I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k neutralitě sítě, řízení provozu a ochraně soukromí a osobních údajů

(2012/C 34/01)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na články 7 a 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]),

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů ([2]), a zejména na čl. 41 odst. 2 tohoto nařízení,

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ([3]),

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

I.1 Souvislosti

1. Dne 19. dubna 2011 přijala Komise sdělení o otevřeném internetu a neutralitě sítě v Evropě ([4]).

2. Toto stanovisko lze považovat za reakci evropského inspektora ochrany údajů na uvedené sdělení. Jeho cílem je přispět k probíhající politické debatě v rámci EU o neutralitě sítě, zejména k aspektům souvisejícím s ochranou údajů a soukromím.

([1]) Úř. věst. L 281, 23.11.1995, s. 31, „směrnice o ochraně údajů".
([2]) Úř. věst. L 8, 12.1.2001, s. 1, „nařízení o ochraně údajů".
([3]) Úř. věst. L 201, 31.7.2002, s. 37, ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009 (viz poznámka pod čarou 15), „směrnice o soukromí a elektronických komunikacích".
([4]) KOM(2011) 222 v konečném znění.

3. Stanovisko vychází z reakce ([5]) evropského inspektora ochrany údajů na veřejné konzultace Komise k otevřenému internetu a neutralitě sítě v Evropě, jež předcházely přijetí sdělení Komise. Evropský inspektor ochrany údajů vzal rovněž v úvahu návrh závěrů Rady k neutralitě sítě ([6]).

I.2 **Koncepce neutrality sítě**

4. Neutralita sítě souvisí s probíhající debatou, zda má být poskytovatelům internetových služeb ([7]) povoleno omezovat, filtrovat nebo blokovat přístup na internet nebo jinak ovlivňovat jeho výkon. Koncepce neutrality sítě vychází z názoru, že informace na internetu mají být přenášeny nestranně, bez ohledu na obsah, místo určení či zdroj a že uživatelé mají mít možnost se rozhodnout, jaké aplikace, služby a hardware chtějí používat. To znamená, že poskytovatelé internetových služeb nemohou z vlastní vůle stanovovat priority nebo zpomalovat přístup k některým aplikacím či službám, jako je např. Peer to Peer („P2P") atd ([8]).

5. Filtrování, blokování a kontrola provozu sítě nastolují důležité otázky, které bývají často přehlíženy nebo opomíjeny, a to důvěrnost komunikace a respektování soukromí jednotlivců a jejich osobních údajů při používání internetu. Například některé kontrolní metody zahrnují monitorování obsahu sdělení, navštívených internetových stránek, zaslaných a obdržených e-mailových zpráv, času, kdy k tomu dochází, atd., což umožňuje filtrování komunikace.

6. Kontrolou údajů při komunikaci mohou poskytovatelé internetových služeb porušovat důvěrnost komunikace, což je základní právo zaručené v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod a v článcích 7 a 8 Listiny základních práv Evropské unie. Důvěrnost dále chrání sekundární právní předpisy EU, konkrétně článek 5 směrnice o soukromí a elektronických komunikacích.

I.3 **Zaměření a struktura stanoviska**

7. Evropský inspektor ochrany údajů se domnívá, že seriózní politická debata o neutralitě sítě se musí soustředit na důvěrnost komunikace, jakož i na další souvislosti spojené se soukromím a ochranou údajů.

8. Toto stanovisko přispívá k uvedené probíhající debatě v EU. Má tři cíle:

— Zdůrazňuje význam soukromí a ochrany údajů v současných diskuzích o neutralitě sítě. Konkrétněji pak zdůrazňuje nutnost dodržovat stávající pravidla v oblasti důvěrnosti komunikace. Povoleny by měly být pouze takové metody, které tato pravidla respektují.

— Neutralita sítě se týká relativně nových – technologických – možností a je jen málo zkušeností s tím, jak uplatňovat právní rámec. Toto stanovisko proto poskytuje návod, jak musí poskytovatelé internetových služeb uplatňovat a dodržovat právní rámec v oblasti ochrany údajů, jestliže filtrují, blokují a kontrolují provoz sítě. Toto stanovisko by mělo být užitečné pro poskytovatele internetových služeb a také pro orgány, které mají na starosti vymáhání právního rámce.

— V oblasti ochrany údajů a soukromí toto stanovisko označuje oblasti, které vyžadují zvláštní pozornost a v kterých mohou být zapotřebí opatření na úrovni EU. To je zvláště důležité vzhledem k probíhající debatě na úrovni EU a politickým opatřením, jež by v tomto smyslu mohla Komise zavést.

([5]) Evropský inspektor ochrany údajů ve své reakci zdůraznil, jak je důležité brát v úvahu problematiku ochrany údajů a soukromí společně s dalšími stávajícími právy a hodnotami. Reakce je k dispozici na adrese http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) K dispozici na adrese http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Tento výraz zahrnuje poskytování pevného i mobilního přístupu na internet.

([8]) Přestože se tato zásada nevztahuje na poskytovatele internetových služeb omezující rychlost nebo množství informací, účastník může odesílat nebo přijímat v rámci předplacené služby s omezením šířky pásma nebo objemu informací. Podle zásady neutrality sítě budou tedy poskytovatelé internetových služeb stále moci nabízet přístup na internet s omezením podle takových kritérií, jako je rychlost nebo objem, pokud to nebude zahrnovat diskriminaci ve prospěch či neprospěch konkrétního obsahu.

9. Evropský inspektor ochrany údajů si je vědom skutečnosti, že neutralita sítě nastoluje další otázky, jež jsou podrobněji popsány níže. Jde například o problematiku přístupu k informacím. Tyto otázky jsou rozebrány pouze v rozsahu jejich souvislosti s ochranou údajů a soukromí nebo dopadem na ochranu údajů a soukromí.

10. Struktura stanoviska je následující. V části II je uveden stručný přehled způsobu filtrování údajů ze strany poskytovatelů internetových služeb. V části III je nastíněn právní rámec EU v oblasti neutrality sítě. V části IV následuje technický popis a poté hodnocení dopadů na soukromí v závislosti na použitých metodách. Část V pak analyzuje praktické detaily spojené s uplatňováním současného právního rámce EU v oblasti soukromí a ochrany údajů. Na základě této analýzy jsou v části VI uvedeny návrhy na další vývoj politiky a označeny oblasti, které mohou vyžadovat objasnění a zlepšení. V části VII jsou uvedeny závěry.

II. **NEUTRALITA SÍTĚ A ZÁSADY ŘÍZENÍ PROVOZU**

Větší využívání zásad řízení provozu

11. Poskytovatelé internetových služeb tradičně provádějí monitorování a ovlivňování provozu sítě pouze omezeně. Poskytovatelé internetových služeb například uplatňují metody kontroly a omezené toky informací, aby zajistili bezpečnost sítě, např. proti virům. Proto, obecně řečeno, se internet rozšířil a současně si zachovává velký stupeň neutrality.

12. V posledních letech se však někteří poskytovatelé internetových služeb zajímají o kontrolu provozu sítě, aby jej mohli diferencovat a uplatňovat na něj různé zásady, například blokovat konkrétní služby nebo upřednostňovat přístup k určitým službám oproti jiným. Někdy se tomu říká „zásady řízení provozu“ ([9]).

13. Důvody, proč poskytovatelé internetových služeb kontrolují a diferencují provoz, jsou různé. Zásady řízení provozu mohou například pomáhat poskytovatelům internetových služeb při řízení provozu v období přetížení sítě, např. stanovením priority pro určitý časově citlivý provoz, jako je video-streaming, a přeřazením jiných druhů provozu, které nejsou tak časově citlivé, např. P2P, na nižší úroveň ([10]). Řízení provozu může být také prostředek, kterým si poskytovatelé internetových služeb zajišťují možný tok příjmů, které mohou pocházet z různých zdrojů. Na jedné straně by poskytovatelé internetových služeb mohli účtovat poplatky poskytovatelům obsahu, např. těm poskytovatelům, jejichž služby vyžadují použití širšího pásma, výměnou za prioritní přenesení jejich obsahu (a tedy vyšší rychlost). To by znamenalo, že přístup k určité službě, například službě poskytující videa na vyžádání, by byl rychlejší než přístup k jiné podobné službě, která nemá předplacenou vysokou přenosovou rychlost. Příjmy by mohly plynout také od účastníků, kteří chtějí platit vyšší (nebo nižší) poplatky za určitý druh diferencované předplacené služby. Například předplacená služba bez přístupu k P2P by mohla být levnější než služba poskytující neomezený přístup.

14. Kromě důvodů pro používání zásad řízení provozu na straně poskytovatelů internetových služeb mohou mít zájem o zásady řízení provozu i jiné strany. Jestliže poskytovatelé internetových služeb řídí své sítě a provádějí kontrolu obsahu, který přes jejich zařízení prochází, mohou pravděpodobně zvýšit svou schopnost zjišťovat možné nezákonné používání, např. porušení autorských práv nebo používání pro pornografické účely.

([9]) Viz například zpráva OFCOM nazvaná „Site blocking to reduce online copyright infringement“ (Blokování stránek s cílem omezit porušování autorských práv na síti), která byla přijata dne 27. května 2011 a je k dispozici na adrese http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Někteří poskytovatelé internetových služeb již ve své síti zavedli systémy kontroly paketů pro řízení provozu a jiné účely, takže předpokládáme, že toto lze zavést, přestože by to bylo velmi složité a nákladné pro ty poskytovatele, kteří takové služby zatím neprovozují. Je možné, že v krátkodobém až střednědobém horizontu bude metoda DPI vzhledem k potřebným investicím používána pouze většími poskytovateli internetových služeb“.

([10]) Kvalita aplikací v reálném čase, jako je video-streaming, závisí mimo jiné na latenci, tj. zpoždění v důsledku např. přetížení sítě.

Jiné zájmy, jež mohou být ohroženy, včetně ochrany údajů a soukromí

15. Tento trend spustil debatu o oprávněnosti těchto praktik a konkrétně pak o tom, zda mají být v zákoně dále upraveny konkrétní povinnosti v oblasti neutrality sítě.

16. Rostoucí využívání zásad řízení provozu ze strany poskytovatelů internetových služeb by zřejmě mohlo omezit přístup k informacím. Pokud se takovéto jednání stane běžným a uživatelé již nebudou mít přístup k celému internetu (nebo tento přístup bude velmi drahý), jak jej známe dnes, ohrozí to přístup k informacím a možnost uživatelů zasílat a přijímat obsah, který chtějí, pomocí aplikací či služeb dle jejich výběru. Tento problém může odstranit právně závazná zásada o neutralitě sítě.

17. To přivádí evropského inspektora ochrany údajů k důsledkům v oblasti ochrany údajů a soukromí v případě, že poskytovatelé internetových služeb provádějí řízení provozu. Konkrétněji:

— Když poskytovatelé internetových služeb zpracovávají údaje o provozu výhradně za účelem směrování toku informací od odesílatele k příjemci, provádějí obecně omezené zpracování osobních údajů ([11]). Stejně jako poštovní služba zpracovává informace uvedené na obálce dopisu, také poskytovatel internetových služeb zpracovává informace potřebné k nasměrování komunikace k příjemci. To není v rozporu se zákonnými požadavky na ochranu údajů, soukromí a důvěrnost komunikace.

— Když však poskytovatelé internetových služeb kontrolují údaje v rámci komunikace, aby mohli diferencovat jednotlivé komunikační toky a uplatňovat na ně zvláštní zásady, což může být vůči jednotlivcům nevýhodné, důsledky jsou závažnější. V závislosti na okolnostech každého případu a na druhu prováděné analýzy může takové zpracování velmi narušovat soukromí a osobní údaje jednotlivce. Ještě zřejmější je to v případech, kdy zásady řízení odhalují obsah internetové komunikace jednotlivců, včetně odeslaných a přijatých e-mailových zpráv, navštívených internetových stránek, stažených či odeslaných souborů apod.

III. **PŘEHLED PRÁVNÍHO RÁMCE EU PRO NEUTRALITU SÍTĚ A DALŠÍ VÝVOJ POLITIKY**

III.1 **Právní rámec v kostce**

18. Do roku 2009 neobsahovaly právní nástroje EU ustanovení, jež by poskytovatelům internetových služeb výslovně zakazovala provádět filtrování nebo blokování či účtovat účastníkům vyšší cenu za přístup ke službám. Zároveň ani neobsahovaly ustanovení, jež by takovouto praxi výslovně připouštěla. Tento stav způsoboval do určité míry nejistotu.

19. Telekomunikační balíček z roku 2009 tuto situaci změnil, když zavedl ustanovení ve prospěch otevřenosti internetu. Například čl. 8 odst. 4 o společném předpisovém rámci pro sítě a služby elektronických komunikací („rámcová směrnice“) stanoví regulačním orgánům povinnost posilovat schopnost koncových uživatelů dostat se k obsahu, aplikacím či službám dle své volby ([12]). Toto ustanovení platí pro síť jako celek, nikoli jen na úrovni jednotlivých poskytovatelů. V nedávném návrhu závěrů Rady byla také zdůrazněna nutnost zachovat otevřenost internetu ([13]).

([11]) To nezahrnuje operace, jejichž účelem je zvýšit bezpečnost sítě a detekovat škodlivý provoz, ani operace potřebné pro fakturaci a propojení. Dále to nezahrnuje povinnosti vyplývající ze směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (Úř. věst. L 105, 13.4.2006, s. 54) („směrnice o uchovávání údajů“).

([12]) Směrnice 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací ve znění směrnice 2009/140/ES a nařízení (ES) č. 544/2009 (Úř. věst. L 337, 18.12.2009, s. 37).

([13]) Viz bod 3 písm. e), v němž Rada uznává: „Nutnost zachovat otevřenost internetu a současně zajistit, aby i nadále poskytoval kvalitní služby v rámci, který podporuje a dodržuje základní práva, jako jsou například svoboda projevu a svoboda podnikání“, a čl. 8 písm. d), v němž jsou členské státy vyzývány, aby „podporovaly otevřený a neutrální charakter internetu jako svůj politický cíl“.

20. Směrnice o univerzální službě ([14]) obsahuje konkrétnější povinnosti. V článcích 20 a 21 jsou stanoveny požadavky na transparentnost týkající se omezení přístupu k službám a aplikacím anebo jejich využívání. Rovněž je zde stanovena minimální úroveň kvality služeb.

21. K praktikám poskytovatelů internetových služeb, které zahrnují kontrolu komunikace jednotlivců, je v 28. bodě odůvodnění směrnice, kterou se mění směrnice o univerzální službě a soukromí v elektronických komunikacích ([15]), zdůrazněno, že „některé typy použité technologie a druhy omezení mohou vyžadovat souhlas uživatele podle směrnice o soukromí a elektronických komunikacích". V 28. bodě odůvodnění je tedy připomenuta nutnost souhlasu podle čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích u všech omezení na základě monitorování komunikace. V následující části IV je dále analyzováno uplatňování čl. 5 odst. 1 a celkový právní rámec ochrany údajů a soukromí.

22. Konečně čl. 22 odst. 3 směrnice o univerzální službě dává nyní vnitrostátním regulačním orgánům pravomoc stanovit v případě potřeby poskytovatelům internetových služeb požadavky na minimální kvalitu služeb, aby nedocházelo k zhoršení kvality služeb a ztěžování či zpomalování provozu na veřejných sítích.

23. Výše uvedené znamená, že na úrovni EU se obecně usiluje o otevřený internet (viz čl. 8 odst. 4 rámcové směrnice). Tento politický cíl, který se vztahuje na síť jako celek, však přímo nesouvisí se zákazy nebo povinnostmi jednotlivých poskytovatelů internetových služeb. Jinými slovy, poskytovatel internetových služeb může používat zásady řízení provozu, které vylučují přístup k některým aplikacím, pokud o tom v plné míře informuje koncové uživatele a pokud s tím koncoví uživatelé svobodně vysloví svůj konkrétní a jednoznačný souhlas.

24. Situace se může v jednotlivých členských státech lišit. V některých členských státech mohou poskytovatelé internetových služeb za určitých podmínek používat zásady řízení provozu například za účelem blokování takových aplikací, jako je VoIP (v rámci levnější předplacené služby přístupu na internet), pokud s tím jednotliví uživatelé vysloví svobodný, konkrétní a jednoznačný informovaný souhlas. Jiné členské státy se rozhodly posílit zásadu neutrality sítě. Například nizozemský parlament schválil v červenci 2011 zákon, který obecně zakazuje poskytovatelům internetových služeb ztěžovat či zpomalovat aplikace nebo služby na internetu (např. VoIP), pokud to není nutné pro minimalizaci vlivů přetížení, z důvodů integrity nebo bezpečnosti, boje proti spamům nebo pokud to není v souladu se soudním příkazem ([16]).

III.2 **Sdělení o neutralitě sítě**

25. Ve svém sdělení o neutralitě sítě ([17]) dospěla Evropská komise k závěru, že situace v oblasti neutrality sítě je taková, že je nutné ji sledovat a dále analyzovat. Zahájila politiku „vyčkávání", než zváží další regulační kroky.

([14]) Směrnice 2002/22/ES ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (Úř. věst. L 337,, 18.12.2009, s. 11). Srovnej také s čl. 1 odst. 3, v němž se uvádí, že směrnice nepřikazuje ani nezakazuje poskytovatelům internetových služeb, aby v souladu s vnitrostátním právem a právem Společenství omezovali přístup koncových uživatelů ke službám a aplikacím nebo jejich využívání, ale stanoví povinnost poskytnout informace o těchto podmínkách.

([15]) Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.

([16]) Původní nizozemský dodatek lze nalézt na adrese https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Důvody pro tento politický krok – jak bylo uvedeno v tisku – se nevztahovaly k ochraně údajů a soukromí, ale spíše šlo o potřebu zajistit, aby uživatelé nebyli zbaveni přístupu k informacím nebo aby tento přístup nebyl omezován. Zdá se tedy, že tato novelizace byla motivována záležitostmi souvisejícími s přístupem k informacím.

([17]) Viz poznámka pod čarou 4.

26. Ve sdělení Komise se uvádí, že všechna opatření a další regulační kroky budou podrobeny důkladnému posouzení s ohledem na aspekty ochrany údajů a soukromí. V návrhu závěrů Komise je rovněž uvedeno, že jsou v sázce otázky ochrany údajů a soukromí ([18]).

27. Otázka, kterou je třeba posoudit z hlediska ochrany údajů a soukromí, zní, zda je vyčkávací politika dostatečná. I když rámec ochrany údajů a soukromí v současnosti předjímá některé bezpečnostní mechanismy, zejména ve formě zásady důvěrnosti komunikace, zdá se, že bude nezbytné pečlivě sledovat úroveň dodržování předpisů a poskytnout návod k několika aspektům, které nejsou zcela jasné. Dále je vzhledem k technologickému vývoji třeba se vyslovit k tomu, jak by mohl být objasněn a dále vylepšen právní rámec. Jestliže bude zjištěno, že se trh vyvíjí směrem k masivní kontrole komunikace v reálném čase a objevují se problémy v oblasti dodržování rámce, bude třeba přijmout legislativní opatření. Konkrétní návrhy v tomto smyslu jsou uvedeny v části VI.

IV. **TECHNICKÉ OKOLNOSTI A SOUVISEJÍCÍ DŮSLEDKY PRO SOUKROMÍ A OCHRANU ÚDAJŮ**

28. Než se začneme touto otázkou zabývat podrobněji, je důležité lépe poznat kontrolní metody, které mohou poskytovatelé internetových služeb používat při řízení provozu, a jaký to může mít dopad na zásadu neutrality sítě. Důsledky pro soukromí a ochranu údajů, které z těchto metod vyplývají, se značně liší podle toho, jaké metody jsou použity. Pro pochopení a správné uplatňování právního rámce na ochranu osobních údajů, který je popsán v části V, je nutné tyto technické okolnosti uvést. Je však třeba poznamenat, že jde o neustále se měnící a složitou oblast. Níže uvedený popis proto není míněn jako vyčerpávající a zcela aktuální, poskytuje pouze technické informace, které jsou nepostradatelné pro pochopení právního odůvodnění.

IV.1 **Přenos informací přes internet: základy**

29. Když uživatel přenáší přes internet své sdělení, je přenášená informace rozdělena na pakety. Tyto pakety se přenášejí přes internet od odesílatele k příjemci. Každý paket zahrnuje mimo jiné informaci o zdroji a místu určení. Poskytovatelé internetových služeb mohou dále tyto pakety zabalit do dalších vrstev a protokolů ([19]), které se používají na řízení různých toků provozu v rámci sítě poskytovatele internetových služeb.

30. Jestliže se vrátíme k analogii s poštovním dopisem, je použití síťového přenosového protokolu ekvivalentní vložení obsahu poštovního dopisu do obálky a uvedení adresy místa určení, kterou si má poštovní služba přečíst a dopis na ni doručit. Poštovní služba může používat další protokoly v rámci svého interního provozu, podle nichž řídí všechny obálky, jež mají být doručeny, přičemž cílem je, aby každá obálka dorazila na místo svého určení, které původně uvedl odesílatel. Podle této analogie má každý paket dvě části. *IP payload (uživatelská data)*, což představuje obsah sdělení a odpovídá dopisu. Obsahuje informace určené pouze příjemci. Druhá část paketu, *IP header (hlavička)*, obsahuje mimo jiné adresu příjemce a odesílatele a odpovídá obálce. Hlavička umožňuje poskytovatelům internetových služeb a dalším zprostředkovatelům směrovat uživatelská data z jejich zdrojové adresy na cílovou adresu.

31. Poskytovatelé internetových služeb a další zprostředkovatelé zajišťují, aby IP pakety cestovaly sítí přes uzly, kde je přečtena informace z IP hlavičky a porovnána se směrovacími tabulkami, a poté jsou pakety

([18]) Viz bod 4 písm. e), v němž Rada uvádí: „Existence některých obav, zejména na straně orgánů zabývajících se ochranou spotřebitelů a osobních údajů, v souvislosti s ochranou osobních údajů".

([19]) Jak je dále popsáno v části IV.2, tyto protokoly dohodnutým způsobem kódují informace přenášené z jednoho místa na druhé, aby si účastníci komunikace vzájemně rozuměli, např. HTTP, FTP atd.

odeslány k dalšímu uzlu na dráze k místu určení. Tento proces se provádí v celé síti s využitím bezpaměťového přístupu, protože všechny pakety, které do uzlu dorazí, jsou zpracovány neutrálně. Když jsou přeneseny do dalšího uzlu, není třeba ve směrovači dále uchovávat informace ([20]).

IV.2 **Kontrolní metody**

32. Jak je vysvětleno výše, poskytovatelé internetových služeb si přečtou IP hlavičky za účelem nasměrování do místa určení. Jak je však výše rovněž uvedeno, analýza provozu (zahrnující IP hlavičky a IP uživatelská data) může být prováděna pro jiné účely a s využitím jiných technologií. Nové trendy mohou zahrnovat například zpomalení některých aplikací, které uživatelé používají, např. P2P, nebo naopak zvýšení rychlosti u některých služeb, jako jsou služby poskytující video na vyžádání pro důležité účastníky. Přestože všechny kontrolní metody *technicky* provádějí kontrolu paketů, úroveň narušování soukromí je jiná. Existují dvě hlavní kategorie kontrolních metod. Jedna vychází pouze z IP hlavičky, druhá kontroluje také IP uživatelská data.

Na základě informací z IP hlavičky. Kontrola IP hlavičky paketu zjišťuje některá pole, podle nichž mohou poskytovatelé internetových služeb uplatňovat řadu konkrétních zásad řízení provozu. Tyto metody vycházejí pouze z kontroly procesních dat IP hlaviček, které v zásadě obsahují jen směrovací informace, a to za jiným účelem (tj. diferenciace provozu). Když se poskytovatel internetových služeb podívá na zdrojovou IP adresu, může ji spojit s konkrétním účastníkem a může uplatnit určité zásady, například směrovat paket přes rychlejší nebo pomalejší spoj. Když se poskytovatel internetových služeb podívá na cílovou IP adresu, může také uplatnit určité zásady, například zablokovat nebo filtrovat přístup na některé internetové stránky.

Na základě hloubkové kontroly. Technologie DPI (z angl. deep packet inspection, hloubková kontrola paketů) umožňuje poskytovateli internetových služeb získat přístup k informacím určeným pouze příjemci sdělení. Jestliže se vrátíme k příkladu s poštovní službou, tato metoda se rovná otevření obálky a přečtení dopisu uvnitř za účelem provedení analýzy obsahu sdělení (zabaleného v IP paketech), aby mohla být uplatněna určitá síťová zásada. Kontrolu lze provádět různými způsoby, z nichž každý představuje pro subjekt údajů ohrožení.

— *DPI založená na analýze protokolů a statistických záznamů*. Kromě protokolu IP, jehož smyslem je umožnit přenos dat přes internet, existují i další protokoly, které stanoveným způsobem kódují přenášené informace (přenos, relace, prezentace a aplikace apod.) Cílem těchto protokolů je zajistit, aby si pakety účastnící se komunikace vzájemně rozuměly. Existují například protokoly, které jsou spojeny s prohlížením internetu ([21]), jiné protokoly se používají při přenosu souborů ([22]) atd. Proto se kontrolní metody, které vycházejí z prohlídky protokolů a kombinují se se statistickou analýzou, zaměřují na hledání konkrétních vzorů či charakteristických rysů, které určují, jaké protokoly jsou použity ([23]). Tyto kontrolní metody umožňují, aby poskytovatelé internetových služeb poznali druh sdělení (e-mail, prohlížení internetu, stahování souborů atd.) a v některých případech identifikovali konkrétní použitou službu nebo aplikaci, jako je tomu v případě přenosu digitalizovaného hlasu (VoIP), kdy jsou používané protokoly velmi specifické pro konkrétního prodejce či poskytovatele služeb. Znalost druhu komunikace sama o sobě může umožnit poskytovatelům internetových služeb uplatnit konkrétní zásady řízení provozu. Například blokovat internetový provoz. Může to být také první krok umožňující poskytovateli internetových služeb provádět hlubší analýzu, která může vyžadovat plný přístup k metadatům a obsahu komunikace.

([20]) Internetové síťové zařízení však používá směrovací protokoly, které zaznamenávají činnost, a vyměňuje si tyto informace s jiným síťovým zařízením, aby nasměrovalo IP pakety na nejefektivnější cestu. Když je například některý spoj přetížen nebo nefunguje a směrovač obdrží takovouto informaci, aktualizuje svou směrovací tabulku o alternativu, která tento spoj nepoužívá. Rovněž je třeba uvést, že sběr a zpracování se může v některých případech provádět za účelem fakturování, nebo dokonce v souladu s požadavky směrnice o uchovávání údajů.

([21]) HTTP – internetový protokol pro výměnu hypertextových souborů – nebo HTML – značkovací jazyk pro hypertext.

([22]) FTP – protokol pro přenos souborů.

([23]) Existují různé způsoby identifikace použitých protokolů. Například je možné vyhledávat ve zvláštních polích ve vnitřních protokolech, např. za účelem identifikace portů použitých k navázání komunikace. Statistickou charakterizaci komunikačního toku lze také odvodit z analýzy některých konkrétních polí – korelace protokolů použitých současně mezi dvěma IP adresami.

— *DPI na základě analýzy obsahu sdělení*. A nakonec je také možné kontrolovat metadata ([24]) a vlastní komunikaci. Tato metoda zahrnuje zachycení všech IP paketů, které jsou součástí původního toku komunikace, aby mohl být v plném rozsahu rekonstruován a analyzován původní obsah sdělení. Pro detekci škodlivého nebo nezákonného obsahu, jakým jsou viry, dětská pornografie atd., je nezbytné rekonstruovat vlastní obsah, aby mohl být analyzován. Je třeba poznamenat, že komunikace může být někdy speciálně zakódována mezi účastníky, což znesnadňuje provádění analýzy obsahu ze strany poskytovatelů internetových služeb.

IV.3 **Důsledky pro soukromí a ochranu údajů**

33. Kontrolní metody vycházející z kontroly IP hlaviček, a zejména pak kontroly paketů, zahrnují monitorování a filtrování těchto dat, což má závažné důsledky z hlediska soukromí a ochrany osobních údajů. Mohou být také v rozporu s právem na důvěrnost komunikace.

34. Sledování komunikace osob má samo o sobě závažné důsledky pro soukromí a ochranu osobních údajů. Tento problém je však širší, protože v závislosti na výsledku monitorování a zachycování komunikace se mohou důsledky pro soukromí dále zvyšovat. Není samozřejmě totéž pouze kontrolovat komunikaci, např. proto, aby byla zajištěna správná funkce systému, a kontrolovat komunikaci proto, aby mohly být uplatněny zásady, které mohou mít dopad na jednotlivé osoby. Pokud je účelem uplatněných zásad pouze eliminace přetížení sítě, obvykle to nemá na soukromí jednotlivců žádný větší dopad. Ale zásady řízení provozu mohou být používány proto, aby byly zablokovány určité informace obsahu, neboli aby byla komunikace ovlivněna například behaviorální (cílená podle zájmů uživatele) reklamou. V těchto případech je dopad na soukromí závažnější. Tento problém nabývá na závažnosti, když si uvědomíme, že takovéto informace se shromažďují ne za malou skupinu jednotlivců, ale obecně za všechny zákazníky poskytovatelů internetových služeb ([25]). Pokud budou filtrovací metody používat všichni poskytovatelé internetových služeb, mohlo by to vést ke všeobecnému monitorování používání internetu. Navíc, pokud se zaměříme na druh zpracovávaných informací, jsou rizika pro soukromí samozřejmě vysoká, neboť řada shromažďovaných informací bude zřejmě velmi citlivá a tyto informace mají po shromáždění k dispozici poskytovatelé internetových služeb i ti, kdo si je od nich vyžádají. Navíc tyto informace mohou být velice cenné z komerčního hlediska. Samo o sobě to představuje vysoké riziko, že se původní účel plíživě změní na komerční či jiné využití shromážděných informací.

35. Správné uplatňování monitorování a kontroly a metod filtrování musí probíhat v souladu s příslušnými kontrolními mechanismy na ochranu osobních údajů a soukromí, které stanoví hranice toho, co a za jakých okolností ještě lze. Následuje přehled příslušných kontrolních mechanismů podle současného právního rámce EU v oblasti ochrany osobních údajů a soukromí.

V. **UPLATŇOVÁNÍ PRÁVNÍHO RÁMCE EU V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ A SOUKROMÍ**

36. Právní rámec EU v oblasti ochrany osobních údajů je technologicky neutrální; jako takový neupravuje konkrétní kontrolní metody, které jsou popsány výše. Směrnice o soukromí a elektronických komunikacích upravuje ochranu soukromí při poskytování služeb elektronických komunikací ve veřejných

([24]) Každý protokol má ve své hlavičce některá speciální pole, která poskytují doplňující neformální informace o přenášené komunikaci. Obsah těchto polí je tedy možné označit za metadata komunikace. Jako příklad takovýchto polí lze uvést číslo použitého portu: např. když je to číslo 80, druh komunikace bude pravděpodobně prohlížení internetu.

([25]) Možnosti sledování nemají pochopitelně jen poskytovatelé internetových služeb. I další poskytovatelé internetu mohou pomocí cookies třetích stran sledovat uživatele na internetu. Viz například nedávný akademický článek ukazující, že Google je přítomen na 97 ze 100 internetových stránek, což znamená, že Google dokáže sledovat uživatele, kteří si při prohlížení těchto oblíbených internetových stránek nezvolili zablokování cookies třetích stran. Viz: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan a Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (29. července 2011). K dispozici na SSRN: http://ssrn.com/abstract=1898390. Sledování uživatelů pomocí cookies třetích stran bylo řešeno pracovní skupinou zřízenou podle článku 29. Viz stanovisko 2/2010 o online behaviorální reklamě, přijaté dne 22. června 2010 (WP 171).

sítích (typicky jde o přístup k internetu a telefonování) ([26]) a směrnice o ochraně údajů upravuje zpracování osobních údajů obecně. Tento právní rámec jako celek stanoví různé povinnosti, jež se vztahují na poskytovatele internetových služeb, kteří zpracovávají a monitorují data o provozu a komunikaci.

V.1 **Právní důvody pro zpracování údajů o provozu a obsahu**

37. Podle právních předpisů o ochraně údajů vyžaduje zpracování osobních údajů, jako je tomu v případě zpracování údajů o provozu a komunikaci, přiměřený právní důvod. Kromě tohoto obecného požadavku mohou v některých případech platit zvláštní požadavky.

38. V tomto případě se druh osobních údajů, které poskytovatelé internetových služeb zpracovávají, týká údajů o provozu a obsahu sdělení. Jak obsah sdělení, tak i údaje o provozu jsou chráněny právem na důvěrnost korespondence, které je zaručeno v článku 8 Evropské úmluvy o ochraně lidských práv a v článcích 7 a 8 Listiny základních práv Evropské unie. Konkrétněji čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích, který má název „Důvěrný charakter sdělení", požaduje, aby členské státy zajistily důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Současně čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích předjímá, že za určitých okolností může být se souhlasem uživatelů povoleno zpracování údajů o provozu a obsahu ze strany poskytovatelů internetových služeb. Stanoví zákaz „příposlechu, odposlechu, uchovávání nebo jiných druhů zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1". To je dále rozebráno níže.

39. Kromě souhlasu dotčených uživatelů předjímá směrnice o soukromí a elektronických komunikacích i jiné důvody, které mohou opravňovat poskytovatele internetových služeb ke zpracování údajů o provozu a komunikaci. Relevantní právní důvody pro zpracování v tomto případě jsou i) poskytování služby; ii) zajištění bezpečnosti služby a iii) minimalizace přetížení sítě. Další možné důvody, které opravňují využívání řízení na základě údajů o provozu a komunikaci, jsou probrány níže pod bodem iv).

i) Právní důvody pro poskytování služby

40. Jak je objasněno v části IV, poskytovatelé internetových služeb zpracovávají informace o IP hlavičkách pro účely nasměrování jednotlivých IP paketů k jejich místu určení. Čl. 6 odst. 1 a 2 směrnice o soukromí a elektronických komunikacích umožňuje zpracování údajů o provozu pro účely přenosu sdělení. Poskytovatelé internetových služeb tedy mohou zpracovávat informace, které jsou nezbytné pro poskytnutí služby.

ii) Právní důvody pro zajištění bezpečnosti služby

41. Podle článku 4 směrnice o soukromí a elektronických komunikacích má poskytovatel internetových služeb obecnou povinnost učinit přiměřená opatření, aby zajistil bezpečnost svých služeb. Při filtrování virů může docházet ke zpracování IP hlaviček a uživatelských dat. Vzhledem k tomu, že článek 4 směrnice o soukromí a elektronických komunikacích vyžaduje, aby poskytovatelé internetových služeb zajistili bezpečnost sítě, opravňuje toto ustanovení kontrolní metody, při nichž jsou kontrolovány IP hlavičky a obsah výhradně za účelem dosažení tohoto cíle. V praxi to znamená, že poskytovatelé internetových služeb mohou ve stanovených hranicích dle zásady přiměřenosti (viz část V.3) monitorovat a filtrovat údaje o komunikaci, aby tak bojovali s viry a celkově zajistili bezpečnost sítě ([27]).

([26]) 10. bod odůvodnění směrnice o soukromí a elektronických komunikacích stanoví: „V odvětví elektronických komunikací se směrnice 95/46/ES vztahuje zejména na všechny záležitosti týkající se ochrany základních práv a svobod, které nejsou zvláštním způsobem upraveny touto směrnicí, včetně povinností správce a práv jednotlivců. V souvislosti se souhlasem subjektu údajů je podstatný také 17. bod odůvodnění: „Pro účely této směrnice by měl mít souhlas uživatele nebo účastníka, bez ohledu na to, zda účastník je fyzická či právnická osoba, stejný význam jako souhlas subjektu údajů definovaný a dále upřesněný ve směrnici 95/46/ES".

([27]) Stanovisko 2/2006 pracovní skupiny zřízené podle článku 29 směrnice 95/46/ES, které se zabývá problematikou ochrany soukromí v kontextu poskytování služeb spočívajících ve screeningu elektronické pošty, přijaté dne 21. února 2006 (WP 118). V tomto stanovisku pracovní skupina uvádí, že používání filtrů pro účely článku 4 může být slučitelné s článkem 5 směrnice o soukromí a elektronických komunikacích.

iii) Právní důvody pro minimalizaci vlivů přetížení sítě

42. Zdůvodnění k tomuto právnímu důvodu lze nalézt v 22. bodě odůvodnění směrnice o soukromí a elektronických komunikacích, který vysvětluje zákaz uchovávání sdělení uvedený v čl. 5 odst. 1. Tím se nezakazuje automatické, průběžné a přechodné uchovávání, pokud k němu dochází výhradně za účelem uskutečnění přenosu a pokud netrvá déle, než je nezbytně nutné pro účely přenosu a řízení provozu, a pokud je zaručena důvěrnost sdělení.

43. Jestliže dojde k přetížení sítě, vyvstává otázka, zda poskytovatelé internetových služeb mají provoz přerušit, nebo opozdit, nebo raději zpomalit komunikaci, která není citlivá na čas, např. P2P nebo e-mailový provoz, aby tak umožnili průchod hlasového provozu v přijatelné kvalitě.

44. Vzhledem k obecnému zájmu společnosti na zaručení použitelné komunikační sítě mohou poskytovatelé internetových služeb argumentovat tím, že stanovení priorit nebo přiškrcení provozu za účelem omezení přetížení sítě je legitimní opatření, které je potřebné pro poskytnutí adekvátní služby. To znamená, že v těchto případech a pro tento účel bude existovat obecný právní důvod pro zpracování osobních údajů a výslovný souhlas uživatelů není nutný.

45. Současně však možnost zasahovat tímto způsobem není neomezená. Jestliže poskytovatelé internetových služeb potřebují kontrolovat komunikaci, musí z pohledu důvěrnosti a při přísném uplatnění zásady přiměřenosti používat nejméně narušující způsob, který mají k dispozici, aby dosáhli daného účelu (nesmějí používat technologii DPI), a mohou jej používat pouze tak dlouho, jak je nutné, aby se vyřešilo přetížení sítě.

iv) Právní důvody pro zpracování údajů pro jiné účely

46. Poskytovatelé internetových služeb mohou také chtít kontrolovat údaje o provozu a komunikaci pro jiné účely, například za účelem cíleného nabízení služeb (např. službu s omezeným přístupem k P2P nebo službu, při níž je u některých aplikací rychlost zvýšena). Kontrola a další použití údajů o provozu a komunikaci pro účely jiné než poskytování služby či zajištění její bezpečnosti a omezení přetížení sítě je povoleno pouze za přísných podmínek v souladu s právním rámcem.

47. Právní rámec představuje zejména čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích, který vyžaduje souhlas příslušných uživatelů s příposlechem, odposlechem, uchováváním či používáním jiných způsobů zachycování či kontrolování komunikace a souvisejících údajů o provozu. V praxi to znamená, že je nutný souhlas účastníků komunikace, aby bylo zpracování údajů o provozu a komunikaci oprávněné podle čl. 5 odst. 1.

48. Jak je vysvětleno výše, vychází používání kontrolních a filtrovacích metod buď z IP hlaviček, které představují údaje o provozu, nebo z analýzy obsahu (DPI), což zahrnuje také uživatelská data a představuje údaje o komunikaci. Proto je v zásadě použití takovýchto metod pro účely jiné než poskytování služby nebo zajištění bezpečnosti zakázáno, pokud ke zpracování neexistuje oprávněný důvod, například souhlas (čl. 5 odst. 1). Příkladem uplatnění čl. 5 odst. 1 je situace, kdy se poskytovatel internetových služeb rozhodne nabízet zákazníkům nižší sazbu za přístup k internetu výměnou za souhlas se zasíláním behaviorální reklamy pomocí DPI, a tedy i s využitím údajů o komunikaci, aby tak mohl činit. Proto je podle čl. 5 odst. 1 nezbytný skutečný, konkrétní a informovaný souhlas.

49. Navíc článek 6 směrnice o soukromí a elektronických komunikacích nazvaný „provozní údaje“ stanoví některá pravidla, jež se vztahují konkrétně na údaje o provozu. Předjímá totiž, že poskytovatelé

internetových služeb budou zpracovávat údaje o provozu na základě souhlasu uživatelů s přijímáním služeb s přidanou hodnotou ([28]). Toto ustanovení upřesňuje požadavek na souhlas uvedený v čl. 5 odst. 1, pokud jde o údaje o provozu.

50. V praxi nemusí být vždy snadné zjistit, například, kdy je souhlas nezbytný a kdy může zajištění bezpečnosti sítě oprávnit zpracování údajů, zejména pak v případě, že důvody pro použití kontrolních metod jsou dvojí (např. vyloučit přetížení sítě a poskytovat služby s přidanou hodnotou). Je třeba zdůraznit, že souhlas nelze považovat za snadný a systematický způsob dodržování zásad ochrany osobních údajů.

51. S uplatňováním právního rámce a konkrétně s různými aspekty popsanými výše je jen málo zkušeností. Je to oblast, kde jsou podrobnější pokyny velmi potřebné, jak je dále rozebráno v části VI. Navíc existují další relevantní aspekty související se získáváním souhlasu, které rovněž potřebují zvláštní posouzení. Jsou popsány níže.

V.2 **Otázky týkající se poskytnutí informovaného souhlasu jako právního důvodu**

52. Souhlas požadovaný podle článků 5 a 6 směrnice o soukromí a elektronických komunikacích má stejný význam jako souhlas subjektu údajů definovaný a dále upřesněný ve směrnici 95/46/ES ([29]). Podle čl. 2 písm. h) směrnice o ochraně údajů „souhlas subjektu údajů" znamená „jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování". Nedávno byla role souhlasu a požadavky na to, aby byl takový souhlas platný, předmětem stanoviska pracovní skupiny zřízené podle článku 29 (stanovisko 15/2011 o souhlasu ([30])).

53. Poskytovatelé internetových služeb vyžadující souhlas s prováděním kontroly a filtrování údajů o provozu a obsahu musí proto zajistit, aby byl souhlas svobodný a výslovný a aby představoval plně informovaný projev vůle dané osoby vyjadřující srozumění s tím, že její osobní údaje budou zpracovány. 17. bod odůvodnění směrnice o soukromí a elektronických komunikacích to potvrzuje „(…) Souhlas může být udělen jakýmkoli vhodným způsobem, který umožňuje vyjádřit svobodně poskytnutý, zvláštní a informovaný projev vůle uživatele, včetně označení zaškrtnutím políčka při návštěvě webové stránky na internetu". V dalším textu je uvedeno několik praktických příkladů, co v této souvislosti znamená svobodný, výslovný a informovaný souhlas.

Souhlas: svobodný, výslovný a informovaný projev vůle

54. *Svobodný souhlas*. Uživatelé by neměli být omezováni tím, že služba přístupu na internet bude spojována s udělením souhlasu.

55. Souhlas by nebyl dán svobodně, kdyby příslušné osoby musely souhlasit s monitorováním své komunikace, aby získaly přístup ke komunikační službě. To platí zejména v případě, kdy by *všichni* poskytovatelé na daném trhu prováděli řízení provozu pro účely, jež jdou nad rámec zajištění bezpečnosti sítě. Jedinou zbývající možností by bylo službu přístupu na internet nepoužívat vůbec. Vzhledem

([28]) 18. bod odůvodnění směrnice obsahuje seznam příkladů služeb s přidanou hodnotou. Není jasné, zda lze služby, u nichž jsou použity zásady řízení provozu, považovat za služby spadající do tohoto seznamu. Zásady řízení provozu směřující ke stanovení priorit pro určitý obsah by mohly být chápány jako zajišťování kvality služby. Například řízení provozu, které zahrnuje pouze zpracování IP hlaviček a jehož cílem je nabízet hráčské služby s prémiovou cenou, kdy jsou stanoveny priority pro osobní hráčský provoz uživatelů v síti, lze považovat za službu s přidanou hodnotou. Na druhé straně není zdaleka jasné, zda lze takto posuzovat řízení provozu za účelem zpomalení určitých druhů provozu, například zpomalení provozu P2P.

([29]) Viz 17. bod odůvodnění a čl. 2 písm. f) směrnice o soukromí a elektronických komunikacích.

([30]) Přijaté dne 13. července 2011 (WP 187).

k tomu, že internet se stal základním nástrojem pro práci i zábavu, nevyužívání služby přístupu na internet není platnou alternativou. Výsledkem by bylo, že by tyto osoby neměly skutečnou možnost volby, tj. nemohly by dát svůj svobodný souhlas ([31]).

56. Evropský inspektor ochrany údajů se domnívá, že je jednoznačně potřebné, aby Komise a vnitrostátní orgány monitorovaly trh, zejména proto, aby zjistily, zda se tento scénář, tj. spojování telekomunikačních služeb s monitorováním komunikace ze strany poskytovatelů – nestává převažujícím trendem. Poskytovatelé musí nabízet i alternativní služby včetně takového přístupu na internet, u nějž není provoz řízen, aniž by za to účtovali vyšší ceny.

57. *Výslovný souhlas*. Nutnost, aby byl souhlas výslovný, v tomto případě vyžaduje, aby poskytovatelé internetových služeb požádali o souhlas s monitorováním údajů o provozu a komunikaci jasně a zřetelně. Podle pracovní skupiny zřízené podle článku 29: „… aby byl souhlas výslovný, musí být srozumitelný: musí jasně a přesně vyjadřovat rozsah a důsledky zpracování údajů. Nemůže se týkat neurčitých činností v rámci zpracování. Jinými slovy to znamená, že kontext, v němž souhlas platí, je omezený.“ Výslovný souhlas zřejmě nebude poskytnut, pokud bude souhlas s kontrolou údajů o provozu a komunikaci „spojen“ s celkovým souhlasem s objednáním služby. Výslovnost vyžaduje použití cílených prostředků, aby byl souhlas získán, např. zvláštního formuláře pro vyjádření souhlasu nebo samostatného políčka jasně určeného pro účely monitorování (místo uvedení této informace do všeobecných smluvních podmínek a vyžadování podpisu smlouvy, tak jak je).

58. *Informovaný souhlas*. Aby byl souhlas platný, musí být informovaný. Nutnost poskytnout předem přiměřené informace vyplývá nejen ze směrnice o soukromí a elektronických komunikacích a směrnice o ochraně údajů, ale také z článků 20 a 21 směrnice o univerzální službě ve znění směrnic 2009/136/ES ([32]). Nutnost, aby byly informace a souhlas výslovný, je potvrzena v 28. bodě odůvodnění směrnice 2009/136/ES: „Uživatelé by měli být v každém případě plně informováni o všech omezeních při používání služeb elektronických komunikací ze strany poskytovatele služby nebo sítě. Tyto informace by měly upřesnit buď typ dotčeného obsahu, aplikace nebo služby, nebo tyto konkrétní aplikace či služby, popřípadě obojí, podle rozhodnutí poskytovatele“. Dále je upřesněno, že: „Některé typy použité technologie a druhy omezení mohou vyžadovat souhlas uživatele podle směrnice 2002/58/ES“.

59. Vzhledem ke složitosti metod monitorování je podání smysluplné informace předem jedním z hlavních problémů při získávání platného souhlasu. Spotřebitelé musí být v každém případě informováni tak, aby pochopili informace, které jsou zpracovávány, jak se používají a jaký to má vliv na výsledek pro uživatele a úroveň narušení soukromí v souvislosti s těmito metodami.

60. To znamená, že nejen sama informace musí být jasná a pochopitelná pro průměrné uživatele, ale také že je informace podána přímo příslušným osobám, a to nápadným způsobem, aby ji nemohly přehlédnout.

61. *Projev vůle*. Souhlas podle platného právního rámce rovněž vyžaduje potvrzující krok ze strany uživatele, který tím projevuje svou vůli. Implikovaný souhlas tento požadavek nesplňuje. To rovněž potvrzuje nutnost používat specializované prostředky na získání souhlasu, aby mohl poskytovatel internetových služeb kontrolovat údaje o provozu a komunikaci při používání zásad řízení provozu. Ve svém nedávném stanovisku k souhlasu zdůraznila pracovní skupina zřízená podle článku 29 nutnost nespojitosti při získávání souhlasu s ohledem na různé prvky při zpracování údajů.

([31]) Podobným případem je jmenná evidence cestujících, kdy se diskutovalo o tom, zda je platný souhlas cestujících s přenosem údajů o rezervaci orgánům USA. Pracovní skupina usoudila, že souhlas cestujících nemůže být dán svobodně, neboť aerolinky jsou povinny zaslat údaje před odletem, a cestující tedy nemají žádnou skutečnou volbu, pokud chtějí letět. Stanovisko 6/2002 pracovní skupiny zřízené podle článku 29 o přenosu informací o cestujících a dalších údajů z aerolinek do USA.

([32]) Směrnice 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (viz poznámka pod čarou 15).

62. Dalo by se argumentovat tím, že pokud účastníci komunikace nechtějí, aby poskytovatelé internetových služeb jejich komunikaci sledovali a mohli tak používat zásady řízení provozu, mohou svou komunikaci zakódovat. Tento přístup by mohl být považován v praxi za užitečný, vyžaduje však určité úsilí a technické znalosti a nelze jej považovat za podobný svobodnému, výslovnému a informovanému souhlasu. Navíc ani používání kódovacích metod neznamená, že komunikace bude zcela důvěrná, protože poskytovatel internetových služeb bude mít přístup minimálně k informacím v IP hlavičce, aby mohl komunikaci nasměrovat, a bude také moci použít statistickou analýzu.

63. Podle čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích musí být od příslušných uživatelů získán souhlas. V mnoha případech bude uživatelem stejná osoba jako účastník, což umožňuje podání souhlasu v okamžiku předplacení telekomunikační služby. V jiných případech, kdy se komunikace účastní více než jedna osoba, musí být souhlas dotčených uživatelů získán zvlášť. To může v praxi působit problémy, jak je rozebráno níže.

Souhlas všech dotčených uživatelů

64. V čl. 5 odst. 1 je stanovena nutnost souhlasu uživatele, aby bylo zpracování oprávněné. Souhlas musí být získán od *všech uživatelů* účastnících se komunikace. Důvodem je to, že komunikace se obvykle týká alespoň dvou osob (odesílatele a příjemce). Jestliže například poskytovatel internetových služeb sleduje uživatelská data odkazující na e-mail, kontroluje informace, jež se týkají jak odesílatele, tak i příjemce e-mailu.

65. Při monitorování a sledování provozu a komunikace (například určitého provozu na internetu) může stačit, aby poskytovatelé internetových služeb získali souhlas uživatele, tedy účastníka. Je tomu tak proto, že druhý účastník komunikace, v tomto případě navštívená internetová stránka, nemůže být považován za „dotčeného uživatele“ ([33]). Situace však může být složitější, když takovéto monitorování zahrnuje kontrolu obsahu e-mailů, a tedy osobních údajů odesílatele a příjemce zprávy, kteří nemusí mít smluvní vztah se stejným poskytovatelem internetových služeb. V takovýchto případech poskytovatel internetových služeb skutečně zpracovává osobní údaje (jméno, e-mailovou adresu, případně i citlivé údaje o obsahu) osob, které nejsou jeho zákazníky. Z praktického hlediska by získání souhlasu těchto osob mohlo být obtížnější, neboť je nutné případ od případu, a nikoli při uzavření smlouvy o telekomunikačních službách. Není ani realistické předpokládat, že souhlas účastníka byl dán i za jiné uživatele, jak tomu často bývá u soukromých domácností.

66. V tomto kontextu se evropský inspektor ochrany údajů domnívá, že poskytovatelé internetových služeb musí dodržovat stávající právní požadavky a realizovat takové zásady, které nezahrnují monitorování a kontrolu informací. Je to ještě důležitější s ohledem na komunikační služby, které zahrnují třetí strany, jež nemohou poskytnout souhlas s monitorováním, zejména pak u odeslaných a přijatých e-mailů (to neplatí, když účel vychází z nutnosti zajistit bezpečnost).

67. Současně je třeba poznamenat, že vnitrostátní zákony provádějící čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích nemusí být v tomto směru vždy uspokojivé a že obecně je zřejmě nutné poskytnout lepší pokyny k požadavkům stanoveným v tomto směru ve směrnici o soukromí a elektronických komunikacích. Evropský inspektor ochrany údajů proto vyzývá Komisi, aby byla v tomto smyslu aktivnější a aby zahájila iniciativu, která by mohla čerpat z doporučení, jež orgány dozoru shromáždily v pracovní skupině zřízené podle článku 29 a od účastníků. V případě potřeby je třeba tuto záležitost předat Soudnímu dvoru, aby bylo vyjasněno, co čl. 5 odst. 1 znamená a jaké to má důsledky.

([33]) Bez ohledu na ty případy, kdy internetový provoz zahrnuje přenos osobních údajů, jako jsou například fotografie identifikovatelných fyzických osob uveřejněné na internetové stránce. Zpracování takovýchto informací vyžaduje právní základ, ale nevztahuje se na něj čl. 5 odst. 1, neboť tyto osoby nejsou „dotčenými uživateli“.

V.3 **Přiměřenost – zásada minimalizace údajů**

68. V čl. 6 písm. c) směrnice o ochraně údajů je stanovena zásada přiměřenosti ([34]), což se vztahuje na poskytovatele internetových služeb, neboť tito poskytovatelé jsou správci údajů ve smyslu směrnice, když provádějí monitorování a filtrování.

69. Podle této zásady musí být osobní údaje zpracovávány pouze, pokud jsou „přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány nebo dále zpracovávány". Uplatňování této zásady zahrnuje nutnost posoudit, jaké prostředky použité při zpracování údajů a jaký druh osobních údajů je vhodný a může pravděpodobně tento cíl splnit. Jestliže je zjištěno, že je shromažďováno více údajů, než je nezbytné, není tato zásada splněna.

70. Dodržení zásady přiměřenosti u některých druhů kontrolních metod musí být posuzováno případ od případu. Nelze vyslovovat abstraktní závěry. Je však možné ukázat na různé konkrétní aspekty, které je třeba posoudit při hodnocení, zda je zásada přiměřenosti splněna.

71. *Množství zpracovávaných informací*. Dohled nad komunikací zákazníků poskytovatelů internetových služeb na nejhlubší možné úrovni bude ve většině případů nadbytečný a nezákonný. Skutečnost, že to lze provádět pomocí prostředků, které nejsou pro jednotlivce zjevné, a že může být obtížné, aby zjistili, co se děje, zvyšuje dopad na jejich soukromí. Poskytovatelé internetových služeb musí posoudit, jaké méně narušující prostředky jsou k dispozici, aby byl dosažen potřebný výsledek. Může například místo použití analýzy obsahu dosáhnout potřebného výsledku monitorování IP hlaviček? I při používání technologie DPI může potřebné informace přinést identifikace jen některých protokolů. Vhodné může být také uplatnění bezpečnostních mechanismů na ochranu údajů, včetně pseudo-anonymizace. Výsledek takovéhoto posouzení musí potvrzovat, že zpracování osobních údajů je přiměřené.

72. *Účinky zpracování (přímo související s účely)*. Přiměřenost může chybět v případech, kdy poskytovatelé internetových služeb používají zásady řízení provozu vylučující přístup k některým službám, aniž by tím uživatelé získali spravedlivý podíl na výsledném výtěžku.

73. Je důležité připomenout, že zásada přiměřenosti platí i v případě, že byly splněny ostatní závazné právní požadavky, jestliže poskytovatel internetových služeb například získal souhlas od jednotlivců s monitorováním obsahu. To znamená, že zpracování údajů prováděné formou monitorování obsahu může být nezákonné, pokud porušuje základní zásadu přiměřenosti.

V.4 **Bezpečnost a organizační opatření**

74. V článku 4 směrnice o soukromí a elektronických komunikacích je stanoven výslovný požadavek, aby poskytovatelé internetových služeb učinili technická a organizační opatření na zajištění i) toho, že k osobním údajům bude mít přístup pouze oprávněný personál, a to pro zákonné účely; ii) ochrany osobních údajů před náhodným či nezákonným zpracováním a iii) implementace bezpečnostní politiky v oblasti zpracování osobních údajů. Umožňuje také, aby příslušné vnitrostátní orgány prováděly kontroly těchto opatření.

75. Dále podle čl. 4 odst. 3 a 2 směrnice o soukromí a elektronických komunikacích jsou poskytovatelé internetových služeb také povinni oznámit příslušným vnitrostátním orgánům případy narušení údajů a jednotlivce, kteří byli postiženi, pokud pro ně může mít odhalení jejich osobních údajů negativní důsledky.

76. Zpracování osobních údajů uvedených v komunikaci s cílem použít zásady řízení provozu může dát poskytovatelům internetových služeb přístup k údajům, které jsou dokonce citlivější než údaje o provozu.

([34]) Jak je uvedeno výše, směrnice o ochraně údajů se vztahuje na všechny záležitosti týkající se ochrany základních práv a svobod, jež nejsou výslovně upraveny ve směrnici o soukromí a elektronických komunikacích.

77. Proto musí bezpečnostní zásady vyvinuté poskytovateli internetových služeb zahrnovat zvláštní kontrolní mechanismy, aby bylo zajištěno, že učiněná opatření jsou těmto rizikům přiměřená. Současně musí být příslušné vnitrostátní orgány, které tato opatření kontrolují, zvláště náročné. Konečně je třeba zajistit, aby byly zavedeny efektivní oznamovací postupy, kdy budou informovány subjekty údajů, jejichž údaje byly narušeny a pro něž to tedy může mít negativní důsledky.

VI. **DOPORUČENÍ POLITICKÝCH A LEGISLATIVNÍCH OPATŘENÍ**

78. Kontrolní metody vycházející z údajů o provozu a kontroly uživatelských dat, tj. obsahu komunikace, mohou odhalit činnost uživatelů internetu: navštívené internetové stránky a činnosti prováděné na těchto stránkách, používání aplikací P2P, stahování souborů, odeslané a přijaté e-maily, od koho, s jakým předmětem a v jaké formě atd. Poskytovatelé internetových služeb by mohli chtít používat tyto informace pro účely stanovení vyšší priority u některých druhů komunikace, například u videa na vyžádání, než u jiných. Mohli by chtít používat tyto informace za účelem identifikace virů nebo vytvoření profilů, které budou sloužit behaviorální reklamě. Tyto činnosti narušují právo na důvěrnost komunikace.

79. V závislosti na použitých metodách a specifických okolnostech daného případu se důsledky pro soukromí zvyšují. Čím hlubší je sledování a analýza shromážděných informací, tím větší je rozpor se zásadou důvěrnosti komunikace. Účely, pro něž probíhá monitorování, a bezpečnostní mechanismy, které byly zavedeny, jsou také důležité pro posouzení stupně narušení soukromí a osobních údajů jednotlivců. Blokování a monitorování pro účely boje se škodlivým obsahem s přísným omezením doby uchovávání a použití kontrolovaných údajů nelze srovnávat se situacemi, kdy jsou informace zaznamenávány za účelem vytváření individuálních profilů za účelem behaviorální reklamy.

80. Evropský inspektor ochrany údajů se v zásadě domnívá, že stávající právní rámec EU v oblasti soukromí a ochrany osobních údajů by postačoval na zaručení, že bude dodržováno právo na důvěrnost a že nebude obecně docházet k ohrožení ochrany soukromí a osobních údajů jednotlivců ([35]). Poskytovatelé internetových služeb nesmí používat takové mechanismy, pokud řádně neuplatňují právní rámec. Konkrétně, mezi příslušné prvky právního rámce, které musí poskytovatelé internetových služeb vzít v úvahu a dodržovat, patří:

— Poskytovatelé internetových služeb mohou používat zásady řízení provozu, jejichž cílem je zajistit bezpečnost služby, poskytování služby včetně omezení přetížení sítě podle článků 4 a 6 směrnice o soukromí a elektronických komunikacích.

— Poskytovatelé internetových služeb potřebují jiný konkrétní právní důvod, popřípadě souhlas uživatelů, aby mohli používat zásady řízení provozu, které zahrnují zpracování údajů o provozu anebo komunikaci pro účely jiné, než je uvedeno výše. Například je nutný informovaný souhlas uživatelů, aby mohla být monitorována a filtrována komunikace jednotlivců za účelem omezení (nebo umožnění) přístupu k některým aplikacím a službám, jako je P2P nebo VoIP.

— Souhlas musí být svobodný, výslovný a informovaný. Musí být dán potvrzujícím způsobem. Tyto požadavky silně zdůrazňují nutnost zvýšit úsilí, aby bylo zajištěno, že jednotlivci budou řádně informováni, a to přímo, srozumitelně a konkrétně, aby mohli posoudit účinky takovýchto metod a nakonec dospět k informovanému rozhodnutí. Vzhledem ke složitosti těchto metod je podání smysluplné informace uživatelům předem jedním z hlavních problémů při získávání platného souhlasu. Kromě toho nesmí být vyvozovány negativní důsledky (včetně finančních nákladů) vůči uživatelům, kteří nesouhlasí s jakýmkoli monitorováním.

([35]) To platí, aniž by tím byla dotčena nutnost změn zákonů z jiných důvodů, zejména v kontextu celkové revize právního rámce EU v oblasti ochrany osobních údajů s cílem zefektivnit jej vzhledem k novým technologiím a globalizaci.

— Nejdůležitější je přiměřenost, pokud poskytovatelé internetových služeb používají zásady řízení provozu bez ohledu na právní důvod zpracování a účel: poskytování služby, eliminace přetížení sítě nebo poskytování cíleného připojení s přístupem k určitým službám a aplikacím nebo bez něj. Tato zásada omezuje možnost poskytovatelů internetových služeb provádět monitorování obsahu komunikace jednotlivců, které zahrnuje zpracování nadbytečných informací nebo získávání výhod pouze pro poskytovatele. To, co mohou poskytovatelé internetových služeb logisticky provádět, závisí na úrovni narušení soukromí při použití těchto metod, požadovaném výsledku (z nějž mohou těžit) a konkrétních použitých bezpečnostních mechanismech na ochranu soukromí a osobních údajů. Před využitím kontrolních metod musí poskytovatelé internetových služeb posoudit, zda tyto metody splňují zásadu přiměřenosti.

81. I když právní rámec nyní obsahuje příslušné podmínky a bezpečnostní mechanismy, zvláštní pozornost je třeba věnovat tomu, zda poskytovatelé internetových služeb skutečně plní právní požadavky, zda poskytují spotřebitelům potřebné informace, aby spotřebitelé mohli provést smysluplnou volbu, a zda dodržují zásadu přiměřenosti. Na vnitrostátní úrovni patří mezi orgány k tomuto příslušné vnitrostátní telekomunikační úřady na straně jedné a na druhé straně vnitrostátní úřady na ochranu osobních údajů. Na úrovni EU patří mezi příslušné evropské subjekty BEREC. V této souvislosti může hrát roli také evropský inspektor ochrany údajů.

82. Kromě monitorování současné úrovně dodržování právního rámce vzhledem k relativní novosti možností masivní kontroly komunikace v reálném čase vyžadují některé aspekty související s uplatňováním právního rámce, které jsou probírány v tomto stanovisku, další hlubší analýzu a bližší vysvětlení. Bude třeba vydat pokyny týkající se několika oblastí, a to:

— stanovení, které kontrolní metody jsou oprávněné pro zajištění hladkého průběhu provozu a které nevyžadují souhlas uživatelů, jako je například boj proti spamům. Kromě narušování soukromí při použitém monitorování jsou podstatné takové aspekty, jako je například úroveň narušení hladkého průběhu provozu, který by jinak probíhal,

— stanovení, které kontrolní metody lze používat pro účely bezpečnosti, aniž by byl požadován souhlas uživatelů,

— stanovení, které kontrolní metody vyžadují souhlas uživatelů, zejména pak souhlas všech dotčených uživatelů, a stanovení přípustných technických parametrů, aby bylo zajištěno, že tyto kontrolní metody nezahrnují zpracování údajů, jež nejsou přiměřené vzhledem k zamýšleným účelům,

— navíc může být ve třech výše uvedených případech nutné vydat pokyny k uplatňování nezbytných bezpečnostních opatření na ochranu údajů (omezení účelu, bezpečnost atd.).

83. Vzhledem k tomu, že kompetence jsou v této oblasti jak na vnitrostátní úrovni, tak i na úrovni EU, evropský inspektor ochrany údajů se domnívá, že je velmi důležité vyměňovat si názory a zkušenosti, aby byly nalezeny harmonizované přístupy k výše uvedené problematice. Za tímto účelem evropský inspektor ochrany údajů navrhuje vytvořit platformu či expertní skupinu, která by zahrnovala zástupce vnitrostátních regulačních orgánů, pracovní skupinu zřízenou podle článku 29, evropského inspektora ochrany údajů a BEREC. Prvním cílem této platformy by bylo vypracovat pokyny alespoň k výše uvedeným bodům, aby byly zajištěny pevné a harmonizované přístupy a stejné podmínky. Evropský inspektor ochrany údajů vyzývá Komisi, aby se této iniciativy ujala.

84. V neposlední řadě vnitrostátní orgány i jejich unijní protějšky, včetně sdružení BEREC a Komise EU, musí pečlivě sledovat vývoj trhu v této oblasti. Z pohledu ochrany osobních údajů a soukromí by byl scénář, kdy by poskytovatelé internetových služeb rutinně používali zásady řízení provozu a nabízeli služby na základě filtrování přístupu k obsahu a aplikacím, vysoce problematický. Pokud by k tomu mělo někdy dojít, bylo by nutné přijmout takové zákony, které by se touto situací zabývaly.

VII. **ZÁVĚRY**

85. Stále větší používání monitorování a kontrolních metod ze strany poskytovatelů internetových služeb ohrožuje neutralitu sítě a důvěrnost komunikace. S tím souvisejí závažné otázky týkající se ochrany soukromí uživatelů a jejich osobních údajů.

86. Přestože se sdělení Komise k otevřenému internetu a neutralitě sítě v Evropě těmito otázkami krátce zabývá, evropský inspektor ochrany údajů se domnívá, že je třeba učinit více, abychom dospěli k uspokojivé politice do budoucna. V tomto stanovisku proto přispívá k probíhající politické debatě o neutralitě sítě, zejména pak k aspektům souvisejícím s ochranou osobních údajů a soukromí.

87. Evropský inspektor ochrany údajů je přesvědčen, že je třeba, aby vnitrostátní orgány a BEREC monitorovaly situaci na trhu. Toto monitorování by mělo přinést jasný obraz popisující, zda se trh vyvíjí směrem k masivní kontrole komunikace v reálném čase a problémy spojené s dodržováním právního rámce.

88. Monitorování trhu by nemělo probíhat bez další analýzy účinků, které mají nové metody v souvislosti s ochranou osobních údajů a soukromí, na internet. V tomto stanovisku jsou uvedeny některé oblasti, které by potřebovaly objasnit. I když mají agentury a subjekty EU, jako je např. BEREC, pracovní skupina zřízená podle článku 29 a evropský inspektor ochrany údajů, možnost objasnit podmínky uplatňování právního rámce, evropský inspektor ochrany údajů se domnívá, že koordinovat a řídit tuto debatu je povinností Komise. Proto vyzývá Komisi, aby se v tomto smyslu ujala iniciativy začleňující všechny zainteresované strany do platformy nebo pracovní skupiny. Mezi záležitostmi, které potřebují další analýzu, je třeba vyřešit toto:

— stanovit kontrolní metody, které jsou oprávněné pro zajištění hladkého průběhu provozu a které lze provádět za účelem zajištění bezpečnosti,

— stanovit, kdy monitorování vyžaduje souhlas jednotlivců, zejména pak souhlas všech dotčených uživatelů, a přípustné technické parametry, aby bylo zajištěno, že kontrolní metody nezahrnují zpracování osobních údajů, které nejsou přiměřené vzhledem k zamýšlenému účelu,

— ve výše uvedených případech může být potřebné vydat pokyny k uplatňování nezbytných bezpečnostních opatření na ochranu osobních údajů (omezení účelu, bezpečnost atd.).

89. V závislosti na těchto zjištěních může být nutné přijmout další legislativní opatření. V takovém případě musí Komise zavést politická opatření směřující k posílení právního rámce a zajištění právní jistoty. Nová opatření musí objasnit praktické důsledky zásady neutrality sítě, jak to již bylo učiněno v některých členských státech, a zajistit, aby uživatelé měli skutečnou možnost volby, a to zejména tak, že poskytovatelé internetových služeb budou nuceni nabízet nemonitorované připojení.

V Bruselu dne 7. října 2011.

Peter HUSTINX

evropský inspektor ochrany údajů