I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese toezichthouder voor gegevensbescherming over netneutraliteit, beheer van verkeersstromen en bescherming van de persoonlijke levenssfeer en persoonsgegevens

(2012/C 34/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16,

Gezien het Handvest van de grondrechten van de Europese Unie, en met name artikelen 7 en 8,

Gezien Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([1]),

Gezien Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens ([2]), en met name artikel 41, lid 2,

Gezien Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ([3]),

BRENGT HET VOLGENDE ADVIES UIT:

I. **INLEIDING**

I.1. **Achtergrond**

1. Op 19 april 2011 heeft de Commissie een mededeling over het open internet en netneutraliteit in Europa ([4]) goedgekeurd.

2. Dit advies kan worden beschouwd als de reactie van de EDPS op deze mededeling en is bedoeld als bijdrage aan het lopende beleidsdebat binnen de EU over netneutraliteit, vooral over aspecten in verband met gegevensbescherming en privacy.

([1]) PB L 281 van 23.11.1995, blz. 31, de „richtlijn gegevensbescherming".
([2]) PB L 8 van 12.1.2001, blz. 1, de „verordening gegevensbescherming".
([3]) PB L 201 van 31.7.2002, blz. 37, als gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (vgl. voetnoot 15), de „richtlijn e-privacy".
([4]) COM(2011) 222 definitief.

3. Het advies bouwt voort op het antwoord ([5]) dat de EDPS heeft gegevens tijdens de openbare raadpleging van de Commissie over het open internet en netneutraliteit in Europa, die voorafging aan de mededeling van de Commissie. De EDPS heeft ook kennisgenomen van de recente ontwerpconclusies van de Raad betreffende netneutraliteit ([6]).

I.2. **Het begrip netneutraliteit**

4. Netneutraliteit verwijst naar een debat over de vraag of het internetaanbieders (*Internet Service Providers* — „ISP's ([7])") moet zijn toegestaan de toegang tot internet te beperken, filteren of blokkeren, of anderszins de prestaties van internet te beïnvloeden. Het begrip netneutraliteit komt voort uit de visie dat informatie op internet onpartijdig moet worden doorgegeven, ongeacht de inhoud, bestemming of bron, en dat de gebruikers moeten kunnen beslissen welke toepassingen, diensten en apparatuur zij willen gebruiken. Dit betekent dat ISP's niet naar eigen goeddunken de toegang tot bepaalde toepassingen, zoals peer-to-peer („P2P") en dergelijke, voorrang kunnen geven of mogen vertragen ([8]).

5. Het filteren, blokkeren en controleren van netwerkverkeer roept belangrijke, vaak genegeerde of terzijde geschoven vragen op ten aanzien van de vertrouwelijkheid van de communicatie en de eerbiediging van de privacy en persoonsgegevens van internetgebruikers. Bij bepaalde controletechnieken wordt bijvoorbeeld toezicht gehouden op de inhoud van communicatie, bezochte websites, verzonden en ontvangen e-mails, de tijden waarop dit alles plaatsvindt, enzovoort, waardoor filteren van de communicatie mogelijk is.

6. Met de controle van communicatiegegevens kunnen ISP's inbreuk maken op de vertrouwelijkheid van de communicatie, een grondrecht dat wordt gewaarborgd door artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (het „EVRM") en artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (het „Handvest"). De vertrouwelijkheid wordt verder beschermd in afgeleide EU-wetgeving, te weten artikel 5 van de richtlijn e-privacy.

I.3. **Focus en structuur van het advies**

7. De EDPS is van mening dat bij een serieuze beleidsdiscussie over netneutraliteit moet worden ingegaan op de vertrouwelijkheid van de communicatie en andere gevolgen voor de privacy en gegevensbescherming.

8. Dit advies is een bijdrage aan de lopende discussie in de EU. Het heeft een drieledig doel:

— het vestigt de aandacht op de relevantie van privacy- en gegevensbescherming in de huidige discussies over netneutraliteit. Meer in het bijzonder belicht het de noodzaak om de bestaande regels inzake de vertrouwelijkheid van communicatie te eerbiedigen. Alleen praktijken die met dergelijke regels in overeenstemming zijn, dienen te worden toegelaten;

— netneutraliteit heeft betrekking op betrekkelijk nieuwe — technologische — mogelijkheden en er is weinig ervaring met de toepassing van het wettelijk kader. Daarom bevat dit advies richtlijnen voor de wijze waarop ISP's het wettelijk kader voor gegevensbescherming moeten toepassen en eerbiedigen als zij betrokken zijn bij het filteren, blokkeren en controleren van netwerkverkeer. Deze zouden van nut moeten zijn voor ISP's en ook voor instanties die zijn belast met de handhaving van het wettelijk kader;

— binnen het domein van gegevensbescherming en privacy wordt in dit advies gewezen op aspecten die speciale aandacht verdienen en wellicht optreden van de EU vereisen. Dit is vooral van belang in het licht van de lopende discussie op EU-niveau en de beleidsmaatregelen die in dit verband door de Commissie kunnen worden geïntroduceerd.

([5]) In zijn antwoord benadrukte de EDPS hoe belangrijk het is om naast andere bestaande rechten en waarden ook aspecten van gegevensbescherming en privacy in aanmerking te nemen. Het antwoord is beschikbaar op http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

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

([7]) Dit omvat het aanbieden van zowel vaste als mobiele internettoegang.

([8]) ISP's mogen wel beperkingen opleggen aan de overdrachtssnelheid of de hoeveelheid informatie die een abonnee kan verzenden of ontvangen in het geval van abonnementen met bandbreedte- of volumebegrenzing. Derhalve zouden ISP's op grond van het netneutraliteitsbeginsel nog steeds abonnementen met beperkte toegang tot internet op basis van criteria als snelheid of volume mogen aanbieden, mits daarbij niet wordt gediscrimineerd op grond van inhoud.

9. De EDPS is zich ervan bewust dat netneutraliteit ook andere vragen opwerpt, die in het vervolg worden beschreven, bijvoorbeeld in verband met de toegang tot informatie. Deze vragen komen alleen aan de orde voor zover ze verband houden met of gevolgen hebben voor gegevensbescherming en privacy.

10. Dit advies is als volgt gestructureerd. In hoofdstuk II wordt eerst een kort overzicht gegeven van filterpraktijken bij ISP's. In hoofdstuk III wordt het wettelijk kader van de EU inzake netneutraliteit geschetst. Hoofdstuk IV vervolgt met een technische beschrijving en een beoordeling van de implicaties voor de privacy, afhankelijk van de gebruikte techniek. In hoofdstuk V worden de praktische details in verband met de toepassing van het huidige EU-kader voor privacy- en gegevensbescherming geanalyseerd. Op basis van de analyse bevat hoofdstuk VI suggesties voor verdere beleidsontwikkeling en worden de gebieden aangeduid waarop verduidelijking en verbetering van het wettelijk kader nodig zouden kunnen zijn. Hoofdstuk VII bevat de conclusies.

II. **NETNEUTRALITEIT EN BELEID VOOR VERKEERSSTROOMBEHEER**

Toenemend gebruik van beleid voor verkeersstroombeheer

11. ISP's hebben zich van oudsher slechts op beperkte schaal beziggehouden met het bewaken en beïnvloeden van het netwerkverkeer. Zo hebben ze controletechnieken en beperking van informatiestromen toegepast om de beveiliging van het netwerk in stand te houden, bijvoorbeeld ter bestrijding van virussen. Daardoor heeft internet in het algemeen kunnen groeien met behoud van een grote mate van neutraliteit.

12. De laatste jaren hebben bepaalde ISP's echter belangstelling getoond voor controles van het netwerkverkeer om hun beleid te differentiëren, bijvoorbeeld om sommige diensten te blokkeren of voorrang te geven aan andere. Deze tendens wordt wel „beleid voor verkeersstroombeheer" („traffic management policies") genoemd ([9]).

13. ISP's hebben vele redenen om het verkeer te controleren en te differentiëren. Beleid voor verkeersstroombeheer kan ISP's bijvoorbeeld helpen hun verkeer te beïnvloeden in perioden met grote congestie door bepaald tijdgevoelig verkeer, zoals videokanalen, voorrang te geven en andere soorten verkeer die minder tijdgevoelig zijn, zoals P2P, te vertragen ([10]). Verder kan verkeersstroombeheer een middel zijn waarmee ISP's potentiële inkomstenbronnen aanboren. Enerzijds kunnen ISP's vergoedingen aan aanbieders van inhoud vragen, bijvoorbeeld aan degenen wier diensten meer bandbreedte vereisen, in ruil voor voorrang (en dus snelheid). Dit zou betekenen dat het aanroepen van een bepaalde dienst, zoals video op afroep, sneller verloopt dan het aanroepen van een soortgelijke dienst waarmee geen overeenkomst voor snellere overdracht is gesloten. Inkomsten kunnen ook worden verkregen van abonnees die een hogere (of lagere) bijdrage willen betalen voor bepaalde soorten abonnementen. Zo zou een abonnement zonder toegang tot P2P goedkoper kunnen zijn dan een abonnement met onbeperkte toegang.

14. Naast de redenen die ISP's zelf kunnen hebben voor toepassing van een beleid voor verkeersstroombeheer, kunnen ook andere partijen daarbij belang hebben. Als ISP's hun netwerken beheren en zich bezighouden met controles van de inhoud die door hun faciliteiten wordt overgedragen, verhogen ze waarschijnlijk hun vermogen om vermeend onwettig gebruik, bijvoorbeeld inbreuken op het auteursrecht of pornografisch gebruik, te constateren.

([9]) Zie bijvoorbeeld het rapport van OFCOM getiteld „Site blocking to reduce online copyright infringement" van 27 mei 2011, beschikbaar op http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf „Sommige ISP's passen al systemen voor „packet inspection" in hun netwerk toe voor verkeersstroombeheer en andere doeleinden; we nemen daarom aan dat dit beheer uitvoerbaar is, zij het dat het veel complexiteit en kosten met zich meebrengt voor wie nog niet van dergelijke diensten gebruikmaakt. Wellicht dat gezien de vereiste kapitaalinvesteringen DPI op korte tot middellange termijn alleen kan worden ingezet door de grotere ISP's".

([10]) De kwaliteit van onvertraagde toepassingen zoals videokanalen is onder andere afhankelijk van de latentie, d.w.z. vertraging, bijvoorbeeld als gevolg van netwerkcongestie.

Andere belangen die in het geding zijn, waaronder gegevensbescherming en privacy

15. Deze trend heeft een discussie op gang gebracht over de rechtmatigheid van dit soort praktijken en met name over de vraag of specifieke verplichtingen inzake netneutraliteit nader moeten worden uitgewerkt in wetgeving.

16. Toenemend gebruik van beleid voor verkeersstroombeheer door ISP's zou mogelijk de toegankelijkheid van informatie kunnen beperken. Als dit gedrag de norm wordt en het voor gebruikers onmogelijk (of heel duur) wordt om toegang te krijgen tot het hele internet zoals wij dat kennen, zou dat een gevaar betekenen voor de toegankelijkheid van informatie en de mogelijkheid voor gebruikers om de door hen gewenste inhoud te verzenden en te ontvangen met de toepassingen of diensten van hun keuze. Met een wettelijk verplicht beginsel van netneutraliteit wordt dit probleem wellicht vermeden.

17. Dit brengt de EDPS tot de gevolgen voor de gegevensbescherming en de privacy wanneer ISP's zich bezighouden met verkeersstroombeheer, meer in het bijzonder tot de volgende overwegingen:

— wanneer ISP's verkeersgegevens verwerken met als enige doel het kanaliseren van de informatiestroom van de verzender naar de ontvanger, verwerken zij in het algemeen slechts op beperkte schaal persoonsgegevens ([11]). Zoals een postdienst de informatie op de envelop van een brief verwerkt, zo verwerkt de ISP de informatie die nodig is om de communicatie tot de ontvanger te richten. Dit is niet strijdig met de wettelijke verplichtingen inzake gegevensbescherming, privacy en vertrouwelijkheid van communicatie;

— wanneer ISP's echter communicatiegegevens controleren om de communicatiestromen te differentiëren en daarop een specifiek beleid toe te passen, hetgeen voor bepaalde personen nadelig kan zijn, zijn de gevolgen van groter belang. Afhankelijk van de specifieke omstandigheden en van de soort analyse die wordt uitgevoerd, kan de verwerking in hoge mate inbreuk maken op iemands privacy en de vertrouwelijkheid van zijn persoonsgegevens. Dit is des te sterker het geval wanneer het beheersbeleid de inhoud van individuele internetcommunicatie aan het licht brengt, waaronder verzonden en ontvangen e-mails, bezochte websites, gedownloade of geüploade bestanden, enz.

III. **HET WETTELIJK KADER VAN DE EU VOOR NETNEUTRALITEIT EN VERDERE BELEIDSONTWIKKELINGEN**

III.1. **Het wettelijk kader in een notendop**

18. Tot 2009 bevatten de wetgevingsinstrumenten van de EU geen bepalingen waarin het ISP's uitdrukkelijk verboden werd zich toe te leggen op het filteren of blokkeren of duurder maken voor abonnees van de toegang tot hun diensten. Ze bevatten echter ook geen bepalingen waarin deze praktijken uitdrukkelijk erkend werden. De situatie was tot op zekere hoogte onzeker.

19. Het telecompakket van 2009 bracht hierin verandering met bepalingen ten gunste van de openheid van internet. Zo worden in artikel 8, lid 4, van de richtlijn inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten („kaderrichtlijn") regelgevende instanties verplicht de mogelijkheden voor eindgebruikers te bevorderen om zich toegang te verschaffen tot de inhoud, toepassingen of diensten van hun keuze ([12]). Deze bepaling geldt voor het netwerk als geheel, niet op het niveau van de afzonderlijke aanbieders. Ook in de recente ontwerpconclusies van de Raad over netneutraliteit wordt de noodzaak onderstreept om het open karakter van internet te handhaven ([13]).

([11]) Dit is exclusief activiteiten die zijn gericht op het vergroten van de veiligheid van het netwerk en het opsporen van schadelijk verkeer alsook activiteiten die vereist zijn voor facturering en interconnectie. Eveneens uitgesloten zijn verplichtingen die voortkomen uit Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, (PB L 105 van 13.4.2006, blz. 54) („richtlijn gegevensbewaring").

([12]) Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, als gewijzigd bij Richtlijn 2009/140/EG en Verordening (EG) nr. 544/2009, (PB L 337 van 18.12.2009, blz. 37).

([13]) Zie punt 3, onder e), waar de Raad zijn erkenning uitspreekt van „de noodzaak om de openheid van internet te handhaven en tegelijkertijd te waarborgen dat het hoogwaardige diensten kan blijven bieden in een kader dat grondrechten zoals de vrijheid van meningsuiting en de vrijheid van zakendoen bevordert en respecteert" en punt 8, onder d), waar de lidstaten worden uitgenodigd „het open en neutrale karakter van internet als beleidsdoelstelling te bevorderen".

20. De universele-dienstrichtlijn ([14]) bevat meer concrete verplichtingen. In artikelen 20 en 21 worden transparantie-eisen gesteld aan beperkingen van de toegang tot en/of het gebruik van diensten en toepassingen. Ook worden minimumniveaus voor de servicekwaliteit voorgeschreven.

21. Voor praktijken van ISP's die de controle van individuele communicatie met zich meebrengen, wordt in overweging 28 van de richtlijn tot wijziging van de universele-dienstrichtlijn en de richtlijn e-privacy ([15]) onderstreept: „Afhankelijk van de gebruikte technologie en het soort van beperking, kan voor deze beperkingen de instemming van de gebruiker vereist zijn, overeenkomstig Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)". Aldus herinnert overweging 28 aan de noodzaak van instemming op grond van artikel 5, lid 1, van de richtlijn e-privacy met beperkingen op basis van bewaking van de communicatie. In hoofdstuk IV wordt de toepassing van artikel 5, lid 1, en het algemene wettelijke kader voor gegevensbescherming en privacy nader geanalyseerd.

22. Ten slotte verleent artikel 22, lid 3, van de universele-dienstrichtlijn nationale regelgevende instanties nu de bevoegdheid indien nodig minimumeisen betreffende de servicekwaliteit op te leggen aan ISP's teneinde aantasting van diensten en belemmering of vertraging van het verkeer op openbare netwerken te voorkomen.

23. Het voorgaande betekent dat op EU-niveau het streven naar een open internet breed wordt gedragen (zie artikel 8, lid 4, van de kaderrichtlijn). Dit beleidsdoel, dat voor het netwerk als geheel geldt, is echter niet rechtstreeks gekoppeld aan verboden of geboden voor afzonderlijke ISP's. Met andere woorden, een ISP zou een verkeersstroombeleid kunnen voeren dat de toegang tot bepaalde toepassingen uitsluit, mits de eindgebruikers volledig worden geïnformeerd en vrijwillig, specifiek en ondubbelzinnig hun instemming betuigen.

24. De situatie kan van lidstaat tot lidstaat verschillen. In sommige lidstaten kunnen ISP's onder bepaalde voorwaarden verkeersstroombeheer toepassen, bijvoorbeeld om toepassingen zoals VoIP te blokkeren (in het kader van een goedkoper internetabonnement), mits de betrokken abonnees hun vrijwillige, specifieke en ondubbelzinnige geïnformeerde instemming hebben gegeven. Andere lidstaten hebben gekozen voor versterking van het beginsel van netneutraliteit. Zo heeft het Nederlandse parlement in juli 2011 een wetswijziging aangenomen die aanbieders in het algemeen verbiedt om toepassingen of diensten op internet (zoals VoIP) te belemmeren of te vertragen, tenzij dat nodig is om congestie-effecten te minimaliseren, om redenen van integriteit of beveiliging, om spam te bestrijden of op gerechtelijk bevel ([16]).

III.2. **Mededeling over netneutraliteit**

25. In haar mededeling over netneutraliteit ([17]) concludeert de Europese Commissie dat de situatie dienaangaande toezicht en nadere analyse vereist. Haar beleid wordt wel getypeerd als afwachtend omdat zij nog geen verdergaande regelgevende stappen zou overwegen.

([14]) Richtlijn 2002/22/EG als gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, (PB L 337 van 18.12.2009, blz. 11). Vergelijk ook artikel 1, lid 3, waarin staat dat deze richtlijn niet voorziet in een verplichting noch in een verbod van voorwaarden die aanbieders van openbare elektronischecommunicatiediensten aan eindgebruikers opleggen, waarbij de toegang tot en/of het gebruik van diensten en toepassingen wordt beperkt, indien deze krachtens de nationale wetgeving zijn toegestaan en in overeenstemming zijn met het Gemeenschapsrecht, maar wel verplicht tot het verstrekken van informatie over dergelijke voorwaarden.

([15]) Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

([16]) Het oorspronkelijke amendement is te vinden op https://zoek.officielebekendmakingen.nl/kst-32549-A.html. De in de pers genoemde redenen voor deze beleidsoptie hielden geen verband met overwegingen van gegevensbescherming en privacy, maar met de waarborg dat gebruikers niet verstoken blijven van of slechts beperkte toegang wordt geboden tot informatie. Klaarblijkelijk is deze wijziging dus ingegeven door overwegingen betreffende de toegang tot informatie.

([17]) Vgl. voetnoot 4.

26. In de mededeling van de Commissie wordt erkend dat eventuele maatregelen en verdergaande wetgeving zou moeten worden onderworpen aan een diepgaande beoordeling van de gegevensbeschermings- en privacyaspecten. Ook in de ontwerpconclusies van de Raad worden de in het geding zijnde kwesties van gegevensbescherming en opgemerkt ([18]).

27. De vraag die vanuit het oogpunt van gegevensbescherming en privacy moet worden beantwoord, is of een afwachtend beleid voldoende is. Hoewel in het kader voor gegevensbescherming en privacy op het ogenblik wel enige waarborgen zijn voorzien, met name op grond van het beginsel van vertrouwelijkheid van de communicatie, lijkt het noodzakelijk om de mate van naleving nauwgezet te volgen en richtlijnen te verschaffen over verscheidene aspecten die niet bijzonder duidelijk zijn. Bovendien zouden enkele gedachten moeten worden ontvouwd over de wijze waarop het kader kan worden verduidelijkt en verbeterd in het licht van de technologische ontwikkelingen. Als uit het toezicht blijkt dat de markt zich ontwikkelt in de richting van massale onvertraagde controle van de communicatie en van problemen in verband met de naleving van het kader, zijn wetgevingsmaatregelen noodzakelijk. Concrete suggesties in dat verband worden gepresenteerd in hoofdstuk VI.

IV. **TECHNISCHE ACHTERROND EN DAARMEE SAMENHANGENDE GEVOLGEN VOOR PRIVACY- EN GEGEVENSBESCHERMING**

28. Voordat we dieper op het onderwerp ingaan, is het van belang een beter inzicht te hebben in de controletechnieken die ISP's kunnen toepassen om verkeersstroombeheer uit te voeren en de wijze waarop dit het beginsel van netneutraliteit kan beïnvloeden. De gevolgen voor de privacy- en gegevensbescherming van dergelijke technieken verschillen aanmerkelijk en zijn afhankelijk van de toegepaste techniek(en). Deze technische achtergrond is nodig om het in hoofdstuk V beschreven wettelijk kader voor gegevensbescherming te kunnen begrijpen en correct te kunnen toepassen. Daarbij moet echter worden aangetekend dat dit een voortdurend veranderend en complex terrein is. De onderstaande beschrijving beoogt daarom niet uitputtend en volledig up-to-date te zijn, maar slechts de technische informatie te verschaffen die onontbeerlijk is voor inzicht in de juridische argumentatie.

IV.1. **Informatieoverdracht via internet: basisfeiten**

29. Wanneer een gebruiker iets via internet verstuurt, wordt de overgedragen informatie verdeeld in pakketjes („packets"). Deze packets worden via het internet van de verzender naar de ontvanger overgebracht. Elk packet bevat informatie over de oorsprong en de bestemming. Daarnaast kunnen ISP's deze packets insluiten in aanvullende lagen en protocollen ([19]), die worden gebruikt om de verschillende verkeersstromen binnen het ISP-netwerk te beheren.

30. Om terug te komen op de vergelijking met gewone post, het protocol voor netwerkoverdracht is het equivalent van het in een envelop stoppen van een brief. De envelop draagt het bestemmingsadres dat wordt gelezen door de postdienst, die de brief vervolgens bezorgt. De postdienst kan gebruikmaken van aanvullende protocollen voor zijn interne zendingen om alle enveloppen te beheren, met als doel dat elke envelop de bestemming bereikt die de verzender oorspronkelijk bedoeld heeft. Analoog hieraan bestaat elk packet uit twee delen. Het eerste is de *IP payload*, die de inhoud van de communicatie bevat en het equivalent van de brief is. Deze bevat informatie die alleen aan de ontvanger is gericht. Het tweede deel is de *IP header*, die onder andere het adres van de ontvanger en de verzender bevat en het equivalent van de envelop is. Dankzij de IP header kunnen ISP's en andere intermediairs de payload van het adres van oorsprong naar het adres van bestemming leiden.

31. ISP's en andere intermediairs zorgen ervoor dat IP packets door het netwerk worden geleid via knooppunten die de informatie in de IP header lezen en vergelijken met routetabellen, en vervolgens de packets doorsturen naar het volgende knooppunt op weg naar de bestemming. Dit proces wordt op het hele netwerk uitgevoerd volgens een benadering die „best effort memoryless" (met optimale inspanning

([18]) Zie punt 4, onder e), waar de Raad spreekt van „het bestaan van zorgen, voornamelijk van de kant van consumenten en gegevensbeschermingsinstanties, ten aanzien van de bescherming van persoonsgegevens".

([19]) Zoals uitvoeriger wordt beschreven in paragraaf IV.2, versleutelen dergelijke protocollen, zoals HTTP, FTP, enz., de overgedragen informatie van begin tot eind op een overeengekomen manier zodat de bij de communicatie betrokken partijen elkaar kunnen begrijpen.

en zonder geheugen) wordt genoemd, aangezien alle packets op een knooppunt neutraal behandeld worden. Nadat ze zijn doorgestuurd naar het volgende knooppunt hoeft er verder geen informatie bewaard te worden in de router ([20]).

IV.2. **Controletechnieken**

32. Zoals hiervoor is toegelicht, lezen ISP's de IP headers om ze naar hun bestemming te leiden. Maar zoals hiervoor is geschetst, kan de analyse van het verkeer (met IP headers en IP payloads) ook voor andere doeleinden en met andere technologieën worden uitgevoerd. Nieuwe trends zouden bijvoorbeeld kunnen betekenen dat bepaalde gebruikte toepassingen, zoals P2P, worden vertraagd of dat voor andere diensten, zoals video op afroep, de snelheid juist wordt verhoogd voor abonnees die daarvoor betalen. Hoewel met alle controletechnieken *technisch gezien* packets worden gecontroleerd, maken ze in verschillende mate inbreuk op de vertrouwelijkheid. Controletechnieken zijn onder te verdelen in twee hoofdcategorieën. De ene is gebaseerd op alleen de IP header, de andere ook op de IP payload.

Op basis van de informatie in de IP header. De controle van de IP header brengt bepaalde velden aan het licht waarmee ISP's een aantal specifieke beheersmaatregelen kunnen uitvoeren om de verkeersstroom te beheren. Met deze technieken uitsluitend op basis van controle van IP headers worden gegevens die in beginsel bedoeld zijn als route-informatie voor een ander doel (te weten differentiatie van verkeersstromen) verwerkt. Door te kijken naar het IP-adres van oorsprong kan de ISP dit koppelen aan een concrete abonnee en specifieke maatregelen toepassen, bijvoorbeeld het packet langs een snellere of tragere verbinding leiden. Door te kijken naar het IP-adres van bestemming kan de ISP ook specifieke maatregelen toepassen, bijvoorbeeld de toegang tot bepaalde websites blokkeren of filteren.

Op basis van verdergaande controle. Door diepgaande packetcontrole kan de ISP toegang krijgen tot informatie die alleen bestemd is voor de ontvanger van de communicatie. Als we teruggaan naar de vergelijking met de postdienst, komt deze aanpak neer op het openen van de envelop en het lezen van de daarin gestoken brief om een analyse van de communicatie (vervat in de IP packets) uit te voeren teneinde een specifiek netwerkbeleid toe te passen. Er zijn verschillende manieren waarop deze controle kan worden uitgevoerd, die elk een andere bedreiging voor het gegevensonderwerp vormen.

— *Diepgaande packetcontrole op basis van protocolanalyse en statistische informatie*. Naast het IP-protocol, dat bedoeld is om de overdracht van gegevens via internet mogelijk te maken, zijn er aanvullende protocollen die de overgedragen informatie op een afgesproken manier coderen (voor transport, sessies, presentatie en toepassing, enz.). Doel van deze protocollen is ervoor te zorgen dat de bij de communicatie betrokken partijen elkaar kunnen begrijpen. Er zijn bijvoorbeeld protocollen die verband houden met websurfen ([21]), andere zijn bestemd voor bestandsoverdracht ([22]), enz. Controletechnieken op basis van de controle van protocollen in combinatie met statistische analyse zijn dan ook gericht op het zoeken naar specifieke patronen of vingerafdrukken die bepalen welke protocollen aanwezig zijn ([23]). Deze controletechnieken stellen de ISP's in staat om de soort communicatie (e-mail, websurfen, uploaden van bestanden) te begrijpen en in sommige gevallen om de specifieke gebruikte dienst of toepassing te identificeren, zoals bij bepaalde VoIP-communicatie waarvoor de gebruikte protocollen zeer specifiek zijn voor een concrete fabrikant of dienstverlener. Op zich kan de kennis van de soort communicatie een ISP in staat stellen concrete maatregelen voor verkeersstroombeheer toe te passen, bijvoorbeeld om webverkeer te blokkeren. Deze kennis kan ook de eerste stap zijn voor de uitvoering van nadere analyses door de ISP waarvoor volledige toegang tot de metagegevens en inhoud van de communicatie vereist is.

([20]) Desalniettemin maakt internetapparatuur gebruik van routeprotocollen die activiteiten registreren, verkeersstatistieken verwerken en informatie uitwisselen met andere netwerkapparatuur om IP packets langs het meest efficiënte pad te leiden. Wanneer een router bijvoorbeeld informatie ontvangt dat een verbinding overbelast of verbroken is, zal hij in zijn routetabel een alternatief opnemen zonder deze verbinding. Ook vermeldenswaard is het verzamelen en verwerken van informatie dat in bepaalde gevallen plaatsvindt voor factureringsdoeleinden of zelfs overeenkomstig de voorschriften van de richtlijn gegevensbewaring.

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

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

([23]) De gebruikte protocollen kunnen op verschillende manieren worden geïdentificeerd. Zo is het mogelijk om in specifieke velden in de binnenste protocollen te zoeken, bijvoorbeeld om de poorten te vinden waarmee de communicatie tot stand wordt gebracht. Een statistische karakterisering van een communicatiestroom kan ook worden afgeleid uit de analyse van bepaalde specifieke velden en de correlatie van de protocollen die gelijktijdig tussen twee IP-adressen worden gebruikt.

— *Diepgaande packetcontrole op basis van een analyse van de inhoud van de communicatie.* Ten slotte is het ook mogelijk om de metagegevens ([24]) en de inhoud van de communicatie zelf te controleren. Deze techniek houdt in dat alle IP packets van de oorspronkelijke communicatiestroom worden onderschept zodat de oorspronkelijke inhoud volledig kan worden gereconstrueerd en geanalyseerd. Om bijvoorbeeld schadelijke of illegale inhoud te detecteren, zoals virussen, kinderpornografie en dergelijke, moet de inhoud zelf worden gereconstrueerd opdat deze kan worden geanalyseerd. Hierbij moet worden aangetekend dat de communicatie soms uitdrukkelijk van begin tot eind door de betrokkenen kan worden versleuteld en dat deze praktijk verhindert dat ISP's de inhoud van de communicatie analyseren.

IV.3. **Gevolgen voor privacy- en gegevensbescherming**

33. Controletechnieken op basis van IP headers en meer in het bijzonder op basis van packetcontrole houden in dat deze gegevens worden bewaakt en gefilterd en hebben ernstige gevolgen voor de privacy- en gegevensbescherming. Ze kunnen ook in strijd zijn met het recht op de vertrouwelijkheid van communicatie.

34. Kijken in de communicatie van individuele personen heeft op zichzelf ernstige gevolgen voor de privacy en de gegevensbescherming. Maar het probleem is breder, want afhankelijk van de met de bewaking en onderschepping beoogde effecten kunnen de privacy-implicaties nog toenemen. Het is uiteraard niet hetzelfde als communicatie alleen wordt gecontroleerd om bijvoorbeeld te waarborgen dat het systeem goed werkt of als dat gebeurt om een beleid toe te passen dat gevolgen kan hebben voor personen. Wanneer met het verkeersstroom- en selectiebeleid alleen wordt getracht netwerkcongestie te vermijden, zijn er gewoonlijk geen grote gevolgen voor de individuele privacy. Met verkeersstroombeheer kan echter ook worden getracht bepaalde informatie te blokkeren of de communicatie te beïnvloeden via bijvoorbeeld gedragsgericht adverteren. In die gevallen zijn de privacy-effecten indringender. De bezorgdheid wordt groter wanneer men zich realiseert dat dit soort informatie niet voor een kleine groep wordt verzameld, maar veeleer op algemene basis, voor alle klanten van een ISP ([25]). Als alle ISP's filtertechnieken gaan toepassen, zou dat kunnen leiden tot een veralgemeniseerde bewaking van het internetgebruik. Daar komt bij dat als men zich concentreert op het type informatie dat wordt verwerkt, de risico's voor de privacy uiteraard groot zijn, omdat veel van de verzamelde informatie waarschijnlijk zeer gevoelig is en na het verzamelen beschikbaar is voor ISP's en voor degenen die bij hen informatie zoeken. Verder zou de informatie ook commercieel heel waardevol kunnen zijn. Dit vertegenwoordigt op zich al een groot gevaar voor functieverschuiving waarbij de aanvankelijke bedoelingen eenvoudig kunnen overgaan in commerciële of andere exploitatie van de verzamelde informatie.

35. De juiste toepassing van bewakings-, controle- en filtertechnieken moet in overeenstemming zijn met de geldende waarborgen voor gegevensbescherming en privacy, die grenzen stellen aan wat onder welke omstandigheden mogelijk is. Hierna volgt een overzicht van de geldende waarborgen krachtens het huidige wettelijke kader van de EU voor gegevensbescherming en privacy.

V. **TOEPASSING VAN HET WETTELIJK KADER VAN DE EU VOOR PRIVACY EN GEGEVENSBESCHERMING**

36. Het EU-kader voor gegevensbescherming is technologisch neutraal. Als zodanig bevat het geen regels voor de specifieke controletechnieken die hiervoor zijn beschreven. De richtlijn e-privacy regelt de privacy bij het aanbieden van elektronische communicatiediensten in openbare netwerken (meestal

([24]) Elk protocol heeft een aantal specifieke velden in de header die extra informatie geven over de communicatieoverdracht. Daarom worden die velden wel de metagegevens van de communicatie genoemd. Een voorbeeld van een dergelijk veld kan het gebruikte poortnummer zijn; als dat nummer 80 is, gaat het waarschijnlijk om webbrowsing als commuinicatiesoort.

([25]) Natuurlijk beperken de mogelijkheden om het verkeer te volgen zich niet tot ISP's. Ook aanbieders van advertentienetwerken zijn met behulp van cookies van derden in staat gebruikers op websites te volgen. In een recent wetenschappelijk artikel wordt bijvoorbeeld aangetoond dat Google aanwezig is op 97 van de 100 meest bezochte websites, hetgeen inhoudt dat Google gebruikers die cookies van derden niet hebben uitgeschakeld, kan volgen wanneer zij deze populaire websites bezoeken. Zie: Mika Ayenson, Dietrich James Wambach, Ashkan Soltani, Nathan Good en Chris Jay Hoofnagle, „Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning" (29 juli 2011). Beschikbaar op SSRN: http://ssrn.com/abstract=1898390 Het volgen van cookies is behandeld door de Groep gegevensbescherming artikel 29. Zie haar Advies 2/2010 over online reclame op basis van surfgedrag („behavioural advertising"), goedgekeurd op 22 juni 2010 (WP 171).

internettoegang en telefonie) ([26]) en de richtlijn gegevensbescherming regelt gegevensbescherming in het algemeen. Als geheel legt dit wettelijk kader verschillende verplichtingen op aan ISP's die verkeers- en communicatiegegevens verwerken en bewaken.

V.1. **Wettelijke grondslagen voor de verwerking van verkeers- en inhoudelijke gegevens**

37. Op grond van de wetgeving inzake gegevensbescherming vereist de verwerking van persoonsgegevens, zoals in dit geval de verwerking van verkeers- en communicatiegegevens, een toereikende wettelijke grondslag. In aanvulling op dit algemene vereiste kunnen in bepaalde gevallen specifieke eisen gelden.

38. In dit geval heeft het type persoonsgegevens dat door ISP's wordt verwerkt, betrekking op de verkeersgegevens en de inhoud van de communicatie. De inhoud van de communicatie en de verkeersgegevens worden beide beschermd door het recht op vertrouwelijkheid van correspondentie, dat wordt gewaarborgd door artikel 8 van het EVRM en artikelen 7 en 8 van het Handvest. Meer in het bijzonder schrijft artikel 5, lid 1, van de richtlijn e-privacy, getiteld „Vertrouwelijk karakter van de communicatie", de lidstaten voor in nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten te garanderen. Tegelijkertijd voorziet artikel 5, lid 1, van de richtlijn e-privacy dat de verwerking van verkeers- en communicatiegegevens door ISP's in bepaalde omstandigheden en met instemming van de gebruikers kan zijn toegestaan. Dit gebeurt door middel van een verbod op „het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1". Dit wordt hierna verder uitgewerkt.

39. Naast de toestemming van de gebruikers voorziet de richtlijn e-privacy in andere gronden waarop de verwerking door ISP's van verkeers- en communicatiegegevens rechtmatig kan zijn. De ter zake dienende wettelijke grondslagen voor verwerking houden in dit geval verband met i) het verlenen van de dienst; ii) het waarborgen van de beveiliging van de dienst en iii) de beperking van congestie. Andere mogelijke gronden voor de legitimering van een beheersbeleid op basis van verkeers- of communicatiegegevens worden hierna behandeld onder iv).

i) Wettelijke grondslagen in verband met het leveren van de dienst

40. Zoals is geïllustreerd in hoofdstuk IV, verwerken ISP's de informatie in IP headers met de bedoeling om elk IP packet naar zijn bestemming te leiden. Artikel 6, lid 1 en lid 2, van de richtlijn e-privacy staat de verwerking van verkeersgegevens ten behoeve van de communicatieoverdracht toe. ISP's mogen derhalve de informatie verwerken die nodig is om de dienst te verlenen.

ii) Wettelijke grondslagen in verband met het waarborgen van de beveiliging van de dienst

41. Op grond van artikel 4 van de richtlijn e-privacy is een ISP in het algemeen verplicht passende maatregelen te nemen om de beveiliging van zijn diensten te garanderen. Het filteren van virussen kan met zich meebrengen dat de IP headers en de IP payload worden verwerkt. Aangezien artikel 4 van de richtlijn e-privacy voorschrijft dat ISP's zorgen voor de beveiliging van hun netwerk, wettigt deze bepaling de toepassing van controletechnieken op basis van IP headers en inhoud die uitsluitend gericht zijn op het bereiken van dat doel. In de praktijk betekent dit dat ISP's, binnen de grenzen van het evenredigheidsbeginsel (zie paragraaf V.3), communicatiegegevens mogen bewaken en filteren ter bestrijding van virussen en in het algemeen ter waarborging van de netwerkbeveiliging ([27]).

([26]) In overweging 10 van de richtlijn e-privacy staat: „In de sector elektronische communicatie is Richtlijn 95/46/EG van toepassing, met name op alle aangelegenheden met betrekking tot de bescherming van fundamentele rechten en vrijheden die niet specifiek onder het bepaalde in deze richtlijn vallen, met inbegrip van de plichten van de verantwoordelijke en de rechten van personen". Ook overweging 17 is relevant ten aanzien van de toestemming van de betrokkene: „In deze richtlijn dient „toestemming van een gebruiker of abonnee", ongeacht of deze laatste een natuurlijke of rechtspersoon is, dezelfde betekenis te hebben als „toestemming van de betrokkene" zoals gedefinieerd en nader bepaald in Richtlijn 95/46/EG".

([27]) Advies 2/2006 van de Groep gegevensbescherming artikel 29 over de privacyaspecten van e-mailscreeningdiensten, goedgekeurd op 21 februari 2006 (WP 118). In dit advies wordt geoordeeld dat het gebruik van filters voor de doeleinden van artikel 4 verenigbaar kan zijn met artikel 5 van de richtlijn e-privacy.

iii) Wettelijke grondslagen in verband met de beperking van congestie-effecten

42. De idee achter deze rechtsgrondslag is te vinden in overweging 22 van de richtlijn e-privacy, waarin het verbod op de opslag van communicatiegegevens (artikel 5, lid 1) wordt toegelicht. Dit verbod geldt niet voor automatische, tussentijdse en tijdelijke opslag voor zover deze plaatsvindt met als enig doel het uitvoeren van de overdracht en deze niet langer duurt dan nodig is voor de doeleinden van overdracht en verkeersstroombeheer, en mits de vertrouwelijkheid van de communicatie gegarandeerd blijft.

43. Als er congestie optreedt, komt de vraag op of ISP's mogen overwegen verkeer willekeurig te blokkeren of te vertragen, of communicatie mogen vertragen die niet tijdgevoelig is, zoals P2P- of e-mailverkeer, waardoor bijvoorbeeld spraakverkeer met aanvaardbare kwaliteit kan doorgaan.

44. Gezien het algemeen maatschappelijk belang van het waarborgen van een bruikbaar communicatienetwerk, kunnen ISP's betogen dat het verlenen van voorrang aan of het afremmen van verkeer ter bestrijding van congestie een gerechtvaardigde maatregel is, noodzakelijk om een toereikende dienst te verlenen. Dit betekent dat in deze gevallen en voor dit doel een algemene rechtsgrond zou bestaan voor de verwerking van persoonsgegevens zonder dat specifieke instemming van de gebruikers noodzakelijk zou zijn.

45. Toch is de mogelijkheid om op deze wijze in te grijpen niet onbegrensd. Als het nodig is dat ISP's communicatie controleren, moeten zij vanuit het oogpunt van vertrouwelijkheid en met strikte inachtneming van het evenredigheidsbeginsel gebruikmaken van de minst indringende methode die beschikbaar is om hun doel te bereiken (waarbij diepgaande packetcontrole wordt vermeden) en mogen zij die slechts toepassen zolang dat noodzakelijk is om de congestie te bestrijden.

iv) Wettelijke grondslagen voor gegevensverwerking voor andere doeleinden

46. Het kan ook zijn dat ISP's verkeers- en inhoudelijke gegevens willen controleren voor andere doeleinden, bijvoorbeeld het gericht aanbieden van abonnementen (bijvoorbeeld een abonnement met beperkte toegang tot P2P of een abonnement waarbij de snelheid van bepaalde toepassingen wordt verhoogd). Controle en verder gebruik van verkeers- en communicatiegegevens voor andere doeleinden dan het verlenen van de dienst of het waarborgen van de beveiliging en het verminderen van de congestie ervan, is alleen toegestaan op strikte voorwaarden overeenkomstig het wettelijk kader.

47. Het wettelijk kader is hoofdzakelijk artikel 5, lid 1, van de richtlijn e-privacy, waarin de toestemming van de betrokken gebruikers wordt vereist voor het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens. In de praktijk betekent dit dat de toestemming van de bij de communicatie betrokken gebruikers nodig is om de verwerking van zowel verkeers- als communicatiegegevens uit hoofde van artikel 5, lid 1, te legitimeren.

48. Zoals in het voorgaande is toegelicht, is de toepassing van controle- en filtertechnieken gebaseerd op hetzij IP headers, die verkeersgegevens vormen, hetzij diepgaande packetcontroles, waarbij ook IP payloads betrokken zijn en die communicatiegegevens opleveren. Daarom is de toepassing van dergelijke technieken voor andere doeleinden dan instandhouding van de dienst of de beveiliging in beginsel verboden tenzij er een rechtsgrond bestaat voor verwerking, zoals toestemming (artikel 5, lid 1). Artikel 5, lid 1, zou bijvoorbeeld van toepassing zijn wanneer een ISP zou besluiten zijn klanten een gereduceerd tarief voor internettoegang aan te bieden in ruil voor de ontvangst van gedragsgerichte advertenties aan de hand van diepgaande packetcontrole, dus communicatiegegevens. Echte, specifieke en geïnformeerde toestemming is daarom volgens artikel 5, lid 1, noodzakelijk.

49. Verder worden in artikel 6 van de richtlijn e-privacy, getiteld „Verkeersgegevens", bepaalde regels vastgesteld die specifiek voor verkeersgegevens gelden. Meer in het bijzonder wordt voorzien in de mogelijkheid dat ISP's verkeersgegevens verwerken op basis van de toestemming van gebruikers voor de

ontvangst van diensten met toegevoegde waarde ([28]). In deze bepaling wordt de toestemmingseis gespecificeerd die in artikel 5, lid 1, is voorzien wanneer het om verkeersgegevens gaat.

50. In de praktijk is het wellicht niet altijd eenvoudig om vast te stellen in welke gevallen bijvoorbeeld toestemming noodzakelijk is en in welke gevallen de beveiliging van het netwerk een rechtvaardiging kan zijn voor de verwerking, met name als de doeleinden van de controletechnieken tweeledig zijn (bijvoorbeeld het vermijden van congestie en het aanbieden van diensten met toegevoegde waarde). Benadrukt moet worden dat toestemming niet mag worden beschouwd als een makkelijke systematische toegangspoort tot naleving van de beginselen van gegevensbescherming.

51. Er is nog weinig ervaring opgedaan met de toepassing van het kader en meer in het bijzonder met de verschillende aspecten die in het voorgaande zijn geschetst. Op dit gebied zijn nadere aanwijzingen van essentieel belang, zoals verder wordt uitgewerkt in hoofdstuk VI. Bovendien zijn er aanvullende relevante aspecten met betrekking tot het verkrijgen van toestemming die ook speciale overweging verdienen. Deze worden hierna beschreven.

V.2. **Vraagstukken met betrekking tot geïnformeerde toestemming als wettelijke grondslag**

52. De toestemming die is vereist op grond van artikelen 5 en 6 van de richtlijn e-privacy heeft dezelfde betekenis als de toestemming van de betrokkene zoals gedefinieerd en nader bepaald in Richtlijn 95/46/EG ([29]). Volgens artikel 2, onder h), van de richtlijn gegevensbescherming betekent de toestemming van de betrokkene „elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt". Recentelijk zijn de rol van de toestemming en de eisen die aan geldige toestemming gesteld worden door de Groep gegevensbescherming artikel 29 behandeld in haar Advies 15/2011 over de definitie van „toestemming" ([30]).

53. ISP's die toestemming nodig hebben om de verkeers- en communicatiegegevens te controleren en te filteren, moeten er derhalve voor zorgen dat de toestemming vrijwillig en specifiek is, en dat deze een volledig geïnformeerde aanwijzing is voor de wensen van de betrokkene, die daarmee aangeeft dat hij instemt met de verwerking van zijn of haar persoonsgegevens. In overweging 17 van de richtlijn e-privacy wordt dit bevestigd: „(…) Toestemming kan worden gegeven op elke wijze die de gebruiker in staat stelt vrijelijk een specifieke en geïnformeerde indicatie te geven omtrent zijn wensen, onder andere door bij een bezoek aan een internetwebsite op een vakje te klikken." Hierna volgen enkele praktische voorbeelden van wat het in dit verband betekent dat toestemming vrijwillig, specifiek en geïnformeerd is.

Toestemming: een vrije, specifieke en geïnformeerde indicatie van wensen

54. *Vrije toestemming*. Gebruikers mogen geen beperkingen ondervinden doordat hun toestemming wordt gekoppeld aan het internetabonnement waarvoor zij zich willen aanmelden.

55. Toestemming wordt niet vrij gegeven als men moet toestemmen in de monitoring van zijn communicatiegegevens om toegang te kunnen krijgen tot een communicatiedienst. Dit zou des te sterker gelden als *alle* aanbieders in een bepaalde markt zich zouden toeleggen op verkeersstroombeheer voor doeleinden die verder gaan dan de beveiliging van het netwerk. De enige andere optie zou dan zijn om helemaal geen abonnement op een internetdienst te nemen. Gegeven het feit dat internet een essentieel

([28]) In overweging 18 wordt een aantal voorbeelden van diensten met toegevoegde waarde opgesomd. Of diensten waarop verkeersstroombeheer wordt toegepast kunnen worden uitgelegd als onderdeel van deze opsomming, is niet duidelijk. Een beleid voor verkeersstroombeheer dat is gericht op het geven van voorrang aan bepaalde inhoud zou kunnen worden opgevat als het aanbieden van een betere kwaliteit van de dienst. Verkeersstroombeheer dat alleen de verwerking van IP headers inhoudt en bedoeld is om hoger geprijsde speldiensten aan te bieden, waarbij het persoonlijke spelverkeer van de gebruiker voorrang krijgt in het netwerk, zou bijvoorbeeld kunnen worden beschouwd als een dienst met toegevoegde waarde. Anderzijds is het verre van duidelijk of verkeersstroombeheer gericht op het afremmen van bepaalde soorten verkeer, bijvoorbeeld een lagere snelheid voor P2P-verkeer, als zodanig kan worden beschouwd.

([29]) Zie overweging 17 en artikel 2, onder f), van de richtlijn e-privacy.

([30]) Goedgekeurd op 13 juli 2011 (WP 187).

instrument is geworden voor zowel werk- als vrijetijdsdoeleinden, vormt niet-abonneren op een internetdienst geen deugdelijk alternatief. Het resultaat zou zijn dat de betrokkenen geen reële keuze zouden hebben, dat wil zeggen dat zij geen vrije toestemming zouden kunnen geven ([31]).

56. De EDPS meent dat er een duidelijke behoefte bestaat aan toezicht op de markt door de Commissie en nationale instanties, met name om vast te stellen of dit scenario — waarin aanbieders telecommunicatiediensten koppelen aan communicatiebewaking — gemeengoed wordt. Aanbieders dienen alternatieve diensten aan te bieden, waaronder een internetabonnement dat geen onderwerp van verkeersstroombeheer is, zonder abonnees hogere kosten op te leggen.

57. *Specifieke toestemming*. De noodzaak van specifieke toestemming vereist in dit geval dat ISP's op heldere en onderscheiden wijze toestemming verkrijgen voor de bewaking van verkeers- en communicatiegegevens. Volgens de Groep gegevensbescherming artikel 29 kan toestemming alleen specifiek zijn als zij begrijpelijk is: „zij moet duidelijk en exact verwijzen naar de reikwijdte en de gevolgen van de gegevensverwerking. Zij kan niet gelden voor een reeks verwerkingsactiviteiten met een open einde. Dit betekent met andere woorden dat de context waarin toestemming van toepassing is, beperkt is." Specifieke toestemming wordt waarschijnlijk niet verkregen als de toestemming voor de controle van verkeers- en communicatiegegevens wordt gebundeld met de algemene toestemming om zich voor de dienst te abonneren. In plaatst daarvan vergt specificiteit het gebruik van gerichte middelen om toestemming te verkrijgen, zoals een specifiek toestemmingsformulier of een apart vak dat duidelijk alleen maar bedoeld is voor bewaking (in plaats van de informatie op te nemen in de algemene voorwaarden van de overeenkomst en de overeenkomst als geheel te laten ondertekenen).

58. *Geïnformeerde toestemming*. Toestemming is alleen geldig als zij geïnformeerd is. De noodzaak om vooraf toereikende informatie te verstrekken komt niet alleen voort uit de richtlijnen voor e-privacy en gegevensbescherming, maar ook uit artikelen 20 en 21 van de universeledienstrichtlijn als gewijzigd bij Richtlijn 2009/136/EG ([32]). De noodzaak van informatie en toestemming is uitdrukkelijk bevestigd in overweging 28 van Richtlijn 2009/136/EG: "de gebruikers (moeten) in ieder geval volledig worden geïnformeerd over alle beperkingen die door de aanbieder van de diensten en/of de exploitant van het netwerk op het gebruik van de elektronischecommunicatiediensten worden opgelegd. Bij deze informatie moet, volgens de keuze van de aanbieder, ofwel het type van inhoud, toepassing of dienst in kwestie, ofwel de afzonderlijke toepassingen of diensten, of beide worden gespecificeerd.". Vervolgens wordt bepaald: „Afhankelijk van de gebruikte technologie en het soort van beperking, kan voor deze beperkingen de instemming van de gebruiker vereist zijn, overeenkomstig Richtlijn 2002/58/EG".

59. Gezien de complexiteit van deze bewakingstechnieken is het geven van betekenisvolle voorafgaande informatie een van de belangrijkste uitdagingen voor het verkrijgen van geldige toestemming. Consumenten dienen zodanig te worden geïnformeerd dat zij kunnen begrijpen welke informatie wordt verwerkt, hoe deze wordt gebruikt, wat de gevolgen voor de gebruikerservaring zijn en in hoeverre de privacy wordt geschonden in verband met de toegepaste technieken.

60. Dit betekent niet alleen dat de informatie zelf duidelijk en begrijpelijk moet zijn voor gemiddelde gebruikers, maar ook dat de informatie duidelijk en expliciet aan mensen wordt verstrekt zodat zij haar niet over het hoofd kunnen zien.

61. *Indicatie van wensen*. Toestemming op grond van het toepasselijke wettelijke kader vereist ook een bevestigende handeling van de gebruiker als indicatie van zijn of haar instemming. Impliciete toestemming voldoet niet aan deze norm. Dit bevestigt tevens de noodzaak van het gebruik van speciale middelen om toestemming te verkrijgen waarmee de ISP verkeers- en communicatiegegevens kan controleren in het kader van de toepassing van een beleid voor verkeersstroombeheer. In haar recente advies over toestemming benadrukt de Groep gegevensbescherming artikel 29 de noodzaak van granulariteit bij het verkrijgen van toestemming ten aanzien van de verschillende elementen waaruit de gegevensverwerking bestaat.

([31]) Een soortgelijk geval is PNR (persoonsgegevens van passagiers), waarbij discussie is ontstaan over de geldigheid van de toestemming die passagiers geven om hun gegevens over te dragen aan de Amerikaanse autoriteiten. De Groep gegevensbescherming was van mening dat de toestemming van de passagiers niet vrij kan worden gegeven omdat de luchtvaartmaatschappijen verplicht zijn de gegevens te verzenden voordat de vlucht vertrekt en de passagiers daardoor geen reële keuze hebben als zij willen vliegen (Advies 6/2002 van de Groep gegevensbescherming artikel 29 over de doorgifte van informatie over passagiers, bemanningsleden en andere gegevens door de luchtvaartmaatschappijen aan de Verenigde Staten).

([32]) Richtlijn 2009/136/EG van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten (vgl. voetnoot 15).

62. Men zou kunnen aanvoeren dat als de bij de communicatie betrokken partijen niet willen dat ISP's die communicatie onderscheppen ten behoeve van verkeersstroombeheer, zij de communicatie altijd kunnen versleutelen. Deze aanpak kan in praktische termen als nuttig worden beschouwd, maar vereist enige inspanning en technische kennis en kan daarom niet worden opgevat als gelijk aan vrije, specifieke en geïnformeerde toestemming. Ook houdt het gebruik van versleutelingstechnieken de communicatie niet volledig vertrouwelijk, aangezien de ISP in elk geval toegang krijgt tot de informatie in de IP header om de communicatie naar haar bestemming te leiden en ook in een positie verkeert om statistische analyse uit te voeren.

63. Volgens artikel 5, lid 1, van de richtlijn e-privacy moet toestemming worden verkregen van de betrokken gebruikers. In veel gevallen zal de gebruiker dezelfde persoon zijn als de abonnee, waardoor het mogelijk is toe te stemmen op het moment van abonneren op de telecommunicatiedienst. In andere gevallen, waaronder die waarbij meer dan één persoon betrokken kan zijn, zal de toestemming van de betrokken gebruikers afzonderlijk moeten worden verkregen. Dit kan praktische vragen opwerpen, zoals hierna wordt uitgewerkt.

Toestemming van alle betrokken gebruikers

64. Artikel 5, lid 1 voorziet in toestemming van de gebruiker om de verwerking te legitimeren. De toestemming moet worden verkregen van *alle gebruikers* die bij een communicatie betrokken zijn. De gedachte hierachter is dat bij elke communicatie gewoonlijk minstens twee personen (de verzender en de ontvanger) betrokken zijn. Als een ISP bijvoorbeeld IP payloads scant die betrekking hebben op een e-mail, wordt informatie gecontroleerd die zowel de verzender als de ontvanger van die e-mail betreft.

65. Wanneer ISP's verkeer en communicatie bewaken en onderscheppen (bijvoorbeeld webverkeer), kan het voor hen voldoende zijn om de toestemming van de gebruiker, dat wil zeggen de abonnee, te verkrijgen. Dat komt doordat in dit geval de andere partij in de communicatie, een bezochte website, niet kan worden beschouwd als een „betrokken gebruiker" ([33]). De situatie kan echter complexer zijn wanneer dergelijke bewaking inhoudt dat de inhoud van e-mails en daardoor ook persoonsgegevens van de verzender en de ontvanger worden gecontroleerd, terwijl ze wellicht niet beiden een contractuele relatie met dezelfde ISP hebben. In deze gevallen zou de ISP persoonsgegevens (naam, e-mailadres en mogelijk gevoelige inhoudelijke gegevens) verwerken van niet-klanten. Vanuit praktisch oogpunt kan het verkrijgen van toestemming van dergelijke personen moeilijker zijn, omdat het van geval tot geval moet gebeuren in plaats van bij het sluiten van de overeenkomst voor de telecommunicatiedienst. Ook zou het niet realistisch zijn om ervan uit te gaan dat de toestemming van de abonnee tevens is gegeven namens andere gebruikers, zoals vaak het geval kan zijn in het geval van particuliere huishoudens.

66. In dit verband meent de EDPS dat ISP's zich moeten houden aan bestaande wettelijke voorschriften en een beleid moeten uitvoeren dat geen bewaking en controle van informatie met zich meebrengt. Dit is des te essentiëler in verband met communicatiediensten waarbij derde partijen betrokken zijn die niet kunnen toestemmen in de bewaking, met name ten aanzien van verzonden en ontvangen e-mails (dit geldt niet wanneer het doel is gebaseerd op beveiligingsoverwegingen).

67. Tegelijkertijd moet worden geconstateerd dat het nationale recht waarmee uitvoering wordt gegeven aan artikel 5, lid 1, van de richtlijn e-privacy, op dit punt wellicht niet altijd bevredigend is en dat er in het algemeen behoefte lijkt te bestaan aan betere richtlijnen met betrekking tot de voorschriften van de richtlijn e-privacy in dit verband. De EDPS nodigt de Commissie daarom uit om in dit opzicht actiever te zijn en een initiatief te ontplooien dat zou kunnen profiteren van de inbreng van de toezichthoudende instanties die zijn verenigd in de Groep gegevensbescherming artikel 29 en van andere belanghebbenden. Indien nodig zou een zaak moeten worden voorgelegd aan het Hof van Justitie om volledige duidelijkheid te scheppen over de betekenis en de consequenties van artikel 5, lid 1.

([33]) Niettegenstaande die gevallen waarin het webverkeer de overdracht betreft van persoonlijke informatie, zoals bijvoorbeeld afbeeldingen van herkenbare natuurlijke personen die op een website zijn geplaatst. De verwerking van dergelijke informatie vereist een wettelijke grondslag maar valt niet onder artikel 5, lid 1, omdat die personen geen „betrokken gebruikers" zijn.

V.3. **Evenredigheid: het beginsel van gegevensminimalisatie**

68. In artikel 6, onder c), van de richtlijn gegevensbescherming is het evenredigheidsbeginsel vastgelegd ([34]), dat voor ISP's geldt omdat zij houders van persoonsgegevens zijn in de zin van deze richtlijn wanneer zij bewaking en filtering toepassen.

69. Op grond van dat beginsel mogen persoonsgegevens alleen worden verwerkt voor zover ze „toereikend, ter zake dienend en niet bovenmatig (…) zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt". De toepassing van dit beginsel brengt de noodzaak met zich mee om te beoordelen of de middelen die voor de gegevensverwerking worden ingezet en de soorten persoonsgegevens die worden gebruikt, passend zijn en redelijkerwijs mogen worden geacht tot de nagestreefde doelen te leiden. Als de conclusie is dat meer gegevens worden verzameld dan nodig is, wordt niet aan het evenredigheidsbeginsel voldaan.

70. De overeenstemming met het evenredigheidsbeginsel van bepaalde soorten controletechnieken moet van geval tot geval worden beoordeeld. Het is niet mogelijk om conclusies te trekken *in abstracto*. Wel is het mogelijk om op verschillende concrete aspecten te wijzen die moeten worden geëvalueerd om vast te stellen of het evenredigheidsbeginsel wordt nageleefd.

71. *De hoeveelheid informatie die wordt verwerkt*. Toezicht op de communicatie van ISP-klanten op de diepst mogelijke niveaus zal in de meeste gevallen buitensporig en onwettig zijn. Het feit dat dergelijk toezicht kan worden uitgevoerd met middelen waarvan de individuele gebruikers zich niet bewust zijn en dat het voor hen moeilijk te begrijpen is wat er gebeurt, verhoogt het effect op hun privacy. ISP's dienen te beoordelen welke minder indringende methoden tot hun beschikking kunnen staan om de vereiste resultaten te boeken. Kan bijvoorbeeld met bewaking van IP headers in plaats van diepgaande packetcontrole ook het vereiste resultaat worden bereikt? Zelfs bij toepassing van diepgaande packetcontrole kan de identificatie van slechts bepaalde protocollen misschien de nodige informatie opleveren. Ook het gebruik van waarborgen voor gegevensbescherming, met inbegrip van pseudo-anonimisering, kan relevant zijn. De uitkomst van de beoordeling moet de evenredigheid van de gegevensverwerking bevestigen.

72. *De effecten van verwerking (rechtstreeks gekoppeld aan de doeleinden)*. De evenredigheid kan ontbreken in gevallen waarin ISP's verkeersstroombeheer toepassen waarmee de toegang tot bepaalde diensten wordt uitgesloten zonder dat zij in ruil daarvoor een redelijk deel van het daaruit voortvloeiende voordeel aan de gebruikers laten.

73. Het is van belang eraan te herinneren dat het evenredigheidsbeginsel blijft gelden, zelfs als aan andere verplichte wettelijke eisen is voldaan, ook als een ISP bijvoorbeeld toestemming heeft verkregen van individuele gebruikers om de inhoud van communicatie te bewaken. Dit betekent dat de via inhoudbewaking uitgevoerde gegevensverwerking nog steeds onwettig kan zijn als zij het onderliggende fundamentele beginsel van evenredigheid schendt.

V.4. **Beveiligings- en organisatorische maatregelen**

74. Artikel 4 van de richtlijn e-privacy eist van ISP's uitdrukkelijk dat zij technische en organisatorische maatregelen nemen om te waarborgen dat i) persoonsgegevens alleen toegankelijk zijn voor gemachtigd personeel en voor wettige doeleinden, ii) persoonsgegevens worden beschermd tegen onbedoelde of onwettige verwerking, en iii) een beveiligingsbeleid inzake de verwerking van persoonsgegevens wordt uitgevoerd. Ook biedt het de nationale bevoegde instanties de mogelijkheid om controles uit te voeren op deze maatregelen.

75. Daarnaast zijn ISP's op grond van artikel 4, lid 2 en lid 3, van de richtlijn e-privacy ook verplicht om bevoegde nationale instanties op de hoogte te stellen van inbreuken op de gegevensbescherming, alsmede de getroffen personen voor het geval de bekendmaking van de gegevens negatieve gevolgen voor hen kan hebben.

76. Verwerking van in communicatie aanwezige persoonlijke informatie met de bedoeling om verkeersstroombeheer toe te passen, kan ISP's toegang geven tot gegevens die gevoeliger zijn dan verkeersgegevens.

([34]) Zoals in het voorgaande is geschetst, is de richtlijn gegevensbescherming van toepassing op alle zaken met betrekking tot de bescherming van fundamentele rechten en vrijheden die niet specifiek worden geregeld in de richtlijn e-privacy.

77. Daarom dient het beveiligingsbeleid dat door ISP's ontwikkeld wordt, specifieke waarborgen te omvatten om ervoor te zorgen dat de genomen maatregelen toereikend zijn voor deze risico's. Tegelijkertijd dienen de nationale bevoegde instanties die deze maatregelen controleren, bijzonder veeleisend te zijn. Ten slotte moet worden gewaarborgd dat er doeltreffende waarschuwingsprocedures bestaan om betrokkenen te informeren van wie informatie is blootgesteld en die daardoor geschaad kunnen worden.

VI. **SUGGESTIES VOOR BELEIDS- EN WETGEVINGSMAATREGELEN**

78. Controletechnieken op basis van verkeersgegevens en de controle van IP payloads, dat wil zeggen de inhoud van communicatie, kunnen de internetactiviteiten van gebruikers aan het licht brengen: bezochte websites en activiteiten op die sites, gebruik van P2P-toepassingen, gedownloade bestanden, verzonden en ontvangen e-mails, van wie, over welk onderwerp en in welke bewoordingen, enz. ISP's willen deze informatie wellicht gebruiken om sommige communicatie, zoals video op afroep, voorrang te geven op andere. Misschien willen ze haar gebruiken om virussen te identificeren of om profielen op te bouwen ten behoeve van gedragsgerichte advertenties. Deze handelingen grijpen in op het recht op vertrouwelijkheid van de communicatie.

79. Afhankelijk van de gebruikte technieken en de specifieke omstandigheden van het geval, zullen de gevolgen voor de privacy groter worden. Hoe diepgaander de onderschepping en analyse van de verzamelde informatie, hoe groter de strijdigheid met het beginsel van vertrouwelijkheid van communicatie. Ook de doeleinden waarvoor de bewaking plaatsvindt en de waarborgen voor gegevensbescherming die zijn toegepast, zijn belangrijke elementen bij de vaststelling van de mate van inbreuk op de privacy en persoonsgegevens van individuele personen. Blokkering en bewaking ten behoeve van de bestrijding van malware, met strikte begrenzing van de bewaartermijn en het gebruik van de gecontroleerde gegevens, laat zich niet vergelijken met situaties waarin de informatie worden geregistreerd om individuele profielen op te bouwen voor gedragsgerichte advertenties.

80. In beginsel meent de EDPS dat het bestaande EU-kader voor privacy- en gegevensbescherming, mits goed geïnterpreteerd, toegepast en gehandhaafd, toereikend is om te garanderen dat het recht op vertrouwelijkheid wordt gehandhaafd en dat de bescherming van de privacy en de gegevens van individuele burgers niet wordt ondergraven ([35]). ISP's zouden dergelijke mechanismen niet mogen gebruiken tenzij ze het wettelijk kader correct hebben toegepast. Meer in het bijzonder zouden ISP's de volgende relevante elementen van het kader moeten overwegen en eerbiedigen:

— ISP's kunnen beleid voor verkeersstroombeheer toepassen dat is bedoeld om de beveiliging van de dienst te bevorderen en de dienst te verlenen, met inbegrip van beperking van congestie, op grond van artikelen 4 en 6 van de richtlijn e-privacy;

— ISP's hebben een andere specifieke wettelijke grondslag, en mogelijk de toestemming van gebruikers, nodig om een beleid voor verkeersstroombeheer toe te passen dat de verwerking van verkeers- en/of communicatiegegevens voor andere dan voornoemde doeleinden met zich meebrengt. Zo is bijvoorbeeld de geïnformeerde toestemming van gebruikers nodig voor het bewaken en filteren van individuele communicatie met de bedoeling de toegang tot bepaalde toepassingen en diensten, zoals P2P of VoIP, te beperken (of toe te staan);

— de toestemming moet vrij, uitdrukkelijk en geïnformeerd zijn. Zij moet worden aangegeven met een bevestigende actie. In deze eisen ligt grote nadruk op de noodzaak van grotere inspanningen om te waarborgen dat individuele gebruikers voldoende worden geïnformeerd op een wijze die direct, begrijpelijk en specifiek is, zodat zij de effecten van de praktijken kunnen beoordelen en uiteindelijk een geïnformeerd besluit kunnen nemen. Gezien de complexiteit van deze technieken is het geven van betekenisvolle voorafgaande informatie aan gebruikers een van de belangrijkste uitdagingen voor het verkrijgen van geldige toestemming. Daarnaast mogen er geen schadelijke gevolgen (daarbij inbegrepen financiële kosten) zijn voor gebruikers die geen toestemming geven voor bewaking;

([35]) Dit is onverminderd de noodzaak van wettelijke veranderingen op basis van andere overwegingen, met name in het kader van de algemene herziening van het wettelijk kader van de EU voor gegevensbescherming om het meer doeltreffend te maken in het licht van nieuwe technologieën en de globalisering.

— het evenredigheidsbeginsel speelt een cruciale rol wanneer ISP's een beleid voor verkeersstroombeheer toepassen, ongeacht de wettelijke grondslag voor de verwerking en het doel ervan: verlening van de dienst, vermijding van congestie of het aanbieden van gerichte abonnementen met of zonder toegang tot bepaalde diensten en toepassingen. Dit beginsel beperkt de mogelijkheden van ISP's om de inhoud van individuele communicatie te bewaken met methoden die de verwerking van buitensporige hoeveelheden informatie met zich meebrengen of alleen voordelen voor ISP's opleveren. Wat ISP's logistiek kunnen doen, hangt af van de mate van inbreuk die de technieken maken, de vereiste resultaten (die hun voordeel kunnen opleveren) en de specifieke waarborgen voor privacy- en gegevensbescherming die zijn toegepast. Voordat zij controletechnieken in gebruik nemen, moeten ISP's een beoordeling uitvoeren van hun overeenstemming met het evenredigheidsbeginsel.

81. Hoewel het wettelijk kader op het ogenblik relevante voorwaarden en waarborgen bevat, is het nodig om in het bijzonder aandacht te besteden aan de vraag of ISP's daadwerkelijk aan de wettelijke vereisten voldoen, of zij de informatie verstrekken die consumenten nodig hebben om zinvolle keuzes te kunnen maken en of zij zich houden aan het evenredigheidsbeginsel. Op nationaal niveau omvatten de bevoegde instanties enerzijds de toezichthouders voor telecommunicatie en anderzijds de toezichthouders voor gegevensbescherming. Op EU-niveau is Berec een van de ter zake dienende organen. De EDPS kan in dit verband wellicht ook een rol spelen.

82. Naast het toezicht op het huidige nalevingsniveau vereisen sommige in dit advies besproken aspecten met betrekking tot de toepassing van het kader, gezien de betrekkelijke noviteit van de mogelijkheid voor massale onvertraagde controle van communicatie, nadere, meer diepgaande analyse en secundaire opheldering. Op verschillende gebieden zullen aanwijzingen bijzonder relevant zijn:

— de controlepraktijken vaststellen die gerechtvaardigd zijn om een probleemloze verkeersstroom te waarborgen en waarvoor geen toestemming van de gebruikers nodig is, bijvoorbeeld de bestrijding van spam. Naast de mate van inbreuk van de toegepaste bewaking zijn ook aspecten zoals de mate van verstoring van de probleemloze verkeersstroom die anders zou optreden, relevant;

— vaststellen welke controletechnieken kunnen worden uitgevoerd voor beveiligingsdoeleinden en waarvoor geen toestemming van de gebruikers is vereist;

— vaststellen wanneer bewaking individuele toestemming vereist, met name de toestemming van alle betrokken gebruikers, en wat de toelaatbare technische parameters zijn om te waarborgen dat de controletechniek geen gegevensverwerking met zich meebrengt die niet evenredig is met de beoogde doelen ervan;

— verder kunnen in de drie voornoemde gevallen aanwijzingen nodig zijn voor de toepassing van de nodige waarborgen voor gegevensbescherming (doelbeperking, beveiliging, enz.).

83. Aangezien op dit terrein zowel nationale als EU-bevoegdheden bestaan, meent de EDPS dat het delen van zienswijzen en ervaringen met het oog op een geharmoniseerde aanpak van het voorgaande van essentieel belang is. Om dat te bereiken, doet de EDPS de suggestie om een platform of een expertisegroep op te richten met vertegenwoordigers van nationale regelgevende instanties, de Groep gegevensbescherming artikel 29, de EDPS en Berec. Het eerste doel van dit platform zou zijn om aanwijzingen te ontwikkelen, in elk geval voor de zaken die hiervoor zijn aangeduid, teneinde een solide en geharmoniseerde aanpak en een gelijk speelveld te garanderen. De EDPS doet een beroep op de Commissie om dit initiatief te organiseren.

84. Ten slotte moeten zowel nationale instanties als hun tegenvoeters van de EU, waaronder Berec en de Commissie, de marktontwikkelingen op dit gebied nauwgezet volgen. Vanuit het oogpunt van gegevensbescherming en privacy zou het scenario waarin ISP's routinematig verkeersstroombeheerbeleid toepassen om abonnementen aan te bieden op basis van het filteren van de toegang tot inhoud en toepassingen, hoogst problematisch zijn. Als dit scenario werkelijkheid zou worden, zou wetgeving moeten worden ingevoerd om de situatie aan te pakken.

VII. **CONCLUSIES**

85. De toenemende mate waarin ISP's vertrouwen op bewakings- en controletechnieken tast de neutraliteit van internet en de vertrouwelijkheid van de communicatie aan. Dit werpt ernstige vragen op met betrekking tot de bescherming van de privacy en persoonsgegevens van gebruikers.

86. Hoewel deze zaken in de mededeling van de Commissie over open internet en netneutraliteit in Europa kort worden aangestipt, gelooft de EDPS dat er meer moet worden gedaan om te komen tot een bevredigend toekomstgericht beleid. In dit advies heeft hij daarom bijgedragen aan het lopende beleidsdebat over netneutraliteit, in het bijzonder over aspecten in verband met gegevensbescherming en privacy.

87. De EDPS meent dat er behoefte bestaat aan toezicht op de marktsituatie door nationale instanties en Berec. Dit toezicht moet een helder beeld opleveren met een antwoord op de vraag of de markt zich ontwikkelt in de richting van massale onvertraagde controle van de communicatie en van problemen in verband met de naleving van het wettelijk kader.

88. Toezicht op de markt dient samen te gaan met een nadere analyse van de effecten van nieuwe praktijken met betrekking tot gegevensbescherming en privacy op internet. In dit advies worden enkele gebieden geschetst waarop opheldering voordeel zou opleveren. Hoewel EU-agentschappen en organen zoals Berec, de Groep gegevensbescherming artikel 29 en de EDPS goed in staat zijn om de voorwaarden voor toepassing van het kader toe te lichten, meent de EDPS dat de Commissie de plicht heeft om het debat te coördineren en te sturen. Daarom doet hij een beroep op de Commissie om een initiatief te nemen waarin al deze belanghebbenden worden betrokken inj een platform of werkgroep met dit doel. Van de kwesties die nadere analyse vergen, moeten in elk geval de volgende punten worden aangepakt:

— de controlepraktijken vaststellen die gerechtvaardigd zijn om een probleemloze verkeersstroom te waarborgen en die kunnen worden uitgevoerd voor beveiligingsdoeleinden;

— vaststellen wanneer bewaking individuele toestemming vereist, met name de toestemming van alle betrokken gebruikers, en wat de toelaatbare technische parameters zijn om te waarborgen dat de controletechniek geen gegevensverwerking met zich meebrengt die niet evenredig is met het beoogde doel ervan;

— in de voornoemde gevallen kunnen aanwijzingen nodig zijn voor de toepassing van de nodige waarborgen voor gegevensbescherming (doelbeperking, beveiliging, enz.).

89. Afhankelijk van deze bevindingen kunnen aanvullende wetgevingsmaatregelen noodzakelijk zijn. In dat geval dient de Commissie beleidsmaatregelen voor te stellen die gericht zijn op versterking van het wettelijk kader en bevordering van de rechtszekerheid. Nieuwe maatregelen moeten de praktische consequenties van het beginsel van netneutraliteit verduidelijken, zoals dat al is gebeurd in enkele lidstaten, en ervoor zorgen dat gebruikers een reële keuze kunnen maken, met name door ISP's te dwingen onbewaakte verbindingen aan te bieden.

Gedaan te Brussel, 7 oktober 2011.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming