



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia 30 grudnia 2015 r.

DOLiS – 033-640/15/BG/108752/15

Pan

Marek Kuchciński

Marszałek Sejmu

Rzeczypospolitej Polskiej

Sejm Rzeczypospolitej Polskiej

ul. Wiejska 4/6/8

00-902 Warszawa

w związku z wniesieniem do Sejmu **projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154)**, Generalny Inspektor Ochrony Danych Osobowych pragnie wyrazić swoje zastrzeżenia do proponowanych regulacji.

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, pocztowych lub internetowych został: sąd okręgowy właściwy dla siedziby podmiotu, któremu udostępniono dane – 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 **zaproponowana 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 przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

W ramach kontroli sąd **może** zapoznać się z materiałami uzasadniającymi udostępnianie danych – sądom nie przyznano przy tym kompetencji do oceny zasadności pozyskania danych w określonej sytuacji oraz nie przewidziano procedury niszczenia danych w przypadku stwierdzenia braku podstaw do ich pozyskania (a zatem pozyskanych niezgodnie z prawem). Spod jakiegokolwiek kontroli wyłączono m. in. pozyskiwanie danych określonych w art. 161 ustawy Prawo telekomunikacyjne oraz danych z wykazu, o którym mowa w art. 179 ust. 9 tej ustawy.

Proponowany w projekcie model przewiduje jedynie fakultatywną kontrolę następczą pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych (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, 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**”. Z powyższego wynika, że w sytuacjach, kiedy nie potrzeba pilnego działania służb nie zachodzi, kontrola powinna mieć charakter uprzedni. Dzięki temu przypadki sięgania po dane mogłyby podlegać ocenie pod względem spełniania kryteriów adekwatności, niezbędności i celowości. Tymczasem, projektowane przepisy w żadnej sytuacji nie przewidują przeprowadzania kontroli uprzedniej – nawet, gdy miałyby zostać pozyskane dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego.

Jak wynika z informacji przygotowanej przez Urząd Komunikacji Elektronicznej, **w 2014 r. służby, sądy i prokuratury złożyły łącznie 2 177 916 zapytań o dane telekomunikacyjne.** Większa kontrola nad tym procesem pomogłaby zapobiec przypadkom sięgania po dane w sposób automatyczny i tym samym ograniczyć skalę zjawiska. Skoro bowiem pozyskiwanie danych dokonuje się w sposób niejawnny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, **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.

Nie można uznać za wystarczający modelu kontroli zaproponowanego przez projektodawcę, który nie przewiduje jako zasady **każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych, pocztowych i internetowych.** Nadal nie istnieje zatem gwarancja odpowiedniego poziomu ochrony prywatności i tajemnicy komunikowania się osób, których dane są pozyskiwane przez Policję i służby. Nie

przesądzać 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 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**”.

Zgodnie z opublikowanym w 2011 r. *sprawozdaniem Komisji Europejskiej na temat implementacji dyrektywy 2006/24/WE przez kraje członkowskie Unii Europejskiej* (stanowiącym wynik analizy porównawczej 25 raportów krajowych) **tylko w trzech państwach – w Irlandii, na Malcie i w Wielkiej Brytanii – nie była sprawowana kontrola uprzednia nad udostępnianiem**

danych telekomunikacyjnych, a w trzech kolejnych – w Polsce, na Łotwie i Słowacji – brak było jakiegokolwiek organu kontroli zewnętrznej.

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, pocztowych i internetowych.** W tym miejscu należy również zauważyć, iż **projekt nie zakłada stosowania zasady subsydiarności**, tj. ograniczenia możliwości sięgania po dane do sytuacji, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne. Sądy nie mogłyby zatem ocenić, na ile sięgnięcie w określonej sytuacji po dane było rzeczywiście niezbędne i należycie uzasadnione, co dodatkowo osłabia poziom ochrony prywatności jednostek.

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 oraz Służbę Kontrwywiadu Wojskowego. 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 przedłużenie kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (podczas gdy w przypadku innych podmiotów uprawnionych do prowadzenia kontroli operacyjnej łączna długość okresów nie może przekraczać 12 miesięcy). 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, pisemnych zgód, wniosków i zarządzeń dot. kontroli operacyjnej. Nie został przy tym określony sposób prowadzenia tych rejestrów oraz wzory dokumentów wchodzących w ich zakres, co – jeżeli w rejestrach takich miałyby być przetwarzane również dane osobowe – nie może zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych. **Przepisy rangi ustawowej powinny bowiem regulować zasadnicze kwestie dotyczące prowadzenia rejestru**, w szczególności zaś 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 brak określenia w projekcie okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane

telekomunikacyjne, pocztowe i internetowe. Stoi to w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego, zgodnie z którą **dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania**. Projekt przewiduje jedynie, iż dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi wykorzystanymi w postępowaniu, w tym kwestia weryfikacji potrzeby ich dalszego przetwarzania. **W praktyce może prowadzić to do nieuzasadnionego, bezterminowego przechowywania danych**. Okres przetwarzania danych telekomunikacyjnych, pocztowych i internetowych powinien zatem 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).

W uzasadnieniu do wyroku Trybunał Konstytucyjny podkreślił również, że niejawnie pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych – przede wszystkim **ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat** (bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli). W opinii Trybunału, ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie (gdyż powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji narażałoby te działania na nieskuteczność). Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r., sygn. S 2/06). Zapewnienie informacji jest przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji prawa dostępu do urzędowych dokumentów i zbiorów danych. Jak zauważył Trybunał, **zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji**. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji – ponieważ dokonało się to w sposób niejawnym, bez jej wiedzy i zgody – nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji. Z uwagi na powyższe, Generalny Inspektor wskazuje na konieczność uzupełnienia projektu o obowiązek informacyjny wobec osób, których dane zostały pozyskane przez Policję i służby.

Należy ponadto dodać, iż **kwestia sięgania przez Policję i służby po dane telekomunikacyjne nie może zostać uregulowana w sposób prawidłowy bez odniesienia się do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r.,**

stwierdzającego nieważność dyrektywy 2006/24 w sprawie zatrzymywania danych w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland. TSUE uznał nieważność dyrektywy ze względu na naruszenie art. 7 (poszanowanie życia prywatnego i rodzinnego) i 8 (ochrona danych osobowych) w zw. z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej. Jako przyczynę nieważności dyrektywy Trybunał wskazał brak proporcjonalności zawartych w niej rozwiązań, które, mimo iż adekwatne do celu, który ma zostać za ich pomocą osiągnięty, ingerują zbyt głęboko w prawa podstawowe. TSUE uznał, że ten sam cel (zwalczanie poważnej przestępczości oraz zapewnienie bezpieczeństwa publicznego) można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa obywateli. W odniesieniu do szczegółowych regulacji, Trybunał zauważył między innymi następujące uchybienia:

- w dyrektywie nie przewidziano jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw,
- dyrektywa nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw, które z uwagi na zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, można uznać za wystarczająco poważne, by taką ingerencję uzasadnić,
- dyrektywa nie określa żadnych materialnych i proceduralnych przesłanek, w przypadku zaistnienia których właściwe organy krajowe będą mogły uzyskać dostęp do danych i następnie je wykorzystać,
- dyrektywa nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty.

Mimo iż wyrok w sprawie Digital Rights Ireland nie powoduje automatycznie nieważności aktów prawa krajowego implementujących dyrektywę 2006/24, to konieczne jest uwzględnienie go w pracach legislacyjnych nad projektem ustawy, który dotyczy tej samej materii. Tymczasem, zaproponowanych w projekcie rozwiązań nie można uznać za zgodne z wytycznymi Trybunału Sprawiedliwości Unii Europejskiej.

Przykładowo, zaproponowany art. 20c ust. 1 ustawy o Policji przewiduje możliwość pozyskiwania przez Policję danych telekomunikacyjnych, pocztowych i internetowych m.in. w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw – bez ograniczenia tego uprawnienia do sytuacji związanych z przestępstwami poważnymi. Zachodzi zatem potrzeba ponownego przeglądu katalogu sytuacji, w których dopuszczalne jest sięganie po dane przez Policję i służby.

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).