



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Edyta Bielak-Jomaa*

Warszawa, dnia 15 lipca 2015 r.

DOLIS – 033 – 284/15/BG / 62915 / 15

**Pan**

**Piotr Zientarski**

**Przewodniczący Komisji Ustawodawczej**

**Senat Rzeczypospolitej Polskiej**

**ul. Wiejska 6**

**00 – 902 Warszawa**

*Szanowny Panie Przewodniczący,*

w odpowiedzi na pismo z dnia 26 czerwca 2015 r. – znak: BPS/KU-034/967/25/15 – uprzejmie informuję, że do projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967), Generalny Inspektor Ochrony Danych Osobowych zgłasza następujące uwagi.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) za niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji uznał przepisy art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej, w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy Prawo telekomunikacyjne.

W opiniowanym projekcie ustawy zaproponowano, aby podmiotem wyznaczonym do kontroli nad uzyskiwaniem danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku – w odniesieniu do Policji, Straży

Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Zdaniem Generalnego Inspektora **zapropozowana przez senatorów forma kontroli jest niewystarczająca** – przepisy nie nakładają bowiem na Policję i służby innych nowych obowiązków poza przekazywaniem sądom raz na 6 miesięcy sprawozdań obejmujących liczbę i rodzaj pozyskanych danych telekomunikacyjnych lub pocztowych, podstawę prawną ich pozyskania, rodzaje przestępstw, w związku z którymi wystąpiono o dane.

W ramach kontroli sąd **może** zapoznać się z materiałami uzasadniającymi udostępnianie danych, a w przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych, podlegają one zniszczeniu (s. 8, 15, 19, 28, 41, 47, 53, 56 projektu). Upřednia kontrola miałaby mieć miejsce jedynie wtedy, gdy z materiałów sprawy wynikałoby, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego. Jednak co do zasady, **proponowany w projekcie model w rzeczywistości przewiduje jedynie fakultatywną kontrolę następczą** (zachodzi zatem podstawowa obawa, że w praktyce sądy nie będą z tego uprawnienia korzystać), co nie może zostać uznane za należyte wykonanie wyroku Trybunału Konstytucyjnego.

Przypomnieć należy, iż Trybunał uznał za konieczne wprowadzenie proceduralnego wymogu, którym jest **kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa**. Status ustrojowy i zakres ustawowych kompetencji takiego organu ma gwarantować efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa. Konieczne jest, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to uznać należy za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej (jak wskazane zostało w cz. III, pkt 2 i 3 uzasadnienia wyroku – np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05).

Trybunał nie przesądził jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Zdaniem Trybunału, nie jest wobec tego wykluczone – w

odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Jak wskazano w wyroku, „regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. **Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach.** W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb”.

Skoro pozyskiwanie danych telekomunikacyjnych dokonuje się w sposób niejawnny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, **brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć.** Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji.

Z całą pewnością nie można uznać za wystarczający model kontroli zaproponowanego przez projektodawcę, który nie przewiduje jako zasady **każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych.** Nadal nie istnieje zatem gwarancja odpowiedniego poziomu ochrony prywatności i tajemnicy komunikowania się osób, których dane są pozyskiwane przez Policję i służby. Nie przesądzając jakie konkretnie organy miałyby zajmować się taką kontrolą, Generalny Inspektor stoi na stanowisku, iż projektowane przepisy powinny szczegółowo określać mechanizmy kontroli. Wskazać również należy, iż **kontrola następcza powinna być traktowana jako wyjątek i stosowana jedynie w sprawach niecierpiących zwłoki.** W każdym jednak przypadku niezależny organ powinien ocenić czy pozyskanie danych telekomunikacyjnych jest w konkretnej sytuacji rzeczywiście niezbędne i należycie uzasadnione oraz czy cel, w którym dane są udostępniane nie mógłby zostać zrealizowany przy użyciu innych, mniej ingerujących w prywatność jednostki środków.

**Zapowiedzi uregulowania w przepisach zewnętrznej kontroli przez niezależny autonomiczny organ,** znalazły się już w opracowanym w 2011 r. *Raporcie dotyczącym retencji danych telekomunikacyjnych. Propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych.* Przedmiotowy raport podkreślał ograniczone możliwości takiej

kontroli wobec służb specjalnych realizujących swoje kompetencje w zakresie wykonywania czynności operacyjno – rozpoznawczych i jako remedium proponował model niezależnego, powoływanego przez parlament, organu kontrolnego, którego celem byłaby **kontrola przestrzegania przez służby specjalne Konstytucji Rzeczypospolitej Polskiej oraz innych przepisów prawa, szczególnie w zakresie praw i wolności obywatelskich**. W dokumencie tym dość kompleksowo odniesiono się do przedmiotowej instytucji, omawiając tak istotne z punktu widzenia jego działania zagadnienia, jak powoływanie i skład, zadania, kompetencje oraz wyniki pracy organu kontrolnego.

Ponadto należy przypomnieć, że w informacji o wynikach kontroli *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, Najwyższa Izba Kontroli wskazała, iż „sięganie po dane retencyjne stanowi istotną ingerencję w prawa i wolności obywatelskie, w szczególności prawo do prywatności. (...) W obecnym stanie prawnym nie istnieje żaden podmiot, który mógłby sprawować rzeczywistą kontrolę nad wykorzystaniem tego środka przez uprawnione organy, służby i formacje. **Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej. W 24 państwach taką kontrolę sprawuje sąd lub prokuratura albo niezależny organ administracyjny**”.

Również przedstawiony w styczniu 2012 r. projekt unijnej dyrektywy o przetwarzaniu danych osobowych w policji i w wymiarze sprawiedliwości w sprawach karnych wyraźnie wskazuje na konieczność istnienia niezależnego organu, który sprawowałby zewnętrzną kontrolę nad danymi retencyjnymi wykorzystywanymi przez służby.

Z uwagi na powyższe, Generalny Inspektor wskazuje, iż projektowane przepisy przewidywać powinny **każdorazową, obowiązkową kontrolę przez niezależny organ adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych**.

Odnosząc się do innych zmian wprowadzonych przez projekt, za niedostateczną realizację wyroku Trybunału Konstytucyjnego należy uznać przepisy ograniczające czas przeprowadzania kontroli operacyjnej przez Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu (s. 36 projektu), Służbę Kontrwywiadu Wojskowego (s. 42 projektu) oraz Centralne Biuro Antykorupcyjne (s. 49 projektu). Zgodnie ze stanowiskiem Trybunału, „ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. (...) Ustawodawca musi mieć także na uwadze, że w demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów”. Tymczasem, w przypadku wyżej wymienionych służb, dopuszczalne byłoby wydawanie kolejnych



postanowień o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (bez ograniczenia, że może być to tylko jedno postanowienie). W praktyce, proponowane rozwiązanie stwarzałoby zatem możliwość bezterminowego prowadzenia czynności operacyjno-rozpoznawczych, co stoi w sprzeczności ze standardami konstytucyjnymi i intencją Trybunału.

Projekt przewiduje ponadto prowadzenie rejestrów postanowień, zgód, wniosków i zarządzeń dot. kontroli operacyjnej (s. 3, 11, 21, 31, 37, 43, 49 projektu). Założenie, iż sposób prowadzenia tych rejestrów oraz wzory dokumentów wchodzących w ich zakres miałyby określać rozporządzenia, nie może zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych. Należy w tym miejscu zwrócić uwagę na stanowisko Trybunału Konstytucyjnego, wyrażone w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007), „zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej”. Wymóg umieszczenia bezpośrednio w ustawie wszystkich zasadniczych elementów regulacji prawnej musi być stosowany ze szczególnym rygoryzmem, gdy regulacja ta dotyczy korzystania przez obywateli z ich praw i wolności (wyrok Trybunału Konstytucyjnego z dnia 25 maja 1998 r., sygnatura U 19/97). Podobnie orzekł Trybunał w wyroku z dnia 18 grudnia 2014 r. (sygnatura K 33/13), dotyczącym tworzenia rejestrów danych medycznych na podstawie rozporządzenia przez ministra zdrowia. W związku z powyższym, **przepisy rangi ustawowej powinny regulować zasadnicze kwestie dotyczące prowadzenia rejestru**, w szczególności zaś: kto jest administratorem danych osobowych, katalog danych znajdujących się w rejestrze, okres przechowywania tych danych, zasady udostępniania informacji z rejestru, krąg podmiotów mających dostęp do danych.

Kolejną kwestią, która budzi zastrzeżenia Generalnego Inspektora jest określenie w projekcie, że dane telekomunikacyjne i pocztowe są przetwarzane przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym nie rzadziej niż co 5 lat dokonuje się weryfikacji potrzeby ich dalszego przetwarzania (s. 6, 13, 17, 26, 39, 46, 51, 55 projektu). **Tego rodzaju sformułowanie jest zbyt szerokie, stwarza ryzyko swobodnej oceny i w praktyce może doprowadzić do nieuzasadnionego, bezterminowego przechowywania danych**, co stoi w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego. Okres przetwarzania danych telekomunikacyjnych i pocztowych powinien być określony w sposób precyzyjny, tak, aby wyeliminować ryzyko nadużyć (istniejące obecnie wobec faktu, iż nie przewidziano zewnętrznej kontroli niezbędności dalszego przetwarzania danych

do realizacji ustawowych zadań) a ewentualna weryfikacja potrzeby ich dalszego przetwarzania powinna odbywać się częściej niż raz na 5 lat.

Podsumowując, w opinii Generalnego Inspektora Ochrony Danych Osobowych, zaproponowana nowelizacja ustawy o Policji i innych ustaw nie stwarza wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowi pełnej realizacji wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

*Zr powrotom*

GENERALNY INSPEKTOR  
OCHRONY DANYCH OSOBOWYCH

*efm*  
dr Beata Bielak-Jomaa