I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannenom nätneutralitet, trafikstyrning och integritetsskydd och skydd av personuppgifter

(2012/C 34/01)

EUROPEISKA DATATILLSYNSMANNEN HAR AVGETT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 och 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]),

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter ([2]), särskilt artikel 41.2, och

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation ([3]).

HÄRIGENOM FRAMFÖRS FÖLJANDE

I. INLEDNING

I.1 Bakgrund

1. Den 19 april 2011 antog kommissionen meddelandet *Ett öppet internet och nätneutralitet i Europa* ([4]).

2. Det här yttrandet kan ses som datatillsynsmannens reaktion på detta meddelande och syftar till att bidra till den pågående politiska debatten inom EU om nätneutralitet, särskilt i fråga om dataskydd och integritet.

([1]) EGT L 281, 23.11.1995, s. 31, dataskyddsdirektivet.
([2]) EGT L 8, 12.1.2001, s. 1, dataskyddsförordningen.
([3]) EGT L 201, 31.7.2002, s. 37, ändrat genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (se fotnot 15), direktivet om integritet och elektronisk kommunikation.
([4]) KOM(2011) 222 slutlig.

3. Yttrandet utgår från datatillsynsmannens svar ([5]) på kommissionens offentliga samråd om ett öppet internet och nätneutralitet i Europa, som föregick kommissionens meddelande. Datatillsynsmannen har också tagit del av det färska utkastet till rådets slutsatser om nätneutralitet ([6]).

I.2 **Begreppet nätneutralitet**

4. Begreppet nätneutralitet hänvisar till en pågående diskussion om huruvida internetleverantörer ([7]) ska få begränsa, filtrera eller blockera internetanslutningar eller på annat sätt påverka deras prestanda. Begreppet nätneutralitet bygger på tanken att informationen på internet ska förmedlas opartiskt utan hänsyn till innehåll, destination eller källa och att användare ska få bestämma vilka tillämpningar, tjänster och maskinvara de vill använda. Detta betyder att internetleverantörer inte själva får välja, prioritera eller sänka åtkomsthastigheten för vissa tillämpningar eller tjänster, som t.ex. fildelning (*Peer to Peer*, P2P) ([8]).

5. Filtrering, blockering och kontroll av nättrafik ger upphov till viktiga frågor som ofta förbises eller kringgås i fråga om kommunikationens konfidentialitet och respekten för enskildas integritet och personuppgifter när de använder internet. Vissa kontrolltekniker innebär t.ex. övervakning av innehållet i kommunikationerna, besökta webbplatser, skickade och mottagna e-postmeddelanden, tidpunkt för utbytet osv., för att göra det möjligt att filtrera kommunikationen.

6. Vid sin kontroll av kommunikationsuppgifter kan internetleverantörer bryta mot konfidentialiteten i kommunikationen, som är en grundläggande rättighet enligt artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (*Europakonventionen*) och artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*). Konfidentialiteten skyddas dessutom i EU:s sekundärlagstiftning genom artikel 5 i direktivet om integritet och elektronisk kommunikation.

I.3 **Yttrandets inriktning och struktur**

7. Datatillsynsmannen anser att en seriös politisk diskussion om nätneutralitet måste gå in på konfidentialiteten vid kommunikation såväl som andra konsekvenser för integritets- och uppgiftsskydd.

8. Detta yttrande är ett bidrag till denna pågående diskussion inom EU. Yttrandet har tre mål:

— Att lyfta fram vikten av integritets- och uppgiftsskydd i de pågående diskussionerna om nätneutralitet, särskilt behovet av att följa de befintliga bestämmelserna om konfidentialitet vid kommunikation. Endast metoder som respekterar dessa bestämmelser bör vara tillåtna.

— Nätneutralitet berör förhållandevis nya – tekniska – möjligheter och det saknas erfarenhet av hur den rättsliga ramen ska tillämpas. Därför innehåller detta yttrande riktlinjer för hur internetleverantörer måste tillämpa och följa den rättsliga ramen för uppgiftsskydd om de filtrerar, blockerar och kontrollerar nättrafik. Detta bör underlätta för internetleverantörerna och även för de myndigheter som ansvarar för att verkställa reglerna.

— Inom ramen för integritets- och uppgiftsskydd identifieras de områden som kräver särskild uppmärksamhet och där det kan behövas åtgärder på EU-nivå. Detta är särskilt viktigt med hänsyn till den pågående diskussionen på EU-nivå och de politiska åtgärder som kommissionen kan vidta i sammanhanget.

([5]) Datatillsynsmannen svarade med att framhålla vikten av att ta hänsyn till uppgifts- och integritetsskyddsfrågor tillsammans med andra befintliga rättigheter och värderingar. Svaret finns på http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Finns på http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Detta innefattar tillhandahållandet av både fast och mobil tillgång till internet.

([8]) Principen gäller dock inte internetleverantörers begränsning av hastighet eller mängd information som en abonnent kan skicka eller ta emot genom abonnemang med begränsningar för volym eller bandbredd. Enligt principen om nätneutralitet skulle internetleverantörer alltså fortfarande kunna erbjuda internetabonnemang med begränsningar utifrån kriterier som hastighet eller volym så länge detta inte innebär diskriminering av något särskilt innehåll.

9. Datatillsynsmannen är medveten om att nätneutralitet ger upphov till andra frågor som beskrivs närmare nedan, t.ex. i fråga om tillgång till information. Dessa frågor behandlas bara i den mån de är relevanta för eller inverkar på integritets- och uppgiftsskyddet.

10. Yttrandet är uppbyggt på följande sätt: Avsnitt II inleds med en kort överblick över internetleverantörers praxis i fråga om filtrering. I avsnitt III sammanfattas EU:s rättsliga ram för nätneutralitet. Därefter ges en teknisk beskrivning i avsnitt IV, följd av en bedömning av konsekvenserna för integriteten, beroende på vilken teknik som används. Avsnitt V innehåller en analys av de praktiska detaljerna för tillämpningen av EU:s nuvarande regelverk för integritets- och uppgiftsskydd. Avsnitt VI innehåller förslag till politisk utveckling och en beskrivning av de områden där det kan krävas förtydliganden och förbättringar av den rättsliga ramen. Avsnitt VII innehåller slutsatserna.

II. **NÄTNEUTRALITET OCH TRAFIKSTYRNINGSPOLITIK**

Ökad användning av trafikstyrningspolitik

11. Traditionellt sett har internetleverantörer endast övervakat och påverkat nättrafiken i begränsad omfattning. Internetleverantörer har t.ex. använt kontrolltekniker och begränsat informationsflöden för att upprätthålla säkerheten i nätet, t.ex. för att bekämpa virus. Generellt sett har internet alltså vuxit och samtidigt bevarat en hög grad av neutralitet.

12. På senare år har dock vissa internetleverantörer visat intresse för att kontrollera nättrafik för att differentiera och tillämpa olika policyer på den för att t.ex. blockera vissa tjänster eller ge förmånligare åtkomst till andra. Detta kallas ibland *trafikstyrningspolitik* ([9]).

13. Internetleverantörerna har många skäl för att kontrollera och differentiera trafiken. Trafikstyrningspolitiken kan t.ex. hjälpa internetleverantörerna att styra trafiken under perioder av hög belastning genom t.ex. prioritera viss tidskänslig trafik som direktuppspelning av video och försämra andra trafikformer som kan vara mindre tidskänsliga, som fildelning ([10]). Trafikstyrning kan också vara ett sätt för internetleverantörerna att skaffa sig en möjlig intäktsström, och denna kan komma från olika källor. Å ena sidan kan internetleverantörerna ta ut avgifter från innehållstjänsteleverantörer, t.ex. vars tjänster kräver större brandbedd, i utbyte mot att ge dem prioritet (och därmed hastighet). Detta skulle innebära att åtkomsten till en viss tjänst, t.ex. en tjänst som erbjuder beställvideo, skulle vara snabbare än åtkomsten till en annan liknande tjänst som inte har anslutit sig till höghastighetsöverföringen. Intäkter kan också komma från abonnenter som vill betala mer (eller mindre) för vissa typer av differentierade abonnemang. Ett abonnemang utan tillgång till fildelning skulle t.ex. kunna vara billigare än ett som ger obegränsad tillgång.

14. Vid sidan av internetleverantörens egna skäl för att använda trafikstyrningspolitik kan även andra parter ha ett intresse av att internetleverantörerna använder en sådan. Om internetleverantörerna styr sina nät och kontrollerar innehåll som passerar deras anläggningar kan de sannolikt öka sin förmåga att upptäcka påstådd olaglig användning, t.ex. brott mot upphovsrättslagen eller pornografisk användning.

([9]) Se till exempel rapporten från OFCOM *Site blocking to reduce online copyright infringement* av den 27 maj 2011. Den finns att ladda ned från http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: ”Vissa internetleverantörer använder redan system för s.k. *deep packet inspection* eller informationsextraktion i sina nät för trafikstyrning och andra syften, varför vi antar att det går att införa även om det skulle vara mycket komplicerat och medföra stora kostnader för dem som inte redan har sådana tjänster. Det är möjligt att endast de större internetleverantörerna skulle kunna använda informationsextraktion på kort till medellång sikt med tanke på de kapitalinvesteringar som krävs”.

([10]) Kvaliteten i realtidstillämpningar, som direktuppspelning av video beror bl.a. på latenstiden, dvs. fördröjningar på grund av t.ex. överbelastning i nätet.

Andra intressen som berörs, däribland uppgiftsskydd och integritet

15. Denna utveckling har väckt debatt om huruvida dessa metoder är legitima och i synnerhet om huruvida särskilda skyldigheter i fråga om nätneutralitet bör fastställas i lag.

16. En ökad användning av trafikstyrningspolitik från internetleverantörernas sida kan begränsa tillgången till information. Om detta beteende blir allmänt utbrett och användare inte kan få tillgång (eller detta blir mycket dyrt) till hela internet, skulle detta hota tillgången till information och användarnas förmåga att skicka och ta emot det innehåll de vill ha med hjälp av de tillgångar eller tjänster som de själva väljer. Med en rättsligt bindande princip om nätneutralitet skulle det kanske gå att undvika detta problem.

17. Här vill datatillsynsmannen ta upp konsekvenserna för uppgiftsskydd och integritet när internetleverantörer använder trafikstyrning. Det gäller i synnerhet följande:

— När internetleverantörer behandlar trafikuppgifter med det enda syftet att dirigera informationsflödet från sändaren till mottagare, utför de i allmänhet endast en begränsad behandling av personuppgifter ([11]). På samma sätt som posten behandlar de uppgifter som står på kuvertet till ett brev, behandlar internetleverantören de uppgifter som krävs för att dirigera kommunikationen till mottagaren. Detta strider inte mot de rättsliga kraven på uppgiftsskydd, integritet och konfidentialitet vid kommunikation.

— När internetleverantörer kontrollerar kommunikationsuppgifter för att skilja ut varje kommunikationsflöde och tillämpa särskilda policyer som kan vara ogynnsamma för enskilda personer, blir konsekvenserna emellertid större. Beroende på omständigheterna i varje fall och på vilken typ av analys som görs kan behandlingen medföra mycket stora intrång i en persons integritet och personuppgifter. Detta blir tydligare när styrningspolitiken avslöjar innehållet i enskilda personers internetkommunikation, som skickade och mottagna e-postmeddelanden, besökta webbplatser, nedladdade eller uppladdade filer osv.

III. ÖVERSIKT ÖVER EU:S RÄTTSLIGA RAM FÖR NÄTNEUTRALITET OCH VIDARE POLITISKA ÅTGÄRDER

III.1 III.1 Den rättsliga ramen i korthet

18. Fram till 2009 innehöll EU-lagstiftningen inga bestämmelser där internetleverantörer uttryckligen förbjöds att använda filtrering eller blockering eller ta ut extra avgifter för att ge abonnenter tillgång till tjänster. Den innehöll inte heller några bestämmelser där dessa metoder uttryckligen erkändes. Läget var alltså i viss mån osäkert.

19. Detta ändrades 2009 genom telekompaketet där det ingick bestämmelser för att främja öppenheten på internet. I artikel 8.4 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) införs t.ex. en skyldighet för regleringsmyndigheterna att främja användarnas förmåga att skaffa sig tillgång till information, tillämpningar och tjänster efter eget val ([12]). Denna bestämmelse gäller för nätet i sin helhet och inte för enskilda leverantörer. I rådets slutsatser nyligen framhölls också behovet av att bevara ett öppet internet ([13]).

([11]) Detta utesluter operationer som syftar till att öka säkerheten i nätet och upptäcka skadlig trafik och även operationer som krävs för fakturering och samtrafik. Det utesluter även skyldigheter som följer av direktivet om lagring av uppgifter, Europaparlamentets och rådets direktiv 2006/24/EC av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, (EUT L 105, 13.4.2006, s. 54).

([12]) Direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, ändrat genom direktiv 2009/140/EG och förordning (EG) nr 544/2009 (EUT L 337, 18.12.2009, s. 37).

([13]) Se punkt 3 e där rådet erkänner behovet av att bevara ett öppet internet och samtidigt se till att det kan fortsätta att tillhandahålla tjänster av hög kvalitet inom en ram som främjar och respekterar grundläggande rättigheter som yttrandefrihet och näringsfrihet och punkt 8 d där rådet uppmanar medlemsstaterna att ha som politiskt mål att främja internets öppna och neutrala karaktär.

20. I direktivet om samhällsomfattande tjänster ([14]) finns mer konkreta skyldigheter. I artiklarna 20 och 21 fastställs krav på öppenhet i fråga om begränsningar av tillgång till och/eller användning av tjänster och tillämpningar. Dessutom ställs krav på nivån för minimitjänstekvalitet.

21. När internetleverantörernas metoder innebär en kontroll av enskilda personers kommunikation betonas det i skäl 28 i direktivet om ändring av direktivet om samhällsomfattande tjänster och direktivet om integritet och elektronisk kommunikation ([15]) att sådana begränsningar kan kräva användarnas samtycke i enlighet med direktivet om integritet och elektronisk kommunikation. I skäl 28 erinras alltså om behovet av samtycke i enlighet med artikel 5.1 i direktivet om integritet och elektronisk kommunikation i fråga om alla begränsningar som bygger på övervakning av kommunikation. I avsnitt IV analyseras tillämpningen av artikel 5.1 och den övergripande rättsliga ramen för uppgiftsskydd och integritet närmare.

22. Slutligen ger artikel 22.3 i direktivet om samhällsomfattande tjänster nationella regleringsmyndigheter möjlighet att vid behov fastställa krav på lägsta tjänstekvalitet hos internetleverantörer för att förebygga försämring av tjänster och förhindrad eller långsam trafik i offentliga nät.

23. Detta innebär att det på EU-nivå finns en stark ambition att bevara ett öppet internet (se artikel 8.4 i ramdirektivet). Detta politiska mål, som gäller för nätet i sin helhet, är dock inte direkt kopplat till förbud eller skyldigheter för enskilda internetleverantörer. En internetleverantör kan med andra ord bedriva en trafikstyrningspolitik som kan utesluta tillgång till vissa tillämpningar, förutsatt att slutanvändarna är fullständigt informerade och har gett sitt frivilliga samtycke, särskilt och otvetydigt.

24. Läget kan variera mellan de olika medlemsstaterna. I vissa medlemsstater kan internetleverantörer under vissa omständigheter använda trafikstyrningspolitik för att t.ex. blockera tillämpningar som IP-telefoni (som del av ett billigare internetabonnemang), förutsatt att enskilda personer har givit sitt frivilliga, särskilda och otvetydiga informerade samtycke till detta. Andra medlemsstater har valt att stärka principen om nätneutralitet. I juli 2011 antog t.ex. det nederländska parlamentet en lag om ett generellt förbud för leverantörer mot att hindra eller sänka hastigheten för tillämpningar eller tjänster på internet (t.ex. IP-telefoni), så länge det inte krävs för att minimera effekterna av överbelastning, av integritets- eller säkerhetsskäl, för att bekämpa skräppost eller enligt ett domstolsbeslut ([16]).

III.2 **Meddelandet om nätneutralitet**

25. I sitt meddelande om nätneutralitet ([17]) konstaterade Europeiska kommissionen att situationen i fråga om nätneutralitet behöver övervakas och analyseras mer ingående. Denna politik handlar om att ”vänta och se” innan nya regleringsåtgärder övervägs.

([14]) Direktiv 2002/22/EG, ändrat genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen (EUT L 337, 18.12.2009, s. 11). Se även artikel 1.3 där det anges att internetleverantörer i direktivet varken föreskrivs eller förbjuds att begränsa användarnas tillgång till och/eller användning av tillämpningar och tjänster, om dessa villkor är tillåtna enligt nationell lagstiftning och stämmer överens med gemenskapsrätten; däremot införs en skyldighet att lämna information om sådana villkor.

([15]) Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen.

([16]) Det ursprungliga nederländska ändringsförslaget finns på https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Enligt medierna fanns det i skälen till detta politiska alternativ inte någon hänvisning till överväganden om integritets- och uppgiftsskydd, utan det handlade om att se till att användare inte hindrades att få, eller erbjöds begränsad, tillgång till information. Det verkar alltså som om frågor i samband med tillgång till information låg bakom ändringsförslaget.

([17]) Se fotnot 4.

26. I kommissionens meddelande anges att alla åtgärder och nya regleringar ska föregås av en djupgående bedömning av aspekterna för uppgiftsskydd och integritet. Även i utkastet till rådets slutsatser noteras de uppgiftsskydds- och integritetsfrågor som berörs ([18]).

27. Den fråga som ska bedömas ur uppgiftsskydds- och integritetsperspektiv är huruvida ”vänta och se”-politiken är tillräcklig. Regelverket för uppgiftsskydd och integritet innehåller visserligen i dagsläget vissa skyddsmekanismer, särskilt genom principen om konfidentialitet vid kommunikation, men det verkar vara nödvändigt med en noggrann övervakning av efterlevnaden och att utfärda riktlinjer för flera aspekter som inte är särskilt tydliga. Dessutom bör det sägas något om hur regelverket kan förtydligas och förbättras ytterligare mot bakgrund av den tekniska utvecklingen. Om övervakningen visar att marknaden utvecklas mot massiv kontroll av kommunikationer i realtid och att det finns problem med efterlevnaden av regelverket, kommer det att krävas lagstiftningsåtgärder. Konkreta förslag i det avseendet kommer att lämnas i avsnitt VI.

IV. **TEKNISK BAKGRUND OCH KONSEKVENSER FÖR INTEGRITETS- OCH UPPGIFTSSKYDD**

28. Innan vi går djupare in i frågan är det viktigt att få en bättre överblick över de kontrolltekniker som internetleverantörer kan använda i sin trafikstyrning och hur detta kan påverka principen om nätneutralitet. Konsekvenserna för integritets- och uppgiftsskyddet av dessa tekniker varierar kraftigt beroende på vilken eller vilka tekniker som används. Denna tekniska bakgrund är nödvändig för att förstå hur det regelverk för uppgiftsskydd som beskrivs i avsnitt V ska tillämpas på korrekt sätt. Det bör dock påpekas att detta område är mycket komplext och ständigt förändras. Den följande beskrivningen är alltså inte avsedd att vara uttömmande och fullständigt aktuell utan endast att ge den tekniska information som krävs för att man ska förstå det rättsliga resonemanget.

IV.1 **Överföring av information via internet: grunderna**

29. När en användare kommunicerar via internet delas den överförda informationen upp i paket. Dessa paket skickas genom internet från avsändaren till mottagaren. Varje paket innehåller bl.a. information om källan och om destinationen. Dessutom kan internetleverantören lägga in dessa paket i ytterligare lager och protokoll ([19]) för att styra de olika trafikflödena i internetleverantörens nät.

30. För att gå tillbaka till analogin med vanliga brev så motsvarar användningen av ett nätöverföringsprotokoll att lägga innehållet i ett brev i ett kuvert med en mottagaradress som ska läsas av en posttjänst och sedan levereras av posttjänsten. Posttjänsten får använda ytterligare protokoll i sin interna hantering för att styra alla kuvert som ska överföras för att se till att varje kuvert kommer fram till den mottagare som sändaren ursprungligen angav. Enligt samma analogi har varje paket två delar: Först *IP-nyttolasten* som omfattar innehållet i kommunikationen och som motsvarar själva brevet. Den innehåller information som enbart är avsedd för mottagaren. Paketets andra del utgörs av *IP-filetiketten* som bl.a. innehåller mottagarens och sändarens adresser. Denna del motsvarar själva kuvertet. IP-filetiketten gör det möjligt för internetleverantörer och andra mellanhänder att dirigera nyttolasten från källadressen till destinationsadressen.

31. Internetleverantörer och andra mellanhänder ser till att IP-paket flyttas i nätet genom noder som läser informationen på IP-filetiketten, kontrollerar den gentemot routertabeller och sedan skickar dem vidare till nästa nod på väg mot destinationen. Denna process sker i nätet med hjälp av en minneslös strategi

([18]) Se punkt 4 e där rådet konstaterar att det finns vissa farhågor, främst hos myndigheter för konsumentskydd och uppgiftsskydd, i fråga skyddet för personuppgifter.

([19]) Som beskrivs närmare i avsnitt IV.2 kodar dessa protokoll den överförda informationen genomgående på ett överenskommet sätt så att de parter som deltar i kommunikationen kan förstå varandra – t.ex. HTTP, FTP osv.

för ”best effort”, eftersom alla paket som kommer till en nod behandlas neutralt. När de har skickats vidare till nästa nod finns inget behov av att lagra ytterligare information i routern ([20]).

IV.2 **Kontrolltekniker**

32. Som visas ovan läser internetleverantörer IP-filetiketter för att dirigera paketen till sin destination. Men som också framgår ovan kan trafikanalysen (av IP-filetiketter och IP-nyttolaster) göras för andra syften och med andra typer av teknik. Nya trender kan t.ex. handla om att göra trafiken långsammare för vissa tillämpningar som användarna använder, t.ex. fildelning, eller höja hastigheten för vissa tjänster som beställvideo för premiumabonnenter. Rent *tekniskt* innebär alla kontrolltekniker en kontroll av paketen, men de innebär olika grad av intrång i integriteten. Det finns två huvudsakliga kategorier av kontrolltekniker. Den ena bygger enbart på IP-filetiketten, den andra omfattar även IP-nyttolasten.

Baserad på informationen i IP-filetiketten. Kontrollen av en IP-filetikett på ett paket visar vissa fält som kan göra det möjligt för internetleverantören att tillämpa ett antal särskilda policyer för att styra trafiken. Dessa tekniker som enbart baseras på IP-filetiketter innebär att uppgifter som i princip är avsedda för routerinformation behandlas i ett annat syfte (t.ex. för att differentiera trafiken). Genom att titta på källans IP-adress kan internetleverantören koppla den till en konkret abonnent och tillämpa en viss politik, t.ex. dirigera paketet genom en snabbare eller långsammare länk. Genom att titta på IP-adressen för destinationen kan internetleverantören också tillämpa en viss politik och t.ex. blockera eller filtrera tillgång till vissa webbplatser.

Baserad på en djupare kontroll. Med *deep packet inspection* kan internetleverantören komma åt information som är avsedd enbart för mottagaren av kommunikationen. Om vi går tillbaka till exemplet med vanliga brev skulle detta vara detsamma som att öppna kuvertet och läsa brevet inuti för att analysera innehållet i kommunikationen (det som finns inuti IP-paketen) för att tillämpa en särskild nätpolitik. Det finns olika sätt att göra denna kontroll och vart och ett av dem innebär olika hot mot den registrerade.

— Deep packet inspection *baserad på analys av protokoll och statistikuppgifter*. Utöver IP-protokollet som ska göra det möjligt att överföra uppgifterna genom internet, finns det andra protokoll som kodar den överförda informationen på ett överenskommet sätt (transport, session, presentation och tillämpning osv.). Målet för dessa protokoll är att se till att de parter som deltar i kommunikationen kan förstå varandra. Det finns t.ex. vissa protokoll som hör ihop med webbläsning ([21]), andra är avsedda för filöverföring ([22]) osv. Kontrolltekniker som är baserade på kontroll av protokoll och kombineras med statistisk analys syftar alltså till att leta efter särskilda mönster eller fingeravtryck som avgör vilka protokoll som används ([23]). Med dessa kontrolltekniker kan internetleverantörerna förstå vilken typ av kommunikation det är fråga om (e-post, webbläsning, uppladdning av filer) och i vissa fall identifiera den specifika tjänst eller tillämpning som används, vilket t.ex. är fallet för vissa former av IP-telefoni där de protokoll som används är mycket specifika för en viss försäljare eller tjänsteleverantör. Kännedomen om kommunikationstypen kan i sig göra det möjligt för internetleverantörer att tillämpa konkret trafikstyrningspolitik och t.ex. blockera webbtrafik. Det kan också vara första steget mot att låta internetleverantören göra ytterligare analyser som kan kräva fullständig tillgång till kommunikationens metadata och innehåll.

([20]) Nätutrustningen för internet använder dock routerprotokoll som loggar aktivitet, behandlar trafikstatistik och utbyter information med annan nätutrustning för att dirigera IP-paket till den mest effektiva vägen. Om en länk t.ex. är överbelastad eller bruten och en router tar emot denna information kommer den att uppdatera sin routertabell med ett alternativ som inte använder den länken. Det är också värt att notera den insamling och behandling som i vissa fall görs för faktureringsändamål eller till och med i enlighet med kraven i direktivet om lagring av uppgifter.
([21]) HTTP — Hypertext transfer protocol — eller HTML — Hypertext Markup Language.
([22]) FTP — File transfer protocol.
([23]) Det finns olika metoder för att identifiera vilka protokoll som används. Det går t.ex. att söka i särskilda fält i de inre protokollen för att t.ex. identifiera vilka portar som används för att upprätta kommunikationen. Det går också att göra en statistik karakterisering av ett kommunikationsflöde genom analysen av vissa specifika fält och korrelera protokoll som används samtidigt mellan två IP-adresser.

— Deep packet inspection *baserad på analys av innehållet i kommunikationen*. Slutligen går det också att kontrollera metadata ([24]) och innehåll i själva kommunikationen. Med denna teknik avlyssnas alla IP-paket som ingår i det ursprungliga kommunikationsflödet så att kommunikationens ursprungliga innehåll kan rekonstrueras och analyseras i sin helhet. För att exempelvis upptäcka skadligt eller olagligt innehåll som virus, barnpornografi osv. måste man rekonstruera innehållet i sig så att det går att analysera. Ibland är kommunikationen genomgående krypterad av de berörda parterna och denna metod kommer att hindra internetleverantörerna från att analysera kommunikationens innehåll.

IV.3 **Konsekvenser för integritets- och uppgiftsskydd**

33. Kontrolltekniker som baseras på IP-filetiketter och i synnerhet dem som baseras på paketkontroll omfattar övervakning och filtrering av dessa uppgifter och har allvarliga konsekvenser i fråga om integritets- och uppgiftsskydd. De kan också stå i konflikt med rätten till konfidentialitet vid kommunikation.

34. Att titta närmare på enskilda personers kommunikationer innebär i sig allvarliga konsekvenser för integritets- och uppgiftsskyddet. Ändå är problemet större än så, eftersom konsekvenserna för integriteten kan bli ännu större, beroende på vilka syften som finns med övervakningen och avlyssningen. Det är inte samma sak att enbart kontrollera kommunikation för att exempelvis se till att systemet fungerar bra som att kontrollera kommunikation i syfte att tillämpa en politik som påverkar enskilda personer. När trafik- och urvalspolitik enbart syftar till att undvika överbelastningar på nätet medför detta oftast inte några större konsekvenser för enskilda personers integritet. Men trafikstyrningspolitiken kan syfta till att blockera viss information om innehåll eller påverka kommunikationen genom t.ex. beteendestyrd reklam. I dessa fall innebär effekterna ett större intrång. Farhågorna blir ännu större om man inser att den här typen av information skulle samlas in, inte bara för en liten grupp av enskilda personer utan på generell basis för alla kunder till internetleverantören ([25]). Om alla internetleverantörer börjar använda filtreringstekniker skulle detta kunna leda till en allmän övervakning av internetanvändningen. Om man dessutom ser på vilken typ av uppgifter som behandlas finns det uppenbart stora risker för integriteten, eftersom en stor del av de uppgifter som samlas in sannolikt är mycket känsliga och efter insamlingen finns tillgängliga för internetleverantörer och för dem som vill hämta information ur dem. Uppgifterna kan dessutom vara mycket värdefulla ur kommersiell synvinkel. Detta innebär i sig stor risk för en funktionsglidning där de ursprungliga syftena lätt kan utvecklas till kommersiell eller annan användning av de insamlade uppgifterna.

35. En korrekt tillämpning av tekniker för övervakning, kontroll och filtrering måste ske i enlighet med gällande mekanismer för integritets- uppgiftsskydd där det fastställs gränser för vad som får göras och under vilka omständigheter. Nedan följer en översikt över gällande skyddsmekanismer enligt EU:s nuvarande rättslig ram för uppgiftsskydd och integritet.

V. **TILLÄMPNING AV EU:S RÄTTSLIGA RAM FÖR INTEGRITETS- OCH UPPGIFTSSKYDD**

36. EU:s ram för uppgiftsskydd är teknikneutral, dvs. den reglerar inte specifika kontrolltekniker, som dem som beskrivs ovan. Direktivet om integritet och elektronisk kommunikation reglerar integriteten i tillhandahållandet av elektroniska kommunikationstjänster i offentliga nät (som internettillgång och

([24]) Varje protokoll har vissa specifika fält i sin filetikett som innehåller ytterligare informell information om den kommunikation som överförs. Innehållet i de fälten kan kallas för kommunikationens metadata. Ett exempel på sådana fält kan vara numret på den port som används. Om det t.ex. är nummer 80 utgörs kommunikationen sannolikt av webbläsning.

([25]) Det är förstås inte bara internetleverantörer som har spårningskapacitet. Även annonseringstjänster kan spåra användare på webbplatser med hjälp kakor från tredje part. Se t.ex. en färsk akademisk artikel som visar att Google är närvarande på 97 av de 100 populäraste webbplatserna, vilket innebär att Google kan spåra användare som inte har valt bort kakor från tredje part när de surfar på dessa populära webbplatser. Se 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 juli 2011). Finns på http://ssrn.com/abstract=1898390. Spårningen av användare med hjälp av kakor från tredje part har tagits upp av artikel 29-arbetsgruppen. Se yttrande nr 2/2010 om beteendestyrd annonsering online som antogs den 22 juni 2010 (WP 171).

telefoni) ([26]) och direktivet om uppgiftsskydd reglerar behandling av uppgifter i allmänhet. Sammantaget fastställs i denna rättsliga ram de olika skyldigheter som gäller för internetleverantörer som behandlar och övervakar trafik och kommunikationsuppgifter.

V.1 **Rättslig grund för behandling av trafik- och innehållsuppgifter**

37. Enligt lagstiftningen om uppgiftsskydd måste det finnas en tillfredsställande rättslig grund för behandlingen av personuppgifter, som i det här fallet med behandling av trafik- och kommunikationsuppgifter. Utöver detta generella krav kan särskilda krav vara tillämpliga i vissa fall.

38. I det här fallet består de personuppgifter som behandlas av internetleverantörer av trafikuppgifter och kommunikationens innehåll. Innehållet i kommunikationen och trafikuppgifterna skyddas båda av rätten till brevhemlighet som garanteras genom artikel 8 i Europakonventionen och artiklarna 7 och 8 i stadgan. I artikel 5.1 i direktivet om integritet och elektronisk kommunikation, med rubriken ”Konfidentialitet vid kommunikation” krävs i synnerhet att medlemsstaterna ska säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Samtidigt anges i artikel 5.1 i direktivet om integritet och elektronisk kommunikation att internetleverantörers behandling av trafik- och innehållsuppgifter får tillåtas under vissa omständigheter, med användarnas samtycke. Detta görs genom ett förbud mot ”avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1”. Detta utvecklas närmare nedan.

39. Utöver samtycke från berörda användare föreskrivs i direktivet om integritet och elektronisk kommunikation andra legitima grunder för internetleverantörers behandling av trafik- och kommunikationsuppgifter. De relevanta rättsliga grunderna för behandling är i detta fall i) leverans av tjänsten, ii) skydd av tjänstens säkerhet, och iii) minimering av överbelastning. Andra möjliga legitima grunder för trafikstyrningspolitik baserad på trafik- eller kommunikationsuppgifter diskuteras nedan i punkt iv).

i) Rättsliga grunder för leverans av tjänsten

40. Som framgår av avsnitt IV behandlar internetleverantörerna informationen i IP-filetiketter i syfte att dirigera varje IP-paket mot dess destination. Enligt artikel 6.1 och 6.2 i direktivet om integritet och elektronisk kommunikation är det tillåtet att behandla trafikuppgifter för att överföra en kommunikation. Internetleverantörer får alltså behandla den information som krävs för att leverera tjänsten.

ii) Rättslig grund för att skydda tjänstens säkerhet

41. Enligt artikel 4 i direktivet om integritet och elektronisk kommunikation har en internetleverantör en generell skyldighet att vidta lämpliga åtgärder för att skydda säkerheten i sina tjänster. Metoden med att filtrera virus kan omfatta behandling av IP-filetiketter och IP-nyttolaster. Med hänsyn till att internetleverantörer enligt artikel 4 i direktivet om integritet och elektronisk kommunikation ska garantera säkerheten i nätet legitimerar denna bestämmelse kontrolltekniker som är baserade på IP-filetiketter och innehåll och som enbart syftar till detta. I praktiken innebär detta att internetleverantörer inom de gränser som följer av proportionalitetsprincipen (se avsnitt V.3) får övervaka och filtrera kommunikationsuppgifter för att bekämpa virus och rent generellt garantera säkerheten i nätet ([27]).

([26]) I skäl 10 i direktivet om integritet och elektronisk kommunikation anges följande: ”Direktiv 95/46/EG är tillämpligt på området för elektronisk kommunikation, i synnerhet beträffande alla de frågor avseende skydd av grundläggande fri- och rättigheter som inte särskilt omfattas av bestämmelserna i det här direktivet, inbegripet den registeransvariges skyldigheter och enskilda personers rättigheter”. Även skäl 17 är relevant i fråga om den registrerades samtycke: ”I detta direktiv bör en användares eller abonnents samtycke, oavsett om den senare är en fysisk eller juridisk person, ha samma betydelse som den registrerades samtycke enligt vad som definieras och i övrigt fastställs i direktiv 95/46/EG”.

([27]) Artikel 29-arbetsgruppens yttrande nr 2/2006 om skydd av personuppgifter i samband med tillhandahållandet av kontroll av innehållet i e-post, antaget den 21 februari 2006 (WP 118). I detta yttrande anser arbetsgruppen att det kan vara förenligt med artikel 5 i direktivet om integritet och elektronisk kommunikation att använda filter för tillämpningen av artikel 4.

iii) Rättslig grund för att minimera effekterna av överbelastning

42. Den logiska grunden för denna rättsliga grund återfinns i skäl 22 i direktivet om integritet och elektronisk kommunikation, där förbudet i artikel 5.1 om lagring av kommunikationer förklaras. Detta förbud innebär inte något förbud mot automatisk, mellanliggande och tillfällig lagring, i den mån lagringen enbart görs för att utföra överföringen och informationen inte lagras längre än vad som är nödvändigt för överföringen och trafikstyrningen och att konfidentialiteten förblir garanterad.

43. Om det finns en överbelastning uppstår frågan om huruvida internetleverantörer slumpvis får sänka hastigheten eller fördröja trafiken eller i stället ska skänka hastigheten för kommunikationer som inte är tidskänsliga, som fildelning eller e-posttrafik och på så sätt göra det möjligt för t.ex. rösttrafik att fungera med acceptabel kvalitet.

44. Med hänsyn till det övergripande samhällsintresset för att garantera ett användbart kommunikationsnät kan internetleverantörer hävda att det är nödvändigt att göra prioriteringar eller strypa trafik för att hantera överbelastningar för att leverera en tillfredsställande tjänst. Detta betyder att det i dessa fall och för detta syfte skulle finnas en generell rättslig grund för att behandla personuppgifter och att det inte skulle behövs något särskilt samtycke från användarna.

45. Samtidigt är möjligheten att ingripa på detta sätt inte obegränsad. Om internetleverantörer behöver kontrollera kommunikationer måste de ur konfidentialitetssynvinkel och med strikt tillämpning av proportionalitetsprincipen använda den minst ingripande metod som finns tillgänglig för att uppnå ändamålet (undvika *deep packet inspection*) och de får endast tillämpa den så länge som krävs för att avhjälpa överbelastningen.

iv) Rättslig grund för behandling av uppgifter för andra ändamål

46. Internetleverantörer kan också vilja kontrollera trafik- och innehållsuppgifter för andra ändamål, t.ex. för att erbjuda målinriktade abonnemang (t.ex. ett abonnemang som begränsar tillgången till fildelning eller ett abonnemang som ökar hastigheten för vissa tillämpningar). Kontroll och ytterligare användning av trafik- och kommunikationsuppgifter för andra syften än att leverera tjänsten eller säkerställa dess säkerhet eller undvika överbelastning är endast tillåten på stränga villkor, i enlighet med den rättsliga ramen.

47. Den rättsliga ramen utgörs främst av artikel 5.1 i direktivet om integritet och elektronisk kommunikation där det krävs samtycke från de berörda användarna för avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder för att fånga upp eller övervaka kommunikationer och tillhörande trafikuppgifter. I praktiken innebär detta att användare som deltar i en kommunikation måste ge sitt samtycke för att legitimera behandling av trafik- och kommunikationsuppgifter i enlighet med artikel 5.1.

48. Som förklaras ovan är tillämpningen av kontroll- och filtreringstekniker antingen baserad antingen på IP-filetiketter, som utgör trafikuppgifter, eller på *deep packet inspection* som även omfattar IP-nyttolaster och utgör kommunikationsuppgifter. Därför skulle i princip tillämpningen av dessa tekniker för andra ändamål än leverans av tjänsten eller säkerhet vara förbjuden såvida inte det finns en legitim grund för behandlingen, exempelvis samtycke (artikel 5.1). Ett exempel där artikel 5.1 skulle vara tillämplig är när en internetleverantör erbjuder kunder en lägre taxa för internettillgång i utbyte mot att de tar emot beteendestyrd reklam och använder *deep packet inspection* och därmed kontroll av kommunikationsuppgifter för att göra detta. Därför krävs ett verkligt, särskilt och informerat samtycke enligt artikel 5.1.

49. Vidare innehåller artikel 6 i direktivet om integritet och elektronisk kommunikation, med rubriken *Trafikuppgifter,* vissa bestämmelser som särskilt gäller trafikuppgifter. I synnerhet förskrivs att

internetleverantörer kan behandla trafikuppgifter på grundval av användarnas samtycke för att tillhandahålla mervärdestjänster ([28]). I denna bestämmelse fastställs det krav på samtycke som anges i artikel 5.1 i fråga om trafikuppgifter.

50. I praktiken är det inte alltid lätt att t.ex. kontrollera i vilka fall det krävs samtycke och i vilka fall nätets säkerhet kan göra behandlingen legitim, särskilt om kontrolltekniken har ett dubbelt syfte (t.ex. undvika överbelastning och tillhandahålla mervärdestjänster). Det bör understrykas att samtycke inte får betraktas som en enkel och systematisk väg att följa principerna om uppgiftsskydd.

51. Det finns liten erfarenhet av tillämpning av regelverket, särskilt när det gäller de olika aspekter som har beskrivits ovan. Detta är ett område där det krävs ytterligare vägledning, vilket utvecklas närmare i avsnitt VI. Dessutom finns det andra relevanta aspekter på samtycke som också måste övervägas. Dessa beskrivs nedan.

V.2 **Frågor om informerat samtycke som rättslig grund**

52. Det samtycke som krävs enligt artiklarna 5 och 6 i direktivet om integritet och elektronisk kommunikation har samma innebörd som den registrerades samtycke och beskrivs närmare i direktiv 95/46/EG ([29]). Enligt artikel 2 h i direktivet om uppgiftsskydd avses med *den registrerades samtycke* ”varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom”. Samtyckets roll och kraven för att det ska vara giltigt har nyligen behandlats av artikel 29-arbetsgruppen i dess yttrande nr 15/2011 om samtycke ([30]).

53. Internetleverantörer som kräver samtycke för kontroll och filtrering av trafikuppgifter och innehållsuppgifter måste alltså se till att samtycket är frivilligt och särskilt och det måste ske i form av en fullständigt informerad viljeyttring genom vilken den enskilda personen godtar behandling av personuppgifter som rör honom. Detta bekräftas i skäl 17 i direktivet om integritet och elektronisk kommunikation: ”(…) Samtycke kan ges i varje lämplig form som gör det möjligt att frivilligt lämna särskilda och informerade uppgifter om användarens önskemål, däribland genom markeringar i en ruta vid besök på en webbplats”. Nedan följer några konkreta exempel på vad det innebär att samtycke är frivilligt, särskilt och informerat.

Samtycke: Frivillig, särskild och informerad viljeyttring

54. *Frivilligt samtycke* Användare bör inte utsättas för begränsningar som där samtycke knyts till det internetabonnemang de vill teckna.

55. Enskilda personers samtycke skulle inte vara frivilligt om de var tvungna att samtycka till övervakning av deras kommunikationsuppgifter för att få tillgång till en kommunikationstjänst. Detta skulle gälla i ännu högre grad om *samtliga* leverantörer på en viss marknad skulle använda trafikstyrningspolitik för andra syften än nätets säkerhet. Det enda återstående alternativet skulle i så fall vara att inte abonnera

([28]) I skäl 18 i direktivet finns en förteckning med exempel på mervärdestjänster. Det är inte klart huruvida tjänster som omfattas av trafikstyrningspolitik kan anses omfattas av den förteckningen. Trafikstyrningspolitik som syftar till att prioritera visst innehåll kan uppfattas som ett tillhandahållande av en kvalitet i tjänsten. Trafikstyrning som exempelvis enbart innebär behandling av IP-filetiketter och vars mål är att erbjuda speltjänster till premiumpris, där användarens personliga speltrafik prioriteras i nätet, kan betraktas som en mervärdestjänst. Å andra sidan är det långt ifrån uppenbart om trafikstyrningspolitik för att strypa vissa typer av trafik, t.ex. försämra fildelningstrafiken, kan betraktas som en sådan.

([29]) Se skäl 17 och artikel 2 f i direktivet om integritet och elektronisk kommunikation.

([30]) Antaget den 13 juli 2011 (WP 187).

på någon internettjänst alls. Eftersom internet har blivit ett nödvändigt verktyg för både arbete och fritid är lösningen att inte abonnera på en internettjänst inte något verkligt alternativ. Resultatet skulle bli att de enskilda personerna inte hade något verkligt val, dvs. de skulle inte kunna ge sitt frivilliga samtycke ([31]).

56. Datatillsynsmannen anser att det finns ett tydligt behov av att kommissionen och de nationella myndigheterna övervakar marknaden, särskilt för att kontrollera om detta scenario – alltså att leverantörer kopplar telekommunikationstjänster till kommunikationsövervakning – blir standardpraxis. Leverantörer bör erbjuda alternativa tjänster, däribland ett internetabonnemang som inte omfattas av trafikstyrningspolitik, utan högre kostnader för enskilda personer.

57. *Särskilt samtycke*. Behovet av att samtycke ska vara särskilt kräver i detta fall att internetleverantörerna begär samtycke till övervakning av trafikuppgifter och kommunikationsuppgifter på ett tydligt och distinkt sätt. Artikel 29-arbetsgruppen anger att ”… för att vara särskilt måste samtycket vara begripligt: uppgiftsbehandlingens omfattning och konsekvenser måste framgå tydligt och exakt. Det får inte gälla en obegränsad uppsättning behandlingsverksamheter. Det sammanhang som samtycket gäller ska med andra ord vara begränsat.” Det är inte sannolikt att särskilt samtycke erhålls om samtycket till kontroll av trafikuppgifter och kommunikationsuppgifter ”buntas ihop” med det övergripande samtycket till att abonnera på tjänsten. Kravet på särskilt samtycke innebär i stället att man använder riktade metoder för att erhålla samtycke, t.ex. genom att användaren får markera en särskild ruta där det tydligt framgår att syftet är övervakning (i stället för att lägga in informationen i de allmänna avtalsvillkoren och begära att avtalet ska undertecknas i befintligt skick).

58. *Informerat samtycke*. För att samtycket ska vara giltigt måste det vara informerat. Behovet av att lämna tillräcklig förhandsinformation följer inte bara av direktiven om integritet och elektronisk kommunikation och om uppgiftsskydd, utan även av artiklarna 20 och 21 i direktivet om samhällsomfattande tjänster, ändrat genom direktiv 2009/136/EG ([32]). Behovet av information och samtycke bekräftas uttryckligen i skäl 28 i direktiv 2009/136/EG där det anges att ”användare under alla omständigheter [bör] vara fullt informerade om eventuella begränsningar av användningen av elektroniska kommunikationstjänster som införts av tjänstens och/eller nätets leverantör Leverantören bör ha möjlighet att själv specificera informationen så att den anger antingen vilket slags innehåll, tillämpning eller tjänst det är fråga om, eller de individuella tillämpningarna och tjänsterna, eller bådadera”. Därefter anges följande: ”Beroende på den använda tekniken och vilken begränsning som tillämpas kan dessa begränsningar kräva användarnas samtycke i enlighet med direktiv 2002/58/EG”.

59. Med tanke på komplexiteten i dessa övervakningstjänster är frågan om att ge meningsfull förhandsinformation en av de största utmaningarna för att erhålla ett giltigt samtycke. Konsumenterna bör informeras på ett sådant sätt att de förstår vilka uppgifter som behandlas, hur de används och vilka konsekvenser det får för användarupplevelsen och graden av intrång i den personliga integriteten som tekniken innebär.

60. Detta betyder inte bara att informationen i sig måste vara tydlig och begriplig för den genomsnittlige användaren utan också att informationen ska ges direkt till enskilda personer på ett framträdande sätt så att de inte missar den.

61. *Viljeyttring*. Enligt den gällande rättsliga ramen kräver samtycket också att användaren aktivt bekräftar sitt samtycke. Ett underförstått samtycke uppfyller alltså inte kravet. Detta bekräftar också behovet av att använda särskilda metoder för att erhålla samtycke till att internetleverantörer kontrollerar trafikuppgifter och kommunikationsuppgifter i samband med tillämpning av trafikstyrningspolitik. I sitt yttrande om samtycke nyligen betonade artikel 29-arbetsgruppen behovet av att samtycke måste ges för varje enskild del av de olika moment som ingår i uppgiftsbehandlingen.

([31]) Ett liknande fall är passageraruppgifter där det diskuterades huruvida passagerares samtycke till att bokningsuppgifter överfördes till amerikanska myndigheter var giltigt. Artikel 29-arbetsgruppen ansåg att passagerarnas samtycke inte kunde ges frivilligt eftersom flygbolagen är skyldiga att skicka uppgifterna innan flygets avgång och att passagerarna därför inte har något verkligt val, om de vill flyga – artikel 29-arbetsgruppens yttrande nr 6/2000 om överföring av passagerarlistor och andra uppgifter från flygbolag till Förenta staterna.

([32]) Direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (se fotnot 15).

62. Man kan hävda att om de parter som deltar i en kommunikation inte vill att internetleverantörer ska avlyssna den för att tillämpa trafikstyrningspolitik kan de alltid kryptera sin kommunikation. Detta kan vara bra rent praktiskt, men det kräver en viss ansträngning och teknisk kunskap och kan inte betraktas som likvärdigt med ett frivilligt, särskilt och informerat samtycke. Användning av krypteringsteknik skapar inte heller fullständig konfidentialitet för kommunikationen eftersom internetleverantören åtminstone kommer att kunna komma åt uppgifterna i IP-filetiketten för att kunna dirigera kommunikationen och också kommer att kunna göra en statistisk analys.

63. Enligt artikel 5.1 i direktivet om integritet och elektronisk kommunikation måste de berörda användarna ge sitt samtycke. I många fall är användaren samma person som abonnenten vilket innebär att samtycke kan ges samtidigt som abonnemanget på telekommunikationstjänsten tecknas. I andra fall, t.ex. när mer än en person berörs, måste samtycket inhämtas från var och en av de berörda personerna. Detta kan ge upphov till praktiska problem, vilket beskrivs nedan.

Samtycke från alla berörda användare

64. Enligt artikel 5.1 krävs användarnas samtycke för att behandlingen ska vara legitim. Samtycket måste inhämtas från *alla användare* som deltar i en kommunikation. Den logiska grunden för detta är att en kommunikation oftast omfattar minst två enskilda personer (sändaren och mottagaren). Om en internetleverantör t.ex. läser av IP-nyttolaster för ett e-postmeddelande, kontrollerar de uppgifter som berör både sändaren och mottagaren av meddelandet.

65. När de övervakar och avlyssnar trafik och kommunikation (t.ex. viss webbtrafik) kan det räcka att internetleverantören inhämtar användarens, dvs. abonnentens, samtycke. Anledningen är att den andra parten i kommunikationen, i detta fall en besökt webbplats, inte kan betraktas som en ”berörd användare” ([33]). Situationen kan dock bli mer komplicerad om övervakning omfattar kontroll av innehållet i e-postmeddelanden och därmed av personlig information om sändaren och mottagaren av meddelandet och de kanske inte båda har ett avtalsmässigt förhållande med samma internetleverantör. I dessa fall skulle internetleverantören i själva verket behandla personuppgifter (namn, e-postadress och eventuellt känsligt innehåll) från personer som inte är kunder. Ur ett praktiskt perspektiv kan det vara svårare att få dessa personers samtycke eftersom detta skulle göras från fall till fall i stället för när personen tecknar abonnemang på telekommunikationstjänsten. Det skulle inte heller vara realistiskt att anta att abonnentens samtycke också lämnas på andra användares vägnar, vilket ofta kan vara fallet för enskilda hushåll.

66. I det här sammanhanget anser datatillsynsmannen att internetleverantörerna bör följa befintliga rättsliga krav och tillämpa en politik som inte omfattar övervakning och kontroll av uppgifter. Detta blir ännu mer viktigt när det gäller kommunikationstjänster som omfattar tredje parter som inte kan ge sitt samtycke till övervakningen, särskilt i fråga om skickade och mottagna e-postmeddelanden (detta gäller inte när syftet bygger på säkerhetshänsyn).

67. Samtidigt bör det noteras att nationell lagstiftning för att genomföra artikel 5.1 i direktivet om integritet och elektronisk kommunikation inte alltid är tillfredsställande på denna punkt och att det i allmänhet tycks finnas ett behov av bättre riktlinjer i fråga om kraven i direktivet om integritet och elektronisk kommunikation i detta sammanhang. Därför uppmanar datatillsynsmannen kommissionen att agera mer aktivt i detta avseende och ta ett initiativ som skulle kunna dra nytta av synpunkter från de tillsynsmyndigheter som deltar i artikel 29-arbetsgruppen och från andra intressenter. Vid behov skulle ett fall kunna anmälas till EU-domstolen för att få ett förtydligande av vad artikel 5.1 betyder och innebär.

([33]) Oaktat de fall där webbtrafiken omfattar överföring av personlig information som t.ex. bilder på identifierbara fysiska personer som läggs upp på en webbplats. Behandlingen av sådana uppgifter kräver en rättslig grund, men skulle inte omfattas av artikel 5.1 eftersom dessa personer inte skulle vara ”berörda användare”.

V.3 **Proportionalitet – principen om dataminimering**

68. I artikel 6 c i direktivet om uppgiftsskydd föreskrivs proportionalitetsprincipen ([34]), som ska tillämpas på internetleverantörer eftersom de är registeransvariga i den mening som avses i det direktivet när de utför övervakning och filtrering.

69. Enligt den principen får personuppgifter endast behandlas om de är ”adekvata och relevanta och inte [] omfatta[r] mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas”. Tillämpningen av denna princip innebär att det måste göras en bedömning av om de metoder som används för uppgiftsbehandlingen och de typer av personuppgifter som används är lämpliga och med rimlig sannolikhet bidrar till att målen uppnås. Om man konstaterar att fler uppgifter än nödvändigt samlas in, har principen inte följts.

70. Det måste avgöras från fall till fall huruvida kontrolltekniker följer proportionalitetsprincipen eller ej. Det går inte att dra hypotetiska slutsatser. Det går dock att peka på olika konkreta aspekter som bör bedömas när efterlevnaden av proportionalitetsprincipen kontrolleras.

71. *Mängden behandlade uppgifter.* Övervakning av internetleverantörernas kunders kommunikation på djupast möjliga nivåer kommer i de flesta fall att vara alltför omfattande och olaglig. Det faktum att övervakningen kan göras med metoder som inte är uppenbara för enskilda personer och att det kan vara svårt för dem att förstå vad som händer förstärker effekterna för deras integritet. Internetleverantörer bör bedöma om det går att använda metoder som innebär mindre intrång för att nå det önskade resultatet. Kan t.ex. övervakning av IP-filetiketter ge det resultat som behövs, i stället för *deep packet inspection*? Även när *deep packet inspection* används kan identifiering av enbart vissa protokoll leda fram till den information som krävs. Tillämpningen av mekanismer för att skydda personuppgifter, bl.a. pseudoanonymisering, kan också vara relevant. Resultatet av bedömningen måste bekräfta att uppgiftsbehandlingen är proportionell.

72. *Behandlingens effekter (direkt kopplade till ändamålen).* Det kan finnas bristande proportionalitet i fall där internetleverantörer använder trafikstyrningspolitik som utesluter tillgång till vissa tjänster utan att i gengäld ge användarna en rimlig andel av fördelen med detta.

73. Det är viktigt att påpeka att proportionalitetsprincipen fortsätter att gälla även när andra obligatoriska rättsliga krav har uppfyllts, t.ex. om en internetleverantör har fått enskilda personers samtycke till innehållsövervakning. Detta betyder att den behandling av uppgifter som görs via innehållsövervakningen fortfarande kan vara olaglig om den strider mot den underliggande grundläggande proportionalitetsprincipen.

V.4 **Säkerheter och organisatoriska åtgärder**

74. I artikel 4 i direktivet om integritet och elektronisk kommunikation krävs uttryckligen att internetleverantörer ska vidta tekniska och organisatoriska åtgärder för att säkerställa att i) endast auktoriserad personal, och endast i lagliga syften, får tillgång till personuppgifter, ii) personuppgifter skyddas mot oavsiktlig eller olaglig behandling, och iii) en säkerhetspolitik införs för behandlingen av personuppgifter. Dessutom föreskrivs att nationella behöriga myndigheter ska kunna granska dessa åtgärder.

75. Enligt artikel 4.3 och 4.2 i direktivet om integritet och elektronisk kommunikation är internetleverantörer också skyldiga att anmäla personuppgiftsbrott till de behöriga nationella myndigheterna och till de berörda enskilda personerna om brottet kan inverka menligt på dem.

76. Behandling av personuppgifter som ingår i kommunikationer i syfte att tillämpa trafikstyrningspolitik kan ge internetleverantörer tillgång till uppgifter som är ännu känsligare än trafikuppgifter.

([34]) Som beskrivs ovan ska direktivet om uppgiftsskydd tillämpas i alla frågor som gäller skyddet av grundläggande fri- och rättigheter och som inte täcks specifikt av direktivet om integritet och elektronisk kommunikation.

77. Den säkerhetspolitik som internetleverantörer utvecklar bör därför innehålla särskilda skyddsmekanismer för att se till att de vidtagna åtgärderna är lämpliga för dessa risker. Samtidigt bör de nationella behöriga myndigheter som granskar dessa åtgärder ställa särskilt höga krav. Slutligen bör effektiva anmälningsförfaranden införas för att informera de registrerade vars uppgifter har utsatts för risker och som därför kan påverkas negativt.

VI. **FÖRSLAG TILL POLITISKA ÅTGÄRDER OCH LAGSTIFTNINGSÅTGÄRDER**

78. Kontrolltekniker som baseras på trafikuppgifter och kontroll av IP-nyttolaster, dvs. innehållet i kommunikationer, kan avslöja användarnas aktivitet på internet: Besökta webbplatser och aktiviteter på dessa platser, användning av fildelningstillämpningar, nedladdade filer, skickade och mottagna e-postmeddelanden, från vem, om vilket ändamål och på vilka villkor osv. Internetleverantörer kan vilja använda dessa uppgifter för att prioritera vissa former av kommunikation, t.ex. beställvideo, framför andra. De kan vilja använda uppgifterna för att upptäcka virus eller skapa profiler för beteendestyrd reklam. Dessa åtgärder inskränker rätten till konfidentialitet vid kommunikation.

79. Effekterna för integriteten förstärks beroende på vilken teknik som används och omständigheterna i det specifika fallet. Ju mer djupgående kontrollen och analysen av de insamlade uppgifterna är, desto större blir konflikten med principen om konfidentialitet vid kommunikation. Syftet med övervakningen och de mekanismer för uppgiftsskydd som har använts är också viktiga för att avgöra graden av intrång i enskilda personers integritet och personuppgifter. Blockering och övervakning för att bekämpa sabotageprogram, med strikta begränsningar för lagring och användning av de uppgifter som kontrolleras, kan inte jämföras med situationer där uppgifter registreras för att skapa individuella profiler till stöd för beteendeinriktad reklam.

80. I princip anser datatillsynsmannen att EU:s befintliga regelverk för integritetsskydd och uppgiftsskydd skulle vara tillräckligt för att garantera att rätten till konfidentialitet respekteras och att enskilda personers integritet och uppgiftsskydd inte hotas, om det tolkas, tillämpas och verkställs på rätt sätt ([35]). Internetleverantörer bör endast använda sådana mekanismer om de har tillämpat den rättsliga ramen korrekt. I synnerhet bör internetleverantörerna ta hänsyn till och respektera följande delar i regelverket:

— Internetleverantörer kan använda trafikstyrningspolitik i avsikt att garantera säkerhet för tjänsten och leverera tjänsten, inbegripet begränsning av överbelastningar, enligt artiklarna 4 och 6 i direktivet om integritet och elektronisk kommunikation.

— Internetleverantörerna behöver en annan särskild rättslig grund och eventuellt användarnas samtycke för att använda trafikstyrningspolitik som innebär behandling av trafikuppgifter och/eller kommunikationsuppgifter för andra syften än de ovannämnda. Det krävs t.ex. informerat samtycke från användarna för att övervaka och filtrera enskilda personers kommunikationer i syfte att begränsa (eller tillåta) tillgång till vissa tillämpningar och tjänster som fildelning och IP-telefoni.

— Det krävs frivilligt, uttryckligt och informerat samtycke. Samtycket bör ges genom en aktiv viljeyttring. Dessa krav lägger stark tonvikt vid behovet av att intensifiera ansträngningarna för att se till att enskilda personer får ordentlig information på ett sätt som är direkt, begripligt och specifikt, så att de kan bedöma effekterna av metoderna och i slutändan fatta ett informerat beslut. Med tanke på komplexiteten i dessa tekniker är frågan om att ge meningsfull förhandsinformation till användarna en av de största utmaningarna för att erhålla ett giltigt samtycke. Dessutom bör det inte finnas några negativa konsekvenser (där ekonomiska kostnader) för användare som inte ger sitt samtycke till någon övervakning.

([35]) Detta påverkar inte behovet av ändringar i lagstiftningen på grundval av andra överväganden, särskilt inom ramen för den allmänna översynen av EU:s rättsliga ram för uppgiftsskydd i syfte att göra den mer effektiv med hänsyn till ny teknik och globalisering.

— Proportionalitetsprincipen spelar en avgörande roll när internetleverantörer använder trafikstyrningspolitik, oberoende av den rättsliga grunden för och syftet med behandlingen: Leverera tjänsten, undvika överbelastning eller erbjuda anpassade abonnemang med eller utan tillgång till vissa tjänster och tillämpningar. Principen begränsar internetleverantörernas förmåga att övervaka innehållet i enskilda personers kommunikationer på ett sätt som medför behandling av alltför många uppgifter eller som skapar fördelar enbart för internetleverantören. Vad internetleverantören kan göra rent logistikmässigt beror på graden av intrång som tekniken medför, vilka resultat som eftersträvas (som de kan dra fördel av) och de särskilda mekanismer för integritetsskydd och uppgiftsskydd som tillämpas. Innan internetleverantören börjar använda kontrolltekniker måste denne göra en bedömning av huruvida tekniken uppfyller proportionalitetsprincipen.

81. I dagsläget omfattar den rättsliga ramen relevanta villkor och skyddsmekanismer, men det bör särskilt uppmärksammas huruvida internetleverantören faktiskt uppfyller de rättsliga kraven, om de ger den information till konsumenter som krävs för att fatta meningsfulla beslut och om de respekterar proportionalitetsprincipen. På nationell nivå omfattar de behöriga myndigheterna för detta dels de nationella telekommunikationsmyndigheterna, dels de nationella myndigheterna för skydd av personuppgifter. På EU-nivå berörs bl.a. Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec). Datatillsynsmannen kan också ha betydelse i detta sammanhang.

82. Utöver övervakningen av den nuvarande efterlevnadsnivån behöver vissa aspekter av den ram som har diskuterats i detta yttrande analyseras mer ingående och förklaras ytterligare, med hänsyn till att den förhållandevis nya möjligheten till massiv kontroll av kommunikationer i realtid. Den typ av vägledning som är särskilt relevant inom flera områden handlar bl.a. om följande:

— Avgöra vilka kontrollmetoder som är legitima för att garantera ett avbrottsfritt trafikflöde och som kanske inte kräver användarnas samtycke, t.ex. bekämpning av skräppost. Utöver graden av intrång som den använda övervakningen medför är det relevant med aspekter som t.ex. graden av störning av det obrutna trafikflödet som annars skulle uppstå.

— Avgöra vilka kontrollmetoder som kan användas för säkerhetsändamål och som kanske inte kräver användarnas samtycke.

— Avgöra när övervakning kräver den enskilda personens samtycke, framför allt samtycke från alla berörda användare, och tillåtna tekniska parametrar för att se till att kontrolltekniken inte innebär uppgiftsbehandling som inte står i proportion till ändamålen.

— I de tre ovannämnda fallen kan det också behövas vägledning om tillämpningen av de mekanismer för uppgiftsskydd som krävs (begränsning av ändamål, säkerhet osv.).

83. Eftersom behörigheterna inom detta område ligger på både nationell nivå och på EU-nivå anser datatillsynsmannen att det är mycket viktigt att det sker ett utbyte av synpunkter och erfarenheter för att ta fram harmoniserade strategier. Därför föreslår datatillsynsmannen att det ska bildas en plattform eller en expertgrupp med företrädare för nationella regleringsmyndigheter, artikel 29-arbetsgruppen, datatillsynsmannen och Berec. Denna plattforms första mål bör vara att ta fram riktlinjer om åtminstone de frågor som identifieras ovan, för att skapa solida och harmoniserad strategier och lika villkor. Datatillsynsmannen uppmanar kommissionen att organisera detta initiativ.

84. Sist men inte minst måste både nationella myndigheter och deras EU-motsvarigheter, däribland Berec och kommissionen, noggrant följa utvecklingen på marknaden inom detta område. Ur uppgiftsskydds- och integritetsperspektiv skulle ett scenario där internetleverantörer rutinmässigt använder trafikstyrningspolitik med abonnemang som baseras på filtrering av tillgång till innehåll och tjänster vara mycket problematiskt. Om detta inträffar skulle det behövas lagstiftning för att hantera situationen.

VII. **SLUTSATSER**

85. Internetleverantörer förlitar sig i allt högre grad på övervaknings- och kontrolltekniker som inskränker nätneutraliteten och konfidentialiteten vid kommunikation. Detta skapar allvarliga problem för skyddet av användarnas integritet och personuppgifterna.

86. I kommissionens meddelande om ett öppet internet och nätneutralitet i Europa berörs dessa frågor kortfattat, men datatillsynsmannen anser att det bör göras mer för att nå fram en tillfredsställande politik för utvecklingen. Detta yttrande är därför ett inlägg i den pågående politiska diskussionen om nätneutralitet, särskilt om aspekter på uppgiftsskydd och integritet.

87. Datatillsynsmannen anser att nationella myndigheter och Berec behöver övervaka situationen på marknaden. Denna övervakning bör leda fram till en tydlig bild av huruvida marknaden går mot massiv kontroll av kommunikationer i realtid och av problem i samband med efterlevnaden av den rättsliga ramen.

88. Övervakningen av marknaden bör åtföljas av en mer ingående analys av hur nya metoder påverkar uppgiftsskyddet och integriteten på internet. I detta yttrande beskrivs några områden som skulle behöva förtydligas. EU-organ och organ som Berec, artikel 29-arbetsgruppen och datatillsynsmannen kan vara väl lämpade att förtydliga villkoren för att tillämpa ramen, men datatillsynsmannen anser att kommissionen är skyldig att samordna och leda debatten. Därför uppmanar datatillsynsmannen kommissionen att ta ett initiativ för att ge alla dessa intressenter möjlighet att delta i en plattform eller arbetsgrupp med detta syfte. Bland de frågor som behöver analyseras mer bör följande punkter tas upp:

— Avgöra vilka kontrollmetoder som är legitima för att garantera ett trafikflöde utan avbrott och som kan användas för säkerhetsändamål.

— Avgöra när övervakning kräver den enskilda personens samtycke, framför allt samtycke från alla berörda användare, och tillåtna tekniska parametrar för att se till att kontrolltekniken inte innebär uppgiftsbehandling som inte står i proportion till ändamålen.

— I de ovannämnda fallen kan det också behövas vägledning om tillämpningen av de mekanismer för uppgiftsskydd som krävs (begränsning av ändamål, säkerhet osv.).

89. Beroende på resultaten kan det komma att krävas ytterligare lagstiftningsåtgärder. I så fall bör kommissionen föreslå politiska åtgärder för att stärka den rättsliga ramen och garantera rättslig säkerhet. Nya åtgärder bör förtydliga de praktiska konsekvenserna av principen om nätneutralitet, precis som redan har skett i vissa medlemsstater, och se till att användarna har en verklig valmöjlighet, främst genom att tvinga internetleverantörer att erbjuda anslutningar som inte är övervakade.

Utfärdat i Bryssel den 7 oktober 2011.

Peter HUSTINX

Europeiska datatillsynsmannen