



# Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dnia 6 października 2021 roku  
KIGEiT/1796/10/2021

Szanowny Pan Jacek Oko  
Prezes  
Urząd Komunikacji Elektronicznej  
ul. Giełdowa 7/9  
01-211 Warszawa

## Stanowisko w sprawie określenia lokalizacji punktu zakończenia sieci w różnych topologiach sieci

*Szanowny Panie Prezisie,*

wynikający z art 61 ust. 7 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1992 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: „EKŁE”) obowiązek, nałożony na krajowe organy regulacyjne w zakresie określenia lokalizacji punktu zakończenia sieci, uwzględniając w jak największym stopniu wytyczne Organu Europejskich Regulatorów Łączności Elektronicznej (dalej „BEREC”) dotyczące wspólnych podejść<sup>1</sup> (dalej: „Wytyczne”), daje Prezesowi Urzędu Komunikacji Elektronicznej (dalej: „Prezes UKE”) uprawnienie do wskazania punktu granicznego pomiędzy publiczną siecią telekomunikacyjną będącą własnością przedsiębiorcy a należącą do użytkownika końcowego siecią prywatną, w szczególności należącymi do niego urządzeniami. Przedmiotowe zagadnienie związane jest z szeregiem uwarunkowań wymienionych w Wytycznych, w tym z koniecznością zapewnienia interoperacyjności, prostoty operacji i bezpieczeństwa sieci i urządzeń, a konsekwencje wyznaczenia punktu zakończenia sieci (dalej: „NTP”) będą miały wpływ na dużą część rynku obejmującą w szczególności użytkowników, dostawców usług, operatorów sieci oraz producentów i dystrybutorów urządzeń.

W pierwszej kolejności należy podkreślić, że z treści omawianego przepisu (art. 61 ust. 7 EKŁE) jednoznacznie wynika, że krajowy organ regulacyjny – Prezes UKE, w przypadku określenia lokalizacji NTP uwzględnia różne topologie sieci: „*ust. 7. Do dnia 21 czerwca 2020 r., aby przyczynić się do spójnego określania przez krajowe organy regulacyjne lokalizacji punktów zakończenia sieci, BEREC, po odbyciu konsultacji z zainteresowanymi stronami oraz w ścisłej współpracy z Komisją, przyjmie wytyczne w sprawie wspólnych podejść do określania punktu zakończenia sieci w różnych topologiach sieci. Krajowe organy regulacyjne w jak największym stopniu uwzględniają te wytyczne przy określaniu lokalizacji punktów zakończenia sieci*”.

Literalna wykładnia omawianego przepisu zakłada, że EKŁE nie uznaje za właściwe by zasadnym było przyjęcie jednego rozwiązania dla każdej topologii sieci. Powyższe wynika z zastosowania zwrotów „wspólnych podejść” oraz „różnych topologiach sieci”.

Warto zwrócić uwagę, że art. 2 pkt 9 EKŁE definiując „punkt zakończenia sieci” wskazuje, że jest to fizyczne miejsce, w którym użytkownik końcowy otrzymuje dostęp do publicznej sieci łączności

<sup>1</sup> BEREC guidelines on common approaches to the identification of the network termination point in different network topologies 5.03.2020, BoR (20)46.

elektronicznej i które w przypadku sieci stosujących przełączanie lub przekierowywanie identyfikuje się za pomocą konkretnego adresu sieciowego i może być łączone z numerem lub nazwiskiem użytkownika końcowego. Podkreślenia wymaga, że w świetle EKŁE, NTP nie może znajdować się w miejscu uniemożliwiającym jednoznaczny identyfikację użytkownika końcowego, będącego beneficjentem usług łączności elektronicznej. Powyższe ma szczególne znaczenie, w sytuacji gdy tzw. ostatnia mila jest wybudowana w oparciu o współdzielone przez wielu użytkowników medium. Zatem, o miejscu zakończenia sieci, według EKŁE, decyduje kwestia dostępu do sieci, a w przypadku różnych technologii i topologii sieci nie można zakładać istnienia wyłącznie jednego, wspólnego miejsca, w którym użytkownik otrzymuje dostęp do usług danego dostawcy/operatora.

Ponadto, analiza dokumentów konsultacyjnych dotyczących przyjętych 10 marca 2020 roku Wytycznych wskazuje, że byłyby one niepotrzebne, gdyby zdefiniowanie lokalizacji NTP miało nastąpić w jednym, określonym miejscu bez względu na okoliczności. BEREC jednoznacznie wskazał, że wybór technologii świadczenia usług łączności elektronicznej przez operatora telekomunikacyjnego należy wyłącznie do decyzji operatora i wszelkie obiektywnie istniejące wymagania technologiczne wpływające na uznanie, że punkt zakończenia sieci przynależy do domeny operatora wynikają właśnie z tej biznesowej decyzji. Powyższe sugeruje jednoznacznie, że wolność wyboru technologii świadczenia usług łączności elektronicznej ma duży wpływ na to, w jakim miejscu użytkownik końcowy otrzymuje dostęp do publicznej sieci łączności elektronicznej. Wytyczne BEREC nie wyznaczają w sposób bezwzględny definicji lokalizacji zakończenia sieci. Tym bardziej nie definiują jednego podejścia dla wszystkich możliwych technologii sieci publicznych. Wskazują jedynie możliwe kierunki działań regulacyjnych w tej kwestii, podkreślając konieczność uwzględnienia istnienia obiektywnych technologicznie wymogów (konieczności), uzasadniających by wybór sprzętu końcowego przez użytkownika końcowego nie był nieograniczony.

Prezes UKE wyznaczając NTP powinien mieć na uwadze spodziewany rozwój rynku urządzeń CPE (Customer Premises Equipment), z uwagi na wprowadzanie kolejnych elementów systemu IoT oraz dążenie do zapewnienia wsparcia technicznego, szybkiego usuwania awarii i usterek tych urządzeń oraz komfortu użytkowania i bezpieczeństwa.

Wskazanie lokalizacji NTP będzie wymagało przeprowadzenia szerokich konsultacji i pogodzenia często przeciwstawnych interesów zainteresowanych podmiotów, a także zagwarantowania respektowania przepisów krajowych, w tym praw nabytych. Wprowadzenie jakichkolwiek rozstrzygnięć kwestii identyfikacji lokalizacji punktu zakończenia sieci powinno zostać poprzedzone analizą polskiego rynku dostawców i producentów sprzętu telekomunikacyjnego. W szczególności analiza taka powinna dotyczyć poziomu konkurencyjności tego rynku. Należy mieć na względzie, że rynek producentów sprzętu telekomunikacyjnego w zakresie sprzętu operatorskiego notuje wzrost sprzed pandemii, a w zakresie sieci szkieletowych analitycy prognozują w najbliższym czasie nawet dwu cyfrowe wzrosty przychodów producentów sprzętu. Nie ulega wątpliwości, że konkurencyjność na rynku sprzętu telekomunikacyjnego nie istniałaby gdyby nie operatorzy, którzy de facto dzięki dostarczaniu swoich usług kreują popyt na sprzęt telekomunikacyjny każdego rodzaju.

Z uwagi na zasadę neutralności technologicznej wyznaczenie lokalizacji NTP nie będzie zapewne uzależnione od medium, za pomocą którego usługa jest dostarczana do lokalu użytkownika końcowego, a co za tym idzie NTP powinien być wyznaczony w miejscu, w którym każda z usług, obojętnie w jakiej technologii dostępowej jest świadczona, jest możliwa technicznie do realizacji nie powodując problemów z interoperacyjnością i bezpieczeństwem sieci i danych oraz przy ograniczeniu kosztów przyjętych rozwiązań. Jeśli lokalizacja NTP mogłaby być uzależniona od rodzaju linii dostępowej (kabel miedziany, światłowodowy, Ethernetowy czy koncentryczny)

podział na punkt A i C wynikałby z możliwości stosowania własnych urządzeń przez użytkownika końcowego i określałby zakończenie publicznej sieci w punkcie A dla usług xDSL i Ethernet oraz w punkcie C dla PON i HFC. Oczywistym wydaje się, że nie należy wyznaczać lokalizacji NTP w zależności od rodzaju świadczonej usługi, ponieważ mogłoby to spowodować uznanie, że w niektórych przypadkach modem lub router mógłby być częścią publicznej sieci telekomunikacyjnej i jednocześnie nią nie być w stosunku do innej usługi. Natomiast faktem jest, że techniczne uwarunkowania mają istotny wpływ na łatwość podłączenia urządzeń, bezpieczeństwo sieci i usług oraz możliwość łatwej diagnostyki czy naprawy urządzeń. W celu uniknięcia wymienionych niżej problemów wydaje się, że optymalną lokalizacją zakończenia sieci jest punkt C (C2) wskazany w Wytycznych.

Obecnie, w większości przypadków wymienionych w aneksie do Wytycznych punkt zakończenia sieci jest zlokalizowany w C lub B, jedynie w przypadku starszych technologii dostępowych opartych o kable miedziane i Ethernet, możliwe jest stosowanie własnych urządzeń i za zakończenie sieci publicznej można uznać punkt A.

Niezależnie od powyższego, Izba podnosi, że podstawą podjęcia prac nad określeniem lokalizacji NTP jest zbadanie potrzeb i preferencji klientów w zakresie odpowiedzialności za zapewnienie sprzętu abonenckiego umożliwiającego dostęp do usług telekomunikacyjnych. Prace nad określeniem lokalizacji NTP powinny opierać się o przejrzyste dane w zakresie ilości reklamacji podnoszących kwestię zapewniania urządzeń typu modemy i routery. Warto również pochylić się nad analizą świadomości i wiedzy klientów w zakresie sprzętu telekomunikacyjnego służącego do korzystania z usług telekomunikacyjnych, zasad jego obsługi, aktualizacji oraz zasad zabezpieczeń. Powyżej wskazane dane, w ocenie Izby, będą bazą pozwalającą ocenić zapotrzebowanie użytkowników końcowych na identyfikację lokalizacji punktu zakończenia sieci w sposób uwzględniający ich interesy w zakresie korzystania z usług łączności elektronicznej.

Należy również zauważyć, że istotnym zagadnieniem związanym z identyfikacją lokalizacji NTP jest rozstrzygnięcie sporów konsumenckich na linii konsument – operator, w przypadku ewentualnego dopuszczenia do swobodnego i niczym nieograniczonego wyboru przez klienta urządzeń umożliwiających dostęp do sieci operatora. Na tym gruncie Izba dostrzega wątpliwość czy Prezes UKE nie powinien uznać za zasadne dokonanie zmian procedur związanych z rozstrzygnięciem sporów konsumenckich przez Regulatora. Warto zauważyć, że pojawiające się na tym tle spory konsumenckie (m.in. w zakresie dyskryminacji abonentów z uwagi na korzystanie z własnego sprzętu abonenckiego co do zasad obsługi awarii), które zostały przekazane do rozstrzygnięcia krajowemu organowi regulacyjnemu, w niektórych państwach (Niemcy) długo oczekują na rozstrzygnięcie z uwagi na problem określenia granic odpowiedzialności pomiędzy użytkownikiem końcowym a operatorem.

Przedstawiając swoje stanowisko w sprawie identyfikacji NTP, Izba pragnie wskazać, na istnienie obiektywnych technologicznie wymogów uzasadniających określenie lokalizacji NTP w taki sposób, aby to dostawca usług był odpowiedzialny za zapewnienie sprzętu telekomunikacyjnego umożliwiającego skorzystanie z jego usług przez użytkowników końcowych. Jak wynika z Wytycznych BEREC, obiektywna technologicznie konieczność skorzystania przez użytkownika końcowego wyłącznie ze sprzętu zapewnianego przez dostawcę usług wynika z modelu technologicznego w jakim operuje dany dostawca usług i jest tym samym w pełni uzasadnione by dostawca usług był jednocześnie wyłącznym dostawcą sprzętu abonenckiego.

W ocenie Izby istnieje kilka wskazanych poniżej zagadnień, które należy uznać za obiektywne technologicznie wymogi uzasadniające taką identyfikację lokalizacji NTP by to dostawca usług był odpowiedzialny za zapewnienie sprzętu abonenckiego

## 1. Bezpieczeństwo sieci

- Eliminowanie naruszeń

Głównym zagrożeniem, jakie może wynikać z określenia lokalizacji NTP w punkcie A wskazanym w Wytycznych, jest potencjalnie zwiększone ryzyko naruszenia bezpieczeństwa sieci i danych użytkowników. Wpływ urządzeń niezabezpieczonych lub celowo wykorzystywanych w celu uszkodzenia sieci może mieć negatywne skutki dla pozostałych użytkowników tej sieci, jak i jej operatora. Stosowane przez dostawców usług i operatorów sieci zabezpieczenia i szyfrowanie przesyłanych komunikatów są zoptymalizowane pod kątem użycia z dostarczającymi urządzeniami a wykorzystywanie sprzętu własnego użytkowników końcowych nie daje gwarancji zabezpieczenia. Korzystanie z własnych urządzeń (w szczególności modemów i routerów) przez użytkowników końcowych często wiąże się z uchybieniami w aktualizacji ich oprogramowania, gdyż stopień technicznej znajomości zagadnień, umożliwiający konfigurację własnego routera, często nie wystarcza do jego aktualizacji. Operator sieci dysponujący wykwalifikowaną kadrą oraz spełniający kryteria wymagane przez przepisy dotyczące bezpieczeństwa sieci i usług oraz cyberbezpieczeństwa w zakresie przeciwdziałania zagrożeniom, jest zobowiązany m.in. do zapewnienia i stosowania środków minimalizujących skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo lub integralność sieci lub usług, a także monitoruje sieć w celu wykrycia naruszeń bezpieczeństwa. Naruszenie tych wymagań zagrożone jest wysokimi karami, więc należy przypuszczać, że przedsiębiorcy telekomunikacyjni kładą duży nacisk na kwestie bezpieczeństwa własnej infrastruktury.

Izba zwraca uwagę, że przeniesienie odpowiedzialności za naruszenia bezpieczeństwa sieci i danych użytkowników na użytkownika końcowego (jak ma to miejsce w Holandii oraz Niemczech) może narazić klientów na kosztowne procesy odszkodowawcze, z uwagi na możliwość naruszenia ochrony danych nie tylko sieci dostawcy usług ale również i innych użytkowników usług telekomunikacyjnych. Należy wskazać, że analitycy tematu wskazują na bardzo niski poziom zabezpieczeń routerów zakupionych przez użytkowników końcowych na wolnym rynku<sup>2</sup>. Dodatkowo warto wskazać, że w Niemczech, klienci będąc odpowiedzialni za naruszenie bezpieczeństwa sieci i ochrony danych są zobowiązani do wypłaty odszkodowań i są narażeni na możliwość odłączenia im usług telekomunikacyjnych za zgodą organu regulacyjnego, a w sytuacjach awaryjnych i nadzwyczajnych dostawca usług ma możliwość odłączenia klienta bez zgody regulatora.

- Wyłączenie urządzenia

Istotnym zagadnieniem związanym z bezpieczeństwem sieci jest możliwość opcjonalnego odłączenia urządzenia będącego własnością użytkownika końcowego od sieci w określonych przypadkach. Bez specjalnej procedury, opartej na przepisach prawa, nie jest możliwe odłączenie urządzenia powodującego zakłócenia sieci nawet w momencie ich wykrycia. W przypadku, gdy urządzenie końcowe jest własnością operatora i stanowi element publicznej sieci, odłączenie i wymiana zainfekowanego urządzenia nie powoduje większych problemów.

- Dostęp i utrwalanie

Kolejny problem dotyczy zapewnienia możliwości kontroli informacji przesyłanej w sieci telekomunikacyjnej oraz danych związanych z kontrolowaną informacją. W sytuacji, gdy publiczna sieć będzie zakończona w punkcie A, wiele danych będzie niedostępnych dla uprawnionych podmiotów co w sposób oczywisty ma wpływ na bezpieczeństwo państwa.

---

<sup>2</sup> [https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity\\_2020\\_Bericht.pdf](https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf)

- Spoofing

W przypadku punktu A ułatwiona jest dodatkowo inna działalność mająca na celu wprowadzenie w błąd odbiorcy przekazu. Spoofing, polegający na podmianie identyfikatora numeru dzwoniącego jest jednym z nadużyć telekomunikacyjnych, które w przypadku ograniczenia kontrolowanej przez operatora sieci publicznej do minimum (w szczególności punktu A) będzie się nasilało.

Można przyjąć, że przypadki blokowania dostępu do usług przez użytkownika końcowego występowałyby znacznie częściej niż obecnie w związku z jego działaniami lub podejrzeniami o naruszenie integralności sieci operatora.

### 2. Zapewnienie interoperacyjności pomiędzy siecią operatora a TTE

W przypadku, gdy wymagane jest zapewnienie interoperacyjności pomiędzy siecią operatora a modemem i pozostałymi urządzeniami należącymi do użytkownika końcowego (punkt A), w stosunku do niektórych usług stosowane są autorskie rozwiązania, niedostępne na rynku masowym co powoduje, że w przypadku lokalizacji NTP w punkcie A nie ma możliwości zapewnienia interoperacyjności. Rozwiązanie takie zwiększa również koszty obsługi użytkownika końcowego.

W przypadku zlokalizowania NTP w punkcie A, zapewnienie interoperacyjności dotyczyć będzie urządzeń (router, modem, media box) użytkownika oraz technologii dostępowej stosowanej na linii abonenckiej, co powinno być uszczegółowione w specyfikacji technicznej każdego zakończenia sieci. Wybór lokalizacji NTP na punkcie B lub C pozwala na określenie standardowych specyfikacji technicznych urządzeń w celu zapewnienia interoperacyjności tylko pomiędzy nimi. Można przyjąć, że ze względu na mniejszą liczbę standardów urządzeń, mniejsza liczba problemów będzie dotyczyła tego przypadku niż lokalizacja NTP w punkcie A.

### 3. Problem sieci HFC

Wytyczne opisują problem występujący w sieciach kablowych, którego przyczyną jest fakt, że sygnał elektryczny, który przenosi informacje dla jednego klienta w sieci, jest również fizycznie obecny w kablach koncentrycznych, które wchodzą do domów wszystkich innych klientów podłączonych do tego samego węzła światłowodowego. W upstream sygnały ze wszystkich modemów są łączone na stacji czołowej. Jeśli jeden modem nadaje z niewłaściwym czasem, częstotliwością lub poziomem mocy, powoduje to zakłócenia w usługach odbieranych przez wszystkie inne modemy w tym węźle światłowodowym. W związku z tym potrzebna jest zaawansowana synchronizacja, a wszystkie urządzenia podłączone do sieci muszą respektować reguły transmisji. Wymaga to silnego uwierzytelnienia urządzenia, aby zidentyfikować je w publicznej sieci. Jest to głównym powodem stosowania urządzeń dedykowanych do tych usług i zmodyfikowanych do użycia w sieci konkretnego operatora. Stosowanie dowolnych modemów HFC jest działaniem nie rekomendowanym przez operatorów sieci. W celu ochrony prywatności użytkowników i bezpieczeństwa ich komunikacji oraz sieci, zaimplementowano silne mechanizmy szyfrowania i uwierzytelniania. Ponadto, tylko specjalnie zaprojektowane oprogramowanie operatora jest dozwolone do instalacji w modemach. W celu poprawnej identyfikacji modemu kablowego, a co za tym idzie konkretnego klienta wykorzystywany jest adres MAC modemu. Adres ten umożliwia prawidłowe podłączenie klienta do usług dostawcy i świadczenia ich zgodnie z zawartą umową. Mac adres modemu zabezpieczony jest kluczem. Jeśli siła szyfrowania jest osłabiona, hakerzy mogą to wykorzystać do działań, w przypadku których trudno jest zidentyfikować sprawcę.

### 4. Współpraca hurtowa

Analizując temat możliwości zdefiniowania lokalizacji NTP nie można pominąć sytuacji, w których dostawcy usług świadczą usługi detaliczne w oparciu o umowy hurtowe, będąc niejednokrotnie

uzależnionymi od wynikających z tych umów wymagań. W jednym z krajów UE (Grecja), w którym lokalizację NTP określono również dla usług hurtowych, odnotowano przypadek, gdy zmiana technologii w sieci operatora hurtowego (na vectoring) wpłynęła negatywnie na interoperacyjność urządzeń użytkowników końcowych operatorów alternatywnych. Operatorzy korzystający z sieci operatora hurtowego nie mieli możliwości świadczenia usług swoim klientom. Operator hurtowy musiał wstrzymać się z wprowadzeniem zmian technologicznych do czasu dostosowania urządzeń klienckich u operatorów korzystających. Operator SMP zmieniając technologię świadczenia usług dla operatorów alternatywnych uniemożliwił im świadczenie usług abonenckich z uwagi na brak zapewnienia interoperacyjności klienckich urządzeń końcowych. W sytuacji, gdy polski rynek telekomunikacyjny opiera się w znacznym zakresie na współpracy hurtowej, w tym w oparciu o usługi przedsiębiorców telekomunikacyjnych korzystających z Programu Operacyjnego Polska Cyfrowa, kwestia interoperacyjności i kompatybilności urządzeń klienckich ma podstawowe znaczenie dla identyfikacji NTP z uwzględnieniem różnych rozwiązań technologicznych.

### 5. Licencje

Wykorzystywanie licencji na nadawanie określonych kanałów TV powoduje, że w niektórych przypadkach nadawcy ograniczają możliwość przesyłania treści wyłącznie do własnej sieci operatora. Postanowienia umowne zakazują wprost dystrybucji sygnału przez elementy sieci nie będące własnością podmiotu zobowiązanego do ochrony przed nieuprawnionym dostępem. Kary przewidziane w umowach, szczególnie z nadawcami spoza UE są horrendalne i w efekcie przyjęcia niekorzystnych, z punktu widzenia operatora i dostawcy usług, regulacji, będą miały wpływ na ograniczenie treści dla użytkowników końcowych lub wymuszą stosowanie dodatkowych zabezpieczeń, co podniesie koszty świadczenia usług.

Dla niektórych usług, takich jak IPTV, lokalizacja NTP w punkcie A oznacza wręcz brak możliwości świadczenia usług, ponieważ przez dostawców treści wymagana jest zamknięta sieć uniemożliwiająca kontrolę dostępu do chronionych prawem i umowami treści. Odpowiedni poziom szyfrowania, możliwy do osiągnięcia jedynie na preinstalowanych urządzeniach jest wymagany przez dostawców treści w zamian za możliwość świadczenia usług dostarczania ich w technologii IPTV. Wskazanie zakończenia sieci publicznej w punkcie A spowoduje zatem, na obecnym etapie rozwoju rynku przy założeniu konsekwentnej postawy dostawców *contentu* wobec treści umów, że niemożliwym stanie się świadczenie usług telewizji przez sieci internetowe (IPTV) i sieci kablowe.

### 6. Koszty

Obecne rozwiązania stosowane przez operatorów i dostawców w przypadku usług, dla których wykorzystywany jest modem, router czy inne urządzenie dostarczane wraz z usługą są zoptymalizowane pod kątem provisioningu, a więc każda zmiana tego modelu będzie wymagała oszacowania dodatkowych kosztów związanych z podłączeniem, utrzymywaniem, rozwiązywaniem problemów i usuwaniem awarii. Przyjęty model świadczenia usług w oparciu o sprzęt należący do operatora zapewnia odpowiednią marżę przy efekcie skali, niskie koszty operacyjne oraz daje wystarczająco wysoki poziom wydajności i bezpieczeństwa co nie będzie możliwe do osiągnięcia w przypadku, gdy NTP będzie zlokalizowany w punkcie A, a użytkownik będzie wymagał wsparcia przy korzystaniu z własnych urządzeń.

### 7. Usuwanie awarii

Przyczyną stosowania urządzeń operatora jest szybkość usuwania awarii i łatwość obsługi zgłoszeń przez Zespoły wsparcia technicznego. Wyeliminowanie usterek sprzętu wymaga znajomości ich technicznych specyfikacji oraz kodów dostępu. W przypadku dużej liczby urządzeń na rynku zapewnienie ich kompatybilności jest zadaniem skomplikowanym. Ponadto, użytkownik końcowy,

który jest odpowiedzialny za własne urządzenia może nie dysponować odpowiednim przygotowaniem technicznym koniecznym do podłączenia i uruchomienia usług. Odpowiedzialność operatora sieci kończy się w NTP a brak jest przepisów umożliwiających wypowiedzenie umowy w sytuacji, gdy została ona dostarczona do tego punktu a mimo tego użytkownik nie potrafi z niej skorzystać.

Można również przyjąć, że naprawa usterek w większości przypadków, gdy umożliwiony zostanie wybór dowolnego urządzenia przez użytkownika końcowego, będzie wiązała się z koniecznością wizyty technika, który dokona naprawy lub stwierdzi, że wina leży po stronie urządzenia użytkownika. Obecnie większość napraw wykonywanych jest zdalnie.

Ponadto, nie ma obecnie możliwości dokonania analizy kosztów jakie operatorzy będą musieli ponieść w związku ze zwiększoną ilością skarg, reklamacji i zgłoszeń awarii w sytuacji, gdy to klient będzie wyłącznie odpowiedzialny za dostarczenie sprzętu w celu skorzystania z usług u danego operatora. Podobnie nie można dzisiaj określić skali zaangażowania finansowego klientów w sytuacji, gdy konieczna będzie naprawa lub wymiana sprzętu abonenckiego w przypadku jego degradacji lub konieczności dokonania aktualizacji do nowych standardów usług.

### 8. Komfort

Przywiązanie klientów do ułatwień stosowanych na etapie aktywacji i w trakcie korzystania z usług wykorzystujących zoptymalizowany sprzęt dostarczany przez operatora powoduje, że zapewnienie możliwości wykorzystywania dowolnych urządzeń przez znikomy odsetek użytkowników chcących skorzystać ze swojego uprawnienia, ma wpływ na wzrost kosztów świadczenia usług dla pozostałych. Jako analogię można wskazać na rynek systemów operacyjnych na urządzenia mobilne jako odzwierciedlający podobne problemy. Urządzenia obsługiwane przez system iOS są niemal perfekcyjnie skonfigurowane, łącząc się między sobą w sposób niewymagający zaangażowania ich użytkownika, zapewniają duże poczucie komfortu oraz są aktualizowane regularnie, szybko i przez długi okres czasu od ich produkcji. Jako opozycja wobec nich występuje system Android z ogromną liczbą różnorodnych urządzeń, które przestały być aktualizowane i ich używanie po kilku latach jest uciążliwe, więc stanowią problem dla użytkowników i środowiska.

- usługi FON/WiFREE.

Jeśli NTP będzie określony w punkcie A, to operator publicznej sieci przy wykorzystaniu urządzeń użytkownika końcowego świadczyć będzie usługę dla podłączonych do WiFi użytkowników zewnętrznych. Tworzona jest sieć bezprzewodowa, do której dostęp mają anonimowi użytkownicy. Udostępnianie urządzeń w celu umożliwienia korzystania z tej usługi jest ryzykowne dla użytkownika ponieważ ruch z sieci prywatnej zostaje skierowany do sieci operatora. Bierze on wtedy pełną odpowiedzialność za czyny i treści przesłane przez nieznanych użytkowników. Określenie NTP w punkcie B lub C daje możliwość odseparowania ruchu za pomocą identyfikatorów oraz pozwala na łatwe określenie z jakiego urządzenia pochodził ruch.

Izba pragnie wyraźnie podkreślić, że konkurencyjność na rynku sprzętu telekomunikacyjnego nie istniałaby gdyby nie dostawcy usług telekomunikacyjnych. Operatorzy telekomunikacyjni dzięki tworzeniu nowych usług (wspieranie start-up'ów), w nowych rozwiązaniach technologicznych, inwestowaniu w rozwój sieci i usług dodatkowych kreują popyt na urządzenia końcowe. Bez innowacji i inwestycji w sieci i usługi nie byłoby zapotrzebowania na sprzęt.


Z punktu widzenia przyszłych regulacji, w których NTP może być kluczowym elementem, należy określić lokalizację NTP na podstawie przesłanek określających nowoczesne technologie dostępowe. Sieci xDSL są rozwijane w niewielkim stopniu i stosunkowa łatwość podłączenia dowolnych urządzeń w sieciach opartych na tej technologii nie może wyznaczać kierunku w jakim przyszłe regulacje sieci i usług powinny się kierować. Z doświadczeń operatora sieci stosującego

w ramach nowoczesnych technologii dostępowych urządzenia zapewniające bezpieczeństwo, łatwość, bezawaryjność i komfort użytkownikowi końcowemu za pomocą preinstalowanych i personalizowanych urządzeń wynika, że lokalizacja NTP w punkcie C daje największą korzyść dla użytkownika i operatora sieci.

Na marginesie powyższych rozważań, Izba zauważa, że w obecnym stanie prawnym brak jest przepisów dla wydania wiążących rozstrzygnięć w tym zakresie. W związku z tym zasadnym po stronie Prezesa UKE wydaje się wskazanie w jaki sposób planuje przeprowadzić proces identyfikacji lokalizacji zakończenia sieci ze skutkiem dla całego rynku telekomunikacyjnego, zapewniając transparentność procedury i zgodność z przepisami EKŁE. Transparentność działań regulacyjnych w kwestii punktu zakończenia sieci sprzyjać będzie zapewnieniu stabilności i pewności regulacyjnych rozstrzygnięć nie tylko na poziomie polskim ale również europejskim.

Mając powyższe na uwadze, Izba zwraca się z prośbą o uwzględnienie, w przypadku dokonywania przez Prezesa UKE oceny zasadności identyfikacji lokalizacji NTP na polskim rynku telekomunikacyjnym, w szczególności specyfiki rynku telekomunikacyjnego, zróżnicowanego pod względem technologicznym i usługowym, jak również dobrostanu użytkowników końcowych w zakresie konieczności zapewnienia im wysokiej jakości usług telekomunikacyjnych, w najwyższych standardach obsługi.

*z poważaniem*

Prezes Zarządu  
  
Stefan Kamiński