Warszawa, 19 marca 2012 r.

Trybunał Konstytucyjny
Al. Jana Christiana Szucha 12A
00-918 Warszawa

Sygn. K 23/11

Opinia *amicus curiae* w sprawie wniosku Rzecznik Praw Obywatelskich (sygn. K 23/11)

1. Wprowadzenie

Fundacja PANOPTYKON pragnie przedstawić Wysokiemu Trybunałowi opinię przyjaciela sądu ze względu na doniosłość problematyki objętej wnioskiem Rzecznik Praw Obywatelskich oraz jej zbieżność z zainteresowaniami oraz działaniami Fundacji.

Fundacja PANOPTYKON powstała w 2009 roku i działa na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego". W naszej działalności zajmujemy się współczesnymi formami kontroli i nadzoru nad społeczeństwem oraz zagrożeniami, jakie się z nimi wiążą, m.in. coraz szerszymi uprawnieniami służb specjalnych.

Fundacja PANOPTYKON podziela argumentację zawartą w obu wnioskach Rzecznik Praw Obywatelskich połączonych i rozpoznawanych pod sygn. K 23/11, jednak ze względu na doświadczenie Fundacji niniejsza opinia ogranicza się do problematyki zawartej we wniosku z 1 sierpnia 2011 r. (pierwotnie zarejestrowanym pod sygn. K 29/11).

Naszym celem jest przedstawienie w niniejszej opinii Wysokiemu Trybunałowi szerszego kontekstu problemu podniesionego przez Rzecznik Praw Obywatelskich. Wniosek Rzecznik zawiera bowiem argumentację bardzo precyzyjnie przedstawiającą niezgodność badanych przepisów z powołanymi wzorcami kontroli, nie naświetla jednak zarówno kontekstu ich uchwalenia, jak i praktyki stosowania.

Wniosek z 1 sierpnia 2011 r. dotyczy:

1) zgodności z art. 49 Konstytucji w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8

Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (dalej: **Konwencja**) przepisów: art. 20c ust. 1 ustawy z 6 kwietnia 1990 r. o Policji[1], art. 10b ust. 1 ustawy z 12 października 1990 r. o Straży Granicznej[2], art. 36b ust. 1 pkt 1 ustawy z 28 września 1991 r. o kontroli skarbowej[3], art. 30 ust. 1 ustawy z 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych[4], art. 28 ust. 1 pkt 1 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[5], art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym[6], art. 32 ust. 1 pkt 1 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[7];

2) zgodności z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP przepisów: art. 36b ust. 5 ustawy z 28 września 1991 r. o kontroli skarbowej, art. 28 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, art. 32 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego **w zakresie**, w jakim przepisy te zezwalając na pozyskiwanie danych telekomunikacyjnych nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenia dla prowadzonego postępowania.

Wskazane powyżej przepisy stanowią w istocie konsekwencję implementowania 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 zmieniająca dyrektywę 2002/58/WE (dalej: **dyrektywa retencyjna**).

Ustawa z 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw[8] (dalej: **ustawa implementująca**), implementująca dyrektywę retencyjną, nałożyła na operatorów telekomunikacyjnych obowiązek zatrzymywania i przechowywania, a następnie udostępniania tzw. danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy – Prawo telekomunikacyjne[9] (dalej: **Prawo telekomunikacyjne**). Przepisy objęte wnioskiem regulują dostęp konkretnych służb do danych.

2. Dyrektywa retencyjna

Podstawowym założeniem dyrektywy retencyjnej jest nałożenie na dostawców obowiązku zatrzymywania danych o połączeniach telekomunikacyjnych oraz zapewnienie dostępu do nich odpowiednim organom w celu wykrywania i ścigania poważnych przestępstw. Dyrektywa retencyjna dotyczy danych, które służą do zidentyfikowania obu stron rozmowy (numery telefonu bądź adresy IP), ale także czasu trwania połączenia czy lokalizacji użytkowników.

[1] Dz. U. z 2007 r. Nr 43, poz. 277 ze zm.
[2] Dz. U. z 2011 r. Nr 116, poz. 675.
[3] Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.
[4] Dz. U. Nr 123, poz. 1353 ze zm.
[5] Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.
[6] Dz. U. Nr 104, poz. 708 ze zm.
[7] Dz. U. Nr 104, poz. 709 ze zm.
[8] Dz. U. Nr 85, poz. 716 ze zm.
[9] Dz. U. Nr 171, poz. 1800 ze zm.

2.1. Nadmierne ograniczenie prywatności

Rozpatrując zagrożenia dla prywatności związane z obligatoryjnych zatrzymywaniem danych telekomunikacyjnych, warto zwrócić uwagę na fakt, że procesy komunikacyjne odbywają się w coraz większym stopniu za pośrednictwem nowych technologii. Oznacza to, że obowiązkowi retencji podlega bardzo szeroki i szczegółowy zakres danych i wszystko wskazuje na to, że z upływem czasu zarówno skala zbieranych danych, jak i ich szczegółowość, będzie jeszcze większa. Już obecnie dane telekomunikacyjne pozwalają na stworzenie szczegółowego obrazu życia prywatnego jednostki zbudowanego z informacji na temat sieci społecznych kontaktów, mapy przemieszczania się i nawyków[10]. Takie dane umożliwiają profilowanie na szeroką skalę, które może być wykorzystywane do podejmowania konkretnych rozstrzygnięć dotyczących obywateli.

Autorzy dyrektywy, biorąc pod uwagę fakt, że dyrektywa wkracza w sferę prywatności, zauważyli, że „artykuł 8 EKPC, zgodnie z wykładnią Europejskiego Trybunału Praw Człowieka, wymaga, by ingerencja organów publicznych w prawo do prywatności spełniała wymogi konieczności i proporcjonalności i w związku z tym służyła konkretnym, wyraźnie określonym i uzasadnionym celom oraz była dokonywana w sposób adekwatny, odpowiedni i nie była nadmierna w stosunku do swojego celu" (pkt 25 uzasadnienia). W związku z tym dyrektywa retencyjna zakłada ograniczenia w zakresie dostępu do danych. Ma być on możliwy jedynie subsydiarnie, w związku z „poważnymi przestępstwami".

Pomimo tych deklarowanych gwarancji dyrektywa retencyjna budzi wiele daleko idących wątpliwości. Zdaniem Petera Hustinxa[11]: „dyrektywa jest bez wątpienia najbardziej ingerującym w prywatność narzędziem, jakie zostało wdrożone w Unii Europejskiej ze względu na skalę zbierania danych oraz liczbę osób, których dotyczy"[12]. Jego zdaniem retencja danych telekomunikacyjnych wszystkich obywateli UE stanowi ogromną ingerencję w prywatność.

Poważne zastrzeżenia podnosiły również inne podmioty zajmujące się ochroną prywatności na poziomie Unii Europejskiej. Grupa Robocza do spraw ochrony danych ustanowiona na mocy art. 29 dyrektywy 95/46/WE (dalej: **Grupa Robocza**) w Opinii 9/2004[13] podniosła, że rutynowe zbieranie i przechowywanie wszystkich danych powoduje, że wyjątek – zbieranie informacji o obywatelach – staje się regułą. Dyrektywa retencyjna dotyczy bowiem wszystkich osób, które korzystają z komunikacji elektronicznej. Grupa Robocza wskazuje, że „nie wszystko, co może okazać się przydatne dla organów ścigania, jest pożądane i może być uznane za konieczne w społeczeństwie demokratycznym". Zdaniem Grupy Roboczej dyrektywa nie zawiera żadnych przekonywujących argumentów, że zatrzymywanie danych o ruchu na tak dużą skalę jest jedynym możliwym rozwiązaniem problemu przestępczości oraz bezpieczeństwa narodowego.

---

[10] Nowe możliwości unaocznia przypadek Maltego Spitza – niemieckiego polityka Partii Zielonych. Na drodze sądowej udało mu się uzyskać nakaz udostępnienia przez operatora telekomunikacyjnego wszystkich danych związanych z używaniem jego prywatnego telefonu komórkowego. Okazało się, że polityk otrzymał w sumie od firmy telekomunikacyjnej 35 831 informacji zgromadzonych w ciągu poprzedzających 6 miesięcy. Obok historii połączeń, czy wykazu wiadomości tekstowych znalazły się tam również dane geolokalizacyjne. Informatycy jednej z niemieckich gazet powiązali otrzymane informacje i stworzyli interaktywną mapę, dzięki której można prześledzić życie polityka (mapa dostępna jest pod adresem: http://www.zeit.de/datenschutz/malte-spitz-data-retention).

[11] Konferencja „Taking on the Data Retention Directive", Bruksela, 3 grudnia 2010 r.

[12] Tłum. własne („The Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the numer of people it affects").

[13] Opinia dostępna pod adresem:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf.

2.2. Orzeczenia sądów konstytucyjnych w innych krajach Unii Europejskiej

Omawiając wątpliwości dotyczące dyrektywy warto zwrócić uwagę na orzecznictwo sądów konstytucyjnych niektórych krajów członkowskich UE dotyczące implementacji dyrektywy retencyjnej.

Najbardziej kategoryczną opinię w tej kwestii wyraził rumuński Sąd Konstytucyjny (decyzja nr 1258 z 8 października 2009 r.). Uznał, że zasada prewencyjnego gromadzenia danych o obywatelach godzi w domniemanie niewinności i jest sprzeczna z prawem do prywatności i wolności wypowiedzi. Według opinii tego sądu, ingerencja w prawa podstawowe może być dopuszczalna tylko wtedy, gdy jest realizowana zgodnie z pewnymi regułami oraz gdy wiąże się z odpowiednimi i wystarczającymi zabezpieczeniami przed potencjalnie arbitralnym działaniem państwa. Rezultatem orzeczenia było uchylenie przepisów, które wdrażały do prawa rumuńskiego dyrektywę retencyjną.

Niemiecki Federalny Sąd Konstytucyjny orzekł (11 marca 2010 r., sygn. 1 BvR 256/08), iż retencja danych telekomunikacyjnych stanowi poważne ograniczenie prawa do prywatności, powinna być zatem dopuszczalna wyłącznie w ściśle określonych okolicznościach. Podkreślił również, że tylko okres zatrzymywania danych wynoszący 6 miesięcy może zostać uznany za proporcjonalny. W wyniku tego wyroku zostały uchylone przepisy wdrażające dyrektywę retencyjną do prawa niemieckiego.

Również Czeski Trybunał Konstytucyjny (wyrok z 22 marca 2011 r. w sprawie ustawy nr 127/2005 i dekretu nr 485/2005) zakwestionował krajowe przepisy implementujące dyrektywę retencyjną, jako niedostatecznie jasne i precyzyjne (zwłaszcza biorąc pod uwagę fakt, iż stanowią one ingerencję w sferę praw podstawowych), co w konsekwencji doprowadziło do ich uchylenia. Zdaniem Trybunału skala i zakres obowiązku zatrzymywania danych były zbyt szerokie w odniesieniu do celowości tych działań, a przepisy nie wyposażały indywidualnych obywateli w dostateczne gwarancje i zabezpieczenia przed potencjalnymi nadużyciami ze strony organów publicznych.

Przepisy implementujące dyrektywę retencyjną zostały uchylone także w Bułgarii, decyzją Najwyższego Sądu Administracyjnego (nr 13627 z 11 grudnia 2008 r.). Stwierdzono w niej, iż regulacje te nie stwarzają wystarczających gwarancji ochrony praw obywatelskich, a dane osobowe powinny być zatrzymywane wyłącznie do działań mających na celu wykrycie poważnych przestępstw lub poszukiwanie zaginionych osób. Ostatecznie Bułgaria ponownie wdrożyła dyrektywę do swojego porządku prawnego.

2.3. Alternatywa dla obowiązku blankietowej retencji danych

Warto w tym miejscu zaznaczyć, że powszechna retencja danych nie jest jedynym rozwiązaniem umożliwiającym dostęp służb do danych telekomunikacyjnych. Inną możliwością jest instytucja tzw. zabezpieczenia danych. Rozwiązanie to zostało przyjęte w art. 16 Konwencji Rady Europy o cyberprzestępczości z 2001 r. Zgodnie z jej art. 16 właściwe organy mają możliwość nakazania niezwłocznego zabezpieczenia danych informatycznych, gdy istnieją podstawy do tego, by sądzić, że dane te są podatne na ryzyko utraty. Zamrożenie dokonywane jest natychmiastowo, co skutecznie zapobiega utracie cennych informacji. Aby jednak uzyskać dostęp do zamrożonych danych, potrzebna jest zgoda sądu.

Stosowanie takiego rozwiązania zamiast powszechnej retencji danych znacznie zwiększyłoby poziom ochrony praw i wolności, bez dużego uszczerbku dla sprawności działania organów

ścigania. Model „zabezpieczenia danych" stosowany jest z powodzeniem w Niemczech. Ocenę skuteczności tego systemu przeprowadzoną przez Instytut Maxa Plancka opisał szczegółowo prof. Andrzej Adamski w analizie „Retention of telecommunication data in Poland: does the legal regulation pass the proportionality test?". Wskazane w badaniu statystyki dowodzą, że zabezpieczenie danych może być realną alternatywą dla reżimu retencji danych. Mechanizm ten pozwala na realizację niemal w całości potrzeb organów ścigania.

3. Implementacja dyrektywy retencyjnej

Pomimo wskazanych wyżej wątpliwości w Polsce dyrektywa retencyjna implementowana została ustawą z 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw. Ustawa implementująca wprowadziła do Prawa telekomunikacyjnego art. 180a i 180c, które przewidują obowiązek zatrzymywania i przechowywania przez operatorów, a następnie udostępniania danych telekomunikacyjnych. Drugą częścią implementacji były zmiany w tzw. ustawach kompetencyjnych, które regulują działanie konkretnych służb. Przepisy te, umożliwiające służbom dostęp do danych są objęte wnioskiem Rzecznik Praw Obywatelskich z 1 sierpnia 2011 r.

3.1. Zastrzeżenia dotyczące sposobu implementacji dyrektywy retencyjnej do polskiego porządku prawnego

Ustawodawca, wprowadzając do krajowego porządku prawnego dyrektywę retencyjną winien uwzględnić wymogi wynikające z art. 8 EKPC i tym samym wprowadzić odpowiednie zabezpieczenia przed nadmierną ingerencję w prywatność. Grupa Robocza w opinii nr 3/2006[14] wskazała na 8 kryteriów, które powinny być brane pod uwagę przy wprowadzaniu dyrektywy. Są to m.in. niezależny (być może sądowy) nadzór nad udostępnianiem danych czy minimalizacja danych podlegających przechowywaniu.

W opinii Fundacji PANOPTYKON sposób implementacji dyrektywy nie spełnia tych kryteriów. Nasze zastrzeżenia budzą w szczególności:

1) wykroczenie przez ustawodawcę poza ramy dyrektywy – wprowadzenie szerszych uprawnień dla służb, niż te, które wynikają z dyrektywy;
2) wadliwość uzasadnienia przyjętych rozwiązań;
3) brak zewnętrznych form kontroli na korzystaniem z danych retencyjnych;
4) brak gwarancji realizacji tajemnicy zawodowej: lekarskiej, adwokackiej, notarialnej lub dziennikarskiej, których zniesienie jest możliwe tylko w ściśle określonych przypadkach;
5) brak obowiązku niszczenia zbędnych danych w przypadku niektórych służb.

Ponieważ zarzuty zasygnalizowane w punktach 3-5 są szczegółowo omawiane we wniosku Rzecznik Praw Obywatelskich, zdecydowaliśmy się rozwinąć jedynie zastrzeżenia, o których mowa w dwóch pierwszych punktach.

[14] Opinia nr 3/2006 przyjęta dnia 25 marca 2006 r. w sprawie dyrektywy Parlamentu Europejskiego i Rady nr 2006/24/WE 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, przyjętej przez Radę dnia 21 lutego 2006 r.

Ad. 1) Dyrektywa retencyjna w art. 1 ust. 1 określa, że jej celem jest zbliżenie przepisów państw członkowskich w zakresie dostępności danych „do celu dochodzenia, wykrywania i ścigania **poważnych przestępstw**, określonych w ustawodawstwie każdego państwa członkowskiego". Już to rozwiązanie budzi wątpliwości ze względu na swoją niedookreśloność. Tymczasem przepisy objęte wnioskiem RPO pozwalają na znacznie szerszy dostęp. Policja dla przykładu może sięgać po dane telekomunikacyjne „w celu zapobiegania lub wykrywania przestępstw" (art. 20c ustawy o Policji), a CBA czy ABW – w zakresie realizacji ustawowych zadań. Zwłaszcza w kontekście Policji stanowi to znaczne poszerzenie kompetencji służby względem wymogu dyrektywy.

Ad. 2) Uzasadnienie ustawy implementującej nie wskazuje, dlaczego niezbędne jest wprowadzenie tak daleko idącej ingerencji w prawa jednostki. W szczególności nie zawiera ono wskazania przyczyn rozszerzenia zakresu przestępstw, w których możliwy jest dostęp do danych telekomunikacyjnych (nie tylko poważne przestępstwa). Uzasadnienie wyboru najdłuższego możliwego okresu przechowywania danych przez operatorów (dwa lata) sprowadza się do stwierdzenia, że Polska może być wykorzystywana przez ugrupowania terrorystyczne jako „zaplecze logistyczne lub punkt tranzytowy". Wynika to, zdaniem autorów uzasadnienia, z „położenia geograficznego Polski, na szlakach wschód-zachód i północ-południe". Konieczność zastosowania powszechnej retencji danych telekomunikacyjnych ma wynikać również z ryzyka utworzenia szlaku przemytu heroiny za pośrednictwem żołnierzy służących w Afganistanie. „W sytuacji uczestnictwa polskich żołnierzy w przemycie narkotyków mogłaby zostać zagrożona sojusznicza wiarygodność Polski. Polscy żołnierze pomagaliby bowiem pośrednio, nie wiedząc o tym, finansować działalność al-Kaidy oraz talibów". W naszej ocenie takie wyjaśnienia są daleko niewystarczające – okoliczności te, nie poparte żadnymi dowodami, stanowią raczej przykład zaostrzania przepisów ze względu na niedookreśloną „wojnę z terroryzmem", niż rzetelnej pracy legislacyjnej.

Jak wskazaliśmy wyżej, istnieje alternatywna (mniej inwazyjna) metoda wykorzystywania danych telekomunikacyjnych w celu walki z poważnymi przestępstwami. Ustawodawca winien wytłumaczyć w uzasadnieniu projektu, dlaczego zdecydował się nałożyć na wszystkich operatorów obowiązek powszechnej retencji, rezygnując przy tym z modelu „zabezpieczenia danych".

3.2. Wniosek grupy posłów

Przyjęcie konstrukcji powszechnej retencji danych było przedmiotem wniosku grupy posłów na Sejm z 28 stycznia 2011 r. W sprawie o sygn. K 2/11 podniesiono m.in. niezgodność art. 180a i 180c Prawa telekomunikacyjnego z art. 2, art. 47, art. 49, art. 51 ust. 2 i ust. 4 w związku z art. 31 ust. 3 Konstytucji RP. Trybunał Konstytucyjny, postanowieniem z 30 listopada 2011 r. (sygn. K 2/11), umorzył postępowanie w sprawie ze względu na niedopuszczalność orzekania spowodowaną zakończeniem kadencji Sejmu. Należy jednak zwrócić uwagę na argumentację przedstawioną we wniosku.

Zdaniem grupy posłów w zakresie art. 180a i 180c w związku z przepisami ustaw kompetencyjnych ustawodawca dopuścił się pominięcia legislacyjnego w sferze gwarancji proceduralnych i instytucjonalnych, dotyczących ochrony przed arbitralnością decyzji stosownych służb w zakresie pozyskiwania i przechowywania informacji. Wnioskodawcy zwrócili uwagę m.in. na brak konieczności informowania jednostki o pozyskiwaniu dotyczących jej danych telekomunikacyjnych, nawet po zakończeniu postępowania, czy uzyskania zgody sądu

na pozyskanie tych danych. Wniosek został poparty przez Prokuratora Generalnego, który wniósł o stwierdzenie niekonstytucyjności wszystkich przepisów objętych wnioskiem[15].

3.3. Wniosek Rzecznik Praw Obywatelskich

Fundacja PANOPTYKON w pełni podziela stanowisko przedstawione we wniosku przez Rzecznik Praw Obywatelskich. Nie chcąc powtarzać zaprezentowanej w nim argumentacji, pragniemy jedynie wskazać, że minimalnym wymogiem konstytucyjnym względem dopuszczalności sięgania przez służby po dane telekomunikacyjne jest to, by metody te przeszły test „konieczności w demokratycznym państwie prawnym". Dla dopuszczalności przyjętych rozwiązań, jak wskazał Trybunał Konstytucyjny w wyroku z 12 grudnia 2005 r. (sygn. K 32/04), „nie wystarczy zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę".

3.4. Praktyka korzystania z danych retencyjnych

W naszej ocenie mamy do czynienia z problemem bezrefleksyjnego sięgania po dane wszystkich osób znajdujących się w kręgu zainteresowania uprawnionych instytucji. Na skalę problemu wskazują statystyki sporządzane Urząd Komunikacji Elektronicznej na podstawie danych przekazanych przez operatorów. Ze statystyk tych wynika, że w 2009 r. służby, policja i sądy sięgały po dane telekomunikacyjne ponad milion razy, a w 2010 r. – prawie milion czterysta tysięcy. Badanie przeprowadzone przez Sekretarza Kolegium ds. Służb Specjalnych Jacka Cichockiego pokazało, że bardzo trudno ustalić, co kryje się za tymi statystykami. Sądy, prokuratura i policja, które łącznie – jak można oszacować – generują ponad połowę zapytań, odpowiedziały, że nie prowadzą statystyk związanych z pobieraniem danych.

Statystyki pobierania danych telekomunikacyjnych niechlubnie wyróżniają Polskę na tle innych państw Unii Europejskiej, choć pamiętać należy, że ze względu na brak szczegółowych statystyk interpretacji wskazanych statystyk należy dokonywać z dużą dozą ostrożności[16].

3.5. Wdrożenie dyrektywy – Polska na tle innych krajów Unii Europejskiej

Porównanie przepisów dotyczących retencji w krajach członkowskich Unii Europejskiej wskazuje, że polskie prawo pozwala na najszerszy i najmniej ograniczony dostęp do danych telekomunikacyjnych. W 22 państwach okres przechowywania danych trwa rok albo krócej. Ponadto w większości Państw ograniczono możliwość dostępu do danych retencyjnych jedynie w związku z poważnymi przestępstwami. Za takie uznane zostały albo enumeratywnie wyliczone przestępstwa (np. w Portugalii wskazano m.in. na terroryzm, przestępczość zorganizowaną, porwania dla okupu) bądź w przypadku których zagrożenie karą przekracza określoną wysokość (np. w Irlandii i Hiszpanii – 5 lat, w Finlandii – 4). W niektórych krajach wprowadzono wymóg subsydiarności – w Portugalii i Grecji dostęp do danych jest możliwy, jeśli

[15] Stanowisko Prokuratora Generalnego z 5 lipca 2011 r., dostępne pod adresem: http://157.25.47.5/sprawa/sprawa_pobierz_plik.asp?plik=F-167232394/K_2_11_PG_2011_07_05.pdf&syg=K%202/11.

[16] Report form the Commision to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Bruksela, 18 kwietnia 2011 r. (http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf).

uzyskanie dowodów w inny sposób byłoby niemożliwe lub bardzo trudne. W wielu państwach wprowadzono również niezależną kontrolę nad działaniami służb[17].

4. Podsumowanie

Fundacja PANOPTYKON pragnie podkreślić, że przepisy objęte wnioskiem Rzecznik Praw Obywatelskich stanowią jedynie element wprowadzonego w związku z dyrektywą retencyjną reżimu retencji danych. Naszym zdaniem zbieranie na przyszłość danych telekomunikacyjnych o aktywności wszystkich obywateli jest niezgodne z konstytucyjną zasadą ochrony prywatności i autonomii informacyjnej jednostki. Liczymy, że opinia Fundacji wzmocni argumenty przedstawione przez Rzecznik Praw Obywatelskich.

W imieniu Fundacji PANOPTYKON

Małgorzata Szumańska
Członkini Zarządu

[17] Por. Raport Kolegium do spraw służb specjalnych dotyczący retencji danych telekomunikacyjnych wraz z załącznikami, dostępny pod adresem: http://bip.kprm.gov.pl/portal/kpr/69/613/Rapot_dotyczacy_retencji_danych_telekomunikacyjnych.html?search=71039.