RETENCJA DANYCH TELEKOMUNIKACYJNYCH – NIEROZWIĄZANY PROBLEM

Czym jest „retencja danych"?

Retencja danych telekomunikacyjnych to obowiązkowe, systematyczne gromadzenie i przechowywanie tzw. danych transmisyjnych, czyli informacji o szczegółach wszystkich rodzajów połączeń telekomunikacyjnych w celach związanych z bezpieczeństwem publicznym. Obowiązek wprowadzenia blankietowej retencji danych telekomunikacyjnych wynika z przepisów Unii Europejskiej. W Polsce dane przechowywane są przez operatorów przez dwa lata i udostępniane bezpłatnie (na koszt operatorów) na żądanie wybranych służb oraz sądu i prokuratury.

W praktyce oznacza to, że operatorzy sieci i dostawcy publicznie dostępnych usług telekomunikacyjnych muszą przechowywać wszystkie informacje niezbędne do ustalenia kto, kiedy, gdzie, z kim i w jaki sposób połączył się lub próbował połączyć. W przypadku sieci telefonicznych są to takie dane, jak numer telefonu, czas połączenia czy stacja przekaźnikowa, w zasięgu której znajdował się wykonujący i odbierający połączenie. W przypadku Internetu jest to ok. 60 rodzajach śladów elektronicznych, jakie pozostawiają po sobie użytkownicy w różnych miejscach sieci.

Dyrektywa o retencji: obowiązek blankietowego przechowywania informacji o połączeniach

Dyrektywa 2006/24/WE nałożyła na kraje członkowskie Unii Europejskiej obowiązek zbierania danych na temat wszystkich połączeń telekomunikacyjnych, bez względu na to, czy wobec osoby wykonującej połączenie istnieją jakiekolwiek podejrzenia popełnienia przestępstwa. Przyjęcie rozwiązania, w którym dane gromadzone są niejako „na wszelki wypadek", stawia wszystkich w roli potencjalnych podejrzanych.

Wdrożenia Dyrektywy w Polsce: szeroki i niekontrolowany dostęp do gromadzonych danych

Retencja w wersji zaproponowanej przez Dyrektywę – mimo swojego blankietowego charakteru, zakładającego gromadzenie danych o wszystkich obywatelach – pomyślana była jako środek nadzwyczajny, wykorzystywany w przypadku najgroźniejszych przestępstw, takich jak terroryzm. Polski ustawodawca wdrożył dyrektywę w sposób sprzeczny z tą ideą. Rozwiązania wprowadzone nowelizacją Prawa telekomunikacyjnego z 2009 roku przewidują możliwość wykorzystywania dostępu do danych retencyjnych w celu wykrywania wszystkich przestępstw, a także w ogólnie pojętych celach prewencyjnych. Nie zapewniono przy tym kontroli sądowej ani żadnej innej realnej metody weryfikacji tego, czy przyznane służbom uprawnienie do korzystania z tych danych nie jest nadużywane.

Argumenty przeciwko retencji danych w obecnym kształcie:

I. Nieproporcjonalne ograniczenie prawa do prywatności

- Nie wykazano, że retencja jest środkiem koniecznym dla realizacji celu, jakim jest zapewnienie bezpieczeństwa i porządku publicznego. Doświadczenia innych państw, które nie wprowadziły retencji danych, pokazują, że najpoważniejsze przestępstwa (takie jak terroryzm) można z powodzeniem ścigać za pomocą innych technik operacyjnych, w tym tradycyjnych metod śledczych.
- O ile zbieranie informacji o połączeniach można uzasadnić w przypadku podejrzeń popełnienia przestępstwa, o tyle trudno znaleźć usprawiedliwienie dla rutynowego zbierania informacji o wszystkich obywatelach.
- Ponieważ polskie prawo umożliwia wykorzystywanie tych danych do wykrywania wszystkich przestępstw (a nie tylko tych najcięższych) oraz w ogólnie pojętych celach prewencyjnych, istnieje realne zagrożenie, że ten głęboko ingerujący w prywatność środek jest wykorzystywany w sytuacjach, w których jest to nieadekwatne.
- przechowywanie informacji o połączeniach w przypadku zawodów zaufania publicznego (dziennikarzy, lekarzy, prawników) stwarza poważne ryzyko podważenia zasady poufności w kontaktach profesjonalnych oraz zagrożenie dla tajemnicy korespondencji i ochrony źródeł informacji dziennikarskich.
- Obywatel nie ma żadnej możliwości dotarcia do zbiorów danych retencyjnych i zweryfikowania ich rzetelności.
- Ograniczenia prywatności związane z realizacją retencji danych trudno obronić na gruncie obowiązującego porządku konstytucyjnego. Gromadzenie szczegółowych danych na temat komunikacji wszystkich obywateli uważamy za niezgodne z art. 8 Europejskiej Konwencji Praw Człowieka oraz art. 47, 51 i 31 Konstytucji Rzeczpospolitej Polskiej. Trudno tak daleko idące ograniczenie prawa do prywatności uznać za konieczne w demokratycznym państwie.

II. Realne zagrożenie inwigilacją

- Ze względu na specyfikę telefonii i Internetu, wykorzystywanie danych retencyjnych pozwala na stworzenie szczegółowego obrazu życia prywatnego danej osoby – swoistego „cyfrowego profilu", zbudowanego z wrażliwych informacji na temat sieci jej społecznych kontaktów, mapy przemieszczania się i nawyków.

- Brak precyzyjnych ograniczeń co do tego, w jakich sytuacjach służby mogą korzystać z dostępu do danych retencyjnych, sprawia, że możliwe jest wykorzystywanie informacji o połączeniach telekomunikacyjnych na masową wręcz skalę.
- W praktyce dostęp służb do danych retencyjnych jest bardzo prosty. Są one udostępniane za darmo, również za pomocą sieci telekomunikacyjnej (bez udziału pracowników operatora). Z wypowiedzi przedstawicieli operatorów wynika, że uprawnione podmioty mają zwykle właśnie taki bezpośredni i niekontrolowany dostęp do gromadzonych danych.
- Przepisy zobowiązujące operatorów do przechowywania danych i udostępniania uprawnionym podmiotom są bardzo ogólnikowe, brakuje ustawowych procedur udostępniania danych, a istniejące prawdopodobnie reguły operacyjne są niejawne i realizowane bez kontroli demokratycznej. Wszystkie uprawnione służby mają dostęp do danych retencyjnych bez kontroli sądu i prokuratora. Przekłada się to na potencjalnie wysokie ryzyko nadużyć.
- Z informacji przekazanych Fundacji Panoptykon przez Urząd Komunikacji Elektronicznej wynika, że w samym 2009 roku podmioty uprawnione skierowały do operatorów ponad milion zapytań dotyczących połączeń, co stawia Polskę na pierwszym miejscu wśród krajów Unii Europejskiej. Skala wykorzystywania informacji może poważnie niepokoić, choć bez wiedzy o tym, jakie konkretnie podmioty i w jakich sytuacjach sięgały po te dane, trudno jednoznacznie zinterpretować tę informację.

III. Ograniczona skuteczność w walce z najpoważniejszymi przestępstwami

- Przekonanie o użyteczności danych retencyjnych bazuje na bardzo iluzorycznych założeniach: przekonaniu, że zbieranie jak największej ilości informacji pozwala zachować kontrolę nad otaczającą rzeczywistością i prowadzi do wzrostu bezpieczeństwa. Tymczasem nie przedstawiono żadnych dowodów na to, że w państwach które wprowadziły retencje wzrosła wykrywalność najpoważniejszych przestępstw czy też zmniejszyło się ryzyko ataku terrorystycznego.
- Retencja danych, ze względu na używaną technologię oraz ogromną ilość gromadzonych rutynowo danych, nie może służyć za narzędzie wczesnego wykrywania zagrożeń i zapobiegania przestępstwom.
- Sprawcy najpoważniejszych przestępstw, w przypadku których sięganie po dane retencyjne mogłaby być uzasadnione, na ogół zdają sobie sprawę z konsekwencji gromadzenia danych telekomunikacyjnych i znają sposoby pozwalające uniknąć identyfikacji. Sprawia to, że w praktyce retencję danych najłatwiej wykorzystać nie do walki z przestępczością zorganizowaną czy terroryzmem, ale w stosunku do osób nieświadomych istnienia retencji i niemających podstaw, by sądzić, że mogą się znaleźć się w „kręgu zainteresowania" służb.
- Automatyczne procesy, na których opiera się blankietowa retencja danych nie działają bezbłędnie. Istnieje prawdopodobieństwo, że informacje o powiązaniach i kontaktach jednej osoby mogą zostać przypisane do działań podjętych przez kogoś innego.

IV. Koszty finansowe

- Szacuje się, że retencja danych generuje koszty w wysokości ponad stu milionów złotych rocznie (koszt wdrożenie, utrzymania i bieżącej obsługi odpowiednich systemów). Koszty te pośrednio ponoszą wszyscy obywatele, jako klienci usług telekomunikacyjnych, ponieważ w Polsce koszty retencji są przerzucone na operatorów telekomunikacyjnych (inaczej niż np. w Wielkiej Brytanii, gdzie to podmioty korzystające z retencji ponoszę jej koszty).
- Wysoki koszt retencji i obciążenie nim przedsiębiorców telekomunikacyjnych pozostaje w sprzeczności z celem Dyrektywy, jakim jest usuwanie przeszkód dla wewnętrznego rynku łączności elektronicznej.

Nasza propozycja: co zamiast retencji?

Zabezpieczenie danych – rozwiązanie przewidziane w Konwencji Rady Europy o cyberprzestępczości, polegające na „zamrażaniu" na żądanie uprawnionego organu danych znajdujących w dyspozycji operatorów. Doświadczenia innych krajów wskazują, że jest to narzędzie wystarczające do realizacji celów stawianych przed retencją danych. Jednocześnie jest ono zgodne z zasadą proporcjonalności i – pod warunkiem poddania sądowej kontroli – nie stwarza tak poważnych zagrożeń dla realizacji konstytucyjnych praw i wolności obywateli.

Proponowane przez nas zmiany wymagają nowelizacji Dyrektywy. Obecnie odbywa się jej rewizja i Fundacja Panoptykon aktywnie działa na rzecz jej zmiany. Niemniej jednak w Polsce również należy podejmować działania zmierzające do zmiany obowiązującego stanu prawnego, zwłaszcza że wdrożenie Dyrektywy narusza jej podstawowe założenia i wydaje się sprzeczne z polską Konstytucją. W kilku państwach europejskich wdrożenia dyrektywy retencyjnej zostały zakwestionowane przez sądy konstytucyjne. Między innymi niemiecki trybunał zwrócił uwagę na nieproporcjonalność wprowadzanych do niemieckiego prawa rozwiązań. Uważamy, że również polskie przepisy dotyczące retencji danych powinny zostać zbadane przez Trybunał Konstytucyjny pod kątem zgodności z Konstytucją. Dlatego zwracamy się do Rzecznika Praw Obywatelskich o wystąpienie z odpowiednim wnioskiem.

O Fundacji Panoptykon

Fundacja Panoptykon powstała w kwietniu 2009 r. Jej głównym celem jest działanie na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego" – współczesnych form kontroli i nadzoru nad społeczeństwem. W obszarze zainteresowania Fundacji znajdują się takie zagadnienia jak: powstawanie i rozbudowa baz danych, rozwój monitoringu wizyjnego, retencja danych telekomunikacyjnych, wykorzystywanie technologii biometrycznych, uprawnienia służb specjalnych, techniki nadzoru nad pracownikami, praktyki kontroli przepływu informacji w Internecie.