

Czy w 9 miesięcy uda się ograniczyć dostęp służb do billingów?

22 maja 2015

Przewodniczący senackiej Komisji Praw Człowieka, Praworządności i Petycji, Michał Seweryński na wczorajszym posiedzeniu komisji postawił sprawę jasno: Senat nie będzie dłużej czekał, aż Ministerstwo Spraw Wewnętrznych zaproponuje wdrożenie wyroku Trybunału Konstytucyjnego (TK) i przejmuje inicjatywę. Chodzi o wyrok nakazujący stworzenie niezależnego mechanizmu kontroli nad policją i innymi służbami, kiedy sięgają po nasze dane telekomunikacyjne. Ponad rok temu Senat miał gotowy projekt ustawy, ale zawiesił nad nim prace ze względu na zapowiedzi rządu, że ten podejmie temat. Zostało już tylko dziewięć miesięcy na wdrożenie wyroku, a ustawy jak nie było, tak nie ma. Skąd ten opór materii po stronie rządu? I dlaczego nowe prawo jest tak pilnie potrzebne?

W 2006 r. – po zamachach terrorystycznych w Madrycie i Londynie – Unia Europejska zdecydowała się na radykalny krok: zbieranie „na wszelki wypadek” danych o wszystkich połączeniach telekomunikacyjnych. Tzw. dyrektywa retencyjna została okrzyknięta najbardziej ingerującym w prywatność prawem, jakie kiedykolwiek przyjęto w UE. Trzy lata później polski ustawodawca poszedł jednak jeszcze dalej: policja i służby specjalne dostały swobodny dostęp do billingów, danych o lokalizacji i tzw. danych abonenckich. W ubiegłym roku TK uznał, że tak szerokie uprawnienia zbyt głęboko ingerują w prawo do prywatności i nakazał zmianę przepisów. W maju mija dziewięć miesięcy od wyroku – połowa czasu, jaki rząd i parlament mają na zmierzenie się z tym zadaniem.

MSW zapewnia, że pracuje nad dostosowaniem prawa do wytycznych TK, jednak żaden dokument nie ujrzał jeszcze światła dziennego

ani nie został poddany konsultacjom społecznym. Przy tak skomplikowanej i kontrowersyjnej materii rząd powinien zakładać kilka tur konsultacji i sam zadbać o żywą debatę publiczną. A tymczasem jakby jej unika. Cała nadzieja w determinacji Senatu, który w osobie Michała Seweryńskiego zapowiedział, że daje rządowi miesiąc na odniesienie się do senackiego projektu (tego samego, który już rok temu został opublikowany i poddany pod dyskusję) i oczekuje konstruktywnych uwag, a nie rozpoczynania pracy od nowa.

Na tym swoistym impasie legislacyjnym korzystają policja i służby specjalne, które nadal sięgają po billingi i inne dane telekomunikacyjne bez zewnętrznej kontroli. Jeśli przez kolejne dziewięć miesięcy rząd i parlament nie potraktują tego projektu priorytetowo i nie przeprowadzą rzetelnych, wielostronnych konsultacji – grozi nam pogorszenie prawa. Wpływ, jaki na kształt powstającego prawa mają trzy zmienne: zaangażowane środki, długość prac i poziom skomplikowania kwestii, byłby oczywisty dla każdego, kto zarządzał jakimkolwiek projektem (por. grafika). Z podniesionego tonu dyskusji na Komisji Praw Człowieka, Praworządności i Petycji wynika, że senatorzy dobrze rozumieją, ile czasu potrzeba na napisanie dobrej ustawy, i dlatego tak bezpardonowo dopingują Ministerstwo Spraw Wewnętrznych.

Czekając na reformę zasad udostępniania danych telekomunikacyjnych, przypominamy: skąd wziął się ten problem, jak poradzili sobie z nim nasi sąsiedzi i jakie działania – m.in. Fundacji Panoptikon, Rzecznika Praw Obywatelskich i sądów – doprowadziły do przełomu w postaci unieważnienia dyrektywy retencyjnej i wyroku polskiego Trybunału Konstytucyjnego.

POLSKA WALCZY Z TERRORYZMEM

Państwa członkowskie podchodziły do wprowadzonego przez UE obowiązku zatrzymywania i udostępniania danych telekomunikacyjnych z różnym entuzjazmem – Polska była wówczas

w niechlubnej czołówce. Byliśmy jednym z trzech państw, które nie stworzyło mechanizmu kontroli nad sięganiem po dane, i jedynym, które zdecydowało się przechowywać wszystkie rodzaje danych przez maksymalny okres, jaki dopuszczała dyrektywa (24 miesiące).

Klimat towarzyszący tym decyzjom oddają absurdalne argumenty, na jakie powołali się ustawodawcy: „Polska jest lub może być wykorzystywana jako zaplecze logistyczne lub punkt tranzytowy dla ugrupowań terrorystycznych. Z uwagi na położenie geograficzne Polski, na szlakach wschód–zachód i północ–południe, istnieje bardzo duże prawdopodobieństwo wykorzystania terytorium naszego państwa właśnie w ten sposób” (cytat z uzasadnienia ustawy).

Inne państwa – np. Szwecja i Austria – długo opierały przed wprowadzeniem europejskich przepisów. Z kolei w sąsiadujących z nami Niemczech, Czechach i Słowacji krajowe sądy konstytucyjne uznały przepisy wdrażające dyrektywę retencyjną za nadmiernie ingerujące w prywatność i je unieważniły.

W listopadzie 2010 r., po ujawnieniu przez Panoptikon informacji na temat potężnej liczby zapytań o dane telekomunikacyjne, w Polsce przynajmniej pojawiła się dyskusja: czy jesteśmy najbardziej inwigilowanym narodem Europy? Od tego momentu co roku będziemy publikować informacje (uzyskane nie tylko od UKE, ale z czasem także bezpośrednio od policji i innych służb) o rosnącej liczbie zapytań o billingi i pozostałe dane telekomunikacyjne. Mimo uderzającej tendencji wzrostowej – od 1 mln zapytań w 2009 r., do ponad 2 mln w 2014 r. – będziemy podkreślać, że w Polsce brakuje nawet spójnej metodologii ich liczenia i sprawozdawczości po stronie samych organów.

2013 – ZBIERA SIĘ LAWINA

Pod wpływem krytycznej debaty publicznej posłowie skracają o połowę okres (z 24 do 12 miesięcy), na jaki są zatrzymywane

dane telekomunikacyjne – dla operatorów i służb ta zmiana wchodzi w życie w styczniu 2013 r. Nie rozwiązało to jednak problemu niekontrolowanego dostępu do danych, co potwierdziła sprawa dziennikarza Bogdana Wróblewskiego. W kwietniu 2013 r. Wróblewski wygrał sprawę przeciwko Centralnemu Biuru Antykorupcyjnemu, które bezpodstawnie pobierało jego billingi. Skończyło się na przeprosinach, jednak przekonanie, że prawo trzeba zmienić, zaczęło się przebijać w kolejnych kręgach. W wakacje Rzecznik Praw Obywatelskich i Prokurator Generalny skierowali do Trybunału Konstytucyjnego wnioski o stwierdzenie niezgodności z konstytucją przepisów, które pozwalały policji i innym służbom sięgać po dane. W październiku Najwyższa Izba Kontroli opublikowała raport, w którym sygnalizowała potrzebę pilnych zmian, m.in. wprowadzenia niezależnej kontroli nad pozyskiwaniem i wykorzystywaniem danych oraz rzetelnej sprawozdawczości.

2014 – ZEJŚCIE LAWINY

2014 r. w całej Europie okazał się przełomowy dla walki z niekontrolowanym dostępem do danych telekomunikacyjnych: w kwietniu Trybunał Sprawiedliwości UE uznał, że dyrektywa retencyjna narusza Kartę Praw Podstawowych i od początku była nieważna. Za największy problem Trybunał uznał brak jakichkolwiek mechanizmów gwarantujących, że dane telekomunikacyjne będą wykorzystywane tylko w sprawie ścigania poważnych przestępstw, a dostęp do nich będzie kontrolowany przez sąd lub inny niezależny organ.

Orzeczenie TSUE wywołało drugą falę wyroków sądów konstytucyjnych, które stwierdziły, że krajowe przepisy naruszają podstawowe prawa obywateli. Takie wyroki zapadły m.in. w Austrii, Słowacji i Rumunii. Również polski Trybunał Konstytucyjny uznał, że krajowe przepisy naruszają Konstytucję. Ograniczył się on jednak do stwierdzenia, że niedopuszczalny jest brak zewnętrznej (niezależnej) kontroli nad pozyskiwaniem danych telekomunikacyjnych. Inne problemy, takie jak wykorzystywanie danych nawet w związku z drobną

przestępczością czy brak rzetelnej sprawozdawczości, pozostały bez odpowiedzi.

2015/2016 – PYŁ OPADA. CO WIDAĆ NA HORYZONCIE?

Po unieważnieniu dyrektywy retencyjnej przez Trybunał Sprawiedliwości UE, z Brukseli płyną sprzeczne sygnały. Wydaje się jednak całkiem prawdopodobne, że Komisja Europejska nie podejmie ponownej próby uregulowania tej kontrowersyjnej materii. Co w tej sytuacji zrobią poszczególne państwa? Zobaczymy. Byłoby najlepiej, gdyby poszły w ślad za Niemcami i ucywilizowały zasady dostępu do billingów i innych danych telekomunikacyjnych. Zgodnie z dyskutowanym właśnie za naszą zachodnią granicą projektem, dane mają być przechowywane jedynie przez 10 tygodni, a niektóre (jak lokalizacja telefonu) – nawet przez 4. Dostęp do nich będzie możliwy wyłącznie za zgodą sądu i tylko na potrzeby ścigania najpoważniejszych przestępstw. Tak wygląda prawo, które rzeczywiście równoważy względy prywatności i bezpieczeństwa.

Autorstwo: Katarzyna Szymielewicz, Wojciech Klicki

Źródło: Panoptikon.org