KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ
ul. Lindleya 16
02-013 Warszawa
Tel. + 48 22 29 28 700, Fax +48 22 29 28 701
e-mail: biuro@kike.pl, grap@kike.pl, http://www.kike.pl
KRS 0000316678, REGON: 141637224, NIP 9512270210

Warszawa, 11 stycznia 2016 r.

ID KIKE: GRAP-1/2016

Sz. P. Anna Streżyńska
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Sz. P. Maciej Wasik
Sekretarz Stanu
Sekretarz Kolegium
ds. Służb Specjalnych
Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

OPINIA W SPRAWIE PROJEKTU USTAWY O ZMIANIE USTAWY O POLICJI ORAZ NIEKTÓRYCH INNYCH USTAW

W nawiązaniu do spotkania konsultacyjnego 4.01.2016 r. i możliwości wyrażenia pisemnej opinii w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (dalej jako: „**Projekt**") skierowanego do Sejmu w dniu 23 grudnia 2015 roku, Krajowa Izba Komunikacji Ethernetowej (dalej jako: „**KIKE**" lub „**Izba**") poniżej przedstawia swoje stanowisko odnośnie Projektu, mając nadzieję, że przyczyni się ona do prac nad należytą realizacją wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), a także stanowić będzie impuls do rozważenia innych zmian, które zdaniem przedsiębiorców telekomunikacyjnych zrzeszonych w KIKE powinny być przy tej okazji także rozpatrzone.

I. Zapewnianie warunków kontroli operacyjnej i retencji danych, a problem odpłatność w tym zakresie.

W ocenie Izby, większość obecnych regulacji w zakresie ustawy z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (dalej jako: „**PT**") (np. dotyczących retencji danych) nie uwzględnia wielkości

przedsiębiorców telekomunikacyjnych lub przyjmuje zbyt niskie progi wielkości sieci w odniesieniu do nakładanych na PT obowiązków na kolejnych poziomach wielkości sieci (np. obowiązek utworzenia kancelarii tajnych, czy wymóg posiadania świadectwa bezpieczeństwa przemysłowego). Nade wszystko jednak – co do zasady całością kosztów jakie wiążą się z zapewnieniem warunków dla przeprowadzania kontroli operacyjnej i retencją danych obciążeni są przedsiębiorcy telekomunikacyjni. Co jednak w opinii KIKE jest kluczowe – z jednym wyjątkiem dot. retencji (tu zapytania są kierowane regularnie do dużych i małych PT) – w praktyce MŚP występują jedynie pojedyncze i odosobnione przypadki, w których uprawnione instytucje korzystają z zasobów informatycznych małych firm. W praktyce więc (dobrym przykładem jest tu art. 179 PT) sektor MŚP ponosi koszty przygotowania infrastruktury, z której w praktyce operacyjnej uprawnione służby nie korzystają lub korzystają incydentalnie. Omawiana nowelizacja powiela i umacnia niestety ten niewłaściwy model, w którym projektowane obowiązki nie uwzględniają nie tylko możliwości realizacji obowiązków przez sektor MŚP, ale i realnych potrzeb uprawnionych służb w tym zakresie. W ocenie Izby koniecznym jest sporządzenie przez właściwe instytucje gruntownego raportu z wykorzystania poszczególnych uprawnień operacyjnych z uwzględnieniem grup docelowych – w szczególności wielkości przedsiębiorstw telekomunikacyjnych, ich sieci i profilu działalności. Projektowanie regulacji nieadekwatnie do realnych potrzeb służb i możliwości adresatów powoduje bowiem trzy niezwykle negatywne skutki:

a. Przeregulowanie rynku i obciążenie małych firm kosztami, których firmy te nie mogą z uwagi na swoją wielkość unieść jest szczególnie nieuzasadnione w sytuacji, gdy nakładane na MŚP wymagania w praktyce nie są oparte na realnych potrzebach w zakresie bezpieczeństwa Państwa.
b. Konsekwencją powyższej sytuacji jest fakt, iż nawet jeśli wyposażenie oraz kompetencje techniczne lokalnych operatorów, a także mechanizmy jednorazowego dopuszczenia do czynności operacyjnych gwarantują realizację pojedynczych w skali lat działalności firm procedur operacyjnych, to brak realizacji ustawowo nałożonych wymagań stanowi od lat formalne zagrożenie dla ciągłości działalności polskich firm telekomunikacyjnych. Z groźbą taką konfrontowana jest corocznie część firm. I to niezależnie od jakiejkolwiek operacyjnej potrzeby uprawnionych instytucji.
c. Należy również wyraźnie powiedzieć, że do realizacji czynności operacyjnych w danej sieci, konieczna jest jej znajomość. Nie jest więc rozwiązaniem, choć zmuszonych jest po nie sięgać wielu operatorów, zatrudnianie zewnętrznych „konsultantów ds. bezpieczeństwa przemysłowego", którzy zapewniają formalne bezpieczeństwo firm (z uwagi na nałożone obowiązki ustawowe), ale w praktyce będąc podmiotami zewnętrznymi, nie gwarantują technicznej realizacji ewentualnych działań operacyjnych. *Outsourcing* możliwy jest jedynie przy części zadań, takich jak np. organizacja kancelarii tajnych (jeśli rzeczywiście w segmencie MŚP są one potrzebne – w ocenie KIKE w firmach małych i mikro nie są). Obecna sytuacja powoduje więc ponoszenie istotnych i nieuzasadnionych kosztów przez sektor MŚP, których beneficjentami jest niestety nie interes publiczny kraju, a prywatne firmy konsultingowe i dostawcy wymaganych rozwiązań.

Niestety takie są trudne fakty, z którymi od lat próbujemy się przebić i rozpocząć dialog o kształcie przepisów. Nie chodzi nam bowiem o wyłączenie spod obowiązków sektora MŚP, ale o dostosowanie przepisów do potrzeb i możliwości, z wykorzystaniem dostępnych procedur i wymagań technicznych, które muszą zostać zastosowane w infrastrukturze operatorów.

Przepis art. 180c ust. 2 pkt. 2 ustawy PT zawiera delegację ustawową zgodnie z którą, *„Minister właściwy do spraw łączności w porozumieniu z ministrem właściwym do spraw wewnętrznych, mając*

na uwadze rodzaj wykonywanej działalności telekomunikacyjnej przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych, dane określone w ust. 1, koszty pozyskania i utrzymania danych oraz potrzebę unikania wielokrotnego zatrzymywania i przechowywania tych samych danych, określi, w drodze rozporządzenia (…)

2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych.”. Powyższy zapis (gdyby stanowił zasadę w określaniu obowiązków) mógłby stanowić podstawę do określania wymagań z uwzględnieniem wielkości przedsiębiorstw lub ich sieci. Niestety nawet w tym przypadku wydane na jego podstawie rozporządzenie nie uwzględnia wielkości PT. Ponadto już kolejny artykuł 180d ustawy PT nie przewiduje podobnej delegacji.

Tymczasem wracając na grunt omawianej nowelizacji – podobne do w/w wątpliwości Izby budzą propozycje zmiany przepisów dotyczących zapewniania warunków do kontroli operacyjnej oraz zasad udostępnienia danych telekomunikacyjnych.

Artykuł 19 ust. 12 ustawy o Policji, ma otrzymać następujące brzmienie: *„**Przedsiębiorca telekomunikacyjny**, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia **na własny koszt** warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej”*.

Z kolei art. 20c ust. 2 ustawy o Policji proponuje się w brzmieniu: „*Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną **udostępnia nieodpłatnie** dane, o których mowa w ust. 1: (…)*”

KIKE przy okazji nowelizacji ustawy o Policji (ale także pozostałych ustaw o charakterze kompetencyjnym) wskazuje na istniejące w dalszym ciągu dwa problemy wynikające z powyższych przepisów:

1. przeniesienie w całości kosztów realizacji uprawnień służb na przedsiębiorców telekomunikacyjnych, oraz
2. nie powiązanie w/w obowiązków z realnymi potrzebami uprawnionych instytucji i wielkością (potencjałem gospodarczym) przedsiębiorców telekomunikacyjnych.

Zdaniem Izby koniecznym rozważenia jest zmiana zarówno zasad formułowania obowiązków (z uwzględnieniem potrzeb i powiązania ich z wielkością PT), jak i finansowania udostępniania danych telekomunikacyjnych oraz zapewniania warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję (a także inne upoważnione podmioty) kontroli operacyjnej.

Warto również wskazać, iż z otrzymywanych od operatorów informacji wynika, iż w najczęściej występujących zapytaniach dot. retencji danych, istotna część zapytań zawiera błędy, do których najczęściej zaliczyć trzeba:

a. Przekazywanie zapytań po okresie roku od zdarzenia.
b. Przekazywanie zapytań niekompletnych – np. nie zawierających pełnych sygnatur czasowych, czy kompletu adresów i portów nadawców oraz odbiorców transmisji. Braki w tym zakresie są szczególnie widoczne i kłopotliwe oraz mogą skutkować błędnym wskazaniem abonenta przy dużych ilościach transmisji i sieciach prywatnych maskowanych do wspólnego, pojedynczego adresu publicznego.

Izba podziela powszechnie podnoszone w konsultacjach przekonanie, iż wprowadzenie odpłatności za udostępnienie danych telekomunikacyjnych spowoduje nie tylko ograniczenie liczby wniosków ze strony uprawnionych podmiotów i przyczyni się do zapewniania zasady subsydiarności w

pozyskiwaniu danych, ale ma szansę także poprawić jakość i precyzję formułowanych zapytań. Jest to szczególnie ważne, gdyż odpowiedzi udzielone na nieprecyzyjne pytania mogą skutkować podjęciem czynności wobec niewłaściwych osób.

Izba równocześnie w pełni podziela w tym zakresie stanowisko wyrażone w uchwale nr 10 Rady do Spraw Cyfryzacji w sprawie projektu ustawy nowelizacji ustawy o Policji.

Konkludując powyższy wywód – w efekcie niepowiązania obowiązków z zakresu zapewniania warunków dla kontroli operacyjnej z potencjałem ekonomicznym przedsiębiorców, podobnymi obowiązkami obciąża się zarówno małą sieć wiejską lub osiedlową zarządzaną z prywatnego mieszkania właściciela, jak i duży telekom. Tymczasem inne są nie tylko możliwości techniczne i zasoby sieci (lokalowe, kadrowe i techniczne), ale i różne faktyczne potrzeby służb. Stosowaną praktyką realizacji działań operacyjnych jest jednorazowe dopuszczenie pracowników do danych niejawnych. W małych firmach nie ma bowiem rozbudowanych kadr i działów administracji i bezpieczeństwa sieci. Często funkcje te pełni właściciel lub pojedynczy administrator. Większość małych firm nigdy nie była i prawdopodobnie nie będzie adresatem zapytań operacyjnych służb. W innych przypadkach mają miejsce pojedyncze zdarzenia tego typu w skali lat działalności firmy. W ocenie KIKE istnieje konieczność powiązania obowiązków z realnymi potrzebami służb zależnymi w praktyce od wielkości sieci.

W związku z powyższym, zdaniem KIKE w ramach prowadzonych konsultacji, konieczne jest sporządzenie raportu dotyczącego ilości zapytań o dostęp do danych z retencji i innych działań obejmujących rejestrację i dostęp do korespondencji w zależności od wielkości operatora. Zgodnie z PT, przedsiębiorcy telekomunikacyjni zobowiązani są do składania Prezesowi Urzędu Komunikacji Elektronicznej raportów dotyczących ilości zapytań obejmujących retencję danych. Niestety nie znamy żadnych danych dot. ilości zapytań operacyjnych w zakresie innym, niż retencja. Jednak z naszych wewnętrznych konsultacji wynika, iż firmy mikro i małe w całej historii swojej działalności albo nigdy nie były adresatami działań operacyjnych polegających np. na rejestracji przekazów, albo zdarzenia takie były incydentalne i w praktyce oparte właśnie na pojedynczym dopuszczeniu do udziału w czynnościach.

Innym dobrym przykładem konieczności weryfikacji nakładanych na operatorów obowiązków, jest jeden z przepisów z art. 179 ust. 3 pkt. 1 lit. A wraz z ust. 3b PT od lat już opisywany jest zbiorczo, jako „wymóg utrzymywania 8-stanowiskowej kafejki internetowej" przez każdego operatora i na własny koszt mimo, iż mikro, mali i średni operatorzy statystycznie nie przetwarzają zapytań uzasadniających utrzymywanie tak rozbudowanego obowiązku, ani nie mają fizycznego zaplecza do realizacji tylu równoległych operacji.

W związku z powyższym zdaniem KIKE cytowany powyżej przepis art. 180c pkt. 2 ust. 2 ustawy PT lub podobny, powinien znaleźć się również w Projekcie i stać się podstawą do dookreślenia obowiązków również w kontekście wielkości przedsiębiorstwa, ale także szczegółowych wymagań technicznych (o czym niżej).

Ponadto, dyskutowana nowelizacja powinna w ocenie KIKE stać się przyczyną do szerszej redefinicji w przepisach obowiązków, sformułowanych przede wszystkim pod adresem dużych operatorów i powiązanie obowiązków z wielkością przedsiębiorcy telekomunikacyjnego. Należy wprost zdefiniować możliwość realizacji obowiązków na podstawie jednorazowych zwolnień lub obniżenie kosztów uzyskania świadectwa bezpieczeństwa przemysłowego przez sektor MŚP. Ponadto, należy określić zasady pozwalające na wspólną realizację obowiązków przez grupy operatorów zrzeszone w konsorcja lub izby, gdyż obecnie takie możliwości dotyczą jedynie części z nich.

KIKE rozumiejąc celowość wsparcia przez przedsiębiorstwa telekomunikacyjne uzasadnionej działalności operacyjnej upoważnionych służb, jako jedyna Izba branżowa reprezentująca rynek MŚP, nie może w toczącej się dyskusji pominąć w/w zagadnień nie tylko z uwagi na możliwości małych operatorów, ale i zapewnienie efektywności wsparcia działań operacyjnych tam, gdzie są one rzeczywiście potrzebne.

Celem postulowanych przez KIKE prac nie jest jednak wyłączenie MŚP z realizacji omawianych obowiązków, a wręcz przeciwnie – zapewnienie realnych względem potrzeb ram realizacji tych obowiązków w sposób równocześnie możliwy do spełnienia przez cały rynek obejmujący również, także kluczowy dla polskiej gospodarki segment MŚP.

II. Zabezpieczenie bezpieczeństwa i poufności przekazywanych danych

Kolejną wątpliwość Izby w zakresie zapewnienia bezpieczeństwa i poufności przekazywanych danych budzi proponowany przepis art. 20c ust. 3 i 4, zgodnie z którym:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.

4. Udostępnienie Policji danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:

a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,

b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;

2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.”

Proponowane przepisy nie definiują ani sposobu zabezpieczenia danych, ani tym bardziej formy autoryzacji osoby uzyskującej dane.

Zgodnie z powyższym artykułem, zarówno wszyscy świadczący bezpośrednio, jak i pośrednio usługi internetowe (m.in. wydawcy i właściciele portali internetowych, sprzedawcy internetowi, portale aukcyjne, portale wideo, administratorzy portali społecznościowych, czy randkowych) podlegają temu obowiązkowi, jednak nie wskazano w niniejszym Projekcie na jakich zasadach ma się to odbywać.

Zdaniem KIKE, wydaje się wskazane, iż podstawą tego typu systemu powinny być rozwiązania podobne np. do zastosowanych w PLI CBD (certyfikaty, baza danych, tunele VPN), z tym że **koniecznym jest** nie tylko zabezpieczenie przez stronę publiczną narzędzi do realizacji bezpiecznej i autoryzowanej komunikacji wskazanej w w/w przepisach, ale również zakresu danych w ten sposób udostępnianych, a dla zdalnej rejestracji transmisji – również wymaganych i realnie osiągalnych parametrów transmisji do zewnętrznych serwerów rejestrujących. W sytuacji, gdy na rynku oferowane są już dziś pakiety o przepustowości od kilkaset Mb do 1 Gb, zarówno pasmo, jak i potencjał konieczny do szyfrowania, a nawet transmisji tak dużych strumieni danych od grup abonentów, nie mogą być pominięte milczeniem. Niestety po raz kolejny zaskakuje nas brak refleksji w zakresie

technologicznych wymagań dla rejestracji np. 100Mb strumienia danych. Spróbujmy więc w największym uproszczeniu przybliżyć jedynie dwie najprostsze konsekwencje w/w zapisu dla wymagań technicznych.

a. Wymagania w zakresie pasma. Dla zapewnienia możliwości rejestracji zdalnej lokalizacji transmisji pojedynczego abonenta dysponującego pakietem szerokopasmowym o przepustowości powyżej 100 Mb, koszt pojedynczego łącza punkt-punkt (od operatora do pojedynczej instytucji) wynosi od kilkuset do tysiąca kilkuset złotych plus koszty budowy stosownego przyłącza. Stałe utrzymywanie sieci takich łączy od 4 tysięcy operatorów do wszystkich uprawnionych instytucji tworzyłoby więc obciążenia rzędy ok. 40 mln złotych miesięcznie (licząc ostrożnie 4 tys. operatorów x 1000 zł x w zaokrągleniu 10 instytucji). Z kolei czas zestawienia łącza na żądanie służby może wynieść i kilka miesięcy procesu inwestycyjnego. Konieczne jest więc wypracowanie rozsądnej procedury operacyjnej i rozważenie rejestracji w siedzibie operatora.
b. Rejestracja danych wymaga jednak dużych zasobów dyskowych. Transmisja 100 Mb/s (bity są wykorzystywane dla określenia prędkości transmisji), to ok. 12,5 MB/s (Bajty z kolei stanowią podstawę określania pojemności dysków). Jeśli rejestrowany abonent zapewni stały strumień danych, w ciągu godziny wygeneruje 45GB zapisu, a w jeden dzień – 1 TB. TeraBajty są jednostkami pojemności dużych dysków twardych. Zasoby techniczne i koszty rejestracji tak dużej ilości danych są więc znaczne już na poziomie pojedynczego abonenta. Problem będzie narastał wraz ze wzrostem ilości przesyłanych danych (w tym zwykłych transmisji multimedialnych, jak IPTV i VoD w których łatwo ukryć inne dane), gdyż operator rejestrować musi całość przekazu, nie wnikając w jego zawartość. Koszt 2-tygodniowej rejestracji może być więc znaczny już dla pojedynczego abonenta. A doświadczenie uczy, iż po rejestracji wykorzystane do niej dyski, prawdopodobnie mogłyby być zabezpieczane (pobierane) przez upoważnione służby, co uniemożliwia ich wykorzystanie w kolejnych przypadkach rejestracji.

Jeśli procedury przewidziane w nowelizacji miałyby wyglądać inaczej, niż w w/w punktach, to nie wynika to z treści omawianej noweli.

III. Kontrola udostępniania danych przez niezależny organ

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) uznał za niezgodne z Konstytucją przepisy m.in. ustawy o Policji, w zakresie w jakim nie przewidują one kontroli udostępniania danych telekomunikacyjnych przez niezależny od podmiotów żądających udostępnienia dane organ – najlepiej sąd. Tymczasem Projekt w zakresie kontroli udostępniania danych zakłada jedynie przekazywanie przez organy Policji właściwemu sądowi okręgowemu, co pół roku sprawozdania, które obejmować będzie liczbę przypadków w których zwrócono się o udostępnienie danych wraz z określeniem kwalifikacji prawnej czynów, w związku z zaistnieniem których wystąpiono o te dane.

Sąd okręgowy wyznaczony do przeprowadzenia kontroli, **może** w ramach swoich uprawnień zapoznać się z „*materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych* (…)", rezultatem czego mają być wyniki kontroli przekazywane przez ten sąd organowi Policji. Na przekazaniu wyników kontroli, rola sądu w toku weryfikacji poprawności udostępniania danych telekomunikacyjnych w zasadzie się kończy.

Projekt przewiduje zatem kontrolę o **charakterze fakultatywnym**, bez nadania sądom uprawnień o charakterze nadzorczym. Brak jest bowiem określenia dalszych działań sądu lub innego organu w

przypadku wykrycia, że udostępnienie danych miało miejsce niezgodnie z obowiązującymi przepisami.

Z tą ostatnią obawą Izby wiąże się również wątpliwość odnośnie proponowanego modelu **następczej kontroli sądu** w każdym przypadku. Zasadniczo bowiem, zdaniem KIKE kontrola sądu powinna przybrać charakter kontroli uprzedniej. Z kolei kontrola następcza sądu mogłaby mieć zastosowanie w wymagających działania Policji i pozostałych służb przypadkach niecierpiących zwłoki. Uprzednia kontrola sądu przyczyniłaby się zapewne także do zwiększenia poprawności formułowania przez organy Policji i inne służby wniosków, które kierowane są do przedsiębiorców telekomunikacyjnych w związku z udostępnieniem danych.

Wprowadzenie modelu kontroli uprzedniej sądu w zakresie uzyskania dostępu do danych telekomunikacyjnych mogłaby zostać również wykorzystana dla wprowadzenia **zasady subsydiarności pozyskiwania danych**, tj. sytuacji gdzie warunkiem dostępu do danych będzie wyczerpanie przez Policję i inne służby pozostałych środków prawnych, które mniej oddziałują na sferę prywatności oraz tajemnicę komunikowania się.

Pomimo tego, że Trybunał Konstytucyjny nie wskazał jak z punktu widzenia zgodności z Konstytucją powinien prezentować się przebieg kontroli nad udostępnianiem danych telekomunikacyjnych, rola sądu w przedstawionej w Projekcie procedurze sprawia, że obowiązek wdrożenia kontroli ze strony niezależnego organu może przybrać jedynie pozorny charakter, a przedsiębiorcy telekomunikacyjni w dalszym ciągu będą zasypywani wnioskami o udostępnienie danych, których w istocie nie przetwarzają i nie mają obowiązku przetwarzać. Dodatkowo wnioski te dotyczyć będą mogły w zasadzie każdego rodzaju zdarzeń, bez ograniczenia ich do katalogu spraw, które mogłyby uzasadniać ingerencję w sferę prywatności i tajemnicy komunikowania się.

Analogiczne do omawianych powyżej propozycji zmian wprowadzane są również do innych ustaw o charakterze kompetencyjnym, (m.in. ustawy o Straży Granicznej - art. 10b, ustawie o kontroli skarbowej - art. 36b itd.).

O konieczności wprowadzenia realnych mechanizmów kontroli wykorzystywania danych telekomunikacyjnych i internetowych, uwzględniania zasady subsydiarności oraz określenia katalogu spraw, w których uprawnione podmioty mogą pozyskiwać dane telekomunikacyjne zwraca również uwagę Rada do Spraw Cyfryzacji w swojej uchwale nr 10 dotyczącej projektu nowelizacji ustawy o Policji.

IV. Podsumowanie

W uzasadnieniu do Projektu w pkt 4 „*Wstępna ocena skutków regulacji*" w związku z uchyleniem art. 180g ustawy PT, wskazane zostały wyłącznie pozytywne skutki dla operatorów, pomijając negatywne skutki w zakresie zapewnienia na własny koszt realizacji licznych czynności operacyjnych oraz braki w zakresie opracowania i wprowadzenia zasad utrwalania transmisji i komunikatów do wyniesionych lokalizacji zdalnych. W podsumowaniu wskazuje się jedynie, że *„nowelizacja może przyczynić się do wzrostu wydatków z budżetu państwa związanego z nałożonym na sądy okręgowe zadaniem kontroli pozyskiwania przez uprawnione służby danych (...)"(*str. 65) oraz *„wskutek likwidacji tego* (art. 180g ustawy PT) *obowiązku zmniejszeniu ulegnie także liczba obciążeń administracyjnych nałożonych na przedsiębiorców telekomunikacyjnych, co spowoduje niewielki spadek kosztów ich działalności."* **Jednak należy wskazać, że w wyniku proponowanej nowelizacji ustawy PT całość kosztów związanych z udostępnianiem i przesyłaniem danych upoważnionym instytucją ponosić będą**

wyłącznie operatorzy. Tym samym należy uznać ocenę skutków regulacji za niepełną, zaś w odniesieniu do przedsiębiorców telekomunikacyjnych – błędną.

Mając na uwadze powyższe zastrzeżenia, w ocenie Izby wniesiony do Sejmu Projekt nie stanowi dostatecznej realizacji wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w szczególności poprzez brak realnej kontroli ze strony niezależnego od podmiotów żądających udostępniania danych telekomunikacyjnych organu. Proponowany model kontroli w ocenie KIKE jest rozwiązaniem jedynie pozornym, który nie stworzy należytego systemu weryfikacji poprawności udostępniania danych telekomunikacyjnych.

Dodatkowo nowelizacja ustaw kompetencyjnych oraz ustawy Prawo telekomunikacyjne stanowi dogodny moment na dostosowanie obowiązków MŚP w zakresie przechowywana i udostępniania danych telekomunikacyjnych do ich rzeczywistych możliwości i uzależnienie niektórych spośród obowiązków od potencjału ekonomicznego jaki reprezentują poszczególni przedsiębiorcy telekomunikacyjni.

Z poważaniem

Piotr Marciniak

V-ce Prezes KIKE

Grupa Robocza ds.
Administracji Publicznej KIKE