FUNDACJA PANOPTYKON

Warszawa, 25 października 2012 r.

Szanowny Pan
Marek Biernacki
Przewodniczący Komisji Administracji
i Spraw Wewnętrznych Sejmu

Do sejmowej Komisji Administracji i Spraw Wewnętrznych trafił senacki projekt ustawy o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (druk sejmowy nr 633, **dalej: projekt**). Fundacja Panoptykon pragnie przedstawić Wysokiej Komisji opinię w przedmiocie projektu.

Projekt realizuje postanowienie Trybunału Konstytucyjnego (**dalej: TK**) z 15 listopada 2010 r. (sygn. S 4/10), w którym TK zwrócił uwagę na konieczność precyzyjnego określenia w ustawie z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (tekst jednolity Dz. U. z 2010, nr 29 poz. 154, **dalej: ustawa o ABW**) zakresu przestępstw, w związku z którymi Agencja Bezpieczeństwa Wewnętrznego (**dalej: ABW**) uprawniona jest do prowadzenia kontroli operacyjnej. Proponowany w projekcie katalog tych przestępstw co do zasady wymóg ten spełnia, choć dyskusyjny może być jego zakres. Kwestia ta została podniesiona w stanowisku Helsińskiej Fundacji Praw Człowieka[1], my natomiast zwracamy uwagę na inny ważny problem, który został pozostawiony poza zakresem projektu.

Uważamy, że wprowadzenie katalogu przestępstw ograniczającego typy spraw, w których możliwe jest prowadzenie kontroli operacyjnej, powinno dotyczyć również uprawnienia ABW do sięgania, na podstawie art. 28 ustawy o ABW, po dane telekomunikacyjne.

Poniżej przedstawiamy argumenty, które przemawiają za koniecznością ograniczenia możliwości sięgania po dane telekomunikacyjne do spraw dotyczących ściśle określonych przestępstw.

1. Postanowienie Trybunału Konstytucyjnego o sygn. S 4/10

TK w postanowieniu S 4/10 wskazał, że w zakresie czynności operacyjnych niezbędny jest precyzyjny katalog przestępstw, w związku z którymi powinna ona być dopuszczalna. Zdaniem TK „niemożność identyfikacji typów przestępstw, określonych przez ustawę karną, cechująca przepis art. 5 ust. 1 pkt 2 lit. b ustawy o ABW, powoduje w konsekwencji uchybienie dotyczące art. 27 ust. 1 ustawy o ABW. Z przepisu tego nie wynika bowiem, w związku **z jakim typem przestępstwa**, określonego przez ustawę karną, sąd zarządza kontrolę operacyjną, gdy powołuje się na zadania ABW – w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw godzą-

[1] Por. stanowisko Helsińskiej Fundacji Praw Człowieka dotyczące projektu, w którym Fundacja zwróciła uwagę na brak uzasadnienia przyznania ABW tak szerokich uprawnień (szerszych, niż innych służb), a także krzyżowanie się uprawnień ABW z uprawnieniami innych podmiotów uprawnionych do prowadzenia kontroli operacyjnej.

cych w podstawy ekonomiczne państwa, o których mowa w art. 5 ust. 1 pkt 2 lit. b ustawy o ABW".

W naszej ocenie stanowisko TK odnosi się również do zasad dostępu do danych telekomunikacyjnych. Jedyną bowiem różnicą między dopuszczalnością kontroli operacyjnej a sięganiem po dane telekomunikacyjne jest konieczność uzyskiwania zgody sądu. Potwierdza to art. 28 ust. 1 ustawy o ABW, który wyłącza konieczność uzyskania zgody sądu na dostęp do danych telekomunikacyjnych, jednak nie wyłącza pozostałych rygorów, które ABW musi spełnić w związku z kontrolą operacyjną. Nie ma zatem powodów, by sformułowanego przez TK wymogu określoności przestępstw, w związku z którymi dopuszczalna jest kontrola operacyjna, nie odnosić również do dostępu do danych telekomunikacyjnych.

2. Wadliwe wdrożenie tzw. dyrektywy retencyjnej

Konieczność sprecyzowania, w zakresie jakich przestępstw dopuszczalne jest sięganie po dane telekomunikacyjne, wynika pośrednio również z Dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności[2] (tzw. dyrektywa retencyjna), której implementację stanowi m.in. art. 28 ustawy o ABW. Zgodnie z art. 1 ust. 1 dyrektywy retencyjnej celem retencji danych ma być „**dochodzenie, wykrywanie i ściganie poważnych przestępstw**, określonych w ustawodawstwie każdego państwa członkowskiego". Oznacza to, że prawidłowe wdrożenie przepisów dyrektywy powinno zawierać dwa ograniczenia: celu sięgania po dane (jedynie „dochodzenie, wykrywanie i ściganie") oraz zakresu przestępstw, których może to dotyczyć („poważne przestępstwa"). Obecnie sięganie po dane telekomunikacyjne przez ABW dopuszczalne jest w celu realizacji zadań określonych w art. 5 ust. 1 ustawy o ABW, czyli np. w celu uzyskiwania, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa. Wykracza to poza wynikające z dyrektywy retencyjnej ramy dopuszczalności sięgania przez służby po dane telekomunikacyjne. Z tego powodu pożądane jest ograniczenie go jedynie do sytuacji, w których dopuszczalne będzie prowadzenie kontroli operacyjnej.

3. Kolejna sprawa przed Trybunałem Konstytucyjnym z wniosku Rzecznik Praw Obywatelskich

Wątpliwość co do zgodności z Konstytucją zasad dostępu do danych telekomunikacyjnych podniosła Rzecznik Praw Obywatelskich we wniosku do TK (sygn. K 23/11, czeka na rozpoznanie). W stanowisku przedstawionym w tej sprawie przez Sejm zwrócono uwagę, że „w doktrynie i orzecznictwie uznaje się, iż **wymóg precyzyjności podstaw ingerencji w tajemnicę komunikowania się** (prawo do prywatności) nakazuje w szczególności **określenie charakteru przestępstw**, przy ściganiu których dopuszczalne jest zastosowanie tego środka" (…), czego **w wypadku kwestionowanych przepisów zabrakło**". W związku z tym Sejm przedstawił stanowisko o niezgodności art. 28 ustawy o ABW z art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności.

---

[2] Dyrektywa 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.

Podsumowanie

Naszym zdaniem istnieje konieczność stworzenia precyzyjnego katalogu przestępstw, w związku z którymi ABW uprawnione jest do sięgania po dane telekomunikacyjne.

Zdajemy sobie sprawę, że ewentualna realizacja formułowanego przez nas postulatu doprowadziłaby do ograniczenia kompetencji ABW przy jednoczesnym pozostawieniu swobodnego dostępu do danych telekomunikacyjnych innym uprawnionym podmiotom. Jednocześnie takie ograniczenie stanowiłoby jedynie **częściowe** rozwiązanie problemu swobodnego dostępu uprawnionych podmiotów do danych telekomunikacyjnych.

Jednak w naszej ocenie **niezbędne** jest podjęcie prac nad zmianami zmierzającymi w kierunku ograniczenia dostępu policji i innych służb do danych telekomunikacyjnych. Jest to ważne szczególnie ze względu na wielokrotnie powtarzane zapowiedzi rządu dotyczące wprowadzenia zmian prawa idących w tym kierunku, a także przyszłe orzeczenie TK w sprawie o sygn. K 23/11.

Zarówno przygotowywany projekt rządowy, jak i wyrok TK – co prawdopodobne – stwierdzający niekonstytucyjność przepisów dotyczących zasad dostępu do danych telekomunikacyjnych, zrodzi konieczność trudnej debaty na forum Parlamentu dotyczącej nowego kształtu tej regulacji. Wcześniejsze uregulowanie tej problematyki w sposób zgodny z konstytucyjnymi standardami ochrony praw człowieka, chociażby w zakresie jednej z uprawnionych służb (ABW) stanowić będzie wyraz odpowiedzialności polskiego Parlamentu za jakość obowiązującego prawa i jego zgodność ze standardami ochrony praw człowieka.

Z wyrazami szacunku,

W imieniu Fundacji Panoptykon,

Małgorzata Szumańska
Członkini Zarządu

Katarzyna Szymielewicz
Prezeska