I

(Uznesenia, odporúčania a stanoviská)

STANOVISKÁ

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko európskeho dozorného úradníka pre ochranu údajov k neutralite siete, riadeniu dátových tokov a ochrane súkromia a osobných údajov

(2012/C 34/01)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 16,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej články 7 a 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov ([1]),

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov ([2]), a najmä na jeho článok 41 ods. 2,

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ([3]),

PRIJAL TOTO STANOVISKO:

I. ÚVOD

I.1. Východiská

1. Dňa 19. apríla 2011 Komisia prijala oznámenie s názvom Otvorený internet a neutralita siete v Európe ([4]).

2. Toto stanovisko sa môže považovať za reakciu európskeho dozorného úradníka pre ochranu údajov na toto oznámenie a jeho cieľom je prispieť k prebiehajúcej politickej diskusii v EÚ o neutralite siete, najmä o aspektoch týkajúcich sa ochrany údajov a súkromia.

([1]) Ú. v. ES L 281, 23.11.1995, s. 31, „smernica o ochrane údajov".
([2]) Ú. v. ES L 8, 12.1.2001, s. 1, „nariadenie o ochrane údajov".
([3]) Ú. v. ES L 201, 31.7.2002, s. 37, zmenená a doplnená smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (pozri 15. poznámku pod čiarou), „smernica o súkromí a elektronických komunikáciách".
([4]) KOM(2011) 222 v konečnom znení.

3. Stanovisko sa zakladá na reakcii ([5]) európskeho dozorného úradníka pre ochranu údajov na verejnú konzultáciu Komisie o otvorenom internete a neutralite siete v Európe, ktorá sa konala pred prijatím oznámenia Komisie. Európsky dozorný úradník pre ochranu údajov takisto vzal do úvahy nedávne závery Komisie o neutralite siete ([6]).

I.2. **Pojem neutralita siete**

4. Neutralita siete je predmetom diskusie o otázke, či by poskytovatelia internetových služieb ([7]) mali mať možnosť obmedzovať, filtrovať alebo blokovať prístup na internet, alebo inak ovplyvňovať jeho funkcie. Pojem neutralita siete sa zakladá na názore, že informácie na internete by sa mali prenášať nestranne bez ohľadu na obsah, miesto určenia alebo zdroj a že užívatelia by sa mali rozhodnúť, ktoré aplikácie, služby a hardvér chcú používať. To znamená, že poskytovatelia internetových služieb nemôžu svojvoľne uprednostniť alebo spomaliť prístup k určitým aplikáciám alebo službám, ako napríklad peer-to-peer (P2P) atď ([8]).

5. S filtrovaním, blokovaním a prezeraním dátových tokov sa spájajú dôležité otázky, ktoré sa často neberú do úvahy, alebo sa považujú za menej dôležité a týkajú sa dôvernosti komunikácií a rešpektovania súkromia jednotlivcov a ich osobných údajov pri používaní internetu. Napríklad niektoré metódy prezerania zahŕňajú monitorovanie obsahu komunikácií, navštívených webových stránok, odoslaných a prijatých e-mailov, času ich realizácie atď., na základe ktorých je možné filtrovanie komunikácie.

6. Poskytovatelia internetových služieb porušujú prostredníctvom prezerania komunikačných údajov dôvernosť komunikácie, ktorá je základným právom stanoveným v článku 8 Európskeho dohovoru o ľudských právach a v článkoch 7 a 8 Charty základných práv Európskej únie. Dôvernosť chránia takisto sekundárne právne predpisy EÚ, konkrétne článok 5 smernice o súkromí a elektronických komunikáciách.

I.3. **Zameranie a štruktúra stanoviska**

7. Európsky dozorný úradník pre ochranu údajov sa domnieva, že v rámci vážnej politickej diskusie o neutralite siete je nevyhnutné zaoberať sa dôvernosťou komunikácií, ako aj ostatnými aspektmi ochrany súkromia a údajov.

8. Toto stanovisko prispieva k uvedenej prebiehajúcej európskej diskusii. Jeho cieľ je trojaký:

— Zdôrazňuje význam ochrany súkromia a údajov v súčasných diskusiách o neutralite siete. Presnejšie, zdôrazňuje nevyhnutnosť dodržiavať existujúce pravidlá týkajúce sa dôvernosti komunikácií. Mali by byť dovolené iba postupy, ktoré dodržiavajú uvedené pravidlá.

— Neutralita siete sa týka pomerne nových technických možností a v tejto súvislosti existuje málo skúseností s uplatňovaním právneho rámca. Toto stanovisko preto poskytuje odporúčania týkajúce sa plnenia povinnosti poskytovateľov internetových služieb uplatňovať a dodržiavať právny rámec v oblasti ochrany údajov, ak filtrujú, blokujú a prezerajú dátové toky na internete. Budú užitočné pre poskytovateľov internetových služieb a takisto pre orgány poverené presadzovaním rámca.

— Z hľadiska ochrany údajov a súkromia toto stanovisko určuje oblasti, ktorým je potrebné venovať osobitnú pozornosť a v ktorých môžu byť nevyhnutné opatrenia na úrovni EÚ. To je dôležité najmä vzhľadom na prebiehajúcu diskusiu na úrovni EÚ a politické opatrenia, ktoré môže Komisia v tejto súvislosti začať.

([5]) Európsky dozorný úradník pre ochranu údajov zdôraznil, že je dôležité brať do úvahy otázky ochrany údajov a súkromia spolu s ostatnými existujúcimi právami a hodnotami. Jeho reakcia je k dispozícii na webovej stránke: 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 dispozícii na webovej stránke http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Týka sa to poskytnutia pevného a mobilného prístupu na internet.

([8]) Aj keď sa táto zásada neuplatňuje na obmedzenia, ktoré poskytovatelia internetových služieb stanovujú v súvislosti s rýchlosťou alebo množstvom informácií, ktoré môže účastník odoslať alebo prijať prostredníctvom pripojenia na internet s obmedzením šírky pásma a objemu dát. Preto by poskytovatelia internetových služieb mohli aj v rámci zásady neutrality poskytovať pripojenie na internet s obmedzeným prístupom na základe kritérií, ako napríklad rýchlosť alebo objem dát, pokiaľ nie je nevyhnutná diskriminácia v prospech určitého obsahu alebo proti určitému obsahu.

9. Európsky dozorný úradník pre ochranu údajov si uvedomuje, že neutralita siete sa spája s ďalšími otázkami, ktoré sa uvádzajú ďalej v texte a ktoré sa týkajú napríklad prístupu k informáciám. Tieto otázky sa riešia, iba pokiaľ sa týkajú ochrany údajov a súkromia, alebo majú na ňu vplyv.

10. Štruktúra stanoviska je nasledujúca. II. časť sa začína stručným prehľadom postupov filtrovania poskytovateľmi internetových služieb. Predmetom III. časti je právny rámec EÚ pre neutralitu siete. Vo IV. časti sa ďalej uvádza technický opis a posúdenie vplyvu na súkromie v závislosti od použitého postupu. V V. časti sa analyzujú praktické údaje týkajúce sa uplatňovania súčasného rámca EÚ pre ochranu súkromia a údajov. Na základe uvedenej analýzy sa v VI. časti uvádzajú návrhy na ďalšie politické zmeny a určujú sa oblasti, v ktorých môže byť nevyhnutné spresnenie a zlepšenie. VII. časť obsahuje závery.

II. **NEUTRALITA SIETE A METÓDY RIADENIA DÁTOVÝCH TOKOV**

Intenzívnejšie používanie metód riadenia dátových tokov

11. Poskytovatelia internetových služieb spravidla monitorujú a ovplyvňujú dátové toky na internete iba za obmedzených okolností. Napríklad poskytovatelia internetových služieb uplatňujú metódy prezerania a obmedzené informačné toky s cieľom zachovať bezpečnosť siete, napr. bojovať proti vírusom. Preto sa internet všeobecne rozšíril a zároveň zachováva vysokú úroveň neutrality.

12. V posledných rokoch však niektorí poskytovatelia internetových služieb vyjadrili záujem o prezeranie dátových tokov na internete s cieľom diferencovať ich a uplatňovať na ne odlišné metódy, napríklad blokovať osobitné služby alebo poskytnúť prednostný prístup k iným službám. Niekedy sa to označuje ako „metódy riadenia dátových tokov“ ([9]).

13. Dôvody poskytovateľov internetových služieb na prezeranie a diferenciáciu dátových tokov sú rôzne. Napríklad metódy riadenia dátových tokov môžu pomôcť poskytovateľom internetových služieb riadiť dátové toky v čase vysokého preťaženia siete napríklad prostredníctvom uprednostnenia niektorých na čas citlivých dátových tokov, ako napríklad streaming videozáznamu, a degradovaním ostatných druhov dátových tokov, ktoré môžu byť menej citlivé na čas, ako napríklad P2P ([10]). Okrem toho riadenie dátových tokov môže byť pre poskytovateľov internetových služieb prostriedkom na získanie prípadného toku príjmov, ktorý môže pochádzať z rôznych zdrojov. Na jednej strane by poskytovatelia internetových služieb mohli vyberať poplatky od poskytovateľov služieb obsahu, napríklad od tých, ktorých služby vyžadujú použitie väčšieho rozsahu šírky pásma, a na základe toho ich uprednostnia (a poskytnú im vyššiu rýchlosť). To by znamenalo, že prístup k určitým službám, napríklad k službe poskytujúcej video na požiadanie, by bol rýchlejší ako prístup k inej podobnej službe, ktorá nepoužíva vysokorýchlostný prenos dát. Príjmy by takisto bolo možné získať od účastníkov, ktorí majú záujem zaplatiť vyššie (alebo nižšie) poplatky za určité diferencované druhy pripojenia. Napríklad pripojenie bez prístupu k P2P by mohlo byť lacnejšie ako pripojenie s neobmedzeným prístupom.

14. Okrem toho, že poskytovatelia internetových služieb majú svoje vlastné dôvody na používanie metód riadenia dátových tokov, takisto ostatné strany môžu mať záujem o to, aby poskytovatelia internetových služieb používali uvedené metódy. Ak poskytovatelia internetových služieb riadia svoje siete a prezerajú obsah, ktorý prechádza ich zariadeniami, pravdepodobne zvýšia svoju kapacitu na zistenie údajného protizákonného použitia, napr. porušenia autorských práv alebo použitia na pornografické účely.

([9]) Pozri napríklad správu orgánu OFCOM s názvom Site blocking to reduce online copyright infringement (Blokovanie stránok s cieľom znížiť porušovanie autorských práv online), prijatú 27. mája 2011, ktorá je dostupná na: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Niektorí poskytovatelia internetových služieb už v rámci svojej siete používajú takzvané systémy kontroly balíkov (z angl.: packet inspection) na riadenie dátových tokov a iné účely, preto predpokladáme, že sa môžu použiť, aj keď s tým bude súvisieť vysoká úroveň zložitosti a nákladov pre tých, ktorí ešte uvedené služby neprevádzkujú. Môže vzniknúť situácia, keď vzhľadom na nevyhnutnú kapitálovú investíciu budú môcť systém DPI používať v krátkodobom až strednodobom horizonte iba väčší poskytovatelia internetových služieb.“

([10]) Kvalita aplikácií v reálnom čase, ako napríklad streamig videozáznamu, okrem iného závisí od čakacej lehoty, t. j. omeškania spôsobeného napríklad preťažením siete.

Ostatné príslušné záujmy vrátane ochrany údajov a súkromia

15. Tento vývoj podnietil diskusiu o oprávnenosti tohto druhu postupov a presnejšie o otázke, či je potrebné, aby sa prostredníctvom právnych predpisov podrobnejšie stanovili osobitné povinnosti súvisiace s neutralitou siete.

16. Intenzívnejšie používanie opatrení na riadenie dátových tokov zo strany poskytovateľov internetových služieb by mohlo prípadne obmedziť prístup k informáciám. Pokiaľ by bol tento postup bežný a užívatelia by nemali úplný prístup na internet, ako ho poznáme (alebo by bol veľmi nákladný), ohrozilo by to prístup k informáciám a možnosť užívateľov odosielať a prijímať obsah, ktorý si vyberú, pomocou aplikácií alebo služieb, pre ktoré sa rozhodnú. Tomuto problému by mohla predísť právne záväzná zásada neutrality siete.

17. Preto sa európsky dozorný úradník pre ochranu údajov domnieva, že účasť poskytovateľov internetových služieb na riadení dátových tokov má vplyv na ochranu údajov a súkromia. Presnejšie:

— Ak poskytovatelia internetových služieb spracúvajú prevádzkové dáta na jediný účel, a to nasmerovať tok informácií od odosielateľa k príjemcovi, vo všeobecnosti vykonávajú obmedzené spracovanie osobných údajov ([11]). Tak isto ako poštové služby spracúvajú informácie uvedené na obálke listu, poskytovateľ internetových služieb spracúva informácie nevyhnutné na nasmerovanie komunikácie k príjemcovi. Tento postup nie je v rozpore s právnymi požiadavkami ochrany údajov, súkromia a dôvernosti komunikácií.

— Ak však poskytovatelia internetových služieb prezerajú komunikačné údaje s cieľom diferencovať každý komunikačný tok a uplatniť osobitné metódy, ktoré môžu byť pre jednotlivcov nevýhodné, následky sú vážnejšie. Spracovanie údajov môže mať veľmi nepriaznivý vplyv na súkromie a údaje jednotlivca, a to v závislosti od okolností každého prípadu a druhu vykonanej analýzy. To je zrejmejšie v prípadoch, keď metódy riadenia odhaľujú obsah internetových komunikácií jednotlivcov vrátane odoslaných a prijatých e-mailov, navštívených webových stránok, prijatých súborov atď.

III. PREHĽAD PRÁVNEHO RÁMCA EÚ PRE NEUTRALITU SIETE A ĎALŠÍ POLITICKÝ VÝVOJ

III.1. Stručne o právnom rámci

18. Až do roku 2009 európske právne nástroje neobsahovali ustanovenia, ktoré by poskytovateľom internetových služieb výslovne zakazovali filtrovanie, blokovanie alebo stanovenie dodatočných poplatkov účastníkom za prístup k službám. Takisto neobsahovali ustanovenia, ktoré by výslovne uznávali takýto postup. Táto situácia bola do istej miery neistá.

19. Zmenil ju súbor opatrení v telekomunikačnej oblasti, prijatý v roku 2009 vrátane ustanovení uprednostňujúcich otvorenosť internetu. Napríklad v článku 8 ods. 4 spoločného regulačného rámca pre elektronické komunikačné siete a služby (rámcová smernica) sa stanovuje regulačným orgánom povinnosť podporovať prípadný prístup koncových užívateľov k obsahu, aplikáciám alebo službám podľa svojho výberu ([12]). Toto ustanovenie sa uplatňuje na sieť ako celok, a nie na úrovni jednotlivých poskytovateľov. V nedávnych záveroch Rady sa takisto zdôrazňuje nevyhnutnosť zachovať otvorenosť internetu ([13]).

([11]) To vylučuje operácie zamerané na zvýšenie bezpečnosti siete a zistenie škodlivých dátových tokov, a takisto operácie nevyhnutné na fakturáciu a prepojenie. Takisto vylučuje povinnosti, ktoré vyplývajú zo smernice o uchovávaní údajov, smernice Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES, (Ú. v. EÚ L 105, 13.4.2006, s. 54) (smernica o uchovávaní údajov).

([12]) Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby, zmenená a doplnená smernicou 2009/140/ES a nariadením č. 544/2009 (Ú. v. EÚ L 337, 18.12.2009, s. 37).

([13]) Pozri bod 3 písm. e), v ktorom Rada uznáva: „nevyhnutnosť zachovať otvorenosť internetu a zároveň zabezpečiť, aby mohol naďalej poskytovať kvalitné služby v rámci, ktorý podporuje a dodržiava základné práva, ako napríklad slobodu prejavu a slobodu podnikania“ a odsek 8 písm. d), v ktorom vyzýva členské štáty, aby „podporovali otvorený a neutrálny charakter internetu ako svoj politický cieľ“.

20. Smernica univerzálnej služby ([14]) obsahuje viac konkrétnych povinností. Články 20 a 21 stanovujú požiadavky transparentnosti týkajúce sa obmedzení prístupu a/alebo používania služieb a aplikácií. Takisto stanovuje minimálnu úroveň kvality služieb.

21. Pokiaľ ide o postupy poskytovateľov internetových služieb zahŕňajúce prezeranie komunikácií jednotlivcov, v 28. odôvodnení smernice, ktorou sa mení a dopĺňa smernica univerzálnej služby a smernica o súkromí a elektronických komunikáciách ([15]), sa zdôrazňuje, že „v závislosti od použitej technológie a typu obmedzení môžu takéto obmedzenia vyžadovať súhlas užívateľa v súlade so smernicou 2002/58/ES (smernica o súkromí a elektronických komunikáciách)". V 28. odôvodnení sa teda pripomína, že v súvislosti s každým obmedzením založeným na monitorovaní komunikácií je nevyhnutný súhlas užívateľa, ako sa stanovuje v článku 5 ods. 1 smernice o súkromí a elektronických komunikáciách. V ďalej uvedenej IV. časti sa analyzuje uplatňovanie článku 5 ods. 1 a právny rámec pre celkovú ochranu údajov a súkromia.

22. Podľa článku 22 ods. 3 smernice univerzálnej služby môžu vnútroštátne regulačné orgány stanoviť poskytovateľom internetových služieb, ak je to nevyhnutné, minimálne požiadavky na kvalitu s cieľom zabrániť zníženiu úrovne služieb a obmedzeniu alebo spomaleniu dátových tokov vo verejných sieťach.

23. Z uvedených skutočností vyplýva, že na európskej úrovni existuje všeobecné úsilie o otvorený internet (pozri článok 8 ods. 4 rámcovej smernice). Tento cieľ, ktorý sa uplatňuje na sieť ako celok, sa priamo nespája so zákazmi alebo povinnosťami jednotlivých poskytovateľov internetových služieb. Inými slovami, poskytovateľ internetových služieb by mohol uplatňovať metódy riadenia dátových tokov, ktoré môžu vylučovať prístup k niektorým aplikáciám, pod podmienkou, že koncoví užívatelia budú úplne informovaní a slobodne, výslovne a jednoznačne vyjadria svoj súhlas.

24. Táto situácia môže byť v jednotlivých členských štátoch odlišná. V niektorých členských štátoch môžu poskytovatelia internetových služieb za určitých podmienok uplatňovať metódy riadenia dátových tokov, napríklad blokovať aplikácie, ako napríklad prenos hlasu cez IP (v rámci lacnejšieho pripojenia na internet) pod podmienkou, že jednotlivci poskytli svoj slobodný, výslovný, jednoznačný a informovaný súhlas. Ostatné členské štáty sa rozhodli podporovať zásadu neutrality siete. Napríklad v júli 2011 holandský parlament prijal zákon, ktorý vo všeobecnosti zakazuje poskytovateľom obmedzovať alebo spomaľovať aplikácie alebo služby na internete (napríklad prenos hlasu cez IP), pokiaľ z dôvodu integrity alebo bezpečnosti nie je nevyhnutné minimalizovať vplyv preťaženia siete s cieľom bojovať proti nevyžiadanej pošte alebo na základe súdneho príkazu ([16]).

III.2. **Oznámenie o neutralite siete**

25. Európska komisia vo svojom oznámení o neutralite siete ([17]) konštatuje, že situácia v oblasti neutrality siete vyžaduje monitorovanie a ďalšiu analýzu. Jej prístup pred prijatím ďalších regulačných opatrení sa označuje za vyčkávací.

([14]) Smernica 2002/22/ES zmenená a doplnená smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa (Ú. v. EÚ L 337, 18.12.2009, s. 11). Porovnaj takisto článok 1 ods. 3, v ktorom sa uvádza, že táto smernica nenariaďuje ani nezakazuje podmienky uložené poskytovateľmi verejne dostupných elektronických komunikačných služieb, obmedzujúce prístup koncových užívateľov k službám a aplikáciám a/alebo ich využívanie, ak je to povolené v rámci vnútroštátneho práva a v súlade s právom Spoločenstva, ale ustanovuje povinnosť poskytovať informácie o týchto podmienkach.

([15]) Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa.

([16]) Pôvodná zmena a doplnenie holandského zákona je k dispozícii na: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Dôvody, ktoré tlač uvádza v súvislosti s prijatím uvedeného politického opatrenia, nesúvisia s ochranou údajov a súkromia, ale sú skôr zamerané na zabezpečenie, aby sa užívateľom nebránilo v prístupe k informáciám alebo aby tento prístup nebol obmedzený. Preto sa zdá, že podnetom na zmenu a doplnenie zákona boli otázky týkajúce sa prístupu k informáciám.

([17]) Porovnaj poznámku pod čiarou 4.

26. Komisia vo svojom oznámení uznáva, že každé opatrenie a ďalšie regulačné opatrenia budú podliehať hĺbkovému posúdeniu aspektov ochrany údajov a súkromia. V záveroch Rady sa takisto berú do úvahy príslušné otázky ochrany údajov a súkromia ([18]).

27. Z hľadiska ochrany údajov a súkromia je potrebné posúdiť otázku, či je vyčkávací prístup dostatočný. Aj keď rámec pre ochranu údajov a súkromia v súčasnosti predpokladá niektoré ochranné opatrenia, najmä prostredníctvom zásady dôvernosti komunikácií, zdá sa, že je nevyhnutné dôkladne monitorovať úroveň dodržiavania pravidiel a usmernení o niektorých aspektoch tejto otázky, ktoré nie sú veľmi jasné. Okrem toho je vzhľadom na technický vývoj potrebné uviesť niektoré úvahy týkajúce sa možného spresnenia a ďalšieho zlepšenia rámca. Legislatívne opatrenia budú nevyhnutné, ak sa v rámci monitorovania zistí, že trh sa vyvíja smerom k podstatnému prezeraniu komunikácií v reálnom čase a otázkam súvisiacim s dodržiavaním rámca. V tejto súvislosti sa v VI. časti uvádzajú konkrétne návrhy.

IV. **TECHNICKÉ OKOLNOSTI A SÚVISIACI VPLYV NA OCHRANU SÚKROMIA A ÚDAJOV**

28. Pred dôkladnejším preskúmaním otázky je dôležité získať lepší prehľad o metódach prezerania, ktoré môžu používať poskytovatelia internetových služieb na riadenie dátových tokov, a o ich prípadnom vplyve na zásadu neutrality siete. Vplyv na ochranu súkromia a údajov, vyplývajúci z uvedených postupov sa podstatne odlišuje v závislosti od použitých postupov. Je nevyhnutné uvedomiť si tieto technické okolnosti a primerane uplatňovať rámec pre ochranu údajov uvedený v V. časti. Je však potrebné uviesť, že je to zložitá oblasť, ktorá sa stále mení. Preto opis, ktorý sa uvádza ďalej v texte, nemá byť všestranný a úplne aktuálny, má len poskytovať technické informácie, ktoré sú nevyhnutné na porozumenie právnemu odôvodneniu.

IV.1. **Prenos informácií prostredníctvom internetu: základy**

29. Ak užívateľ prenáša komunikáciu prostredníctvom internetu, prenášané informácie sa rozdelia do dvoch tzv. paketov. Tieto pakety sa prenášajú v rámci internetu od odosielateľa k príjemcovi. Každý paket bude okrem iného obsahovať informácie o zdroji a mieste určenia. Navyše poskytovatelia internetových služieb môžu vložiť tieto pakety do ďalších vrstiev a protokolov ([19]), ktoré sa použijú na riadenie rôznych dátových tokov v rámci siete poskytovateľa internetových služieb.

30. Ak uvedieme podobnosť s poštovými listami, používanie protokolu prenosu v sieti sa zhoduje s vložením obsahu listu do obálky označenej adresou miesta určenia, na základe ktorej poštové služby list doručia. Poštové služby môžu v rámci svojej vnútornej prepravy používať dodatočné protokoly na prenos všetkých zásielok s cieľom doručiť každú zásielku na miesto určenia, ako ho pôvodne uviedol odosielateľ. Ak použijeme túto podobnosť, každý paket má dve časti, časť *IP užívateľské dáta* (*IP payload*), ktorá zahŕňa obsah komunikácie a zhoduje sa s listom. Obsahuje informácie určené iba príjemcovi. Druhá časť paketu je *IP hlavička* (*IP header*), ktorá obsahuje okrem iného adresu príjemcu a odosielateľa a zhoduje sa s obálkou. Na základe IP hlavičky môžu poskytovatelia internetových služieb a ostatní sprostredkovatelia nasmerovať užívateľské dáta od zdrojovej adresy k adrese miesta určenia.

31. Poskytovatelia internetových služieb a ostatní sprostredkovatelia zabezpečujú, aby sa IP pakety pohybovali v rámci siete cez uzly, ktoré čítajú informácie z IP hlavičky, porovnajú ju so smerovacími tabuľkami a nasmerujú k ďalšiemu uzlu na trase k miestu určenia. Tento proces sa vykonáva v sieti

([18]) Pozri odsek 4 písm. e), v ktorom Rada berie do úvahy: „znepokojenie najmä orgánov pre ochranu údajov, týkajúce sa ochrany osobných údajov".

([19]) Ako sa uvádza v časti IV.2, uvedené protokoly kódujú informácie, ktoré sa prenášajú medzi koncovými užívateľmi dohodnutým spôsobom tak, že strany zúčastňujúce sa na komunikácii si navzájom rozumejú, ako napríklad HTTP, FTP atď.

prostredníctvom takzvaného bezpamäťového prístupu, keďže so všetkými súbormi v uzle sa zaobchádza neutrálne. Keď sa presunú k ďalšiemu uzlu, nie je potrebné ďalej uchovávať informácie v smerovacom programe ([20]).

IV.2. **Metódy prezerania**

32. Ako sa uvádza predtým v texte, poskytovatelia internetových služieb čítajú IP hlavičky na účely ich nasmerovania k miestu určenia. Analýzu dátových tokov (vrátane IP hlavičiek a IP užívateľských dát) je však možné vykonať na iné účely a pomocou rôznych druhov technológií. Nové trendy môžu zahŕňať napríklad spomalenie niektorých aplikácií, ktoré užívateľ používa, napríklad P2P, alebo podobne zvýšenie rýchlosti niektorých služieb, napríklad služieb poskytovania videozáznamu na požiadanie pre dôležitých účastníkov. Aj keď sa v rámci všetkých metód prezerania *technicky* vykonáva prezeranie paketov, tieto metódy sa spájajú s odlišnými úrovňami narušenia. Existujú dve hlavné kategórie metód prezerania. Jedna sa zakladá iba na IP hlavičke, druhá aj na IP užívateľských dátach.

Na základe informácií z IP hlavičky. Prezeranie IP hlavičky paketu odhalí niektoré oblasti, ktoré môžu poskytovateľom internetových služieb umožniť uplatňovanie viacerých osobitných metód riadenia dátových tokov. Tieto postupy, ktoré sa zakladajú iba na prezeraní IP hlavičiek, spracúvajú na rôzne účely (napr. diferenciácia dátových tokov) údaje, ktoré sú v zásade určené na smerovanie informácií. Na základe zdrojovej IP adresy ich poskytovateľ internetových služieb môže spojiť s konkrétnym účastníkom a uplatniť niektoré osobitné metódy, napríklad smerovanie paketu prostredníctvom rýchlejšieho alebo pomalšieho spojenia. Na základe IP adresy miesta určenia môže poskytovateľ internetových služieb takisto uplatniť osobitné metódy, napríklad blokovanie alebo filtrovanie prístupu k niektorým webovým stránkam.

Na základe dôkladnejšieho prezerania. Dôkladné prezeranie paketov umožňuje poskytovateľom internetových služieb prístup k informáciám určeným iba príjemcovi komunikácie. Ak sa vrátime k príkladu poštových služieb, tento prístup sa zhoduje s otvorením obálky a prečítaním listu s cieľom analyzovať obsah komunikácie (uzatvorenej v IP paketoch) v záujme uplatnenia osobitných metód na riadenie siete. Existujú rôzne spôsoby prezerania, pričom každý ohrozuje dotknutú osobu inak.

— *Dôkladné prezeranie paketu na základe analýzy protokolov a štatistických záznamov*. Okrem protokolu IP, ktorého úlohou je umožniť prenos dát v rámci internetu, existujú ďalšie protokoly, ktoré dohodnutým spôsobom kódujú prenášané informácie (preprava, spojenie s databázou, prezentácia a aplikácia atď.). Cieľ týchto protokolov je zabezpečiť, aby si strany zúčastnené na komunikácii navzájom rozumeli. Existuje napríklad niekoľko protokolov, ktoré sa spájajú s prehľadávaním siete ([21]), ďalšie sú na prenos súborov ([22]) atď. Preto metódy prezerania založené na prezeraní protokolov sa spolu so štatistickou analýzou zameriavajú na hľadanie osobitných vzorov alebo odtlačkov prstov, ktoré určia, ktoré protokoly sú prítomné ([23]). Tieto metódy prezerania umožňujú poskytovateľom internetových služieb zistiť, o aký druh komunikácie ide (e-mail, prehľadávanie siete, presúvanie súborov), a v niektorých prípadoch určiť osobitnú službu alebo používanú aplikáciu, ako je to v prípade niektorých komunikácií prenosu hlasu cez IP, v ktorých sú použité protokoly veľmi špecifické pre konkrétneho dodávateľa alebo poskytovateľa služieb. Keď poskytovateľ internetových služieb pozná druh komunikácie, môže uplatniť konkrétne metódy riadenia dátových tokov. Napríklad blokovať prevádzku siete. Takisto to môže byť prvý krok, na základe ktorého môžu poskytovatelia internetových služieb vykonať ďalšie analýzy, ktoré môžu vyžadovať úplný prístup k metaúdajom a obsahu komunikácie.

([20]) Sieťové zariadenie internetu používa smerovacie protokoly, ktoré vedú záznamy o činnosti, spracúvajú štatistické údaje o dátových tokoch a vymieňajú informácie s ostatnými sieťovými zariadeniami s cieľom smerovať IP pakety najefektívnejšou trasou. Napríklad ak je spojenie nepriechodné alebo prerušené a smerovací program dostane túto informáciu, program aktualizuje svoju smerovaciu tabuľku o niekoľko alternatív, ktoré nepoužívajú toto spojenie. Takisto je potrebné uviesť zber a spracovanie, ktoré sa v niektorých prípadoch môžu vykonať na účely fakturácie alebo dokonca v súlade s požiadavkami smernice o uchovávaní údajov.

([21]) HTTP – hypertextový prenosový protokol (Hypertext transfer protocol) – alebo HTML – hypertextový značkový jazyk (Hypertext Markup Language).

([22]) FTP – protokol prenosu súborov (File transfer protocol).

([23]) Existujú rôzne spôsoby identifikácie použitých protokolov. Napríklad je možné vyhľadávať v osobitných oblastiach vo vnútorných protokoloch, napr. identifikovať porty použité na vytvorenie komunikácie. Štatistická charakteristika komunikačného toku sa môže takisto odvodzovať z analýzy niektorých osobitných oblastí, korelácie protokolov, ktoré sa súčasne používajú medzi dvomi IP adresami.

— *Dôkladné prezeranie paketov na základe analýzy obsahu komunikácie.* Takisto je možné prezerať metaúdaje ([24]) a obsah komunikácie. Podstatou tejto metódy je zachytenie všetkých IP paketov, ktoré sú súčasťou pôvodného komunikačného toku tak, že je možné úplne obnoviť a analyzovať pôvodný obsah komunikácie. Napríklad na zistenie škodlivého alebo protizákonného obsahu, ako sú napríklad vírusy, detská pornografia atď., je nevyhnutné obnoviť obsah tak, aby ho bolo možné analyzovať. Je potrebné uviesť, že niekedy môžu zúčastnené strany výslovne zakódovať komunikáciu po celej dĺžke spojenia a tento postup zabráni poskytovateľom internetových služieb vykonať analýzu obsahu komunikácie.

IV.3. **Vplyv na ochranu súkromia a údajov**

33. Metódy prezerania založené na kontrole IP hlavičiek a najmä na prezeraní paketu zahŕňajú monitorovanie a filtrovanie uvedených údajov a majú vážny vplyv z hľadiska ochrany súkromia a údajov. Takisto môžu byť v rozpore s právom na dôvernosť komunikácií.

34. Nahliadnutie do komunikácie jednotlivcov má vážny vplyv na ochranu súkromia a údajov. Tento problém je širší, keďže vplyv na súkromie sa môže ďalej zväčšovať, a to v závislosti od účinkov, na dosiahnutie ktorých sa monitorovanie a zachytávanie súborov zameriava. Prezeranie komunikácií napríklad s cieľom zabezpečiť správne fungovanie systému nie je v skutočnosti to isté ako prezeranie komunikácií s cieľom uplatniť opatrenia, ktoré môžu mať vplyv na jednotlivcov. Ak sú prevádzkové a selektívne opatrenia zamerané iba na predchádzanie preťaženiu siete, spravidla nemajú veľký vplyv na súkromie jednotlivcov. Metódy riadenia dátových tokov však môžu byť zamerané na blokovanie niektorých informácií v obsahu, alebo majú vplyv na komunikáciu napríklad prostredníctvom behaviorálnej reklamy. V tých prípadoch je vplyv rušivejší. Znepokojenie je vážnejšie, ak si uvedomíme, že tento druh informácií sa nezbiera pre malé skupiny jednotlivcov, ale na všeobecnom základe, pre všetkých zákazníkov poskytovateľov internetových služieb ([25]). Keby všetci poskytovatelia internetových služieb používali metódy filtrovania, výsledkom by mohlo byť všeobecné monitorovanie používania internetu. Okrem toho, ak sa zameriame na druh spracúvaných informácií, ohrozenie súkromia je zjavne vyššie, lebo pravdepodobne mnohé informácie, ktoré sa zbierajú, sú veľmi citlivé a po získaní sú dostupné poskytovateľom internetových služieb a subjektom, ktoré by ich požiadali o informácie. Navyše informácie môžu byť veľmi hodnotné z obchodného hľadiska. To predstavuje veľké riziko využívania údajov na neplánované účely, pričom sa pôvodné účely môžu ľahko zmeniť na obchodné alebo iné využívanie získaných údajov.

35. Správne uplatňovanie metód monitorovania, prezerania a filtrovania sa musí vykonávať v súlade s platnými opatreniami na ochranu údajov a súkromia, ktoré stanovujú obmedzenia týkajúce sa toho, čo je možné vykonať a za akých okolností. Ďalej sa uvádza prehľad platných ochranných opatrení podľa súčasného právneho rámca EÚ pre ochranu údajov a súkromia.

V. **UPLATŇOVANIE PRÁVNEHO RÁMCA EÚ PRE OCHRANU SÚKROMIA A ÚDAJOV**

36. Rámec EÚ pre ochranu údajov je technicky neutrálny; neupravuje uvedené osobitné metódy prezerania. V smernici o súkromí a elektronických komunikáciách sa upravuje súkromie v ustanovení o elektronických komunikačných službách vo verejných sieťach (spravidla prístup na internet a

([24]) Každý protokol má vo svojej hlavičke osobitné oblasti, ktoré poskytujú dodatočné neformálne informácie o prenášanej komunikácii. Preto sa obsah uvedených oblastí môže označiť za metaúdaje komunikácie. Príkladom týchto oblastí môže byť použité číslo portu, pričom napríklad ak je to číslo 80, je veľmi pravdepodobné, že druh komunikácie je prehľadávanie siete.

([25]) Samozrejme, možnosti sledovania majú nielen poskytovatelia internetových služieb. Takisto prevádzkovatelia reklamných sietí môžu sledovať užívateľov na webových stránkach prostredníctvom cookies tretích subjektov. Pozri napríklad najnovší akademický článok, z ktorého vyplýva, že Google je prítomný na 97 zo 100 najnavštevovanejších webových stránok, čo znamená, že Google môže sledovať užívateľov, ktorí nevylúčili cookies tretích subjektov pri prehľadávaní týchto obľúbených webových stránok. Pozri: 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. júl 2011). K dispozícii na SSRN: http://ssrn.com/abstract=1898390 Sledovaním užívateľov prostredníctvom cookies tretích subjektov sa zaoberala pracovná skupina zriadená podľa článku 29. Pozri stanovisko 2/2010 k behaviorálnej reklame online, prijaté 22. júna 2010 (WP 171).

telefónne služby) ([26]) a smernica o ochrane údajov všeobecne upravuje spracovanie údajov. Tento právny rámec ako celok stanovuje rôzne povinnosti týkajúce sa poskytovateľov internetových služieb, ktorí spracúvajú a monitorujú prevádzkové a komunikačné dáta.

V.1. **Právne základy spracovania prevádzkových a obsahových dát**

37. V rámci právnych predpisov o ochrane údajov vyžaduje spracovanie osobných údajov, ako v tomto prípade spracovanie prevádzkových a komunikačných dát, primeraný právny základ. Okrem tejto všeobecnej požiadavky sa v niektorých prípadoch môžu uplatňovať osobitné požiadavky.

38. V tomto prípade druh osobných údajov, ktoré spracúvajú poskytovatelia internetových služieb, zahŕňa prevádzkové dáta a obsah komunikácií. Obsah komunikácií a prevádzkové dáta sú chránené právom na dôvernosť korešpondencie, ktoré sa stanovuje v článku 8 EDĽP a v článkoch 7 a 8 charty. Presnejšie v článku 5 ods. 1 smernice o súkromí a elektronických komunikáciách s názvom Dôvernosť správy sa stanovuje, že členské štáty zabezpečia dôvernosť správ a príslušných prevádzkových dát prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí. Zároveň sa v článku 5 ods. 1 smernice o súkromí a elektronických komunikáciách stanovuje, že poskytovatelia internetových služieb za určitých podmienok a so súhlasom užívateľov spracúvajú prevádzkové dáta a údaje o obsahu. Pritom zakážu „počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami zo strany iných osôb než sú užívatelia bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1.“ To je predmetom ďalších odsekov.

39. Okrem súhlasu príslušných užívateľov sa v smernici o súkromí a elektronických komunikáciách stanovujú iné dôvody, na základe ktorých môžu poskytovatelia internetových služieb spracúvať prevádzkové a komunikačné dáta. Príslušné právne základy pre spracovanie v týchto prípadoch sú i) poskytnutie služby; ii) zaručenie bezpečnosti služby; iii) minimalizácia preťaženia siete. Ďalšie dôvody oprávňujúce použitie riadiacich opatrení založených na prevádzkových alebo komunikačných dátach sú uvedené ďalej v bode iv).

i) Právne základy pre poskytovanie služby

40. Ako sa uvádza vo IV. časti, poskytovatelia internetových služieb spracúvajú informácie o IP hlavičkách na účely smerovania každého IP paketu na miesto určenia. Na základe článku 6 ods. 1 a 2 smernice o súkromí a elektronických komunikáciách je možné spracúvať prevádzkové dáta na účely prenosu správy. Poskytovatelia internetových služieb tak môžu spracúvať informácie, ktoré sú nevyhnutné na poskytnutie služby.

ii) Právne základy pre zaručenie bezpečnosti služby

41. Podľa článku 4 smernice o súkromí a elektronických službách má poskytovateľ internetových služieb všeobecnú povinnosť prijať primerané opatrenia na zaručenie bezpečnosti svojich služieb. Filtrovanie vírusov môže zahŕňať spracovanie IP hlavičiek a IP užívateľských dát. Vzhľadom na skutočnosť, že podľa článku 4 smernice o súkromí a elektronických službách sú poskytovatelia internetových služieb povinní zaručiť bezpečnosť siete, toto ustanovenie odôvodňuje metódy prezerania založené na IP hlavičkách a obsahu, ktorých cieľom je iba splnenie uvedeného účelu. V praxi to znamená, že v rámci obmedzení stanovených zásadou primeranosti (pozri časť V.3) poskytovatelia internetových služieb môžu monitorovať a filtrovať komunikačné dáta s cieľom bojovať proti vírusom a celkovo zaručiť bezpečnosť siete ([27]).

([26]) V odôvodnení 10 smernice o súkromí a elektronických komunikáciách sa uvádza: „V elektronickom komunikačnom sektore sa smernica 95/46/ES uplatňuje najmä na všetky záležitosti týkajúce sa ochrany základných práv a slobôd, ktoré nie sú predmetom ustanovení tejto smernice, vrátane povinností spracovávateľov a práv jednotlivcov.“ V súvislosti so súhlasom dotknutej osoby je takisto dôležité 17. odôvodnenie: „Na účely tejto smernice súhlas užívateľa alebo účastníka, bez ohľadu na to, či je účastník fyzickou alebo právnickou osobou, by mal mať rovnaký význam ako súhlas dátového subjektu definovaného a ďalej špecifikovaného v smernici 95/46/ES.“

([27]) Stanovisko č. 2/2006 pracovnej skupiny zriadenej podľa článku 29, ktoré sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty, prijaté 21. februára 2006 (PS 118). Pracovná skupina sa v tomto stanovisku domnieva, že používanie filtra na účely článku 4 môže byť zlučiteľné s článkom 5 smernice o ochrane súkromia v elektronickej sfére.

iii) Právne základy pre minimalizáciu následkov preťaženia

42. Odôvodnenie tohto právneho základu sa nachádza v 22. odôvodnení smernice o súkromí a elektronických komunikáciách, ktoré vysvetľuje zákaz ukladania správ, ktorý je predmetom článku 5 ods. 1. Nezakazuje sa akékoľvek automatické, dočasné a prechodné uloženie informácií, pokiaľ sa uskutočňuje výhradne na účely prenosu a za predpokladu, že informácie sa neukladajú na dlhší čas, než je nevyhnutné na prenos a riadenie chodu prenosu, a že je zaručená dôvernosť informácií.

43. V prípade preťaženia siete vzniká otázka, či poskytovatelia internetových služieb môžu uvažovať o náhodnom vynechaní alebo omeškaní dátových tokov, alebo skôr o spomalení komunikácií, ktoré nie sú citlivé na čas, napr. P2P alebo e-mailov, pričom sa tým umožní napríklad primeraná kvalita hlasových dátových tokov.

44. Vzhľadom na celkový spoločenský záujem zaručiť použiteľné komunikačné siete poskytovatelia internetových služieb môžu namietať, že uprednostnenie alebo spomalenie dátových tokov na riešenie preťaženia siete je legitímne opatrenie nevyhnutné na poskytnutie primeranej služby. To znamená, že v týchto prípadoch a na tento účel by existoval všeobecný právny základ na spracovanie osobných údajov a osobitný súhlas užívateľov by nebol nevyhnutný.

45. Zároveň schopnosť zasahovať týmto spôsobom nie je neobmedzená. Ak je potrebné, aby poskytovatelia internetových služieb prezerali komunikácie, z hľadiska dôvernosti a v prísnom súlade so zásadou primeranosti musia použiť najmenej rušivý dostupný postup na dosiahnutie cieľa (pričom sa predíde dôkladnému prezeraniu paketu) a použijú ho iba na čas nevyhnutný na riešenie preťaženia siete.

iv) Právne základy pre spracovanie údajov na iné účely

46. Poskytovatelia internetových služieb môžu mať takisto záujem o prezeranie prevádzkových a obsahových dát na iné účely napríklad s cieľom ponúknuť cielené pripojenie (napr. pripojenie, ktoré obmedzuje prístup k P2P, alebo pripojenie, ktoré zvyšuje rýchlosť niektorých aplikácií). Prezeranie a ďalšie použitie prevádzkových a komunikačných dát na iné účely ako poskytnutie služby alebo zaručenie jej bezpečnosti a predchádzanie preťaženiu siete je v súlade s právnym rámcom dovolené iba za určitých prísnych podmienok.

47. Právnym rámcom je predovšetkým článok 5 ods. 1 smernice o súkromí a elektronických komunikáciách, v ktorom sa stanovuje súhlas príslušných užívateľov na počúvanie, odpočúvanie alebo iné druhy narušovania a dohľadu nad správami a príslušnými prevádzkovými dátami. V praxi to znamená, že súhlas užívateľov zúčastnených na komunikácii je nevyhnutný na odôvodnenie spracovania prevádzkových a komunikačných dát podľa článku 5 ods. 1.

48. Ako sa uvádza vyššie v texte, uplatňovanie metód prezerania a filtrovania sa zakladá na IP hlavičkách, ktoré sa považujú za prevádzkové dáta, alebo na dôkladnom prezeraní paketu, ktoré takisto zahŕňa užívateľské dáta IP, ktoré sa považujú za komunikačné dáta. Preto by v zásade uplatňovanie uvedených metód na účely iné ako poskytnutie služby alebo zaručenie bezpečnosti bolo zakázané, pokiaľ spracovanie nie je možné na oprávnenom základe, akým je napríklad súhlas (článok 5 ods. 1). Príklad uplatňovania článku 5 ods. 1 je, keď sa prevádzkovateľ internetových služieb rozhodne poskytnúť zákazníkom zníženú sadzbu za prístup na internet ako náhradu za prijímanie behaviorálnej reklamy, pričom na tento účel použije dôkladné prezeranie paketu, a teda aj komunikačných dát. Podľa článku 5 ods. 1 je preto nevyhnutný skutočný, konkrétny a informovaný súhlas.

49. Okrem toho sa v článku 6 smernice o súkromí a elektronických komunikáciách s názvom „Prevádzkové dáta“ stanovujú určité pravidlá týkajúce sa konkrétne prevádzkových dát. Presnejšie, stanovuje poskytovateľom internetových služieb možnosť spracúvať prevádzkové dáta na základe súhlasu užívateľa s

prijímaním služieb s pridanou hodnotou ([28]). Toto ustanovenie špecifikuje požiadavku súhlasu stanovenú v článku 5 ods. 1 v súvislosti s prevádzkovými dátami.

50. V praxi nemusí byť vždy ľahké určiť, napríklad v ktorých prípadoch je nevyhnutný súhlas a v ktorých prípadoch sa môže spracovanie odôvodniť bezpečnosťou siete, najmä ak je účel prezerania dvojaký (napríklad zabránenie preťaženiu siete a poskytnutie služieb s pridanou hodnotou). Je potrebné zdôrazniť, že súhlas sa nemôže považovať za jednoduché a systémové opatrenie na dodržiavanie zásad ochrany údajov.

51. V súvislosti s uplatňovaním rámca a najmä s rôznymi vyššie uvedenými aspektmi existuje málo skúseností. To je oblasť, v ktorej je dôležité ďalšie usmernenie, ako sa uvádza v VI. časti. Navyše existujú ďalšie príslušné aspekty týkajúce sa získania súhlasu, ktoré je takisto nevyhnutné osobitne posúdiť a ktoré sú uvedené ďalej v texte.

V.2. **Otázky týkajúce sa poskytnutia informovaného súhlasu ako právneho základu**

52. Súhlas, ktorý je nevyhnutný podľa článkov 5 a 6 smernice o súkromí a elektronických komunikáciách, má taký istý význam ako súhlas dotknutej osoby, ako sa uvádza a presnejšie vymedzuje v smernici 95/46/EHS ([29]). V článku 2 písm. h) sa stanovuje, že „súhlas osoby pracujúcej s údajmi znamená slobodne poskytnutú a informovanú indikáciu jeho prianí, ktorou osoba pracujúca s údajmi prejaví svoj súhlas, aby sa osobné údaje, ktoré sa ho týkajú, spracovali". Najnovšie sa úlohou súhlasu a požiadavkami stanovujúcimi jeho platnosť zaoberala pracovná skupina zriadená podľa článku 29 vo svojom stanovisku č. 15/2011 týkajúcom sa súhlasu ([30]).

53. Poskytovatelia internetových služieb, pre ktorých je nevyhnutný súhlas, aby mohli vykonávať prezeranie a filtrovanie prevádzkových a obsahových dát, musia preto zabezpečiť slobodný a konkrétny súhlas a je nevyhnutné, aby to bolo úplne informované vyjadrenie želania jednotlivca, ktorým vyjadrí svoj súhlas so spracovaním osobných údajov, ktoré sa ho týkajú. To potvrdzuje 17. odôvodnenie smernice o súkromí a elektronických komunikáciách: „Súhlas môže byť vyjadrený akýmkoľvek vhodným spôsobom umožňujúcim vyjadrenie špecifického želania, ktoré nastane na základe slobodného a vecného rozhodnutia užívateľa, vrátane označenia poľa na webovej stránke internetu." Ďalej sa uvádzajú praktické príklady toho, čo v tejto súvislosti znamená slobodný, konkrétny a informovaný súhlas.

Súhlas: slobodné, špecifické a informované vyjadrenie želania

54. *Slobodný súhlas*. Na užívateľov by nemali mať vplyv obmedzenia súvisiace so súhlasom s pripojením na internet, ktoré chcú získať.

55. Súhlas jednotlivcov sa nepovažuje za slobodný, ak musia súhlasiť s monitorovaním svojich komunikačných dát, aby získali prístup ku komunikačnej službe. To platí najmä v prípade, ak by *všetci* poskytovatelia na príslušnom trhu vykonávali riadenie dátových tokov na účely presahujúce bezpečnosť siete. Jedinou možnosťou by bolo nepredplatiť si internetovú službu. Vzhľadom na skutočnosť, že

([28]) V 18. odôvodnení smernice sa uvádzajú služby s pridanou hodnotou. Nie je jasné, či sa za také môžu považovať služby, na ktoré sa uplatňujú metódy riadenia dátových tokov. Metódy riadenia dátových tokov zamerané na uprednostnenie určitého obsahu by sa mohli považovať za opatrenia na zabezpečenie kvality služieb. Napríklad riadenie dátových tokov, ktoré zahŕňa len spracovanie IP hlavičiek a ktorého cieľom je poskytnúť služby v oblasti hier za vyššiu cenu, pričom osobná prevádzka hier užívateľa je v sieti uprednostnená, sa môže považovať za službu s pridanou hodnotou. Na druhej strane nie je jasné, či sa za také môže považovať riadenie dátových tokov na spomalenie určitých druhov prevádzky, napríklad zníženie dôležitosti prevádzky P2P.

([29]) Pozri 17. odôvodnenie a článok 2 písm. f) smernice o súkromí a elektronických službách.

([30]) Prijaté 13. júla 2011 (PS 187).

internet je dôležitým nástrojom na účely práce a voľného času, nepredplatenie internetovej služby sa nepovažuje za vhodnú alternatívu. Výsledkom by bolo, že jednotlivci by nemali skutočnú voľbu, t. j. ich súhlas by nebol slobodný ([31]).

56. Európsky dozorný úradník pre ochranu údajov sa domnieva, že je zjavne nevyhnutné, aby Komisia a vnútroštátne orgány monitorovali trh, najmä s cieľom uistiť sa, či je tento scenár – t. j. aby poskytovatelia spájali telekomunikačné služby s monitorovaním komunikácie – hlavný. Poskytovatelia by mali bez stanovenia vyšších nákladov jednotlivcom ponúkať alternatívne služby vrátane pripojenia na internet, ktoré nepodlieha riadeniu dátových tokov.

57. *Konkrétny súhlas.* Keďže je nevyhnutné, aby bol súhlas konkrétny, je v tomto prípade potrebné, aby poskytovatelia internetových služieb jasne a zreteľne požiadali o súhlas s monitorovaním prevádzkových a komunikačných dát. V stanovisku pracovnej skupiny zriadenej podľa článku 29 sa uvádza: „Aby bol súhlas konkrétny, musí byť zrozumiteľný: mal by jasne a presne odkazovať na rozsah a následky spracovania údajov. Nemôže sa uplatniť na otvorený súbor činností spracovania. Inými slovami to znamená, že kontext, v ktorom sa súhlas uplatňuje, je obmedzený.“ Konkrétny súhlas sa pravdepodobne nezíska, ak sa súhlas na prezeranie prevádzkových a komunikačných dát pevne spája so všeobecným súhlasom na predplatenie služby. Naopak, konkrétnosť vyžaduje použitie cielených prostriedkov na získanie súhlasu, ako napríklad formulára na konkrétny súhlas alebo osobitného políčka, ktoré je jasne vymedzené na účel monitorovania (a nie vložiť informáciu do všeobecných zmluvných podmienok a žiadať súhlas so zmluvou ako celkom).

58. *Informovaný súhlas.* Aby bol súhlas platný, musí byť informovaný. Nevyhnutnosť vopred poskytnúť primerané informácie vyplýva nielen zo smernice o súkromí a elektronických komunikáciách a smernice o ochrane údajov, ale takisto z článkov 20 a 21 smernice univerzálnej služby, zmenenej a doplnenej smernicou 2009/136/ES ([32]). Nevyhnutnosť informovanosti a súhlasu výslovne potvrdzuje 28. odôvodnenie smernice 2009/136/ES: „prevádzkovateľ siete a/alebo služby (by) mal v každom prípade plne informovať užívateľov o všetkých obmedzeniach súvisiacich s využívaním elektronických komunikačných služieb. Takéto informácie by mali na základe voľby poskytovateľa špecifikovať daný typ obsahu, aplikácie alebo služby, individuálne aplikácie alebo služby, alebo oboje“. Ďalej špecifikuje, že: „V závislosti od použitej technológie a typu obmedzení môžu takéto obmedzenia vyžadovať súhlas užívateľa v súlade so smernicou 2002/58/ES.“

59. Vzhľadom na zložitosť týchto monitorovacích metód je včasné poskytnutie zmysluplných informácií jednou z hlavných úloh súvisiacich so získaním platného súhlasu. Spotrebitelia by mali byť informovaní tak, aby rozumeli informáciám, ktoré sa budú spracúvať, ako sa budú tieto informácie používať a aký vplyv budú mať na skúsenosti spotrebiteľa a úroveň zasahovania do súkromia, ktorá sa spája s uvedenými metódami.

60. To znamená, že informácie musia byť nielen jasné a zrozumiteľné priemerným užívateľom, ale takisto sa musia poskytovať jednotlivcom priamo a viditeľne, aby nebolo možné si ich nevšimnúť.

61. *Vyjadrenie vôle.* Súhlas podľa platného právneho rámca takisto vyžaduje pozitívne konanie užívateľa v záujme podpísania dohody. Naznačený súhlas by nespĺňal túto normu. To takisto potvrdzuje nevyhnutnosť používať určené prostriedky na získanie súhlasu, na základe ktorého môže poskytovateľ internetových služieb prezerať prevádzkové a komunikačné dáta v súvislosti s uplatňovaním metód riadenia dátových tokov. Pracovná skupina zriadená podľa článku 29 vo svojom najnovšom stanovisku zdôraznila, že pri získavaní súhlasu je nevyhnutná podrobnosť vzhľadom na rôzne prvky, ktoré sú podstatou spracovania údajov.

([31]) Podobný prípad je osobný záznam o cestujúcom, v súvislosti s ktorým sa diskutovalo o otázke, či je súhlas cestujúcich na prenos informácií o rezervácii orgánom Spojených štátov platný. Pracovná skupina sa domnieva, že súhlas cestujúcich nemôže byť slobodný, keďže letecké spoločnosti sú povinné poslať údaje pred odletom lietadla, a preto cestujúci nemajú skutočnú voľbu, ak chcú letieť; stanovisko č. 6/2002 pracovnej skupiny zriadenej podľa článku 29 o prenose zoznamu informácií o cestujúcich a iných údajov z leteckých spoločností Spojeným štátom.

([32]) Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (pozri poznámku 15).

62. Mohlo by sa namietať, že ak si strany zúčastnené na komunikácii neželajú, aby poskytovatelia internetových služieb narúšali komunikáciu s cieľom uplatňovať metódy riadenia dátových tokov, môžu správu zakódovať. Tento prístup môže byť užitočný v praxi, vyžaduje však úsilie a technické znalosti a nemôže sa považovať za slobodný, konkrétny a informovaný súhlas. Ani použitie kódovania nezaručí úplnú dôvernosť správy, keďže poskytovateľ internetových služieb bude mať prístup aspoň k IP hlavičke s cieľom smerovať správu, a takisto bude môcť uplatniť štatistickú analýzu.

63. Podľa článku 5 ods. 1 smernice o súkromí a elektronických komunikáciách je nevyhnutný súhlas príslušných užívateľov. V mnohých prípadoch je užívateľ aj účastníkom, a to umožňuje získať súhlas pri predplatení telekomunikačnej služby. V ostatných prípadoch vrátane prípadov, keď sa to týka viacerých osôb, je potrebné získať súhlas dotknutých užívateľov jednotlivo. To sa môže spájať s praktickými otázkami, ktoré sú predmetom ďalšej časti.

Súhlas všetkých dotknutých užívateľov

64. V článku 5 ods. 1 sa stanovuje, že na legitímnosť spracovania je potrebný súhlas užívateľa. Súhlas musia poskytnúť *všetci užívatelia* zúčastnení na komunikácii. Logickým odôvodnením je, že na komunikácii sa spravidla zúčastňujú minimálne dvaja jednotlivci (odosielateľ a príjemca). Napríklad ak poskytovateľ internetových služieb prezerá IP užívateľské dáta, ktoré zodpovedajú e-mailu, prezerá informácie, ktoré sa týkajú odosielateľa aj príjemcu e-mailu.

65. Pri monitorovaní a zachytávaní dátových tokov a komunikácií (napríklad dátových tokov v rámci internetu) môže byť dostačujúce, že poskytovateľ internetových služieb získa súhlas užívateľa, to znamená účastníka, a to preto, lebo druhá strana komunikácie, v tomto prípade navštívená webová stránka, sa nemôže považovať za „dotknutého užívateľa“ ([33]). Situácia však môže byť zložitejšia, keď monitorovanie zahŕňa prezeranie obsahu e-mailov, teda osobných informácií odosielateľa a príjemcu e-mailu, ktorí možno neuzatvorili zmluvný vzťah s tým istým poskytovateľom internetových služieb. V týchto prípadoch by poskytovateľ internetových služieb spracúval osobné údaje (meno, e-mailovú adresu a prípadné citlivé obsahové dáta) subjektov, ktoré nie sú klientmi. Z praktického hľadiska môže byť získanie súhlasu od týchto jednotlivcov problematickejšie, lebo by sa malo vykonať individuálne a nie pri príležitosti uzatvorenia telekomunikačnej služby. Takisto by nebolo reálne predpokladať, že účastník poskytne súhlas aj v mene ostatných užívateľov, ako to môže byť často v prípade súkromných domácností.

66. V tejto súvislosti sa európsky dozorný úradník pre ochranu údajov domnieva, že poskytovatelia internetových služieb by mali dodržiavať existujúce právne požiadavky a vykonávať opatrenia, ktoré nezahŕňajú monitorovanie a prezeranie informácií. To má ešte väčší význam v súvislosti s komunikačnými službami, na ktorých sa zúčastňujú tretie subjekty, ktoré nemôžu súhlasiť s monitorovaním, najmä pokiaľ ide o odoslané a prijaté e-maily (to sa netýka prípadu, keď sa účel zakladá na zaručení bezpečnosti).

67. Zároveň je potrebné uviesť, že vnútroštátne právne predpisy, ktorými sa vykonáva článok 5 ods. 1 smernice o súkromí a elektronických komunikáciách, nemusia byť v tejto otázke vždy uspokojivé a že vo všeobecnosti sa zdá, že je nevyhnutné lepšie usmernenie, pokiaľ ide o požiadavky smernice o súkromí a elektronických komunikáciách v tejto súvislosti. Európsky dozorný úradník pre ochranu údajov preto vyzýva Komisiu, aby bola v tejto súvislosti aktívnejšia a ujala sa iniciatívy, v rámci ktorej môže využiť výhody vyplývajúce z činnosti orgánov dohľadu sústredených v pracovnej skupine zriadenej podľa článku 29 a ostatných zúčastnených strán. Ak to bude nevyhnutné, prípadom by sa mal zaoberať Súdny dvor s cieľom úplne spresniť význam a následky článku 5 ods. 1.

([33]) Bez ohľadu na prípady, keď dátové toky na internete zahŕňajú prenos osobných informácií, ako napríklad fotografií identifikovateľných fyzických osôb umiestnených na webovej stránke. Spracovanie uvedených informácií vyžaduje právny základ, neuplatňuje sa naň však článok 5 ods. 1, keďže príslušné osoby nie sú „dotknutí užívatelia“.

V.3. **Primeranosť – zásada minimalizácie údajov**

68. V článku 6 písm. c) smernice o ochrane údajov sa stanovuje zásada primeranosti ([34]), ktorá sa uplatňuje na poskytovateľov internetových služieb, keďže, ak vykonávajú monitorovanie a filtrovanie, sú prevádzkovateľmi údajov v zmysle tejto smernice.

69. Podľa tejto zásady sa osobné údaje môžu spracúvať, iba pokiaľ sú „adekvátne, relevantné a nie neprimerané vo vzťahu k účelom, pre ktoré sú zhromažďované a/alebo ďalej spracované". Uplatňovanie tejto zásady sa spája s nevyhnutnosťou posúdiť, či prostriedky použité na spracovanie údajov a druh použitých osobných údajov sú vhodné na splnenie určených cieľov a či sa to odôvodnene predpokladá. Ak sa nakoniec konštatuje, že sa zhromaždilo viac údajov, ako je nevyhnutné, táto zásada sa nedodržala.

70. Súlad niektorých druhov metód prezerania so zásadou primeranosti sa musí posúdiť v každom jednotlivom prípade. Nie je možné dospieť k rozhodnutiu *in abstracto*. Je však možné poukázať na niektoré konkrétne aspekty, ktoré je potrebné určiť pri posúdení súladu so zásadou primeranosti.

71. *Množstvo spracovaných informácií*. Dohľad nad správami zákazníkov poskytovateľov internetových služieb na najhlbšej možnej úrovni bude vo väčšine prípadov nadmerný a protizákonný. Skutočnosť, že na jeho vykonávanie sa môžu používať prostriedky, ktoré pre jednotlivcov nie sú zjavné, a že pre nich môže byť problematické rozumieť tomu, čo sa deje, zvyšuje vplyv na ich súkromie. Poskytovatelia internetových služieb by mali posúdiť, ktoré menej rušivé prostriedky môžu byť dostupné na dosiahnutie požadovaného výsledku. Napríklad môže sa požadovaný výsledok dosiahnuť monitorovaním hlavičiek IP namiesto dôkladného prezerania paketu? Aj keď sa použije dôkladné prezeranie paketu, potrebné informácie sa môžu získať prostredníctvom identifikácie iba určitých protokolov. Takisto môže byť dôležité uplatňovanie opatrení na zaručenie bezpečnosti údajov vrátane pseudoanonymizácie. Výsledok posúdenia musí potvrdiť, že spracovanie údajov je primerané.

72. *Vplyv spracovania (priamo spojeného s účelmi)*. Primeranosť môže chýbať v prípadoch, keď poskytovatelia internetových služieb používajú metódy riadenia dátových tokov, ktoré vylučujú prístup k niektorým službám a neumožňujú užívateľom získať primeraný podiel na výhodách z toho vyplývajúcich.

73. Je dôležité pripomenúť, že zásada primeranosti sa ďalej uplatňuje, aj keď sú splnené ostatné záväzné právne požiadavky vrátane napríklad súhlasu na monitorovanie obsahu, ktorý poskytovateľ internetových služieb získal od jednotlivcov. To znamená, že spracovanie údajov, vykonávané prostredníctvom monitorovania obsahu môže byť protizákonné, ak porušuje základnú zásadu primeranosti.

V.4. **Bezpečnostné a organizačné opatrenia**

74. V článku 4 smernice o súkromí a elektronických komunikáciách sa výslovne stanovuje poskytovateľom internetových služieb povinnosť vykonávať technické a organizačné opatrenia s cieľom zabezpečiť i) prístup k osobným údajom iba oprávneným zamestnancom a na zákonom povolené účely; ii) ochranu osobných údajov pred náhodným alebo nezákonným spracovaním a iii) vykonávanie bezpečnostnej politiky vo vzťahu k spracovaniu osobných údajov. Takisto umožňuje príslušným národným regulačným orgánom kontrolovať tieto opatrenia.

75. Okrem toho sa v článku 4 ods. 3 a 2 smernice o súkromí a elektronických komunikáciách takisto stanovuje poskytovateľom internetových služieb povinnosť oznámiť príslušným národným orgánom porušenie ochrany osobných údajov a takisto oznámiť porušenie osobných údajov dotknutým jednotlivom v prípade, že vyzradenie môže mať pre jednotlivcov nepriaznivé následky.

76. Spracovanie osobných informácií, ktoré sú súčasťou správ, s cieľom uplatňovať metódy riadenia dátových tokov môže poskytnúť poskytovateľom internetových služieb prístup k údajom, ktoré sú citlivejšie ako prevádzkové dáta.

([34]) Ako sa uvádza predtým v texte, smernica o ochrane údajov sa uplatňuje na všetky záležitosti týkajúce sa ochrany základných práv a slobôd, ktoré nie sú osobitne predmetom smernice o súkromí a elektronických komunikáciách.

77. Preto by mali bezpečnostné opatrenia vytvorené poskytovateľmi internetových služieb obsahovať osobitné bezpečnostné opatrenia, ktoré zabezpečia, že prijaté opatrenia sú primerané týmto rizikám. Zároveň je potrebné, aby príslušné vnútroštátne orgány, ktoré kontrolujú uvedené opatrenia, boli mimoriadne náročné. Nakoniec je potrebné zabezpečiť zavedenie účinných oznamovacích postupov s cieľom informovať dotknuté osoby, ktorých informácie sú ohrozené a na ktoré to môže mať nepriaznivý vplyv.

VI. **NÁVRHY POLITICKÝCH A LEGISLATÍVNYCH OPATRENÍ**

78. Metódy prezerania založené na prevádzkových dátach a prezeraní užívateľských IP dát, t. j. obsahu správ, môžu odhaliť činnosť užívateľa na internete: navštívené webové stránky a činnosti na týchto stránkach, používanie aplikácií P2P, prijaté súbory, odoslané a prijaté e-maily, od koho, o čom a v akej funkcii atď. Poskytovatelia internetových služieb môžu mať záujem o použitie týchto informácií s cieľom uprednostniť niektoré komunikácie, ako napríklad video na požiadanie. Takisto môžu mať záujem o ich použitie s cieľom identifikovať vírusy alebo vytvoriť profily na účely behaviorálnej reklamy. Tieto činnosti sú v rozpore s právom na dôvernosť komunikácií.

79. Vplyv na súkromie sa bude zvyšovať v závislosti od použitých metód a osobitostí prípadu. Čím hlbšie je zachytávanie a analýza zhromaždených informácií, tým väčší je rozpor so zásadou dôvernosti komunikácií. Účely, na ktoré sa monitorovanie vykonáva, a uplatňované bezpečnostné opatrenia na ochranu údajov sú takisto hlavnými prvkami na určenie úrovne zasahovania do súkromia a osobných údajov jednotlivcov. Blokovanie a monitorovanie na účely boja proti škodlivému softvéru, pričom uchovávanie a používanie prezeraných údajov je prísne obmedzené, nie je možné porovnávať so situáciami, keď sa informácie zaznamenávajú na vytvorenie individuálnych profilov na účely behaviorálnej reklamy.

80. Európsky dozorný úradník pre ochranu údajov sa v zásade domnieva, že existujúci európsky rámec pre ochranu súkromia a údajov, ak sa správne vykladá, uplatňuje a presadzuje, je primeraný na zaručenie, že sa presadí právo na dôvernosť a vo všeobecnosti že sa neohrozí ochrana súkromia a údajov jednotlivcov ([35]). Poskytovatelia internetových služieb by nemali používať uvedené mechanizmy, pokiaľ primerane neuplatňujú právny rámec. Presnejšie, príslušné prvky rámca, ktoré by mali poskytovatelia internetových služieb brať do úvahy a dodržiavať, zahŕňajú:

— Poskytovatelia internetových služieb môžu uplatňovať metódy riadenia dátových tokov na účely zaručenia bezpečnosti služby, poskytnutia služby vrátane obmedzenia preťaženia siete podľa článku 4 a 6 smernice o súkromí a elektronických službách.

— Poskytovatelia internetových služieb potrebujú iný osobitný právny základ a prípadne súhlas užívateľa s cieľom uplatňovať metódy riadenia dátových tokov, ktoré zahŕňajú spracovanie prevádzkových a/alebo komunikačných dát na účely iné ako sa uvádzajú vyššie texte. Napríklad na monitorovanie a filtrovanie komunikácií jednotlivcov na účely obmedzenia (alebo umožnenia) prístupu k niektorým aplikáciám a službám, ako napríklad P2P alebo prenos hlasu cez IP, je nevyhnutný informovaný súhlas užívateľa.

— Súhlas musí byť slobodný, výslovný a informovaný. Mal by sa vyjadriť prostredníctvom pozitívnej činnosti. Tieto požiadavky kladú silný dôraz na nevyhnutnosť zvýšiť úsilie s cieľom zabezpečiť primerané informovanie jednotlivcov priamym, zrozumiteľným a konkrétnym spôsobom, na základe ktorého budú môcť posúdiť následky postupov a nakoniec prijať informované rozhodnutie. Vzhľadom na zložitosť týchto metód je poskytnutie predchádzajúcich zmysluplných informácií užívateľom jednou z hlavných úloh s cieľom získať platný súhlas. Okrem toho by nemal existovať nijaký nepriaznivý vplyv (vrátane finančných nákladov) na užívateľov, ktorí nesúhlasia so žiadnym monitorovaním.

([35]) A to bez toho, aby bola dotknutá nevyhnutnosť zmien právnych predpisov na základe ostatných úvah, najmä v súvislosti so všeobecnou revíziou právneho rámca EÚ pre ochranu údajov s cieľom zabezpečiť jeho väčšiu účinnosť vzhľadom na nové technológie a globalizáciu.

— Zásada primeranosti hrá hlavnú úlohu, keď poskytovatelia internetových služieb uplatňujú metódy riadenia dátových tokov, bez ohľadu na právny základ spracovania a účel: poskytnutie služby, predchádzanie preťaženiu siete alebo poskytnutie cieleného pripojenia s prípadným prístupom k určitým službám a aplikáciám. Táto zásada obmedzuje možnosť poskytovateľov internetových služieb vykonávať monitorovanie obsahu správ jednotlivcov, ktoré sa spája so spracovaním nadmerných informácií alebo vznikom výhod len pre poskytovateľov internetových služieb. To, čo môžu poskytovatelia internetových služieb vykonať z organizačného hľadiska, bude závisieť od úrovne zasahovania metód, požadovaných výsledkov (v súvislosti s ktorými môžu vyplývať výhody) a uplatňovaných osobitných bezpečnostných opatrení na ochranu súkromia a údajov. Skôr ako poskytovatelia internetových služieb použijú metódy prezerania, musia posúdiť, či sú v súlade so zásadou primeranosti.

81. Aj keď v súčasnosti právny rámec obsahuje príslušné podmienky a bezpečnostné opatrenia, je nevyhnutné venovať osobitnú pozornosť otázkam, či poskytovatelia internetových služieb účinne dodržiavajú právne požiadavky, či spotrebiteľom poskytujú nevyhnutné informácie, aby sa mohli zmysluplne rozhodnúť, a či dodržiavajú zásadu primeranosti. Na vnútroštátnej úrovni orgány zodpovedné za uvedené skutočnosti zahŕňajú na jednej strane vnútroštátne telekomunikačné orgány a na strane druhej vnútroštátne orgány pre ochranu údajov. Na úrovni EÚ príslušné európske orgány zahŕňajú orgán BEREC. V tejto súvislosti môže takisto hrať úlohu európsky dozorný úradník pre ochranu údajov.

82. Okrem monitorovania úrovne dodržiavania, vzhľadom na novú možnosť podstatného prezerania správ v reálnom čase, je nevyhnutná dôkladnejšia analýza a ďalšie spresnenie niektorých aspektov týkajúcich sa uplatňovania rámca, ktorými sa zaoberá toto stanovisko. Usmernenie, ktoré je dôležité najmä v niektorých oblastiach, zahŕňa:

— určenie postupov prezerania, ktoré sú zákonom oprávnené na zabezpečenie plynulého toku prevádzkových dát a ktoré nevyžadujú súhlas užívateľa, ako napríklad boj proti nevyžiadanej pošte. Okrem úrovne narušenia prostredníctvom monitorovania sú dôležité ďalšie aspekty, ako napríklad úroveň narušenia plynulého toku prevádzkových dát, ktoré by sa inak vyskytlo,

— určenie metód prezerania, ktoré sa môžu vykonávať na účely bezpečnosti bez potrebného súhlasu užívateľa,

— určenie, kedy monitorovanie vyžaduje súhlas jednotlivcov, najmä všetkých dotknutých užívateľov, a stanovenie prípustných technických parametrov s cieľom zabezpečiť, aby metódy prezerania nezahŕňali neprimerané spracovanie údajov vzhľadom na plánovaný účel,

— okrem toho v troch uvedených prípadoch môže byť nevyhnutné usmernenie týkajúce sa uplatňovania nevyhnutných bezpečnostných opatrení na ochranu údajov (obmedzenie účelu, bezpečnosť atď.).

83. Vzhľadom na skutočnosť, že právomoci v tejto oblasti sú vnútroštátne aj európske, európsky dozorný úradník pre ochranu údajov sa domnieva, že je dôležitá výmena názorov a skúseností s cieľom nájsť harmonizovaný prístup k uvedeným otázkam. V záujme dosiahnutia tohto cieľa európsky dozorný úradník pre ochranu údajov navrhuje vytvoriť platformu alebo expertnú skupinu, v ktorej by mali pracovať zástupcovia vnútroštátnych regulačných orgánov, pracovnej skupiny zriadenej podľa článku 29, európsky dozorný úradník pre ochranu údajov a BEREC. Prvou úlohou tejto platformy by bolo vytvoriť usmernenie týkajúce sa aspoň uvedených otázok s cieľom zabezpečiť pevný a harmonizovaný prístup a rovnaké podmienky. Európsky dozorný úradník pre ochranu údajov vyzýva Komisiu, aby sa ujala tejto iniciatívy.

84. V neposlednom rade je nevyhnutné, aby vnútroštátne aj európske orgány v tejto oblasti vrátane BEREC a Európskej komisie venovali dôkladnú pozornosť vývoju trhu v tejto oblasti. Z hľadiska ochrany údajov a súkromia by bol veľmi problematický scenár, v rámci ktorého by poskytovatelia internetových služieb pravidelne uplatňovali metódy riadenia dátových tokov, pričom by ponúkali pripojenie založené na filtrovaní prístupu k obsahu a aplikáciám. Ak by sa niekedy tento scenár uskutočnil, bolo by nevyhnutné zaviesť právne predpisy na riešenie tejto situácie.

VII. **ZÁVERY**

85. Čoraz častejšie má používanie metód monitorovania a prezerania zo strany poskytovateľov internetových služieb vplyv na neutralitu internetu a dôvernosť komunikácií. S tým súvisia vážne otázky týkajúce sa ochrany súkromia a osobných údajov užívateľov.

86. Aj keď sa Komisia vo svojom oznámení o otvorenom internete a neutralite siete v Európe stručne zaoberá týmito otázkami, európsky dozorný úradník pre ochranu údajov sa domnieva, že je potrebné väčšie úsilie na vytvorenie uspokojivej politiky na ceste vpred. V tomto stanovisku preto prispel k prebiehajúcej diskusii o neutralite siete, najmä o aspektoch týkajúcich sa ochrany údajov a súkromia.

87. Európsky dozorný úradník pre ochranu údajov sa domnieva, že je nevyhnutné, aby vnútroštátne orgány a BEREC monitorovali situáciu na trhu. Výsledkom tohto monitorovania by mal byť jasný obraz toho, či sa trh vyvíja k podstatnému prezeraniu správ v reálnom čase a otázkam týkajúcim sa dodržiavania právneho rámca.

88. Monitorovanie trhu by sa malo spájať s ďalšou analýzou vplyvu nových postupov týkajúcich sa ochrany údajov a súkromia na internet. V tomto stanovisku sa uvádzajú niektoré oblasti, pre ktoré bude spresnenie užitočné. Aj keby európske agentúry a orgány ako BEREC, pracovná skupina zriadená podľa článku 29 a európsky dozorný úradník pre ochranu údajov prípadne mohli spresniť podmienky uplatňovania rámca, európsky dozorný úradník pre ochranu údajov sa domnieva, že je úlohou Komisie koordinovať a riadiť diskusiu. Preto vyzýva Komisiu, aby sa na tento účel ujala iniciatívy, ktorá zoskupí všetky zainteresované strany do platformy alebo pracovnej skupiny. V rámci otázok, ktoré budú vyžadovať ďalšiu analýzu, by sa mali riešiť tieto body:

— určenie metód prezerania, ktoré sú zákonom odôvodnené na zabezpečenie plynulého toku prevádzkových dát a ktoré sa môžu vykonávať na bezpečnostné účely,

— určenie, či monitorovanie vyžaduje súhlas jednotlivca, najmä súhlas všetkých dotknutých užívateľov, a stanovenie prípustných technických parametrov s cieľom zabezpečiť, aby metódy prezerania nezahŕňali neprimerané spracovanie údajov vzhľadom na plánovaný účel,

— v uvedených prípadoch môže byť potrebné usmernenie týkajúce sa uplatňovania nevyhnutných bezpečnostných opatrení na ochranu údajov (obmedzenie účelu, bezpečnosť atď.).

89. V závislosti od uvedených zistení môžu byť nevyhnutné dodatočné legislatívne opatrenia. V takom prípade by mala Komisia navrhnúť politické opatrenia zamerané na posilnenie právneho rámca a zabezpečenie právnej istoty. Nové opatrenia by mali spresniť praktický vplyv zásady neutrality siete, ako to už vykonali niektoré členské štáty, a zaručiť pre užívateľov možnosť skutočnej voľby, najmä prostredníctvom zabezpečenia, že poskytovatelia internetových služieb budú ponúkať nemonitorované pripojenia.

V Bruseli 7. októbra 2011

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov