Warszawa, dnia 26 stycznia 2011 r.

TRYBUNAŁ KONSTYTUCYJNY
Al. J. Ch. Szucha 12a
00-918 Warszawa

Wnioskodawca:
Grupa Posłów
na Sejm RP VI kadencji
według załączonej listy

Adres do korespondencji:
Sejm RP
ul. Wiejska 4/6/8
00 – 902 Warszawa
Klub Parlamentarny SLD

WNIOSEK

o stwierdzenie niezgodności przepisów ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej, ustawy o ABW oraz AW, ustawy o CBA, ustawy o SWW oraz SKW z Konstytucją RP oraz art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz o stwierdzenie niezgodności przepisów ustawy Prawo telekomunikacyjne w zw. z przepisami ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej, ustawy o ABW oraz AW, ustawy o CBA, ustawy o SKW oraz SWW z Konstytucją Rzeczypospolitej Polskiej.

Wniosek na podstawie art. 191 ust. 1 Konstytucji RP

Akty prawne będące przedmiotem badania konstytucyjności:

1. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 1990 r. Nr 30 poz. 179 ze zm.)(dalej: „ustawa o Policji”)
2. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 1990 r. Nr 78 poz. 462 ze zm.) (dalej: „ustawa o Straży Granicznej”)
3. Ustawa z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 1991 r. Nr 100 poz. 442 ze

zm.)(dalej: „ustawa o kontroli skarbowej”)

4. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2001 r. Nr 123 poz. 1353 ze zm.)(dalej: „ustawa o Żandarmerii Wojskowej”)

5. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2002 r. Nr 74 poz. 676 ze zm.)(dalej: „ustawa o ABW oraz AW”)

6. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 ze zm.)(dalej: „Prawo telekomunikacyjne”)

7. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz .U. z 2006 Nr 104 poz. 708 ze zm.)(dalej: „ustawa o CBA”)

8. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2006 r. Nr 104 poz. 709 ze zm.)(dalej: „ustawa o SKW oraz SWW”)

Na podstawie art. 191 ust. 1 w zw. z art. 188 pkt 1 i 2 Konstytucji RP niżej podpisani, którzy wnosimy o stwierdzenie, iż:

I

Art. 19 ust. 7 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej, art. 27 ust. 6 pkt 3 ustawy o ABW oraz AW, art. 17 ust. 5 pkt 3 ustawy o CBA, art. 31 ust. 4 pkt 3 ustawy o SWW oraz SKW **są niezgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz art. 8 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)(dalej: „Konwencja”).**

II

Art. 180 a ust. 1 i art. 180 c Prawa telekomunikacyjnego w zw. z art. 20 c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej**,** art. 28 ustawy o ABW oraz AW, art. 18 ustawy o CBA, art. 32 ustawy o SKW oraz SWW, są niezgodne **z art. 2, art. 47, art. 49, art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji RP.**

***

Do reprezentowania w postępowaniu przed Trybunałem Konstytucyjnym wnioskodawcy

upoważniają posłów Janusza Krasonia, Ryszarda Kalisza oraz adwokata Jacka Kondrackiego z których każdy ma prawo do samodzielnego reprezentowania wnioskodawców wraz z prawem do udzielania dalszych pełnomocnictw oraz z prawem do modyfikowania treści wniosku.

Uzasadnienie

I

Zaskarżona norma, stwarza sytuację, w której zakres środków możliwych do stosowania w ramach kontroli operacyjnej pozostaje praktycznie nieograniczony. Nieprecyzyjnie sformułowane zapisy na temat pozyskiwania danych telekomunikacyjnych dają szerokie ple do nadużyć wymierzonych w chronioną prawnie tajemnicę dziennikarską, adwokacką czy radcowską. Z uwagi na otwarty katalog środków techniki operacyjnej, rodzi się wątpliwość czy pomimo niewymienienia w zaskarżonych przepisach szeregu technik operacyjnych takich jak na przykład nadajnik GPS, czy tzw. koń trojański[1], ich stosowanie jest jeszcze dozwolone czy też jest działaniem *contra legem*. W ocenie wnioskodawców zakwestionowana norma jest niezgodna z zasadą przyzwoitej legislacji (art. 2 Konstytucji RP) i prowadzi do nieproporcjonalnego ograniczenia wolności słowa, prawa do prywatności (art. 47 Konstytucji RP), swobody komunikowania się (art. 49 Konstytucji RP), chronionymi także na gruncie art. 8 Konwencji.

1. Kontrola operacyjna – definicja i zakres stosowania

Kontrola operacyjna może być zarządzona przy wykonywaniu czynności operacyjno - rozpoznawczych, podejmowanych przez Policję, służby specjalne w rozumieniu art. 11 ustawy o ABW oraz AW[2] oraz inne podmioty wykonujące zadania ochrony bezpieczeństwa państwa (Żandarmerię Wojskową, wywiad skarbowy, Straż Graniczną) w celu zapobiegania, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw (lub przestępstw skarbowych). Przestępstwa te zostały określone w specjalnych katalogach.

1 Jest to określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje (programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.). Źródło: wikipedia.
2 Są to: ABW, AW, CBA, SKW oraz SWW.

Warunkiem zarządzenia kontroli operacyjnej jest wykazanie, że inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne. Natomiast wymogiem proceduralnym jej zarządzenia jest zgoda właściwego sądu okręgowego (będzie to w zależności od podmiotu wnioskującego właściwy sąd okręgowy albo wojskowy sąd okręgowy) oraz zgoda właściwego prokuratora (Prokuratora Generalnego, właściwego prokuratora okręgowego, właściwego wojskowego prokuratora okręgowego). Istnieje także możliwość zarządzenia kontroli operacyjnej w *„przypadkach niecierpiących zwłoki”*. Zarządza ją wtedy właściwy organ (Komendant Główny Policji, komendant wojewódzki Policji, Szef CBA, Szef ABW, Szef SKW, Komendant Główny Żandarmerii Wojskowej, komendant oddziału Żandarmerii Wojskowej, Komendant Główny Straży Granicznej, komendant oddziału Straży Granicznej, Generalny Inspektor Kontroli Skarbowej) po uzyskaniu pisemnej zgody Prokuratora Generalnego (ewentualnie właściwego prokuratora okręgowego lub wojskowego prokuratora okręgowego), jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa. Wraz z zarządzeniem kontroli operacyjnej, podmiot zarządzający musi zwrócić się jednocześnie do właściwego miejscowo sądu okręgowego (wojskowego sądu okręgowego) z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania.

Zgodnie z art. 19 ust. 7 ustawy o Policji kontrola operacyjna prowadzona jest niejawnie i może polegać na: 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, oraz **3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych**. Analogiczne brzmienie mają przepisy: art. 27 ust. 6 ustawy o ABW oraz AW, art. 18 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW oraz SWW.
Natomiast art. 31 ust. 7 ustawy o Żandarmerii wojskowej, art. 36c ust. 4 ustawy o kontroli skarbowej, art. 9e ust. 7 ustawy o Straży Granicznej dodają do zakresu informacji gromadzonych przy użyciu „środków technicznych” także obraz.

Wskazane przepisy uprawniają Policję, służby specjalne oraz podmioty wykonujące zadania ochrony bezpieczeństwa państwa do określonego zachowania (sięgania po określone środki) w ramach stosowania kontroli operacyjnej. W ocenie wnioskodawców nie budzą wątpliwości

regulacje przewidujące możliwość dokonywania w ramach kontroli operacyjnej kontroli treści korespondencji oraz zawartości przesyłek, bowiem pkt. 1-2 tych przepisów wprost wskazują, jakie konkretnie czynności godzące w określone dobra prawne (wolności i prawa konstytucyjne) mogą być podejmowane w ramach kontroli operacyjnej.

2. Zaskarżone przepisy a standardy konstytucyjne i konwencyjne

Zdaniem wnioskodawców kompetencja Policji, służb specjalnych oraz innych podmiotów wykonujących zadania ochrony bezpieczeństwa państwa określająca jakie środki mogą być stosowane w ramach kontroli operacyjnej, została skonstruowana w sposób niezgodny ze standardami wypracowanymi na gruncie art. 2, art. 47, art. 49 w zw. z art. 31 ust. 3 Konstytucji RP oraz art. 8 Konwencji.

W pkt. 3 zaskarżonych przepisów ustawodawca posłużył się bowiem nieostrym pojęciem *„środki techniczne umożliwiające uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie”*. Pojęcie *„środki techniczne umożliwiające uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie”* (inne niż wskazane w pkt. 1 – 2 ww. przepisów) ustawodawca próbował doprecyzować używając określenia *„w szczególności”,* wskazując przykładowo, że z całą pewnością wśród informacji mogą znajdować się *„treści rozmów telefonicznych” i „obraz”*, ale także nieokreślone *„inne informacje przekazywane za pomocą sieci telekomunikacyjnych”*. Przyjęty przez ustawodawcę sposób zdefiniowania stanowi przykład błędu logicznego *ignotum per ignotum*. Konstruując drugą część pkt. 3 zaskarżonych przepisów ustawodawca zamiast jasno zdefiniować *„środki techniczne umożliwiające uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie”*, doprowadził do jeszcze dalej posuniętej nieostrości przepisu kompetencyjnego. Kategoria ta pozostaje zatem otwarta, podobnie jak zakres informacji mogących być potencjalnie gromadzonymi w wyniku stosowania kontroli operacyjnej.

W ocenie wnioskodawców, przyjęta przez ustawodawcę technika legislacyjna jest nie do pogodzenia ze standardami konstytucyjnymi. Wnioskodawcy pragną szczególnie podkreślić, iż analizowane przepisy dotyczą stosowania przez organy państwowe środków, które głęboko ingerują w prawa i wolności obywatelskie, a w szczególności w prawo do prywatności (art. 47 Konstytucji RP), która wyraża się m.in. w swobodzie komunikowania się (art. 49 Konstytucji RP), czy też znajduje swoją proceduralną ochronę w art. 51 Konstytucji RP dotyczącym autonomii informacyjnej jednostki, w ramach której organom państwowym zabrania się zbierania informacji innych niż niezbędne w demokratycznym państwie prawnym.

Poprzez użycie otwartego katalogu środków technicznych, czego wyrazem jest posłużenie się określeniem „w szczególności" rodzić się może trudność z określeniem, jakim jeszcze wolnościom prócz ww. może zagrażać stosowanie kontroli operacyjnej. W tym zakresie powstać może na przykład wątpliwość, czy w ramach kontroli operacyjnej możliwe jest stosowanie podsłuchu obiektowego, mikrofonów kierunkowych, oprogramowania szpiegowskiego czy też nadajników GPS[3], których używanie może prowadzić także do naruszenia miru domowego, chronionego na podstawie art. 50 Konstytucji RP i rozumianego jako zakaz wszelkiego nieuprawnionego wkraczania i przebywania w cudzym mieszkaniu/siedzibie.

Poprzez oględne wskazanie, iż w ramach kontroli operacyjnej można w szczególności stosować środki techniczne umożliwiające uzyskiwanie treści rozmów telefonicznych, obrazu oraz niedookreślonych „innych informacji przekazywanych za pomocą sieci telekomunikacyjnych" ustawodawca doprowadził do sytuacji, w której wkroczenie w ww. wolności i prawa konstytucyjne następuje na podstawie nieprecyzyjnej podstawy ustawowej. W tej sytuacji funkcjonariusz sam, autonomicznie podejmuje decyzję o wkroczeniu, bowiem przepis nie wskazuje wyraźnie konkretnych technik działania, poza stosowaniem *„środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie treści rozmów telefonicznych, obrazu i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych"*. Jedynym ograniczeniem w tym zakresie, zamiast przepisów ustawowych, stają się możliwości finansowe, organizacyjne i dostęp ww. formacji do najnowocześniejszych zdobyczy technologicznych.

2.1. Standardy w zakresie konstruowania przepisów regulujących ingerencję w prawa i wolności konstytucyjne

Trybunał Konstytucyjny wielokrotnie już wypowiadał się na temat standardów jakim powinny odpowiadać przepisy regulujące ograniczenia praw i wolności konstytucyjnych. Ustawodawca, konstruując przepis, który ingeruje głęboko w sferę prywatności jednostki, musi uwzględnić nie tylko zasady przyzwoitej legislacji (w tym zasadę dookreśloności i konkretności), ale także rozważyć proporcjonalność zastosowanego środka. Nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, ułatwiały ich osiągnięcie albo były wygodne dla władzy, która ma je wykorzystać do osiągnięcia tych celów. Minimalnym wymogiem konstytucyjnym jest to, aby

3 Podobne wątpliwości w piśmie do Prezesa Rady Ministrów z dnia 13 października 2010 r. w związku z publikacją "Dziennikarze na celowniku służb specjalnych". Pismo dostępne jest na stronie: http://www.hfhrpol.waw.pl/precedens/images/stories/file/pismo_2538_2010_DP.pdf

przeszły one test „konieczności w demokratycznym państwie prawnym”. Nie wystarczy, zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę – w odniesieniu do użytego środka, ale o zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają ograniczeniu4. Poza tym z zgodnie z poglądem pełnego składu TK wyrażonym w wyroku z 23 marca 2006 r.5 „*zwroty niedookreślone mogą być używane przez ustawodawcę, jeżeli ich desygnaty można ustalić,* a samo użycie zwrotu nieostrego *„wymaga istnienia szczególnych gwarancji proceduralnych, zapewniających przejrzystość i ocenność praktyki wypełniania nieostrego zwrotu konkretną treścią przez organ decydujący o jego wypełnieniu”.*

Przepis ustawy musi być sformułowany w sposób dostatecznie precyzyjny, bowiem ustawodawca nie może poprzez niejasne formułowanie tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki. Dla oceny zgodności zakwestionowanego przepisu z art. 31 ust 3 i art. 2 Konstytucji istotne są trzy założenia: *„Po pierwsze – każdy przepis ograniczający konstytucyjne wolności i prawa winien być sformułowany w sposób pozwalający jednoznacznie ustalić, kto i w jakiej sytuacji podlega ograniczeniom. Po drugie – przepis ten powinien być na tyle precyzyjny, aby zapewniona była jego jednolita wykładnia i stosowanie. Po trzecie – przepis taki winien być ujęty tak, aby zakres jego zastosowania obejmował tylko te sytuacje, w których działający racjonalnie ustawodawca istotnie zamierzał wprowadzić regulację ograniczającą korzystanie z konstytucyjnych wolności i praw”*[6]. Natomiast *„przekroczenie pewnego stopnia niejasności przepisów prawnych stanowić może samoistną przesłankę stwierdzenia ich niezgodności z art. 31 ust. 3 zdanie 1 i z art. 2 Konstytucji”*[7].

2.2. Orzecznictwo Europejskiego Trybunału Praw Człowieka – standardy na gruncie art. 8 Konwencji

Zaskarżone przepisy dotyczące zakresu środków technicznych możliwych do stosowania w ramach kontroli operacyjnej należy przeanalizować także pod kątem standardów wypracowanych w orzecznictwie Europejski Trybunał Praw Człowieka (dalej: „ETPCz”) dotyczącym art. 8 Konwencji

4 Por. wyrok z 3 października 2000 r., sygn. K 33/99, OTK ZU 2000, Nr 6, poz. 188.
5 Wyrok z 23 marca 2006 r., sygn. K 4/06, OTK ZU nr 3/A/2006, poz. 32.
6 Wyrok z 30 października 2001 r. sygn. K 33/00, Z.U. 2001 / 7 / 217.
7 Wyrok z 22 maja 2002 r. sygn. K 6/02, Z.U. 2002 / 3A / 33.

(ochrona korespondencji oraz życia prywatnego). Kluczowe znaczenie ma tu analiza z punktu widzenia ograniczeń jakie władze publiczne mogą nakładać na obywateli na podstawie art. 8 ust. 2 Konwencji, w tym zwłaszcza w celu zwalczania przestępczości oraz ochrony bezpieczeństwa państwowego. Powaga ingerencji dokonywanej przy użyciu technik operacyjnych w prawo do prywatności została szczególnie wyeksponowana w wyroku *Associaton for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii*[8], w którym ETPCz stwierdził naruszenie art. 8 i 13 Konwencji oraz podkreślił, iż środki tajnej inwigilacji *(*ang. *secret measures of surveillance)* stosowane przez organy państwowe stanowić mogą nieuzasadnioną w demokratycznym społeczeństwie ingerencję w prawo do prywatności. W wyroku *Klass i Inni przeciwko Niemcom*[9], ETPCz ocenił, że zakres ingerencji, funkcjonujących w demokratycznym państwie służb specjalnych w obywatelskie prawo do prywatności, musi być ściśle ograniczony do zapewnienia bezpieczeństwa państwa, co oznacza, iż to właśnie ochrona ww. dobra stanowi zasadniczy determinant podejmowania działań operacyjnych. Dlatego też niezmiernie ważne jest, aby jednostkom w ramach systemów prawnych tworzyć mechanizm ochrony ich wolności i praw, eliminujący arbitralność po stronie władz krajowych.

ETPCz dokonuje oceny ingerencji w sferę prywatności poprzez ustalenie legalności w sensie formalnym (fakt istnienia przepisów prawnych odpowiedniej rangi), a następnie legalności substancjalnej (jakość obowiązujących przepisów) eksponującej przejrzystość i przewidywalność przepisów prawnych, w oparciu o które dokonano ingerencji.

W wyroku *Malone przeciwko Wielkiej Brytanii*[10] ETPCz podkreślił, iż w kolizji z art. 8 Konwencji pozostaje sytuacja, gdy część uprawnień służb specjalnych ma podstawę w przepisach, a część pozostawiona jest do swobodnego uznania władzy. Podobnie w wyroku *Heglas przeciwko Czechom*, ETPCz uznał, iż instalowanie przez policję urządzenia podsłuchowego na ciele rozmówcy nie było uregulowane przez ustawę, a zatem nie odpowiadała kryteriom ustalonym w orzecznictwie strasburskim, a służby mimo to stosowały ten środek, gdyż takie techniki wynikały z praktyki organów ścigania. Taka podstawa stosowania środków tajnej inwigilacji nie może być zdaniem ETPCz uznana za odpowiednią podstawę prawną określającą z dostateczną precyzją warunki dopuszczalności stosowania techniki operacyjnej, jej zakresu, kontroli oraz wykorzystania informacji zdobytych w ten sposób[11]. Z kolei w wyroku *Bykov przeciwko Rosji*[12] ETPCz uznał, iż

8 Wyrok z 28 czerwca 2007 r. w sprawie *Associaton for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii*, skarga nr 62540/00.
9 Wyrok z 6 września 1978 r. w sprawie *Klass i Inni przeciwko Niemcom*, skarga nr 5029/71.
10 Wyrok z 2 sierpnia 1984 r. w sprawie *Malone przeciwko Wielkiej Brytanii*, skarga nr 8691/79
11 Wyrok z 1 marca 2007 r. w sprawie *Heglas przeciwko Czechom*, skarga nr 5935/02.
12 Wyrok z 10 marca 2009 r. w sprawie *Bykov przeciwko Rosji*, skarga nr 4378/02. J. McBride, The case law of the

użycie przez służby urządzenia nagrywającego w postaci dyktafonu było jedynie podobne pod względem ingerencji do podsłuchu lub korespondencji przekazywanej drogą elektroniczną. Z racji tego, iż obowiązujące prawo przewidywało dokonywanie kontroli za pośrednictwem urządzeń komunikacji elektronicznej, nie zaś urządzeń mechanicznych, doszło do arbitralnego naruszenia art. 8 Konwencji. Podobnie w decyzji *Weber i Saravia przeciwko Niemcom*[13] ETPCz stwierdził, iż prawo krajowe musi być sformułowane wystarczająco jasno, aby dać obywatelom odpowiednie wskazówki co do okoliczności i warunków, w których władze publiczne mogą sięgnąć po te środki i chronić ich przed arbitralną ingerencją. ETPCz nakreślił też wymogi minimalne, które powinny być ujęte w ustawie regulującej działalność operacyjną. Są to: natura przestępstw w ramach których mogą być prowadzone (zasadniczo najcięższe), definicja kategorii podmiotów, przeciwko którym można te środki stosować, ograniczenie długości stosowania środków, stworzenie procedury badania, wykorzystywania i przechowywania, stworzenie środków ostrożności przy przekazywaniu tych informacji, okoliczności w jakich zapisy mogą lub muszą być usunięte lub zniszczone. Ważne jest także stworzenie w przepisach prawa zabezpieczeń przed przekazywaniem prokuratorowi lub sądowi materiałów zebranych w sposób fragmentaryczny[14].

Legalność substancjalna była natomiast oceniana m.in. w orzeczeniu *Liberty i Inni przeciwko Wielkiej Brytanii*, w którym ETPCz stwierdził, iż wymóg „zgodności z prawem" (z ustawą) ingerencji w prawo do poszanowania życia prywatnego i rodzinnego (art. 8 ust. 2 EKPC) odnosi się także do jakości prawa i oznacza, że regulacja krajowa powinna respektować zasadę rządów prawa[15]. Natomiast w wyroku *Kruslin przeciwko Francji*, ETPCz wskazał, iż powaga ingerencji w sferę prywatną z jaką wiążą się kontrole rozmów telefonicznych powoduje, iż prawo na podstawie, którego taka ingerencja jest dokonywana musi być szczególnie precyzyjne, a to w szczególności z tego powodu, iż wykorzystywana przy tym technologia jest coraz bardziej zaawansowana. Warto w tym miejscu wskazać jeszcze na wyrok *Iordachi i Inni przeciwko Mołdawii*[16], w którym ETPCz dopatrzył się naruszenia przez władze mołdawskie art. 8 Konwencji m.in. poprzez dopuszczenie nazbyt szerokiego zakresu przedmiotowego stosowania kontroli operacyjnej (niedoskonałość przepisów miała m.in. polegać na tym, iż środki te mogły być wykorzystywane w przypadku postępowań dotyczących bliżej nieokreślonej grupy poważnych przestępstw *„very serious and exceptionally serious crimes"*, co w opinii skarżących prowadziło do tego, iż podsłuch można było stosować w postępowaniach dotyczących ponad połowy przestępstw

---

European Court of Human Rights, Human rights and criminal procedure, Council of Europe 2009, s. 124-126.

13 Decyzja z 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, skarga nr 54934/00.

14 Por. wyrok z 18 lutego 2003 r. w sprawie *Prado Bugallo przeciwko Hiszpanii*, skarga nr 58496/00 .

15 Tak też w wyrokach *Kruslin przeciwko Francji*, wyrok z 24 kwietnia 1990 r., Seria A nr 176-A, § 27; *Huvig przeciwko Francji*, wyrok z 24 kwietnia 1990, Seria A nr 176-B, § 26; *Dumitru Popescu przeciwko Rumunii*, wyrok z 26 kwietnia 2007, skarga nr 71525/01, § 61.

16 Wyrok z 10 lutego 2009 r. w sprawie *Iordachi i Inni przeciwko Mołdawii*, skarga nr 25198/02.

wymienionych w kodeksie karnym).

Z kolei w wyroku w sprawie *Uzun przeciwko Niemcom*[17], ETPCz nie dopatrzył się naruszenia art. 6 i 8 Konwencji, bowiem przepisy art. 101 c niemieckiego k.p.k. przewidywały, że technikę GPS stosuje się „w celu wykrycia pobytu sprawcy" („*to detect the perpetrator's whereabouts"*), a jednocześnie prawo krajowe przewidywało ograniczenie stosowania takich technik do osób podejrzewanych o popełnienie najcięższych przestępstw. ETPCz wskazał też, że niemieckie prawo zostało zmodyfikowane w konsekwencji pojawienia się sprawy skarżącego, poprzez dalsze zwiększenie gwarancji ochrony praw człowieka, przy czym nawet przed modyfikacją przepisów system prawny przewidywał mechanizm kontroli sądowej stosowania takiej techniki operacyjnej jak GPS.

Reasumując, ETPCz stoi na stanowisku, iż zasada poszanowania praworządności obliguje strony Konwencji do ograniczenia działań policji tylko do sytuacji dozwolonych i dostatecznie uzasadnionych przez prawo krajowe[18]. Wypełnienie tego obowiązku powinno w szczególności polegać na tym, iż stosowne przepisy powinny być dostępne dla obywateli, a po wtóre przepisy powinny być jasne w swoim zakresie, tak aby obywatel wiedział w jakich okolicznościach i na jakich warunkach władze publiczne są uprawnione do uciekania się do działań tajnych, ingerujących w ich życie prywatne[19].

3. Niezgodność zaskarżonych przepisów z art. 2, art. 47 w zw. z art. 31 ust. 3 Konstytucji RP oraz art. 8 Konwencji

W ocenie wnioskodawców zaskarżone przepisy, naruszają zasady poprawnej legislacji i pozostają w sprzeczności z art. 2, art. 47 w związku z art. 31 ust. 3 Konstytucji RP oraz art. 8 Konwencji. Niejasne jest bowiem na gruncie zaskarżonych przepisów, jakich konkretnie środków można używać przy prowadzeniu kontroli operacyjnej, a po drugie jakie konkretnie informacje, Policja, służby specjalne oraz inne organy odpowiedzialne za zapewnienie bezpieczeństwa mogą pozyskiwać w ramach prowadzonej kontroli operacyjnej.

Użycie przez ustawodawcę w przepisie kształtującym upoważnienie do stosowania określonych środków w ramach kontroli operacyjnej, która ze swej natury stanowi głęboką ingerencję w prawa i wolności konstytucyjne, pojęcia nieostrego i zdefiniowanego tylko w części,

17 Wyrok z 2 września 2010 r. w sprawie *Uzun przeciwko Niemcom*, skarga nr 35623/05.
18 Wyrok z 26 kwietnia 1979 r. w sprawie *Sunday Times przeciwko Wielkiej Brytanii*, skarga nr 6538/74, § 49.
19 Wyrok z 26 marca 1987 r. w sprawie *Laender przeciwko Szwecji*, skarga nr 9248/81, § 51.

stanowi o naruszeniu zasady prawidłowej legislacji, w tym wymogu legalności substancjalnej. Przepisy te nie dają pełnego obrazu czynności, które organy państwowe mogą przedsięwziąć w stosunku do obywateli, w ramach kontroli operacyjnej. W szczególności powstaje wątpliwość, czy w ramach kontroli operacyjnej mogą być obecnie stosowane takie środki jak: nadajniki GPS, mikrofony kierunkowe czy instalowanie oprogramowania szpiegowskiego. Powstaje zatem sytuacja, gdzie nie wiadomo kto i kiedy, a nawet jakim ograniczeniom może podlegać z uwagi na zarządzenie kontroli operacyjnej.

Wnioskodawcy pragną podkreślić, iż interpretacja zaskarżonych przepisów jest w tym zakresie niejednolita. Na pewno zdaniem wnioskodawców, nie można przyjąć, iż konstruując zaskarżone przepisy, zamiarem ustawodawcy było umożliwienie Policji, służbom specjalnym oraz innym podmiotom wykonującym zadania ochrony bezpieczeństwa państwa, sięgania po wszelkie dostępne na danym etapie rozwoju technologicznego środki techniczne. Zdaniem wnioskodawców, przepis określający zakres środków, które mogą być stosowane w ramach kontroli operacyjnej powinna cechować daleko posunięta precyzja. Każdy z możliwych do stosowania środków powinien być wzorem ww. art. 101c ust. 1 niemieckiego k.p.k. określony w konkretny i niebudzący wątpliwości sposób, tak by jednostka wiedziała jakie środki i w jaki sposób mogą być wobec niej zastosowane, a także jakie konkretnie informacje na temat jej życia prywatnego mogą być gromadzone[20]. W przeciwnym razie, prócz ekstensywnej wykładni przepisów dotyczących kontroli operacyjnej może powstać też nieuprawnione przekonanie, iż skoro dany środek nie został wprost wskazany w przepisie dotyczącym kontroli operacyjnej, to jego stosowanie nie jest obwarowane szczególnymi wymogami: subsydiarności i zgody właściwego sądu oraz prokuratora[21].

Z racji tego, iż przedmiotem analizy jest przepis kompetencyjny, regulujący określone uprawnienie – stosowanie kontroli operacyjnej służb specjalnych, Policji oraz podmiotów

20 Problem ten był szeroko dyskutowany w trakcie seminarium „*Stosowanie podsłuchów i kontroli operacyjnej a gwarancje praw i wolności jednostki – niezbędne zmiany prawne”* zorganizowanego przez Helsińską Fundację Praw Człowieka w dniu 16 listopada 2009 r. W czasie przedmiotowego seminarium T. Tomaszewski wskazał, iż nie unikniemy rozwoju technologicznego, który pociągnie za sobą konieczność przyznania kolejnych uprawnień służbom specjalnym. Zaznaczył przy tym, iż zapisanie wprost możliwości wykorzystywania przez służby specjalne nowych zdobyczy techniki umożliwia przynajmniej kontrolę nad ich działalnością w tym zakresie. Konieczne jest przy tym zapisanie pewnych wymogów proporcjonalności w postaci zakresu przedmiotowego oraz okoliczności sięgania po te środki. Opracowanie seminarium jest dostępne pod adresem: http://www.hfhrpol.waw.pl/precedens/sluzby/opracowanie-seminarium-stosowanie-podsluchow-i-kontroli-operacyjnej-a-gwarancje-praw-i-wolnosci-jednostki-niezbedne-zmiany-prawne.html.

21 Zdaniem J. Widackiego służby pomimo korzystania z materiałów, np. z monitoringu czy z danych operatorów telefonii komórkowej pozwalających śledzić ruch obiektu, niesłusznie nie traktują tego jako inwigilacji wymagającej sądowej zgody. S. Waltoś wskazuje z kolei, iż *“przepis nieprzypadkowo mówi o konieczności uzyskania sądowej zgody na "stosowanie środków technicznych". Obejmuje tym samym wszelkie sposoby stosowania takich środków, nie tylko podsłuch telefoniczny”*. Por. E. Siedlecka, *Całe nasze życie na podglądzie*, Gazeta Wyborcza z 7 października 2010 r. Artykuł dostępny jest na stronie: http://wyborcza.pl/1,75478,8475018,Cale_nasze_zycie_na_podgladzie.html.

wykonujących zadania ochrony bezpieczeństwa państwa - doprecyzowanie ustawodawstwa w tym zakresie leży także w ich interesie. Wnioskodawca pragnie jedynie zasygnalizować, iż w 2009 r. Ministerstwo Spraw Wewnętrznych i Administracji przygotowało *projekt ustawy o zmianie ustawy o Policji i niektórych innych ustaw*[22], zmierzający do doprecyzowania zakresu środków możliwych do stosowania w ramach kontroli operacyjnej o *„stosowanie środków elektronicznych umożliwiających niejawne i zdalne uzyskanie dostępu do zapisu na informatycznym nośniku danych, treści przekazów nadawanych i odbieranych oraz ich utrwalanie”*. Podjęta próba zmiany przepisów stanowiła w ocenie wnioskodawców właśnie przejaw wątpliwości co do zakresu środków możliwych do stosowania w ramach kontroli operacyjnej, bowiem w piśmiennictwie[23] pojawiały się już głosy co do możliwości stosowania tych technik operacyjnych na gruncie aktualnego brzmienia ww. przepisów. Za inny przykład tychże wątpliwości można także uznać zapisanie w art. 14 ust. 6 *poselskiego projektu ustawy o czynnościach operacyjno – rozpoznawczych*[24], że prócz stosowania środków wskazanych w pkt 1-3, kontrola operacyjna może polegać na „tajnej lustracji pomieszczeń i środków transportu”. Dookreślenie przez ustawodawcę zaskarżonego przepisu jest w ocenie wnioskodawców także konieczne z punktu widzenia rzetelności kontroli sądowej nad wnioskiem o zarządzanie kontroli operacyjnej, bowiem wskazać w nim należy m.in. *„dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub* ***sposobu jej stosowania****”* czy też *„cel, czas i* ***rodzaj prowadzonej kontroli operacyjnej****”*.

Z tych też powodów, w ocenie wnioskodawców zaskarżone przepisy należy uznać za niezgodne z art. 2, art. 47, art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz art. 8 Konwencji.

II

Zaskarżone normy, nakładają na operatorów telekomunikacyjnych obowiązek gromadzenia określonych danych telekomunikacyjnych (m.in. numeru telefonu, czasu połączenia czy stacja przekaźnikowa w zasięgu której znajdował się wykonujący i odbierający połączenie, ale także danych dotyczących ruchu w Internecie). Dane te dotyczą wszystkich abonentów, bez względu na to czy dana osoba popełniła jakiekolwiek przestępstwo czy też zagraża bezpieczeństwu państwa. Z drugiej strony, normy te przyznają Policji, służbom specjalnym oraz organom odpowiedzialnym za

22 Projekt dostępny jest pod adresem: http://bip.mswia.gov.pl/portal/bip/178/18317/Projekt_Ustawy_z_dnia__2009_r_o_zmianie_ustawy_o_Policji_i_niektorych_innych_ust.html

23 A. Kiedrowicz, *Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej*, Prok. i Pr. 10/2008, s. 134.

24 Druk sejmowy nr 353.

bezpieczeństwo możliwość bezpłatnego pozyskiwania tych danych w związku z wykonywaniem zadań ustawowych, w tym wykrywaniem i zapobieganiem wszelkiego rodzaju przestępczości. Pozyskanie tych danych nie podlega jakiejkolwiek zewnętrznej kontroli, pod kątem celowości i niezbędności. Pobranie danych może zostać dokonane na podstawie wniosku upoważnionego funkcjonariusza jak i za pomocą sieci telekomunikacyjnej. Zaskarżone normy wykazują także deficyt w zakresie regulacji dotyczących prawidłowości przechowywania i niszczenia ww. danych.

W ocenie wnioskodawców, wskazane normy prowadzą do nieproporcjonalnego ograniczenia prawa do prywatności (art. 47 Konstytucji RP), swobody komunikowania się (art. 49 Konstytucji RP) oraz autonomii informacyjnej jednostki (art. 51 Konstytucji RP).

1. Zatrzymywanie, przechowywanie i przekazywanie uprawnionym podmiotom danych telekomunikacyjnych.

Zgodnie z art. 28 ust. 1 ustawy o ABW oraz AW obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez ABW zadań, o których mowa w art. 5 ust. 1, w postaci danych:
1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.),
2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.
Analogiczne uregulowanie znajduje się w art. 32 ust. 1 ustawy o SKW oraz SWW oraz art. 18 ust. 1 ustawy o CBA.

Te same dane, zgodnie z art. 36b ust. 1 ustawy o kontroli skarbowej, wywiad skarbowy może pozyskiwać w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b, oraz naruszeń krajowych przepisów celnych.

Z kolei zgodnie z art. 20c ust. 1 ustawy o Policji, w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej „danymi telekomunikacyjnymi”, oraz może je przetwarzać. Analogiczne uregulowanie znajduje się w art. 10b ust. 1 ustawy o Straży Granicznej, przy czym ustawodawca wprost nie wskazał, iż Straż Graniczna może przetwarzać te dane.

Natomiast art. 30 ust. 1 ustawy o Żandarmerii Wojskowej stanowi, iż w celu zapobiegania lub wykrywania przestępstw, w tym skarbowych, Żandarmeria Wojskowa, może mieć udostępniane dane telekomunikacyjne oraz je przetwarzać.

Podmiot wykonujący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia ww. dane nieodpłatnie, odpowiednio:
1) funkcjonariuszowi wskazanemu w pisemnym wniosku właściwego podmiotu lub osoby upoważnionej przez ten organ;
2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu upoważnienie, o którym mowa w pkt 2.

Udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy szefem danej formacji a tym podmiotem.

Udostępnienie danych telekomunikacyjnych 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.
W przypadku ustawy o Policji, Straży Granicznej, Żandarmerii Wojskowej, o CBA, o SKW oraz SWW zastrzeżono, iż pozyskanie danych z użyciem sieci telekomunikacyjnej musi być uwarunkowane specyfiką lub zakresem wykonywanych zadań albo prowadzonych czynności.

Zgodnie z art. 180a ust. 1 Prawa telekomunikacyjnego, z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:
1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;

2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonym w przepisach odrębnych;
3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159-175 i art. 180e.

Zgodnie z art. 180c ust. 1 obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do:
1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
a) inicjującego połączenie,
b) do którego kierowane jest połączenie;
2) określenia:
a) daty i godziny połączenia oraz czasu jego trwania,
b) rodzaju połączenia,
c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Dane niezbędne, o których mówi art. 180c ust. 1 Prawa telekomunikacyjnego zostały doprecyzowane przepisami rozporządzenia z Ministra Infrastruktury z 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[25], wydanego na podstawie art. 180c ust. 2 Prawa telekomunikacyjnego.

W rozporządzeniu dane te zostały podzielone na podkategorie (§ 3 - 7):
a) niezbędne do ustalenia w stacjonarnej publicznej sieci telekomunikacyjnej (tu m.in. imię i nazwisko abonenta telefonu stacjonarnego i jego adres),
b) niezbędne do ustalenia w ruchomej publicznej sieci telekomunikacyjnej (tu m.in. identyfikator anteny stacji BTS, współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe, azymut, wiązkę i zasięg roboczy anteny stacji BTS)
c) niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego, do których jest kierowane połączenie, w przypadku usług polegających na przekierowaniu lub przełączaniu połączenia,
d) niezbędne w przypadku usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej (tu m.in. identyfikator użytkownika, adres IP)

25 Dz. U. z 2009 r. Nr 226, poz. 1828.

e) niezbędne w przypadku usługi poczty elektronicznej i usługi telefonii internetowej (tu m.in. imię i nazwisko albo nazwa oraz adres zarejestrowanego użytkownika końcowego usługi poczty elektronicznej lub usługi telefonii internetowej, do którego jest kierowane połączenie, oraz identyfikator tego użytkownika).

Zgodnie natomiast z art. 180g ust. 1 Prawa telekomunikacyjnego przedsiębiorca telekomunikacyjny, w terminie do dnia 31 stycznia, składa Prezesowi UKE, za rok poprzedni informacje o:
1) łącznej liczbie przypadków, w których uprawnionym podmiotom, sądowi i prokuratorowi były udostępnione dane, o których mowa w art. 180c ust. 1;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w pkt 1, wniosku lub ustnego żądania o ich udostępnienie;
3) łącznej liczbie przypadków, w których wniosek lub ustne żądanie, o którym mowa w pkt 2, nie mógł być zrealizowany.
Informacje te Prezes UKE przekazuje z kolei Komisji Europejskiej[26].

2. Niekonstytucyjność art. 180 a ust. 1 i art. 180 c Prawa telekomunikacyjnego w zw. z art. 20 c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej, art. 28 ustawy o ABW oraz AW, art. 18 ustawy o CBA, art. 32 ustawy o SKW oraz SWW

W ocenie wnioskodawców, zaskarżone przepisy są niezgodne z art. 47, art. 49, art. 51 w związku z art. 31 ust. 3 Konstytucji RP.

Mechanizm upoważniający Policję, służby specjalne oraz inne podmioty wykonujące zadania ochrony bezpieczeństwa państwa do pozyskiwania danych telekomunikacyjnych wymienionych w art. 180 c Prawa telekomunikacyjnego (doprecyzowanych w ww. rozporządzeniu) oraz danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług, został skonstruowany przez ustawodawcę w sposób nieprawidłowy. Dostęp i korzystanie z zatrzymanych danych

26 W świetle informacji przytoczonych przez sekretarza Kolegium do Spraw Służb Specjalnych przy Radzie Ministrów w trakcie debaty w dniu 2 grudnia 2010 r. u Rzecznika Praw Obywatelskich wynika, że wszystkie służby specjalne występują do operatorów o udostępnienie ok. 60-70 tys. billingów rocznie. W 2009 r. najczęściej występowała o nie Agencja Bezpieczeństwa Wewnętrznego (50 tys. razy), rzadziej zaś Centralne Biuro Antykorupcyjne i Służba Kontrwywiadu Wojskowego (po ok. 7 tys. razy). PAP: Debata w biurze Rzecznika o stosowaniu technik operacyjnych, depesza z 2 grudnia 2010 r.

telekomunikacyjnych przez organy państwowe zalicza się do środków inwigilacji[27]. Zatem, jest rzeczą oczywistą, że przepisy prawne dotyczące inwigilacji w oparciu o retencję danych muszą przejść test proporcjonalności w celu sprawdzenia, czy środek ten jest konieczny w demokratycznym społeczeństwie.

Na prawidłowo skonstruowany mechanizm pozyskiwania danych telekomunikacyjnych w państwie demokratycznym powinny się składać[28]:

1) przepisy określające zakres działania, zadania i kompetencję w ścisłym tego słowa znaczeniu do podejmowania przez funkcjonariuszy poszczególnych formacji działań wobec jednostek w zakresie ich wolności i prywatności (gwarancje kompetencyjne),

2) system gwarancji proceduralnych i instytucjonalnych innych niż gwarancje wynikające z regulacji zakresu zadań i kompetencji.

Gwarancje kompetencyjne polegają w założeniu na precyzyjnym związaniu władzy publicznej adekwatnym oraz jasnym określeniem norm legitymizujących podjęcie konkretnych zachowań przez funkcjonariuszy. Gwarancje proceduralne i instytucjonalne dotyczą natomiast nadzoru (zewnętrznego) nad poszczególnymi formacjami, oraz uprawnień i procedur umożliwiających jednostce dotkniętej ich działaniem obronę jej sfery prywatnej, a także zewnętrznym wobec nich organom – orientację niezbędną do realizacji nadzoru (kontroli).

By mechanizm dający możliwość wkroczenia w prawa i wolności jednostki mógł być określony jako pozostający w zgodzie ze standardami konstytucyjnymi, musi być komplementarny co do swych składników. Oznacza to, że jeśli braki wykazuje regulacja kompetencji (za szeroka, luźna, niejasna, nieprecyzyjna), wówczas precyzja i sprawne ujęcie gwarancji proceduralnych i instytucjonalnych może powodować, że kontrolowana regulacja pomyślnie przejdzie przez test konstytucyjności. I odwrotnie: im precyzyjniejsze i jasne operowanie normami kompetencyjnymi, tym większe szanse na pomyślny test konstytucyjności ustawy, nawet przy innych usterkach regulacji gwarancji proceduralnych i instytucjonalnych[29].

Zdaniem wnioskodawców, na gruncie zaskarżonych przepisów, ustawodawca tworząc

27 A. Taracha, Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe, Lublin 2006, s. 75 i n.
28 Zdanie odrębne prof. E. Łętowskiej do wyroku TK z 23 czerwca 2009 r., sygn. K 54/07.
29 Zdanie odrębne prof. E. Łętowskiej do wyroku TK z 23 czerwca 2009 r., sygn. K 54/07.

system retencji danych wadliwie skonstruował:

1) obowiązek operatorów telekomunikacyjnych zatrzymywania i przechowywania danych telekomunikacyjnych;

2) kompetencję do pozyskiwania ww. danych przez służby specjalne, Policję, Straż Graniczną, wywiad skarbowy oraz Żandarmerię Wojskową;

3) regulacje gwarancyjne w zakresie kontroli wewnętrznej i zewnętrznej.

2.1. Obowiązek zatrzymywania i przechowywania danych telekomunikacyjnych

Art. 180a Prawa telekomunikacyjnego jest wynikiem implementacji do krajowego porządku prawnego 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 oraz zmieniającej dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.04.2006, s. 54)(dalej: „Dyrektywa retencyjna"). Przepis ten nakazuje operatorom zachowywać i przetrzymywać dane telekomunikacyjne, udostępniać je w trybie wskazanym w przepisach, a także chronić te dane. Ustawodawca nałożył maksymalny, przewidziany przez dyrektywę, 24-miesięczny okres zatrzymywania i przechowywania danych. Co więcej, w art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego ustawodawca zakazuje niszczenia ww. danych nawet po upływie 24 miesięcy - licząc od dnia połączenia lub nieudanej próby połączenia - w sytuacji, gdy dane zostały zabezpieczone zgodnie z przepisami odrębnymi. Okres maksymalny przechowywania danych zabezpieczonych na podstawie odrębnych przepisów nie został w Prawie Telekomunikacyjnym jak i w odrębnych przepisach określony. Zapis ten jest zatem sprzeczny z art. 6 Dyrektywy retencyjnej.

Art. 180c Prawa telekomunikacyjnego dookreśla natomiast jakie dane podlegają retencji. Zakres zatrzymywania danych w Polsce jest zgodny z przewidzianym w art. 5 Dyrektywy retencyjnej i obejmuje wszystkie wymienione w tym artykule rodzaje danych. Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w § 3 – 4 i § 6 - 7, określa szczegółowo kategorie danych, jakie należy zatrzymywać.

Prawo telekomunikacyjne nakłada obowiązek zatrzymania i przechowywania ww. danych przez operatorów jako formę realizacji zadań na rzecz obronności i bezpieczeństwa państwowego.

Jest to obowiązek, który powstaje przy praktycznie każdym użyciu telefonu stacjonarnego lub komórkowego, faksu, e-maila, telefonii internetowej (dotyczy wszystkich zrealizowanych i nieudanych prób połączeń) i nie jest konieczne wykazywanie związku zatrzymania danych z dochodzeniem, wykrywaniem czy też ściganiem „poważnego przestępstwa". Retencja danych ma zatem charakter powszechny i w przypadku danych zabezpieczonych nieograniczony czasowo.

2.2. Kompetencja służb specjalnych, Policji, Straży Granicznej, wywiadu skarbowego oraz Żandarmerii Wojskowej do pozyskiwania danych telekomunikacyjnych

W art. 1 Dyrektywy retencyjnej stanowi, iż jej celem *„jest zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego."*

Tymczasem w zaskarżonych przepisach, ustawodawca wskazał, iż pozyskanie danych telekomunikacyjnych nie wymaga zgody sądu okręgowego i zgody właściwego prokuratora, jeśli są one:

- niezbędne do realizacji ustawowych zadań (w przypadku ABW, SKW, CBA),
- pozyskane w celu zapobiegania lub ścigania przestępstw/przestępstw skarbowych (Policja, Straż Graniczna, Żandarmeria Wojskowa, kontrola skarbowa),
- niezbędne do ustalania naruszeń krajowych przepisów celnych (kontrola skarbowa).

Zatem warunkiem *sine qua non* pozyskania tych danych jest wykazanie, iż spełniona została jedna z powyższych przesłanek. Ustawodawca nie ograniczył zatem pozyskania danych do dochodzenia, wykrywania i ścigania poważnych przestępstw. Wyszedł tym samym poza zakres celów określonych w Dyrektywie retencyjnej.

Ustawodawca pominął przy tym zupełnie okoliczność, iż przepisy określające zadania nałożone na służby specjalne i podmioty wykonujące zadania ochrony bezpieczeństwa państwa nacechowane są nieostrością, wynikającą z nadużywania określeń niezdefiniowanych w przepisach obowiązującego prawa, a w szczególności klauzul generalnych (np. bezpieczeństwo państwa), czy też zwrotów otwartych („w szczególności"). Dla przykładu do zadań ustawowych służb specjalnych, Policji i podmiotów wykonujących zadania bezpieczeństwa państwa należy m.in.:

- *„rozpoznawanie, zapobieganie i zwalczanie **zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny**, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa”* - art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW;

- *„**rozpoznawanie**, zapobieganie i wykrywanie przestępstw: a) szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej **i innych przestępstw godzących w bezpieczeństwo państwa**, b) **godzących w podstawy ekonomiczne państwa**, c) **korupcji** osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584, z 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375), jeśli może to godzić w bezpieczeństwo państwa (...)”* - art. 5 ust. 1 pkt 2 ustawy o ABW oraz AW;

- *„ujawnianie i przeciwdziałanie **przypadkom nieprzestrzegania** przepisów ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne”* - art. 2 ust. 1 pkt 2 ustawy o CBA.

W tej sytuacji kompetencja do pozyskania danych telekomunikacyjnych została określona w luźny sposób, co powoduje, iż w efekcie, nawet arbitralna decyzja funkcjonariusza o podjęciu działania (w tym przypadku pozyskania danych) zawsze będzie mogła być uznana za mieszczącą się w „zakresie realizacji zadań”, a co więcej decyzja ta pozostaje poza nadzorem zewnętrznym. Ustawodawca doprowadził tu więc do autonomii operacyjnej funkcjonariuszy (ABW, CBA, wywiadu skarbowego, SKW). Oględne powołanie się na realizację zadań, legitymizuje działania operacyjne nawet w obliczu wysoce abstrakcyjnych zagrożeń, których realne wystąpienie jest znikome (szczególnie, gdy podstawą wystąpienia z wnioskiem jest zapobieżenie przestępstwu). Przecież to funkcjonariusz dokonuje decyzji co do podjęcia działań, a taka decyzja nie podlega niczyjej weryfikacji, także *ex post.*

Natomiast w przypadku Policji, Straży Granicznej, wywiadu skarbowego oraz Żandarmerii Wojskowej jedynym wymogiem pozyskania danych telekomunikacyjny określonych w art. 180 c Prawa telekomunikacyjnego jest wykazanie dość luźnego związku pozyskania danych z zapobieganiem lub ściganiem przestępstw/przestępstw skarbowych. Co więcej wywiad skarbowy może także pozyskiwać ww. dane w związku z zapobieganiem i wykrywaniem naruszeń krajowych przepisów celnych oraz ściganie naruszeń krajowych lub wspólnotowych przepisów celnych przez

wykonywanie nadzoru transgranicznego osób, miejsc, środków transportu i towarów oraz dostawy kontrolowanej, w rozumieniu Konwencji sporządzonej na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi, sporządzonej w Brukseli dnia 18 grudnia 1997 r. (Dz. U. z 2008 r. Nr 6, poz. 31). Ustawodawca nie widział tu konieczności ograniczenia pozyskiwania danych dla zapobiegania przestępstw najcięższych. Nie dostrzegł również problemu tzw. czynów przepołowionych – sytuacji, gdy o zaistnieniu przestępstwa decyduje spełnienie określonego kryterium „ilościowego" (np. wartość skradzionego lub zniszczonego mienia).

2.3. Deficyt regulacji gwarancyjnych w zakresie kontroli wewnętrznej i zewnętrznej

Zaskarżone przepisy, w ocenie wnioskodawców budzą uzasadnione wątpliwości konstytucyjne także w sferze gwarancji proceduralnych i instytucjonalnych dotyczących ochrony przed arbitralnością decyzji organów państwowych w zakresie pozyskiwania danych. Regulacje te, przede wszystkim nie uwzględniają konieczności zapewnienia jakichkolwiek (czy to wewnętrznych czy zewnętrznych) form nadzoru nad działalnością poszczególnych formacji, nie tworzą też uprawnień i procedur umożliwiających jednostce dotkniętej ich działaniem obronę jej prywatności, a także zewnętrznym wobec nich organom – orientację niezbędną do realizacji nadzoru (kontroli). Zdaniem wnioskodawców, w zaskarżonych przepisach ustawodawca dopuścił się w tym zakresie pominięcia legislacyjnego.

1) nadzór wewnętrzny

W zakresie procedur wewnętrznych dotyczących pozyskiwania i przechowywania, jedynie ustawy o Policji (art. 20 c ust. 7), Żandarmerii Wojskowej (art. 30 ust. 7) oraz Straży Granicznej (art. 10b ust. 6) przewidują, iż uzyskane materiały, które nie zawierają informacji mających znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Zatem tylko na gruncie tych ustaw istnieje obowiązek dokonywania weryfikacji przydatności pozyskanych informacji, którego realizacja jest wewnętrzną sprawą funkcjonariuszy Policji, Żandarmerii Wojskowej oraz Straży Granicznej. Zaskarżone przepisy nie przewidują natomiast żadnej zewnętrznej kontroli nad prawidłowością procesu niszczenia tychże danych, nawet dokonywanej w sposób wyrywkowy.

2) nadzór zewnętrzny

Jedynie w art. 36b ust. 4-5 ustawy o kontroli skarbowej ustawodawca wprowadził namiastkę zewnętrznej kontroli nad prawidłowością pozyskiwania ww. danych. Przepisy te wskazują, iż informację o wystąpieniu z wnioskiem o udostępnienie danych przekazuje się niezwłocznie ministrowi właściwemu do spraw finansów publicznych. Minister właściwy do spraw finansów publicznych w każdej chwili może zażądać od Generalnego Inspektora Kontroli Skarbowej informacji o przyczynach uzasadniających wystąpienie z wnioskiem, a także o sposobie wykorzystania danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe. Ponadto minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, za nieuzasadnione. Pozostałe zaskarżone regulacje nie przewidują jakichkolwiek form zewnętrznego nadzoru nad prawidłowością pozyskiwania danych telekomunikacyjnych.

Natomiast na gruncie przepisów ustawy o CBA, o ABW oraz AW, o SKW oraz SWW ustawodawca, zupełnie pominął kwestię procedur kontrolnych o charakterze wewnętrznym jak i zewnętrznym, nad prawidłowością pozyskiwania, przetwarzania jak i niszczenia ww. danych. Nie ma w tych przepisach, w szczególności wskazań co do okresu przechowywania ww. danych, kwestii niwelacji skutków „ekscesu" przy pozyskiwaniu danych, czy też samego wskazania o konieczności usuwania danych niemających znaczenia dla realizacji ustawowych zadań. Nie ma także we wskazanych przepisach pozytywnego obowiązku poinformowania jednostki o pobraniu danych telekomunikacyjnych ją dotyczących. W tej sytuacji, zdaniem wnioskodawców, zaskarżone przepisy w pełni sankcjonują możliwość zbierania danych ze względu na potencjalną przydatność, co stoi w sprzeczności ze standardami konstytucyjnymi.

Brak regulacji w zakresie nadzoru (wewnętrznego i zewnętrznego) nad gromadzeniem, przechowywaniem i niszczeniem danych, należy rozpatrywać w kategoriach tzw. pominięcia legislacyjnego. Z pominięciem legislacyjnym mamy do czynienia wtedy, gdy ustawodawca zaniecha uregulowania w ustawie pewnych kwestii, a które należy następnie wypełnić w drodze wykładni[30]. Kontrola konstytucyjności w przypadku pominięcia legislacyjnego dotyczy obowiązującego aktu normatywnego z punktu widzenia tego, czy w jego przepisach nie brakuje unormowań, bez których może on budzić wątpliwości natury konstytucyjnej.

Pominięcie legislacyjne na gruncie zaskarżonych przepisów stwarza niebezpieczeństwo

30 Wyrok TK z dnia 8 września 2005 r., sygn. P 17/04, Z.U. 2005 / 8A / 90.

pozyskiwania przez organy państwa wskazanych danych „na wypadek", czyli ze względu na potencjalną przydatność. Na gruncie zaskarżonych przepisów pozyskanie danych odbywa się poprzez powołanie się na konieczność realizacji ustawowych zadań, przy czym czynność funkcjonariusza w tym zakresie nie podlega jakiejkolwiek zewnętrznej kontroli. Jednocześnie jednostka może nigdy nie posiąść informacji na temat pozyskiwania jej danych telekomunikacyjnych przez organy państwowe.

2.4. Niezgodność zaskarżonych regulacji z art. 47, art. 49, art. 51 ust. 2 i ust. 4, art. 31 ust. 3 Konstytucji RP

Retencja danych regulowana na gruncie zaskarżonych przepisów, jako obowiązek operatorów spełniany na rzecz obronności państwa, sprowadzający się do zatrzymywania, przechowywania, ochrony i przekazywania uprawnionym organom ww. danych telekomunikacyjnych, godzi w nieproporcjonalny sposób w prawo do prywatności, swobodę komunikowania się oraz autonomię informacyjną. W ocenie wnioskodawców, na gruncie zaskarżonych przepisów w sposób niekonstytucyjny określono zarówno obowiązek operatorów zatrzymania i przechowywania danych telekomunikacyjnych, jak i mechanizm upoważniający organy państwowe do ich pozyskiwania.

Retencja danych telekomunikacyjnych narusza prawo do prywatności, gwarantowane w art. 47 Konstytucji i doprecyzowane także w art. 49 Konstytucji RP (swoboda komunikowania się). Ogranicza ona swobodę zawierania i podtrzymywania znajomości i daje organom państwowym możliwość poznania także zainteresowań jednostki oraz sposobu spędzania czasu wolnego. Na podstawie tych informacji, organy państwowe wiedzą, gdzie, kiedy i z kim jednostka próbowała nawiązać kontakt. W pewnym sensie można powiedzieć, że wzmożonemu zainteresowaniu poddawana jest także swoboda poruszania się[31] i przebywania w określonych miejscach – bowiem dane te pozwalają ustalić położenie geograficzne jednostek oraz „ślady" w internecie.

Z kolei jeśli idzie o stosunek retencji danych i konieczności ochrony autonomii informacyjnej, to należy wskazać, iż zgodnie z art. 51 ust. 2 Konstytucji władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Przepis ten dotyczy każdego rodzaju informacji. Za informację niezbędną uznaje się taką wiedzę bez której posiadania organy władzy publicznej nie

31 8 października 2009 roku rumuński Sąd Konstytucyjny wydał wyrok nr 1258, w którym wskazał, iż przepisy rumuńskiej ustawy dotyczącej retencji danych, naruszały prawo do swobodnego poruszania się.

będą zdolne do podjęcia działań w ramach przyznanych im kompetencji[32]. Zatem „niezbędność" zakłada subsydiarny charakter działania mającego na celu pozyskanie informacji. Granicę pozyskiwania danych stanowią z jednej strony – ich szczegółowość, z drugiej zakres pozyskiwania (potrzeby je uzasadniające np. tworzenie wysoce wyspecjalizowanych baz danych, gromadzenie na wypadek). Warto jedynie wspomnieć, iż na gruncie art. 51 Konstytucji RP istnieje domniemanie naruszenia autonomii informacyjnej, przedmiotem dowodu jest tylko to, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne" lub „użyteczne" dla władzy. To po stronie organów publicznych leży wykazanie, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym[33]. Na gruncie przepisów retencyjnych, obowiązek gromadzenia danych telekomunikacyjnych powstaje z samego faktu skorzystania z określonych narzędzi komunikacyjnych, bez związku ze zwalczaniem najcięższych przestępstw. W tej sytuacji, gromadzenie i dostęp do ww. danych telekomunikacyjnych nie może być uznane za gromadzenie danych „niezbędnych w demokratycznym państwie prawnym".

Jak już wyżej wskazano pozyskanie tych danych odbywa się poprzez przekazanie:
1) funkcjonariuszowi wskazanemu w pisemnym wniosku właściwego podmiotu lub osoby upoważnionej przez ten organ;
2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu upoważnienie, o którym mowa w pkt 2[34].
Zatem może się ono odbywać bez udziału operatora telekomunikacyjnego. Z wyjątkiem ustawy o kontroli skarbowej, żaden zewnętrzny podmiot spoza struktury danej formacji nie nadzoruje prawidłowości pobierania ww. danych. Ustawodawca zrezygnował zatem ze standardu kontroli sprawowanej przez organ zewnętrzny.

Wnioskodawcy pragną przy tej okazji wskazać, iż blankietowa retencja danych została zakwestionowana już przez niemiecki Federalny Sąd Konstytucyjny oraz rumuński Trybunał Konstytucyjny.

W wyroku z 8 października 2009 r.[35] rumuński Sąd Konstytucyjny uznał, że brak precyzji przepisów prawnych (tzw. ustawa nr 298/2008) określających zakres danych niezbędnych do

32 B. Banaszak, Komentarz do art. 51, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2009, s. 262.
33 Wyrok TK z 20 listopada 2002 r., sygn. K 41/02, Z.U. 2002 / 6A / 83.
34 W świetle informacji przedstawionych przez sekretarza Kolegium ds. Służb Specjalnych przy Radzie Ministrów, w CBA kartę indywidualizującą, uprawniającą do pozyskania danych poprzez sieć telekomunikacyjną posiada 41 osób.
35 Wyrok z 8 października 2009 r. nr 1258, dostępny na stronie: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

określenia osób fizycznych i prawnych, otwiera możliwość nadużyć w sferze przechwytywania danych przez dostawców usług elektronicznych. Sąd Konstytucyjny podkreślił, że ograniczenie prawa do życia prywatnego i tajemnicy korespondencji i wolności słowa, musi być dokonywane w sposób przejrzysty, przewidywalny i jednoznaczny oraz tak, aby uniknąć możliwości dowolności i nadużyć ze strony władz. Trybunał powołując się na orzecznictwo ETPCz[36] przypomniał, że państwa, które przyjęły zobowiązania w celu zapewnienia praw gwarantowanych przez Konwencję muszą stosować konkretne i efektywne gwarancje ochrony praw, nie zaś teoretyczne i iluzoryczne.

Sąd Konstytucyjny zwrócił także uwagę, iż retencji podlegają nie tylko dane autora połączenia, ale także dane adresata. Adresat zostaje bez własnej woli, narażony na naruszenie jego prywatności jedynie na podstawie zachowania innej osoby, na które nie ma on wpływu, a często jest to zachowanie wynikające ze złej woli. Zatem przepisy dotyczące retencji danych, powinny także skutecznie chronić w określonych sytuacjach przed ekscesem, polegającym na przypadkowym, okazyjnym zbieraniu danych na temat jednostek niezwiązanych z zasadniczym powodem pozyskania danych.

Co ważne, Sąd Konstytucyjny zaakcentował, iż ograniczenia prawa do prywatności są wyjątkiem i muszą być bardzo precyzyjnie określone. Tworzenie pozytywnego obowiązku, który przewiduje ciągłe ograniczenia prawa do prywatności i tajemnicy korespondencji narusza istotę wolności i praw przez usunięcie zabezpieczeń w odniesieniu do wykonania tych wolności i praw.

Z punktu widzenia oceny proporcjonalności, Sąd Konstytucyjny nie kwestionował celu, dla którego ustawodawca postanowił przyjąć przepisy implementujące dyrektywę 2006/24/WE, uznając, że istnieje pilna potrzeba zapewnienia odpowiednich i skutecznych narzędzi prawnych (ze względu na ciągły rozwój istniejących środków łączności), tak, by zwalczać i kontrolować zjawisko przestępczości. Jednak skonstatował, że prawa jednostek nie mogą być sprowadzane ad absurdum, a ograniczenie wykonywania niektórych praw osobistych w celu ochrony interesu publicznego, zwłaszcza zaś związanego z bezpieczeństwem narodowym, porządkiem publicznym lub zwalczaniem przestępczości, wymaga zachowania równowagi. Sąd Konstytucyjny przywołał wyrok w sprawie *Klass i inni przeciwko Niemcom*, w którym ETPCz uznał, że przyjmowanie środków nadzoru bez stosownych zabezpieczeń praw jednostek może doprowadzić do „zniszczenia demokracji w jej obronie".

36 Wyrok z 12 lipca 2001 r. w sprawie *Książę Hans-Adam II of Liechtenstein przeciwko Niemcom*, skarga nr 42527/98.

Niemiecki Federalny Sąd Konstytucyjny w wyroku z 2 marca 2010 r.[37] dokonał natomiast pogłębionej analizy przepisów §§ 113a und 113b prawa telekomunikacyjnego (*Telekommunikationsgesetzes*) w brzmieniu, które tym przepisom nadała ustawa o retencji danych telekomunikacyjnych, wdrażająca przepisy Dyrektywy 2006/24/WE, z punktu widzenia wymogu proporcjonalności.

Federalny Sąd Konstytucyjny zwrócił uwagę, iż względy proporcjonalności wymagają od ustawodawcy tworzenia precyzyjnych przepisów, w zakresie ograniczeń czasowych, ochrony danych przed nadmiernym korzystaniem z nich oraz kontroli nad ich pozyskiwaniem. Zdaniem Federalnego Sądu Konstytucyjnego wykorzystanie tych danych powinno być ograniczone tylko do przypadków konkretnych podejrzeń dotyczących poważnych przestępstw, co do których ustawodawca przewidział możliwość pozyskiwania danych telekomunikacyjnych. Ustawodawca ma zatem obowiązek stworzenia zamkniętego katalogu najcięższych przestępstw, wyznaczającego zakres przedmiotowy retencji danych.

Federalny Sąd Konstytucyjny zauważył też, iż zakazane jest wykorzystanie danych dotyczących komunikowania się z osobą wykonującą zawód związany z obowiązkiem zachowania tajemnicy (prawnik, lekarz, dziennikarz). Natomiast w zakresie transparentności sięgania przez organy państwowe po dane telekomunikacyjne konieczne jest wprowadzenie kontroli sądowej oraz obowiązku poinformowania o pozyskaniu danych, przy czym wyjątki od tej zasady (m.in. w przypadku służb wywiadowczych) powinny podlegać kontroli sądowej.

Test proporcjonalności zaskarżonych regulacji

W ocenie wnioskodawców zaskarżone regulacje nie zdają testu proporcjonalności ograniczenia praw i wolności konstytucyjnych z uwagi na interes publiczny. W wyroku z dnia 12 grudnia 2005 r., (sygn. K 32/04), Trybunał Konstytucyjny orzekł, że w celu ustalenia proporcjonalności środków nadzoru policyjnego należy zbadać, czy takie środki:
a) są w stanie doprowadzić do zamierzonych przez nie skutków,
b) są niezbędne dla ochrony interesu publicznego, z którym są powiązane,
c) czy ich efekty pozostają w proporcji do ciężarów nakładanych przez nie na obywatela[38].

Ad. a) wymóg celowości

37 Wyrok FSK z 2 marca 2010 r., 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, relacja w wersji anglojęzycznej dostępna jest na stronie: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html.
38 Wyrok z 12 grudnia 2005 r., sygn. K 32/04, Z.U. 2005 / 11A / 132.

Celem dyrektywy, było zapewnienie dostępu do danych telekomunikacyjnych dla celów dochodzenia, wykrywania i ścigania poważnych przestępstw. Potencjalna użyteczność danych o ruchu i lokalizacji jest trudna do podważenia. W środkach masowego przekazu lub przy okazji debat pojawiają się informacje na temat pożyteczności retencji danych. Na przykład w uzasadnieniu do projektu ustawy o zmianie ustawy Prawo telekomunikacyjne wskazano, iż „*w latach 2000-2005 dane o ruchu uzyskane przez prokuratorów od operatorów telekomunikacyjnych miały zasadnicze znaczenie dla skutecznego ścigania przestępców w 402 poważnych sprawach o przestępstwo*”[39]. Natomiast nie oznacza to, że skuteczne działanie organów ścigania nie możliwe jest bez korzystania z tego instrumentu prawnego.

Należy pamiętać, iż jest to instrument bardzo restrykcyjny, jeśli idzie o ochronę praw jednostki - dla Policji, służb specjalnych oraz innych podmiotów wykonujących zadania ochrony bezpieczeństwa państwa narzędzie wygodne, stanowiące kopalnię wiedzy na temat obywateli, szczególnie jeśli zważyć, iż obowiązek przechowywania tych danych wynosi 24 miesiące, o ile nie zostały one zabezpieczone we właściwej procedurze (art. 180a ust. 1 pkt 3 Prawa telekomunikacyjnego). Jednakże sama łatwość i taniość[40] pozyskania tych danych nie może usprawiedliwiać utrzymywania w aktualnym kształcie zaskarżonych przepisów.

Ad. b) wymóg niezbędności

W dyskusjach nad niezbędnością istnienia obowiązku retencji danych przywołuje się argument, iż alternatywne „niezwłoczne zabezpieczenie danych”, wskazane w art. 16 Konwencji o cyberprzestępczości[41] zawiera o wiele silniejsze gwarancje ochronne praw jednostki. Zabezpieczenie danych przede wszystkim nie wymaga od operatorów gromadzenia danych „na przyszłość”, ani nie pozwala na zabezpieczenia wszystkich danych w systemie operatora. Zabezpieczeniu podlegają jedynie te, które dotyczą konkretnego śledztwa – wiążą się z konkretnym podejrzeniem przestępstwa42.

39 Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne, http://www.pis2.home.pl/dokumenty.php?s=rzad&iddoc=49&st=1

40 Należy w tym miejscu wspomnieć, iż w postanowieniu z 25 marca 2010 r. Sąd Najwyższy (sygn. I KZP 37/09) wskazał, iż *„przepis art. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Z 2004 r., nr 171, poz. 1800 ze zmianami) nakłada na operatorów publicznej sieci telekomunikacyjnej oraz dostawców ogólnie dostępnych usług telekomunikacyjnych obowiązek udostępniania, to jest wyszukiwania, tworzenia stosownych zestawień i przesyłania za pomocą sieci telekomunikacyjnej uprawnionym podmiotom, w tym sądowi i prokuratorowi danych, o których mowa w art. 180c ust. 1 ustawy. Tak rozumiane koszty udostępniania tych danych obciążają operatora lub dostawcę i nie mogą wchodzić w skład kosztów sądowych, a zatem nie stanowią wydatków, o których mowa w art. 618 k.p.k.”*

41 Konwencja Rady Europy o cyberprzestępczości, otwarta do podpisu 23 listopada 2001 r. w Budapeszcie.

42 Konwencja o cyberprzestępczości (ETS nr 185), Raport Wyjaśniający, s. 152 i n.

Przeprowadzone w innych krajach badania pokazują, że oparcie organów ścigania tylko na zabezpieczeniu danych nie powoduje uszczerbku dla potrzeb organów ścigania odnośnie do żądanych danych o ruchu. Jak wynika z ustaleń dokonanych na podstawie dwóch niemieckich analiz, wskaźnik wniosków o udostępnienie danych załatwionych odmownie (tj. odsetek spraw karnych, w których niemieckie organa ścigania zażądały danych o ruchu, ale dane te zostały już wcześniej usunięte przez operatorów telekomunikacyjnych), był bardzo niski w ramach systemu tzw. „szybkiego zamrożenia”[43]. W świetle ujawnianych wyników badań nad zwalczaniem przestępczości można zaryzykować twierdzenie, że retencja danych nie jest niezbędna dla skutecznego ścigania przestępczości.

Ad. c) wymóg proporcjonalności

Zaskarżone przepisy wprowadzają nieproporcjonalne ograniczenie praw i wolności konstytucyjnych, a w szczególności art. 47, art. 49 oraz art. 51 ust. 2 i ust. 4 Konstytucji RP.

Przede wszystkim, zdaniem wnioskodawców wskazać należy, iż nałożenie na operatorów obowiązku zatrzymywania i przechowywania danych telekomunikacyjnych stanowi zaprzeczenie negatywnemu obowiązkowi państwa do powstrzymywania się od zbierania informacji na temat obywateli. Jest to co prawda obowiązek nałożony na operatorów telekomunikacyjnych, jednakże ci dane te udostępniają właściwym organom państwowym na podstawie stosownego upoważnienia lub poprzez wykorzystanie sieci telekomunikacyjnej. Jest to gromadzenie danych na przyszłość, ograniczone czasowo (do 24 miesięcy od daty połączenia) ale tylko wtedy, gdy dane nie zostały zabezpieczone. Na gruncie zaskarżonych przepisów, wyjątek w postaci wkroczenia w prawa i wolności konstytucyjne polegającego na zgromadzeniu danych, prowadzi do podważenia zasady nieingerowania organów państwowych w prywatność jednostki.

Zdaniem wnioskodawców, także kompetencja polegająca na upoważnieniu ww. formacji do pozyskania danych skonstruowana została w sposób zbyt ekstensywny, a przez to niezgodny z Konstytucją. Celem pozyskania danych telekomunikacyjnych funkcjonariusz musi wykazać jedynie dość luźny związek pozyskania z realizacją zadań ustawowych, ściganiem i zapobieganiem przestępczość albo wykrywaniem naruszeń krajowych przepisów celnych. Przy czym ustawodawca

43 Badanie przeprowadzone przez Instytut Maxa Plancka na próbie 467 spraw karnych z lat 2003 - 2004 (zgłoszono w nich 1257 żądań dotyczących danych o ruchu), wskazuje, że wskaźnik żądań danych załatwionych odmownie, wynosił około 4%. Z kolei analiza *Bundeskriminalamt* (Federalne Biuro Śledcze) pokazała, że w 2005 r. w Niemczech było 381 spraw tj. 0,001% (na 6,4 mln sprawy prowadzone w ciągu roku), w których żądano od operatorów danych już niedostępnych.

niejednokrotnie zadania ustawowe sformułował w sposób mało precyzyjny. Ustawodawca nie przewidział także kontroli nad prawidłowością pozyskiwania ww. danych z punktu widzenia przydatności tych informacji. Dlatego też pozyskanie danych odbywa się na podstawie arbitralnej decyzji funkcjonariusza.

Wreszcie, sama czynność pozyskania danych telekomunikacyjnych nie jest poddawana na gruncie zaskarżonych przepisów kontroli ze strony organów wewnętrznych (pewne szczątkowe regulacje zawierają w tym zakresie ustawy o Policji, Straży Granicznej oraz Żandarmerii Wojskowej) i zewnętrznych (z wyjątkiem ministra do spraw finansów w przypadku kontroli skarbowej). W przypadku zaskarżonych przepisów ustawy o ABW oraz AW, ustawy o CBA oraz ustawy o SKW oraz SWW nie ma nawet przepisów dotyczących konieczności niszczenia materiałów nie mających znaczenia dla realizacji ustawowych zadań.

Ustawodawca nie nałożył także na Policję, służby specjalne oraz podmioty wykonujące zadania ochrony bezpieczeństwa państwa obowiązków, które dawałyby jednostce dotkniętej pozyskaniem ww. danych, uprawnień i procedur umożliwiających obronę jej prywatności.
Nie ma w szczególności na gruncie zaskarżonych przepisów obowiązku:

- uzyskania zgody sądu na pozyskanie ww. danych, nawet zgody o charakterze następczym,
- poinformowania jednostki o pozyskaniu ww. danych dotyczących jej osoby, nawet po zakończeniu postępowania,
- niszczenia danych nie mających znaczenia dla potrzeb dochodzenia, wykrywania i ścigania najcięższych przestępstw (np. danych wrażliwych),
- powstrzymywania się od pozyskiwania danych, które nie mogą być wykorzystane dla potrzeb dochodzenia, wykrywania i ścigania najcięższych przestępstw (informacji chronionych na postawie tajemnicy lekarskiej, obrończej, dziennikarskiej itp).

W szczególności ten ostatni obowiązek powinien podlegać wzmożonej ochronie w państwie demokratycznym, którego fundamentami jest zasada prawa do obrony we wszystkich stadiach postępowania karnego (art. 42 ust. 2 Konstytucji RP) oraz wolność słowa i rozpowszechniania informacji (art. 54 ust. 1 Konstytucji RP)[44].

Powyższe uwagi częściowo korespondują ze stanowiskiem Prokuratora Generalnego z dnia 8 listopada 2010 r. w którym wskazał on, iż „*uzyskiwanie tzw. bilingów dziennikarzy i danych identyfikujących stacje BTS w działalności operacyjnej odpowiednich podmiotów informacje te trzeba obecnie uznać za rodzaj kontroli operacyjnej, choć stosowne przepisy nie traktują ich*

44 Por. też J. Kondracki, K. Stępiński, Billingi dziennikarzy tylko za zgodą sądu, http://www.rp.pl/artykul/551208.html.

wyraźnie w ten sposób. Pomimo, że czynności takie wkraczają w sferę wolności i praw obywatelskich, regulujące je ustawy o Policji, ABW i innych organach stosujących kontrolę operacyjną wyłączają potrzebę uzyskania zgody sądu na pozyskanie tych danych. Nowe rozwiązania prawne zostały wprowadzone niedawno ustawą z dnia 24 kwietnia 2009 r. o zmianie ustawy Prawo telekomunikacyjne oraz niektórych ustaw (Dz. U. z 2009 r. Nr 85 poz. 716). Prokurator Generalny uważa za niezbędne wprowadzenie kontroli sądowej (następczej) nad tymi czynnościami"[45].

Jak wskazał Trybunał Konstytucyjny w wyroku z 5 grudnia 2005 r., sygn. K 32/04 w ramach standardów demokratycznego państwa prawa dopuszczalne jest nawet głębokie wkroczenie w sferę prywatności, o ile wkroczenie to opatrzone zostanie należytymi gwarancjami proceduralnymi i w efekcie nie doprowadzi do naruszenia godności osoby poddanej kontroli. Na gruncie zaskarżonych przepisów takiej, właściwej proporcji ustawodawca nie zachował.

W ocenie wnioskodawców, na gruncie zaskarżonych przepisów ustawodawca doprowadził do zbyt ekstensywnego określenia kompetencji Policji, służb specjalnych oraz pozostałych organów odpowiedzialnych za zapewnienie bezpieczeństwa do zbierania ww. danych. Regulacja ta jest zbyt szeroka już w zakresie samego określenia obowiązku operatorów telekomunikacyjnych. W aspekcie zaś pozyskiwania tych danych przez organy państwowe jest ona zbyt luźna na gruncie materialnoprawnym, gdyż pozyskanie tych danych uzależniono właściwie od werbalnego powołania się na wykonywanie ustawowych zadań (sformułowanych często w sposób nieostry46) lub zwalczanie przestępczości. Natomiast luźnej kompetencji materialnoprawnej, nie towarzyszy system gwarancji proceduralnych, bowiem ustawodawca problem ten w ogóle pominął.

Warto przy tej okazji jedynie powtórzyć za ETPCz, iż zakres ingerencji funkcjonujących w demokratycznym państwie służb specjalnych w prawo do prywatności przysługujące obywatelom musi być ściśle ograniczony do zapewnienia bezpieczeństwa państwa47. Co interpretować należy, jako konieczność ścisłego wykazania zasadności użycia określonego środka z uwagi na konkretne, a nie potencjalne niebezpieczeństwo. Nie zachowanie proporcjonalności wyznaczającej miarę zakresu i procedury ingerencji, powoduje, iż wkroczenie organów państwowych może prowadzić do przekreślenia istoty praw i wolności konstytucyjnych, w tym przypadku prawa do prywatności, swobodę komunikowania się i autonomię informacyjną.

45 Stanowisko jest dostępne pod adresem: http://www.pg.gov.pl/index.php?0,0,221.

46 Dobrym przykładem tych wątpliwości jest postanowienie sygnalizacyjne TK z 15 listopada 2010 r., sygn. S 4/10, ZU 2010/8A/88, dotyczące określenia zadań ABW.

47 Wyrok z 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*, skarga 5029/71.

Z tych też powodów, zdaniem wnioskodawców zaskarżone przepisy uznać należy za niezgodne z art. 47, art. 49, art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji RP.

III

W związku z koniecznością stwierdzenia niekonstytucyjności, wnioskodawcy stoją na stanowisku, iż najlepszym rozwiązaniem w przypadku stwierdzenia niezgodności z Konstytucją RP przedmiotowych przepisów byłoby odroczenie o 12 miesięcy wejścia w życie wyroku. Odroczenie pozwoliłoby na dokonanie stosowanych zmian w przepisach ww. ustaw. Zdaniem wnioskodawców termin 12 miesięczny jest wystarczający, aby dokonać odpowiednich zmian.