

*dr Piotr Ładny*¹

Katedra Efektywności Innowacji, Wydział Zarządzania i Ekonomiki Usług
Uniwersytet Szczeciński

Neutralność sieci – dogmat czy postulat

WPROWADZENIE

Neutralność sieci (*net neutrality*) to pojęcie, które związane jest z Internetem od początku jego istnienia. Jednak pomimo tego, że termin ten funkcjonuje od dawna i jest powszechnie używany, to nie został jednoznacznie zdefiniowany i w literaturze można znaleźć wiele różnych definicji odnoszących się do aspektów technicznych, ekonomicznych i społecznych oraz ujmujących ten problem od strony użytkowników sieci i dostawców usług internetowych.

Neutralność sieciowa jest często określana jako zasada, zgodnie z którą wszyscy użytkownicy Internetu mogą uzyskać dostęp do zasobów sieci na równych prawach². Dzięki zasadzie neutralności każdy podmiot, bez względu na rolę, wielkość i obszar, w jakim prowadzi działalność, ma w internetowym ekosystemie równe prawa w zakresie świadczenia i korzystania z usług, a każdy rodzaj treści (informacji) jest przesyłany w oparciu o takie same zasady. Internauci mogą więc dowolnie tworzyć i wykorzystywać dostępne w sieci usługi, aplikacje i treści bez ograniczeń i restrykcji ze strony operatorów infrastruktury teleinformatycznej lub władzy [*Net*, 2013].

Z technicznego punktu widzenia neutralność oznacza swobodę ruchu pomiędzy dowolnymi punktami sieci, bez ingerencji operatorów i dyskryminacji tego ruchu, ze względu np. na jego źródło (skąd), cel (dokąd) oraz rodzaj transmitowanych danych. Brak ingerencji w dane przesyłane pomiędzy użytkownikami końcowymi sieci określa się jako zasadę *end-to-end*, a praktycznym przykładem jej nieprzestrzegania jest sytuacja, w której operator sieci spowalnia lub wręcz blo-

¹ Adres korespondencyjny: Katedra Efektywności Innowacji, Wydział Zarządzania i Ekonomiki Usług, Uniwersytet Szczeciński, ul. Cukrowa 8, 71-004 Szczecin, e-mail: piotr.ladny@wzieu.pl, tel. 91 444 31 87.

² Zasada ta nie dotyczy, co oczywiste, dostępu do tych zasobów Internetu, które zawierają np. informacje niejawne czy też informacje podlegające ochronie ustawowej oraz tych serwisów, do których dostęp możliwy jest po wniesieniu opłaty (np. specjalistyczne serwisy informacyjne, elektroniczne wydania gazet, gry sieciowe itp.).

kuje swoim klientom dostęp do określonych usług internetowych (np. wybranych stron WWW, wyszukiwarek internetowych, serwisów udostępniających muzykę czy filmy), jednocześnie przyznając wyższy priorytet dla połączeń z innymi serwisami (np. własnymi).

Z perspektywy dostawców usług świadczonych na platformie internetowej neutralność sieci jest gwarancją, że niezależnie od rodzaju świadczonych usług, udostępnianych treści czy pozycji rynkowej będą oni przez operatorów sieci telekomunikacyjnych traktowani w sposób niedyskryminujący, a przesyłane przez nich pakiety danych nie będą podlegać ingerencji.

Równouprawienie w zakresie dostępu i wykorzystania zasobów Internetu jakie wynika z zasady jej neutralności wydaje się ze wszech miar uzasadnione i przez wiele osób oraz środowisk jest traktowane jako fundament wolnego Internetu i warunek jego dalszego rozwoju. Otwartość i neutralność sieci uznawana jest za kluczowy element przyczyniający się do rozwoju innowacyjnych usług, konkurencji i swobodnego przepływu informacji.

Organizacje obywatelskie wskazują również na fakt, że przestrzeganie tej zasady ma ogromny wpływ na tworzenie nowych środków sprzyjających realizacji praw obywatelskich, w tym szczególnie w zakresie wolności wypowiedzi oraz prawa do otrzymywania i przekazywania informacji. Na konieczność utrzymania neutralnego Internetu wskazywali wielokrotnie w swoich publicznych wypowiedziach m.in. Vinton Cerf [Hearing on „Network Neutrality”, 2006] uznawany za jednego z „ojców” Internetu, współtwórca protokołu TCP/IP oraz Tim Berners-Lee [Berners-Lee, 2006] – twórca i jeden z pionierów usługi WWW, a także Viviane Reding [Reding, 2008] – wiceprzewodnicząca Komisji Europejskiej oraz Neelie Kroes [Commissioner..., 2010] – wiceprzewodnicząca Komisji Europejskiej i komisarz europejski ds. agendy cyfrowej. Jednak pomimo szerokiego poparcia, jakie deklarowane jest dla idei neutralności sieci, pojęcie to nie znalazło pełnego odzwierciedlenia w przepisach i funkcjonuje raczej jako niepisana zasada, aniżeli usystematyzowana regulacja.

Tymczasem problem ingerencji operatorów sieci w warstwę przesyłanych przez Internet danych staje się na przestrzeni ostatnich kilkunastu lat przedmiotem coraz liczniejszych dyskusji i sporów dotyczących możliwości i zasadności takiej ingerencji oraz konieczności wpisania neutralności do systemu krajowych i międzynarodowych regulacji prawnych. Głównym powodem debaty dotyczącej przekształcenia neutralności sieci z niepisanej zasady w obowiązek regulacyjny jest narastający konflikt pomiędzy podmiotami reprezentującymi różnorodne interesy związane z wykorzystaniem sieci.

Rosnąca rola dostawców treści i usług oraz postępująca od końca lat 90. integracja pionowa operatorów sieci oraz dostawców i agregatorów treści (np. Comcast i NBC czy AOL i Time Warner) są wskazywane jako podstawy tego konfliktu [Lemley, Lessig, 2000, s. 925, 2001].

OGRANICZANIE NEUTRALNOŚCI INTERNETU PRZEZ OPERATORÓW SIECI TELEKOMUNIKACYJNYCH

Wśród podmiotów, które najczęściej krytykują działania mające na celu wprowadzenie przepisów zakazujących naruszania zasady neutralności sieci są bez wątpienia operatorzy dostarczający infrastrukturę sieciową (w tym szczególnie infrastrukturę dostępową oraz operatorzy sieci komórkowych). Podnoszone przez nich argumenty dotyczą głównie swobody działań w ramach tzw. inżynierii ruchu, czyli możliwości ingerencji w parametry przesyłanych danych w celu zapobiegania negatywnym skutkom przeciążenia sieci czy też zapewnienia odpowiedniej jakości tym usługom, które mają szczególne wymagania dotyczące prędkości transmisji czy opóźnień związanych z przesyłaniem pakietów (usługi typu *real-time*, czyli np. połączenia głosowe czy wideo oraz usługi realizowane w technologii *streamingu*)³.

Argumenty takie należy uznać za uzasadnione, a regulacje zmierzające do ograniczenia operatorom sieci możliwości zarządzania ruchem w celu efektywnego wykorzystania zasobów za nadmierne i niezgodne z zasadą swobody gospodarczej. Trzeba jednak podkreślić, że u podstaw debaty na temat otwartego i neutralnego Internetu leżały liczne naruszenia tych zasad ze strony operatorów sieci, których ze względu na dyskryminujący charakter nie można w żaden sposób uznać za związane z zarządzaniem ruchem IP.

Przykładem takich działań były różnorodne ograniczenia, jakie operatorzy sieci nakładali na klientów chcących wykorzystywać niektóre usługi internetowe. Ograniczenia te dotyczyły głównie nowych usług lub też usług konkurencyjnych w stosunku do oferowanych przez dostawcę sieci i miały na celu wymuszenie dodatkowych opłat za możliwość ich wykorzystania (np. specjalne – biznesowe plany taryfowe). W opublikowanym w 2003 roku artykule Tim Wu [Wu, 2003, s. 160] profesor Columbia Law School wskazał 13 różnych rodzajów dyskryminujących i naruszających zasadę neutralności ograniczeń jakie w tym czasie, w swoich umowach z klientami stosowali dostawcy Internetu⁴ w Stanach Zjednoczonych. Za najistotniejsze zostały uznane zapisy ograniczające:

- publikowanie treści i świadczenie usług w oparciu o serwery klientów,

³ Należy zauważyć, że w odniesieniu do zarządzania ruchem, czyli działań operatorów sieci polegających na blokowaniu lub ograniczaniu ruchu stanowiącego zagrożenie dla funkcjonowania sieci (spam, wirusy, ataki DoS itp.) oraz określaniu priorytetów dla usług dla pakietów przesyłanych w usługach wrażliwych na opóźnienia, panuje powszechna zgoda, że działania takie nie stanowią naruszenia neutralności sieci. Warunkiem jest jednak, aby zarządzanie ruchem miało charakter techniczny i nie wiązało się z komercyjną dyskryminacją klientów, dostawców usług lub innych użytkowników sieci. Niezbędne jest także, aby działania dotyczące zarządzania ruchem IP miały charakter przejrzysty, czyli gwarantowały wszystkim użytkownikom sieci dostęp do informacji na temat zasad, zgodnie z którymi są realizowane.

⁴ W artykule autor odniósł się do zapisów, jakie znajdowały się w umowach operatorów oferujących dostęp do Internetu za pośrednictwem sieci telewizji kablowej i technologii DSL.

- komercyjne wykorzystanie usług internetowych,
- tworzenie sieci domowych w oparciu o urządzenia (routery) klientów,
- tworzenie sieci bezprzewodowych (wykorzystanie urządzeń i technologii WiFi).

Zapisy zabraniające publikowania treści i świadczenia usług innym internautom znalazły się w umowach praktycznie wszystkich operatorów sieci kablowych i około 30% operatorów wykorzystujących technologię DSL. Ograniczenia takie znalazły się w umowach, jakie klienci zawierali m.in. z Cox Systems, Charter Communications, Sprint czy Verizon. Do najbardziej restrykcyjnych należała firma AT&T Broadband, która zabraniała klientom realizowania w oparciu o własne serwery takich usług jak: poczta elektroniczna, ftp, współdzielenie plików, gry sieciowe, strony internetowe, grupy dyskusyjne czy czaty internetowe (IRC). W praktyce zabronione było wszystko, co wiązało się z udostępnianiem treści lub świadczeniem usług poza lokalem użytkownika.

Kolejnym ograniczeniem był stosowany przez wszystkich z analizowanych operatorów sieci kablowych i większość operatorów DSL zakaz wykorzystywania łącza w celach komercyjnych i biznesowych przez użytkowników domowych. Najbardziej kontrowersyjnym przejawem tego ograniczenia był zakaz tworzenia i wykorzystywania prywatnych sieci wirtualnych (VPN). W swoich umowach firma Time Warner określała, że klienci mogą korzystać z Internetu wyłącznie w celach osobistych i niekomercyjnych, a BellSouth zabraniała udostępniania jakiegokolwiek treści o charakterze publicznym lub biznesowym.

Efektom wzrostu popularności urządzeń do tworzenia sieci lokalnych, wśród użytkowników indywidualnych były zakazy lub ograniczenia (np. dotyczące maksymalnej liczby podłączonych komputerów) związane z tworzeniem takich sieci przez klientów. W 2002 roku 4 z 10 największych dostawców Internetu w USA (MediaOne, Comcast, AT&T and Adelphia) stosowało takie ograniczenia. Szczególnie restrykcyjnie traktowała tworzenie przez klientów lokalnych sieci domowych firma AT&T Broadband, uznając takie działanie za „kradzież usług” i grożąc swoim klientom odpowiedzialnością karną i cywilną. Inni operatorzy, jak np. BellSouth, ograniczali się do zakazu „dzielenia łącza”, czyli udostępniania łącza internetowego poza lokal klienta i członkom najbliższej rodziny (*immediate family members*).

Ostatnia grupa dyskryminujących zapisów scharakteryzowana przez profesora Wu dotyczyła również tworzenia sieci domowych, ale odnosiła się do technologii bezprzewodowej (WiFi). Całkowity zakaz tworzenia bezprzewodowych sieci lokalnych umieszczała w umowach z klientami AT&T Broadband, natomiast część operatorów sieci kablowych (np. Cox Systems) w dokumentach określających zasady świadczenia usług umieszczała zakazy tworzenia sieci radiowych, z których możliwe będzie korzystanie poza lokalem klienta.

Przedstawione powyżej przykłady dotyczą operatorów sieci działających na rynku amerykańskim, jednak praktyki naruszające neutralność sieci stosują dostawcy Internetu również w innych krajach, w tym europejskich. 29 maja 2012

roku opublikowany został raport opracowany przez europejski organ regulacyjny (BEREC) we współpracy z Komisją Europejską [A view..., 2012], prezentujący wyniki dochodzenia przeprowadzonego w sprawie działań związanych z zarządzaniem ruchem oraz innych praktyk ograniczających zasadę wolnego i otwartego Internetu. W raporcie przeanalizowano 381 operatorów sieci (266 stacjonarnych i 115 mobilnych) działających w 32 krajach europejskich. Dodatkowo Komisja Europejska zebrała opinie i informacje pochodzące od dostawców treści i aplikacji, organizacji konsumenckich, branżowych oraz od osób fizycznych.

W raporcie scharakteryzowano siedem głównych praktyk, które wiążą się z ingerencją operatorów sieci w przesyłane dane. Praktyki te zostały podzielone na cztery grupy:

1. Ograniczenia (techniczne oraz zawarte w umowach) związane z blokowaniem lub spowalnianiem ruchu związanego z konkretnymi usługami (np. VoIP, P2P⁵, FTP, gry sieciowe, streaming audio/wideo) lub konkretnymi dostawcami usług. Działania takie mogły się przejawiać spowalnianiem ruchu dla wybranych usług (np. Skype czy Spotify). W efekcie ograniczano prędkość pakietów dla takich usług, wymuszając od internautów chcących z nich korzystać dodatkowe opłaty. Do grupy tej zaliczono również przypadki odwrotne, polegające np. na faworyzowaniu określonych usług czy dostawców poprzez zapewnienie im lepszych parametrów transmisji. Sytuacje takie miały miejsce w odniesieniu do dostawców, którzy byli skłonni zapłacić operatorowi sieci za „lepsze traktowanie” ich usług lub też w odniesieniu do usług oferowanych przez operatora sieci.
2. Ochrona bezpieczeństwa i integralności sieci, czyli działania obejmujące np. blokowanie spamu czy ataków DoS (odmowa dostępu – *Denial of Services*) oraz przeciwdziałanie przeciążeniom sieci (zarządzanie ruchem).
3. Działania związane z implementacją określonych modeli biznesowych, czyli np. świadczenia usług specjalistycznych lub usług, których cena jest uzależniona od rozmiaru przesyłanych danych (wolumen ruchu). Przykładem specjalistycznych usług są usługi telewizyjne lub telefoniczne, które z uwagi na konieczność zapewnienia wysokich parametrów, mogą negatywnie wpływać na inne, publiczne usługi. Innym przykładem działań wynikającym z przyjętego modelu biznesowego są stosowane przez większość operatorów mobilnych oraz część operatorów stacjonarnych limity transferu (*data cap*)⁶, w których po wyczerpaniu limitu operator zmniejsza prędkość transmisji lub nalicza wyższe opłaty (ewentualnie wymaga wykupienia dodatkowego pakietu). Choć takie rozwiązania nie są uznawane za sprzeczne z zasadą neutralności (jeśli limity

⁵ P2P (ang. *Peer-to-Peer*) – model komunikacji sieciowej, w którym dane przesyłane są pomiędzy komputerami użytkowników. W takim modelu komunikacji nie stosuje się urządzeń pośredniczących – serwerów. Model P2P najczęściej stosowany jest w systemach wymiany plików lub w usługach komunikacyjnych, np. Skype.

⁶ Z przedstawionych w raporcie BEREC danych wynika, że limity transferu stosuje 83% operatorów sieci komórkowych.

obowiązują w stosunku do wszystkich dostawców i usług), to w raporcie wskazano na kilka przykładów, które budziły wątpliwości. Dotyczyło to np. ograniczania po przekroczeniu limitu prędkości tylko wybranych usług (np. P2P) czy też uprzywilejowane traktowanie wybranych serwisów/aplikacji, których transfer nie był wliczany do limitów⁷. Praktyki takie stosuje m.in. firma Deutsche Telecom oferując klientom dostęp do usługi Entertain (IPTV), której transfer jest niezależny od pakietu danych z jakiego korzysta klient. Oznacza to, że w przeciwieństwie do innych usług (również wideo) po przekroczeniu limitu usługa Entertain jest nadal świadczona bez ograniczeń [Masnick].

4. Ograniczenia wynikające z przepisów prawa – ograniczenia te nie są nakładane z inicjatywy operatorów sieci, ale są skutkiem krajowych czy też międzynarodowych regulacji prawnych oraz wyroków sądowych. Ograniczenia o takim charakterze najczęściej dotyczą filtrowania stron udostępniających treści niezgodne z prawem (treści chronione prawem autorskim, materiały o charakterze pedofilskim, propagujące przemoc, nawołujące do nienawiści czy też umożliwiające zawieranie nielegalnych transakcji) oraz blokowania użytkowników sieci naruszających przepisy prawa. Przejawem działań wymuszonych przez regulacje prawne jest również automatyczne blokowanie usług internetowych w przypadku przekroczenia określonego poziomu opłat użytkownikom korzystającym z roamingu międzynarodowego.

Za ewidentnie sprzeczne z zasadą neutralności sieci Komisja Europejska i europejski organ regulacyjny uznały jedynie działania przedstawione w grupie pierwszej oraz częściowo w grupie trzeciej (wybiórcze stosowanie limitów transferu). Z zebranych danych wynika, że kwestionowane praktyki związane z blokowaniem lub spowalnianiem usług P2P zostały stwierdzone u 18,4% operatorów stacjonarnych i 35,6% komórkowych. Restrykcje dotyczące usług VoIP stwierdzono niemal wyłącznie u operatorów komórkowych (23,5% analizowanych sieci). W sieciach stacjonarnych praktyki takie stosowało zaledwie 0,7% operatorów. Ograniczenia dotyczące innych usług stwierdzono u 3,7% operatorów stacjonarnych i 8,7% komórkowych. Odsetek operatorów stacjonarnych i komórkowych, u których stwierdzono preferencyjne traktowanie wybranych usług lub dostawców był taki sam i wyniósł 11,9%.

Należy jednak podkreślić, że przedstawione dane należy traktować jedynie orientacyjnie, bowiem liczba operatorów nie przekłada się na ich pozycję rynkową (różna liczba obsługiwanych abonentów i bezpośrednich konkurentów), a stwierdzone przypadki naruszenia zasady neutralności miały różny charakter i zasięg u różnych operatorów. Poszczególne praktyki mogły mieć zastosowanie dla części lub wszystkich klientów, zróżnicowany mógł być też czas ich stosowania. Dla lepszego zobrazowania skali problemu w raporcie przedstawiono sza-

⁷ Problem ten został szerzej omówiony w dokumencie BEREC opublikowanym w ramach konsultacji prowadzonych przez Komisję Europejską w sprawie otwartego i neutralnego Internetu we wrześniu 2010 r. Zob.: [Response..., 2010, s. 15).

cunki wskazujące jakiej części użytkowników Internetu mogły dotyczyć poszczególne naruszenia zasady neutralności.

Z szacunków tych wynika, że ograniczenia związane z technologią *peer-to-peer* dotyczyły ok. 21% internautów korzystających z sieci stacjonarnych i 36% korzystających z sieci komórkowych, natomiast blokowania lub spowalniania usług VoIP (np. Skype czy Viber) doświadczyło ok. 21% internautów korzystających z dostępu mobilnego.

Oznacza to, że blokady i ograniczenia takich usług w europejskich sieciach komórkowych obejmowały przynajmniej 44 mln użytkowników. Restrykcje dotyczące innych usług dotyczyły ok. 1,8% internautów korzystających ze stacjonarnych technologii dostępowych i 11,6% mobilnych. Z efektami preferencyjnego traktowania wybranych usług lub operatorów zetknęło się ok. 3,6% internautów stacjonarnych i 5,7% komórkowych. W raporcie wskazano również, że z uwagi na złożony charakter tych praktyk grupa internautów, których one dotyczą, może być większa, bowiem w stosunku do części klientów nie można było jednoznacznie potwierdzić ani wykluczyć, że dotyczyły ich działania naruszające neutralność sieci.

Z przedstawionych danych wynika, że naruszenia zasady otwartego i neutralnego Internetu przez europejskich operatorów są najczęściej związane z technologią P2P oraz VoIP i w większym stopniu dotyczą klientów sieci komórkowych aniżeli stacjonarnych. Raport pozwala również na stwierdzenie pewnych zmian, jakie w porównaniu do analiz przeprowadzonych na rynku amerykańskim nastąpiły w sferze ingerencji operatorów w przesyłane treści. Zmiany te polegają głównie na odejściu operatorów od ograniczeń związanych z wykorzystywanymi przez klientów urządzeniami sieciowymi, w tym szczególnie urządzeniami pozwalającymi na dzielenie pasma i tworzenie lokalnych sieci (również w oparciu o technologie WiFi).

Drugi obszar zmian, to wprowadzanie coraz częściej pod pozorem tworzenia nowych modeli biznesowych rozwiązań, pozwalających na priorytetowe traktowanie własnych usług lub wybranych dostawców usług i treści. Pomimo że działania takie mogą negatywnie wpływać na poziom konkurencyjności i innowacyjności usług, to jednocześnie budzą największe wątpliwości i kontrowersje w związku z możliwością wprowadzenia prawnych gwarancji dla neutralności sieci.

NEUTRALNOŚĆ SIECI W ŚWIETLE DZIAŁAŃ WŁADZ PAŃSTWOWYCH

Zróznicowane i, w niektórych przypadkach, niejednoznaczne stanowisko dotyczące przestrzegania zasady neutralnego i otwartego Internetu prezentują władze państw oraz organy regulacyjne. W wielu krajach, szczególnie tych o niedemokratycznym ustroju, dostęp do Internetu, udostępniane w sieci treści i usługi

oraz przesyłane dane podlegają ścisłej kontroli. W krajach takich jak: Chiny, Korea Północna, Iran, Syria, Wietnam, Arabia Saudyjska czy Zjednoczone Emiraty Arabskie, kontrola ta ma najczęściej charakter cenzury politycznej lub religijnej, a jej przejawem jest blokowanie określonych stron internetowych lub usług umożliwiających swobodną komunikację oraz stosowanie represji w stosunku do osób, które nie stosują się do zakazów i ograniczeń. Skrajnym przykładem ingerencji w funkcjonowanie sieci jest tworzenie przez niektóre państwa własnego „Internetu”⁸, którego zasoby są w znacznym stopniu (Iran) lub całkowicie (Korea Północna) oddzielone od światowej sieci.

Znacznie lepiej wygląda pod tym względem sytuacja w krajach, których ustrój oparty jest na stabilnym systemie prawnym i przestrzeganiu zasad demokracji. Przykładem takich państw są przede wszystkim kraje Ameryki Północnej (USA, Kanada), niektóre kraje azjatyckie (Japonia, Filipiny) oraz większość krajów europejskich⁹.

Jednak nawet w państwach, które formalnie wyrażają poparcie dla idei neutralności i deklarują podjęcie działań zmierzających do prawnego zagwarantowania wolnego i otwartego Internetu, zaledwie kilka wprowadziło takie regulacje w oparciu o ustawy lub inne przepisy. Z przeprowadzonych przez Open Forum Academy badań dotyczących działań zmierzających do usankcjonowania neutralności sieciowej w krajach Unii Europejskiej [Olmos, 2013] wynika, że zdecydowana większość (23 na 28) państw członkowskich ogłosiło oficjalne stanowisko w tej sprawie. Jednak jedynie cztery kraje umieściły taki obowiązek w krajowym systemie prawnym (Holandia, Słowacja) lub zapowiedziały rozpoczęcie prac legislacyjnych zmierzających do jego wprowadzenia (Belgia, Luksemburg). Poza Europą, nakaz zachowania neutralności przez operatorów sieci został wprowadzony w 2010 roku w Chile [*Chile...*]. W USA zasady dotyczące neutralności sieci wprowadzono nie poprzez przepisy ustawy ale regulacje narzucone przez Federalną Komisję Łączności (FCC), która w 2010 roku zakazała operatorom sieci stosowania dyskryminujących praktyk w stosunku do dostawców usług takich jak np. Netflix czy Amazon, a w 2011 roku opublikowała zasady dotyczące zapewnienia wolnego i otwartego Internetu. Wprowadzone regulacje zostały jednak uchylone przez sąd w styczniu 2014 roku w wyniku pozwu złożonego m.in. przez firmę Verizon.

Brak zdecydowanych działań zmierzających do zagwarantowania neutralności sieci przez władze państw demokratycznych to w znacznej mierze skutek argumentów operatorów sieci wskazujących, że zbytnia ingerencja ograniczająca swobodę działalności oraz implementację nowych modeli biznesowych może

⁸ Działania takie określane są pojęciem bałkanizacji Internetu lub cyberbałkanizacji.

⁹ Informacje dotyczące zakresu wolności oraz restrykcji nakładanych na operatorów sieci i internautów przez rządy poszczególnych krajów można znaleźć m.in. w opracowaniach organizacji Freedom House. W opublikowanym w październiku 2013 roku raporcie Freedom on the Net 2013 przeanalizowano sytuację w 60 krajach na świecie [*Freedom...*, 2013].

ograniczyć przychody operatorów, a tym samym zmniejszyć skalę inwestycji związanych z budową szerokopasmowej infrastruktury. Ponieważ tworzenie społeczeństwa informacyjnego, którego podstawą jest właśnie infrastruktura szerokopasmowa jest uznawane za jeden z priorytetów w krajach Unii Europejskiej, podobnie jak wielu innych, wątpliwości co do ekonomicznych i społecznych skutków regulacji doprowadziły do przyjęcia przez wiele państw strategii „przeczekania” problemu. Dodatkowo, nawet kraje oficjalnie deklarujące poparcie dla wolności i otwartości Internetu podejmują wiele działań, które w efekcie tę wolność ograniczają. Ograniczenia takie sprowadzają się najczęściej do filtrowania (blokowania dostępu) witryn internetowych i usług służących do prowadzenia działań niezgodnych z prawem (grupa 4. klasyfikacji zawartej w raporcie BEREC). W wielu przypadkach nakładane przez poszczególne państwa ograniczenia są jednak krytykowane jako nieuzasadnione, nadmierne bądź nieadekwatne do problemów, których rozwiązaniu mają służyć. Inicjatywom rządowym zmierzającym do wprowadzania internetowych blokad zarzuca się, że służą realizacji doraźnych celów i wynikają z niezrozumienia mechanizmów Internetu. Krytycy takich działań wskazują, że zamiast zwalczać negatywne zjawiska i usuwać niepożądane treści z Internetu, jedynie utrudniają – często nieskutecznie, dostęp do nich. Przykładem jak nieskuteczne może być filtrowanie określonych treści są np. próby blokowania treści pornograficznych. Stosowane przez operatorów czy użytkowników (szkoły, pracodawcy) filtry mogą blokować dostęp do innych treści, związanych np. z edukacją seksualną czy medycyną, a przy tym są dosyć łatwe do ominięcia za pomocą powszechnie dostępnych mechanizmów ukrywania i anonimizacji przesyłanych danych (serwery proxy, usługi TOR, dodatki do przeglądarek internetowych).

W Wielkiej Brytanii, gdzie w 2013 roku wprowadzono jedne z najbardziej restrykcyjnych w Europie przepisy ograniczające internautom dostęp do treści pornograficznych¹⁰, okazało się, że stosowane filtry, poza pornografią spowodowały zablokowanie wielu innych stron poświęconych np. problemom przemocy domowej oraz wykorzystywaniu seksualnemu [Smith, 2014; Burrell, 2014]. Wśród zablokowanych stron znalazła się także witryna Claire Perry, konserwatywnej parlamentarzystki, która poparła wprowadzenie regulacji umożliwiających cenzurę w Internecie. Również premier Wielkiej Brytanii Dawid Cameron i jednocześnie współautor nowych regulacji przyznał, że wprowadzanie nowych rozwiązań jest skomplikowanym i kłopotliwym procesem [Cameron, 2014].

Obok treści pornograficznych obszarem, gdzie władze coraz powszechniej stosują przepisy ograniczające dostęp do określonych treści (cenzura prewencyjna

¹⁰ Przyjęte w UK rozwiązania nakładają na dostawców sieci obowiązek zastosowaniu oprogramowania filtrującego treści w stosunku do wszystkich swoich klientów. Osoby, które chcą uzyskać dostęp do niefiltrowanych treści muszą złożyć odpowiednie oświadczenie (system *opt out*). Obowiązek cenzurowania treści pornograficznych nałożono na wszystkich operatorów stacjonarnych, jednak rozważa się jego rozszerzenie na operatorów sieci mobilnych.

i represyjna), są usługi związane z udostępnianiem i wymianą plików zawierających filmy, muzykę czy książki (ebooki). W ostatnich latach coraz więcej jest krajów, które wprowadzają przepisy „antypirackie” mające na celu uniemożliwienie internautom swobodnej wymiany treści chronionych prawem autorskim, a co za tym idzie – ochronę interesów twórców takich treści. Stosowane w tym zakresie regulacje prawne różnią się znacznie pod względem podejmowanych przez państwo ograniczeń, jak również sankcji jakie grożą za ich złamanie.

Wśród szczególnie restrykcyjnych państw znajdują się np. USA, gdzie nawet za niewielkie naruszenia w zakresie praw autorskich można zostać skazanym na wielomilionowe grzywny, czy Francja, gdzie na mocy uchwalonej w 2009 roku ustawy Hadopi, za łamanie praw autorskich internautom grożą kary do dwóch lat więzienia i grzywna do 300 tys. euro, a operatorzy po trzech ostrzeżeniach dotyczących stwierdzonych naruszeń mogli „odcinać” internautom dostęp do sieci¹¹. W innych krajach, w tym także w Polsce, dzięki szerokiej interpretacji tzw. dozwolonego użytku obowiązujące przepisy oraz działania związane z blokowaniem treści naruszających prawa autorskie można uznać za liberalne.

Nie ulega wątpliwości, że działania prowadzone w przestrzeni wirtualnej, tak samo jak w realnej, muszą być zgodne z prawem, a własność intelektualna i prawo autorskie podlegać ochronie. Zwolennicy neutralności sieciowej wskazują jednak, że naruszanie tej zasady oraz nadmierne rozszerzanie uprawnień do administracyjnej kontroli (cenzury) przesyłanych treści w celu ochrony praw autorskich może wywołać wiele niekorzystnych skutków gospodarczych i społecznych. Wśród negatywnych efektów wykorzystywania mechanizmów kontroli Internetu jako głównego narzędzia do walki z „piractwem” sieciowym najczęściej wymienia się:

- utrwalenie tradycyjnego i nieefektywnego systemu dystrybucji treści i brak innowacji w zakresie modeli biznesowych związanych z tworzeniem i udostępnianiem treści,
- nadużywanie (wykorzystywanie) organów ścigania do egzekucji należności z tytułu prawa autorskiego w drodze postępowania karnego, a nie cywilnego,
- błędy skutkujące blokowaniem legalnych treści i serwisów,
- bezpodstawne oskarżenia o łamanie praw autorskich i związane z tym wymuszanie odszkodowań (*copyright trolling*).

W odniesieniu do podejmowanych przez państwo działań dotyczących ochrony praw autorskich w Internecie, warta podkreślenia jest również niejednoznaczna ocena skutków, jakie wywołuje piractwo komputerowe. Kontrowersyjne są zwłaszcza wyliczenia strat, jakie właściciele praw autorskich ponoszą w wyniku nielegalnego pobierania i udostępniania w sieci treści objętych ochroną¹².

¹¹ W lipcu 2013 roku przepisy pozwalające na blokowanie internautom dostępu do sieci zostały uznane za nieproporcjonalne i zliberalizowane [*Francja...*, 2013].

¹² Do obliczenia strat wykorzystuje się zwykle iloczyn ceny danego dobra (film, utwór muzyczny, program komputerowy) i liczby jego „ściągnięć” przez internautów. Wiarygodność takich

Coraz częściej w wątpliwość podawana jest również teza o niekorzystnym wpływie, jaki swobodny dostęp do treści i wymiana plików w Internecie wywierają na gospodarkę. W raporcie opublikowanym w 2010 roku przez Government Accountability Office (GAO) – jedną z rządowych instytucji USA – stwierdzono, że nie jest możliwe jednoznaczne potwierdzenie negatywnego wpływu „piractwa komputerowego” na gospodarkę. Wskazano jednocześnie, że istnieją branże, które dzięki temu zjawisku odniosły korzyści, np. operatorzy telekomunikacyjni i dostawcy sprzętu telekomunikacyjnego, producenci i sprzedawcy odtwarzaczy muzycznych i filmowych oraz producenci dodatkowych towarów i usług związanych z filmami. Stwierdzono również pozytywny wpływ na szeroko rozumianą innowacyjność [*Intellectual Property...*, 2010]. Brak negatywnego wpływu nieautoryzowanej wymiany plików muzycznych w Internecie na sprzedaż muzyki z legalnych źródeł potwierdziło również w swoim raporcie Wspólne Centrum Badawcze Komisji Europejskiej (JRC) [*Digital...*, 2014]. W raporcie wskazano, że w niektórych przypadkach dostęp do bezpłatnych treści może nawet stymulować wzrost przychodów ze sprzedaży muzyki.

Przedstawione powyżej problemy, jakie wiążą się z cenzurowaniem Internetu, wskazują, że rozwiązania polegające na filtrowaniu, blokowaniu i ingerowaniu w przesyłane treści nie mogą być traktowane jako skuteczne sposoby ochrony porządku prawnego i przeciwdziałania negatywnym zjawiskom w sieci. Wykorzystanie takich mechanizmów nie rozwiązuje problemów, a jedynie ukrywa je, co można porównać do terapii, która nie usuwa przyczyn, a jedynie objawy choroby.

Niezależnie od tego, jak ocenia się szkodliwość różnych treści przesyłanych i udostępnianych w globalnej sieci, działania których istota sprowadza się do cenzurowania treści, niezależnie od tego, czy dotyczą one pornografii, mowy nienawiści, czy utworów chronionych prawem autorskim, to są kosztowne, a ich skuteczność jest ograniczona. Dodatkowo wraz z upływem czasu pojawiają się kolejne rozwiązania pozwalające internautom omijać stosowane blokady, co jeszcze bardziej zmniejsza ich skuteczność¹³.

Szczególnie niebezpieczna jest jednak możliwość, że wprowadzone z inicjatywy operatorów lub też narzucane przez administrację państwową ograniczenia zostaną wykorzystane w innym celu niż zostały wprowadzone. Przykładem mogą

kalkulacji podważa jednak przyjęte do obliczeń założenie, że w przypadku braku dostępu do nielegalnych treści, Internauci kupiliby w taką samą liczbę dóbr w legalnej dystrybucji. Nieuwzględnia się również faktu, że przynajmniej część internautów traktuje wymianę plików jako sposób na zapoznanie się z dziełem i następnie kupuje je w sposób legalny.

¹³ Przykładem mogą być blokady operatorów sieci nałożone na przełomie 2011 i 2012 r. m.in. w Wielkiej Brytanii i Holandii na serwis wymiany plików The Pirate Bay. Badania przeprowadzone przez dwa ośrodki naukowe (Northeastern University w Bostonie oraz University of Amsterdam) wskazały, że blokady wywołują jedynie krótkotrwałe ograniczenie „piractwa”, a w niektórych przypadkach dało się zauważyć nawet wzrost liczby plików pobieranych z nieautoryzowanych źródeł. [Poorta i in., 2014; Lauinger i in., 2014].

być tutaj Rosja [*Kreml blokuje...*, 2014] i Turcja [*Rewolucja...*, 2014], gdzie rozwiązania służące początkowo do blokowania treści niezgodnych z prawem zostały wykorzystane do blokowania stron przeciwników politycznych. Również w Wielkiej Brytanii pojawiły się zapowiedzi, że rozległy system filtrowania obejmie kolejne obszary, w tym np. niesprecyzowane „ekstremistyczne” treści polityczne [Neal, 2014].

WNIOSKI

Przemiany zachodzące we współczesnym świecie powodują, że Internet staje się nieodłącznym elementem życia codziennego, a dostęp do narzędzi informacyjno-komunikacyjnych oraz umiejętność ich wykorzystania wskazywane są jako warunki niezbędne dla rozwoju społeczno-gospodarczego.

Mając na uwadze znaczenie globalnej sieci oraz fakt, że fundamentem rozwoju i popularności Internetu był brak dyskryminacji w zakresie dostępu i wykorzystania jego zasobów, niezbędne wydaje się przekształcenie neutralności sieci z niepisanej zasady w obowiązujące na poziomie krajowym i międzynarodowym prawo.

Na konieczność taką wskazuje rosnąca skala ingerencji operatorów sieci oraz organów administracji rządowej wielu państw, które zmierzają do zwiększenia kontroli nad infrastrukturą sieciową i w swojej istocie sprowadzają się do ograniczenia swobody przesyłu informacji.

Konsekwencją braku przestrzegania zasady otwartości i neutralności przy jednoczesnym zwiększaniu administracyjnej kontroli nad Internetem może być wiele negatywnych zjawisk, a w skrajnym przypadku utworzenie „zamkniętych Internetów krajowych”, czyli praktyczny rozpad sieci globalnej (cyberbałkanizacja).

Ponieważ otwartość i neutralność sieci nie może mieć charakteru absolutnego, i jak wskazano wcześniej, istnieją uzasadnione przypadki związane np. z inżynierią ruchu czy też ochroną porządku prawnego, kiedy to ingerencja w przesyłane informacje jest uzasadniona, podstawą dla wprowadzanych regulacji powinno być precyzyjne określenie takich wyjątków przy jednoczesnym dążeniu do minimalizowania ograniczeń stosowanych w cyberprzestrzeni. Pewne ramy dla proponowanych przepisów mogą stanowić dokumenty określające podstawowe prawa i zasady obowiązujące przy dostępie do sieci i usług internetowych.

Wśród wielu dokumentów określających zestawy uniwersalnych zasad dotyczących Internetu na szczególną uwagę zasługują: opracowany przez Komisję Europejską „Kodeks unijnych praw internetowych” [www.euofundsnews], Karta Praw Cyfrowych [www.wepromise] przygotowana przez koalicję 35 europejskich

organizacji działających na rzecz praw człowieka w środowisku cyfrowym (*European Digital Rights – EDRi*) oraz zestaw „10 Praw Internetowych” [*10 praw*], którego autorem jest Koalicja na Rzecz Regulacji Prawa Internetowego (*Internet Rights and Principles Dynamic Coalition*).

Praktycznym przykładem regulacji gwarantujących neutralność Internetu są przepisy wprowadzone w Holandii i Słowenii. Zgodnie z przyjętymi w tych krajach regulacjami, operatorzy sieci mają prawo ingerowania w przesyłane informacje oraz blokowania i priorytetowania ruchu tylko w określonych przypadkach, które związane są z:

- zagwarantowaniem bezawaryjnej pracy sieci i usług i wynikają np. z przeciwdziałania przeciążeniom sieci, przy czym dane tego samego typu powinny być traktowane w jednakowy sposób,
- zachowaniem integralności i bezpieczeństwa sieci, w tym np. przeciwdziałanie atakom DoS czy blokowanie szkodliwego oprogramowania (wirusy, trojany itp.).
- ograniczeniem dystrybucji niezamówionych informacji (SPAM),
- egzekucją prawomocnych nakazów lub wyroków sądowych.

Warunkiem koniecznym jest, aby działania takie były proporcjonalne, niedyskryminujące oraz podejmowane w czasie i zakresie niezbędnym do realizacji powyższych celów.

Dodatkowo wprowadzone w Holandii przepisy ograniczają operatorom możliwość analizy (podśluchu) przesyłanych danych z wykorzystaniem m.in. takich technik jak głęboka analiza pakietów (*deep packet inspection – DPI*), a także odcinania użytkownikom dostępu do sieci.

Przenosząc takie regulacje na grunt prawa międzynarodowego należy jednak zwrócić uwagę na pewne wątpliwości, jakie wzbudziły przepisy przyjęte 19 marca 2014 r. przez komisję Parlamentu Europejskiego odpowiedzialną za przemysł (tzw. komisja ITRE).

Przepisy te umożliwiają operatorom świadczenie „usług specjalistycznych”, a więc takich e-usług, które dają dostęp tylko do wybranych treści, aplikacji, usług lub ich dowolnej kombinacji [*Net...*, 2014]. Nie określono jednak dokładnie definicji takich usług, co może stworzyć operatorom możliwość nadużyć przy ich wprowadzaniu i tym samym ograniczyć skuteczność uregulowań dotyczących zapewnienia neutralności sieci.

Akceptując konieczność zapewnienia operatorom swobody w zakresie inżynierii ruchu oraz rozwoju nowych usług i związanych z nimi modeli biznesowych, niezbędne jest jednak nałożenie na operatorów sieci telekomunikacyjnych obowiązku przejrzystości w zakresie działań obejmujących te obszary. Brak takiego obowiązku może znacząco ograniczyć internautom dostęp do informacji o szczegółach oferty oraz możliwość wyboru dostawcy usługi internetowej, a w konsekwencji istotnie zakłócić konkurencję na rynku dostępu do Internetu i świadczonych w sieci usług.

BIBLIOGRAFIA

- 10 *praw i zasad Internetu*, <http://irpcharter.org/site/wp-content/uploads/2011/09/pdf/po-lish.pdf>
- A view of traffic management and other practices resulting in restrictions to the open Internet in Europe*, Body of European Regulators of Electronic Communications (BEREC), 29 May 2012, http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.
- Berners-Lee T., *Net Neutrality: This is serious*, 21.06.2006, <http://dig.csail.mit.edu/bread-crumbs/node/144>.
- Burrell I., *O2 changes porn filter after charity sites blocked*, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/o2-changes-porn-filterafter-charity-sites-blocked-9023209.html> (dostęp: 20.03.2014).
- Cameron: Blokada pornografii internetowej może być kłopotliwa. Będą wyjątki*, http://wiadomosci.gazeta.pl/wiadomosci/1,114871,14323998,Cameron_Blokada_pornografii_internetowej_moze_byc.html (dostęp: 21.03.2014).
- Chile: A Leader in Net Neutrality Legislation*, <https://openmedia.ca/plan/international-comparisons/chile>.
- Commissioner Kroes on net neutrality*, 27.01.2010, <http://edri.org/edriagramnumber8-2-kroes-net-neutrality>.
- Digital music consumption on the Internet: Evidence from clickstream data*, <http://publications.jrc.ec.europa.eu/repository/handle/111111111/27891> (dostęp: 21.03.2014).
- Francja: koniec odcinania od Internetu*, 11.07.2013, <http://7thguard.net/11779/francja-koniec-odcinania-od-internetu> (dostęp: 21.03.2014).
- Freedom on the Net 2013, 2013*, <http://www.freedomhouse.org/report/freedom-net/freedom-net-2013>.
- Hearing on "Network Neutrality"*, U.S. Senate Committee on Commerce, Science, and Transportation, 7 lutego 2006, <http://www.commerce.senate.gov/pdf/cerf-020706.pdf>.
- Intellectual Property – Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, april 2010, United States Government Accountability Office, <http://www.gao.gov/new.items/d10423.pdf>.
- Kreml blokuje antyputinowskie portale*, <http://www.rp.pl/artykul/1094147.html> (dostęp: 20.03.2014).
- Lauinger T., Szydłowski M., Onarlioglu K., Wondracek G., Kirda E., Krügel C., *Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting*. NDSS, The Internet Society, <http://internetsociety.org/doc/clickonomics-determining-effect-anti-piracy-measures-one-click-hosting> (dostęp: 22.03.2014).
- Lemley M.A., Lessig L., 2001, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era (October 1, 2000)*, „UCLA Law Review”, Vol. 48, <http://ssrn.com/abstract=247737>.
- logie.gazeta.pl/internet/1,104530,15679236,Rewolucja_nie_będzie_tweetowana_Burzliwa_walka_rządu.html (dostęp: 20.03.2014).
- Masnick M., *Deutsche Telekom Dumps Net Neutrality; Will Limit Bandwidth For Competing Video & Voice Products*, <https://www.techdirt.com/articles/20130425/0225512>

- 2829/deutsche-telekom-dumps-net-neutrality-will-limit-bandwidth-competing-video-voice-products.shtml.
- Neal R.W., *UK Internet Censorship: David Cameron Says Government Will Block „Extremist” Websites*, <http://www.ibtimes.com/uk-internet-censorship-david-cameron-says-government-will-block-extremist-websites-1486872> (dostęp: 20.03.2014).
- Net neutrality, The EDRI papers*, issue 8, http://www.edri.org/files/paper08_netneutrality.pdf (dostęp: 26.11.2013).
- Net neutrality: Industry MEPs want stricter rules against blocking rival services*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20140318IPR39210+0+DOC+PDF+V0//EN&language=PL> (dostęp: 19.03.2014).
- Olmos A., Castro J., *Net Neutrality in the EU – Country Factsheets, OpenForum Academy*, September 2013, <http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20-%20Country%20Factsheets%2020130905.pdf>.
- Poorta J., Leenheerb J., Hamc J., Dumitruc C., *Baywatch: Two Approaches to Measure the Effects of Blocking Access to The Pirate Bay*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314297 (dostęp: 15.03.2014).
- Reding V., *Net Neutrality and Open Networks – Towards a European Approach*, Conference „Network Neutrality – Implications for Innovation and Business Online”, Copenhagen 30.09.2008.
- Response to the European Commission’s consultation on the open internet and net neutrality in Europe, BoR (10)42, September 2010, [http://www.irg.eu/streaming/BoR%20\(10\)%2042%20BEREC%20response_ECconsultation_Net%20neutrality_final.pdf?contentId=546969&field=ATTACHED_FILE](http://www.irg.eu/streaming/BoR%20(10)%2042%20BEREC%20response_ECconsultation_Net%20neutrality_final.pdf?contentId=546969&field=ATTACHED_FILE).
- Rewolucja nie będzie tweetowana. Burzliwa walka rządu Turcji z Twitterem*, http://technologie.gazeta.pl/internet/1,104530,15679236,Rewolucja_nie_będzie_tweetowana__Burzliwa_walka_rzadu.html (dostęp: 20.03.2014).
- Smith M.D., *Porn filters block sex education websites*, <http://www.bbc.com/news/uk-25430582> (dostęp: 20.03.2014).
- Wu T., 2003, *Network Neutrality, Broadband Discrimination*, „Journal of Telecommunications and High Technology Law”, Vol. 2.
- www.eurofundsnews.pl/content/view/20049/104.
- www.wepromise.eu/pl/page/karta.

Streszczenie

W artykule scharakteryzowano genezę i znaczenie pojęcia neutralności sieciowej w odniesieniu do infrastruktury teleinformatycznej, w tym szczególnie sieci Internet. Na przykładzie praktyk rynkowych operatorów sieci oraz regulacji prawnych stosowanych w różnych krajach przedstawiono ewolucję zasady otwartej i neutralnej sieci oraz jej przyczyny i potencjalne skutki dla dalszego rozwoju sieci i świadczonych za jej pośrednictwem usług. W końcowej części artykułu przedstawione zostały propozycje dotyczące prawnego usankcjonowania zasad dotyczących neutralności sieciowej na poziomie międzynarodowym i krajowym.

Słowa kluczowe: neutralność sieci, regulacje

Net Neutrality – A Dogma or A Postulate

Summary

The article describes the origins and meaning of the concept of net neutrality in relation to ICT infrastructure, especially the Internet. The evolution of open and neutral network and its foundations and consequences for the development of the network and the services provided are presented on the example of market practices of network operators and regulations applicable in the various countries. The final part of the article presents proposals relating to the determination of the rules on net neutrality at the international and national levels.

Keywords: net neutrality, regulations

JEL: O30, O34, O38