I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om netneutralitet, trafikstyring og beskyttelse af privatlivets fred og personoplysninger

(2012/C 34/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16,

under henvisning til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 7 og 8,

under henvisning til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([1]),

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ([2]), særlig artikel 41, stk. 2,

under henvisning til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor ([3]) —

VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

I.1. Baggrund

1. Den 19. april 2011 vedtog Kommissionen en meddelelse om det åbne internet og netneutraliteten i Europa ([4]).

2. Denne udtalelse kan ses som den tilsynsførendes reaktion på denne meddelelse, og sigtet er at bidrage til den igangværende politiske debat i EU om netneutralitet, navnlig aspekter vedrørende databeskyttelse og beskyttelse af privatlivets fred.

([1]) EFT L 281 af 23.11.1995, s. 31, »databeskyttelsesdirektivet«.
([2]) EFT L 8 af 12.1.2001, s. 1, »databeskyttelsesforordningen«.
([3]) EFT L 201 af 31.7.2002, s. 37, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (se fodnote 15), »e-databeskyttelsesdirektivet«.
([4]) KOM(2011) 222 endelig.

3. Udtalelsen er baseret på den tilsynsførendes svar ([5]) på Kommissionens offentlige høring om det åbne internet og netneutralitet i Europa, der blev afholdt forud for Kommissionens meddelelse. Den tilsynsførende har også noteret sig det nylige udkast til Rådets konklusioner om netneutraliteten ([6]).

I.2. **Begrebet netneutralitet**

4. Netneutralitet er genstand for en aktuel debat om, hvorvidt internetudbyderne (ISP'er ([7])) skal have lov til at begrænse, filtrere eller spærre for internetadgangen eller på anden vis påvirke internettets virkemåde. Begrebet netneutralitet bygger på den opfattelse, at oplysninger på internettet skal overføres upartisk og uden hensyntagen til indhold, bestemmelsessted og kilde, og at brugerne skal kunne bestemme, hvilke applikationer, tjenester og hardware de ønsker at benytte. Internetudbyderne kan således ikke efter eget valg opprioritere eller nedsætte hastigheden på adgangen til visse applikationer eller tjenester, f.eks. peer-to-peer (»P2P«) osv ([8]).

5. Filtrering, spærring og inspektion af nettrafik rejser en række vigtige spørgsmål, der ofte overses eller køres ud på et sidespor, om kommunikationshemmelighed og fysiske personers ret til beskyttelse af privatlivets fred og personoplysninger, når de bruger internettet. Der kan f.eks. være tale om visse inspektionsteknikker, der indebærer overvågning af kommunikationsindhold, besøgte websteder, sendte og modtagne e-mails, tidspunktet for aktiviteten osv., og som gør det muligt at filtrere kommunikationen.

6. Internetudbydere, som inspicerer kommunikationsdata, kan bryde kommunikationshemmeligheden, der er en grundlæggende ret sikret i artikel 8 i den europæiske konvention om beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (»den europæiske menneskerettighedskonvention«) og artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder (»chartret«). Kommunikationshemmeligheden er yderligere beskyttet i afledt EU-lovgivning, nemlig artikel 5 i e-databeskyttelsesdirektivet.

I.3. **Udtalelsens fokus og struktur**

7. Den tilsynsførende mener, at der i en seriøs politisk debat om netneutralitet skal være fokus på kommunikationshemmeligheden og andre aspekter vedrørende beskyttelse af privatlivets fred og databeskyttelse.

8. Denne udtalelse bidrager til denne igangværende EU-debat. Den har tre formål:

— Der sættes fokus på relevansen af beskyttelsen af privatlivets fred og databeskyttelse i den igangværende debat om netneutralitet, og det understreges navnlig, at de eksisterende bestemmelser om kommunikationshemmelighed skal overholdes. Vi bør kun tillade praksis, der er i overensstemmelse med disse bestemmelser.

— Netneutralitet hænger sammen med udnyttelsen af relativt nye — teknologiske — muligheder, og der er kun få erfaringer med anvendelsen af den retlige ramme på dette område. Denne udtalelse indeholder således retningslinjer for, hvordan internetudbyderne skal anvende og overholde den retlige ramme for databeskyttelse i forbindelse med filtrering, spærring og inspektion af nettrafik. De vil kunne hjælpe internetudbyderne samt de myndigheder, der har til opgave at håndhæve lovgivningen.

— I denne udtalelse udpeges en række områder, der kræver særlig opmærksomhed, og hvor det kan være nødvendigt at gribe ind på EU-plan for at sikre beskyttelsen af privatlivets fred og databeskyttelse. Det er navnlig vigtigt i lyset af den igangværende debat på EU-plan og Kommissionens eventuelle politiske foranstaltninger på dette område.

([5]) Den tilsynsførende understregede i sit svar betydningen af at tage hensyn til aspekter vedrørende databeskyttelse og beskyttelse af privatlivets fred samt andre eksisterende rettigheder og værdier. Svaret er tilgængeligt på følgende websted: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

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

([7]) Udbydere af både fast og mobil internetadgang.

([8]) Princippet berører dog ikke internetudbydernes ret til at begrænse hastigheden eller mængden af oplysninger, som abonnenten kan sende eller modtage via abonnementer med båndbredde- eller volumenbegrænsninger. I henhold til princippet om netneutralitet har internetudbyderne således stadig mulighed for at tilbyde internetabonnementer med begrænset adgang baseret på kriterier som hastighed eller volumen, såfremt det ikke indebærer forskelsbehandling til fordel for eller på bekostning af særligt indhold.

9. Den tilsynsførende er opmærksom på, at netneutralitet rejser en række andre spørgsmål, som der redegøres nærmere for nedenfor, såsom spørgsmål vedrørende adgang til oplysninger. Disse spørgsmål behandles kun i det omfang, de er relateret til eller har en direkte indvirkning på databeskyttelsen og beskyttelsen af privatlivets fred.

10. Udtalelsen er struktureret som følger: Afsnit II indledes med en kort oversigt over internetudbydernes praksis med hensyn til filtrering. I afsnit III redegøres der for EU's retlige ramme for netneutralitet. Afsnit IV indeholder en teknisk beskrivelse efterfulgt af en vurdering af konsekvenserne for privatlivets fred af de anvendte teknikker. I afsnit V analyseres de praktiske aspekter i forbindelse med anvendelsen af den nuværende EU-lovgivning om beskyttelse af privatlivets fred og databeskyttelse. Med udgangspunkt i denne analyse fremsættes der i afsnit VI en række forslag til videreudvikling af politikken, og de områder, hvor det kan være nødvendigt at præcisere og forbedre den retlige ramme, identificeres. Afsnit VII indeholder konklusionerne.

II. **POLITIKKER FOR NETNEUTRALITET OG TRAFIKSTYRING**

Stigende brug af trafikstyringspolitikker

11. Internetudbyderne har traditionelt kun overvåget og påvirket nettrafikken i begrænset omfang. Internetudbyderne har f.eks. anvendt inspektionsteknikker og begrænset informationsstrømme for at opretholde netsikkerheden, f.eks. for at bekæmpe virus. Internettet er således generelt vokset, samtidig med at dets neutralitet i vidt omfang er blevet beskyttet.

12. I de senere år har nogle internetudbydere imidlertid ønsket at foretage inspektion af nettrafikken for at differentiere og anvende forskellige politikker på dette område, f.eks. for at spærre for specifikke tjenester eller skabe særlig adgang til andre. Dette kaldes undertiden »trafikstyringspolitikker« ([9]).

13. Der er mange årsager til, at internetudbyderne ønsker at inspicere og differentiere trafikken. Trafikstyringspolitikker kan f.eks. anvendes af internetudbyderne til at forvalte trafikken i spidsbelastningsperioder, f.eks. ved at opprioritere nogle former for tidsfølsom trafik såsom videostreaming og nedprioritere andre former for trafik, der måske er mindre tidsfølsomme, f.eks. P2P ([10]). Internetudbyderne kan desuden på forskellig vis gøre brug af trafikstyring som en potentiel indtægtskilde. Internetudbyderne kan på den ene side pålægge indholdsudbyderne et gebyr, f.eks. de udbydere, hvis tjenester kræver anvendelse af større båndbredde, mod at opprioritere dem (og således stille større hastighed til rådighed). Der vil således være hurtigere adgang til en bestemt tjeneste, f.eks. video on demand, end til en anden tilsvarende tjeneste uden højhastighedstransmission. Abonnenter, der gerne vil betale højere (eller lavere) gebyrer for visse former for differentierede abonnementer, er ligeledes en indtægtskilde. Et abonnement uden adgang til P2P kan f.eks. være billigere end et abonnement med ubegrænset adgang.

14. Internetudbyderne har deres egne grunde til at anvende trafikstyringspolitikker, men andre parter kan også have en interesse i, at internetudbyderne anvender trafikstyringspolitikker. Hvis internetudbyderne styrer deres net og foretager inspektion af indhold, der fremsendes via disse, vil de sandsynligvis øge deres muligheder for at spore påstået ulovlig anvendelse, f.eks. overtrædelse af ophavsrettigheder eller pornografisk brug.

([9]) Se f.eks. Ofcoms rapport »Site blocking to reduce online copyright infringement« af 27. maj 2011, der er tilgængelig på http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: »Nogle internetudbydere anvender pakkeinspektionssystemer i deres net til trafikstyring og andre formål, og vi formoder således, at de kan anvendes, selv om det vil være meget komplekst og omkostningskrævende for udbydere, der ikke allerede har indført sådanne systemer. På kort og mellemlang sigt vil DPI-systemer muligvis kun blive anvendt af de større internetudbydere, da de kræver store kapitalinvesteringer«.

([10]) Kvaliteten af realtidsapplikationer såsom videostreaming afhænger bl.a. af latenstid, dvs. forsinkelse, f.eks. på grund af overbelastning af nettet.

Andre berørte interesser, herunder databeskyttelse og beskyttelse af privatlivets fred

15. Denne udvikling har givet anledning til en debat om legitimiteten af denne form for praksis, herunder især om der skal indføres yderligere specifikke lovgivningsmæssige forpligtelser til beskyttelse af netneutraliteten.

16. Der er en risiko for, at internetudbydernes stigende brug af trafikstyringspolitikker vil begrænse adgangen til oplysninger. Hvis denne praksis blev almindelig, og det ikke var muligt (eller meget dyrt) for brugerne at få adgang til hele internettet, som vi kender det, ville det bringe adgangen til oplysninger og brugerens mulighed for at sende og modtage det indhold, de ønsker, ved hjælp af applikationer eller tjenester efter eget valg, i fare. Et retligt bindende princip om netneutralitet kan løse dette problem.

17. Dette bringer den tilsynsførende frem til aspekterne ved databeskyttelse og beskyttelse af privatlivets fred i forbindelse med internetudbydernes trafikstyring. Nærmere bestemt:

— Når internetudbyderne behandler trafikdata med det ene formål at sende informationsstrømmen fra afsenderen til modtageren, er der generelt tale om en begrænset behandling af personoplysninger ([11]). På samme måde som posttjenesten behandler oplysningerne på en kuvert, behandler internetudbyderne de nødvendige oplysninger til at dirigere kommunikationen til modtageren. Dette er ikke i strid med lovkravene om databeskyttelse, beskyttelse af privatlivets fred og kommunikationshemmeligheden.

— Når internetudbyderne foretager inspektion af kommunikationsdata for at differentiere de enkelte kommunikationsstrømme og indføre specifikke politikker, der kan være ufordelagtige for den enkelte bruger, er konsekvenserne større. Afhængigt af omstændighederne i den enkelte sag og analysens art kan behandlingen i høj grad være en krænkelse af retten til privatlivets fred og beskyttelse af personoplysninger. Det gælder især, når styringspolitikkerne afslører indholdet af den enkeltes internetkommunikation, herunder sendte og modtagne e-mails, besøgte websteder og downloadede eller uploadede filer osv.

III. OVERSIGT OVER EU'S RETLIGE RAMME FOR NETNEUTRALITET OG VIDEREUDVIKLING AF POLITIKKEN

III.1. Den retlige ramme kort fortalt

18. Indtil 2009 omfattede EU's lovgivningsinstrumenter ikke bestemmelser, der udtrykkeligt forbød internetudbyderne at filtrere, spærre eller pålægge abonnenterne yderligere omkostninger for adgang til tjenester. De omfattede heller ikke bestemmelser, der udtrykkeligt anerkendte denne praksis. Situationen var forbundet med en vis usikkerhed.

19. Det ændrede sig med telekommunikationspakken fra 2009, der indeholdt bestemmelser til fremme af internettets åbenhed. I artikel 8, stk. 4, i direktivet om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (»rammedirektivet«) pålægges tilsynsmyndighederne bl.a. at fremme slutbrugerens mulighed for at få adgang til indhold, applikationer eller tjenester efter eget valg ([12]). Denne bestemmelse gælder for nettet som helhed og ikke kun for de enkelte udbydere. I det nylige udkast til Rådets konklusioner understreges det ligeledes, at det er nødvendigt at bevare internettets åbenhed ([13]).

([11]) Omfatter ikke operationer, der har til formål at øge netsikkerheden og spore skadelig trafik, eller operationer, der er nødvendige for debitering og afregning af samtrafik. Omfatter heller ikke forpligtelserne i datalagringsdirektivet, Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006, s. 54) (»datalagringsdirektivet«).

([12]) Direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester som ændret ved direktiv 2009/140/EF og forordning (EF) nr. 544/2009 (EUT L 337 af 18.12.2009, s. 37).

([13]) Se punkt 3, litra e), hvor Rådet anerkender behovet for at bevare internettets åbenhed og samtidig sikre, at det fortsat kan levere ydelser af høj kvalitet inden for rammer, som fremmer og respekterer de grundlæggende rettigheder som ytrings- og næringsfrihed, og punkt 8, litra d), hvor medlemsstaterne opfordres til at fremme internettets åbne og neutrale karakter som et politisk mål.

20. Forsyningspligtdirektivet ([14]) indeholder mere konkrete forpligtelser. I artikel 20 og 21 stilles der krav om gennemsigtighed, for så vidt angår begrænsning af adgangen til og/eller anvendelsen af tjenester og applikationer. Der stilles ligeledes krav om et mindstemål af kvalitet.

21. Med hensyn til internetudbydernes inspektion af den enkelte brugers kommunikation understreges det i betragtning 28 i direktivet om ændring af direktiverne om forsyningspligt og e-databeskyttelse ([15]), at »afhængigt af den anvendte teknologi og hvilken form for begrænsning der gør sig gældende, kan sådanne begrænsninger kræve brugerens samtykke,« jf. e-databeskyttelsesdirektivet. I betragtning 28 understreges således kravet om samtykke i henhold til artikel 5, stk. 1, i e-databeskyttelsesdirektivet til eventuelle begrænsninger baseret på overvågning af kommunikationsdata. Afsnit IV nedenfor indeholder en grundig analyse af anvendelsen af artikel 5, stk. 1, og den overordnede retlige ramme for databeskyttelse og beskyttelse af privatlivets fred.

22. Endelig har de nationale tilsynsmyndigheder nu i henhold til artikel 22, stk. 3, i forsyningspligtdirektivet mulighed for at fastsætte mindstekrav til tjenesters kvalitet over for internetudbyderne for at hindre, at tjenesten forringes, og at trafikken over offentlige net hæmmes eller forsinkes.

23. Der er således på EU-plan et bredt ønske om et åbent internet (se artikel 8, stk. 4, i rammedirektivet). Denne politiske målsætning for nettet som helhed er imidlertid ikke direkte forbundet med forbud og forpligtelser i forhold til de enkelte internetudbydere. En internetudbyder kan med andre ord kun anvende trafikstyringspolitikker, der udelukker adgang til visse applikationer, hvis slutbrugerne er fuldt ud informeret og frivilligt, specifikt og utvetydigt har givet deres samtykke.

24. Situationen er forskellig i de enkelte medlemsstater. I nogle medlemsstater kan internetudbyderne under særlige betingelser anvende trafikstyringspolitikker, f.eks. for at spærre for applikationer, f.eks. VoIP (internettelefoni) (i forbindelse med i et billigere internetabonnement), såfremt brugeren har givet et frivilligt, specifikt, utvetydigt og informeret samtykke. Andre medlemsstater har valgt at styrke princippet om netneutralitet. I juli 2011 vedtog det nederlandske parlament f.eks. en lov, der generelt forbød udbydere at hindre eller forsinke internetapplikationer eller -tjenester (f.eks. VoIP), medmindre det var nødvendigt for at minimere virkningerne af overbelastning, af integritets- eller sikkerhedsgrunde, for at bekæmpe spam eller i medfør af en retsafgørelse ([16]).

III.2. **Meddelelsen om netneutralitet**

25. I sin meddelelse om netneutralitet ([17]) konkluderede Europa-Kommissionen, at situationen med hensyn til netneutralitet skal overvåges og analyseres yderligere. Kommissionens politik er blevet beskrevet som en politik, hvor man afventer og ser, hvad der sker, inden nye lovgivningstiltag overvejes.

([14]) Direktiv 2002/22/EF som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse. (EUT L 337 af 18.12.2009, s. 11). Sammenlign endvidere med artikel 1, stk. 3, hvori det anføres, at direktivet hverken kræver eller forbyder, at udbydere fastsætter betingelser, der begrænser slutbrugernes adgang til og/eller benyttelse af tjenester og applikationer, hvor dette er tilladt i henhold til national ret og er i overensstemmelse med fællesskabsretten, men fastsætter en forpligtelse til at give oplysninger om sådanne betingelser.

([15]) Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse.

([16]) Den nye nederlandske lov kan ses på: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Ifølge pressen var baggrunden for denne politiske løsningsmodel ikke at sikre databeskyttelse og beskyttelse af privatlivets fred, men snarere at sikre, at brugerne ikke nægtes adgang til eller kun tilbydes begrænset adgang til oplysninger. Denne nye lov er således tilsyneladende begrundet i spørgsmål vedrørende adgang til oplysninger.

([17]) Se fodnote 4.

26. Det understreges i Kommissionens meddelelse, at alle foranstaltninger og yderligere lovgivningstiltag vil blive vurderet grundigt, for så vidt angår aspekterne ved databeskyttelse og beskyttelse af privatlivets fred. Rådet kommer i sit udkast til konklusioner ligeledes ind på en række relevante spørgsmål vedrørende beskyttelse af privatlivets fred og databeskyttelse ([18]).

27. Spørgsmålet er, om en afventende politik er tilstrækkelig i relation til databeskyttelse og beskyttelse af privatlivets fred. Selv om den retlige ramme for databeskyttelse og beskyttelse af privatlivets fred indeholder en række beskyttelsesbestemmelser, navnlig baseret på princippet om kommunikationshemmelighed, er det tilsyneladende nødvendigt at overvåge overholdelsen nøje og udstikke retningslinjer for en række aspekter, der ikke er særlig klare. Det skal desuden overvejes, hvordan den retlige ramme kan præciseres og forbedres yderligere i lyset af den teknologiske udvikling. Hvis overvågningen viser, at markedet går i retning af massiv realtidsinspektion af kommunikation, og at der er problemer med overholdelse af lovgivningen, skal der træffes lovgivningsmæssige foranstaltninger. Der fremsættes en række konkrete forslag på dette område i afsnit VI.

IV. **TEKNISK BAGGRUND OG KONSEKVENSERNE FOR BESKYTTELSEN AF PRIVATLIVETS FRED OG DATABESKYTTELSEN**

28. Inden der ses nærmere på dette spørgsmål, er det vigtigt at få et bedre overblik over, hvilke inspektionsteknikker internetudbyderne kan anvende til trafikstyring, og hvorledes de kan indvirke på princippet om netneutralitet. Konsekvenserne for databeskyttelsen og beskyttelsen af privatlivets fred af anvendelsen af disse teknikker er meget forskellige afhængigt af den/de anvendte teknikker. Det er nødvendigt at kende denne tekniske baggrund for at forstå og anvende den lovgivning om databeskyttelse, der er beskrevet i afsnit V, korrekt. Det skal imidlertid bemærkes, at der er tale om et komplekst område i konstant udvikling. Beskrivelsen nedenfor tilsigter således ikke at være udtømmende og helt opdateret, men skal blot give de tekniske oplysninger, der er nødvendige for at forstå den juridiske argumentation.

IV.1. **Overførsel af oplysninger via internettet: grundlæggende principper**

29. Når en bruger overfører en meddelelse via internettet, opdeles de overførte oplysninger i pakker. Disse pakker overføres via internettet fra afsenderen til modtageren. Den enkelte pakke indeholder bl.a. oplysninger om kilde og bestemmelsessted. Udbyderne kan desuden pakke disse pakker i yderligere lag og protokoller ([19]), der anvendes til at styre de forskellige trafikstrømme på udbyderens net.

30. For at vende tilbage til analogien med postbrevet kan anvendelsen af en protokol til overførsel via nettet sammenlignes med at lægge et postbrev i en kuvert med en destinationsadresse, som skal læses af posttjenesten, der herefter udbringer brevet. Posttjenesten kan anvende yderligere protokoller i dets interne forsendelsessystem for at håndtere alle de kuverter, der skal udbringes, med henblik på at sikre, at hver enkelt kuvert når frem til det bestemmelsessted, som afsenderen oprindeligt anførte. I analogi hermed består hver enkelt pakke af to dele. Den første del er *IP-payloadet*, der omfatter kommunikationens indhold, og som svarer til brevet. Det indeholder oplysninger, der udelukkende er adresseret til modtageren. Den anden del af pakken er *IP-headeren*, der bl.a. omfatter modtagerens og afsenderens adresse, og som svarer til kuverten. IP-headeren giver internetudbyderne og andre formidlere mulighed for at sende payloadet fra kildeadressen til destinationsadressen.

31. Internetudbyderne og andre formidlere sikrer, at IP-pakkerne sendes over nettet ved hjælp af knudepunkter, som læser oplysningerne i IP-headeren, holder dem op imod routingtabellerne og herefter fremsender dem til det næste knudepunkt hen imod bestemmelsesstedet. Denne proces gentages på hele

([18]) Se punkt 4, litra e), hvor Rådet gør opmærksom på en række aspekter vedrørende beskyttelse af personoplysninger, der navnlig er blevet påpeget af forbrugerbeskyttelsesorganisationer og databeskyttelsesmyndigheder.

([19]) Som beskrevet nærmere i afsnit IV.2 koder sådanne protokoller de end-to-end-transmitterede oplysninger, således at parterne i kommunikationen kan forstå hinanden, som f.eks. HTTP, FTP osv.

nettet ved anvendelse af en »best effort memoryless«-tilgang, da alle de pakker, der når frem til et knudepunkt, behandles neutralt. Når de er blevet fremsendt til det næste knudepunkt, er der ingen grund til at beholde yderligere oplysninger i routeren ([20]).

IV.2. **Inspektionsteknikker**

32. Som beskrevet ovenfor læser internetudbyderne IP-headerne med henblik på at sende dem til deres bestemmelsessted. Som anført ovenfor kan analysen af trafikken (IP-headere og IP-payload) imidlertid foretages med andre formål for øje og ved hjælp af forskellige typer teknologier. Som led i den nye udvikling er internetudbyderne f.eks. begyndt at nedsætte hastigheden på visse applikationer, der anvendes af brugerne, f.eks. P2P, eller alternativt øge trafikhastigheden for visse tjenester som video on demand til premium-abonnenter. Selv om alle inspektionsteknikker *teknisk set* anvendes til at foretage pakkeinspektion, indebærer de forskellige grader af indgriben. Der er to hovedkategorier af inspektionsteknikker. Den ene er kun baseret på IP-headeren, mens den anden også er baseret på IP-payloadet.

Baseret på oplysningerne i IP-headeren. Inspektionen af en IP-pakkeheader afslører en række felter, der giver internetudbyderne mulighed for at anvende en række specifikke trafikstyringspolitikker. Disse teknikker, som udelukkende er baseret på inspektion af IP-headere, behandler data, der i princippet har til formål at dirigere oplysninger til et andet formål (f.eks. differentiering af trafik). Internetudbyderen kan forbinde IP-kildeadressen til en konkret abonnent og anvende en række specifikke politikker, f.eks. sende pakken gennem et hurtigere eller langsommere link. Internetudbyderen kan også bruge IP-destinationsadressen i forbindelse med andre specifikke politikker, f.eks. til at spærre eller filtrere adgangen til visse websteder.

Baseret på en mere dybdegående inspektion. Deep packet inspection giver internetudbyderen mulighed for at få adgang til oplysninger, der udelukkende er adresseret til modtageren af meddelelsen. For at vende tilbage til eksemplet med posttjenesten kan denne tilgang sammenlignes med at åbne kuverten og læse brevet for at foretage en analyse af kommunikationsindholdet (indkapslet i IP-pakkerne) med henblik på at anvende en specifik netpolitik. Der er forskellige inspektionsteknikker, som hver især indebærer forskellige risici for den registrerede.

— *Deep packet inspection baseret på analyse af protokoller og statistiske data*. Ud over IP-protokollen til overførsel af dataene via internettet er der en række yderligere protokoller, som koder de fremsendte oplysninger på en bestemt måde (transport, session, visning, applikation osv.). Formålet med disse protokoller er at sikre, at parterne i kommunikationen kan forstå hinanden. Nogle protokoller anvendes f.eks. til webbrowsing ([21]), mens andre anvendes til filoverførsel ([22]) osv. Derfor er formålet med inspektionsteknikker baseret på inspektion af protokoller og statistisk analyse at finde specifikke mønstre eller fingeraftryk, der viser, hvilke protokoller der anvendes ([23]). Disse inspektionsteknikker giver internetudbyderne mulighed for at identificere kommunikationstypen (e-mail, webbrowsing, uploading af filer) og den specifikke tjeneste eller applikation, der anvendes, f.eks. visse VoIP-kommunikationstyper, hvor de anvendte protokoller er helt specifikt bundet til en konkret leverandør eller tjenesteudbyder. Så snart internetudbyderne har identificeret kommunikationstypen, har de mulighed for at anvende konkrete trafikstyringspolitikker, f.eks. spærre for webtrafik. Det kan også være det første skridt, der giver internetudbyderen mulighed for at foretage yderligere analyser, som kan kræve fuld adgang til metadata og kommunikationsindhold.

([20]) I internetudstyr anvendes der imidlertid routingprotokoller, som benyttes til generering af logfiler over aktiviteten, behandling af trafikstatistik og udveksling af oplysninger med andet netudstyr med henblik på at sende IP-pakker ad den mest effektive vej. Hvis et link er overbelastet eller brudt, og routeren modtager denne oplysning, vil den opdatere routingtabellen med et alternativt link. Det skal også understreges, at indsamling og behandling af data undertiden sker i faktureringsøjemed eller endog i overensstemmelse med kravene i datalagringsdirektivet.

([21]) HTTP — hypertext transfer protocol — eller HTML — hypertext markup language.

([22]) FTP — file transfer protocol.

([23]) Der er forskellige metoder til at identificere, hvilke protokoller, der anvendes. Det er f.eks. muligt at søge i specifikke felter i interne protokoller, f.eks. at identificere porte, der anvendes til at etablere kommunikationen. Der kan også udledes en statistisk karakterisering af en kommunikationsstrøm ved analyse af en række specifikke felter gennem korrelation af de protokoller, der anvendes samtidigt mellem to IP-adresser.

— *Deep packet inspection baseret på analyse af kommunikationsindholdet.* Endelig er det også muligt at foretage inspektion af metadataene ([24]) og selve indholdet af kommunikationen. Denne teknik består i at opfange alle de IP-pakker, der indgår i den oprindelige kommunikationsstrøm, således at hele kommunikationens oprindelige indhold kan rekonstrueres og analyseres. For at spore skadeligt eller ulovligt indhold som f.eks. virus, børnepornografi osv. er det nødvendigt at rekonstruere selve indholdet, således at det kan analyseres. Det skal bemærkes, at de implicerede parter nogle gange bevidst krypterer kommunikationen end-to-end, og denne praksis begrænser internetudbydernes muligheder for at analysere kommunikationens indhold.

IV.3. **Konsekvenser for beskyttelsen af privatlivets fred og databeskyttelsen**

33. Inspektionsteknikker baseret på IP-headere, herunder navnlig teknikker baseret på pakkeinspektion, indebærer overvågning og filtrering af disse data og har alvorlige konsekvenser for beskyttelsen af privatlivets fred og databeskyttelsen. De kan også være i strid med retten til kommunikationshemmelighed.

34. Det har i sig selv alvorlige konsekvenser for beskyttelsen af privatlivets fred og databeskyttelsen at læse den enkeltes kommunikation. Problemet er imidlertid mere alvorligt, da det vil få større konsekvenser for beskyttelsen af privatlivets fred afhængigt af formålet med overvågningen og opfangelsen. At inspicere kommunikation, f.eks. for at sikre, at systemet fungerer efter hensigten, er ikke det samme som at inspicere kommunikation for at anvende politikker, der kan få konsekvenser for den enkelte. Hvis trafik- og udvælgelsespolitikkerne udelukkende har til formål at undgå overbelastning af nettet, vil der normalt ikke være nogen større konsekvenser for beskyttelsen af privatlivets fred. Formålet med trafikstyringspolitikker kan imidlertid være at spærre for visse former for indhold eller påvirke kommunikationen, f.eks. gennem adfærdsbetinget reklame. I disse tilfælde er konsekvenserne mere alvorlige. Det bliver endnu mere kritisk, når man tænker på, at oplysninger af denne art ikke blot indsamles for en lille gruppe af individer, men snarere generelt for alle internetudbyderens kunder ([25]). Hvis alle internetudbydere begynder at anvende filtreringsteknikker, kan det indebære en generel overvågning af brugen af internettet. Med hensyn til den type af oplysninger, der behandles, er risiciene for privatlivets fred desuden helt klart store, da mange af de oplysninger, der indsamles, vil være meget følsomme, og da de indsamlede oplysninger er tilgængelige for internetudbyderne og for dem, der søger i oplysningerne. Disse oplysninger kan desuden også have meget stor kommerciel værdi. Det indebærer i sig selv en stor risiko for funktionsskred, hvor det oprindelige formål nemt kan udvikle sig til kommerciel eller anden udnyttelse af de indsamlede oplysninger.

35. Overvågnings-, inspektions- og filtreringsteknikkerne skal anvendes korrekt i overensstemmelse med gældende bestemmelser om databeskyttelse og beskyttelse af privatlivets fred, hvori der er fastsat grænser for, hvad der er tilladt og under hvilke betingelser. Nedenfor gives en oversigt over gældende beskyttelsesbestemmelser i den nuværende EU-lovgivning om databeskyttelse og beskyttelse af privatlivets fred.

V. **ANVENDELSE AF EU'S RETLIGE RAMME FOR BESKYTTELSE AF PRIVATLIVETS FRED OG DATABESKYTTELSE**

36. EU's retlige ramme for databeskyttelse er teknologineutral. Den indeholder således ikke bestemmelser om specifikke inspektionsteknikker såsom de teknikker, der er beskrevet ovenfor. E-databeskyttelsesdirektivet indeholder bestemmelser om beskyttelse af privatlivets fred i forbindelse med tilvejebringelse

([24]) Hver enkelt protokol har en række specifikke felter i headeren, som indeholder yderligere uformelle oplysninger om den fremsendte kommunikation. Indholdet af disse felter kan derfor betegnes som kommunikationens metadata. Et eksempel på disse felter er det anvendte portnummer, hvor der sandsynligvis er tale om webbrowsing, hvis det er nr. 80.

([25]) Det er naturligvis ikke kun internetudbydere, der kan spore oplysninger. Det kan udbydere af annoncenetværk også ved hjælp af tredjepartscookies, der anvendes til at spore brugere på de forskellige websteder. Se f.eks. en artikel offentliggjort for nylig i et akademisk tidsskrift, som viser, at Google er tilstedeværende på 97 af de 100 mest populære websteder, hvilket indebærer, at Google kan spore brugere, som ikke har fravalgt tredjepartscookies, når de browser på disse populære websteder. 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). Findes på følgende websted: http://ssrn.com/abstract=1898390. Spørgsmålet om sporing af brugere ved hjælp af tredjepartscookies er blevet behandlet af Artikel 29-Gruppen. Se udtalelse 2/2010 om adfærdsbetinget annoncering på internettet vedtaget den 22. juni 2010 (WP 171).

af elektroniske kommunikationstjenester via offentlige kommunikationsnet (typisk internetadgang og telefoni) ([26]), og databeskyttelsesdirektivet regulerer databehandling generelt. I denne retlige ramme pålægges internetudbydere, der behandler og overvåger trafik- og kommunikationsdata, en række forskellige forpligtelser.

V.1. **De retlige grundlag for behandling af trafik- og indholdsdata**

37. I henhold til lovgivningen om databeskyttelse skal der være et passende retligt grundlag for behandling af personoplysninger, i denne forbindelse behandling af trafik- og kommunikationsdata. Ud over dette generelle krav kan der i visse tilfælde være specifikke krav.

38. I dette tilfælde er den type personoplysninger, der behandles af udbyderne, trafikdata og kommunikationsindhold. Kommunikationsindholdet og trafikdataene er begge beskyttet af retten til brevhemmelighed, der er garanteret i artikel 8 i den europæiske menneskerettighedskonvention og artikel 7 og 8 i chartret. I henhold til artikel 5, stk. 1, i e-databeskyttelsesdirektivet med titlen »Kommunikationshemmelighed« skal medlemsstaterne således sikre kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata. Det fastslås samtidig i artikel 5, stk. 1, i e-databeskyttelsesdirektivet, at internetudbydere kan få tilladelse til at behandle trafik- og indholdsdata under visse omstændigheder med brugernes samtykke. Det sker ved indførelse af et forbud mod »aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1.» Der redegøres nærmere herfor nedenfor.

39. Ud over de pågældende brugeres samtykke anføres der andre grundlag i e-databeskyttelsesdirektivet, der kan legitimere tjenesteudbydernes behandling af trafik- og kommunikationsdata. De relevante retlige grundlag for behandling i dette tilfælde er i) levering af tjenesten, ii) beskyttelse af tjenesten og iii) minimering af overbelastningen. En række andre mulige grundlag for legitimering af styringspolitikker baseret på trafik- eller kommunikationsdata drøftes nedenfor under iv).

i) Retligt grundlag for levering af tjenesten

40. Som anført i afsnit IV behandler internetudbyderne oplysningerne i IP-headere med henblik på at sende den enkelte IP-pakke til bestemmelsesstedet. I henhold til artikel 6, stk. 1 og stk. 2, i e-databeskyttelsesdirektivet er det tilladt at behandle trafikdata med henblik på overførsel af kommunikation. Internetudbyderne kan således behandle oplysninger, der er nødvendige for levering af tjenesten.

ii) Retligt grundlag for beskyttelse af tjenesten

41. I henhold til artikel 4 i e-databeskyttelsesdirektivet skal en internetudbyder træffe passende foranstaltninger for at beskytte sine tjenester. Filtrering af virus kan indebære behandling af IP-headere og IP-payload. I henhold til artikel 4 i e-databeskyttelsesdirektivet skal internetudbyderne sikre netsikkerheden, og denne bestemmelse legimiterer således inspektionsteknikker baseret på IP-headere og indhold, der udelukkende har dette ene formål. Det betyder i praksis at internetudbyderne inden for rammerne af proportionalitetsprincippet (se afsnit V.3) kan overvåge og filtrere kommunikationsdata med henblik på at bekæmpe virus og sikre netsikkerheden generelt ([27]).

([26]) Betragtning 10 i e-databeskyttelsesdirektivet har følgende ordlyd: »I den elektroniske kommunikationssektor finder direktiv 95/46/EF navnlig anvendelse på alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder, som ikke særligt er omfattet af bestemmelserne i dette direktiv, herunder den registeransvarliges forpligtelser og fysiske personers rettigheder.« Betragtning 17 er også relevant i relation til den registreredes samtykke. »I dette direktiv bør samtykke givet af en bruger eller en abonnent, hvad enten sidstnævnte er en fysisk eller en juridisk person, have samme betydning som den registreredes samtykke, således som defineret og yderligere fastlagt i direktiv 95/46/EF«.

([27]) Udtalelse fra Artikel 29-Gruppen 2/2006 om beskyttelse af privatlivets fred i relation til tilrådighedsstillelse af e-mailscreeningtjenester vedtaget den 21. februar 2006 (WP 118). I denne udtalelse giver gruppen udtryk for den opfattelse, at anvendelse af filtre med henblik på artikel 4 kan være foreneligt med artikel 5 i direktivet om databeskyttelse inden for elektronisk kommunikation.

iii) Retligt grundlag for minimering af virkningerne af overbelastning

42. Rationalet bag dette retlige grundlag er anført i betragtning 22 i e-databeskyttelsesdirektivet, hvori der redegøres for forbuddet mod lagring af kommunikationsdata i artikel 5, stk. 1. Forbuddet omfatter ikke enhver automatisk, midlertidig og kortvarig lagring, når blot lagringen udelukkende sker med henblik på gennemførelse af transmissionen, og oplysningerne ikke lagres længere end det tidsrum, der er nødvendigt for transmissionen og af hensyn til trafikstyringen, og kommunikationshemmeligheden fortsat er garanteret.

43. I tilfælde af overbelastning er spørgsmålet, om internetudbyderne må overveje at droppe eller forsinke vilkårlig trafik eller snarere forsinke kommunikation, der ikke er tidsfølsom, f.eks. P2P eller e-mailtrafik, således at f.eks. telefontrafik kan passere i en acceptabel kvalitet.

44. Da det er i samfundets overordnede interesse at sikre et brugbart kommunikationsnet, kan internetudbyderne anføre, at prioritering eller neddrosling af trafik for at forhindre overbelastning er en legitim foranstaltning og en forudsætning for levering af en tilstrækkelig tjeneste. I disse tilfælde og med dette formål er der således et generelt retligt grundlag for behandling af personoplysninger, og det er således ikke nødvendigt at indhente brugernes specifikke samtykke.

45. Muligheden for at gribe ind på denne måde er imidlertid ikke ubegrænset. Hvis internetudbyderne ønsker at inspicere meddelelser, skal de af fortrolighedshensyn og i fuld overensstemmelse med proportionalitetsprincippet anvende den mindst intrusive tilgængelige metode til opfyldelse af formålet (og således undgå deep packet inspection) og kun så længe som nødvendigt for at forhindre overbelastning.

iv) Retligt grundlag for behandling af data til andre formål

46. Internetudbyderne kan også have et ønske om at inspicere trafik- og indholdsdata til andre formål, f.eks. for at tilbyde særlige abonnementer (f.eks. et abonnement, der begrænser adgangen til P2P, eller et abonnement, der øger hastigheden for visse applikationer). Inspektion og yderligere brug af trafik- og kommunikationsdata til andre formål end at levere eller beskytte tjenesten og forhindre overbelastning er kun tilladt under overholdelse af strenge betingelser i overensstemmelse med den retlige ramme.

47. Den retlige ramme er primært artikel 5, stk. 1, i e-databeskyttelsesdirektivet, der omfatter et forbud mod aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges, uden at de pågældende brugere har indvilget heri. Det betyder i praksis, at de brugere, der er involveret i en kommunikation, skal give samtykke af hensyn til legitimeringen af behandlingen af trafik- og kommunikationsdata i henhold til artikel 5, stk. 1.

48. Som forklaret ovenfor er anvendelsen af inspektions- og filtreringsteknikker enten baseret på IP-headere, der er trafikdata, eller på deep packet inspection, der også omfatter IP-payload og er kommunikationsdata. Anvendelsen af disse teknikker til andre formål end levering af tjenesten eller beskyttelse af sikkerheden er derfor i princippet forbudt, medmindre der er et legitimt grundlag for behandlingen som f.eks. samtykke (artikel 5, stk. 1). Artikel 5, stk. 1, finder f.eks. anvendelse, når en internetudbyder beslutter at tilbyde kunder en reduceret takst for internetadgang, hvis de pågældende kunder indvilger i at modtage adfærdsbaserede reklamer, og der i denne forbindelse foretages deep packet inspection og således gøres brug af kommunikationsdata. I henhold til artikel 5, stk. 1, skal der således indhentes et frit givet, specifikt og informeret samtykke.

49. Artikel 6 i e-databeskyttelsesdirektivet med titlen »Trafikdata« indeholder en række specifikke bestemmelser om trafikdata. Det anføres navnlig, at internetudbyderne kan behandle trafikdata med henblik på

levering af tillægstjenester ([28]), hvis abonnenten giver sit samtykke hertil. I denne bestemmelse præciseres kravet om samtykke i artikel 5, stk. 1, i forbindelse med trafikdata.

50. I praksis er det ikke altid nemt at vurdere, i hvilke tilfælde samtykke f.eks. er påkrævet, og i hvilke tilfælde hensynet til netsikkerheden kan legitimere behandlingen, navnlig hvis inspektionsteknikkerne har to formål (f.eks. at undgå overbelastning og levere tillægstjenester). Det skal understreges, at indhentning af samtykke ikke kan betragtes som en nem og systematisk udvej, der sikrer overholdelsen af principperne om databeskyttelse.

51. Der er kun få erfaringer med anvendelsen af lovgivningen, herunder navnlig med de forskellige aspekter, der er blevet redegjort for ovenfor. Det er meget vigtigt at udstikke yderligere retningslinjer på dette område, hvilket der redegøres nærmere for i afsnit VI. Der er desuden en række yderligere relevante aspekter vedrørende indhentning af samtykke, som også kræver særlig opmærksomhed. Disse aspekter beskrives nedenfor.

V.2. **Informeret samtykke som et retligt grundlag**

52. Det samtykke, der kræves i henhold til artikel 5 og 6 i e-databeskyttelsesdirektivet, har samme betydning som den registreredes samtykke, således som defineret og yderligere fastlagt i direktiv 95/46/EF ([29]). I henhold til artikel 2, litra h), i e-databeskyttelsesdirektivet er »den registreredes samtykke« »enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.« Artikel 29-Gruppen har behandlet spørgsmålet om samtykke og betingelserne for dets gyldighed i sin udtalelse 15/2011 om definitionen af samtykke ([30]).

53. Internetudbydere, der skal indhente samtykke forud for inspektion og filtrering af trafik- og indholdsdata, skal derfor sikre, at samtykket er frit givet og specifikt, og det skal være en fuldt informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling. Dette understreges i betragtning 17 i e-databeskyttelsesdirektivet »(…) Samtykke kan gives ved ethvert passende middel, der muliggør en frit givet, specifik og informeret angivelse af brugerens ønsker, herunder ved at afkrydse en rubrik, når man besøger et internetwebsted.« Nedenfor anføres en række eksempler på, hvad der forstås ved et frivilligt, specifikt og informeret samtykke i denne forbindelse.

Samtykke: frit givet, specifik og informeret viljestilkendegivelse

54. *Frit givet samtykke.* Brugerne bør ikke underlægges begrænsninger, der knytter samtykke til det internetabonnement, de ønsker at tegne.

55. Den enkelte brugers samtykke ville ikke være frit givet, hvis brugerne var tvunget til at give samtykke til overvågning af deres kommunikationsdata for at få adgang til en kommunikationstjeneste. Det ville navnlig være tilfældet, hvis *alle* udbydere på et givent marked gjorde brug af trafikstyring til andre formål end beskyttelse af netsikkerheden. Den eneste mulighed ville da være ikke at tegne et internetabonnement overhovedet. Da internettet er blevet et meget vigtigt redskab både til arbejdsformål og

([28]) I betragtning 18 anføres en række eksempler på tillægstjenester. Det er ikke klart, om betragtningen kan fortolkes således, at tjenester, der reguleres af trafikstyringspolitikker, er omfattet af listen. Trafikstyringspolitikker med fokus på bestemt indhold kan betragtes som politikker til fremme af tjenester af høj kvalitet. Trafikstyring, der udelukkende indebærer behandling af IP-headere og har til formål at tilbyde spilletjenester af høj kvalitet, hvor brugernes personlige spilletrafik prioriteres gennem net, kan f.eks. betragtes som en tillægstjeneste. Det er derimod overhovedet ikke klart, om trafikstyring med henblik på neddrosling af visser former for trafik, f.eks. P2P-trafik, kan betragtes som en tillægstjeneste.

([29]) Se betragtning 17 og artikel 2, litra f), i e-databeskyttelsesdirektivet.

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

fritidsformål, er det ikke et reelt alternativ ikke at tegne et internetabonnement. De enkelte brugere ville således ikke have et reelt valg, dvs. de ville ikke have mulighed for at give frit samtykke ([31]).

56. Det er den tilsynsførendes opfattelse, at Kommissionen og de nationale myndigheder helt klart er nødt til at overvåge markedet, navnlig for at vurdere, om dette scenarie — dvs. udbydernes sammenkobling af teletjenester og overvågning af kommunikation — er ved at blive et generelt fænomen. Udbyderne skal tilbyde alternative tjenester, herunder internetabonnement uden trafikstyring, uden yderligere omkostninger for den enkelte bruger.

57. *Specifikt samtykke*. Kravet om, at samtykket skal være specifikt, indebærer i denne forbindelse, at internetudbyderne skal indhente samtykke til overvågning af trafik- og kommunikationsdata på en klar og præcis måde. Artikel 29-Gruppen understreger følgende: »For at være specifikt skal samtykket være forståeligt. Der skal således klart og præcist henvises til databehandlingens omfang og konsekvenser. Samtykket kan ikke finde anvendelse på et uafgrænset sæt behandlingsaktiviteter. Det betyder med andre ord, at den sammenhæng, hvori samtykket finder anvendelse, er begrænset.« Det indhentede samtykke er sandsynligvis ikke specifikt, hvis samtykket til inspektion af trafik- og kommunikationsdata er bundet til et generelt samtykke om at abonnere på tjenesten. Samtykkets specifikke karakter kræver derimod, at der anvendes særlige midler til at indhente samtykke, f.eks. en formular vedrørende specifikt samtykke eller en helt særskilt rubrik vedrørende overvågning (i stedet for at inkludere oplysningerne i de generelle aftalebetingelser og stille krav om undertegnelse af aftalen, som den foreligger).

58. *Informeret samtykke*. Et samtykke skal være informeret for at være gyldigt. Kravet om forudgående tilvejebringelse af de fornødne oplysninger har ikke kun hjemmel i e-databeskyttelsesdirektivet og databeskyttelsesdirektivet, men også i artikel 20 og 21 i forsyningspligtdirektivet som ændret ved direktiv 2009/136/EF ([32]). Kravet om oplysninger og samtykke bekræftes udtrykkeligt i betragtning 28 i direktiv 2009/136/EF: »… udbyderne af tjenesten og/eller nettet (bør) under alle omstændigheder give brugerne fuldstændige oplysninger om eventuelle begrænsninger i brugen af elektroniske kommunikationstjenester. Efter udbyderens eget valg bør sådanne oplysninger beskrive den pågældende type indhold, applikation eller tjeneste eller individuelle applikationer og tjenester eller begge dele.« Herefter præciseres følgende: »Afhængigt af den anvendte teknologi og hvilken form for begrænsning der gør sig gældende, kan sådanne begrænsninger kræve brugerens samtykke, jf. direktiv 2002/58/EF.«

59. I lyset af disse overvågningsteknikkers komplekse karakter er en af de største udfordringer i forbindelse med indhentning af gyldigt samtykke at give brugerne relevant forhåndsinformation. Forbrugerne skal informeres, således at de kan forstå, hvilke oplysninger der behandles, hvordan de anvendes, hvilken indvirkning de har på brugeren, og i hvilket omfang der sker en krænkelse af privatlivets fred ved brug af disse teknikker.

60. Informationen skal således ikke blot være klar og forståelig for almindelige forbrugere — den skal også være synlig, så de ikke overser den.

61. *Viljetilkendegivelse*. I henhold til gældende lovgivning kræver samtykke også, at forbrugeren udfører en bekræftende handling for at tilkendegive sin accept. Stiltiende samtykke opfylder ikke dette krav. Dette understreger også behovet for at anvende særlige midler til at indhente samtykke, der giver internetudbyderne mulighed for at inspicere trafik- og kommunikationsdata med henblik på trafikstyring. I sin nylige udtalelse om samtykke understregede Artikel 29-Gruppen, at der er et krav om samtykkets granularitet med hensyn til databehandlingens forskellige elementer.

([31]) Et lignende tilfælde er PNR, hvor det blev drøftet, om passagerernes samtykke til overførsel af passagerlisteoplysninger til de amerikanske myndigheder var gyldigt. Gruppen mente, at passagerernes samtykke ikke kunne afgives frivilligt, når luftfartsselskaberne er forpligtede til at overføre oplysningerne inden flyets afgang, hvorfor passagererne ikke har noget reelt valg, hvis de ønsker at flyve. Udtalelse 6/2002 om videregivelse af passagerlisteoplysninger og andre oplysninger fra luftfartsselskaber til USA.

([32]) Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (se fodnote 15).

62. Det kunne anføres, at hvis parterne i kommunikationen ikke ønsker, at internetudbyderne opfanger kommunikationen til trafikstyringsformål, kan de altid kryptere kommunikationen. Denne tilgang er nyttig i praktisk henseende, men den kræver en indsats og teknisk viden, og den kan ikke sidestilles med et frit, specifikt og informeret samtykke. Anvendelsen af krypteringsteknikker sikrer ikke fuld kommunikationshemmelighed, da internetudbyderen som minimum vil kunne få adgang til IP-header-oplysningerne for at sende kommunikationen, og udbyderen vil også kunne foretage statistiske analyser.

63. I henhold til artikel 5, stk. 1, i e-databeskyttelsesdirektivet skal der indhentes samtykke fra de pågældende brugere. I mange tilfælde vil brugeren være den samme person som abonnenten, og der kan således indhentes samtykke på tidspunktet for tegning af abonnement på tjenesten. I andre tilfælde, herunder hvor der er mere end en person involveret, skal brugernes samtykke indhentes særskilt. Det kan rejse en række praktiske spørgsmål, der behandles nærmere nedenfor.

Samtykke fra alle de pågældende brugere

64. I henhold til artikel 5, stk. 1, kan samtykke anvendes til legitimering af behandlingen. Der skal indhentes samtykke fra *alle brugere*, der er involveret i en kommunikation. Begrundelsen er, at en kommunikation normalt berører mindst to personer (afsenderen og modtageren). Hvis en internetudbyder f.eks. scanner IP-payloadet i en e-mail, inspicerer denne oplysninger, der vedrører både afsenderen og modtageren af e-mailen.

65. I forbindelse med overvågning og opfangelse af trafik- og kommunikationsdata (f.eks. webtrafik) skal internetudbyderne blot indhente brugerens, dvs. abonnentens samtykke. Dette skyldes, at den anden part i kommunikationen, i dette tilfælde et besøgt websted, ikke betragtes som den »pågældende bruger« ([33]). Situationen kan imidlertid være mere kompleks, når en sådan overvågning involverer inspektion af indholdet af e-mails og således personoplysninger om afsenderen og modtageren af e-mailen, der ikke begge har indgået en aftale med den samme internetudbyder. I disse tilfælde vil internetudbyderen behandle personoplysninger (navn, e-mailadresse og potentielt følsomme indholdsdata) vedrørende personer, der ikke er deres kunder. Rent praktisk kan det være vanskeligere at indhente samtykke fra disse personer, da det skal ske med udgangspunkt i de enkelte sager og ikke ved indgåelse af aftalen om teletjenesten. Det vil heller ikke være realistisk at antage, at abonnentens samtykke også blev givet på vegne af andre brugere, hvilket ofte er tilfældet i private husholdninger.

66. I denne forbindelse mener den tilsynsførende, at internetudbyderne skal overholde eksisterende lovkrav og gennemføre politikker, der ikke involverer overvågning og inspektion af oplysninger. Det er navnlig meget vigtigt i forbindelse med kommunikationstjenester, der involverer tredjeparter, som ikke har mulighed for at give samtykke til overvågningen, navnlig af sendte og modtagne e-mails (dette gælder ikke overvågning til sikkerhedsformål).

67. Det skal samtidig bemærkes, at den nationale lovgivning til gennemførelse af artikel 5, stk. 1, i e-databeskyttelsesdirektivet ikke altid er tilstrækkelig på dette punkt, og at der generelt synes at være behov for en afklaring af kravene i e-databeskyttelsesdirektivet på dette område. Den tilsynsførende opfordrer derfor Kommissionen til at være mere aktiv på dette område og tage et initiativ, gerne med input fra tilsynsmyndighederne i Artikel 29-Gruppen og andre berørte parter. Om nødvendigt kan der indbringes en sag for Domstolen for at skabe fuld klarhed over betydningen og konsekvenserne af artikel 5, stk. 1.

([33]) Også i de tilfælde, hvor webtrafikken indebærer videregivelse af personoplysninger, f.eks. i form af billeder af identificerbare fysiske personer på et websted. Behandlingen af disse oplysninger skal være baseret på et retligt grundlag, men vil ikke være omfattet af artikel 5, stk. 1, da disse personer ikke betragtes som »de pågældende brugere«.

V.3. **Proportionalitet — dataminimeringsprincippet**

68. I artikel 6, litra c), i databeskyttelsesdirektivet fastlægges proportionalitetsprincippet ([34]), der finder anvendelse på internetudbydere, da de er registeransvarlige i henhold til dette direktiv, når de overvåger og filtrerer data.

69. I henhold til dette princip må personoplysninger kun behandles, når de er »relevante og tilstrækkelige og (må) ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles«. Anvendelsen af dette princip gør det nødvendigt at vurdere, om de anvendte midler til databehandlingen og den anvendte type personoplysninger er passende og med rimelig sandsynlighed vil opfylde formålet. Hvis det konkluderes, at der indsamles flere oplysninger end nødvendigt, er princippet ikke blevet overholdt.

70. Det skal vurderes fra sag til sag, om de forskellige former for inspektionsteknikker er i overensstemmelse med proportionalitetsprincippet. Det er ikke muligt at drage konklusioner ud fra en generel betragtning. Det er imidlertid muligt at pege på forskellige konkrete aspekter, som skal evalueres i forbindelse med vurderingen af overensstemmelsen med proportionalitetsprincippet.

71. *Mængden af behandlede oplysninger.* Overvågning af internetudbydernes kunders kommunikation på de mest dybdegående niveauer vil i de fleste tilfælde være for omfattende og ulovlig. Det forhold, at det kan ske ved anvendelse af midler, der ikke er åbenlyse for de enkelte brugere, og at det kan være vanskeligt for dem at forstå, hvad der sker, svækker beskyttelsen af privatlivets fred. Internetudbyderne skal vurdere, hvilke mindre intrusive midler der er tilgængelige for at opnå det ønskede resultat. Kan det ønskede resultat f.eks. opnås ved overvågning af IP-headere i stedet for deep packet inspection? Selv om der kun anvendes deep packet inspection, er det måske muligt at tilvejebringe de nødvendige oplysninger ved blot at identificere visse protokoller. Det kan også være relevant at anvende databeskyttelsesforanstaltninger, herunder pseudoanonymisering. Resultatet af vurderingen skal bekræfte, at databehandlingen står i rimeligt forhold til formålet.

72. *Behandlingens konsekvenser (direkte forbundet med formålet).* Det er ikke i overensstemmelse med proportionalitetsprincippet, hvis internetudbyderne gør brug af trafikstyringspolitikker, der udelukker adgangen til visse tjenester, uden at brugerne får rimelig andel i de fordele, som er forbundet hermed.

73. Det er også vigtigt at understrege, at proportionalitetsprincippet fortsat finder anvendelse, selv om andre bindende lovkrav er blevet opfyldt, herunder selv om en internetudbyder f.eks. har indhentet samtykke fra den enkelte bruger til at overvåge indhold. Den databehandling, der foretages i forbindelse med overvågning af indhold, kan således stadig være ulovlig, hvis den er i strid med det grundlæggende princip om proportionalitet.

V.4. **Sikkerhedsforanstaltninger og organisatoriske foranstaltninger**

74. Artikel 4 i e-databeskyttelsesdirektivet pålægger udtrykkeligt internetudbyderne at træffe tekniske og organisatoriske foranstaltninger for at sikre, i) at kun autoriserede personer kan få adgang til personoplysninger til lovlige formål, ii) beskyttelsen af personoplysninger mod hændelig eller ulovlig behandling og iii) gennemførelsen af en sikkerhedspolitik for behandling af personoplysninger. Direktivet giver også de nationale kompetente myndigheder mulighed for at kontrollere disse foranstaltninger.

75. I henhold til artikel 4, stk. 2 og 3, i e-databeskyttelsesdirektivet skal internetudbyderne i tilfælde af et brud desuden underrette de kompetente nationale myndigheder. De skal ligeledes underrette de berørte abonnenter, hvis bruddet kan få uheldige konsekvenser for dem.

76. Behandling af personoplysninger i kommunikation til trafikstyringsformål kan give internetudbyderne adgang til data, som er endnu mere følsomme end trafikdata.

([34]) Som angivet ovenfor finder databeskyttelsesdirektivet anvendelse på alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder, som ikke specifikt er omfattet af e-databeskyttelsesdirektivet.

77. Internetudbydernes sikkerhedspolitikker skal derfor omfatte specifikke beskyttelsesforanstaltninger for at sikre, at de trufne foranstaltninger er tilstrækkelige til at imødegå disse risici. De nationale kompetente myndigheder, der kontrollerer disse foranstaltninger, skal samtidig stille strenge krav. Endelig skal det sikres, at der indføres effektive indberetningsprocedurer for at informere registrerede, hvis oplysninger er blevet kompromitteret, og som derfor kan blive negativt berørt.

VI. **FORSLAG TIL POLITISKE OG LOVGIVNINGSMÆSSIGE FORANSTALTNINGER**

78. Inspektionsteknikker baseret på trafikdata og inspektion af IP-payload, dvs. kommunikationsindhold, kan afsløre brugernes internetaktivitet: besøgte websteder og aktiviteter på disse steder, anvendelse af P2P-applikationer, downloadede filer, sendte og modtagne e-mails, afsender, emne og udtryk osv. Internetudbyderne kan have et ønske om at anvende disse oplysninger til at opprioritere nogle former for kommunikation, f.eks. video on demand. De ønsker måske at anvende dem til at identificere virus eller opbygge profiler med henblik på adfærdsbetinget reklame. Disse foranstaltninger er en krænkelse af retten til kommunikationshemmelighed.

79. Afhængigt af de anvendte teknikker og sagens særlige karakter kan det få større konsekvenser for beskyttelsen af privatlivets fred. Jo dybere opfangelsen og analysen af de indsamlede oplysninger er, desto mere vil disse teknikker være i strid med princippet om kommunikationshemmelighed. Baggrunden for overvågningen og karakteren af de indførte databeskyttelsesforanstaltninger er også af afgørende betydning for vurderingen af, i hvilket omfang retten til beskyttelse af privatlivets fred og personoplysninger er blevet krænket. Spærring og overvågning med henblik på bekæmpelse af skadelig software med strenge begrænsninger, for så vidt angår lagring og anvendelse af de inspicerede data, kan ikke sammenlignes med situationer, hvor oplysningerne logges for at opbygge profiler med henblik på adfærdsbetinget reklame.

80. Den tilsynsførende mener i princippet, at den eksisterende EU-lovgivning om beskyttelse af privatlivets fred og databeskyttelse i tilstrækkelig grad garanterer, at retten til fortrolighed opretholdes, og at beskyttelsen af privatlivets fred og personoplysninger generelt ikke bringes i fare ([35]). Internetudbyderne bør ikke anvende sådanne mekanismer, medmindre de har anvendt lovgivningen korrekt. Internetudbyderne bør navnlig tage hensyn til og respektere følgende relevante elementer i lovgivningen:

— Internetudbyderne kan anvende trafikstyringspolitikker med henblik på at beskytte en tjeneste og levere en tjeneste, herunder forhindre overbelastning, i henhold til artikel 4 og 6 i e-databeskyttelsesdirektivet.

— Internetudbyderne skal have et specifikt retligt grundlag, og eventuelt brugernes samtykke, for at anvende trafikstyringspolitikker, der indebærer behandling af trafik- og/eller kommunikationsdata til andre formål end ovennævnte. Brugernes informerede samtykke er f.eks. nødvendigt for at overvåge og filtrere den enkelte brugers kommunikation med henblik på at begrænse (eller tillade) adgang til visse applikationer og tjenester som f.eks. P2P eller VoIP.

— Et samtykke skal være frivilligt, specifikt og informeret. Det skal gives gennem en bekræftende handling. I disse krav lægges der stor vægt på nødvendigheden af at øge bestræbelserne på at sikre, at de enkelte brugere underrettes behørigt på en direkte, forståelig og specifik måde, således at de kan vurdere konsekvenserne af denne praksis og i sidste ende træffe en informeret beslutning. I lyset af disse teknikkers komplekse karakter er en af de største udfordringer i forbindelse med indhentning af gyldigt samtykke at give brugerne relevante forhåndsoplysninger. Der må desuden ikke være nogen skadelige konsekvenser (herunder finansielle omkostninger) for brugere, der ikke giver samtykke til overvågning.

([35]) Dette betyder ikke, at der ikke er behov for lovændringer af andre årsager, navnlig i forbindelse med den generelle gennemgang af EU's retlige ramme for databeskyttelse, med henblik på at gøre den mere effektiv i lyset af nye teknologier og globaliseringen.

— Proportionalitetsprincippet spiller en afgørende rolle, når internetudbyderne anvender trafikstyringspolitikker, uanset det retlige grundlag for behandlingen og formålet, dvs. at levere tjenesten, undgå overbelastning eller tilbyde særlige abonnementer med eller uden adgang til visse tjenester og applikationer. Dette princip begrænser internetudbydernes mulighed for at foretage overvågning af indholdet af den enkeltes kommunikation, som indebærer behandling af for mange oplysninger, eller som kun indebærer fordele for internetudbyderne. Hvad der rent logistisk kan foretages af internetudbyderne vil afhænge af teknikkernes intrusive karakter, de ønskede resultater (som de kan drage fordel af) og navnlig de trufne specifikke foranstaltninger til beskyttelse af privatlivets fred og databeskyttelse. Internetudbyderne skal vurdere, om inspektionsteknikkerne er i overensstemmelse med proportionalitetsprincippet, inden de tages i brug.

81. Den nuværende retlige ramme omfatter en række relevante betingelser og beskyttelsesbestemmelser, men der skal navnlig fokus på, om internetudbyderne rent faktisk opfylder lovkravene, om de giver forbrugerne den nødvendige information, således at de kan træffe meningsfulde beslutninger, og om de overholder proportionalitetsprincippet. På nationalt niveau omfatter de kompetente myndigheder på dette område de nationale telekommunikationsmyndigheder og de nationale databeskyttelsesmyndigheder. På EU-plan omfatter de relevante EU-organer BEREC. Den tilsynsførende kan også spille en rolle i denne forbindelse.

82. I lyset af den relativt nye mulighed for massiv realtidsinspektion af kommunikation er det nødvendigt at foretage en grundigere analyse og afklare en række aspekter vedrørende anvendelsen af den retlige ramme, der er blevet behandlet i denne udtalelse, ud over at overvåge graden af overholdelse. En række retningslinjer er af særlig relevans på flere områder:

— Ved bestemmelse af, hvilke inspektionsteknikker der kan anvendes legitimt til at sikre en glidende trafikafvikling, og som ikke kræver brugernes samtykke, f.eks. bekæmpelse af spam. Ud over overvågningens intrusive karakter er aspekter som f.eks. graden af forstyrrelse af en normalt glidende trafikafvikling relevante.

— Ved bestemmelse af, hvilke inspektionsteknikker der kan anvendes til sikkerhedsformål, og som ikke kræver brugernes samtykke.

— Ved bestemmelse af, hvornår overvågning kræver den enkelte brugers samtykke, navnlig alle de pågældende brugeres samtykke, og de tilladte tekniske parametre for at sikre, at inspektionsteknikken ikke indebærer behandling af data, som ikke står i rimeligt forhold til formålet.

— I de tre ovennævnte tilfælde kan der desuden være behov for retningslinjer for anvendelsen af de nødvendige databeskyttelsesforanstaltninger (formålsbegrænsning, sikkerhed osv.).

83. Da dette område henhører under både medlemsstaternes og EU's kompetence, mener den tilsynsførende, at det er afgørende at udveksle synspunkter og erfaringer for at finde frem til en harmoniseret tilgang på ovennævnte område. Den tilsynsførende foreslår i denne forbindelse, at der etableres en platform eller nedsættes en ekspertgruppe med deltagelse af repræsentanter for de nationale tilsynsmyndigheder, Artikel 29-Arbejdsgruppen, den tilsynsførende og BEREC. Det første mål for denne platform skal være at udarbejde retningslinjer, som minimum vedrørende ovennævnte aspekter, for at sikre en solid og harmoniseret tilgang og lige vilkår. Den tilsynsførende opfordrer Kommissionen til at stå for dette initiativ.

84. Sidst, men ikke mindst, skal de nationale myndigheder samt deres modparter i EU, herunder BEREC og Europa-Kommissionen, holde nøje øje med markedsudviklingen på dette område. I relation til databeskyttelse og beskyttelse af privatlivets fred er et scenarie, hvor internetudbyderne rutinemæssigt anvender trafikstyringspolitikker og tilbyder abonnementer baseret på filtrering af adgang til indhold og applikationer, yderst problematisk. Hvis dette sker en dag, skal der indføres lovgivning for at rette op på denne situation.

VII. **KONKLUSIONER**

85. Internetudbydernes stigende brug af overvågning og inspektionsteknikker indvirker på netneutraliteten og kommunikationshemmeligheden. Dette rejser alvorlige problemer i relation til beskyttelsen af brugernes privatliv og personoplysninger.

86. Selv om Kommissionen kortfattet berører disse problemer i sin meddelelse om det åbne internet og netneutraliteten i Europa, er det den tilsynsførendes opfattelse, at der bør gøres en større indsats for at nå frem til en tilfredsstillende politik om den fremtidige udvikling. Den tilsynsførende har derfor med denne udtalelse bidraget til den igangværende politiske debat om netneutralitet, navnlig aspekter vedrørende databeskyttelse og beskyttelse af privatlivets fred.

87. Den tilsynsførende mener, at de nationale myndigheder og BEREC skal overvåge markedssituationen. Denne overvågning skal give et klart overblik over, om markedet går i retning af massiv realtidsinspektion af kommunikation, og af problemer i forbindelse med overholdelse af lovgivningen.

88. Overvågningen af markedet bør ledsages af en yderligere analyse af konsekvenserne af ny praksis i relation til databeskyttelsen og beskyttelsen af privatlivets fred på internettet. I denne udtalelse redegøres der for en række områder, som bør afklares. Selv om EU-agenturer og -organer som BEREC, Artikel 29-Gruppen og den tilsynsførende har et godt udgangspunkt for at afklare betingelserne for anvendelse af lovgivningen, mener den tilsynsførende, at det er Kommissionens opgave at koordinere og styre debatten. Med henblik på at sikre denne afklaring opfordrer den tilsynsførende derfor Kommissionen til at tage et initiativ og inddrage alle disse berørte parter i en platform eller en arbejdsgruppe. Der skal bl.a. foretages en yderligere analyse af følgende aspekter:

— Bestemmelse af, hvilke inspektionsteknikker der kan anvendes legitimt til at sikre en glidende trafikafvikling, og som kan anvendes til sikkerhedsformål.

— Bestemmelse af, hvornår overvågning kræver den enkelte brugers samtykke, navnlig alle de pågældende brugeres samtykke, og de tilladte tekniske parametre for at sikre, at inspektionsteknikken ikke indebærer behandling af data, som ikke står i rimeligt forhold til formålet.

— I ovennævnte tilfælde kan der desuden være behov for retningslinjer for anvendelsen af de nødvendige databeskyttelsesforanstaltninger (formålsbegrænsning, sikkerhed osv.).

89. Afhængigt af resultaterne kan det blive nødvendigt at træffe lovgivningsmæssige foranstaltninger. I så fald skal Kommissionen forelægge forslag til politiske foranstaltninger rettet mod at styrke den retlige ramme og sikre retssikkerheden. De nye foranstaltninger skal afklare de praktiske konsekvenser forbundet med princippet om netneutralitet, hvilket allerede er sket i nogle medlemsstater, og sikre, at brugerne kan træffe et reelt valg, navnlig ved at tvinge internetudbyderne til at tilbyde uovervågede forbindelser.

Udfærdiget i Bruxelles, den 7. oktober 2011.

Peter HUSTINX

Tilsynsførende for Databeskyttelse