Retencja danych telekomunikacyjnych. Problemy i perspektywy

Stanisław Piątek

Wydział Zarządzania Uniwersytetu Warszawskiego

Ograniczenia tajemnicy komunikowania

Retencja danych
Art. 180a-c PT

Kontrola treści przekazów telekomunikacyjnych
Art. 179 ust. 3 PT

Operacyjny dostęp do treści przekazów telekomunikacyjnych i danych towarzyszących bez podstawy prawnej

Dostęp do danych towarzyszących usłudze telekomunikacyjnej
Art. 180d PT

Dostęp do danych eksploatacyjnych dostawców usług internetowych
Art. 18 ust. 6 UŚUDE

Charakterystyka retencji danych (1)

- **Obowiązek retencji danych**: zatrzymywanie, przechowywanie i udostępnianie tzw. uprawnionym podmiotom danych generowanych przy świadczeniu usług telekomunikacyjnych
- **Gromadzenie i przechowywanie danych:** uregulowane w Prawie telekomunikacyjnym, **udostępnianie –** uregulowane w przepisach o służbach policyjnych i specjalnych, Kodeksie postępowania karnego
- **Usługi objęte retencją**: telefonia stacjonarna i ruchoma, dostęp do Internetu, poczta elektroniczna i telefonia internetowa
- **Rodzaje danych**: dane służące do identyfikacji urządzenia lub użytkownika wywołującego i wywoływanego, daty, godziny, czasu trwania i rodzaju połączenia, lokalizacji urządzenia
- **Okres przechowania** – 12 miesięcy
- **Koszt** – obciąża w całości przedsiębiorcę telekomunikacyjnego

Charakterystyka retencji danych (2)

- **Podmioty zobowiązane**: operatorzy publicznych sieci telekomunikacyjnych i dostawcy publicznie dostępnych usług telekomunikacyjnych
  - problem sieci i usług publicznych
- **Podmioty uprawnione**: Policja, ABW, AW, CBA, SG, SKW, ŻW, Służba Celna, Wywiad Skarbowy, sądy i prokuratura
  - problem żądań innych podmiotów
- **Sposób udostępniania**: pisemnie lub ustnie uprawnionemu funkcjonariuszowi, drogą telekomunikacyjną

Problem legalności retencji

- Przepisy PT o retencji implementują tzw. dyrektywę retencyjną UE z 2006 r.
- Wyrok Trybunału Sprawiedliwości z 8.4.2014 potwierdza niezbędność retencji ale jednocześnie uznaje nieważność dyrektywy retencyjnej z powodu:
  - naruszenia wymogu proporcjonalności retencji w odniesieniu do prawa do prywatności i ochrony danych osobowych
  - objęcia retencją wszystkich użytkowników, w tym wykonujących zawody chronione tajemnicą zawodową
  - wykorzystywania danych retencyjnych nie tylko do zapobiegania poważnym przestępstwom
  - braku w dyrektywie procedur dostępu do danych i kontroli nad dostępem
- Wyrok Trybunału Konstytucyjnego z 30.7.2014 stwierdza sprzeczność przepisów o służbach „policyjnych" i „specjalnych" z Konstytucją w zakresie wykorzystywania danych retencyjnych na skutek braku niezależnej, zewnętrznej kontroli dostępu oraz braku obowiązku niszczenia danych niemających znaczenia dla postępowania
  - 18 miesięcy na zmianę przepisów „policyjnych"
- Skutki wyroków dla wykonywania retencji danych
  - prawdopodobieństwo wycofania się Unii Europejskiej z harmonizowania retencji
  - niepewność co do przyszłych zasad gromadzenia i przechowywania danych
  - konieczność zmiany przepisów krajowych dotyczących wykorzystania danych przez służby

Podmiotowe ograniczenia obowiązku retencji danych

- Podmioty udostępniające klientom punkty WiFi umożliwiające nieodpłatny dostęp do Internetu (w placówkach handlowych, usługowych, hotelach itp.)
  - niezarobkowe zapewnianie dostępu nie jest objęte obowiązkiem retencji (stanowisko MI)
- Podmioty zapewniające usługi dostępowe dla potrzeb „wewnętrznych” (uczelnie, szkoły, itp.)
- Samorządy terytorialne zapewniające dostęp do Internetu bez pobierania opłat (stanowisko Prezesa UKE)
- Przedsiębiorcy tranzytujący ruch telekomunikacyjny
- Przedsiębiorcy dokonujący odsprzedaży usług telekomunikacyjnych – możliwość zawarcia umowy o powierzeniu wykonania zadań związanych z retencją

Granice uprawnień do żądania danych objętych retencją

- Służby policyjne i specjalne – całość danych
- Sądy w sprawach karnych i prokuratura – całość danych
- Służba Celna – całość danych
- Przewodniczący Komisji Nadzoru Finansowego – dane bilingowe i identyfikujące abonenta
- Urząd skarbowy, urząd celny, inspektor kontroli skarbowej – w związku z przestępstwami i wykroczeniami skarbowymi
- Straże gminne / miejskie – brak uprawnień, problem danych identyfikujących abonenta
- Sądy w sprawach o wykroczenia, cywilnych (głównie rozwodowych), pracowniczych – uzyskiwanie danych tylko za zgodą abonenta
- Komornicy

Granice dotyczące udostępniania danych

- Problem tzw. zapytań kaskadowych –
  - są dopuszczalne o ile kolejne „kaskady” oparte są na wyraźnym kryterium wskazanym przez uprawniony organ (np. MSISDN - IMEI – MSISDN dla ustalonych terminali)
  - są niedopuszczalne o ile operator musi samodzielnie przeprowadzić analizę danych w celu ustalenia właściwego kryterium
- Dane o użytkowniku – problem wyłączenia z przepisów o retencji
- Umożliwianie służbom dostępu do danych zachowanych po upływie 12 miesięcy (np. bilingów)
- Problem retencji danych o wykorzystanych usługach internetowych (poczta, portale społecznościowe, wyszukiwarki) – postulat NIK

Koszty retencji danych

- Znaczne koszty inwestycyjne, eksploatacyjne i udzielania odpowiedzi
- Koszty inwestycyjne 0,5 – 5 mln złotych, eksploatacyjne 10-15% kosztów inwestycyjnych rocznie, odpowiedź na zapytanie – ok. 40 złotych
- Całość kosztów ponosi przedsiębiorca
- Bardzo duży zakres wykorzystania danych - ponad połowa zapytań w UE jest realizowana w Polsce
- Brak motywacji po stronie uprawnionych do ograniczania zbędnych zapytań
- Stały i szybki wzrost wolumenu danych - perspektywa Internetu Rzeczy
- Postulaty udziału podmiotów uprawnionych w kosztach inwestycyjnych i wprowadzenia opłaty za udzielenie odpowiedzi

Perspektywy retencji (1)

- Wykonywanie obowiązku retencji w okresie przejściowym:
  - nieważność dyrektywy nie oznacza nieważności przepisów krajowych opartych na dyrektywie
  - wykonywanie obowiązku retencji na dotychczasowych zasadach
  - możliwość ograniczenia danych retencyjnych na skutek żądań abonentów dotyczących usunięcia ich danych (np. adwokatów, dziennikarzy)
  - pożądane interpretacyjne stanowisko regulatora - Prezesa UKE lub Ministra Administracji i Cyfryzacji
- Perspektywy zmian ustawowych
  - zmiana ustaw „policyjnych” w zakresie dotyczącym kontroli
  - nowa dyrektywa lub rozporządzenie UE w sprawach retencji
  - zmiana Prawa telekomunikacyjnego i rozporządzenia o retencji

Perspektywy retencji (2)

- Model kontroli nad dostępem do danych przez służby
  - *ex ante* lub/i *ex post* - *ex post*, z wyjątkiem przypadków tajemnicy zawodowej
  - organ sądowy czy administracyjny – organ niezależny
- Dookreślenie celu korzystania z danych retencyjnych
  - ograniczenie wykorzystania danych do zapobiegania przestępstwom i wykrywania ich sprawców – np. przestępstwa zagrożone karą pozbawienia wolności powyżej 3 lat oraz przestępstw z użyciem środków komunikacji elektronicznej (NIK), wykluczenie celów analitycznych i innych
  - postulat stworzenia katalogu przestępstw uzasadniających dostęp
- Wykluczenie dostępu do danych objętych tajemnicą zawodową – z wyłączeniem najpoważniejszych przypadków
- Zróżnicowanie warunków w zależności od stopnia ingerencji w prywatność:
  - dane identyfikacyjne (imię i nazwisko / numer telefonu)
  - dane o połączeniach
  - dane o lokalizacji

Dziękuję za uwagę

Stanisław Piątek
spiatek@wz.uw.edu.pl