



RZECZNIK PRAW OBYWATELSKICH

Warszawa,

Adam Bodnar

VII.562.1.2019.KŁ

**Pan**  
**Marian Banaś**  
**Prezes Najwyższej Izby Kontroli**  
ul. Filtrowa 57  
02-056 Warszawa

**Jednym z ważnych obszarów zainteresowania Rzecznika Praw Obywatelskich jest zapewnienie bezpieczeństwa publicznego przez właściwe formacje i służby specjalne (dalej również jako: służby) oraz wpływ podejmowanych w tym celu działań na sferę praw i wolności człowieka i obywatela.** Jak wielokrotnie podkreślałem, wymogi bezpieczeństwa państwa nie oznaczają, że zasady inwigilacji nie mają podlegać ograniczeniom wynikającym z konstytucyjnych praw i wolności. Powinny być one wynikiem wyważania między potrzebą ochrony bezpieczeństwa obywateli oraz ich prawa do prywatności. Należy wskazać, że w tym zakresie jednostka ma bardzo ograniczone środki bezpośredniej ochrony prawnej. W związku z powyższym obywatele muszą polegać na organach takich jak Rzecznik Praw Obywatelskich i Najwyższa Izba Kontroli. W mojej ocenie kontrole NIK i publikowane po nich raporty stanowią niezwykle cenny materiał, który powinien stanowić podstawę do działań, w tym podejmowania prac legislacyjnych, dla organów państwa w tym obszarze.

W szczególności pragnę tu przywołać kontrolę planową nr P/12/191 – „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne”. W podsumowaniu wyników kontroli stwierdzono, że: „W ocenie NIK, obowiązujące

przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych telekomunikacyjnych, może nasuwać wątpliwości, co do współmierności stosowanych ograniczeń praw i wolności obywatelskich w sferze wolności komunikacji z zasadami określonymi w Konstytucji RP. Należy ponadto zauważyć, iż obowiązujący system zbierania informacji o zakresie wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne, nie pozwala na określenie rzeczywistej liczby dokonywanych sprawdzeń. Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania<sup>1</sup>. Są to wnioski spójne z wyrażanymi w tym czasie poglądami Rzecznika Praw Obywatelskich, jednak fakt, że zostały one zaprezentowane w wyniku przeprowadzonej kontroli NIK nadaje im nowy ciężar.

Rzecznik Praw Obywatelskich również podejmował działania związane z ochroną informacji o jednostce przetwarzanych w działaniach operacyjnych. Rzecznik między innymi zainicjował postępowanie przed Trybunałem Konstytucyjnym w sprawie K 23/11. Wydany przez TK wyrok z 30 lipca 2014 r. w którym Trybunał stwierdził niekonstytucyjność części zaskarżonych przepisów miał doprowadzić do stworzenia systemu przetwarzania danych opartego o konstytucyjny standard ochrony prywatności.

Należy jednak stwierdzić, że ustawodawca nie spełnił pokładanych w nim nadziei. Mająca wykonywać wyrok ustawa z 5 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147) nowelizując relewantne przepisy, znacząco poszerzyła możliwości ingerencji formacji i służby specjalnych w sferę prywatności obywateli. W lutym 2016 r. Rzecznik Praw Obywatelskich zaskarżył do Trybunału Konstytucyjnego znowelizowane przepisy, które nie tylko nie realizują wyroku

---

<sup>1</sup> Informacja o wynikach kontroli - Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne” Najwyższa Izba Kontroli 2013.

TK z 2014 r., ale „w poważnym zakresie naruszają konstytucyjne prawa i wolności człowieka oraz standardy wyznaczone w prawie międzynarodowym”.

RPO zakwestionował przepisy o uprawnieniach formacji i służb specjalnych do kontroli operacyjnej. Wniosek dotyczył też zasad pobierania przez służby danych telekomunikacyjnych, internetowych i pocztowych obywateli - na co zgoda sądu nie jest obecnie potrzebna.

W wyniku zmiany przepisów służby uzyskały dostęp do danych internetowych za pomocą stałego łącza. Pobieranie danych nie musi się wiązać z żadnym toczącym się postępowaniem. Służby nie muszą już - tak jak przedtem - składać pisemnych wniosków do dostawców usług internetowych i wykazywać, na potrzeby jakiego postępowania dane są im potrzebne. Oznacza to, że dane te mogą być zbierane nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania najpoważniejszym przestępstwom, którym inaczej nie da się przeciwdziałać (jak wskazują standardy wynikające z Konstytucji i prawa europejskiego), ale także wtedy, gdy jest to dla służb wygodne. Zdaniem RPO taki dowolny dostęp służb do tych danych oznacza ryzyko poważnych nadużyć. Służby mogą na tej podstawie np. precyzyjnie odtwarzać różne aspekty życia prywatnego obywatela, zbierać dane o trybie życia, poglądach, upodobaniach czy skłonnościach.

Rzecznik kwestionował również brak realnej kontroli pobierania danych obywateli. Sąd okręgowy ma wprawdzie prawo do kontroli, ale jedynie na podstawie zbiorczych półrocznych sprawozdań służb. Sąd nie musi, ale tylko może weryfikować, czy dane pobrano zasadnie. Tymczasem Konstytucja zakazuje pozyskiwania, gromadzenia i udostępniania informacji o obywatelu innych niż niezbędne. Po kontroli sąd może jedynie poinformować poszczególną służbę o jej wynikach, ale nie może zarządzić np. zniszczenia zgromadzonych danych. W praktyce ta kontrola sądów ma charakter iluzoryczny. Tajne sprawozdania służb nie są informacją publiczną, choć zawierają informacje dotyczące liczby pozyskanych danych telekomunikacyjnych, pocztowych lub internetowych i kwalifikacji prawnej czynów, w związku z którymi o nie wystąpiono.

Kolejnym zarzutem wobec znowelizowanych przepisów był nieproporcjonalnie długi czas trwania kontroli operacyjnej - do 18 miesięcy. Ponadto znowelizowane przepisy

ograniczyły chronioną prawem tajemnicę zawodów zaufania publicznego, m.in. adwokatów, radców prawnych, lekarzy i dziennikarzy. Zdobyte podczas inwigilacji tajemnice mogą być wykorzystane w postępowaniu karnym, gdy „jest to niezbędne ze względu na dobro wymiaru sprawiedliwości, a okoliczność ta nie może być ustalona na podstawie innego dowodu”.

Rzecznik był jednak zmuszony wycofać wniosek, ponieważ w składzie orzekającym znalazły się osoby, których nie tylko status sędziowski ale bezstronność w sprawie uprawnień służb była kwestionowana. Przy tym Rzecznik mocno podkreślił, że wycofując wniosek nie rezygnuje działań, mających doprowadzić do tego aby zasady inwigilacji odpowiadały standardom konstytucji oraz prawa europejskiego.

Należy jednak wskazać, że od wejścia w życie obecnie obowiązujących przepisów regulujących omawianą materię minęło już kilka lat i niezwykle cenne byłoby przeprowadzenie kontroli funkcjonowania wprowadzonych przez nią zmian, szczególnie w zakresie dostępu służb do danych dotyczących obywateli. Byłoby to szczególnie istotne w świetle wniosków i rekomendacji z kontroli NIK w 2013 r.

Mając powyższe na względzie, działając na podstawie art. 12 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2017 r., poz. 2179), zwracam się do Pana Prezesa z uprzejmą prośbą o rozważenie podjęcia stosownych działań kontrolnych w odniesieniu do pozyskiwania danych obywateli, w tym w szczególności danych telekomunikacyjnych i internetowych, przez podmioty uprawnione. Uprzejmie proszę o poinformowanie mnie o stanowisku Najwyższej Izby Kontroli w tym względzie.