych, że w sytuacji uzasadnionego podejrzenia, że zgromadzone materiały zawierają informacje objęte tajemnicę zawodową i z tego powodu wymagają szczególnej ochrony, nastąpi dodatkowa weryfikacja tych materiałów przez sąd i ewentualne zwolnienie z tajemnicy zawodowej, zanim zostaną przekazane funkcjonariuszom służb bądź prokuratorowi.

Zdaniem Trybunału, zakwestionowane przepisy nie przewidują również procedury niszczenia zebranych w toku kontroli operacyjnej informacji, stanowiących tajemnicę zawodową.

Wyjątkowo negatywnie Trybunał ocenił też brak stosownych rozwiązań w odniesieniu do tych tajemnic zawodowych, które z uwagi na ich znaczenie dla urzeczywistnienia takich wartości, jak prawo do obrony oraz wolność prasy, powinny podlegać szczególnej ochronie przed ujawnianiem ich treści służbom stosującym kontrolę operacyjną. Jakkolwiek możliwość niejawnego uzyskiwania informacji objętych tajemnicą obrończą, sama w sobie nie narusza jeszcze istoty prawa do obrony (oskarżony może bowiem korzystać z pomocy prawnej obrońcy, komunikując się z nim osobiście bez wykorzystywania takich kanałów komunikacji, które mogą być objęte kontrolą operacyjną), to jednak, zdaniem Trybunału Konstytucyjnego, ustawodawca nie przeciwdziałał należycie głębokim naruszeniom tego prawa przez służby policyjne i ochrony państwa. Podobne argumenty przemawiają za negatywną oceną zaskarżonych unormowań w odniesieniu do wzorca kontroli w niniejszej sprawie, którym jest art. 54 ust. 1 Konstytucji, gwarantujący ochronę tajemnicy dziennikarskiej. Ustawa nie wyklucza bowiem uzyskania przez funkcjonariuszy Policji materiałów o istotnym znaczeniu dla niezależnego dziennikarstwa, jakimi są np. dane informatorów, i zapoznania się z takimi materiałami. Trybunał przypomniał, że minimalnym standardem w odniesieniu do ochrony

poufności kontaktów oskarżonego z obrońcą i poufności tożsamości dziennikarskich źródeł informacji jest istnienie kontroli sądowej weryfikującej zebrane przez Policję w toku czynności operacyjno-rozpoznawczych materiały, co do których istnieje uzasadnione prawdopodobieństwo, że zawierają treści stanowiące prawnie chronioną tajemnicę zawodową, oraz zarządzającej wyłączenie z dalszego wykorzystania tych materiałów, które są istotne z punktu widzenia ochrony relacji zaufania.

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

Natomiast art. 28 ustawy o ABW, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW, określające zasady udostępniania danych telekomunikacyjnych przez przedsiębiorców telekomunikacyjnych podmiotom wskazanym w ich treści, zakwestionowane zostały z punktu widzenia braku regulacji przewidujących obowiązek oceny ich znaczenia dla postępowania oraz ich zniszczenia w przypadku stwierdzenia nieprzydatności tych danych. Konieczność taka została przez Trybunał wywiedziona z treści art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, które to przepisy zostały wskazane za wzorzec ochrony jednostki przed nieproporcjonalną ingerencją władz publicznych w sferę autonomii informacyjnej. Zgodnie bowiem z art. 51 ust. 2 Konstytucji władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. W ocenie Trybunału wykładnia zwrotu „informacje niezbędne w demokratycznym państwie prawnym" uwzględniać musi zasadę proporcjonalności wynikającą z art. 31 ust. 3 Konstytucji. W świetle tego przepisu niezbędność ingerencji w konstytucyjne wolności lub prawa uzasadniona może być tylko wtedy, gdy jest to 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.

W orzecznictwie Trybunału wykształciły się tezy uzasadniające zawarty w art. 51 ust. 2 Konstytucji dodatkowy zakaz pozyskiwania przez władze publiczne informacji o jednostkach, innych niż niezbędne. Przemawia za tym przekonanie, iż dla współczesnych czasów typowe są naruszenia autonomii informacyjnej poprzez żądanie niekoniecznych,

lecz wygodnych dla władzy publicznej informacji o jednostce. Normatywne wyodrębnienie „niezbędności" pozyskiwania danych ułatwia przeprowadzenie dowodu w celu wykazania, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne" lub „użyteczne" dla władzy. W orzecznictwie Trybunału przez pojęcie „niezbędności danych w demokratycznym państwie prawnym" rozumie się sytuację, w której nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny.

W ocenie Trybunału warunkiem niejawnego uzyskiwania informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów. Ingerencją w sferę prywatności jednostek będzie nie tylko jednorazowe pozyskanie danych o jednostce, ale również każde kolejne operacje na tych danych, w tym przechowywanie, czy wtórne wykorzystywanie w toku innych postępowań.

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

Trybunał Konstytucyjny nie neguje dopuszczalności dalszego przechowywania (to jest po ich analizie i stwierdzeniu ewentualnej nieprzydatności w prowadzonym postępowaniu w konkretnej sprawie) danych telekomunikacyjnych dotyczących cudzoziemców znajdujących się pod władzą Rzeczypospolitej Polskiej, w szczególności jeśli istnieją poważne i uzasadnione podejrzenia co do ich zaangażowania w działalność zagrażającą

bezpieczeństwu państwa, w tym w terroryzm i przestępczość zorganizowaną. Uzasadnienie takiego zróżnicowania ma bowiem swoje oparcie w treści art. 51 ust. 2 i art. 37 ust. 2 Konstytucji. Jednakże brak zawarcia w ustawie mechanizmu weryfikacji przydatności zebranych danych wobec obywateli polskich oraz nakazu ich zniszczenia w przypadku ich nieprzydatności dla prowadzonego postępowania prowadzi do stwierdzenia niezgodności zakwestionowanych regulacji z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji.

Odnosząc się natomiast do treści art. 75d ust 5 ustawy o SC, zgodnie z którym *„Materiały, uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu"*, Trybunał dokonał jego oceny w świetle gwarantowanego, przez art. 51 ust. 4 Konstytucji, prawa podmiotowego do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. W ramach interpretacji zwrotu „informacji (...) zebranych w sposób sprzeczny z ustawą" Trybunał rozróżnił trzy sytuacje: gdy uzyskiwanie danego rodzaju informacji jest w ogóle niedopuszczalne w świetle Konstytucji, gdy nie dokonuje się go na podstawie i w granicach przewidzianych wyraźnie w ustawie, gdy uzyskanie informacji (nawet konstytucyjnie lub ustawowo dopuszczalne) nastąpiło niezgodnie z procedurą określoną w prawie.

Zważywszy, że Służba Celna może pozyskiwać dane telekomunikacyjne w wąsko zakreślonym celu w postaci zapobiegania lub wykrywania przestępstw skarbowych przeciwko organizacji gier hazardowych, to już nie musi niszczyć materiałów, które co prawda nie mają znaczenia z punktu widzenia tego celu, lecz mają znaczenie dla innych postępowań w sprawach o wszelkie wykroczenia skarbowe lub przestępstwa skarbowe. Innymi słowy inny jest cel pozyskiwania danych telekomunikacyjnych przez Służbę Celną i inny jest cel ich przechowywania.

Podzielając zarzut Rzecznika Praw Obywatelskich, iż przepis art. 75d ust. 5 ustawy o Służbie Celnej może być wykładany w ten sposób, iż dane uzyskane przez organ zgodnie z ustawą, można następnie gromadzić i ewentualnie wykorzystać w innym celu, niż cel ich uzyskania, Trybunał uznał, iż taki sposób interpretacji zakwestionowanego przepisu nie odpowiada treści art. 51 ust. 4 Konstytucji.

II. SKUTKI ORZECZENIA:

Kierując się koniecznością ograniczenia wystąpienia ryzyka braku efektywnych

mechanizmów walki z zagrożeniami, a w konsekwencji wzrostu przestępczości bądź choćby osłabienia ich wykrywalności, Trybunał postanowił odroczyć utratę mocy obowiązującej uznanych za niezgodne z Konstytucją przepisów. Wyjątkiem jest art. 75d ustawy o SC, który uznano w sentencji za niezgodny z Konstytucją w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy, nie traci mocy obowiązującej, jednakże mocą powszechnie wiążącej sentencji wyroku TK, wykluczone jest zachowanie przez Służbę Celną materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 Kodeksu karnego skarbowego.

Pozostałe przepisy uznane za niezgodne z Konstytucją mogą być w okresie odroczenia utraty ich mocy obowiązującej stosowane przez organy władzy publicznej, jednakże przy uwzględnieniu utraty domniemania ich konstytucyjności.

III. WSKAZÓWKI DLA PRAWODAWCY:

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

Według Trybunału, najbardziej pożądanym rozwiązaniem z konstytucyjnego punktu widzenia jest uregulowanie rodzajów środków służących niejawnemu pozyskiwaniu informacji o jednostkach w ustawie. Precyzyjne określenie tej kwestii przez ustawodawcę nie tylko wiąże się z realizacją zasady określoności prawa wynikającą z art. 2 Konstytucji, ale przede wszystkim z tą częścią art. 31 ust. 3 Konstytucji, która przewiduje obowiązek

unormowania ograniczeń w korzystaniu z wolności i praw konstytucyjnych w ustawie. Zasadne jest tym samym, by to parlament zaakceptował dopuszczalność stosowania rodzajów środków technicznych, które w szerokim zakresie ingerują w wolności i prawa człowieka.

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

W ustawie ma być również uregulowana procedura zarządzania tymi czynnościami operacyjno-rozpoznawczych, włączywszy w to powierzenie kompetencji do zarządzania tymi czynnościami, a także badanie ich legalności przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej przez sąd. Ustawa ma wskazywać podstawowe elementy proceduralne, zasady wykorzystywania zgromadzonych materiałów oraz przesłanki, czy tryb ich niszczenia. Z punktu widzenia ochrony konstytucyjnych wolności i praw niezbędne jest zobowiązanie organów wnoszących o zarządzenie kontroli do wskazania określonego w prawie środka pozyskiwania informacji i dowodów w konkretnej sprawie oraz nałożenie na organy zarządzające takie czynności obowiązku wyrażenia zgody na konkretny rodzaj środka służącego pozyskiwaniu informacji. Konieczne jest także uregulowanie procedury raportowania z przeprowadzonych w sposób niejawny czynności i środków, gwarantujących przekazanie zapisów w stanie nienaruszonym, umożliwiającym ich późniejszą weryfikację. W powyższym zakresie nie jest konstytucyjnie akceptowalne unormowanie istotnych elementów procedury w wewnętrznych aktach normatywnych ustanawianych w ramach struktury organizacyjnej danej służby prowadzącej te czynności.

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

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

Trybunał Konstytucyjny nie wymaga jednocześnie by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. Konieczne jest natomiast, by był to organ niezależny od administracji rządowej i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to należałoby uznać za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej.

IV. WYKONANIE ORZECZENIA:

1. Potrzeba wykonania orzeczenia:

Z uwagi na wyznaczony przez Trybunał termin utraty mocy obowiązującej niezgodnych z Konstytucją przepisów, w celu uniknięcia ewentualnych luk prawnych oraz zmierzając do urzeczywistnienia zgodności z Konstytucją pozostałych kwestionowanych rozwiązań, konieczne jest pilne podjęcie prac legislacyjnych.

Pomimo, iż przedmiotem kontroli Trybunału w zakresie konieczności niszczenia danych telekomunikacyjnych, które nie mają znaczenia dla postępowania, nie były przepisy

ustawy o kontroli skarbowej (z uwagi na wadliwe odniesienie pominięcia prawodawczego), należy zauważyć, że ustawa ta nie przewiduje w swej treści tego rodzaju mechanizmu, (nie mieści się on w treści art. 36b ust. 5 tejże ustawy). Dlatego również przepisy ustawy o kontroli skarbowej winny być uzupełnione o wskazaną przez Trybunał gwarancję konstytucyjności.

Z uwagi na konieczność zapewnienia jasności i przejrzystości tekstu normatywnego, konieczna jest również interwencja legislacyjna wobec treści art. 75d ust. 5 ustawy o SC, który został uznany przez Trybunał za konstytucyjnie wadliwy w zakresie, w jakim nie zawiera wskazanego przez Trybunał ograniczenia przechowywania danych. Zakresowy charakter przedmiotowego uznania, nie skutkował wprawdzie derogacją przepisu z systemu prawnego, jednakże przepis ten nie może stanowić podstawy dla zatrzymania przez Służbę Celną materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 k.k.s.

Na marginesie analizy niniejszego wyroku zauważyć należy, że w ramach regulacji dotyczącej danych pozyskanych w toku czynności operacyjno-rozpoznawczych, nie można również tracić z pola widzenia skutków wyroku Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE) z dnia 8 kwietnia 2014 r, *Digital Rights Ireland Ltd* (C-293/14)., stwierdzającego nieważność dyrektywy 2006/24 w sprawie zatrzymywania danych z powodu braku proporcjonalności zawartych w niej rozwiązań. W konsekwencji prejudycjalnego wyroku TSUE, funkcjonujące w systemie prawa polskiego przepisy, ustanowione w celu implementacji tejże dyrektywy nie tracą wprawdzie mocy obowiązującej, jednakże brak jest konieczności obowiązywania regulacji krajowych, implementujących dyrektywę, którym również można postawić zarzut braku proporcjonalności. Zważywszy na powyższe względy przepisy określające dostęp uprawnionych podmiotów do przechowywanych przez przedsiębiorców danych telekomunikacyjnych powinny spełniać wymóg proporcjonalności w rozumieniu przyjętym przez TSUE i orzecznictwo Trybunału Konstytucyjnego.

2. Podmiot właściwy w zakresie objętym orzeczeniem:

Podmiotem właściwym w zakresie objętym tym wyrokiem jest Minister - Członek Rady Ministrów, koordynujący działalność Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego

Biura Antykorupcyjnego oraz Minister Spraw Wewnętrznych, Minister Obrony Narodowej i Minister Finansów.

3. Kierunek rozwiązań/brzmienie przepisu:

W celu wykonania przedmiotowego wyroku konieczne jest normatywne określenie granic i celu czynności operacyjno-rozpoznawczych podejmowanych przez ABW, przez jednoznaczne zapewnienie niezależnej kontroli pozyskiwania danych telekomunikacyjnych przez uprawnione podmioty, urzeczywistnienia ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz ustanowienia obowiązku niszczenia zbędnych danych telekomunikacyjnych przez podmioty uprawnione do ich pozyskania.

4. Etap prac nad projektem wykonującym orzeczenie:

Na stronie podmiotowej Rządowego Centrum Legislacji, w zakładce Rządowy Proces Legislacyjny, brak jest informacji wskazujących na podjęcie prac legislacyjnych zmierzających do wykonania ww. wyroku Trybunału Konstytucyjnego.

wykonujący obowiązki
DYREKTORA
Departamentu Prawnego i Orzecznictwa
dr Jacek Krawczyk

opr.: T. Golik, tel. 694-62-01