

I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBECHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming betreffende de huidige onderhandelingen van de Europese Unie over een Handelsovereenkomst ter bestrijding van namaak (ACTA)

(2010/C 147/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBECHERMING,

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

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 8,

Gelet op 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⁾,

Gelet op 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 ⁽²⁾,

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 inzake 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 ⁽³⁾, en met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

1. De Europese Unie neemt deel aan de onderhandelingen over de formulering van een Handelsovereenkomst ter bestrijding van namaak (ACTA). Deze onderhandelingen zijn in 2007 begonnen in een eerste groep van geïnteresseerde partijen en vervolgens voortgezet met een bredere groep deelnemers, die tot nu toe Australië, Canada, de Europese Unie, Japan, Korea, Mexico, Marokko, Nieuw-Zeeland,

Singapore, de Verenigde Staten en Zwitserland omvat. De Europese Commissie heeft in 2008 een mandaat van de Raad ontvangen om deze onderhandelingen aan te gaan.

2. De Europese Toezichthouder voor gegevensbescherming (EDPS) erkent dat de grensoverschrijdende handel in namaakgoederen een punt van toenemende zorg is, waarbij vaak georganiseerde criminele netwerken zijn betrokken en dat vraagt om de uitvoering van passende samenwerkingsmechanismen op internationaal niveau ter bestrijding van deze vorm van criminaliteit.
3. De EDPS meent dat het sluiten door de Europese Unie van een multilaterale overeenkomst met als kernonderwerp de handhaving van intellectuele-eigendomsrechten belangrijke vragen oproept met betrekking tot het effect van de maatregelen ter bestrijding van namaak en piraterij op de grondrechten van individuele personen, in het bijzonder hun recht op eerbiediging van de persoonlijke levenssfeer en gegevensbescherming.
4. In dit verband betreurt de EDPS het bijzonder dat hij door de Europese Commissie niet is geraadpleegd over de inhoud van een dergelijke overeenkomst. Op eigen initiatief heeft de EDPS daarom het onderhavige advies opgesteld op basis van artikel 41, lid 2, van Verordening (EG) nr. 45/2001 met het oogmerk de Commissie sturing te geven inzake privacy- en gegevensbeschermingsaspecten die overweging verdienen in de onderhandelingen over de ACTA.

II. STAND VAN ZAKEN EN VOORZIENE INHOUD VAN DE ACTA

5. Van 26 tot 29 januari 2010 heeft in Mexico de zevende onderhandelingsronde plaatsgevonden met de bedoeling in de loop van 2010 een overeenkomst te sluiten. Er is echter tot nu toe geen officiële ontwerpovereenkomst vrijgegeven.

⁽¹⁾ PB L 281 van 23.11.1995, blz. 31.

⁽²⁾ PB L 201 van 31.7.2002, blz. 37.

⁽³⁾ PB L 8 van 12.1.2001, blz. 1.

6. De onderhandelingen zijn gericht op aanneming van een nieuwe multilaterale overeenkomst ter versterking van de handhaving van intellectuele-eigendomsrechten en ter bestrijding van namaak en piraterij. Als zij wordt aangenomen, zal deze nieuwe overeenkomst in betere internationale normen voorzien voor het optreden tegen grootschalige overtredingen van intellectuele-eigendomsrechten. Het DG Handel van de Europese Commissie heeft in het bijzonder uitgesproken dat de focus moet liggen op namaak en piraterij die belangrijke schade toebrengen aan handelsbelangen, niet op de activiteiten van gewone burgers ⁽⁴⁾.
7. Met betrekking tot de inhoud van de overeenkomst wordt in de *Samenvatting van de belangrijkste discussiepunten*, in november 2009 uitgegeven door het DG Handel van de Europese Commissie, aangegeven dat het doel van de ACTA — bestrijding van namaak en piraterij — zal worden nagestreefd door middel van drie hoofdonderdelen: i) internationale samenwerking, ii) handhavingspraktijken en iii) de vaststelling van een wettelijk kader voor de handhaving van intellectuele-eigendomsrechten op verschillende aangewezen terreinen, met name in de digitale omgeving ⁽⁵⁾. De voorziene maatregelen zullen met name betrekking hebben op wettelijke procedures (zoals tussenvonnissen en voorlopige maatregelen), taken en verantwoordelijkheden van internetaanbieders (ISP's) bij het voorkomen van inbreuken op het auteursrecht op internet, en maatregelen voor internationale samenwerking ter voorkoming van het grensoverschrijdend verkeer van goederen. De gepubliceerde informatie bevat echter slechts de grote lijnen van de overeenkomst en verschaft geen details over specifieke en concrete maatregelen.
8. De EDPS merkt op dat, zelfs als het beoogde doel van de ACTA alleen de bestrijding van grootschalige inbreuk op intellectuele-eigendomsrechten is, niet kan worden uitgesloten dat activiteiten van gewone burgers door de ACTA worden bestreken, vooral wanneer handhavingsmaatregelen worden genomen in de digitale omgeving. De EDPS benadrukt dat dit passende garanties vereist ter bescherming van de grondrechten van individuele personen. Bovendien bestrijken wetten inzake gegevensbescherming alle burgers, met inbegrip van personen die mogelijk betrokken zijn bij namaak en piraterij, en zal de bestrijding van grootschalige overtredingen zeker ook de verwerking van persoonsgegevens inhouden.
9. In dit verband moedigt de EDPS de Europese Commissie ten sterkste aan een openbare en transparante dialoog over de ACTA te beginnen, mogelijk door middel van een openbare raadpleging, die ook zou kunnen bijdragen tot de waarborg dat de te nemen maatregelen in overeenstemming zijn met de voorschriften van het EU-recht inzake privacy- en gegevensbescherming.
- III. REIKWIJDTE VAN HET COMMENTAAR VAN DE EDPS**
10. De EDPS doet een krachtig beroep op de EU, in het bijzonder op de Europese Commissie, die het mandaat heeft
- ontvangen om de overeenkomst te sluiten, om een goed evenwicht te bewaren tussen enerzijds de roep om bescherming van de intellectuele eigendom en anderzijds het recht op privacy- en gegevensbescherming van het individu.
11. De EDPS benadrukt dat privacy- en gegevensbescherming als kernwaarden van de Europese Unie zijn erkend in artikel 8 van het EVRM en de artikelen 7 en 8 van het EU-handvest van de grondrechten ⁽⁶⁾, die moeten worden geëerbiedigd in alle beleidsmaatregelen en regels die door de EU worden vastgesteld uit hoofde van artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU).
12. Verder onderstreept de EDPS dat een overeenkomst die door de Europese Unie wordt bereikt over de ACTA moet voldoen aan de wettelijke plichten die aan de EU zijn opgelegd met betrekking tot het recht inzake bescherming van de persoonlijke levenssfeer en persoonsgegevens, zoals met name bepaald in Richtlijn 95/46/EG, in Richtlijn 2002/58/EG ⁽⁷⁾ en in de jurisprudentie van het Europees Hof voor de Rechten van de Mens ⁽⁸⁾ en het Hof van Justitie ⁽⁹⁾.
13. Met privacy en gegevensbescherming moet vanaf het begin van de onderhandelingen rekening worden gehouden, niet pas wanneer de plannen en procedures zijn gedefinieerd en overeengekomen en het derhalve te laat is om alternatieve oplossingen te vinden waarmee de persoonlijke levenssfeer wordt geëerbiedigd.
14. In het licht van de weinige informatie die openbaar is gemaakt, merkt de EDPS op dat hij zich niet in een positie bevindt om een analyse te geven van de specifieke bepalingen van de ACTA. In dit advies concentreert de EDPS zich daarom op een beschrijving van de mogelijke bedreigingen voor de privacy en gegevensbescherming waartoe mogelijke concrete maatregelen van de overeenkomst, voor zover bekend, zouden kunnen leiden op de volgende twee terreinen: handhaving van intellectuele-eigendomsrechten in de digitale omgeving (hoofdstuk IV) en mechanismen voor internationale samenwerking (hoofdstuk V).

⁽⁴⁾ Zie http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, blz. 2.

⁽⁵⁾ Zie voetnoot 2.

⁽⁶⁾ Handvest van de grondrechten van de Europese Unie, PB C 303 van 14.12.2007, blz. 1.

⁽⁷⁾ 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, PB L 201 van 31.7.2002, blz. 37.

⁽⁸⁾ De interpretatie van de belangrijkste elementen en voorwaarden zoals bepaald in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), vastgesteld in Rome op 4 november 1950, zoals van toepassing op verschillende terreinen. Zie in het bijzonder de jurisprudentie waarnaar elders in dit advies wordt verwezen.

⁽⁹⁾ Zie in het bijzonder zaak C-275/06, *Productores de Música de España (Promusicae)*, Jurispr. [2008], blz. I-271, en zaak C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nng.

IV. HANDHAVING VAN INTELLECTUELE-EIGENDOMSRECHTEN IN DE DIGITALE OMGEVING

IV. 1. De noodzaak om de gevolgen voor de privacy en gegevensbescherming van een „drietrapsafsluitbeleid” te analyseren

15. Volgens de Europese Commissie wordt met de ACTA een wettelijk kader geschapen voor de bestrijding van namaak in de digitale omgeving⁽¹⁰⁾. Dit kader moet de voorwaarden bepalen waaronder ISP's en andere online-intermediairs⁽¹¹⁾ aansprakelijk kunnen worden gesteld voor inbreuken op het auteursrecht van materiaal dat via hun voorzieningen wordt verwerkt. Het kader kan ook voorzien in het treffen van maatregelen en sancties tegen internetgebruikers nadat inbreuk is gemaakt op het auteursrecht door het uploaden of downloaden van materiaal. Hoewel de details van een dergelijk kader nog niet officieel zijn bekendgemaakt, is gezien de uit verschillende kanalen beschikbare informatie te verwachten dat het de verplichting voor ISP's bevat om een „drietrapsafsluitbeleid” (*three strikes Internet disconnection policy*) te hanteren, dat ook wel wordt aangeduid als stapsgewijze respons (*graduated response*). Zo'n beleid houdt in dat auteursrechthebbers het gedrag van internetgebruikers mogen controleren en vermeende overtreders van auteursrechten mogen identificeren. Nadat contact is opgenomen met de ISP's van vermeende overtreders, waarschuwen de ISP's de gebruikers die als overtreders zijn aangemerkt. Een gebruiker wordt afgesloten van toegang tot het internet na driemaal te zijn gewaarschuwd.
16. Terwijl de onderhandelingen over de ACTA gaande zijn, wordt in sommige lidstaten, zoals Frankrijk, een drietrapsafsluitbeleid ingevoerd. Het wordt ook besproken op diverse EU-fora, zoals de dialoog van belanghebbenden over illegaal up- en downloaden, die momenteel op instigatie van DG MARKT wordt gevoerd in verband met de goedkeuring van de mededeling van de Commissie over een versterkte handhaving van intellectuele-eigendomsrechten in de interne markt⁽¹²⁾. Discussies over dit onderwerp vinden ook plaats in het Europees Parlement in afwachting van het debat over een ontwerp-resolutie over versterking van de handhaving van intellectuele-eigendomsrechten in de interne markt (het „Gallo-verslag”).
17. Zulke praktijken dringen diep door in de persoonlijke levenssfeer van het individu. Ze brengen met zich mee dat de

⁽¹⁰⁾ Zie voetnoot 2.

⁽¹¹⁾ De verschillende online-intermediairs kunnen worden gedefinieerd op basis van hun functionele rol. In feite vervullen intermediairs echter meestal meer dan één functie. Online-intermediairs omvatten a) *toegangsaanbieders*: gebruikers maken verbinding met het netwerk door verbinding te maken met de server van een toegangsaanbieder; b) *netwerkaanbieders*: deze verschaffen de routers, dat wil zeggen de noodzakelijke technische voorzieningen voor gegevensoverdracht; c) *aanbieders van hostdiensten*: deze verhuren ruimte op hun server, waarop gebruikers of informatieleveranciers informatie kunnen uploaden. Gebruikers kunnen materiaal uploaden en downloaden naar een onlinedienst, zoals een elektronisch prikbord of een P2P-netwerk.

⁽¹²⁾ Mededeling van de Commissie aan de Raad, het Europees Parlement en het Europees Economisch en Sociaal Comité — Voor een versterkte handhaving van intellectuele eigendomsrechten in de interne markt, Brussel, 11 september 2009, COM(2009) 467 def.

activiteiten van internetgebruikers stelselmatig worden gecontroleerd, met inbegrip van volkomen rechtmatige activiteiten. Ze raken miljoenen internetgebruikers die de wet eerbiedigen, onder wie veel kinderen en jongeren. Ze worden uitgevoerd door particuliere partijen, niet door rechtshandhavinginstanties. Bovendien speelt het internet tegenwoordig een centrale rol in vrijwel alle aspecten van het moderne leven, zodat het afsluiten van de toegang tot internet enorme gevolgen kan hebben en mensen kan afhouden van werk, cultuur, elektronische overheidsdiensten, enzovoort.

18. Tegen deze achtergrond is het relevant om te beoordelen in hoeverre dit beleid in overeenstemming is met de Europese wetgeving betreffende gegevensbescherming en privacy, en meer in het bijzonder of een drietrapsafsluitbeleid een noodzakelijke maatregel is voor de handhaving van intellectuele-eigendomsrechten. In dat verband moet ook worden onderzocht of er andere, minder indringende methoden bestaan.
19. Het is nog onduidelijk of het drietrapsafsluitbeleid deel zal uitmaken van de ACTA. Een dergelijk beleid wordt echter ook op andere terreinen overwogen en kan — potentieel — een enorm effect hebben op de bescherming van persoonsgegevens en privacy. Daarom acht de EDPS het noodzakelijk om het in dit advies te behandelen. Alvorens de genoemde analyse uit te voeren, geeft de EDPS een beknopte beschrijving van het geldende wettelijk kader voor gegevensbescherming en privacy.
20. Opgemerkt moet worden dat een drietrapsafsluitbeleid inzake internettoegang niet alleen gevolgen heeft voor gegevensbescherming en privacy, maar ook zorgen wekt met betrekking tot andere waarden, zoals een behoorlijke rechtsgang en de vrijheid van meningsuiting. In dit advies wordt echter alleen ingegaan op zaken die verband houden met de bescherming van persoonsgegevens en de individuele privacy.

IV.2. Een drietrapsafsluitbeleid en de toepassing van het wettelijk kader van de EU voor gegevensbescherming en privacy

Hoe een drietrapsafsluitbeleid kan worden ingericht

21. Kort gezegd betekent het drietrapsafsluitbeleid dat auteursrechthebbers met behulp van geautomatiseerde technische middelen, mogelijk verschaft door derden, vermeende inbreuken op het auteursrecht opsporen door de activiteiten van internetgebruikers te controleren, bijvoorbeeld via toezicht op fora en blogs of door zich voor te doen als bestandsuitwisselaars in P2P-netwerken teneinde

bestandsuitwisselaars te identificeren die materiaal uitwisselen waarop auteursrechten berusten ⁽¹³⁾.

22. Na de identificatie, aan de hand van hun Internet Protocol-adressen (IP-adressen), van internetgebruikers die ervan worden verdacht auteursrechten te schenden, zenden de auteursrechthebbers de IP-adressen van die gebruikers aan de betrokken internetaanbieders (ISP's). Deze waarschuwen de abonnee aan wie het IP-adres toebehoort over diens mogelijke betrokkenheid bij overtreding van het auteursrecht. Nadat een abonnee een bepaald aantal malen door de ISP is gewaarschuwd, zal de ISP automatisch de internetaansluiting van die abonnee beëindigen of opschorten ⁽¹⁴⁾.

Het toepasselijke Europese wettelijke kader voor gegevensbescherming en privacy

23. Een drietrapsafsluitbeleid moet voldoen aan de voorschriften die voortvloeien uit het recht op privacy zoals vastgelegd in artikel 8 van het EVRM en artikel 7 van het Handvest van de grondrechten, en die voortvloeien uit het recht op gegevensbescherming zoals vastgelegd in artikel 8 van het Handvest van de grondrechten en artikel 16 van het VWEU, zoals ook uitgewerkt in Richtlijn 95/46/EG en Richtlijn 2002/58/EG.
24. Naar de mening van de EDPS komt de controle van het gedrag van internetgebruikers en het op grond daarvan verzamelen van hun IP-adressen neer op overtreding van hun recht op eerbiediging van het privéleven en hun recht op vrije correspondentie; met andere woorden, er is sprake van inmenging in hun persoonlijke levenssfeer. Deze visie is in overeenstemming met de jurisprudentie van het Europees Hof voor de Rechten van de Mens ⁽¹⁵⁾.
25. Richtlijn 95/46/EG is van toepassing ⁽¹⁶⁾ omdat het drietrapsafsluitbeleid de verwerking met zich meebrengt van

IP-adressen die — in elk geval onder de relevante omstandigheden — moeten worden beschouwd als persoonsgegevens. IP-adressen zijn identificatienummers die bestaan uit een reeks getallen gescheiden door punten, zoals 122.41.123.45. Een abonnement bij een internetaanbieder geeft de abonnee toegang tot het internet. Telkens wanneer de abonnee het internet op wil gaan, wordt hem een IP-adres toegewezen via het apparaat waarmee hij verbinding maakt met het internet (bijvoorbeeld een computer) ⁽¹⁷⁾.

26. Als een gebruiker een bepaalde activiteit ontplooit en bijvoorbeeld materiaal uploadt naar het internet, kan de gebruiker door derden worden geïdentificeerd via het gebruikte IP-adres. De gebruiker met het IP-adres 122.41.123.45 zou bijvoorbeeld op 1 januari 2010 om 15.00 uur materiaal dat een inbreuk op het auteursrecht vormt, hebben geüpload naar een P2P-dienst. De ISP kan dan een verband leggen tussen het IP-adres en de naam van de abonnee waaraan hij dit adres heeft toegewezen en aldus zijn of haar identiteit vaststellen.
27. Als men de definitie van persoonsgegevens beschouwt die wordt gegeven in artikel 2 van Richtlijn 95/46/EG, „iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna „betrokkene” te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer” ⁽¹⁸⁾, kan men slechts concluderen dat IP-adressen en informatie over de activiteiten die aan die adressen zijn gekoppeld in alle hier ter zake doende gevallen als persoonsgegevens moeten worden opgevat. Een IP-adres fungeert als identificatienummer waarmee de naam kan worden gevonden van de abonnee aan wie dat adres is toegewezen. Verder is het duidelijk dat de informatie die over de abonnee met het IP-adres wordt verzameld („hij/zij heeft bepaald materiaal geüpload naar website ZS op 1 januari 2010 om 15.00 uur”), de activiteiten van een identificeerbaar individu (de houder van het IP-adres) *betreft* en derhalve moet worden beschouwd als persoonsgegevens.

⁽¹³⁾ P2P-technologie is een softwarearchitectuur voor gedistribueerd computergebruik waarmee afzonderlijke computers rechtstreeks kunnen worden verbonden en kunnen communiceren met andere computers.

⁽¹⁴⁾ Tot de andere mogelijke sancties behoort beperking van de functionaliteit van de internetaansluiting, bijvoorbeeld de snelheid van de verbinding, het gegevensvolume, enzovoort.

⁽¹⁵⁾ Zie met name EVRM 26 juni 2006, *Weber en Saravia/Duitsland* (arr.), nr. 54934/00, para 77, en EVRM 1 juli 2008, *Liberty e.a./Verenigd Koninkrijk*, nr. 58243/00.

⁽¹⁶⁾ Het Hof van Justitie hanteert een ruime opvatting van de toepasselijkheid van Richtlijn 95/46/EG, waarvan de bepalingen moeten worden geïnterpreteerd in het licht van artikel 8 van het EVRM. Volgens het Hof van Justitie in zijn arrest van 20 mei 2003, *Österreichischer Rundfunk*, gevoegde zaken C-465/00, C-138/01 en C-139/01, Jurispr. [2003], blz. I-4989, para 68, „moet richtlijn 95/46/EG, voor zover zij de verwerking regelt van persoonsgegevens die afbreuk kunnen doen aan de fundamentele vrijheden, inzonderheid het recht op persoonlijke levenssfeer, noodzakelijkerwijs worden uitgelegd op basis van de grondrechten, die volgens vaste rechtspraak integrerend deel uitmaken van de algemene rechtsbeginselen welke eerbiediging het Hof verzekert”.

⁽¹⁷⁾ Het IP-adres dat de ISP aan een individuele gebruiker toewijst, kan altijd hetzelfde zijn voor alle keren dat hij op het internet is (statisch IP-adres). Andere IP-adressen zijn dynamisch, dat wil zeggen dat de internetaanbieder telkens wanneer zijn klanten verbinding maken met het internet een ander IP-adres aan hen toewijst. Vanzelfsprekend kan de ISP het IP-adres herleiden tot het account van de abonnee aan wie hij het (dynamische of statische) IP-adres heeft toegewezen.

⁽¹⁸⁾ In overweging 26 wordt deze definitie aangevuld: „Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is; ...”.

28. Deze opvattingen worden geheel gedeeld door de Groep gegevensbescherming artikel 29, die in een document over kwesties van gegevensbescherming in verband met intellectuele eigendom heeft verklaard dat IP-adressen die worden verzameld ten behoeve van de handhaving van intellectuele-eigendomsrechten, dat wil zeggen voor de identificatie van internetgebruikers die vermeende inbreuken zouden maken op intellectuele-eigendomsrechten, persoonsgegevens zijn voor zover ze worden gebruikt voor de handhaving van zulke rechten tegenover een bepaalde persoon⁽¹⁹⁾.
29. Richtlijn 2002/58/EG is eveneens van toepassing, aangezien een drietrapsafsluitbeleid het vergaren van verkeers- en communicatiegegevens met zich meebrengt. Richtlijn 2002/58/EG reglementeert het gebruik van zulke gegevens en voorziet in het beginsel van vertrouwelijkheid van communicatie via openbare communicatienetwerken en van de gegevens die inherent zijn aan zulke communicatie.

IV.3. De noodzaak van een drietrapsafsluitbeleid

30. In artikel 8 van het EVRM is het noodzakelijkheidsbeginsel opgenomen op grond waarvan een maatregel die inbreuk maakt op het individuele recht op privacy, slechts is toegestaan indien hij noodzakelijk is om in een democratische samenleving het gerechtvaardigde doel te bereiken dat ermee wordt nagestreefd⁽²⁰⁾. Het noodzakelijkheidsbeginsel is ook te vinden in de artikelen 7 en 13 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG⁽²¹⁾. Het beginsel schrijft een analyse van de evenredigheid van

de maatregel voor, die moet worden beoordeeld op basis van een evenwicht tussen de betrokken belangen, dat in de context wordt geplaatst van de democratische samenleving als geheel⁽²²⁾. Ook impliceert het een beoordeling van de vraag of er alternatieve maatregelen bestaan die minder indringend zijn.

31. Hoewel de EDPS het belang van de handhaving van intellectuele-eigendomsrechten erkent, is hij van mening dat een drietrapsafsluitbeleid zoals nu bekend — met zekere elementen van algemene toepasbaarheid — een onevenredige maatregel is die daarom niet kan worden beschouwd als een noodzakelijke maatregel. De EDPS gelooft verder dat er alternatieve, minder indringende oplossingen bestaan of dat het voorziene beleid op minder inbreukmakende wijze of met een beperktere reikwijdte kan worden uitgevoerd. Ook op een meer gedetailleerd wettelijk niveau levert de drietrapsaanpak problemen op. Deze conclusies worden hierna toegelicht.

Het drietrapsafsluitbeleid is onevenredig

32. Het EDPS wenst te onderstrepen hoe verstrekkend van aard de opgelegde maatregelen zijn. De volgende elementen verdienen in dat opzicht vermelding:

- i) het feit dat de (onopgemerkte) controle miljoenen personen en *alle* gebruikers zou treffen, ongeacht of zij onder verdenking staan;
- ii) de controle zou inhouden dat stelselmatig gegevens worden geregistreerd waarvan een deel zou kunnen leiden tot civielrechtelijke of zelfs strafrechtelijke vervolging van mensen; bovendien zou daarom een deel van de verzamelde gegevens moeten worden beschouwd als gevoelige gegevens in de zin van artikel 8 van Richtlijn 95/46/EG, die strengere waarborgen voorschrijft;
- iii) de controle zal waarschijnlijk veel fout-positieve uitkomsten opleveren. Inbreuk op het auteursrecht is geen kwestie van een simpel „ja” of „nee”. Vaak moeten rechters een zeer aanzienlijke hoeveelheid technische en wettelijke details bestuderen, beschreven op tientallen bladzijden, teneinde vast te stellen of er sprake is van een overtreding⁽²³⁾;

⁽¹⁹⁾ Groep gegevensbescherming artikel 29, werkdocument over kwesties van gegevensbescherming in verband met intellectuele eigendom (WP 104), aangenomen op 18 januari 2005. Deze werkgroep is opgericht uit hoofde van artikel 29 van Richtlijn 95/46/EG. Zij is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en privacy. Haar taken worden beschreven in artikel 30 van Richtlijn 95/46/EG en artikel 15 van Richtlijn 2002/58/EG. Zie ook het advies 4/2007 van de Groep over het begrip persoonsgegevens (WP 136), aangenomen op 20 juni 2007, met name blz. 16.

⁽²⁰⁾ In artikel 8 van het EVRM wordt uitdrukkelijk voorgeschreven dat een inmenging of beperking „in een democratische samenleving noodzakelijk” moet zijn.

⁽²¹⁾ Artikel 13 van Richtlijn 95/64/EG staat een beperking uitsluitend toe „indien dit noodzakelijk is ter vrijwaring van a) de veiligheid van de Staat; b) de landsverdediging; c) de openbare veiligheid; d) het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepsregels voor gereguleerde beroepen; e) een belangrijk economisch en financieel belang van een lidstaat of van de Europese Unie, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden; f) een taak op het gebied van controle, inspectie of regelgeving, verbonden, ook al is dit incidenteel, met de uitoefening van het openbaar gezag in de onder c), d) en e), bedoelde gevallen; g) de bescherming van de betrokkene of van de rechten en vrijheden van anderen”. Artikel 15 van Richtlijn 2002/58/EG bepaalt dat beperkende maatregelen zijn toegestaan „indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van ongevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG”.

⁽²²⁾ Zie ook EVRM 2 augustus 1984, *Malone/Verenigd Koninkrijk*, serie A nr. 82, blz. 32, para. 81 e.v., en EVRM 4 december 2008, *Marper/Verenigd Koninkrijk* [GC], nr. 30562/04 en 30566/04, para. 101 e.v.

⁽²³⁾ Rechters moeten vaststellen of er rechten op het materiaal berusten, op welke rechten inbreuk is gemaakt, of het gebruik kan worden opgevat als eerlijk gebruik, wat het toepasselijk recht is, wat de schade(vergoeding) is, enzovoort.

- iv) de mogelijke *effecten* van de controle, die kan leiden tot afsluiting van de toegang tot het internet. Een dergelijke afsluiting zou een belemmering zijn voor het recht op vrije meningsuiting en de vrije toegang tot informatie, cultuur, elektronische overheidsdiensten, markten en e-mail, en in sommige gevallen voor werkgerelateerde activiteiten van individuele personen. In dit verband is het van groot belang te bedenken dat de effecten niet alleen de vermeende overtreder treffen, maar ook alle gezinsleden die gebruik maken van dezelfde internetverbinding, onder wie schoolkinderen die het internet gebruiken voor hun schoolactiviteiten;
- v) het feit dat de instelling die de beoordeling uitvoert en de beslissing neemt, veelal een particuliere rechtspersoon (namelijk de auteursrechthebbende of de ISP) zal zijn. De EDPS heeft in een vorig advies al zijn zorg uitgesproken over de controle van individuele personen door de particuliere sector (bijvoorbeeld ISP's of de auteursrechthebbenden) op terreinen die in beginsel tot de bevoegdheden van rechtshandhavinginstanties behoren ⁽²⁴⁾.
33. De EDPS is er niet van overtuigd dat de voordelen van de maatregelen opwegen tegen de gevolgen voor de grondrechten van individuele burgers. De bescherming van het auteursrecht is in het belang van de rechthebbenden en van de samenleving. Beperkingen van de grondrechten lijken echter niet gerechtvaardigd als de ernst van het ingrijpen, dat wil zeggen de mate van inbreuk in de privé sfeer zoals blijkt uit voornoemde elementen, wordt afgezet tegen de verwachte voordelen, te weten de afschrikking van — grotendeels kleinschalige — inbreuken op intellectuele-eigendomsrechten. Zoals het in de conclusie van advocaat-generaal Kokott in de zaak-Promusicae is verwoord: „Het is ... niet zeker dat particuliere filesharing, in het bijzonder als dit zonder winstoogmerk geschiedt, een voldoende ernstige bedreiging voor de bescherming van auteursrechten vormt om een beroep op deze uitzondering te rechtvaardigen. Het is namelijk omstreden in hoeverre particuliere filesharing reële schade veroorzaakt.” ⁽²⁵⁾
34. In dit verband is het waardevol om te herinneren aan de reactie van het Europees Parlement op plannen voor een „drietrapsafsluitbeleid” in het kader van de herziening van het telecompakket, met name amendement 138 op de kaderrichtlijn ⁽²⁶⁾. In dit amendement werd gesteld dat een beperking van de grondrechten of fundamentele vrijheden alleen mag worden opgelegd als deze in een democratische samenleving redelijk, evenredig en noodzakelijk is, en dat de tenuitvoerlegging onderwerp moet zijn van toereikende procedurele waarborgen in overeenstemming met het EVRM en de algemene beginselen van het
- Gemeenschapsrecht, met inbegrip van doeltreffende rechtsbescherming en eerlijke rechtspleging ⁽²⁷⁾.
35. In deze opzicht benadrukt de EDPS verder dat elke beperking van de grondrechten onderwerp moet zijn van zorgvuldig toezicht op EU- en nationaal niveau. In dit verband kan een parallel worden getrokken met Richtlijn 2006/24/EG betreffende de bewaring van gegevens ⁽²⁸⁾, waarin wordt afgeweken van het algemene beginsel dat gegevens dienen te worden verwijderd wanneer ze niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld. De richtlijn schrijft voor dat verkeersgegevens worden bewaard ten behoeve van de bestrijding van ernstige misdrijven. Daarbij moet worden opgemerkt dat bewaring alleen is toegestaan voor „zware criminaliteit”, dat de bewaring beperkt wordt tot „verkeers- en locatiegegevens”, waardoor in beginsel gegevens over de inhoud van de communicatie zijn uitgesloten, en dat strenge waarborgen worden genoemd. Desalniettemin zijn er twijfels gerezen over de verenigbaarheid met grondrechtelijke normen; het Roemeense Constitutionele Hof heeft bepaald dat algemene bewaring onverenigbaar is met de grondrechten ⁽²⁹⁾ en er is op het ogenblik een zaak aanhangig bij het Duitse Constitutionele Hof ⁽³⁰⁾.

Het bestaan van andere, minder indringende middelen

36. Voornoemde bevindingen worden versterkt door het feit dat er minder indringende middelen bestaan om hetzelfde doel te bereiken. De EDPS dringt erop aan dat zulke minder indringende modellen worden onderzocht en beproefd.

⁽²⁷⁾ De definitieve formulering van amendement 138 op artikel 1, punt 3 bis luidt als volgt: „Maatregelen van de lidstaten betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken eerbiedigen de fundamentele rechten en vrijheden van natuurlijke personen zoals die door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht worden gewaarborgd. Maatregelen betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken die die fundamentele rechten en vrijheden kunnen beperken, mogen alleen worden opgelegd indien zij passend, evenredig en noodzakelijk zijn in een democratische samenleving, en zij worden uitgevoerd met inachtneming van adequate procedurele waarborgen overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht, waaronder doeltreffende rechtsbescherming en eerlijke rechtsbedeling. Deze maatregelen mogen derhalve alleen worden genomen met inachtneming van het beginsel van het vermoeden van onschuld en het recht op een persoonlijke levenssfeer. Een voorafgaande, eerlijke en onpartijdige procedure wordt gegarandeerd, inclusief het recht van de betrokkene of betrokkenen om te worden gehoord, met dien verstande dat voor naar behoren gestaaftde spoedeisende gevallen geëigende voorwaarden en procedurele regelingen gelden overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Het recht op een daadwerkelijke en tijdige beroepsmogelijkheid bij een rechterlijke instantie is gegarandeerd.”

⁽²⁸⁾ Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006, PB L 105 van 13.4.2006, blz. 54.

⁽²⁹⁾ <http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html>

⁽³⁰⁾ <http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html>

⁽²⁴⁾ Advies van de EDPS van 23 juni 2008 betreffende het voorstel voor een besluit tot vaststelling van een meerjarenprogramma van de Gemeenschap betreffende de bescherming van kinderen die het internet en andere communicatietechnologieën gebruiken, PB C 2 van 7.1.2009, blz. 2.

⁽²⁵⁾ Zie de zaak-Promusicae, vermeld in voetnoot 8, pt. 106.

⁽²⁶⁾ Zie Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009, PB L 337 van 18.12.2009, blz. 37.

37. In dit verband roept de EDPS in herinnering dat de gewijzigde Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten (de „burgerrechtenrichtlijn”), die onderdeel is van het onlangs herziene telecompakket, bepaalde regels en procedures bevat ter beperking van kleinschalige inbreuken op het auteursrecht bij consumenten⁽³¹⁾. Zulke procedures omvatten de verplichting van de lidstaten om gestandaardiseerde informatie van algemeen belang over verschillende onderwerpen te publiceren, waarin specifiek melding wordt gemaakt van inbreuken op het auteursrecht en verwante rechten, en de wettelijke consequenties daarvan⁽³²⁾. De lidstaten kunnen vervolgens ISP's verzoeken de informatie onder al hun klanten te verspreiden en haar in hun overeenkomsten op te nemen.

38. Het systeem is bedoeld om mensen te informeren en hen ervan te weerhouden door het auteursrecht beschermde informatie te verspreiden en overtredingen te begaan, en tegelijkertijd de controle van het internetgebruik en de daarmee verband houdende zorgen over privacy en gegevensbescherming te vermijden. De burgerrechtenrichtlijn moet ten uitvoer worden gelegd in mei 2011; zulke procedures bestaan derhalve nog niet. Daarom zijn er nog geen mogelijkheden om de voordelen ervan te beproeven. Het lijkt dan ook prematuur om voorbij te gaan aan de mogelijke positieve uitkomst van deze procedures en in plaats daarvan een „drietrapafsluitbeleid” te omarmen, dat de grondrechten veel meer beperkt.

39. In aanvulling op het voorgaande moet in herinnering worden geroepen dat Richtlijn 2004/48/EG van 28 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten („HIER-richtlijn”) in verschillende instrumenten voorziet voor handhaving door de rechterlijke macht (hierna behandeld in paragraaf 43 e.v.)⁽³³⁾.

40. De HIER-richtlijn is pas onlangs omgezet in wetgeving in de lidstaten. Tot nu toe is er niet voldoende tijd geweest

⁽³¹⁾ Zie Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, PB L 337 van 18.12.2009, blz. 11.

⁽³²⁾ Artikel 21, lid 4, van Richtlijn 2009/136/EG bepaalt meer in het bijzonder: „De lidstaten mogen voorschrijven dat de ondernemingen als bedoeld in lid 3 met dezelfde middelen waarmee de ondernemingen doorgaans met abonnees communiceren indien nodig kosteloos informatie van algemeen belang aan bestaande en nieuwe abonnees verstrekken. In dat geval wordt dergelijke informatie door de bevoegde openbare instanties in een gestandaardiseerde vorm aangeleverd en heeft onder meer betrekking op de volgende punten: a) de meest voorkomende vormen van gebruik van elektronische-communicatiediensten voor onwettige activiteiten of de verspreiding van schadelijke inhoud, met name waar dit de eerbiediging van de rechten en vrijheden van derden kan aantasten, inclusief schendingen van het auteursrecht en hiermee samenhangende rechten, en de juridische gevolgen hiervan (...).” Verder geldt op grond van artikel 20, lid 2: „De lidstaten mogen ook voorschrijven dat het contract alle eventueel daartoe door de bevoegde overheidsinstanties verstrekte informatie over het gebruik van elektronische-communicatienetwerken en -diensten voor onwettige activiteiten of de verspreiding van schadelijke inhoud en over beschermingsmaatregelen tegen gevaren voor de persoonlijke veiligheid, de persoonlijke levenssfeer en persoonsgegevens bevat waarnaar in artikel 21, lid 4, wordt gewezen en die van toepassing is op de aangeboden dienst.”

⁽³³⁾ PB L 157 van 30.4.2004, blz. 45 (hierna: HIER-richtlijn).

om te beoordelen of haar bepalingen toereikend zijn voor de doelen in verband met de handhaving van intellectuele-eigendomsrechten. Derhalve is de noodzaak van vervanging van het huidige systeem op basis van gerechtelijke procedures, dat nog niet is beproefd, op zijn minst twijfelachtig. Het bovenstaande roept de onvermijdelijke vraag op waarom bestaande overtredingen niet op passende wijze kunnen worden aangepakt met de bestaande civiel- en strafrechtelijke sancties op auteursrechtinbreuken. Voordat zij zulke beleidsmaatregelen voorstelt, dient de Commissie betrouwbare informatie te presenteren waaruit blijkt dat het huidige wettelijke kader niet de beoogde effecten heeft gesorteerd.

41. Verder is het onduidelijk of er serieus is nagedacht over alternatieve economische bedrijfsmodellen die niet de stelsmatige controle van individuele personen met zich meebrengen. Als auteursrechthebbers bijvoorbeeld kunnen aantonen dat hun verlies te wijten is aan P2P-gebruik, zouden rechthebbers en ISP's bijvoorbeeld gedifferentieerde abonnementen voor internettoegang kunnen uitproberen, waarbij een deel van de prijs voor een abonnement met onbeperkte toegang wordt verdeeld onder auteursrechthebbers.

De mogelijkheid om op minder indringende wijze gericht te controleren

42. Naast het gebruik van volledig andere modellen, dat zoals aangegeven moet worden onderzocht en beproefd, kan gerichte controle in elk geval op een minder inbreukmakende wijze worden uitgevoerd.

43. De doelstelling van handhaving van intellectuele-eigendomsrechten kan ook worden bereikt door slechts een beperkt aantal mensen te controleren die worden verdacht van het plegen van een niet-alledaagse overtreding van het auteursrecht. De HIER-richtlijn verschaft in dit verband enige richtsnoeren. Zij bepaalt de voorwaarden waaronder autoriteiten, met het oogmerk de intellectuele-eigendomsrechten te handhaven, opdracht mogen geven tot bekendmaking van persoonsgegevens die in het bezit zijn van internetaanbieders. In artikel 8 is bepaald dat ISP's van de bevoegde rechtshandhavingsinstanties opdracht kunnen krijgen persoonsgegevens te verstrekken die zij van vermeende overtreders in hun bezit hebben (bijvoorbeeld informatie over de oorsprong en de distributienetwerken van de goederen of diensten die inbreuk maken op intellectuele-eigendomsrechten) naar aanleiding van een gerechtvaardigd en evenredig verzoek in geval van overtredingen op *commerciële schaal*⁽³⁴⁾.

44. Hieruit volgt dat het criterium van de „commerciële schaal” beslissend is. Op grond van dit criterium kan controle

⁽³⁴⁾ Dit wordt nader bevestigd in overweging 14 van de HIER-richtlijn.

evenredig zijn in het kader van beperkte, specifieke ad hoc-situaties waarin gegronde verdenking bestaat van inbreuk op het auteursrecht op commerciële schaal. Dit criterium zou situaties kunnen omvatten van duidelijk misbruik van auteursrecht door particuliere personen met het oogmerk direct of indirect economisch of commercieel voordeel te behalen.

45. In de praktijk zouden auteursrechthebbers, om genoemde methode doeltreffend te doen zijn, gerichte controles van bepaalde IP-adressen kunnen uitvoeren teneinde de schaal van de overtreding van het auteursrecht te verifiëren. Dit zou betekenen dat auteursrechthebbers ook verslagen van vermeende overtredingen zouden mogen bijhouden voor dezelfde doeleinden. Zulke informatie dient alleen te worden gebruikt nadat het belang van de overtreding is geverifieerd, zoals in duidelijke gevallen van belangrijke overtredingen en bij onbelangrijke, maar aanhoudende overtredingen gedurende een bepaalde periode met het oogmerk van commercieel voordeel of financieel gewin. De noodzaak van continuïteit binnen bepaalde perioden wordt hierna benadrukt en nader toegelicht in verband met het beginsel van bewaring.
46. Dit zou betekenen dat in zulke gevallen het verzamelen van informatie met de bedoeling vermeende overtredingen aan te tonen, evenredig en noodzakelijk kan worden geacht voor de voorbereiding van gerechtelijke procedures, zoals een rechtsgeding.
47. De EDPS is van mening dat de wijze van gegevensverwerking die is gericht op het verzamelen van zulke bewijzen als extra waarborg vooraf dient te worden getoetst en goedgekeurd door nationale instanties voor gegevensbescherming. Deze mening is gestoeld op het feit dat de gegevensverwerking specifieke risico's voor de rechten en vrijheden van burgers met zich meebrengt in het licht van haar oogmerk, te weten de uitvoering van handhavingshandelingen die uiteindelijk strafbaar kunnen zijn gezien de gevoelige aard van de verzamelde gegevens. Het feit dat de verwerking ook de controle van elektronische communicatie inhoudt, is een aanvullende factor die versterkt toezicht vergt.
48. De EDPS is van mening dat de „commerciële schaal”, opgenomen in de HIER-richtlijn, een bijzonder passend criterium is om grenzen aan de controle te stellen teneinde het evenredigheidsbeginsel te eerbiedigen. Bovendien lijkt er geen betrouwbaar bewijs te zijn dat aantoonbaar doeltreffend gerechtelijk optreden tegen overtredingen van het auteursrecht op grond van de criteria van de HIER-richtlijn onmogelijk of niet doeltreffend is. Berichten zoals die bijvoorbeeld uit Duitsland komen, waar sinds 2008 na de omzetting van de HIER-richtlijn ongeveer 3 000 rechterlijke uitspraken zijn gedaan op grond waarvan ISP's de gegevens van 300 000 abonnees hebben vrijgegeven, lijken eerder het tegendeel aan te tonen.
49. Nu de HIER-richtlijn twee jaar van kracht is, is het derhalve moeilijk in te zien waarom wetgevers afstand zouden nemen van de criteria in deze richtlijn om over te gaan op indringender methoden, wanneer de EU nog maar net begonnen is met het toepassen van de recentelijk ingevoerde

methoden. Om dezelfde reden is het moeilijk de noodzaak in te zien van vervanging van het huidige rechterlijke stelsel door andere soorten maatregelen (nog afgezien van de twijfels over eerlijke rechtspleging, die hier niet worden behandeld).

IV.4. Overeenstemming van een drietrapsafsluitbeleid met meer gedetailleerde bepalingen inzake gegevensbescherming

50. Er zijn andere, meer specifieke wettelijke redenen waarom de drietrapsafsluitaanpak problematisch is vanuit het oogpunt van gegevensbescherming. De EDPS wil graag de aandacht vestigen op de twijfelachtige rechtsgrondslag voor gegevensverwerking, die wordt voorgeschreven door Richtlijn 95/46/EG, en de in Richtlijn 2002/58/EG opgenomen verplichting om logbestanden te verwijderen.

Rechtsgrondslag voor gegevensverwerking

51. Plannen voor een drietrapsafsluitbeleid brengen de verwerking van persoonsgegevens met zich mee, waarvan sommige worden gebruikt voor wettelijke of administratieve procedures voor de afsluiting van de toegang tot het internet voor recidiverende overtreeders. Vanuit dit oogpunt gelden zulke gegevens als gevoelige gegevens in de zin van artikel 8 van Richtlijn 95/46/EG. In artikel 8, lid 5, wordt bepaald: „Verwerkingen van gegevens inzake overtredingen, strafrechtelijke veroordelingen of veiligheidsmaatregelen mogen alleen worden verricht onder toezicht van de overheid of indien de nationale wetgeving voorziet in passende specifieke waarborgen, behoudens afwijkingen die een lidstaat kan toestaan uit hoofde van nationale bepalingen welke passende en specifieke waarborgen bieden...”
52. In dit verband is het relevant te herinneren aan voornoemd werkdocument van de Groep gegevensbescherming artikel 29, waarin de kwestie van de verwerking van justitiële gegevens aan de orde komt ⁽³⁵⁾. De Groep verklaart: „Hoewel ieder individu uiteraard het recht heeft data die het verloop van zijn of haar eigen rechtszaak betreffen, te verwerken, gaat dit principe niet zo ver dat uitvoering onderzoek en het verzamelen en centraliseren van persoonsgegevens door derden geoorloofd is, evenmin als, in het bijzonder, systematisch onderzoek op algemene schaal, zoals het scannen van het internet (...). Dergelijk onderzoek valt onder de bevoegdheid van de gerechtelijke instanties” ⁽³⁶⁾. Ofschoon het gericht verzamelen van specifiek bewijs, met name in gevallen van ernstige overtredingen, noodzakelijk kan zijn om een juridische eis te formuleren en uit te oefenen, is de EDPS het volledig eens met het standpunt van de Groep gegevensbescherming artikel 29 over het gebrek aan legitimering van breedschalig onderzoek waarbij massale hoeveelheden gegevens van internetgebruikers worden verwerkt.
53. De hiervoor beschreven discussie over het beginsel van evenredigheid en het criterium van de „commerciële schaal” zijn relevant voor de vaststelling onder welke omstandigheden het verzamelen van IP-adressen en daarmee samenhangende informatie gelegitimeerd is.

⁽³⁵⁾ Zie paragraaf 28 van dit advies.

⁽³⁶⁾ Onderstreping toegevoegd.

54. ISP's kunnen de verwerking door auteursrechthebbenden trachten te legaliseren door bepalingen in de overeenkomsten met klanten op te nemen die de controle van hun gegevens en de afsluiting van hun abonnement mogelijk maken. Door het sluiten van dergelijke overeenkomsten zouden klanten dan geacht worden te hebben ingestemd met de controle. Deze methode werpt echter de basisvraag op of iemand aan ISP's wel toestemming kan geven voor gegevensverwerking die niet wordt uitgevoerd door de ISP, maar door derden die niet onder het „gezag” van de ISP staan.
55. Ten tweede is er de vraag van de geldigheid van de toestemming. In artikel 2, onder h), van Richtlijn 95/46/EG wordt „toestemming van de betrokkene” gedefinieerd als „elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt”. Een belangrijk punt is dat een geldige toestemming, onder welke omstandigheden deze ook wordt gegeven, een vrije, specifieke en op informatie berustende wilsuiting moet zijn van degene wiens persoonsgegeven het betreft, zoals gedefinieerd in artikel 2, onder h), van de richtlijn. De EDPS betwijfelt in ernstige mate of personen aan wie wordt gevraagd toe te stemmen in de controle van hun internetactiviteiten, in de gelegenheid zijn een echte keuze te maken, vooral omdat het alternatief is dat zij geen toegang hebben tot het internet, waardoor mogelijk veel ander aspecten van hun leven worden geschaad.
56. Ten derde is het hoogst twijfelachtig of zulke controle ooit *noodzakelijk* kan worden geacht voor de uitoefening van een overeenkomst waarbij degene wiens persoonsgegeven het betreft partij is, zoals voorgeschreven in artikel 7, onder b), van Richtlijn 95/46/EG, aangezien de controle overduidelijk geen onderdeel van de door betrokkene gesloten overeenkomst uitmaakt, maar slechts een middel is waarmee de ISP andere belangen kan dienen.

Verwijderen van logbestanden

57. Uit hoofde van Richtlijn 2002/58/EG, meer in het bijzonder artikel 6, mogen verkeersgegevens zoals IP-adressen alleen worden verzameld en bewaard om redenen die rechtstreeks verband houden met de communicatie zelf, met inbegrip van facturering, verkeersstroombeheer en het oogmerk van fraudepreventie. Na afloop moeten de gegevens worden gewist. Dit doet niets af aan de bepalingen van de richtlijn betreffende de bewaring van gegevens, die — zoals hiervoor besproken — verplicht tot bewaring van verkeersgegevens en overlegging daarvan aan politie en aanklagers ter ondersteuning van het onderzoek naar uitsluitend **zwarte criminaliteit** ⁽³⁷⁾.

58. Overeenkomstig het bovenstaande moeten internetaanbieders elk logbestand verwijderen waarin activiteiten van internetgebruikers worden bekendgemaakt en dat niet langer noodzakelijk is voor voornoemde doeleinden. Aangezien logbestanden niet noodzakelijk zijn voor factureringsdoeleinden, lijkt een periode van drie of vier weken voor het verkeersstroombeheer door ISP's toereikend ⁽³⁸⁾.
59. Dit betekent dat ISP's, wanneer zij worden benaderd door auteursrechthebbenden, tenzij het contact tot stand komt in voornoemde beperkte periode, niet over de logbestanden mogen beschikken op basis waarvan de IP-adressen in verband kunnen worden gebracht met de relevante abonnees. Aanhouden van logbestanden na een dergelijke periode mag alleen worden toegestaan om gerechtvaardigde redenen binnen de reikwijdte van de in het recht verankerde doelen.
60. In de praktijk betekent dit dat verzoeken van auteursrechthebbenden aan een ISP niet kunnen worden gehonoreerd tenzij ze heel snel worden ingediend, eenvoudigweg omdat de ISP niet langer over de gevraagde gegevens beschikt. Dit feit op zich bepaalt de grenzen van wat wordt bedoeld met aanvaardbare controlepraktijken zoals hiervoor beschreven.

Risico's van doorwerkingseffecten

61. De EDPS is verder niet alleen bezorgd over de gevolgen voor privacy en gegevensbescherming van het drietrapsafsluitbeleid, maar ook over de doorwerkingseffecten van dat beleid. Als een drietrapsafsluitbeleid wordt toegestaan, kan dat het begin zijn van een hellend vlak waarop wij afglijden in de richting van legalisering van nog grootschaliger controle van de activiteiten van internetgebruikers, op verschillende gebieden en voor verschillende doeleinden.
62. De EDPS verzoekt de Commissie ervoor te zorgen dat de ACTA niet verder gaat dan en niet ingaat tegen de huidige EU-regeling voor de handhaving van intellectuele-eigendomsrechten, waarin grondrechten, fundamentele vrijheden en burgerrechten, zoals de bescherming van persoonsgegevens, worden geëerbiedigd.

V. ZORG OM GEGEVENS BESCHERMING IN VERBAND MET MECHANISMEN VOOR INTERNATIONALE SAMENWERKING

63. Een van de middelen die door deelnemers aan de ACTA-onderhandelingen naar voren worden gebracht om de

⁽³⁷⁾ Zie paragraaf 35 van dit advies.

⁽³⁸⁾ Verkeersstroombeheer omvat de analyse van het verkeer in een computernetwerk ten behoeve van het optimaliseren of garanderen van prestaties, verkorting van wachttijden en/of uitbreiding van de bruikbare bandbreedte.

kwestie van de handhaving van intellectuele-eigendomsrechten aan te pakken, is uitbreiding van de internationale samenwerking met een aantal maatregelen die een doeltreffende handhaving van intellectuele-eigendomsrechten in de rechtsgebieden van de ACTA-ondertekenaars mogelijk zouden maken.

64. Gezien de beschikbare informatie kan worden verwacht dat bepaalde maatregelen die worden voorgesteld voor de waarborging van de handhaving van intellectuele-eigendomsrechten, zullen leiden tot internationale uitwisseling van informatie over vermeende inbreuken op intellectuele-eigendomsrechten tussen publieke instanties (zoals douane, politie en justitie), maar ook tussen publieke en private partijen (zoals ISP's en organisaties van houders van intellectuele-eigendomsrechten). Zulke gegevensoverdrachten zijn in een aantal opzichten problematisch vanuit het gezichtspunt van gegevensbescherming.

V.1. Zijn de voorziene gegevensuitwisselingen in het kader van de ACTA legitiem, noodzakelijk en evenredig?

65. Bij de huidige stand van het onderhandelingsproces, waarin een aantal concrete elementen van de gegevensverwerking nog niet vastgesteld of onbekend zijn, kan onmogelijk worden geverifieerd of het voorgestelde raamwerk van maatregelen in overeenstemming is met de fundamentele beginselen van gegevensbescherming en met het EU-recht inzake gegevensbescherming.
66. Ten eerste is het de vraag of gegevensoverdrachten naar derde landen in het kader van de ACTA legitiem zijn. De relevantie van het treffen van internationale maatregelen op dit vlak kan in twijfel worden getrokken zolang er tussen de EU-lidstaten geen overeenstemming bestaat over de harmonisatie van handhavingmaatregelen in de digitale omgeving en de soorten strafrechtelijke sancties die moeten worden toegepast⁽³⁹⁾.
67. Gezien het bovenstaande lijkt het erop dat de beginselen van noodzakelijkheid en evenredigheid ten aanzien van de gegevensoverdrachten uit hoofde van de ACTA eenvoudiger kunnen worden nageleefd indien de overeenkomst uitdrukkelijk wordt beperkt tot de bestrijding van de ernstigste overtredingen van intellectuele-eigendomsrechten en geen bulkoverdracht van gegevens in verband met elke verdenking van overtreding van intellectuele-eigendomsrechten toestaat. Dit vereist een exacte definitie van de „ernstigste overtredingen van intellectuele-eigendomsrechten” waarvoor gegevensoverdrachten wel zijn toegestaan.
68. Daarenboven dient bijzondere aandacht te worden besteed aan hen die betrokken zijn bij de gegevensoverdrachten, en aan de vraag of gegevens alleen worden uitgewisseld tussen publieke instanties of dat uitwisseling ook is toegestaan tussen private partijen en publieke instanties. Zoals elders

in dit advies is geschetst, roept de betrokkenheid van private partijen op een terrein dat in beginsel tot de bevoegdheid van rechtshandavingsinstanties behoort, een aantal vragen op⁽⁴⁰⁾. De voorwaarden waaronder private partijen worden betrokken bij het verzamelen en uitwisselen met publieke instanties van persoonsgegevens die betrekking hebben op overtredingen van intellectuele-eigendomsrechten, dienen zich strikt te beperken tot specifieke omstandigheden met passende waarborgen.

V.2. Toepasselijk recht inzake gegevensbescherming ten aanzien van gegevensoverdrachten in het kader van de ACTA

Algemeen regime voor gegevensoverdrachten

69. Het algemene kader voor gegevensbescherming dat in de EU van toepassing is, wordt bepaald door Richtlijn 95/46/EG. De artikelen 25 en 26 van Richtlijn 95/46/EG definiëren het regime dat geldt voor overdrachten van gegevens naar derde landen. Artikel 25 bepaalt dat de doorgifte van gegevens alleen mag plaatsvinden aan landen die een toereikend beschermingsniveau waarborgen; overigens zijn zulke doorgiften in beginsel verboden.
70. De toereikendheid van de bescherming die derde landen bieden, wordt per geval beoordeeld door de Europese Commissie, die verschillende beschikkingen heeft afgegeven waarin de toereikendheid voor een aantal landen werd erkend na een grondige analyse door de Groep gegevensbescherming artikel 29⁽⁴¹⁾.
71. De EDPS merkt op dat de meeste deelnemers aan de ACTA-onderhandelingen geen deel uitmaken van de door de Commissie opgestelde lijst met landen die toereikende gegevensbescherming bieden. Met uitzondering van Zwitserland en — in specifieke omstandigheden — Canada en de Verenigde Staten, wordt geen van de ACTA-deelnemers erkend als land met een toereikend beschermingsniveau. Dit betekent dat voordat er gegevens vanuit de EU naar een van deze landen kunnen worden overgedragen, aan een van de voorwaarden van artikel 26, lid 1, van Richtlijn 95/46/EG moet worden voldaan of dat door partijen toereikende waarborgen moeten worden geboden bij de gegevensoverdracht overeenkomstig artikel 26, lid 2, van de richtlijn.

Specifiek regime voor gegevensoverdrachten op het terrein van strafrechtshandhaving

72. Richtlijn 95/46/EG vormt weliswaar het belangrijkste instrument voor gegevensbescherming in de EU, maar haar werkingsfeer is op het ogenblik beperkt doordat activiteiten die betrekking hebben op onder meer het optreden van

⁽³⁹⁾ Een voorstel over strafrechtelijke sancties is in behandeling bij de Raad, COM(2006) 168 van 26 april 2006.

⁽⁴⁰⁾ Zie paragraaf 32 en 52 van dit advies. Zie ook het advies van de EDPS van 11 november 2008 over het eindverslag van de EU-VS-Contactgroep op hoog niveau inzake informatie-uitwisseling en privacy en bescherming van persoonsgegevens, PB C 128 van 6.6.2009, blz. 1.

⁽⁴¹⁾ Zie de beschikkingen van de Europese Commissie betreffende de passende bescherming van persoonsgegevens door Argentinië, Canada, Zwitserland, het veiligheidsbeginsel van de VS en de Amerikaanse autoriteiten in PNR-context, Guernsey, Isle of Man en Jersey, beschikbaar op http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

de staat op het gebied van het strafrecht, uitdrukkelijk zijn uitgesloten (artikel 3). Gegevensuitwisselingen met het oog op handhaving van het strafrecht vallen derhalve buiten de werkingssfeer van Richtlijn 95/46/EG en zijn onderworpen aan de algemene beginselen van gegevensbescherming die zijn vastgelegd in Verdrag nr. 108 van de Raad van Europa en het Aanvullend Protocol dat door alle EU-lidstaten is onderschreven⁽⁴²⁾. Bovendien gelden de regels die door de EU zijn vastgesteld voor de samenwerking van politie en justitie op het terrein van strafzaken, zoals bepaald in het kaderbesluit 2008/877/JHA van de Raad⁽⁴³⁾.

73. Deze instrumenten stellen eveneens als beginsel voorop dat er een toereikend niveau van gegevensbescherming moet zijn in het derde land waarnaar de gegevens worden overgedragen. Er is voorzien in een aantal uitzonderingen, met name wanneer het derde land toereikende waarborgen verschaft. Net als bij gegevensuitwisselingen op grond van Richtlijn 95/46/EG, moeten bij gegevensuitwisselingen op het terrein van de strafrechtshandhaving tussen de partijen toereikende waarborgen worden geboden voordat de overdracht kan plaatsvinden.

Naar een nieuw regime voor gegevensoverdracht

74. Naar verwachting zal de EU in de nabije toekomst nieuwe gemeenschappelijke regels voor gegevensbescherming vaststellen op grond van artikel 16 van het VWEU, die van toepassing zullen zijn op alle terreinen waarop de EU actief is. Dit betekent dat er over een paar jaar een alomvattend kader voor gegevensbescherming in de EU kan bestaan, waarin samenhangende regels zijn opgenomen voor de bescherming van gegevens op alle terreinen waarop de EU actief is en dat hetzelfde niveau van waarborgen en garanties zal bieden voor alle gegevensverwerkende activiteiten. Zoals is uiteengezet door Viviane Reding⁽⁴⁴⁾, commissaris voor Justitie, grondrechten en burgerschap, moet dit nieuwe kader werken als één „modern en allesomvattend rechtsinstrument” voor gegevensbescherming in de EU. Zo'n kader wordt in het bijzonder toegejuicht omdat het meer duidelijkheid en consistentie zal verschaffen ten aanzien van de regels die in de EU met betrekking tot gegevensbescherming gelden.
75. In internationaal verband wijst de EDPS ook op de resolutie inzake internationale normen voor de bescherming van persoonsgegevens en privacy die onlangs is aangenomen door gegevensbeschermingsautoriteiten, en die een eerste stap is op weg naar mondiale normen voor gegevensbescherming⁽⁴⁵⁾. De internationale normen omvatten een

aantal waarborgen voor gegevensbescherming die vergelijkbaar zijn met die van Richtlijn 95/46/EG en Handvest nr. 108. Hoewel de internationale normen nog niet bindend zijn, verschaffen ze wel nuttige richtsnoeren inzake de beginselen van gegevensbescherming, die vrijwillig kunnen worden toegepast door derde landen om hun wettelijk kader verenigbaar te maken met de normen van de EU. De EDPS meent dat ook de ondertekenaars van de ACTA rekening moeten houden met de beginselen van de internationale normen wanneer zij persoonsgegevens uit de EU verwerken.

V.3. Noodzaak van de invoering van passende waarborgen voor de bescherming van gegevensoverdrachten van de EU naar derde landen

In welke vorm kunnen de waarborgen voor de bescherming van gegevensoverdrachten naar derde landen doeltreffend zijn?

76. Als de noodzaak van de overdracht van persoonsgegevens naar derde landen is aangetoond, benadrukt de EDPS dat de Europese Unie met ontvangers in derde landen moet onderhandelen — in aanvulling op de overeenkomst over de ACTA zelf — over specifieke instrumenten die passende waarborgen voor de bescherming van gegevens bevatten waarmee de uitwisseling van persoonsgegevens wordt geregeld.
77. Passende waarborgen voor gegevensbescherming moeten bij voorkeur worden opgenomen in een bindende overeenkomst tussen de EU en het ontvangende derde land, waarbij de ontvangende partij verklaart het EU-recht inzake gegevensbescherming te eerbiedigen en aan individuen dezelfde rechten en rechtsmiddelen te gunnen als die conform het EU-recht. De noodzaak van een bindende overeenkomst komt voort uit artikel 26, lid 2, van Richtlijn 95/46/EG en artikel 13, lid 3, onder b), van het kaderbesluit, en wordt bovendien ondersteund door de bestaande praktijk van de EU om specifieke overeenkomsten te sluiten voor specifieke gegevensoverdrachten naar derde landen⁽⁴⁶⁾.
78. Evenzo kan de ontvanger op grond van het ontwerp voor de internationale normen worden verplicht te garanderen dat hij voor de overdracht het vereiste beschermingsniveau zal bieden. Zulke garanties kunnen ook de vorm van een overeenkomst aannemen.

Inhoud van de door ACTA-ondertekenaars overeen te komen waarborgen met betrekking tot de overdracht van persoonsgegevens

79. De EDPS benadrukt dat internationale uitwisselingen van informatie met rechtshandhaving als doel bijzonder gevoelig zijn vanuit het oogpunt van gegevensbescherming, omdat in dat kader massale gegevensoverdrachten kunnen

⁽⁴²⁾ Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, aangenomen in Straatsburg op 28 januari 1981, en Raad van Europa, Aanvullend Protocol Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens betreffende toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens, Straatsburg, 8 november 2001.

⁽⁴³⁾ Kaderbesluit 2008/877/JHA van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken, PB L 350 van 30.12.2008, blz. 60.

⁽⁴⁴⁾ Zie de antwoorden op vragen van het Europees Parlement aan kandidaat-commissaris Viviane Reding, blz. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

⁽⁴⁵⁾ Resolutie aangenomen in Madrid in november 2009.

⁽⁴⁶⁾ Voorbeelden zijn overeenkomsten van Europol en Eurojust met de VS, de PNR-overeenkomst, de Swift-overeenkomst en de overeenkomst tussen de EU en Australië over de verwerking en overdracht van uit de Europese Unie afkomstige PNR-gegevens („passenger name records”) door luchtvaartmaatschappijen aan de Australische douane.

worden gelegaliseerd op een terrein waar het effect op individuele burgers bijzonder ernstig is en waar strikte en betrouwbare waarborgen des te noodzakelijker zijn.

80. De EDPS meent dat specifieke voorwaarden en waarborgen alleen per geval kunnen worden gedefinieerd in het licht van alle factoren van de gegevensuitwisselingen. Om toch een leidraad te verschaffen, wordt hieronder ingegaan op een aantal beginselen en waarborgen die door ontvangende derde partijen moeten worden nageleefd voordat de gegevensoverdrachten kunnen plaatsvinden:

— Er moet worden geverifieerd wat de wettelijke rechtvaardiging is voor de gegevensverwerking die plaatsvindt (dat wil zeggen, is de verwerking gebaseerd op een wettelijke verplichting, op toestemming van de betrokkenen of op een andere geldige rechtvaardiging?), en of gegevensoverdrachten voldoen aan het aanvankelijke doel van de gegevensverzameling. Buiten het gespecificeerde doel mogen geen overdrachten plaatsvinden;

— De hoeveelheid en het soort uit te wisselen persoonsgegevens dienen duidelijk te worden gespecificeerd en te worden beperkt tot wat strikt noodzakelijk is om het doel van de overdracht te bereiken. De verzamelde en overgedragen persoonsgegevens kunnen met name het IP-adres van de internetgebruiker, de datum en de tijd van de vermeende overtreding en het soort misdrijf omvatten. De EDPS adviseert gegevens tijdens de onderzoeksfase niet te koppelen aan een specifiek individu en herinnert eraan dat identificatie van een verdachte alleen mag plaatsvinden in overeenstemming met het recht en onder toezicht van een rechter. In dat verband meent de EDPS dat gegevens met betrekking tot overtredingen en vermeende overtredingen van intellectuele-eigendomsrechten een speciale gegevenscategorie vormen, waarvan de verwerking gewoonlijk is voorbehouden aan rechtshandhavingsinstanties, en de toepassing van aanvullende waarborgen vereist. Degenen die gemachtigd zijn gegevens met betrekking tot overtredingen en vermeende overtredingen van intellectuele-eigendomsrechten te verwerken alsmede de voorwaarden voor de verwerking van die gegevens moeten daarom specifiek worden gedefinieerd in overeenstemming met het bestaande recht inzake gegevensbescherming;

— De personen met wie de gegevens mogen worden gedeeld, moeten duidelijk worden bepaald en het doorsturen van de gegevens naar andere ontvangers moet in beginsel verboden zijn, tenzij dit noodzakelijk is voor een specifiek onderzoek. Deze beperking is bijzonder wezenlijk, omdat de aangewezen ontvangers niet ten onrechte informatie mogen delen met niet-gemachtigde ontvangers;

— De EDPS gaat ervan uit dat de ACTA niet alleen zal voorzien in samenwerking tussen overheidsinstanties,

maar ook handhavingstaken zal toebedelen aan private organisaties (zoals ISP's, organisaties van auteursrechthebbers, enzovoort). In het laatstgenoemde geval moeten de voorwaarden voor en de mate van betrokkenheid van private organisaties bij de handhaving van intellectuele-eigendomsrechten zorgvuldig worden beoordeeld, in die zin dat de ACTA-maatregelen niet mogen inhouden dat ISP's en organisaties van houders van intellectuele-eigendomsrechten in feite het recht krijgen om het online-gedrag van gebruikers te controleren. Bovendien mag de verwerking van persoonsgegevens door particuliere organisaties in het kader van rechtshandhaving alleen plaatsvinden op een toereikende rechtsgrond. Ook is het belangrijk dat wordt opgehelderd of particuliere organisaties verplicht worden om samen te werken met de politie en hoe ver die samenwerking mag gaan. Zij dient zich in elk geval te beperken tot „zware criminaliteit”, een begrip waarvan bovendien een precieze definitie moet worden vastgelegd omdat niet alle inbreuken op intellectuele-eigendomsrechten kunnen worden beschouwd als zware misdrijven;

— De methode waarmee persoonsgegevens worden uitgewisseld, moet duidelijk worden gekozen. Er dient met name te worden gespecificeerd of er een push-systeem wordt gehanteerd — waarbij ISP's en organisaties van houders van intellectuele-eigendomsrechten bijvoorbeeld onder hun eigen toezicht een aantal gegevens overdragen aan derden, zoals de politie en rechtshandhavingsinstanties in het buitenland — dan wel een pull-systeem — waarbij de politie en de rechtshandhavingsinstanties bijvoorbeeld rechtstreeks toegang hebben tot databanken van private partijen of databanken waarin informatie centraal wordt opgeslagen. Zoals al is geschetst in verband met de PNR, is een push-systeem de enige optie die voldoet aan de beginselen van gegevensbescherming uit het oogpunt van de EU, omdat het de verzender in de EU, die hoogstwaarschijnlijk voor de verwerking verantwoordelijk is, in staat stelt controle uit te oefenen op de gegevensoverdracht ⁽⁴⁷⁾;

— Er moet worden gespecificeerd gedurende welke periode persoonsgegevens moeten worden bewaard door de ontvangers, en het doel waarvoor dit noodzakelijk is. De bewaarperiode moet evenredig zijn in het licht van het beoogde doel, hetgeen wil zeggen dat gegevens moeten worden verwijderd of gewist wanneer ze niet langer nodig zijn om dat doel te bereiken;

— De plichten van gegevensbeheerders in derde landen moeten duidelijk worden vastgelegd. Er dienen toezichtmechanismen en/of handhaafbare verantwoordingsmechanismen te worden gegarandeerd, met doeltreffende verhaalsmogelijkheden en sancties tegen gegevensbeheerders in gevallen van ongepaste verwerking

⁽⁴⁷⁾ Zie advies 4/2003 van de Groep gegevensbescherming artikel 29 over de mate van bescherming die in de VS wordt geboden voor de uitwisseling van passagiersgegevens, WP78, 13 juni 2003.

of andere relevante incidenten. Bovendien moeten er rechtsmiddelen worden ingevoerd waarmee individuele burgers zich kunnen beklagen bij een onafhankelijke instantie voor gegevensbescherming zodat zij doeltreffend verhaal kunnen halen bij een onafhankelijk en onpartijdig tribunaal ⁽⁴⁸⁾;

- In het instrument dat de partijen overeenkomen, dient duidelijk te worden gespecificeerd wat de rechten van betrokkenen met betrekking tot hun persoonsgegevens zijn wanneer zulke gegevens worden verwerkt door een ontvangende derde partij, teneinde te waarborgen dat zij over doeltreffende middelen beschikken om hun rechten ten aanzien van verwerking in het buitenland uit te oefenen;
- Transparantie is bovendien cruciaal en de bij het rechtsinstrument voor gegevensbescherming betrokken partijen moeten overeenkomen hoe zij betrokkenen informeren over de gegevensverwerking die plaatsvindt, alsmede over hun rechten en de wijze waarop zij die kunnen uitoefenen.

VI. CONCLUSIES

81. De EDPS moedigt de Europese Commissie krachtig aan een openbare en transparante dialoog te beginnen over de ACTA, mogelijk door middel van een openbare raadpleging, waarmee tevens wordt bevorderd dat de te nemen maatregelen voldoen aan de eisen van het EU-recht inzake privacy en gegevensbescherming.
82. De EDPS doet een beroep op de Europese Commissie om tijdens de lopende onderhandelingen over de ACTA een goed evenwicht te bereiken tussen de roep om bescherming van intellectuele-eigendomsrechten en het recht op persoonlijke levenssfeer en gegevensbescherming. De EDPS onderstreept dat het met name van cruciaal belang is om vanaf het begin van de onderhandelingen rekening te houden met privacy en gegevensbescherming, voordat maatregelen worden overeengekomen, zodat er later niet hoeft te worden gezocht naar alternatieve oplossingen die in overeenstemming zijn met de privacyregels.
83. Hoewel intellectuele eigendom een belangrijk punt is voor de samenleving en beschermd dient te worden, mag het niet worden geplaatst boven het fundamentele recht van burgers op privacy en gegevensbescherming, of boven andere rechten zoals het vermoeden van onschuld, doeltreffende rechtsbescherming en vrijheid van meningsuiting.
84. Voor zover het huidige ontwerp van de ACTA een drietrapsafsluitbeleid omvat of daar ten minste indirect op aanstuurt, houdt de ACTA een ingrijpende beperking in van de grondrechten en vrijheden van Europese burgers, met name wat betreft de bescherming van persoonsgegevens en de privacy.
85. De EDPS is van mening dat een drietrapsafsluitbeleid niet noodzakelijk is om de beoogde handhaving van intellectuele-eigendomsrechten te bereiken. De EDPS is ervan overtuigd dat er andere, minder ingrijpende oplossingen bestaan of dat het voorziene beleid in elk geval op een minder inbreukmakende wijze of met een beperktere reikwijdte kan worden uitgevoerd, met name in de vorm van gerichte ad hoc-controle.
86. Het drietrapsafsluitbeleid is ook problematisch op een meer gedetailleerd wettelijk niveau, vooral omdat de verwerking van justitiële gegevens, in het bijzonder door private organisaties, moet zijn gebaseerd op een goede rechtsgrondslag. De toepassing van drietrapsregelingen kan verder leiden tot de langdurige opslag van logbestanden, hetgeen in strijd zou zijn met bestaande wetgeving.
87. Voor zover de ACTA de uitwisseling van persoonsgegevens tussen instanties en/of particuliere organisaties in de deelnemende landen met zich meebrengt, doet de EDPS een beroep op de Europese Unie om toereikende waarborgen in te voeren. Deze waarborgen dienen van toepassing te zijn op alle gegevensoverdrachten die in het kader van de ACTA worden uitgevoerd — ongeacht of deze zich afspelen op het terrein van de strafrechtelijke, civielrechtelijke of digitale rechtshandhaving — en te voldoen aan de beginselen voor gegevensbescherming die zijn vastgelegd in Verdrag nr. 108 en Richtlijn 95/46/EG. De EDPS adviseert de waarborgen de vorm te geven van bindende overeenkomsten tussen de verzenders in de EU en de ontvangers in derde landen.
88. De EDPS wenst verder te worden geconsulteerd over de maatregelen die moeten worden uitgevoerd met betrekking tot de gegevensoverdrachten die uit hoofde van de ACTA zullen worden uitgevoerd, teneinde hun evenredigheid te verifiëren en na te gaan of ze een toereikend niveau van gegevensbescherming waarborgen.

Gedaan te Brussel, 22 februari 2010.

Peter HUSTINX
*Europese Toezichthouder voor
 gegevensbescherming*

⁽⁴⁸⁾ Zie het advies van de EDPS van 11 november 2008 over het eindverslag van de EU-VS-Contactgroep op hoog niveau inzake informatie-uitwisseling en privacy en bescherming van persoonsgegevens.