



Warszawa, 25 stycznia 2016 r.

Opinia do ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw

(druk nr 71)

I. Cel i przedmiot ustawy

Celem ustawy jest nowelizacja 13 ustaw: o Policji, o Straży Granicznej, o kontroli skarbowej, Prawo o ustroju sądów wojskowych, Prawo o ustroju sądów powszechnych, o Żandarmerii Wojskowej i wojskowych organach porządkowych, o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, o świadczeniu usług drogą elektroniczną, Prawo telekomunikacyjne, o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, o Centralnym Biurze Antykorupcyjnym oraz ustawy o Służbie Celnej w zakresie przepisów dotyczących kontroli operacyjnej oraz dostępu służb państwowych do szeroko rozumianych danych telekomunikacyjnych, pocztowych i internetowych.

Ustawa musi wejść w życie najpóźniej w dniu 7 lutego 2016 r. (i tak została określona data wejścia ustawy w życie), ponieważ w tym dniu tracą moc, w wyniku wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), w zakresie określonym przez Trybunał, przepisy regulujące powyższe zagadnienia.

Ustawa zgodnie z ww wyrokiem TK doprecyzowuje, iż kontrolę operacyjną można zarządzić tylko wobec przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej. Szerzej ale i precyzyjniej niż dotychczasowe regulacje, określające uprawnienia służb, wskazuje się sposoby prowadzenia kontroli operacyjnej (uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne, uzyskiwanie i utrwalanie treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych,

systemach informatycznych i teleinformatycznych). W przypadku niektórych służb ustawa określa maksymalny okres, na który można przedłużyć kontrolę operacyjną (w przypadku Policji, wywiadu skarbowego, Żandarmerii Wojskowej, CBA). Ustawa pozwala na upoważnienie zastępców szefów służb do składania wniosków dotyczących zarządzenia kontroli operacyjnej. Ustawa nakazuje niezwłoczne, komisyjne i protokolarne niszczenie materiałów objętych bezwzględnym zakazem dowodowym oraz reguluje procedurę uzyskania zgody sądu w przypadku materiałów objętych tzw. względnym zakazem dowodowym. Ustawa wprowadza obowiązek (dla sądów, organów służb oraz prokuratorów) prowadzenia rejestrów postanowień, zgód, wniosków oraz zarządzeń dotyczących kontroli operacyjnej.

Ustawa doprecyzowuje także przepisy dotyczące uzyskiwania oraz przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych. W tym zakresie wprowadzono następczą kontrolę sądu nad uzyskiwanymi przez służby danymi. Kontrola będzie się odbywała na podstawie przekazywanych sądowi, w okresach półrocznych, sprawozdań.

Ustawa wprowadza także, niepodlegający kontroli sądu, dostęp służb do danych abonamentowych (tzw. książki telefonicznej).

Ponadto ustawa nakłada na sądy obowiązek przekazywania informacji na temat przetwarzania danych telekomunikacyjnych, pocztowych oraz internetowych oraz o wynikach kontroli udostępniania tych danych służbom. Ustawa nakłada także na Ministra Sprawiedliwości obowiązek przedstawiania corocznie takiej zbiorczej informacji Sejmowi i Senatowi.

II. Przebieg prac legislacyjnych

Projekt ustawy został wniesiony jako projekt poselski. W wyniku postępowania legislacyjnego wniesiono szereg poprawek porządkujących i redakcyjnych oraz kilka istotnych o charakterze merytorycznym. Są to przede wszystkim poprawki:

1) uwzględniające szczupłość infrastruktury usługodawców świadczących usługi drogą elektroniczną będących mikro lub małymi przedsiębiorcami;

2) nakazujące zarządzenie bezpośredniego i niezwłocznego niszczenia materiałów objętych bezwzględnym zakazem dowodowym, pozyskanych w wyniku przeprowadzenia kontroli operacyjnej przez organy wnioskujące o zarządzenie kontroli operacyjnej bez pośrednictwa prokuratora i sądu;

3) wyłączające możliwości pozyskania wśród danych telekomunikacyjnych, pocztowych oraz internetowych dostępu do treści indywidualnych komunikatów.

III. Uwagi

Materia regulowana w ustawach nowelizowanych niniejszą ustawą była przedmiotem zainteresowania w szczególności Trybunału Konstytucyjnego (m.in. we wspomnianym wyroku K 23/11), Trybunału Sprawiedliwości Unii Europejskiej (wyrok z dnia 8 kwietnia 2014 r. w sprawach połączonych C-293/12 oraz C-594/12) oraz Najwyższej Izby Kontroli (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).

Oceniając ustawę należy kierować się przede wszystkim ustalonym przez Trybunał Konstytucyjny standardem konstytucyjnym, który znalazł odzwierciedlenie (choć niecałkowicie) w treści samego wyroku K 23/11 oraz w uzasadnieniu do wyroku.

1) Przepisy naruszające wprost wyrok TK:

1.1. Art. 7 pkt 3 lit. d ustawy nowelizującej, w zakresie art. 28 ust. 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz art. 10 pkt 3 lit. e ustawy nowelizującej, w zakresie art. 32 ust. 9 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, które nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych nie mających znaczenia dla prowadzonego postępowania karnego. Ustawa pozwala na zachowanie danych określonych jako "istotne dla bezpieczeństwa państwa" oraz "istotne dla obronności Państwa". Regulacje te nie biorą pod uwagę sentencji Trybunału w zakresie pkt I ppkt 8, który uznał, iż art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz art. 18 ustawy o Centralnym Biurze Antykorupcyjnym w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Ustawa realizuje postulat sądu konstytucyjnego jedynie w zakresie CBA.

Wskazane przepisy w tym zakresie należałoby skreślić.

1.2. Art. 13 - zgodnie z którym do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu, stosuje się przepisy dotychczasowe. Przepis ten nie uwzględnia sentencji wyroku TK w zakresie pkt I ppkt 6. Trybunał uznał za niezgodne z Konstytucją odpowiednie przepisy ustaw dotyczące kontroli operacyjnej w zakresie w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne. Zdaniem Trybunału brak tej gwarancji jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji. Ponieważ na skutek przepisu art. 13 gwarancja ochrony informacji objętych zakazami dowodowymi będzie miała miejsce w jedynie stosunku do spraw wszczętych po dniu wejścia ustawy w życie, przepis ten należy uznać za niezgodny z Konstytucją.

Przepis ten należałoby skreślić lub wprowadzić termin w jakim służby musiałyby wystąpić do sądów o odpowiednie zgody oraz termin w jakim musiałyby zniszczyć materiały zawierające niedopuszczalne jako dowód informacje.

1.3. Art. 15 ustawy umożliwiający stosowanie przepisów dotychczasowych do postępowań w sprawie udostępniania danych telekomunikacyjnych oraz danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług, wszczętych i niezakończonych przed dniem wejścia w życie ustawy, oraz do zgromadzonych danych. Przepis ten nie bierze pod uwagę faktu, iż Trybunał wyraźnie stwierdził, iż po 6 lutego 2016 r. tracą moc przepisy dotyczące pozyskiwania tych danych przez służby, przez to, iż nie przewidują niezależnej kontroli udostępniania danych (pkt I ppkt 5 sentencji wyroku). Przepis ten także nie uwzględnia orzeczenie Trybunału w zakresie obowiązku niszczenia innych danych, niż tylko te które mają znaczenie dla postępowania karnego (vide uwaga 1.3.).

Przepis ten należałoby skreślić lub określić termin w jakim służby rozdzieliłyby materiały dotyczące tzw. książki telefonicznej od tych zawierających wrażliwe dane telekomunikacyjne, sporządziłyby, według nowych przepisów, sprawozdanie dla sądu oraz termin w jakim musiałyby zniszczyć materiały nieprzydatne do postępowań karnych.

1.4. Art. 16 ustawy umożliwiający stosowanie przepisów dotychczasowych do kontroli operacyjnej zarządzanej na podstawie art. 27 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w celu realizacji zadań określonych w art. 5 ust. 1 pkt

2 lit. b tej ustawy i niezakończony do dnia wejścia w życie ustawy. Art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b zgodnie z pkt I ppkt 2 sentencji ww wyroku TK w dniu 6 lutego 2016 r. utraci moc. Nie jest możliwe "przedłużenie" jego działania za pomocą przepisu o charakterze przejściowym, ponieważ stanowiłoby to oczywiste ominięcie wyroku, który uznał, iż kontrola operacyjna prowadzona na podstawie nieprecyzyjnego przepisu określającego kompetencje Agencji Bezpieczeństwa Wewnętrznego stanowi naruszenie art. 2, art. 47 oraz art. 49 w związku z art. 31 ust. 3 Konstytucji.

Przepis ten należy skreślić lub tak ukształtować kompetencje ABW, aby spełniały standardy konstytucyjne np. zgodnie z postanowieniem sygnalizacyjnym Trybunału z dnia z dnia 15 listopada 2010 r. (S 4/10) i wykonaniem tego postanowienia przez Senat w inicjatywie z dnia 6 lipca 2012 r. o zmianie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

2) Przepisy, które budzą wątpliwości co do zgodności z Konstytucją, ze względu na ustalony przez Trybunał standard konstytucyjny:

2.1. Ustawodawca posługuje się dwoma modelami przedłużania czasu trwania kontroli operacyjnej. Pierwszy, zgodnie z którym po upływie okresu na jaki kontrola operacyjna została zarządzona i jego jednorazowego przedłużenia, można wydać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy. Drugi model, zgodnie z którym można wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (regulacje dotyczące ABW i SKW). Tym samym ten drugi model oznacza *de facto* możliwość nieskończonego, bezterminowego przedłużania trwania kontroli operacyjnej. Wydaje się, że ten drugi model nie spełnia postulatu Trybunału zawartego w uzasadnieniu do wyroku w pkt. III ppkt 5.1.3.3 "ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. Nie jest rolą Trybunału Konstytucyjnego, jako sądu prawa, określanie, jak długi ma być to termin. Termin ten ma określić ustawodawca tak, aby umożliwiał osiągnięcie konstytucyjnie uzasadnionego celu. Nie może być to jednak termin ani nadmiernie długi, ani zbyt krótki, który nie pozwala na efektywną pracę operacyjno-rozpoznawczą. 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". Tym samym wydaje się, iż przepisy ustawy nowelizujące w tym zakresie ustawę o ABW (art. 7 pkt 2 lit. c, ust. 9) oraz ustawę o SKW (art. 10 pkt 2 lit. c, ust. 7) naruszają wskazany przez Trybunał standard konstytucyjny kontroli operacyjnej i powinny ulec zmianie.

Przepisy te należy ujednoczyć np. zgodnie z pierwszym modelem przedłużania czasu trwania kontroli operacyjnej lub wskazać nieprzekraczalny odpowiednio dłuższy dla tych służb okres.

2.2. Zagadnienie subsydiarności pozyskiwania wrażliwych danych telekomunikacyjnych, pocztowych i internetowych. O ile przepisy dotyczące kontroli operacyjnej w sposób należyty respektują zasadę subsydiarności, czyli są stosowane "gdy inne środki okazały się bezskuteczne albo będą nieprzydatne", to zagadnienie to jest zupełnie pominięte w zakresie pozyskiwania danych telekomunikacyjnych. Tym bardziej, iż w zakresie np. bilingów lub danych lokalizacyjnych stanowią poważną ingerencję w sferę wolności i prawa jednostki. Zdaniem Trybunału "Niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. To znaczy, że niejawna ingerencja w wolności i prawa, ma stanowić *ultima ratio*. Dotyczy to w takiej samej mierze kontroli operacyjnej, jak i udostępniania danych telekomunikacyjnych czy innych form pracy operacyjno-rozpoznawczej o podobnym skutku dla jednostek" (uzasadnienie do wyroku pkt III ppkt 5.2.4). Należy także wziąć pod uwagę przyczynę, z powodu której Trybunał nie wypowiedział się w kwestii przestrzegania tej zasady - uznano, iż przesądzenie o niekonstytucyjności niedostatecznych gwarancji proceduralnych, związanych z brakiem zewnętrznej kontroli udostępniania danych telekomunikacyjnych czyni zbędnym odnośnienie się do braku przesłanki subsydiarności (uzasadnienie do wyroku pkt III ppkt 10.4.4.).

Przepisy uprawniające służby do pozyskania danych należy uzupełnić o wskazanie, iż mogą to czynić "gdy inne środki okazały się bezskuteczne albo będą nieprzydatne".

Propozycja poprawki:

W art. 1 w pkt 2, w art. 20c w ust. 1 po wyrazach „Policja może” dodaje się wyrazy „, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne,”.

Analogiczne poprawki powinny znaleźć się w przepisach dotyczących pozostałych służb.

2.3. Niezależna kontrola sądowa pozyskiwania danych telekomunikacyjnych, pocztowych oraz internetowych. W przypadku pozyskiwania wrażliwych danych telekomunikacyjnych ustawodawca wybrał model następczej kontroli sądowej opartej na składanych za okresy półroczne sprawozdań. Sąd dokonuje kontroli sprawozdania a o wyniku kontroli informuje właściwy organ, który przedstawił sprawozdania. Wydaje się, że ta kontrola nie spełnia wymogów wskazanych przez Trybunał dotyczących konieczności określenia obiektywnych kryteriów, którymi będzie kierował się sąd przy ocenie przedstawionego sprawozdania. Pomimo prawa sądu do zapoznania się z materiałami uzasadniającymi udostępnienie wrażliwych danych telekomunikacyjnych czy internetowych, wskazanie przesłanek uzasadniających ich udostępnienie jest tak szerokie i ogólne ("w celu zapobiegania lub wykrywania przestępstw" lub jeszcze bardziej ogólnie "niezbędne do realizacji zadań") to wydaje się, że brak określenia kategorii czynów uzasadniających ingerencję w prawa jednostki, brak konieczności przestrzegania zasady subsydiarności i tym samym obiektywnych kryteriów oceny sądu czyni kontrolę sądową fasadową, formalną. Trudno ocenić czy wobec tak ustalonych mechanizmów sąd jest w stanie stwierdzić czy korzystanie z danych telekomunikacyjnych jest rzeczywiście niezbędne i uzasadnia ingerencję w prawo do prywatności i wolność komunikowania.

Ponadto zdaniem Trybunału w pewnych wypadkach wskazana byłaby uprzednia kontrola pozyskiwania danych "W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb".

Częściową realizacją tego postulatu byłoby wpisanie zasady subsydiarności pozyskiwania danych telekomunikacyjnych (vide konkluzja uwagi 2.2.).

3) Uwagi na marginesie wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. w sprawach połączonych C-293/12 oraz C-594/12.

Należy podzielić opinię Biura Analiz Sejmowych z dnia 31 grudnia 2015 r. w zakresie zgodności opiniowanej ustawy z prawem Unii Europejskiej. Autor opinii zwrócił uwagę, iż Trybunał Sprawiedliwości uznając za nieważną tzw. dyrektywę retencyjną 2006/24/WE "wskazał przesłanki legalności przepisów ograniczających prawa i obowiązki odnoszące się do poufności komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie

dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej". Trybunał Sprawiedliwości uznał, że umożliwienie dostępu organom krajowym stanowi ingerencję w prawa podstawowe określone w art. 7 i 8 (poszanowanie do życia prywatnego i ochrony danych osobowych) Karty Praw Podstawowych. Zdaniem Trybunału Sprawiedliwości ze względu na wagę ingerencji w prawa podstawowe, wykorzystanie danych telekomunikacyjnych może mieć miejsce wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw i przestępstwa te powinny być "wystarczająco poważne". Zdaniem autora opinii przepisy ustawy nie spełniają tego kryterium, uzasadniającego ingerencję w prawa podstawowe albo z tego powodu, iż odsyłają do ogólnie określonych "przestępstw" albo prawa do uzyskiwania danych w celu realizacji innych zadań służb (takich jak np. prowadzenie działalności analitycznej CBA). Autor opinii zwrócił uwagę, iż zdaniem Trybunału Sprawiedliwości kontrola sądowa (lub innego niezależnego organu administracji) powinna mieć charakter uprzedni, która zapewniałaby "aby udostępnianie i wykorzystanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu, oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw." (Opinia BAS-WAPEiM-408/15).

4) Pozostałe uwagi

4.1. Należy ujednoczyć redakcję przepisów w zakresie obowiązków prowadzenia rejestrów dotyczących kontroli operacyjnej. Sądy, Prokurator Generalny, prokurator okręgowy i organy służb mają obowiązek prowadzenia rejestrów postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej. Niekiedy przepisy mówią o "odpowiednich" rejestrach, niekiedy nie wskazują tych rejestrów w ogóle a raz (w nowelizacji ustawy o CBA) wskazują prawidłowo "prowadzą rejestry, odpowiednio postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących kontroli operacyjnej".

Tak więc ujednoczenie, wzorem nowelizacji ustawy o CBA, powinno obejmować przepisy zawarte w art. 1 w pkt 2 w lit. i, w art. 2 w pkt 1 w lit. i, w art. 3 w pkt 3 w lit. g, w art. 6 w pkt 3 w lit. h, w art. 7 w pkt 2 w lit. i, oraz w art. 10 w pkt 2 w lit. i.

4.2. Ze względu na fakt, iż ustawa wchodzi w życie w trakcie roku należy określić początkowy okres realizacji obowiązków sprawozdawczych służb wobec sądów. Obowiązek przekazywania sprawozdania za okresy półroczne spowoduje, iż za rok 2016 sądy będą miały

informacje jedynie za jeden pełny okres (drugie półrocze upłynie 7 lutego 2017 r.). Spowoduje to, iż informacja przekazywana Ministrowi Sprawiedliwości, przekazywana do 31 marca będzie niepełna, co utrudni wykonanie temu ostatniemu obowiązkowi informacyjnego przed Sejmem i Senatem.

Propozycja poprawki – należy dodać przepis przejściowy, zgodnie z którym sprawozdanie służb przekazywane sądom po raz pierwszy obejmuje okres od wejścia ustawy w życie do dnia 30 czerwca.

Adam Niemczewski

Wicedyrektor