I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie neutralności sieci, zarządzania ruchem oraz ochrony prywatności i danych osobowych

(2012/C 34/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([2]), w szczególności jego art. 41 ust. 2,

uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([3]),

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

I.1. **Informacje ogólne**

1. W dniu 19 kwietnia 2011 r. Komisja przyjęła komunikat w sprawie otwartego Internetu i neutralności sieci w Europie ([4]).

2. Niniejszą opinię można uznać za reakcję EIOD na ten komunikat; jej celem jest wniesienie wkładu w toczącą się w UE debatę na temat neutralności sieci, zwłaszcza w aspektach związanych z ochroną danych i prywatnością.

([1]) Dz.U. L 281 z 23.11.1995, s. 31 („dyrektywa o ochronie danych").
([2]) Dz.U. L 8 z 12.1.2001, s. 1 („rozporządzenie o ochronie danych").
([3]) Dz.U. L 201 z 31.7.2002, s. 37, zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. (zob. przypis 15) („dyrektywa o prywatności i łączności elektronicznej").
([4]) COM(2011) 222 wersja ostateczna.

3. Opinia stanowi rozwinięcie odpowiedzi ([5]) EIOD na konsultacje społeczne Komisji dotyczące otwartego Internetu i neutralności sieci w Europie, które poprzedziły wydanie komunikatu przez Komisję. EIOD odnotował również niedawny projekt konkluzji Rady w sprawie neutralności sieci ([6]).

I.2. **Koncepcja neutralności sieci**

4. W toczącej się debacie na temat neutralności sieci chodzi o to, czy dostawcom usług internetowych ([7]) należy pozwolić na ograniczanie, filtrowanie lub blokowanie dostępu do Internetu lub też wpływanie na jego parametry w inny sposób. Koncepcja neutralności sieci wywodzi się z poglądu, że informacje w Internecie powinny być przekazywane w sposób bezstronny bez względu na treść, miejsce przeznaczenia lub źródło, a użytkownicy powinni mieć możliwość decydowania, jakich aplikacji, usług i sprzętu chcą używać. Oznacza to, że dostawcy usług internetowych nie mogą według swojego uznania przyznawać priorytetu ani też spowalniać dostępu do pewnych aplikacji lub usług takich jak sieci *peer-to-peer* („P2P") ([8]).

5. Filtrowanie, blokowanie i inspekcja ruchu sieciowego rodzi ważne pytania, często niedostrzegane lub lekceważone, dotyczące poufności komunikacji oraz poszanowania prywatności osób fizycznych i ich danych osobowych podczas korzystania z Internetu. Na przykład niektóre techniki inspekcji wiążą się z monitorowaniem treści komunikacji, odwiedzonych stron internetowych, wysłanych i otrzymanych wiadomości e-mail, czasu poszczególnych zdarzeń itp., co umożliwia filtrowanie komunikacji.

6. Dokonując inspekcji danych o komunikacji, dostawcy usług internetowych mogą naruszać poufność komunikacji, która jest prawem podstawowym zagwarantowanym przez art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności („EKPC") oraz art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karty"). Poufność podlega ponadto ochronie na mocy prawodawstwa wtórnego UE, a mianowicie art. 5 dyrektywy o prywatności i łączności elektronicznej.

I.3. **Treść i struktura opinii**

7. Zdaniem EIOD każda poważna debata na temat neutralności sieci musi uwzględniać kwestię poufności komunikacji, jak również inne implikacje z punktu widzenia prywatności i ochrony danych.

8. Niniejsza opinia stanowi wkład w tę debatę toczącą się w UE. Jej cel jest trojaki:

— wskazuje się w niej na znaczenie prywatności i ochrony danych w kontekście trwających dyskusji o neutralności sieci. W szczególności podkreśla się potrzebę poszanowania istniejących zasad dotyczących poufności komunikacji. Dopuszczalne powinny być jedynie praktyki cechujące się poszanowaniem tych zasad,

— neutralność sieci odnosi się do względnie nowych możliwości technicznych i na razie brakuje doświadczeń co do stosowania ram prawnych w tej dziedzinie. W związku z tym w obecnej opinii zawarto wskazówki dotyczące tego, w jaki sposób dostawcy usług internetowych muszą stosować ramy prawne ochrony danych i przestrzegać ich, jeżeli filtrują i blokują ruch sieciowy oraz dokonują jego inspekcji. Powinny one okazać się pomocne dla dostawców usług internetowych, jak również dla władz odpowiedzialnych za egzekwowanie tych ram,

— jeżeli chodzi o ochronę danych i prywatność, w niniejszej opinii zidentyfikowano obszary zasługujące na szczególną uwagę oraz mogące wymagać działań na szczeblu UE. Jest to szczególnie ważne w związku z toczącą się debatą na szczeblu UE i środkami, które mogą zostać wdrożone przez Komisję w tym kontekście.

([5]) W swojej odpowiedzi EIOD podkreślił znaczenie uwzględnienia obok innych praw oraz wartości zagadnień ochrony danych i prywatności. Odpowiedź ta jest dostępna przed adresem: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Dostępny pod adresem: http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Obejmuje to świadczenie usług dotyczących zarówno stacjonarnego, jak i mobilnego dostępu do Internetu.

([8]) Zasada ta nie dotyczy jednak ograniczania przez dostawców usług internetowych szybkości łącza lub ilości informacji, które abonent może przesłać lub otrzymać w przypadku abonamentu z ograniczeniem szerokości pasma lub ilości danych. W związku z tym zgodnie z zasadą neutralności sieci dostawcy usług internetowych mogliby nadal oferować abonamenty internetowe z ograniczeniem dostępu w oparciu o kryteria takie jak prędkość lub ilość danych, jeżeli tylko nie wymagałoby to faworyzowania lub dyskryminacji konkretnych treści.

9. EIOD ma świadomość, że neutralność sieci pociąga za sobą inne (opisane szerzej w dalszej części opinii) zagadnienia, na przykład związane z dostępem do informacji. Zagadnienia te uwzględniono jedynie w stopniu, w jakim są związane z ochroną danych i prywatnością lub mają na nie wpływ.

10. Struktura niniejszej opinii jest następująca: w sekcji II przedstawiono krótki przegląd praktyk dostawców usług internetowych w zakresie filtrowania. W sekcji III przedstawiono w zarysie ramy prawne UE dotyczące neutralności sieci. W sekcji IV zamieszczono opis techniczny wraz z oceną skutków poszczególnych technik z punktu widzenia prywatności. W sekcji V przeanalizowano aspekty praktyczne związane z zastosowaniem obecnych ram UE dotyczących prywatności i ochrony danych. W sekcji VI rozwinięto tę analizę, przedstawiając sugestie dotyczące kształtowania polityki i wskazując obszary, w których niezbędne może być wyjaśnienie oraz udoskonalenie ram prawnych. W sekcji VII zaprezentowano wnioski.

II. **NEUTRALNOŚĆ SIECI A POLITYKA ZARZĄDZANIA RUCHEM**

Coraz częstsze wykorzystanie polityki zarządzania ruchem

11. Obecnie dostawcy usług internetowych monitorują ruch sieciowy i wpływają na niego tylko w pewnych sytuacjach. Na przykład stosują oni techniki inspekcji i ograniczają przepływ informacji, aby zapewnić bezpieczeństwo sieci, np. w celu zwalczania wirusów. Dlatego też, ogólnie rzecz biorąc, Internet rozwija się, zachowując w znacznym stopniu neutralność.

12. W ostatnich latach część dostawców usług internetowych wykazuje jednak zainteresowanie inspekcją ruchu sieciowego w celu wyodrębnienia poszczególnych jego rodzajów i stosowania wobec nich różnych zasad, na przykład blokowania konkretnych usług lub udostępniania innych na preferencyjnych zasadach. Określa się to czasem mianem „polityki zarządzania ruchem” ([9]).

13. Dostawcy usług internetowych mają różnorakie powody, by dokonywać inspekcji i rozróżniania ruchu. Polityka zarządzania ruchem może na przykład pomagać w zarządzaniu ruchem podczas okresów znacznego obciążenia, choćby przez przyznawanie wysokiego priorytetu ruchowi uwarunkowanemu czasowo (jak transmisja strumieniowa wideo) oraz obniżanie priorytetu innych rodzajów ruchu, które mogą być mniej wrażliwe na upływ czasu (jak P2P) ([10]). Ponadto zarządzanie ruchem może być dla dostawcy usług internetowych sposobem uzyskania potencjalnego strumienia przychodów z różnych źródeł. Z jednej strony dostawcy usług internetowych mogliby pobierać opłaty od dostawców usług związanych z treścią, np. tych, których usługi wymagają większej szerokości pasma, dając im w zamian priorytet (a więc prędkość). Oznacza to, że dostęp do pewnej usługi, na przykład wyświetlania filmów na żądanie, byłby szybszy niż dostęp do innej podobnej usługi, w związku z którą nie podpisano umowy o wyższej prędkości transmisji. Przychody można byłoby również uzyskiwać od abonentów, którzy są zainteresowani wnoszeniem wyższych (lub niższych) opłat za zróżnicowane rodzaje abonamentów. Na przykład abonament bez dostępu do P2P mógłby być tańszy od abonamentu dającego nieograniczony dostęp.

14. Oprócz powodów skłaniających samych dostawców usług internetowych do wykorzystywania polityki zarządzania ruchem, wdrożeniem takiej polityki mogą też być zainteresowane inne podmioty. Jeżeli dostawcy usług internetowych będą zarządzać swoimi sieciami i dokonywać inspekcji treści przepływających przez ich urządzenia, wzrośnie prawdopodobnie ich zdolność do wykrywania domniemanego wykorzystania sieci niezgodnie z prawem, np. naruszania praw autorskich lub rozpowszechniania pornografii.

([9]) Zob. np. przyjęty w dniu 27 maja 2011 r. raport OFCOM zatytułowany „Site blocking to reduce online copyright infringement” („Blokowanie stron internetowych w celu ograniczenia naruszania praw autorskich w internecie”) dostępny pod adresem: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf „Niektórzy dostawcy usług internetowych już teraz stosują w swoich sieciach systemy inspekcji pakietów do celów zarządzania ruchem i innych, zakładamy więc, że rozwiązanie takie można wdrożyć, choć będzie się to wiązać ze znacznymi komplikacjami i kosztami dla podmiotów, które nie uruchomiły jeszcze takich usług. Możliwe, że w perspektywie krótko- i średnioterminowej, ze względu na wymagane nakłady inwestycyjne, głęboką inspekcję pakietów będą w stanie wdrożyć tylko więksi dostawcy usług internetowych”.

([10]) Jakość działania aplikacji czasu rzeczywistego takich jak strumieniowa transmisja wideo zależy między innymi od latencji, tj. opóźnienia wynikającego na przykład z obciążenia sieci ruchem.

Inne interesy, w tym ochrona danych i prywatność

15. Opisana powyżej tendencja wywołała debatę na temat legalności tego rodzaju praktyk, a zwłaszcza tego, czy w prawie należy bardziej szczegółowo określić obowiązki związane z neutralnością sieci.

16. Coraz częstsze wykorzystywanie polityki zarządzania ruchem przez dostawców usług internetowych mogłoby ograniczyć dostęp do informacji. Gdyby takie praktyki stały się powszechne i użytkownicy nie mieliby możliwości dostępu do całego Internetu w jego obecnej postaci (lub byłoby to bardzo kosztowne), zagrażałoby to dostępowi do informacji oraz zdolności użytkowników do wysyłania i otrzymywania wybranych przez siebie treści przy użyciu wybranych przez siebie aplikacji lub usług. Tego problemu mogłaby pozwolić uniknąć wiążąca prawnie zasada neutralności sieci.

17. Tutaj pojawiają się implikacje zarządzania ruchem przez dostawców usług internetowych z punktu widzenia ochrony danych i prywatności. W szczególności:

— gdy dostawcy usług internetowych przetwarzają dane o ruchu wyłącznie w celu skierowania przepływu informacji od nadawcy do odbiorcy, generalnie przetwarzają dane w ograniczonym zakresie ([11]). Podobnie jak poczta przetwarza informacje podane na kopercie listu, dostawca usług internetowych przetwarza informacje niezbędne w celu skierowania wiadomości do odbiorcy. Nie jest to sprzeczne z wymogami prawnymi ochrony danych, prywatności i poufności komunikacji,

— gdy jednak dostawcy usług internetowych dokonują inspekcji danych o komunikacji w celu rozróżnienia poszczególnych strumieni komunikacji i zastosowania konkretnej polityki, która może być niekorzystna z punktu widzenia osób fizycznych, implikacje są bardziej znaczące. Zależnie od okoliczności w danym przypadku i od rodzaju dokonywanej analizy przetwarzanie może wyraźnie naruszać prywatność oraz ingerować w dane osobowe osób fizycznych. Jest to bardziej oczywiste, gdy polityka zarządzania prowadzi do ujawnienia treści komunikacji internetowej osób fizycznych, w tym wysłanych i otrzymanych wiadomości e-mail, odwiedzonych stron internetowych, pobranych lub przesłanych plików itp.

III. **PRZEGLĄD RAM PRAWNYCH UE DOTYCZĄCYCH NEUTRALNOŚCI SIECI ORAZ EWOLUCJI POLITYKI**

III.1. **Ramy prawne w skrócie**

18. Do 2009 r. w instrumentach ustawodawczych UE brakowało przepisów wyraźnie zabraniających dostawcom usług internetowych filtrowania lub blokowania lub też naliczania abonentom dodatkowych opłat za dostęp do usług. Nie było w nich zarazem przepisów wyraźnie uznających istnienie takich praktyk. Sytuacja była do pewnego stopnia niepewna.

19. Pakiet telekomunikacyjny z 2009 r. zmienił to, wprowadzając przepisy sprzyjające otwartości Internetu. Na przykład w art. 8 ust. 4 wspólnych ram regulacyjnych sieci i usług łączności elektronicznej („dyrektywa ramowa") na organy regulacyjne nakłada się obowiązek wspierania zdolności użytkowników końcowych do dostępu do informacji oraz korzystania z dowolnych aplikacji i usług ([12]). Przepis ten dotyczy całości sieci, nie zaś poszczególnych dostawców usług. W niedawnym projekcie konkluzji Rady również podkreślono potrzebę zachowania otwartości Internetu ([13]).

([11]) Nie uwzględnia to działań mających na celu zwiększenie bezpieczeństwa sieci i wykrycie szkodliwego ruchu oraz operacji wymaganych w związku z rozliczeniami i połączeniami z innymi operatorami. Nie uwzględnia też obowiązków wynikających z dyrektywy w sprawie zatrzymywania danych – dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz.U. L 105 z 13.4.2006, s. 54) („dyrektywa w sprawie zatrzymywania danych").

([12]) Dyrektywa 2002/21/WE z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej zmieniona dyrektywą 2009/140/WE i rozporządzeniem (WE) nr 544/2009 (Dz.U. L 337 z 18.12.2009, s. 37).

([13]) Zob. pkt 3 lit. e), w którym Rada wskazuje: „Potrzeba utrzymania otwartości Internetu przy jednoczesnym zagwarantowaniu, że będzie on mógł nadal dostarczać wysokiej jakości usług w ramach wspierających prawa podstawowe takie jak wolność wypowiedzi i wolność działalności gospodarczej oraz cechujących się poszanowaniem tych praw", oraz pkt 8 lit. d), w którym państwa członkowskie zachęca się, aby „celem swojej polityki uczyniły otwarty i neutralny charakter Internetu".

20. Dyrektywa o usłudze powszechnej ([14]) określa bardziej konkretne obowiązki. W art. 20 i 21 ustanowiono wymogi dotyczące przejrzystości w odniesieniu do ograniczeń dostępu do usług i aplikacji lub korzystania z nich. Wprowadzono też wymóg minimalnego poziomu jakości usług.

21. W odniesieniu do praktyk dostawców usług internetowych związanych z inspekcją komunikacji między osobami fizycznymi, w motywie 28 dyrektywy zmieniającej dyrektywę o usłudze powszechnej i dyrektywę o prywatności i łączności elektronicznej ([15]) podkreślono: „w zależności od zastosowanej technologii i rodzaju ograniczenia, takie ograniczenia mogą wymagać zgody użytkownika zgodnie z dyrektywą 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej)". Tak więc w motywie 28 przypomina się o potrzebie zgody na podstawie art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej na wszelkie ograniczenia oparte na monitorowaniu komunikacji. W sekcji IV poniżej przeanalizowano zastosowanie art. 5 ust. 1 oraz ogólnych ram prawnych dotyczących ochrony danych i prywatności.

22. Wreszcie, w art. 22 ust. 3 dyrektywy o usłudze powszechnej przyznano krajowym organom regulacyjnym uprawnienia do nałożenia w razie potrzeby na dostawców usług internetowych minimalnych wymogów w zakresie jakości usług, aby zapobiec pogorszeniu się jakości usług oraz utrudnieniom lub spowolnieniom ruchu w sieciach publicznych.

23. Powyższe oznacza, że ogólną aspiracją na szczeblu UE jest otwarty Internet (zob. art. 8 ust. 4 dyrektywy ramowej). Ten cel polityczny, który dotyczy sieci jako całości, nie wiąże się jednak bezpośrednio z zakazami wobec poszczególnych dostawców usług internetowych ani z nakładanymi na nich obowiązkami. Innymi słowy, dostawca usług internetowych może wdrożyć politykę zarządzania siecią, w ramach której może wyłączyć dostęp do pewnych aplikacji, pod warunkiem, że użytkownicy końcowi uzyskali pełne informacje oraz wyrazili swoją zgodę w dobrowolny, konkretny i jednoznaczny sposób.

24. Sytuacja może się różnić w poszczególnych państwach członkowskich. W niektórych państwach członkowskich dostawcy usług internetowych mogą pod pewnymi warunkami wdrażać politykę zarządzania ruchem, na przykład blokować aplikacje takie jak telefonia internetowa (w ramach tańszego abonamentu internetowego) pod warunkiem, że osoby fizyczne wyraziły na to dobrowolną, konkretną i jednoznaczną, świadomą zgodę. Inne państwa członkowskie zdecydowały się wzmocnić zasadę neutralności sieci. Na przykład w lipcu 2011 r. holenderski parlament uchwalił ustawę ogólnie zabraniającą dostawcom utrudniania lub spowalniania działania aplikacji lub usług w Internecie (takich jak telefonia internetowa), chyba że jest to niezbędne, aby zminimalizować zatory, z powodów związanych z integralnością danych lub bezpieczeństwem, w celu walki ze spamem lub zgodnie z nakazem sądowym ([16]).

III.2. **Komunikat w sprawie neutralności sieci**

25. W swoim komunikacie w sprawie neutralności sieci ([17]) Komisja Europejska stwierdziła, że sytuacja w dziedzinie neutralności sieci wymaga monitorowania i dalszej analizy. Jej politykę określa się jako polegającą na „czekaniu i obserwowaniu" przed rozważeniem dalszych kroków regulacyjnych.

([14]) Dyrektywa 2002/22/WE zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniającą dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.U. L 337 z 18.12.2009, s. 11). Por. również art. 1 ust. 3, w którym stwierdza się, że dyrektywa nie dopuszcza ani nie zakazuje warunków – nakładanych przez dostawców usług internetowych – ograniczających użytkownikom końcowym dostęp do usług i aplikacji lub korzystanie z nich, w przypadku gdy jest to dopuszczalne na mocy prawa krajowego i zgodne z prawem wspólnotowym; ustanawia jednak obowiązek dostarczania informacji dotyczących takich warunków.

([15]) Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów.

([16]) Treść holenderskiej poprawki w oryginale można znaleźć pod adresem: https://zoek.officielebekendmakingen.nl/kst-32549-A.html Jak donosiła prasa, zdecydowano się na nią nie ze względu na kwestie związane z ochroną danych i prywatnością, ale ze względu na potrzebę zagwarantowania, że użytkownicy nie zostaną pozbawieni dostępu do informacji lub nie zostanie on ograniczony. Wydaje się zatem, że motywacją do wprowadzenia poprawki były zagadnienia związane z dostępem do informacji.

([17]) Porównaj: przypis 4.

26. W komunikacie Komisji stwierdza się, że wszelkie środki i dalsze kroki regulacyjne będą podlegać dogłębnej ocenie pod kątem ochrony danych oraz prywatności. W projekcie konkluzji Rady również odnotowano zagadnienia związane z ochroną danych i prywatnością ([18]).

27. Z punktu widzenia ochrony danych i prywatności należy zadać sobie pytanie, czy polityka polegająca na czekaniu i obserwowaniu jest wystarczająca. Chociaż w obecnych ramach ochrony danych i prywatności przewidziano pewne zabezpieczenia, zwłaszcza wynikające z zasady poufności komunikacji, niezbędne wydaje się ścisłe monitorowanie przestrzegania przepisów oraz wydanie wytycznych co do kilku kwestii, które nie są w pełni jasne. Ponadto należy przedstawić pewne przemyślenia co do tego, w jaki sposób można wyjaśnić i dodatkowo udoskonalić te ramy w świetle rozwoju techniki. Jeżeli monitorowanie ujawni, że rynek ewoluuje w kierunku masowej inspekcji komunikacji w czasie rzeczywistym i występują problemy z przestrzeganiem ram, niezbędne okażą się środki ustawodawcze. Konkretne sugestie ich dotyczące zamieszczono w sekcji VI.

IV. **UWARUNKOWANIA TECHNICZNE ORAZ ZWIĄZANE Z NIMI IMPLIKACJE DLA PRYWATNOŚCI I OCHRONY DANYCH**

28. Przed dalszym zagłębieniem się w temat trzeba uważniej przyjrzeć się technikom inspekcji, jakie mogą stosować dostawcy usług internetowych w celu zarządzania ruchem, i temu, jak może to wpłynąć na zasadę neutralności sieci. Implikacje takich technik dla prywatności i ochrony danych znacząco się różnią w zależności od tego, która technika lub techniki są wykorzystywane. Poniższe informacje techniczne są niezbędne w celu zrozumienia i prawidłowego stosowania ram prawnych ochrony danych opisanych w sekcji V. Należy jednak zaznaczyć, że jest to obszar złożony i ulegający nieustannym zmianom. Dlatego też poniższy opis nie został stworzony z założeniem, że będzie przedstawiał wyczerpujący i w pełni aktualny stan rzeczy, ma on jedynie dostarczyć informacji technicznych niezbędnych w celu zrozumienia argumentacji prawnej.

IV.1. **Przesyłanie informacji przez Internet: podstawy**

29. Gdy użytkownik przesyła wiadomość przez Internet, przesyłane informacje są dzielone na pakiety. Pakiety te są przesyłane przez Internet od nadawcy do odbiorcy. Każdy pakiet zawiera między innymi informacje o swoim źródle i miejscu przeznaczenia. Ponadto dostawcy usług internetowych mogą obudowywać pakiety dodatkowymi warstwami i protokołami ([19]) wykorzystywanymi w celu zarządzania poszczególnymi strumieniami ruchu w sieci danego dostawcy usług.

30. Wracając do analogii z listem, korzystanie z protokołu służącego przesyłaniu informacji w sieci jest równoznaczne z włożeniem listu do koperty zaadresowanej w widoczny dla poczty sposób, a następnie z przekazaniem go poczcie do doręczenia. Poczta może w wewnętrznym obiegu używać dodatkowych protokołów w celu zarządzania wszystkimi przesyłanymi kopertami – celem jest, aby każda koperta dotarła do miejsca przeznaczenia zgodnie z pierwotnym zamiarem nadawcy. Posługując się tą analogią, każdy pakiet składa się z dwóch części – jedną jest ładunek IP, który zawiera treść wiadomości i stanowi odpowiednik listu. Zawiera on informacje skierowane jedynie do odbiorcy. Drugą częścią pakietu jest nagłówek IP, który zawiera między innymi adres nadawcy i odbiorcy, stanowiąc odpowiednik koperty. Nagłówek IP pozwala dostawcom usług internetowych i innym pośrednikom przesłać ładunek z adresu źródłowego pod adres docelowy.

31. Dostawcy usług internetowych i inni pośrednicy dbają o to, aby pakiety IP przepływały w sieci między węzłami, które odczytują informacje zawarte w nagłówkach IP, porównują je z tablicami trasowania, a następnie przesyłają pakiet do kolejnego węzła na drodze do jego miejsca przeznaczenia. Proces ten jest dokonywany w sieci przy wykorzystaniu podejścia opartego na zapewnieniu najwyższej możliwej

([18]) Zob. pkt 4 lit. e), w którym Rada wskazuje: „Istnieją pewne obawy, zgłaszane głównie przez konsumentów i organy ochrony danych, dotyczące ochrony danych osobowych".

([19]) Jak opisano bardziej szczegółowo w sekcji IV.2, protokoły takie (HTTP, FTP itp.) służą zakodowaniu informacji przesyłanych między punktem początkowym a końcowym w uzgodniony sposób, aby uczestnicy komunikacji wzajemnie się zrozumieli.

jakości (ang. *best effort*) bez przechowywania danych (ang. *memoryless*) – wszystkie pakiety docierające do węzła są traktowane w neutralny sposób. Po przesłaniu ich do następnego węzła nie ma potrzeby zachowywania informacji o nich w routerze ([20]).

IV.2. **Techniki inspekcji**

32. Jak wskazano powyżej, dostawcy usług internetowych odczytują nagłówki IP, aby kierować pakiety do miejsca przeznaczenia. Jak jednak wspomniano, analiza ruchu (obejmująca nagłówki i ładunek IP) może być dokonywana w innych celach przy użyciu odmiennych technologii. Nowe podejście może wiązać się np. ze spowalnianiem pewnych aplikacji wykorzystywanych przez użytkowników, takich jak P2P, lub też przyspieszaniem ruchu w odniesieniu do pewnych usług takich jak wideo na żądanie dla wnoszących opłaty za to abonentów. Chociaż wszystkie techniki inspekcji polegają formalnie na inspekcji pakietów, wiążą się z różnym stopniem naruszenia prywatności. Istnieją dwie podstawowe kategorie technik inspekcji. Pierwsze bazują tylko na nagłówku IP, drugie natomiast również na ładunku IP.

Techniki bazujące na informacjach zawartych w nagłówku IP. Inspekcja nagłówka pakietu IP ujawnia pewne pola, które mogą pozwolić dostawcom usług internetowych wdrożyć niektóre rodzaje polityki zarządzania ruchem. Te techniki, oparte wyłącznie na inspekcji nagłówków IP, polegają na przetworzeniu danych, które są w zasadzie przeznaczone do trasowania informacji, w innym celu (tj. rozróżniania ruchu). Badając adres źródłowy IP, dostawca usług internetowych może powiązać go z konkretnym abonentem i zastosować konkretną politykę, na przykład polegającą na skierowaniu pakietu szybszym lub wolniejszym łączem. Badając adres docelowy IP, dostawca usług internetowych też może zastosować konkretną politykę, na przykład blokując lub filtrując dostęp do pewnych stron internetowych.

Techniki bazujące na głębszej inspekcji. Głęboka inspekcja pakietów pozwala dostawcy usług internetowych uzyskać dostęp do informacji skierowanych wyłącznie do odbiorcy wiadomości. Wracając do przykładu pocztowego, podejście to jest równoważne otwarciu koperty i przeczytaniu znajdującego się wewnątrz listu w celu dokonania analizy treści wiadomości (zawartej w pakietach IP), aby zastosować konkretną politykę sieciową. Istnieją różne sposoby dokonywania inspekcji, z których każdy wiąże się z innymi zagrożeniami dla osoby, której dane dotyczą.

— *Głęboka inspekcja pakietów oparta na analizie protokołów i danych statystycznych*. Oprócz protokołu IP, którego celem jest umożliwienie przesyłania danych przez Internet, istnieją dodatkowe protokoły (warstwy transportowej, sesji, prezentacji i aplikacji itp.), które służą zakodowaniu przesyłanych informacji w uzgodniony sposób. Celem tych protokołów jest zapewnienie wzajemnego zrozumienia między stronami komunikacji. Istnieją na przykład protokoły związane z przeglądaniem stron internetowych ([21]), inne zaś służą przesyłaniu plików ([22]) itp. W związku z tym celem technik inspekcji opartych na badaniu protokołów w połączeniu z analizą statystyczną jest określenie pewnych wzorców lub „odcisków palca" pozwalających stwierdzić, o jaki protokół chodzi ([23]). Te techniki inspekcji pozwalają dostawcom usług internetowych zidentyfikować rodzaj komunikacji (e-mail, przeglądanie sieci, przesyłanie plików), a w pewnych przypadkach zidentyfikować wykorzystywaną usługę lub aplikację, jak w przypadku niektórych rodzajów telefonii internetowej, gdzie wykorzystywane protokoły bardzo wyraźnie identyfikują konkretnego sprzedawcę lub dostawcę usług. Już sama wiedza o rodzaju komunikacji może umożliwić dostawcom usług internetowych stosowanie konkretnych rodzajów polityki zarządzania ruchem – na przykład zablokowanie ruchu WWW. Może ona też być pierwszym krokiem umożliwiającym dostawcy usług internetowych przeprowadzenie dalszej analizy, potencjalnie wymagającej pełnego dostępu do metadanych i treści wiadomości.

([20]) Osprzęt sieciowy wykorzystywany w Internecie korzysta niemniej z protokołów trasowania opartych na rejestracji aktywności, przetwarzaniu statystyk ruchu i wymianie informacji z pozostałym osprzętem sieciowym w celu kierowania pakietów IP najefektywniejszą drogą. Na przykład jeżeli dane łącze jest przeciążone lub uszkodzone i router otrzyma taką informację, aktualizuje on swoją tablicę trasowania, uwzględniając alternatywną drogę, która nie wykorzystuje tego łącza. Warto również zauważyć, że gromadzenie i przetwarzanie danych może w pewnych przypadkach odbywać się w związku z rozliczeniami, a wręcz zgodnie z wymogami dyrektywy w sprawie zatrzymywania danych.

([21]) HTTP (*Hypertext Transfer Protocol*) lub HTML (*Hypertext Markup Language*).

([22]) FTP (*File Transfer Protocol*).

([23]) Istnieją różne sposoby identyfikacji wykorzystywanych protokołów. Można przeszukiwać konkretne pola protokołów wewnętrznych, np. w celu identyfikacji portów wykorzystywanych do nawiązania łączności. Można też uzyskać charakterystykę statystyczną strumienia komunikacji, analizując pewne konkretne pola i korelując protokoły wykorzystywane równocześnie w komunikacji między dwoma adresami IP.

— *Głęboka inspekcja pakietów oparta na analizie treści wiadomości*. Wreszcie, możliwa jest też inspekcja metadanych ([24]) oraz treści samej wiadomości. Technika ta polega na przechwyceniu wszystkich pakietów IP składających się na pierwotny strumień komunikacji w celu pełnej rekonstrukcji i analizy pierwotnej treści wiadomości. Na przykład w celu wykrycia szkodliwej lub nielegalnej treści takiej jak wirusy czy pornografia dziecięca niezbędna jest rekonstrukcja samej treści w celu jej analizy. Należy zauważyć, że czasem przesyłana wiadomość może być zaszyfrowana przez strony komunikacji między punktem początkowym i końcowym, co utrudnia dostawcom usług internetowych dokonanie analizy treści wiadomości.

IV.3. **Implikacje dla prywatności i ochrony danych**

33. Techniki inspekcji oparte na nagłówkach IP, a w szczególności oparte na inspekcji pakietów wiążą się z monitorowaniem i filtrowaniem danych oraz mają poważne implikacje z punktu widzenia prywatności i ochrony danych. Mogą również być nie do pogodzenia z prawem do poufności komunikacji.

34. Wgląd do komunikacji osób fizycznych ma sam w sobie poważne implikacje z punktu widzenia prywatności i ochrony danych. Problem ten ma jednak charakter ogólniejszy, gdyż zależnie od celów, jakim służą monitorowanie i przechwytywanie danych, implikacje z punktu widzenia prywatności mogą być jeszcze większe. Inspekcja komunikacji jedynie w celu zapewnienia prawidłowego funkcjonowania systemu nie jest bowiem tym samym co inspekcja komunikacji w celu wdrożenia polityki mogącej mieć wpływ na osoby fizyczne. Gdy polityka związana z ruchem i selekcją ma na celu tylko uniknięcie zatorów sieciowych, zazwyczaj nie ma to większych implikacji z punktu widzenia prywatności osób fizycznych. Polityka zarządzania ruchem może jednak służyć blokowaniu pewnych treści lub wpływaniu na komunikację, np. przez stosowanie reklamy behawioralnej. W tych przypadkach naruszenie prywatności jest głębsze. Sytuacja staje się poważniejsza, gdy zdamy sobie sprawę, że takie informacje byłyby gromadzone nie w odniesieniu do niewielkiej grupy osób, ale w sposób uogólniony, w odniesieniu do wszystkich klientów dostawców usług internetowych ([25]). Jeżeli wszyscy dostawcy usług internetowych będą stosować techniki filtrowania, może to doprowadzić do ogólnego monitorowania wykorzystania Internetu. Ponadto, jeżeli skupimy się na rodzaju przetwarzanych informacji, ryzyko dla prywatności jest oczywiście poważne, gdyż znaczna część gromadzonych informacji będzie prawdopodobnie bardzo wrażliwa, a po zgromadzeniu staną się one dostępne dla dostawców usług internetowych i podmiotów pozyskujących od nich informacje. Ponadto informacje te mogą również być bardzo wartościowe z handlowego punktu widzenia. Już sam ten fakt skutkuje dużym ryzykiem rozrastania się funkcji systemu – pierwotny cel może łatwo przekształcić się w komercyjne lub inne wykorzystanie zgromadzonych informacji.

35. Prawidłowe zastosowanie technik monitorowania, inspekcji i filtrowania musi być zgodne ze stosownymi zabezpieczeniami dotyczącymi ochrony danych i prywatności, w których określono ograniczenia co do dopuszczalnych czynności i okoliczności ich dokonywania. W następnej sekcji dokonano przeglądu stosownych zabezpieczeń na mocy obecnych ram prawnych UE dotyczących prywatności i ochrony danych.

V. **ZASTOSOWANIE RAM PRAWNYCH UE DOTYCZĄCYCH PRYWATNOŚCI I OCHRONY DANYCH**

36. Wspólnotowe ramy ochrony danych są neutralne z technologicznego punktu widzenia, nie regulują więc konkretnych technik inspekcji takich jak opisane powyżej. Dyrektywa o prywatności i łączności elektronicznej reguluje kwestie prywatności związane ze świadczeniem usług łączności elektronicznej w

([24]) Każdy protokół zawiera w nagłówku pewne pola dostarczające dodatkowych nieformalnych informacji o przesyłanej wiadomości. Dlatego też zawartość tych pól można określić jako metadane związane z wiadomością. Przykładem takich pól może być numer wykorzystywanego portu – gdy jest to np. numer 80, prawdopodobne jest, że chodzi o przeglądanie stron internetowych.

([25]) Możliwość śledzenia posiadają oczywiście nie tylko dostawcy usług internetowych. Dostawcy reklam również potrafią śledzić korzystanie z różnych stron internetowych przez użytkowników, korzystając z plików *cookie* osób trzecich (ang. *third party cookies*). Niedawno opublikowano artykuł dowodzący, że Google jest obecny na 97 ze 100 najważniejszych stron internetowych, co oznacza, że potrafi śledzić użytkowników, którzy nie zrezygnowali z używania plików *cookie* osób trzecich, gdy wchodzą oni na te popularne witryny. Zob.: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning* (29 lipca 2011 r.). Artykuł dostępny w SSRN: http://ssrn.com/abstract=1898390. Problemem śledzenia użytkowników przy wykorzystaniu plików *cookie* osób trzecich zajęła się Grupa Robocza Art. 29. Zob. opinia 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta w dniu 22 czerwca 2010 r. (WP 171).

sieciach publicznych (zazwyczaj w związku z dostępem do Internetu i telefonią) ([26]), a dyrektywa o ochronie danych reguluje ogólnie przetwarzanie danych. Jako całość wspomniane ramy prawne ustanawiają różne obowiązki spoczywające na dostawcach usług internetowych, którzy przetwarzają oraz monitorują dane dotyczące ruchu i komunikacji.

V.1. **Podstawy prawne przetwarzania danych dotyczących ruchu i treści**

37. Na mocy prawodawstwa o ochronie danych przetwarzanie danych osobowych, jak w tym przypadku przetwarzanie danych dotyczących ruchu i komunikacji, wymaga stosownych podstaw prawnych. Oprócz tego ogólnego wymagania w pewnych przypadkach mogą obowiązywać wymagania szczegółowe.

38. W omawianym przypadku dane osobowe przetwarzane przez dostawców usług internetowych to dane o ruchu i treść komunikacji. Zarówno treść komunikacji, jak i dane o ruchu są chronione przez prawo do poufności korespondencji zagwarantowane przez art. 8 EKPC oraz przez art. 7 i 8 Karty. W szczególności w art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej, zatytułowanym „Poufność komunikacji", zobowiązuje się państwa członkowskie do zapewnienia poufności komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. Jednocześnie w art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej wskazuje się, że przetwarzanie danych o ruchu i treści przez dostawców usług internetowych może być w pewnych okolicznościach dozwolone za zgodą użytkowników. Czyni się to, zakazując „słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1". Poniżej kwestię tę opisano bardziej szczegółowo.

39. Oprócz zgody zainteresowanych użytkowników w dyrektywie o prywatności i łączności elektronicznej przewidziano inne podstawy legalności przetwarzania danych o ruchu i komunikacji przez dostawców usług internetowych. Stosownymi podstawami prawnymi przetwarzania są w tym przypadku: (i) świadczenie usługi; (ii) zapewnienie bezpieczeństwa usługi oraz (iii) minimalizacja zatorów. W punkcie (iv) poniżej omówiono inne możliwe podstawy legalności polityki zarządzania opartej na danych o ruchu lub komunikacji.

(i) Podstawy prawne świadczenia usługi

40. Zgodnie z opisem w sekcji IV dostawcy usług internetowych przetwarzają informacje w nagłówkach IP, aby skierować każdy pakiet IP do jego miejsca przeznaczenia. W art. 6 ust. 1 i ust. 2 dyrektywy o prywatności i łączności elektronicznej dopuszczono przetwarzanie danych o ruchu do celów przekazania komunikatu. Tak więc dostawcy usług internetowych mogą przetwarzać informacje niezbędne w celu świadczenia usługi.

(ii) Podstawy prawne zapewnienia bezpieczeństwa usługi

41. Zgodnie z art. 4 dyrektywy o prywatności i łączności elektronicznej na dostawcy usług internetowych spoczywa ogólny obowiązek podjęcia stosownych działań w celu zapewnienia bezpieczeństwa oferowanych przez niego usług. Filtrowanie wirusów może wiązać się z przetwarzaniem nagłówków IP i ładunku IP. Biorąc pod uwagę fakt, że w art. 4 dyrektywy o prywatności i łączności elektronicznej wymaga się od dostawców usług internetowych, aby zapewnili bezpieczeństwo sieci, zgodnie z przepisem tym legalne są techniki inspekcji oparte na nagłówkach IP i treści, które służą wyłącznie osiągnięciu tego celu. W praktyce oznacza to, że w granicach wyznaczonych przez zasadę proporcjonalności (zob. sekcja V.3) dostawcy usług internetowych mogą monitorować i filtrować dane o komunikacji, aby zwalczać wirusy i ogólnie zapewnić bezpieczeństwo sieci ([27]).

([26]) W motywie 10 dyrektywy 2002/58/WE stwierdza się: „W sektorze łączności elektronicznej dyrektywę 95/46/WE stosuje się w szczególności do wszystkich spraw dotyczących ochrony podstawowych praw i wolności, które nie są szczegółowo objęte przepisami niniejszej dyrektywy, włączając zobowiązania nałożone na kontrolera oraz prawa jednostek". O zgodzie osób, których dane dotyczą, wspomina się w motywie 17: „Do celów niniejszej dyrektywy, zgoda użytkownika lub abonenta, niezależnie od tego czy abonentem jest osoba fizyczna czy prawna, powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE".

([27]) Opinia 2/2006 Grupy Roboczej Art. 29 dotycząca kwestii prywatności w związku ze świadczeniem usług skanowania wiadomości elektronicznych, przyjęta w dniu 21 lutego 2006 r. (WP 118). W opinii tej Grupa Robocza stwierdza, że wykorzystanie filtrów do celów określonych w art. 4 może być zgodne z art. 5 dyrektywy o prywatności i łączności elektronicznej.

(iii) Podstawy prawne minimalizacji skutków zatorów

42. Przesłankę dla tej podstawy prawnej można znaleźć w motywie 22 dyrektywy o prywatności i łączności elektronicznej, w którym wyjaśnia się zakaz przechowywania komunikatów zawarty w art. 5 ust. 1. Zakaz ten nie dotyczy automatycznego, pośredniego i przejściowego przechowywania informacji wówczas, gdy odbywa się to wyłącznie do celu przeprowadzenia transmisji oraz pod warunkiem, że informacja nie jest przechowywana przez okres dłuższy niż jest to konieczne w celu wykonania transmisji i zarządzania ruchem, oraz, że w okresie przechowywania zagwarantowana zostaje poufność.

43. Jeżeli dochodzi do zatorów, pojawia się pytanie, czy dostawcy usług internetowych mogą uciekać się do losowego usuwania lub opóźniania części ruchu, czy też raczej powinni spowalniać komunikację, która nie jest wrażliwa na upływ czasu, np. P2P lub e-mail, co pozwoli na przykład zachować możliwą do przyjęcia jakość komunikacji głosowej.

44. Biorąc pod uwagę ogólny interes społeczny w zagwarantowaniu użytecznej sieci łączności, dostawcy usług internetowych mogą twierdzić, że przyznawanie ruchowi priorytetu lub ograniczanie go w celu radzenia sobie z zatorami jest legalnym środkiem niezbędnym w celu świadczenia właściwej jakości usług. Oznacza to, że w takich przypadkach istniałyby ogólne podstawy prawne przetwarzania danych osobowych w takim celu, a konkretna zgoda użytkowników nie byłaby konieczna.

45. Jednocześnie możliwość ingerencji w ten sposób nie jest nieograniczona. Jeżeli dostawcy usług internetowych muszą dokonywać inspekcji komunikacji, wówczas z punktu widzenia poufności i ściśle stosując zasadę proporcjonalności, mają oni obowiązek wykorzystywania dla osiągnięcia tego celu najmniej naruszającej prywatność metody (unikając głębokiej inspekcji pakietów) i muszą wykorzystywać ją jedynie tak długo, jak jest to konieczne, by usunąć zator.

(iv) Podstawy prawne przetwarzania danych w innych celach

46. Dostawcy usług internetowych mogą również odczuwać potrzebę inspekcji danych o ruchu i treści w innych celach, chociażby oferowania ukierunkowanych abonamentów (np. abonamentu, który ogranicza dostęp do usług P2P, lub abonamentu zwiększającego prędkość dla pewnych aplikacji). Inspekcja oraz dalsze wykorzystanie danych o ruchu i komunikacji w celach innych niż świadczenie usługi lub zapewnienie jej bezpieczeństwa i zapobieżenie zatorom jest możliwe tylko pod ścisłymi warunkami, zgodnie z ramami prawnymi.

47. Ramy prawne stanowi głównie art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej, w którym wymaga się zgody użytkowników na słuchanie, nagrywanie, przechowywanie lub inne rodzaje przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu. W praktyce oznacza to, że w celu uczynienia legalnym przetwarzania zarówno danych o ruchu, jak i o komunikacji na mocy art. 5 ust. 1 potrzebna jest zgoda użytkowników uczestniczących w komunikacji.

48. Jak wyjaśniono powyżej, zastosowanie technik inspekcji i filtrowania opiera się albo na nagłówkach IP, które stanowią dane o ruchu, albo na głębokiej inspekcji pakietów, co oznacza również ładunek IP (dane o komunikacji). Dlatego też zasadniczo stosowanie takich technik do celów innych niż świadczenie usługi lub zapewnienie bezpieczeństwa jest zabronione, chyba że przetwarzanie jest legalne na mocy uzasadnionej podstawy, na przykład zgody (art. 5 ust. 1). Artykuł 5 ust. 1 znalazłby na przykład zastosowanie, gdyby dostawca usług internetowych zdecydował się zaoferować klientom niższą stawkę za dostęp do Internetu w zamian za otrzymywanie reklamy behawioralnej, wykorzystując w celu jej serwowania głęboką inspekcję pakietów, a więc dane o komunikacji. W związku z tym konieczna jest prawdziwa, konkretna i świadoma zgoda zgodnie z art. 5 ust. 1.

49. Ponadto w art. 6 dyrektywy o prywatności i łączności elektronicznej zatytułowanym „Dane o ruchu" zawarto pewne zasady odnoszące się konkretnie do danych o ruchu. W szczególności przewidziano możliwość przetwarzania danych o ruchu przez dostawców usług internetowych w oparciu o zgodę

użytkowników na otrzymywanie usług tworzących wartość dodaną ([28]). W przepisie tym zawarto wymóg zgody przewidziany w art. 5 ust. 1 w odniesieniu do danych o ruchu.

50. W praktyce nie zawsze musi być łatwe określenie na przykład w jakich przypadkach zgoda jest konieczna, a w jakich przypadkach podstawą legalności przetwarzania może być zapewnienie bezpieczeństwa sieci, zwłaszcza jeżeli cele technik inspekcji są dwojakie (na przykład uniknięcie zatorów i świadczenie usług tworzących wartość dodaną). Należy podkreślić, że zgody nie można uważać za łatwą, systemową furtkę umożliwiającą uzyskanie zgodności z zasadami ochrony danych.

51. Do tej pory zebrano niewiele doświadczeń dotyczących stosowania omówionych ram, w szczególności w odniesieniu do aspektów opisanych powyżej. Jest to obszar, w którym konieczne są dalsze wytyczne – zagadnienie to rozwinięto w sekcji VI. Ponadto trzeba rozważyć dodatkowe aspekty odnoszące się do uzyskiwania zgody. Opisano je poniżej.

V.2. **Kwestie odnoszące się do wyrażenia świadomej zgody jako podstawy prawnej**

52. Zgoda wymagana na mocy art. 5 i 6 dyrektywy o prywatności i łączności elektronicznej ma to samo znaczenie, co zgoda osoby, której dane dotyczą, opisana i szerzej określona dyrektywie 95/46/WE ([29]). Zgodnie z art. 2 lit. h) dyrektywy o ochronie danych „zgoda osoby, której dane dotyczą" oznacza „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Grupa Robocza Art. 29 zajęła się niedawno rolą zgody oraz wymogami jej ważności w swojej opinii 15/2011 w sprawie zgody ([30]).

53. Tak więc dostawcy usług internetowych, którzy potrzebują zgody, aby dokonywać inspekcji oraz filtrować dane o ruchu i treść, muszą zapewnić dobrowolność i konkretność zgody, musi ona też być w pełni świadomym wskazaniem przez osobę, której dane dotyczą, na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych. Potwierdzono to w motywie 17 dyrektywy o prywatności i łączności elektronicznej: „Zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej". Poniżej zamieszczono pewne praktyczne przykłady, co oznacza dobrowolność, konkretność i świadomość zgody w tym kontekście.

Zgoda: dobrowolne, konkretne i świadome wyrażenie woli

54. *Zgoda dobrowolna*. Użytkownicy nie powinni napotykać na ograniczenia wiążące zgodę z abonamentem internetowym, który chcą wykupić.

55. Zgoda osób fizycznych nie jest udzielana dobrowolnie, jeżeli muszą one zgodzić się na monitorowanie danych o ich komunikacji, aby uzyskać dostęp do usługi łączności. Byłoby tak tym bardziej, jeżeli wszyscy dostawcy na danym rynku zarządzaliby ruchem w celach wychodzących poza zapewnienie bezpieczeństwa sieci. Jedyną pozostającą możliwością byłoby niekorzystanie z usługi internetowej w ogóle. Biorąc pod uwagę, że Internet stał się niezbędnym narzędziem zarówno pracy, jak

([28]) W motywie 18 dyrektywy zawarto przykładowy wykaz usług tworzących wartość dodaną. To, czy usługi, do których odnosi się polityka zarządzania ruchem, mogłyby być interpretowane jako należące do tego wykazu, nie jest jasne. Politykę zarządzania ruchem mającą na celu przyznanie priorytetu pewnym treściom można uznać za służącą zapewnieniu jakości usług. Na przykład zarządzanie ruchem wiążące się wyłącznie z przetwarzaniem nagłówków IP w celu zaoferowania w wyższej cenie usług związanych z grami, w ramach których generowany przez użytkowników ruch związany z grami jest w sposób priorytetowy przesyłany przez sieć, można uznać za usługę tworzącą wartość dodaną. Z drugiej strony w żadnym wypadku nie jest jasne, czy zarządzanie ruchem mające ograniczyć pewne rodzaje ruchu, na przykład zredukować priorytet ruchu P2P, można uznać za taką usługę.

([29]) Zob. motyw 17 i art. 2 lit. f) dyrektywy o prywatności i łączności elektronicznej.

([30]) Przyjętej w dniu 13 lipca 2011 r. (WP 187).

i rekreacji, niekorzystanie z usługi internetowej nie jest realną alternatywą. Wynikiem byłoby pozbawienie osób fizycznych realnego wyboru, a więc nie byłyby one w stanie dobrowolnie udzielić zgody ([31]).

56. Zdaniem EIOD istnieje oczywista potrzeba, aby Komisja i władze krajowe monitorowały rynek, w szczególności w celu ustalenia, czy opisany scenariusz – łączenie przez dostawców usług telekomunikacyjnych z monitorowaniem komunikacji – staje się powszechny. Dostawcy powinni oferować usługi alternatywne, w tym abonament internetowy niepodlegający zarządzaniu ruchem, nie obciążając osób fizycznych wyższymi kosztami.

57. *Zgoda konkretna*. Wymóg konkretności zgody oznacza w tym przypadku, że dostawcy usług internetowych muszą zwrócić się o zgodę na monitorowanie danych o ruchu i komunikacji w jednoznaczny i wyraźny sposób. Zgodnie z opinią Grupy Roboczej Art. 29: „Aby zgoda była konkretna, musi być zrozumiała: powinna wyraźnie i precyzyjnie odnosić się do zakresu oraz konsekwencji przetwarzania danych. Nie może ona odnosić się do otwartego zbioru czynności przetwarzania. Innymi słowy, oznacza to, że kontekst, w jakim ma zastosowanie zgoda, jest ograniczony". Konkretnej zgody raczej nie da się uzyskać, jeżeli zgoda na inspekcję danych o ruchu i komunikacji jest powiązana z ogólną zgodą na subskrypcję usługi. Konkretność wymaga wykorzystania ukierunkowanych środków w celu uzyskania zgody, jak na przykład odrębnego formularza zgody lub osobnego okna jednoznacznie poświęconego monitorowaniu (nie zaś umieszczenia informacji w ogólnych warunkach umowy i wymogu podpisania umowy w ustalonej formie).

58. *Świadoma zgoda osoby zainteresowanej*. Aby zgoda była ważna, musi być świadoma. Potrzeba uprzedniego przedstawienia wystarczających informacji wynika nie tylko z dyrektyw o prywatności i łączności elektronicznej oraz o ochronie danych, ale też z art. 20 i 21 dyrektywy o usłudze powszechnej zmienionej dyrektywą 2009/136/WE ([32]). Potrzebę informacji i zgody wyraźnie potwierdzono w motywie 28 dyrektywy 2009/136/WE: „Użytkownicy powinni być w każdym przypadku w pełni informowani o wszelkich warunkach ograniczających korzystanie z usług łączności elektronicznej wprowadzanych przez dostawcę usług lub sieci. W zależności od wyboru dostawcy, informacje takie powinny precyzować rodzaj treści, aplikacji lub danej usługi, indywidualne aplikacje lub usługi, albo też oba te elementy". Następnie stwierdza się: „W zależności od zastosowanej technologii i rodzaju ograniczenia, takie ograniczenia mogą wymagać zgody użytkownika zgodnie z dyrektywą 2002/58/WE".

59. Biorąc pod uwagę złożoność tych technik monitorowania, uprzednie przedstawienie zrozumiałych informacji jest jednym z największych wyzwań, jeżeli chodzi o uzyskanie ważnej zgody. Konsumentów należy poinformować w sposób pozwalający im zrozumieć, jakie informacje są przetwarzane i w jaki sposób są wykorzystywane, oraz pojąć wpływ tych technik na poziom zadowolenia użytkowników, jak też stopień naruszenia prywatności z nimi związany.

60. Oznacza to nie tylko, że same informacje muszą być jasne i zrozumiałe dla przeciętnego użytkownika, ale też, że informacje muszą zostać przekazane bezpośrednio osobom fizycznym w wyraźny sposób, aby nie mogły zostać przeoczone.

61. *Wyrażenie woli*. Zgoda na mocy stosownych ram prawnych wymaga też konkretnego działania ze strony użytkownika w celu wyrażenia przyzwolenia. Dorozumiana zgoda nie spełnia tych wymagań. Potwierdza to również potrzebę wykorzystania specjalnych środków, aby uzyskać zgodę umożliwiającą dostawcy usług internetowych inspekcję danych o ruchu i komunikacji w kontekście stosowania polityki zarządzania ruchem. W swojej niedawnej opinii w sprawie zgody Grupa Robocza Art. 29 podkreśliła wymóg szczegółowości uzyskiwanej zgody w odniesieniu do poszczególnych elementów, które składają się na przetwarzanie danych.

([31]) Podobny przypadek zachodzi w odniesieniu do przekazywania danych PNR, gdzie dyskutowano, czy zgoda pasażerów na przekazanie danych o rezerwacji władzom USA jest ważna. Zdaniem Grupy Roboczej zgoda pasażerów nie może być dobrowolna, gdyż linie lotnicze mają obowiązek przesłać te dane przed odlotem, w związku z czym pasażerowie nie mają realnego wyboru, jeżeli chcą odbyć podróż; opinia 6/2002 Grupy Roboczej Art. 29 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym.

([32]) Dyrektywa 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (zob. przypis 15).

62. Można argumentować, że jeżeli strony uczestniczące w komunikacji nie życzą sobie, aby dostawcy usług internetowych przechwytywali ją w celu zastosowania polityki zarządzania ruchem, mogą zawsze zaszyfrować komunikację. To podejście można uznać za przydatne w sensie praktycznym, wymaga ono jednak pewnego wysiłku i wiedzy technicznej oraz nie można go uznać za porównywalne z dobrowolną, konkretną i świadomą zgodą. Wykorzystanie technik szyfrowania nie zapewnia też pełnej poufności komunikacji, gdyż dostawca usług internetowych będzie co najmniej w stanie uzyskać dostęp do informacji zawartych w nagłówku IP w celu skierowania komunikatu do miejsca przeznaczenia; będzie również mógł przeprowadzić analizę statystyczną.

63. Zgodnie z art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej zgodę trzeba uzyskać od zainteresowanych użytkowników. W wielu przypadkach użytkownik będzie tą samą osobą co abonent, co pozwala uzyskać zgodę w chwili dokonywania subskrypcji usług telekomunikacyjnych. W innych przypadkach, również tych, gdzie może chodzić o więcej niż jedną osobę, zgodę zainteresowanych użytkowników trzeba będzie uzyskiwać osobno. Może to wiązać się z problemami praktycznymi, co omówiono poniżej.

Zgoda wszystkich zainteresowanych użytkowników

64. W art. 5 ust. 1 wskazano jako podstawę legalności przetwarzania zgodę użytkowników. Zgodę trzeba uzyskać od wszystkich użytkowników biorących udział w komunikacji. Przesłanką tego wymogu jest fakt, że w komunikacji uczestniczą zazwyczaj co najmniej dwie osoby fizyczne (nadawca i odbiorca). Jeżeli na przykład dostawca usług internetowych skanuje ładunek IP odnoszący się do wiadomości e-mail, dokonuje on inspekcji informacji dotyczących zarówno nadawcy, jak i odbiorcy tej wiadomości.

65. Podczas monitorowania oraz przechwytywania ruchu i komunikacji (np. części ruchu WWW) wystarczające może być uzyskanie zgody użytkownika, czyli abonenta, przez dostawcę usług internetowych. Jest tak, ponieważ drugiej strony komunikacji – w tym przypadku odwiedzanej strony internetowej – można nie uznawać za „zainteresowanego użytkownika" ([33]). Sytuacja może jednak być bardziej złożona, gdy takie monitorowanie wiąże się z inspekcją treści wiadomości e-mail, a więc danych osobowych nadawcy i odbiorcy wiadomości e-mail, którzy niekoniecznie zawarli umowę z tym samym dostawcą usług internetowych. W takich przypadkach dostawca usług internetowych przetwarza w istocie dane osobowe (nazwisko, adres e-mail i potencjalnie wrażliwą treść) należące do osób niebędących jego klientami. Z praktycznej perspektywy uzyskanie zgody takich osób może być trudniejsze, gdyż należy ją uzyskać osobno w każdym przypadku, a nie w chwili zawarcia umowy o usługę telekomunikacyjną. Nie byłoby też realistyczne założenie, że abonent udzielił również zgody w imieniu innych użytkowników, a taka sytuacja może często zachodzić w prywatnych gospodarstwach domowych.

66. W tym kontekście EIOD uznaje, że dostawcy usług internetowych powinni przestrzegać istniejących wymogów prawnych i wdrażać politykę niewiążącą się z monitorowaniem oraz inspekcją informacji. Jest to jeszcze istotniejsze w odniesieniu do usług łączności z udziałem osób trzecich, które nie są w stanie wyrazić zgody na monitorowanie, zwłaszcza w stosunku do wysyłanych i otrzymywanych wiadomości e-mail (nie ma to zastosowania, gdy cel ma związek ze względami bezpieczeństwa).

67. Jednocześnie należy zauważyć, że prawo krajowe wdrażające art. 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej może nie zawsze być zadowalające pod tym względem; ogólnie wydaje się, że istnieje potrzeba lepszych wytycznych co do wymogów dyrektywy o prywatności i łączności elektronicznej w tym kontekście. W związku z tym EIOD zachęca Komisję do większej aktywności w tym względzie i podjęcia inicjatywy, która mogłaby zyskać dzięki wkładowi ze strony organów nadzorczych zebranych w Grupie Roboczej Art. 29 oraz innych zainteresowanych stron. W razie potrzeby należy wnieść sprawę do Trybunału Sprawiedliwości, aby uzyskać pełną jasność co do znaczenia i konsekwencji art. 5 ust. 1.

([33]) Pomimo faktu, że występują przypadki, gdzie ruch WWW wiąże się z przesyłaniem danych osobowych jak np. zdjęć dających się zidentyfikować osób fizycznych zamieszczonych na stronie internetowej. Przetwarzanie takich danych wymaga podstaw prawnych, ale nie jest objęte art. 5 ust. 1, gdyż osoby te nie są „zainteresowanymi użytkownikami".

V.3. **Proporcjonalność – zasada minimalizacji danych**

68. W art. 6 lit. c) dyrektywy o ochronie danych określono zasadę proporcjonalności ([34]), która ma zastosowanie do dostawców usług internetowych, gdyż monitorując i filtrując dane, są oni administratorami danych w rozumieniu tej dyrektywy.

69. Zgodnie z tą zasadą dane osobowe można gromadzić jedynie, jeżeli są one „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone". Zastosowanie tej zasady wiąże się z potrzebą oceny, czy środki wykorzystane przy przetwarzaniu danych oraz rodzaje wykorzystywanych danych osobowych są odpowiednie i czy są podstawy, by założyć, że pozwolą osiągnąć cele. Jeżeli wniosek brzmi, że gromadzonych jest więcej danych, niż jest to potrzebne, wymogi tej zasady nie zostały spełnione.

70. Zgodność pewnych rodzajów technik inspekcji z zasadą proporcjonalności trzeba oceniać osobno w poszczególnych przypadkach. Nie jest tu możliwe wyciągnięcie wniosków *in abstracto*. Można jednak wskazać pewne konkretne aspekty, które należy poddać ocenie, badając zgodność z zasadą proporcjonalności.

71. *Ilość przetwarzanych informacji*. Nadzór nad komunikacją klientów dostawcy usług internetowych na najgłębszym możliwym poziomie będzie w większości przypadków nadmierny i nielegalny. Fakt, że można go prowadzić środkami niewidocznymi dla osób fizycznych, którym może być trudno zrozumieć, co ma miejsce, zwiększa skutki z punktu widzenia ich prywatności. Dostawcy usług internetowych powinni ocenić, jakie środki w mniejszym stopniu naruszające prywatność mogą umożliwić osiągnięcie wymaganego rezultatu. Czy można go osiągnąć na przykład przez monitorowanie nagłówków IP zamiast głębokiej inspekcji pakietów? Nawet przy wykorzystaniu głębokiej inspekcji pakietów niezbędnych informacji może dostarczyć sama identyfikacja pewnych protokołów. Użyteczne może też okazać się zastosowanie zabezpieczeń chroniących dane, w tym pseudoanonimizacji. Wynik oceny musi potwierdzać proporcjonalność przetwarzania danych.

72. *Efekty przetwarzania (bezpośrednio powiązane z celami)*. Zasada proporcjonalności może być naruszona w przypadkach, w których dostawcy usług internetowych wykorzystują politykę zarządzania ruchem wyłączającą dostęp do pewnych usług bez udostępnienia użytkownikom w zamian słusznej części zysku, który z tego wynika.

73. Należy pamiętać, że zasada proporcjonalności obowiązuje nadal, nawet jeżeli inne obowiązkowe wymogi prawne zostały spełnione, w tym jeżeli dostawca usług internetowych uzyskał na przykład zgodę osób fizycznych na monitorowanie treści. Oznacza to, że przetwarzanie danych oparte na monitorowaniu treści może nadal być niezgodne z prawem, jeżeli narusza podstawową zasadę proporcjonalności.

V.4. **Środki bezpieczeństwa i organizacyjne**

74. W art. 4 dyrektywy o prywatności i łączności elektronicznej wyraźnie nakazuje się dostawcom usług internetowych podjęcie środków technicznych i organizacyjnych w celu zagwarantowania, że: (i) dostęp do danych osobowych może mieć wyłącznie uprawniony personel w dozwolonych prawem celach; (ii) dane osobowe będą chronione przed przypadkowym lub bezprawnym przetwarzaniem oraz (iii) zostanie wdrożona polityka bezpieczeństwa w odniesieniu do przetwarzania danych osobowych. Artykuł ten umożliwia też właściwym organom krajowym kontrolowanie tych środków.

75. Ponadto zgodnie z art. 4 ust. 3 oraz art. 4 ust. 2 dyrektywy o prywatności i łączności elektronicznej dostawcy usług internetowych są zobowiązani w przypadku naruszenia danych osobowych powiadomić właściwe organy krajowe, jak również osoby fizyczne, których dotyczy naruszenie, w przypadku, gdy ujawnienie tych danych może mieć dla nich niekorzystne konsekwencje.

76. Przetwarzanie danych osobowych zawartych w komunikacji w celu zastosowania polityki zarządzania ruchem może dać dostawcom usług internetowych dostęp do jeszcze bardziej wrażliwych danych niż dane o ruchu.

([34]) Jak wskazano powyżej, dyrektywa o ochronie danych ma zastosowanie do wszystkich kwestii związanych z ochroną praw i wolności podstawowych, których nie dotyczy konkretnie dyrektywa o prywatności i łączności elektronicznej.

77. Dlatego też polityka bezpieczeństwa stworzona przez dostawców usług internetowych powinna obejmować konkretne zabezpieczenia w celu zapewnienia adekwatności podejmowanych środków do takiego ryzyka. Jednocześnie właściwe organy krajowe kontrolujące te środki powinny stawiać szczególnie wysokie wymagania. Wreszcie, należy zapewnić wdrożenie skutecznych procedur zawiadamiania służących informowaniu osób, których dane zostały ujawnione, co może wywrzeć na nie niekorzystny wpływ.

VI. **SUGESTIE DOTYCZĄCE POLITYKI I ŚRODKÓW USTAWODAWCZYCH**

78. Techniki inspekcji oparte na danych o ruchu i inspekcji ładunków IP, tj. treści komunikacji, mogą ujawniać aktywność internetową użytkowników: odwiedzane strony internetowe oraz działania z nimi związane, korzystanie z aplikacji P2P, pobrane pliki, wysłane i odebrane wiadomości e-mail (od kogo, na jaki temat, w jakim okresie itp.). Dostawcy mogą chcieć wykorzystywać te informacje w celu przyznania niektórym rodzajom komunikacji, jak na przykład wideo na żądanie, priorytetu przed innymi. Mogą też chcieć je wykorzystywać w celu identyfikacji wirusów lub budowy profilów, aby serwować reklamy behawioralne. Działania te ingerują w prawo do poufności komunikacji.

79. Zależnie od wykorzystywanych technik i konkretnych aspektów sprawy implikacje z punktu widzenia prywatności rosną. Im głębiej sięga przechwytywanie i analiza gromadzonych informacji, tym większy konflikt z zasadą poufności komunikacji. Cele, w jakich odbywa się monitoring, i zastosowane zabezpieczenia służące ochronie danych, są również podstawowymi elementami przy ustaleniu, w jakim stopniu dochodzi do naruszenia prywatności i danych osobowych osób fizycznych. Blokowania i monitorowania do celów zwalczania szkodliwego oprogramowania, ze ścisłymi ograniczeniami dotyczącymi zatrzymywania oraz wykorzystywania danych będących przedmiotem inspekcji, nie można porównać z sytuacjami, w których informacje są rejestrowane w celu budowy indywidualnych profilów służących serwowaniu reklamy behawioralnej.

80. EIOD uważa w zasadzie, że istniejące ramy wspólnotowe dotyczące prywatności i ochrony danych, jeżeli będą należycie interpretowane, stosowane oraz egzekwowane, wystarczą w celu zagwarantowania przestrzegania prawa do poufności oraz ogólnie zapobieżenia niebezpieczeństwom dla prywatności i ochrony danych osób fizycznych ([35]). Dostawcy usług internetowych nie powinni wykorzystywać omawianych mechanizmów, jeżeli nie zastosowali w należyty sposób ram prawnych. Elementy tych ram, które dostawcy usług internetowych powinni w szczególności rozważyć i uwzględnić, to między innymi następujące zagadnienia:

— dostawcy usług internetowych mogą stosować politykę zarządzania ruchem w celu zapewnienia bezpieczeństwa usługi oraz świadczenia usługi, w tym ograniczenia zatorów, zgodnie z art. 4 i 6 dyrektywy o prywatności i łączności elektronicznej,

— dostawcy usług internetowych potrzebują innej konkretnej podstawy prawnej, a potencjalnie również zgody użytkowników, aby stosować politykę zarządzania ruchem związaną z przetwarzaniem danych o ruchu lub komunikacji w celach innych niż powyższe. Na przykład świadoma zgoda użytkowników jest niezbędna, aby monitorować i filtrować komunikację osób fizycznych w celu ograniczenia (lub umożliwienia) dostępu do niektórych aplikacji i usług takich jak P2P lub telefonia internetowa,

— zgoda musi być dobrowolna, wyraźna i świadoma. Powinna ona zostać wyrażona przez konkretne działanie. W wymogach tych kładzie się silny nacisk na potrzebę większych wysiłków mających na celu należyte informowanie osób fizycznych w bezpośredni, zrozumiały i konkretny sposób, aby mogły one ocenić skutki danych praktyk i ostatecznie podjąć świadomą decyzję. Biorąc pod uwagę złożoność omawianych technik, uprzednie przedstawienie zrozumiałych informacji użytkownikom jest jednym z największych wyzwań, jeżeli chodzi o uzyskanie świadomej zgody. Oprócz tego użytkownicy, którzy nie zgadzają się na żadne monitorowanie, nie powinni odczuć negatywnych konsekwencji (w tym również kosztów finansowych),

([35]) Nie zmienia to faktu, że istnieje potrzeba zmian prawa w związku z innymi zagadnieniami, szczególnie w kontekście ogólnego przeglądu ram prawnych ochrony danych w UE, aby uczynić je skuteczniejszymi w obliczu nowych technologii i globalizacji.

— gdy dostawcy usług internetowych wdrażają politykę zarządzania ruchem, zasada proporcjonalności odgrywa podstawową rolę niezależnie od podstaw prawnych i celu przetwarzania: świadczenia usług, unikania zatorów lub oferowania ukierunkowanych abonamentów z dostępem do pewnych usług i aplikacji lub bez niego. Zasada ta ogranicza dostawcom usług internetowych możliwość monitorowania treści komunikacji osób fizycznych, które wiąże się z przetwarzaniem nadmiernej ilości informacji lub zyskami wyłącznie dla dostawcy usług internetowych. To, co z logistycznego punktu widzenia mogą robić dostawcy usług internetowych, zależy od stopnia naruszenia prywatności przez stosowane techniki, wymaganych rezultatów (z których mogą wynikać zyski) oraz konkretnych zastosowanych zabezpieczeń prywatności i bezpieczeństwa danych. Przed wdrożeniem technik inspekcji dostawcy usług internetowych muszą przeprowadzić ocenę, czy są one zgodne z zasadą proporcjonalności.

81. Choć obecne ramy prawne uwzględniają stosowne warunki i zabezpieczenia, trzeba zwracać szczególną uwagę na to, czy dostawcy usług internetowych w skuteczny sposób spełniają wymogi prawne, czy dostarczają konsumentom informacji niezbędnych w celu dokonania racjonalnych wyborów i czy przestrzegają zasady proporcjonalności. Na szczeblu krajowym organy odpowiedzialne za powyższe to z jednej strony krajowe organy ds. telekomunikacji, z drugiej zaś krajowe organy ochrony danych. Na szczeblu UE stosownym organem jest m.in. BEREC. EIOD może również być zdolny odegrać rolę w tym kontekście.

82. Oprócz monitorowania aktualnego poziomu zgodności z przepisami, biorąc pod uwagę stosunkowo nową możliwość masowej inspekcji komunikacji w czasie rzeczywistym, niektóre poruszone w obecnej opinii aspekty związane z zastosowaniem ram wymagają dogłębniejszej analizy i dalszego wyjaśnienia. Szczególnie istotne wytyczne w kilku obszarach to między innymi:

— określenie legalnych praktyk w zakresie inspekcji zapewniających płynność ruchu, które mogą nie wymagać zgody użytkowników, jak na przykład zwalczanie spamu. Oprócz stopnia, w jakim stosowany monitoring narusza prywatność, istotne są też aspekty takie jak na przykład stopień zakłócenia płynności ruchu, do jakiego doszłoby w przeciwnym razie,

— określenie technik inspekcji wykorzystywanych w celach związanych z bezpieczeństwem, które mogą nie wymagać zgody użytkowników,

— określenie, kiedy monitorowanie wymaga zgody osoby fizycznej, zwłaszcza zgody wszystkich zainteresowanych użytkowników, oraz dopuszczalnych parametrów technicznych w celu zagwarantowania, że technika inspekcji nie wiąże się z przetwarzaniem danych, które nie jest proporcjonalne z punktu widzenia zamierzonych celów,

— ponadto w trzech powyższych przypadkach mogą być potrzebne wytyczne co do zastosowania niezbędnych zabezpieczeń służących ochronie danych (zasada celowości, bezpieczeństwo itp.).

83. Biorąc pod uwagę, że kompetencje w tej dziedzinie przysługują zarówno państwom członkowskim, jak i UE, zdaniem EIOD niezbędna jest wymiana poglądów oraz doświadczeń w celu wypracowania zharmonizowanego podejścia. W tym celu EIOD sugeruje stworzenie platformy lub grupy eksperckiej, która powinna gromadzić przedstawicieli krajowych organów regulacyjnych, Grupy Roboczej Art. 29, EIOD i BEREC. Pierwszym celem tej platformy byłoby opracowanie wytycznych, przynajmniej w odniesieniu do kwestii wskazanych powyżej, aby zapewnić solidne i zharmonizowane podejście oraz równe warunki działania. EIOD wzywa Komisję do zorganizowania takiej inicjatywy.

84. Wreszcie, zarówno organy krajowe, jak i ich odpowiedniki na szczeblu UE, w tym BEREC i Komisja Europejska, muszą uważnie obserwować wydarzenia zachodzące na rynku w związku z tą dziedziną. Z punktu widzenia ochrony danych i prywatności scenariusz, w którym dostawcy usług internetowych rutynowo zarządzają ruchem, oferując abonamenty oparte na filtrowaniu dostępu do treści i aplikacji, byłby wysoce problematyczny. Gdyby taka sytuacja miała kiedykolwiek zaistnieć, należałoby wprowadzić stosowne prawodawstwo.

VII. **WNIOSKI**

85. Coraz częstsze wykorzystywanie technik monitorowania i inspekcji przez dostawców usług internetowych narusza neutralność sieci oraz poufność komunikacji. Pociąga to za sobą poważne pytania dotyczące ochrony prywatności i danych osobowych użytkowników.

86. Chociaż w komunikacie Komisji w sprawie otwartego Internetu i neutralności sieci w Europie pokrótce omawia się te zagadnienia, zdaniem EIOD należy uczynić więcej, aby wypracować zadowalającą politykę na przyszłość. Dlatego też w obecnej opinii EIOD wnosi wkład w toczącą się debatę na temat neutralności sieci, zwłaszcza w odniesieniu do ochrony danych i prywatności.

87. EIOD uważa, że krajowe organy i BEREC powinny monitorować sytuację na rynku. Monitorowanie powinno poskutkować jasnym obrazem pozwalającym stwierdzić, czy rynek ewoluuje w kierunku masowej inspekcji komunikacji w czasie rzeczywistym i problemów z przestrzeganiem ram prawnych.

88. Monitorowanie rynku nie powinno odbywać się w oderwaniu od dalszej analizy skutków nowych praktyk z punktu widzenia ochrony danych i prywatności w Internecie. W obecnej opinii zarysowano pewne obszary, w których użyteczne byłyby wyjaśnienia. Chociaż agencje i organy UE, takie jak BEREC, Grupa Robocza Art. 29 oraz EIOD mogą być w stanie wyjaśnić warunki stosowania ram, zdaniem EIOD obowiązek koordynacji tej debaty oraz sterowania nią spoczywa na Komisji. Dlatego też EIOD wzywa Komisję do podjęcia w tym celu inicjatywy angażującej wszystkie zainteresowane strony w formie platformy lub grupy roboczej. Jeżeli chodzi o kwestie wymagające dalszej analizy, należy zająć się następującymi zagadnieniami:

— określeniem legalnych praktyk w zakresie inspekcji zapewniających płynność ruchu oraz mających na celu zapewnienie bezpieczeństwa,

— określeniem, kiedy monitorowanie wymaga zgody osoby fizycznej, zwłaszcza zgody wszystkich zainteresowanych użytkowników, oraz dopuszczalnych parametrów technicznych w celu zagwarantowania, że technika inspekcji nie wiąże się z przetwarzaniem danych, które nie jest proporcjonalne z punktu widzenia zamierzonych celów,

— w powyższych przypadkach mogą być potrzebne wytyczne co do zastosowania niezbędnych zabezpieczeń służących ochronie danych (zasada celowości, bezpieczeństwo itp.).

89. W zależności od dokonanych ustaleń niezbędne mogą być dodatkowe środki ustawodawcze. W takim przypadku Komisja powinna przedstawić środki mające na celu wzmocnienie ram prawnych i zagwarantowanie pewności prawa. Nowe środki powinny posłużyć wyjaśnieniu praktycznych konsekwencji zasady neutralności sieci, gdyż dokonano tego już w niektórych państwach członkowskich, jak też umożliwieniu użytkownikom dokonywania rzeczywistych wyborów, w szczególności zmuszając dostawców usług internetowych do oferowania niemonitorowanych połączeń.

Sporządzono w Brukseli dnia 7 października 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych