

# **Problem retencji danych o ruchu na tle przepisów ustawy - Prawo telekomunikacyjne**

**Andrzej Adamski**

Katedra Prawa Karnego i Polityki Kryminalnej Uniwersytetu Mikołaja  
Kopernika w Toruniu

## 1. Wstęp

Tematem wystąpienia jest instytucja, która od kilku lat wywołuje w Europie gorące dyskusje i rozbieżne oceny co do celowości i zasadności jej wprowadzenia do porządku prawnego demokratycznego państwa. Gromadzenie i archiwizowanie danych o ruchu w sieciach telekomunikacyjnych dla potrzeb organów ścigania i służb specjalnych jest koncepcją kontrowersyjną. Wg jednych - stanowi głęboką ingerencję w sferę praw i wolności obywatelskich, która narusza utrwalone w Europie standardy ochrony praw człowieka. Wg drugich – jest niezbędnym warunkiem bezpieczeństwa publicznego w erze społeczeństwa informacyjnego i globalnego zagrożenia terroryzmem. W opinii trzecich – to kosztowne i nieefektywne narzędzie, którego wprowadzenie może przyczynić się nie tyle do podniesienia poziomu bezpieczeństwa obywateli, co poziomu cen usług telekomunikacyjnych.

W założeniu, retencja danych ma zapewnić policji pełną kontrolę nad wirtualnymi interakcjami użytkowników sieci. Pozwala bowiem, nawet po upływie długiego czasu, dotrzeć do "elektronicznych śladów" popełnionego przestępstwa, którymi mogą okazać się dane ruchowe - generowane w toku normalnej działalności gospodarczej przez operatorów telekomunikacyjnych lub dostawców dostępu do Internetu i zazwyczaj po upływie stosunkowo krótkiego czasu - usuwane z pamięci komputerów. Zatrzymanie danych obliguje dostawców dostępu do Internetu i dostawców usług internetowych do rutynowego rejestrowania i archiwizowania danych ruchowych przechodzących przez ich serwery, ze względu na potencjalną przydatność takich informacji dla

organów zajmujących się ściganiem przestępstw. Jest to więc rozwiązanie, które z różnych powodów budzi obawy zarówno dostawców internetowych (problem kosztów i wizerunku firmy), jak i zastrzeżenia organizacji i instytucji odpowiedzialnych za ochronę danych osobowych (groźba naruszenia poufności danych i możliwość inwigilowania kontaktów międzyludzkich w skali masowej).<sup>1</sup>

Retencja danych, niezależnie od toczących się na jej temat sporów i prowadzonych aktualnie przez Komisję Europejską konsultacji<sup>2</sup> jest instytucją, która zyskała w niektórych krajach uznanie polityków i poparcie parlamentów, a w konsekwencji - status prawny.

W Belgii wprowadzono ją ustawą z 28 listopada 2000 r. o przestępstwach komputerowych, która zobowiązała pod groźbą odpowiedzialności karnej operatorów sieci i dostawców usług telekomunikacyjnych do przechowywania przez okres co najmniej 12 miesięcy danych o połączeniach lokalnych i dokonywanych z obszaru Unii Europejskiej. Obowiązek ten nałożono na wszelkie kategorie operatorów, zarówno sieci publicznych, jak i prywatnych, w tym intranetów poszczególnych instytucji i organizacji, bez względu na typ sieci (kablowe, radiowe, telefonii mobilnej, satelitarnej itd.). Do szeroko zdefiniowanej kategorii „dostawców usług telekomunikacyjnych” zaliczono nie tylko dostawców usług i aplikacji internetowych (dostawcy dostępu, usług informacyjnych, wyszukiwarek, portali, list dyskusyjnych), lecz również

---

<sup>1</sup> Por. na ten temat stanowisko Komitetu Doradczego Unii Europejskiej ds. Ochrony Danych Osobowych i Prywatności wyrażone w dwóch dokumentach : Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, 5085/99EN/Final WP 25, oraz Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, adopted on 22 March 2001, 5001/01/EN/Final WP41.

<sup>2</sup> European Commission, DG INFSO – DG JAI CONSULTATION DOCUMENT ON TRAFFIC DATA RETENTION, Brussels, 30 July 2004, [http://europa.eu.int/information\\_society/topics/ecommm/doc/useful\\_information/library/public\\_consult/data\\_retention/consultation\\_data\\_retention\\_30\\_7\\_04.pdf](http://europa.eu.int/information_society/topics/ecommm/doc/useful_information/library/public_consult/data_retention/consultation_data_retention_30_7_04.pdf)

podmioty świadczące usługi o wartości dodanej, np. w zakresie kryptografii, bankowości internetowej, nie wyłączając właścicieli cyberkawiarni i administratorów anonimowych remailerów.<sup>3</sup>

Retencję danych „komunikacyjnych” przewiduje brytyjska ustawa z 2001 r. o przeciwdziałaniu terroryzmowi, przestępczości i bezpieczeństwie, która upoważniła Ministra Spraw Wewnętrznych do wydania szczegółowych regulacji w tym względzie, w szczególności - zbioru zasad (*code of practice*) dobrowolnego zatrzymywania danych komunikacyjnych przez dostawców usług. Opracowany przez Home Office kodeks praktyki określa rodzaje danych komunikacyjnych, które dzieli na trzy kategorie (dane identyfikujące subskrybentów, dane dotyczące ruchu oraz dane o korzystaniu z usług). Precyzuje też czas przechowywania poszczególnych rodzajów danych komunikacyjnych przez dostawców usług (np. dane dotyczące abonenta i dane o połączeniach telefonicznych – 12 miesięcy, dane dotyczące SMS, EMS, e-mail, logi ISP – 6 miesięcy, logi serwerów proxy – 4 dni).<sup>4</sup>

## 2. Ewolucja regulacji prawnej w Polsce

Równie szczegółowych regulacji w omawianym zakresie polskie prawo nie zawiera. Zamiast jasnych, nie budzących wątpliwości interpretacyjnych przepisów określających „kto?”, „co?” i „w jaki sposób?” ma przechowywać, dysponujemy ogólnymi, nie w pełni spójnymi ze sobą unormowaniami, z których nie łatwo wywieść jednoznaczne odpowiedzi na wyżej postawione pytania.

---

<sup>3</sup> Y. Poulet, The fight against crime and/or the protection of privacy: a thorny debate!, *International Review of Law, Computers & Technology*, July 2004, vol. 18, no. 2, s. 251-273.

<sup>4</sup> Home Office, Retention of Communications Data under Part 11: Anti-Terrorism, Crime & Security Act 2001, Voluntary Code of Practice, <http://www.legislation.hms.gov.uk/si/si2003/draft/5b.pdf>

Źródłem trudności interpretacyjnych jest m.in. metoda wprowadzenia do polskiego prawodawstwa instytucji retencji danych. Nie dokonano tego od razu „frontowymi drzwiami”, tj. w drodze odpowiednich zmian ustawodawczych, lecz wykorzystano w tym celu (z naruszeniem, jak się wydaje, art. 49 Konstytucji RP) akty podustawowe. Genezy omawianej instytucji można szukać w projekcie rozporządzenia Ministerstwa Spraw Wewnętrznych i Administracji z grudnia 2000 r. w sprawie szczegółowych wymagań i sposobu wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego,<sup>5</sup> który przewidywał „ciągłe” monitorowanie użytkowników sieci telekomunikacyjnych, w tym Internetu. Projekt tego rozporządzenia wywołał falę krytyki<sup>6</sup>, w wyniku której MSWiA wycofało się z jego popierania.

Instytucja retencji danych wprowadzona jednak została do systemu prawnego „kuchennymi drzwiami” przez inny resort. Pojawiła się ona w obowiązującym do dziś rozporządzeniu, które wydał Minister Infrastruktury w styczniu 2003 r.<sup>7</sup> Ten akt wykonawczy do nieobowiązującej już ustawy – Prawo telekomunikacyjne z 2000 roku, nakłada na operatorów m.in. obowiązek zapewnienia „uprawnionym podmiotom” dostępu do posiadanych przez operatorów danych „z ostatnich 12 miesięcy” ( § 5 pkt 7). Tym samym, rozporządzenie zobowiązuje operatorów do przechowywania - na potrzeby organów ścigania i bezpieczeństwa publicznego - danych „związanych ze świadczoną usługą” (§ 2 ust. 1 pkt 1 rozporządzenia) przez okres 12 miesięcy, od chwili powstania danych.

---

<sup>5</sup> Zob. [http://www.vagla.pl/projekt\\_mswia.htm](http://www.vagla.pl/projekt_mswia.htm)

<sup>6</sup> Zob. np. stanowisko Stowarzyszenia ISOC Polska w tej sprawie [http://www.isoc.org.pl/2001/rozporzadzenie\\_mswia/uchwala.pl.html](http://www.isoc.org.pl/2001/rozporzadzenie_mswia/uchwala.pl.html)

<sup>7</sup> Rozporządzenie Ministra Infrastruktury z dnia 28 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, (Dz. U. Nr 19, poz. 166), zob. <http://www.abc.com.pl/serwis/du/2003/0166.htm>

Obecnie retencja danych jest instytucją prawną o charakterze ustawowym. Uzyskała ten status na mocy przepisów nowego prawa telekomunikacyjnego. Zgodnie z art. 165 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (dalej: Ustawa), operatorzy publicznych sieci telekomunikacyjnych oraz dostawcy publicznie dostępnych usług telekomunikacyjnych są obowiązani („z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa i porządku publicznego”) do przechowywania przez okres 12 miesięcy przetwarzanych przez te podmioty **danych transmisyjnych** dotyczących abonentów i użytkowników końcowych .

Aktualnie mamy więc do czynienia z sytuacją, w której dwa akty prawne – rozporządzenie i ustawa regulują tę samą instytucję w niejednolity sposób. Zakres tej regulacji - z wyjątkiem okresu retencji danych, który w obu przypadkach wynosi 12 miesięcy – wykazuje bowiem różnice, które dotyczą zarówno rodzajów danych podlegających zatrzymaniu, jak i podmiotów do tego zobowiązanych.

### 3. Przedmiot retencji

Na podstawie rozporządzenia Ministra Infrastruktury, 12-miesięczne zatrzymanie danych przez operatora dotyczy trzech kategorii informacji będących w jego posiadaniu: 1) danych identyfikujących abonentów, użytkowników i zakończenia sieci telekomunikacyjnych, 2) danych dotyczących faktu, okoliczności i rodzaju połączenia oraz prób uzyskania połączenia między określonymi zakończeniami sieci telekomunikacyjnych; 3) danych identyfikujących zakończenia sieci telekomunikacyjnych, między którymi wykonano połączenie, w tym połączenie konferencyjne, oraz

lokalizacje tych zakończeń.<sup>8</sup> Chodzi zatem o informacje stanowiące element tajemnicy telekomunikacyjnej w rozumieniu art. 67 ustawy Prawo telekomunikacyjne z 12 maja 2000 r.

W nowym prawie telekomunikacyjnym definicja ustawowa tajemnicy telekomunikacyjnej (art. 159) jest bardziej syntetyczna i posługuje się pojęciem „danych transmisyjnych”, które można uznać za ekwiwalent znaczeniowy danych o ruchu (*traffic data*) i danych dotyczących lokalizacji (*location data*), czyli pojęć występujących na gruncie wielu europejskich instrumentów prawnych, w szczególności Dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej (dyrektywa o prywatności i komunikacji elektronicznej), definiującej oba te terminy.<sup>9</sup> Definicje te mają charakter abstrakcyjny i nie nadają się do bezpośredniego stosowania bez ich odpowiedniej operacjonalizacji. Z uwagi na potrzeby organów stanowiących i stosujących prawo, w Europie podejmowane są próby tworzenia pragmatycznie zorientowanych definicji „danych o ruchu w sieci”.

Stosując kryterium funkcjonalne, do kategorii danych o ruchu, oprócz tzw. danych bilingowych związanych z usługami telefonicznymi, zalicza się ok. 60 rodzajów danych stanowiących ślady elektroniczne, jakie pozostawiają po sobie, w różnych miejscach sieci, użytkownicy usług telekomunikacyjnych związanych z dostępem do Internetu.<sup>10</sup> Na ogół jest to adres poczty elektronicznej, adres IP komputera włączonego do sieci i wszelkiego typu logi. Niekiedy także dane

---

<sup>8</sup> Zob. § 3 pkt 1 rozporządzenia.

<sup>9</sup> Wg artykułu 2 Dyrektywy: „dane o ruchu” oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi; „dane dotyczące lokalizacji” oznaczają wszelkie dane przetwarzane w sieci łączności elektronicznej wskazujące położenie geograficzne terminala użytkownika publicznie dostępnych usług łączności elektronicznej.

<sup>10</sup> Discussion Paper for Expert’s Meeting on Retention of Traffic Data, 6 November 2001, Annex II: Internet Data Types, [http://europa.eu.int/information\\_society/topics/telecoms/internet/crime/wpapnov/index\\_en.htm](http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index_en.htm)

nawigacyjne (ang. *navigation data*), takie jak URL (*Unique Resource Locator*) odwiedzanych stron internetowych, oraz tzw. dane lokalizacyjne (ang. *location data*), które pozwalają określić współrzędne geograficzne mobilnego terminalu, jakim jest telefon komórkowy.<sup>11</sup>

Typologie danych stanowiących potencjalny trop cyberprzestępcy bywają bardzo rozbudowane i chociaż opierają się na różnych założeniach metodologicznych często nawiązują do architektury sieci i protokołów komunikacyjnych TCP/IP. Jedną z klasyfikacji - szczególnie użyteczną z punktu widzenia organów ścigania, dzieli dane dotyczące aktywności sieciowej użytkowników Internetu na trzy podstawowe grupy : dane zawierające treść (*content*), dane o ruchu (*traffic*) i dane o dostępie (*access*). Przykładowo, wspomniane wyżej dane nawigacyjne (*URLs*) oraz nagłówki wiadomości przesyłanych pocztą elektroniczną zaliczane są do kategorii danych zawierających treść ze względu na znajdujące się w nich informacje pochodzące od nadawcy e-maila lub nawigującego po sieci internauty. Logi serwera WWW oraz dane adresowe e-mail (logi SMTP i POP 3), to wg wspomnianej typologii - klasyczne dane o ruchu w sieci, natomiast adresy IP i logi RADIUS zaliczane są do danych dostępowych.<sup>12</sup>

W literaturze spotkać się można z opinią, że cechą większości prawnych definicji danych o ruchu jest brak niezbędnej w tym przypadku precyzji.<sup>13</sup> Uwagę tę można również odnieść do prawa polskiego, które nawet na poziomie

---

<sup>11</sup> Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in electronic communications sector of 12 July 2000 COM (2000), adopted on 2<sup>nd</sup> November 2000.

<sup>12</sup> H.Lamb, Principal Current Data Types, Internet Crime Forum, Data Retention Project Group, March 2003. Zob. też EuroISPA position paper on retention of traffic data, EU Cyber crime Forum, 27 November, <http://cyber-crime-forum.jrc.it>.

<sup>13</sup> C.Goemans, J.Dumortier, Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity (w:) C.Nicoll i in. (red.) Digital Anonymity and the Law. Tensions and Dimensions, The Hague 2003, s. 160.

przepisów wykonawczych nie daje wystarczająco dokładnych wskazówek jakie dane podlegają retencji.

#### 4. Ochrona prawna danych transmisyjnych

Klasyfikacje danych o ruchu mają walory poznawcze także z prawnego punktu widzenia. Pokazują, że nie wszystkie dane przetwarzane dla celów przekazywania komunikatów<sup>14</sup> w sieciach telekomunikacyjnych są generowane automatycznie i mają tym samym charakter czysto techniczny. Część z nich stanowi w istocie przekazy informacji pochodzących od użytkowników. Mimo tego dane o ruchu, które zawierają treść nie podlegają silniejszej ochronie prawnej od danych *stricto* transmisyjnych, tj. generowanych automatycznie przez system.<sup>15</sup> Dane o ruchu są generalnie słabiej chronione pod względem prawnym niż treść indywidualnych komunikatów, mimo iż nie jest to zgodne z orzecznictwem Trybunału Praw Człowieka.<sup>16</sup> Na tle porównawczym, standardy ochrony prawnej tych danych są w Polsce szczególnie niskie na gruncie tzw. „ustaw policyjnych”. Świadczy o tym mało sformalizowany sposób uzyskiwania danych o ruchu od operatorów przez funkcjonariuszy Policji, ABW i innych służb specjalnych. Przekazanie danych transmisyjnych może nastąpić nawet na ustne żądanie uprawnionego funkcjonariusza i w odróżnieniu od zatrzymania np. danych informatycznych jako dowodu przestępstwa lub

---

<sup>14</sup> Wg art. 2 pkt 17 ustawy Prawo telekomunikacyjne, komunikat oznacza każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych; nie obejmuje on informacji przekazanej jako część transmisji radiowych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację.

<sup>15</sup> Tę cechę „danych dotyczących ruchu” eksponuje ich definicja zawarta w Konwencji Rady Europy o cyberprzestępczości: „wszelkie dane przetwarzane elektronicznie, związane z przekazami informacji przesyłanymi przy pomocy systemu teleinformatycznego, które są generowane przez ten system i stanowią element procesu komunikowania się, wskazujący na pochodzenie przekazu informacji, jego przeznaczenie, drogę, godzinę, datę, rozmiar, czas trwania lub rodzaj związanej z nimi usługi” (art. 1 d).

<sup>16</sup> W szczególności z orzeczeniem w sprawie *Malone v. Commissioner for the Metropolitan Police*, zob. np. <http://www.leeds.ac.uk/law/hamlyn/malone-case.htm>

przechwytywania przekazów informacji nie podlega kontroli prokuratora lub sądu.<sup>17</sup>

Trzeba jednak podkreślić, że na gruncie Ustawy dane transmisyjne podlegają ochronie prawnej nie tylko jako element tajemnicy telekomunikacyjnej, lecz także jako dane osobowe. Ocena taka wynika z Dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. o przetwarzaniu danych osobowych i ochronie prywatności w sektorze komunikacji elektronicznej, oraz wzorowanych na tej Dyrektywie przepisów rozdziału 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną<sup>18</sup> (dalej: usude). Kategoria danych transmisyjnych (w rozumieniu prawa telekomunikacyjnego) występuje w usude pod nazwą „danych eksploatacyjnych” (art.18 ust.5) i jest przez tę ustawę *explicite* traktowana jako dane osobowe. Okoliczność ta rodzi określone implikacje prawne (wynikające z ogólnych zasad ochrony danych osobowych) wobec operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych. Podmioty te w ramach reżimu retencji danych transmisyjnych stają się bowiem administratorami danych w rozumieniu art. 7 ust. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ze wszystkimi wynikającymi z tej okoliczności konsekwencjami prawnymi i finansowymi.

Należy dodać, że ustawa o świadczeniu usług drogą elektroniczną zobowiązuje usługodawców jedynie do udzielania informacji o danych eksploatacyjnych organom państwowym na potrzeby prowadzonych przez nie postępowań (art. 18 ust.6). Nie przewiduje natomiast obowiązku przechowywania przez określony czas danych o ruchu przechodzących przez serwery ISP dla potrzeb organów

---

<sup>17</sup> Zob. art. 20c ustawy o Policji i komentarz dotyczący tego przepisu (A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001, s. 94-97.)

<sup>18</sup> Dz. U. Nr 144, poz. 1204.

ścigania. Co więcej, ustawa ta, zgodnie z kanonem prawa europejskiego w dziedzinie ochrony prywatności w sektorze telekomunikacyjnym, w zasadzie zakazuje przetwarzania danych osobowych usługobiorcy po zakończeniu korzystania z usługi (art. 19 ust.1 usude). Przewiduje jednak od tej zasady kilka wyjątków i zezwala na przetwarzanie danych eksploatacyjnych po zakończeniu korzystania z usługi przez usługobiorcę m.in., gdy istnieje ku temu podstawa w odrębnej ustawie (art. 19 ust. pkt 4 usude). Czy i w jakim zakresie art. 165 prawa telekomunikacyjnego stanowi taką podstawę jest jednak kwestią otwartą. W kontekście unormowań zawartych w obu wspomnianych wyżej ustawach nie jest bynajmniej oczywiste „na kim” spoczywają obowiązki wynikające z art. 165 Ustawy. Można zastanawiać się nad tym, czy występujące w tym przepisie pojęcie „dostawcy publicznie dostępnych usług telekomunikacyjnych” jest równie pojemne i rozciągliwe jak jego odpowiednik w prawie belgijskim?

##### 5. Podmioty zobowiązane do retencji danych

Wątpliwości interpretacyjne biorą się stąd, że analizowane pojęcie nie zostało należycie zdefiniowane w Ustawie, nie wspominając już o rozporządzeniu Ministra Infrastruktury, które posługuje się pojęciem „operator”. Z treści art. 2 pkt 27 Ustawy wynika, że „dostawcą usług” jest „przedsiębiorca telekomunikacyjny, uprawniony do świadczenia usług telekomunikacyjnych”. Kluczowe znaczenie dla wykładni terminu „dostawca usług” ma zatem pojęcie „usługi telekomunikacyjnej”. Niestety, jej definicja nie jest szczególnie jasna. Odnosny przepis stwierdza, że jest nią „usługa polegająca **głównie** – (podkr. AA) na przekazywaniu sygnałów w sieci telekomunikacyjnej”. Jednocześnie wspomniany przepis eliminuje z zakresu usługi telekomunikacyjnej usługę

poczty elektronicznej.<sup>19</sup> W tym stanie rzeczy wykładnia językowo-logiczna tego przepisu prowadzić może do następujących wniosków. Po pierwsze - na dostawcy usługi poczty elektronicznej nie ciąży obowiązek retencji danych transmisyjnych, o jakim mowa w art. 165 Ustawy, gdyż nie jest on dostawcą usługi telekomunikacyjnej. Po drugie - z obowiązku retencji danych zwolniony jest również dostawca usługi hostingu, który nie przekazuje sygnałów w sieci telekomunikacyjnej, lecz przechowuje dane dostarczone przez usługobiorców. Po trzecie – nie są zobowiązane do retencji danych także inne podmioty świadczące usługi drogą elektroniczną; istota tych usług polega bowiem na wysyłaniu i odbieraniu danych za pomocą systemów teleinformatycznych<sup>20</sup> (warstwa aplikacji), nie zaś na przekazywaniu sygnałów w sieci telekomunikacyjnej (warstwa transportowa).

Jeżeli przesłanki, na których opiera się powyższe rozumowanie są trafne, to można stwierdzić, że przedsiębiorcami telekomunikacyjnymi, na których spoczywa obowiązek retencji danych transmisyjnych są oprócz operatorów publicznej sieci telekomunikacyjnej<sup>21</sup> dostawcy publicznie dostępnych usług telekomunikacyjnych, których świadczenie wymaga zgłoszenia. Chodzi więc o dostawców: usług telefonicznych, transmisji danych oraz dostępu do sieci Internet.<sup>22</sup>

Jak wynika z przeprowadzonej analizy, polski model prawny retencji danych różni się od belgijskiego głównie tym, że nie obejmuje wszystkich podmiotów zaangażowanych w szeroko pojętą działalność telekomunikacyjną, włączając w to wszelkie kategorie dostawców usług i aplikacji internetowych. Uzasadnia to oczywiście pytanie, czy model ten jest racjonalny? Kwestia ta wiąże się jednak z

---

<sup>19</sup> Art. 2 pkt 48 ustawy – Prawo telekomunikacyjne: **usługa telekomunikacyjna** - usługa polegająca głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej; nie stanowi tej usługi usługa poczty elektronicznej.

<sup>20</sup> Zob. art. 2 pkt 4 oraz art.3 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

<sup>21</sup> Wykaz operatorów publicznych sieci telekomunikacyjnych - zob.

<http://www.urtip.gov.pl/gallery/bip/12/128.doc>

<sup>22</sup> Odnośnie rejestru przedsiębiorców telekomunikacyjnych zob. <http://www.urtip.gov.pl/gallery/bip/13/133.doc>

zasadniczym problem – racjonalności instytucji retencji danych w ogóle. Szczegółowe omówienie tego zagadnienia wykracza poza ramy niniejszego referatu. Spróbujmy zatem ograniczyć się do zasygnalizowania najważniejszych argumentów podnoszonych w toczącej się obecnie w Europie dyskusji na ten temat.

## 6. Standard unijny?

Impulsem do dyskusji i ogłoszonych przez Komisję Europejską konsultacji na temat retencji danych jest projekt decyzji ramowej w tej sprawie, który został zgłoszony przez cztery kraje członkowskie (Francję, Irlandię, Szwecję i Wielką Brytanię) 28 kwietnia 2004 r.<sup>23</sup>

W konsultacjach wzięli udział głównie przedstawiciele sektora gospodarczego ICT (operatorzy telekomunikacyjni, ISP) oraz organizacje pozarządowe zajmujące się ochroną praw i wolności obywatelskich.<sup>24</sup> Wyniki konsultacji, które przedstawiono na otwartym seminarium w Brukseli 21 września 2004 r. są dość jednoznaczne. Większość z 65 otrzymanych odpowiedzi negatywnie ocenia instytucję retencji danych i zajmuje krytyczne stanowisko wobec projektu decyzji ramowej z 28 kwietnia 2004 r.<sup>25</sup>

Podstawowe zastrzeżenia mają charakter prawny. Argumenty techniczne i finansowe przeciwko proponowanym rozwiązaniom są jednak nie mniej istotne.

### a. Zastrzeżenia prawne

---

<sup>23</sup> Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism , <http://www.ispai.ie/fd.pdf>

<sup>24</sup> Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention, 15 September 2004, <http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html>

<sup>25</sup> Results Commission consultation on data retention (21.09.2004), <http://www.edri.org/cgi-bin/index?id=000100000170>

Gromadzenie i przechowywanie danych stanowiących „prawdziwą kopalnię wiedzy o życiu prywatnym i zawodowym użytkowników sieci telekomunikacyjnych”<sup>26</sup> dla potrzeb ewentualnych postępowań karnych jest uznawane za nielegalne. Narusza bowiem zasadę proporcjonalności ingerencji państwa w prawa i wolności obywatelskie, gwarantowane przez Europejską Konwencję Praw Człowieka (art. 8) oraz ustawy zasadnicze większości krajów europejskich, w tym Konstytucję RP (art. 31 ust. 3). Trzeba w związku z tym przypomnieć, że na naruszenie zasady proporcjonalności - w odniesieniu do nadmiernego gromadzenia informacji o obywatelach - powołuje się uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 20 listopada 2002 r., który za niezgodne z konstytucją uznał „nałożenie na obywateli powszechnego obowiązku ujawniania majątku w deklaracjach podatkowych” przez ustawę z dnia 26 września 2002 r. o jednorazowym opodatkowaniu nieujawnionego dochodu oraz o zmianie ustawy – Ordynacja podatkowa i ustawy – Kodeks karny skarbowy (zawetowaną przez Prezydenta RP i uchyloną następnie wspomnianym Wyrokiem Trybunału Konstytucyjnego).

Alternatywnym dla retencji danych i zgodnym z zasadą proporcjonalności rozwiązaniem, które uwzględni m.in. Konwencja Rady Europy o cyberprzestępczości oraz znowelizowane niedawno przepisy kodeksu postępowania karnego, jest instytucja „zabezpieczenia danych” (*preservation of data*).

Dotyczy ona danych, które aktualnie znajdują się w dyspozycji operatora sieci lub dostawcy usług (tzw. dane historyczne) i polega „zamrożeniu” na żądanie uprawnionego organu przez administratora systemu (w tym IAP i ISP) określonych danych, znajdujących się w posiadaniu lub pod kontrolą osoby,

---

<sup>26</sup> Zob. A. Adamski, Obywatel bezpieczny, ale przezroczysty. Nowelizacja ustawy o policji a ochrona danych osobowych, „*Rzeczpospolita*” z dnia 18.08.2000 r.

której taki nakaz dotyczy. Zakres stosowania omawianego środka jest ograniczony do postępowań toczących się w konkretnych sprawach i określa górną granicę czasu zabezpieczenia danych na nie więcej niż 90 dni, z możliwością przedłużenia tego okresu w uzasadnionych przypadkach. „Zabezpieczenie danych” jest środkiem mniej dolegliwym finansowo i organizacyjnie dla dostawców internetowych niż „zatrzymanie danych”. Stanowi też mniejsze zagrożenie dla praw i wolności obywatelskich niż alternatywny z omawianych środków. Z obu tych względów „zabezpieczenie danych” jest uznawane za wyraz racjonalnego kompromisu pomiędzy interesem wymiaru sprawiedliwości a poszanowaniem praw i wolności obywatelskich nie tylko w oficjalnych dokumentach Rady Europy, lecz także stowarzyszeń operatorów telekomunikacyjnych.<sup>27</sup>

#### b. Wątpliwości praktyczne

Operatorzy, w odróżnieniu od „lobby bezpieczeństwa publicznego”, dysponują na poparcie zajmowanego w tej sprawie stanowiska przekonującymi dowodami, z których wynika, że kosztowe przechowywanie gigantycznych ilości danych o ruchu w sieci przez okres 12, 36, czy nawet 60 miesięcy (Włochy) jest w gruncie rzeczy niepotrzebne policji. W praktyce nie zdarza się bowiem, by policja żądała od operatorów danych za okres dłuższy niż trzy miesiące. Nawet po zamachu bombowym na metro w Madrycie w marcu 2004 r., policja zwróciła się do operatora telekomunikacyjnego o dostarczenie danych za okres grudzień 2003 – marzec 2004.<sup>28</sup>

Zwraca się również uwagę, że instytucja retencji danych, oficjalnie uzasadniana potrzebą skutecznej walki z przestępczością zorganizowaną i terroryzmem nie

---

<sup>27</sup> ETNO Reflection Document on Traffic Data retention , September 2004

[http://www.etno.be/upload/down\\_files/8962/RD198%20DP%20traffic%20data%20retention.doc](http://www.etno.be/upload/down_files/8962/RD198%20DP%20traffic%20data%20retention.doc)

<sup>28</sup> Results Commission consultation on data retention (21.09.2004), <http://www.edri.org/cgi-bin/index?id=000100000170>

będzie spełniać pokładanych w niej oczekiwań. Ze względu chociażby na właściwości technologii trudno zakładać, że zatrzymanie danych będzie stanowić jakiś poważny problem dla osób zaangażowanych w poważną działalność przestępczą lub terroryzm. Zarówno bowiem systemy wymiany plików (p2p) jak i poczta webowa, używana jako „skrzynka kontaktowa”, pozwalają obejść system kontroli danych o ruchu, co w konsekwencji niweczy cel tej instytucji.

Wszystko to sprawia, że w chwili obecnej trudno prognozować jakie będą dalsze losy instytucji retencji danych oraz związanego z nią projektu decyzji ramowej z 28 kwietnia 2004 r. Można natomiast stwierdzić, że niezależnie od tego, czy zatrzymanie danych stanie się standardem unijnym czy nie, aktualna polska regulacja prawna w tym względzie wymaga gruntownych zmian. Odbiega ona bowiem wyraźnie od wszelkich standardów.