KANCELARIA SENATU

BIURO LEGISLACYJNE

BL–112–205–TK/14 Warszawa, 17 kwietnia 2015 r.

INFORMACJA PRAWNA O WYROKU TRYBUNAŁU KONSTYTUCYJNEGO Z DNIA 30 LIPCA 2014 R. (K 23/11) DOTYCZĄCYM KONTROLI OPERACYJNEJ STOSOWANEJ PRZEZ SŁUŻBY POLICYJNE I OCHRONY PAŃSTWA

I. METRYKA ORZECZENIA

Wyrok z dnia 30 lipca 2014 r. (sygn. akt K 23/11) dotyczy następujących aktów normatywnych:

– 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.; dalej jako: ustawa o ABW),

– ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, z późn. zm.),

– ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675, z późn. zm.),

– ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, z późn. zm.),

– ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 i 628; dalej jako: ustawa o ŻW),

– ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253 i 502; dalej jako: ustawa o SKW),

– ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, z późn. zm.; dalej jako: ustawa o CBA),

– ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 oraz z 2014 r. poz. 486).

Sentencja orzeczenia została opublikowana w Dz. U. z dnia 6 sierpnia 2014 r., poz. 1055. Pełny tekst orzeczenia wraz z uzasadnieniem ukazał się w OTK ZU z 2014 r. Nr 7A, poz. 80.

ul. Wiejska 6, 00-902 Warszawa, tel. 22 694-95-57, fax 22 694-91-06, e-mail: Katarzyna.Konieczko@senat.gov.pl

II. ROZSTRZYGNIĘCIE TRYBUNAŁU KONSTYTUCYJNEGO

1. Treść sentencji wyroku

Trybunał orzekł, że:

a) 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 zw. z art. 31 ust. 3 Konstytucji,

b) przepisy:

– art. 20c ust. 1 ustawy o Policji,

– art. 10b ust. 1 ustawy o Straży Granicznej,

– art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej,

– art. 30 ust. 1 ustawy o ŻW,

– art. 28 ust. 1 pkt 1 ustawy o ABW,

– art. 32 ust. 1 pkt 1 ustawy o SKW,

– art. 18 ust. 1 pkt 1 ustawy o CBA,

– art. 75d ust. 1 ustawy o Służbie Celnej,

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 zw. z art. 31 ust. 3 Konstytucji,

c) przepisy:

– art. 19 ustawy o Policji,

– art. 9e ustawy o Straży Granicznej,

– art. 36c ustawy o kontroli skarbowej,

– art. 31 ustawy o ŻW,

– art. 27 ustawy o ABW,

– art. 31 ustawy o SKW,

– art. 17 ustawy o CBA,

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 zw. z art. 31 ust. 3 Konstytucji,

d) przepisy:

– art. 28 ustawy o ABW,

– art. 32 ustawy o SKW,

– art. 18 ustawy o CBA,

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

e) 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, z późn. zm.), jest niezgodny z art. 51 ust. 4 Konstytucji.

2. Stan prawny

2.1. W myśl art. 27 ust. 1 ustawy o ABW, 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. Wśród zadań ABW, które wskazane zostały w art. 5 ust. 1, znalazło się m.in. rozpoznawanie, zapobieganie i wykrywanie przestępstw (pkt 2), w tym przestępstw godzących w podstawy ekonomiczne państwa (lit. b).

2.2. Art. 20c ust. 1 ustawy o Policji przewiduje, że w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne oraz może je przetwarzać. Chodzi tu mianowicie o dane, które umożliwiają ustalenie zakończenia sieci, telekomunikacyjnego urządzenia końcowego tudzież użytkownika końcowego inicjującego połączenie albo do którego kierowane jest połączenie, a także dane niezbędne do określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, a ponadto lokalizacji telekomunikacyjnego urządzenia końcowego (art. 180c). Odnosi się to również do danych transmisyjnych oraz danych o próbach uzyskania połączenia między zakończeniami sieci, nie wyłączając nieudanych prób połączeń (art. 159 ust. 1 pkt 3 i 5 w zw. z art. 180d). W przypadku użytkowników będących osobami fizycznymi Policji mogą być udostępniane nade wszystko takie dane jak: nazwisko i imię (imiona), imiona rodziców, miejsce i data urodzenia, adres zamieszkania, numer PESEL, nazwa, seria i numer dowodu osobistego bądź też numer paszportu lub karty pobytu (art. 161 ust. 2 w zw. z art. 180d).

Podsumowując: na podstawie art. 20c ust. 1 możliwe jest pozyskanie trojakiego rodzaju danych telekomunikacyjnych: o abonencie, o ruchu (tzw. dane bilingowe) oraz o lokalizacji. Nie jest za to możliwe pozyskiwanie w tym trybie treści indywidualnych komunikatów przekazywanych za pomocą sieci telekomunikacyjnych.

Analogiczne kompetencje przyznane zostały Straży Granicznej (art. 10b ust. 1 ustawy o Straży Granicznej), wywiadowi skarbowemu (art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej), Żandarmerii Wojskowej (art. 30 ust. 1 ustawy o ŻW), Agencji Bezpieczeństwa Wewnętrznego (art. 28 ust. 1 pkt 1 ustawy o ABW), Służbie Kontrwywiadu Wojskowego (art. 32 ust. 1 pkt 1 ustawy o SKW), a także Centralnemu Biuru Antykorupcyjnemu (art. 18 ust. 1 pkt 1 ustawy o CBA) oraz Służbie Celnej (art. 75d ust. 1).

Powołane powyżej przepisy albo w ogóle nie wspominają o roli jakiegokolwiek innego organu w procesie udostępniania danych telekomunikacyjnych, albo wręcz wprost wyłączają obowiązek uzyskania zgody sądu na prowadzenie czynności z zakresu kontroli operacyjnej, wprowadzony w innych przepisach.

2.3. Przepisy art. 19 ustawy o Policji, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 31 ustawy o SKW i art. 17 ustawy o CBA dotyczą kontroli operacyjnej, która zawsze jest prowadzona niejawnie i może polegać na kontrolowaniu treści korespondencji, kontrolowaniu zawartości przesyłek oraz stosowaniu środków technicznych umożliwiających uzyskiwanie informacji i dowodów oraz ich utrwalanie, w szczególności zaś obrazu, treści rozmów telefonicznych i innych informacji przekazywanych przy pomocy sieci telekomunikacyjnych (por. np. art. 19 ust. 6 ustawy o Policji). Przepisy te determinują okoliczności, od których wystąpienia uzależnione jest stosowanie kontroli operacyjnej (a zwłaszcza odrębnie dla każdej ze służb wprowadzają katalog czynów zabronionych, w przypadku których istnieje możliwość skorzystania ze środków kontroli operacyjnej), jak również tryb, który musi zostać zachowany, aby kontrola taka mogła zostać uznana za legalną. Określają przy tym sąd właściwy do rozpoznania wniosku w przedmiocie uruchomienia kontroli operacyjnej i ewentualnie wydłużenia okresu jej stosowania.

2.4. Według art. 19 ust. 6 ustawy o Policji, materiały uzyskane w wyniku udostępnienia danych telekomunikacyjnych przez podmiot prowadzący działalność telekomunikacyjną, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi. Natomiast te materiały, które nie wnoszą

nic do sprawy prowadzonej przez organy ścigania, podlegają – jak stanowi art. 19 ust. 7 ustawy o Policji – „niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu”. Podobne postanowienia można znaleźć w art. 10b ust. 5 i 6 ustawy o Straży Granicznej, art. 36b ust. 5 ustawy o kontroli skarbowej oraz art. 30 ust. 5 i 6 ustawy o ŻW. Z kolei w art. 28 ustawy o ABW, art. 32 ustawy o SKW i art. 18 ustawy o CBA kwestia niszczenia danych niemających znaczenia dla prowadzonego postępowania została całkowicie pominięta.

2.5. Art. 75d ust. 5 ustawy o Służbie Celnej nakazuje niezwłoczne komisyjne i protokolarne zniszczenie danych telekomunikacyjnych uzyskanych przez upoważnionych funkcjonariuszy zgodnie z ust. 2, jeżeli „nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe”. Formuła ta nie rozróżnia, o jakie typy czynów chodzi, mimo że z art. 75d ust. 1 wynika, iż Służba Celna może zwracać się o udostępnienie danych, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne wyłącznie „w celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego”.

3. Wzorce konstytucyjne

Art. 2 Konstytucji wyraża zasadę demokratycznego państwa prawnego. Zasada ta jest źródłem m.in. wymogu dostatecznej określoności przepisów prawa, który to powinien być odnoszony szczególnie do tych regulacji, które zezwalają na ingerencję organów państwa w sferę wolności i praw konstytucyjnych.

Art. 31 ust. 3 Konstytucji precyzuje granice i warunki dopuszczalnych ograniczeń wolności i praw poręczonych w ustawie zasadniczej.

Art. 42 ust. 2 Konstytucji mówi o prawie do obrony we wszystkich stadiach postępowania karnego, w tym prawie do wyboru obrońcy lub korzystania z pomocy obrońcy wyznaczonego z urzędu.

Art. 47 Konstytucji gwarantuje każdemu prawo do ochrony prawnej życia prywatnego, podczas gdy art. 49 zapewnia wolność i ochronę tajemnicy komunikowania się. Jednocześnie ten ostatni przepis stanowi, że ograniczenie wolności i tajemnicy komunikowania się może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Art. 51 ust. 2 Konstytucji zakazuje władzom publicznym pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Natomiast art. 51 ust. 4 Konstytucji przewiduje, że każdy ma prawo do żądania

sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Art. 54 ust. 1 Konstytucji poręcza tzw. autonomię informacyjną jednostki, czyli wolność każdego w zakresie pozyskiwania i rozpowszechniania informacji.

4. Istota problemu konstytucyjnego

4.1. Oceniając unormowanie z art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, Trybunał przypomniał standardy wyznaczone w dotychczasowym orzecznictwie sądu konstytucyjnego. Przede wszystkim TK podkreślił, że wolności osobiste są – w świetle systematyki przepisów Konstytucji – wyjątkowo silnie eksponowane. Ustawowe ograniczenia w korzystaniu z nich powinny być zatem możliwe do ustalenia już na podstawie wykładni językowej przepisów ustawy, bez potrzeby odwoływania się do wykładni systemowej czy funkcjonalnej.

W przypadku regulacji zezwalającym służbom na prowadzenie czynności operacyjno-rozpoznawczych oznacza to, że 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. Jeżeli chodzi przy tym o przedmiotowe przesłanki zarządzenia czynności operacyjno-rozpoznawczych, to aby można było mówić o zachowaniu standardu konstytucyjnego, ustawodawca winien zdefiniować **zamknięty i możliwie wąski katalog <u>poważnych</u> przestępstw** uzasadniających tego typu ingerencję w status jednostki. Aczkolwiek nie jest konieczne wskazanie „typów przestępstw” przez odwołanie się do konkretnych przepisów ustawy karnej, a za wystarczające należy uznać w tym zakresie określenie przestępstw ich nazwą rodzajową. Tyle że to określenie musi być dostatecznie jednoznaczne.

Takiego waloru – zdaniem Trybunału – nie można przypisać sformułowaniu z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW: „przestępstwa godzące w podstawy ekonomiczne państwa”. Kodeks karny, jak również inne ustawy nie posługują się takim wyrażeniem ani w warstwie terminologicznej odnoszącej się do rodzajów poszczególnych czynów zabronionych, ani w ich elementach definicyjnych, ani tym bardziej w tytułach rozdziałów, w których zebrane są przestępstwa danego rodzaju. Zarazem niejawny charakter czynności sądowych związanych z rozpoznawaniem wniosków dotyczących kontroli operacyjnej (art. 27 ust. 11 ustawy o ABW) i brak uzasadniania postanowień o zarządzeniu tej kontroli utrudnia wykształcenie się jednolitej linii orzeczniczej co do interpretacji analizowanego wyrażenia. Nie jest więc

możliwe usunięcie niejasności określenia „przestępstwa godzące w podstawy ekonomiczne państwa" dzięki sądowej wykładni, a w rezultacie – dostarczenie jednostkom wiedzy o rzeczywistym zakresie ograniczeń prywatności i legalnej ingerencji w tajemnicę komunikowania się.

Wobec tego TK doszedł do wniosku, że na gruncie art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, faktyczne granice niejawnej ingerencji w wartości objęte ochroną na mocy art. 47 i art. 49 Konstytucji nie są wyznaczone w sposób dostatecznie określony przez ustawodawcę, a determinują je w istocie organy stosujące prawo. Takiego stanu rzeczy nie da się z kolei pogodzić z konstytucyjną zasadą określoności prawa (art. 2 Konstytucji) oraz zasadą ustawowej formy ograniczeń wolności i praw konstytucyjnych (art. 31 ust. 3 Konstytucji). Jak wskazał Trybunał, wadą zakwestionowanego uregulowania jest dodatkowo to, że umożliwia ono niejawne pozyskiwanie informacji o osobach także w celu rozpoznawania i wykrywania przestępstw, czy zapobiegania przestępstwom, które trudno byłoby kwalifikować jako poważne, a w konsekwencji uzasadniające głęboką ingerencję w sferę prywatności i tajemnicę komunikowania się.

4.2. W przypadku zaskarżonej grupy przepisów determinujących warunki legalności pozyskiwania przez służby policyjne i ochrony państwa danych telekomunikacyjnych, tzn. art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 32 ust. 1 pkt 1 ustawy o SKW, art. 18 ust. 1 pkt 1 ustawy o CBA oraz art. 75d ust. 1 ustawy o Służbie Celnej, TK podzielił zarzut, iż nie wprowadzają one wymaganego Konstytucją **mechanizmu niezależnej kontroli**. Skoro bowiem pozyskiwanie wspomnianych danych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, których owe dane dotyczą, a zarazem przy ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. „Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji."

Trybunał przypomniał w tym kontekście, że ingerencja w konstytucyjne prawo do ochrony prywatności (art. 47) i tajemnicę komunikowania się (art. 49 Konstytucji) może mieć

miejsce nie tylko w wypadku zapoznawania się organów władzy publicznej z samą treścią komunikatów przekazywanych między jednostkami, ale również w sytuacji pozyskania przez władze informacji towarzyszących temu procesowi.

Jeżeli zatem ustawodawca nie uzależnia możliwości żądania danych telekomunikacyjnych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia czy też wreszcie – wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji (por. np. art. 19 ust. 1 determinujący przesłanki stosowania kontroli operacyjnej), to niezbędnym minimum staje się ustanowienie „(…) gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych".

4.3. Badając kwestię konstytucyjności stosowania kontroli operacyjnej w szczególnej sytuacji, gdy w grę mogą wchodzić zakazy dowodowe związane z informacjami przekazanymi osobom wykonującym zawody zaufania publicznego, Trybunał zaznaczył, że bezwarunkowe wyodrębnienie jakiejkolwiek kategorii podmiotów spod dopuszczalności objęcia czynnościami operacyjno-rozpoznawczymi, w tym pozyskiwania informacji w trybie kontroli operacyjnej, nie znajduje uzasadnienia w płaszczyźnie konstytucyjnej. Konstytucja nie statuuje w tym zakresie żadnych podmiotowych wyłączeń. Niemniej nie implikuje to jeszcze dopuszczalności pozyskiwania informacji w omawianym trybie od wszystkich osób w jednakowym stopniu i na jednakowych zasadach. Ustawodawca obowiązany jest chronić poufność wiadomości przekazywanych w warunkach dyskrecji osobom wykonującym zawody zaufania publicznego znacznie intensywniej niż poufność innych informacji przekazywanych między jednostkami.

Ochrona tajemnicy zawodowej, jak i ściśle związane z nią zakazy dowodowe w postępowaniu karnym nie są wartościami autotelicznymi, lecz powinny być postrzegane raczej jako przejaw ochrony wolności i praw jednostki, zwłaszcza jej prywatności, autonomii informacyjnej, prawa do obrony, prawa do sądu, wolności sumienia i wyznania czy wolności pozyskiwania informacji, w tym wolności prasy.

W swych rozważaniach TK wiele uwagi poświęcił dwóm tajemnicom, a mianowicie: obrończej oraz dziennikarskiej. W opinii Trybunału, doniosłość tajemnicy obrończej jako gwarancji konstytucyjnego prawa do obrony (art. 42 ust. 2), 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. Warunkiem w pełni efektywnej obrony jest zaś istnienie więzi zaufania między oskarżonym a obrońcą,

która to w dużej mierze uzależniona jest od możliwości poufnego porozumiewania się. Już sama świadomość, że rozmowy z obrońcą mogą podlegać niejawnej kontroli może skutkować tym, że oskarżony zaniecha korzystania z profesjonalnej pomocy prawnej bądź nie będzie informował obrońcy o istotnych okolicznościach sprawy. Taki stan rzeczy może z kolei utrudnić skuteczne konstruowanie linii obrony, prowadząc nawet do niesłusznego skazania.

Szczególna ochrona dziennikarskich źródeł informacji jest natomiast konsekwencją uznania mediów za strażnika demokracji i pluralizmu. Brak szczególnej ochrony źródeł informacyjnych prowadzić może do utraty zaufania informatorów do dziennikarzy, a także do obawy przed nawiązywaniem i utrzymywaniem tego rodzaju współpracy. Może to okazać się poważną przeszkodą w prawidłowym funkcjonowaniu prasy oraz innych środków masowego przekazu.

Jak zostało jednak podniesione powyżej, zupełne wyłączenie określonej grupy podmiotów, w tym obrońców i dziennikarzy, spod kontroli operacyjnej nie znajduje uzasadnienia w świetle postanowień konstytucyjnych. Co więcej – ogólne wyłączenie spod kontroli operacyjnej podmiotów obowiązanych do zachowania tajemnicy zawodowej, a nawet wyłączenie informacji uznawanych za stanowiące tajemnicę zawodową jako bezwzględnie niedopuszczalnych do pozyskania w tym trybie, prowadziłoby do istotnych utrudnień w gromadzeniu materiału dowodowego niektórych rodzajów przestępstw, popełnianych np. z wykorzystaniem nowych technologii. Należy mieć ponadto na uwadze, że nie da się zazwyczaj abstrakcyjnie określić relacji między dobrem, którego ochronie mają służyć zakazy dowodowe (i tajemnica zawodowa), a dobrem wymiaru sprawiedliwości, bezpieczeństwem państwa i porządkiem publicznym (art. 31 ust. 3 Konstytucji) w kategoriach „wyższe – niższe” czy „ważniejsze – mniej ważne”. Wreszcie, nie wolno abstrahować od specyfiki kontroli operacyjnej, która polega nie tyle na utrwalaniu indywidualnych komunikatów przekazywanych między oznaczonymi imiennie osobami, ile na trwającym pewien czas monitoringu źródła informacji (np. podsłuch, kontrolowanie korespondencji pisemnej i elektronicznej) wobec podmiotu objętego stosownym zarządzeniem sądowym. Dopiero po zakończeniu kontroli oraz analizie zgromadzonych danych jest więc możliwe zweryfikowanie, jakich treści dotyczą zebrane informacje, a następnie rozstrzygnięcie, które z nich muszą bezwzględnie podlegać ochronie bez możliwości dalszego ich wykorzystania i muszą tym samym zostać unicestwione.

Wobec tego punkt ciężkości przesuwa się w tym wypadku na zapewnienie odpowiednich gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne

informacji, które – z uwagi na ich treść oraz okoliczności przekazania – winny podlegać ochronie prawnej. Innymi słowy, mankamentem art. 19 ustawy o Policji jest to, że przepis ten nie gwarantuje, iż w sytuacji uzasadnionego podejrzenia, że zgromadzone materiały zawierają informacje objęte tajemnicę zawodową i z tego powodu wymagają szczególnej ochrony, nastąpi dodatkowa ich weryfikacja przez właściwy sąd, który ewentualne będzie mógł orzec o zwolnieniu z tajemnicy zawodowej, zanim materiały te zostaną przekazane funkcjonariuszom albo prokuratorowi.

W ocenie TK, taki sam zarzut jest adekwatny w odniesieniu do pozostałych przepisów stanowiących podstawę stosowania kontroli operacyjnej, tj. art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 31 ustawy o SKW oraz art. 17 ustawy o CBA.

4.4. Problemem konstytucyjnym zdiagnozowanym przez Trybunał na gruncie art. 28 ustawy o ABW, art. 32 ustawy o SKW i art. 18 ustawy o CBA było z kolei pominięcie przez ustawodawcę koniecznej – z punktu widzenia art. 54 ust. 2 Konstytucji – regulacji dotyczącej weryfikacji oraz niszczenia danych telekomunikacyjnych, które okazały się nieprzydatne dla postępowania, w toku którego wystąpiono o ich przekazanie. Powołany wzorzec konstytucyjny przesądza, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym, przy czym oceny owej „niezbędności" należy dokonywać przez pryzmat zasady proporcjonalności wynikającej z art. 31 ust. 3 Konstytucji.

W orzecznictwie trybunalskim wyrażony został pogląd, że w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności z uwagi na bezpieczeństwo państwa i porządek publiczny.

W związku z powyższym 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 (m.in. w trybie określonym w art. 28 ust. 1 ustawy o ABW, art. 18 ust. 1 ustawy o CBA i art. 32 ust. 1 ustawy o SKW), ale również każde kolejne operacje na tych danych, w tym przechowywanie czy wtórne wykorzystywanie w toku innych postępowań."

4.5. Porównanie treści art. 75d ust. 5 ustawy o Służbie Celnej z postanowieniem zawartym w art. art. 75d ust. 1 tej ustawy uzasadnia konkluzję, że o ile Służba Cywilna może pozyskiwać dane telekomunikacyjne w wąsko zakreślonym celu w postaci zapobiegania lub wykrywania przestępstw skarbowych przeciwko organizacji gier hazardowych (czyli określonych w rozdziale 9 Kodeksu karnego skarbowego), 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, i to o wszelkie wykroczenia skarbowe lub przestępstwa skarbowe. Krótko mówiąc: inny jest cel pozyskiwania danych telekomunikacyjnych przez Służbę Celną, a inny ich przechowywania.

Według TK, płynący z art. 75d ust. 5 ustawy o Służbie Cywilnej nakaz został ujęty w niewłaściwy sposób i w związku z tym nie czyni zadość wymogom płynącym z art. 51 ust. 4 Konstytucji. Jedynie w przypadku danych telekomunikacyjnych, które – choć nie dostarczyły dowodu popełnienia przestępstwa skarbowego lub nie są przydatne w dalszym postępowaniu dotyczącym przestępstwa skarbowego, co do którego możliwe było ich pozyskanie – będą przydatne do zapobiegania bądź też wykrywania innych czynów zabronionych (tak przestępstw, jak i wykroczeń), o których mowa w rozdziale 9 ustawy karno-skarbowej, możliwe jest przyjęcie, że są to dane zebrane „zgodnie z ustawą", a tym samym można też dopuścić ich dalsze wykorzystanie przez Służbę Celną. „Można też uznać je za konieczne w demokratycznym państwie, ponieważ niewątpliwie legitymowanym konstytucyjnie celem jest wykrywanie wypadków popełniania czynów zabronionych oraz zapobieganie im."

Dlatego Trybunał orzekł, że art. 75d ust. 5 ustawy o Służbie Celnej narusza standard konstytucyjny, jednak wyłącznie w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych przeciwko organizacji gier hazardowych.

III. TERMIN WYKONANIA ORZECZENIA

Trybunał odroczył o 18 miesięcy utratę mocy obowiązującej zaskarżonych przepisów, z wyjątkiem art. 75d ust. 5 ustawy o Służbie Celnej. Odnośnie do normy wywodzonej z tego ostatniego przepisu wyrok wywołał zatem skutki prawne z dniem ogłoszenia, czyli z dniem 6 sierpnia 2014 r.

IV. WSKAZÓWKI DLA USTAWODAWCY WYRAŻONE PRZEZ TRYBUNAŁ KONSTYTUCYJNY W UZASADNIENIU (POSTULATY DE LEGE FERENDA)

W swej wypowiedzi Trybunał sformułował szereg wskazówek i postulatów pod adresem ustawodawcy.

Na uwagę zasługują m.in. wywody dotyczące:

– wymaganej Konstytucją precyzji przepisów określających przesłanki materialne stosowania kontroli operacyjnej (pkt 5.1.3.1. uzasadnienia), w tym ciążącego na ustawodawcy obowiązku uwzględnienia – w przypadku gdy odwołuje się do przestępstw „ściganych na mocy umów i porozumień międzynarodowych" – istniejącego w ustawie zasadniczej rozróżnienia typów umów międzynarodowych i wynikających stąd konsekwencji (por. pkt 1 sentencji wyroku oraz argumentację z pkt 8.2.3. uzasadnienia),

– konieczności ustalenia „zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach" (pkt 5.1.3.2. uzasadnienia),

– konieczności doprecyzowania, iż dane telekomunikacyjne udostępniane służbom policyjnym i ochrony państwa celem umożliwienia im realizacji zadań polegających na rozpoznawaniu, zapobieganiu i wykrywaniu przestępstw, mogą być następnie wykorzystywane jako dowody w postępowaniu karnym (pkt 6.2.4. uzasadnienia),

– zbyt długiego okresu retencji danych (12 miesięcy) przewidzianego w art. 180a ust. 1 pkt 1 ustawy – Prawo telekomunikacyjne[1)], a także braku jednolitych standardów obowiązujących podmioty, od których wymaga się zatrzymywania danych telekomunikacyjnych, co z kolei

---

[1)] W tym zakresie źródłem cennych wskazówek jest również wyrok Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 r. (sygn. C-293/12) stwierdzający nieważność dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności (…), ze względu na naruszenie praw zagwarantowanych w art. 7 i art. 8 Karty praw podstawowych UE (odpowiednio: prawa do ochrony życia prywatnego i prawa do ochrony danych osobowych).

przekłada się na niejednoznaczność upublicznianych statystyk obrazujących skalę sięgania po tego typu dane przez służby policyjne i ochrony państwa (pkt 6.2.6. uzasadnienia),
– braku ustawowego określenia elementów, które powinny znaleźć się w postanowieniu o zarządzeniu kontroli operacyjnej, co skutkuje niejednolitą praktyką orzeczniczą w zakresie wskazywania rodzaju środka technicznego, który ma być używany w danej sprawie (pkt 9.2.5. uzasadnienia).

Ponadto przy wykonywaniu zaleceń związanych z poddaniem pozyskiwania danych telekomunikacyjnych kontroli niezależnego organu warto pamiętać o opinii wyrażonej w pkt 10.4.4. uzasadnienia wyroku. Otóż, TK zastrzegł tam, że nie przesądza, jak dokładnie ma wyglądać procedura dostępu do takich danych, tzn. czy zasadą ma być kontrola następcza (z wyjątkami na rzecz kontroli uprzedniej np. w przypadku danych osób wykonujących zawody zaufania publicznego lub sytuacji gdy „nie ma konieczności pilnego działania służb") oraz czy sprawowanie kontroli powinno zostać powierzone sądom czy też innemu organowi, pod warunkiem wszakże, iż będzie się on cieszył niezależnością od rządu, a jednocześnie nie będzie pozostawał z funkcjonariuszami pozyskującymi dane ani w bezpośredniej, ani nawet pośredniej relacji zwierzchności.

Trzeba poza tym mieć na względzie wzmiankę, którą Trybunał uczynił motywując powody uznania art. 36b ust. 5 ustawy o kontroli skarbowej za zgodny z Konstytucją. Przepis ten stanowi, że minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych telekomunikacyjnych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, o którym mowa w ust. 2, za nieuzasadnione. Zdaniem TK, przytoczonej regulacji nie można zasadnie zarzucić zbyt wąskiego określenia przesłanek zniszczenia danych telekomunikacyjnych zgromadzonych przez wywiad skarbowy (czyli w istocie pominięcia prawodawczego). „Problem konstytucyjny w tej sprawie polega bowiem na zbyt szerokim zakresie normowania art. 36d ust. 3 ustawy, który umożliwia przechowywanie i wykorzystywanie uzyskanych wcześniej danych telekomunikacyjnych w celach niemających konstytucyjnego uzasadnienia. Innymi słowy, problemem nie jest więc to, czego ustawodawca nie unormował, chociaż postępując w zgodzie z Konstytucją powinien był unormować, lecz to, co uregulował w innym przepisie ustawy, który nie został zaskarżony przez wnioskodawcę."

V. INFORMACJA O WYKONANIU ORZECZENIA PRZEZ INNY PODMIOT

Z informacji przesłanej na ręce Przewodniczącego senackiej Komisji Praw Człowieka, Praworządności i Petycji przez Prezesa Rządowego Centrum Legislacji (pismo z dnia 1 kwietnia 2015 r.) wynika, że rząd podjął prace mające na celu wykonanie wyroku wydanego w sprawie K 23/11. W ramach Kolegium do Spraw Służb Specjalnych powołany został specjalny zespół, złożony m.in. z przedstawicieli służb uprawnionych do stosowania kontroli operacyjnej lub pozyskiwania danych telekomunikacyjnych, którego zadaniem jest realizacja wytycznych Trybunału Konstytucyjnego. Po opracowaniu projekt stosownej ustawy zostanie przekazany do uzgodnień międzyresortowych oraz konsultacji.

Niezależnie od tego wypada wspomnieć, że kierując się wnioskami *de lege ferenda* zawartymi w Informacji o wynikach kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne", opublikowanej przez Najwyższą Izbę Kontroli w czerwcu 2013 r., Biuro Legislacyjne Kancelarii Senatu przygotowało projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych. Projekt ten zakłada uzależnienie możliwości pozyskiwania danych o abonencie, bilingów oraz informacji o lokalizacji przez służby policyjne i ochrony państwa od zgody sądu okręgowego, a ponadto przewiduje wprowadzenie instytucji pełnomocników do spraw kontroli przetwarzania przez owe służby danych osobowych. Komisja odbyła w tej sprawie posiedzenie w dniu 4 marca 2014 r. Projekt nie został formalnie zgłoszony do dalszych prac legislacyjnych.

Dodatkowo można też nadmienić, że w lipcu 2012 r. Senat wniósł do Sejmu projekt ustawy o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk sejmowy nr 633). Celem tej inicjatywy było wypełnienie postulatów sformułowanych w postanowieniu sygnalizacyjnym Trybunału z dnia 15 listopada 2010 r. (S 4/10), przez: po pierwsze – doprecyzowanie zadania polegającego na rozpoznawaniu, zapobieganiu i wykrywaniu przestępstw, powierzonego Agencji Bezpieczeństwa Wewnętrznego na mocy art. 5 ust. 1 pkt 2 ustawy o ABW, a po drugie – wskazanie katalogu przestępstw, w przypadku których może dojść do zarządzenia kontroli operacyjnej. W tym zakresie przedmiotowy projekt wychodzi zatem również naprzeciw rozstrzygnięciu z dnia 30 lipca 2014 r. (pkt 2 sentencji wyroku). W dniu 27 lipca 2012 r. senacki projekt ustawy o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu został skierowany do Komisji Spraw Wewnętrznych,

z zaleceniem zasięgnięcia opinii Komisji do Spraw Służb Specjalnych. Prace legislacyjne nie zostały zakończone.

VI. WYKONANIE ORZECZENIA

Nie ulega wątpliwości, że analizowany wyrok TK wymaga pilnej reakcji ustawodawcy. Skala zmian, które trzeba wprowadzić (i to nie tylko tych, które będą stanowiły odpowiedź na pkt 2, 5, 6 i 8, czy uwzględnią zakresową formułę z pkt 9 sentencji, lecz będą także realizować oczekiwania sądu konstytucyjnego przedstawione w części motywacyjnej orzeczenia) jest tak duża, że konieczne jest zaangażowanie w proces ich przygotowania wszystkich służb, które prowadzą czynności operacyjno-rozpoznawcze w formie kontroli operacyjnej oraz korzystają z danych telekomunikacyjnych.

W związku z tym pozytywnie należy ocenić prace zainicjowane w ramach Kolegium do Spraw Służb Specjalnych. Można przy tym postawić tezę, że opracowanie projektu ustawy wykonującej wyrok Trybunału na ścieżce rządowej, przy zagwarantowaniu możliwie szerokich konsultacji, przyczyni się do właściwego wyważenia tych wszystkich wartości konstytucyjnych, które wchodzą w rachubę w przypadku dopuszczenia stosowania kontroli operacyjnej, a więc w szczególności prawa do prywatności i autonomii informacyjnej jednostki z jednej strony, z drugiej natomiast – obowiązku państwa sprowadzającego się do stworzenia warunków, w których obywatele mogą swobodnie korzystać z zagwarantowanych im wolności i praw m.in. dzięki poczuciu bezpieczeństwa oraz braku zagrożeń zewnętrznych i wewnętrznych, w tym zagrożeń związanych z terroryzmem i przestępczością.

Opracowała: Katarzyna Konieczko

Akceptował: Marek Jarentowski