DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een besluit van het Europees Parlement en de Raad tot vaststelling van een meerjarenprogramma van de Gemeenschap betreffende de bescherming van kinderen die het internet en andere communicatietechnologieën gebruiken

(2009/C 2/02)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 286,

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 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 ([2]), en met name op artikel 41,

Gezien het verzoek van de Europese Commissie om advies op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 dat op 4 maart 2008 is ontvangen,

BRENGT HET VOLGENDE ADVIES UIT

I. **INLEIDING**

Raadpleging van de EDPS

1. Het voorstel voor een besluit van het Europees Parlement en de Raad tot vaststelling van een communautair meerjarenprogramma betreffende de bescherming van kinderen die het internet en andere communicatietechnologieën gebruiken (hierna „het voorstel" te noemen), op 4 maart 2008 is door de Commissie op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 voor advies aan de EDPS (Europese Toezichthouder voor gegevensbescherming) toegezonden. Deze raadpleging dient uitdrukkelijk te worden vermeld in de preambule van het besluit.

De context van het voorstel

2. Het nieuwe meerjarenprogramma (hierna „het programma" genoemd) ligt in het verlengde van het programma Veiliger internet (1999-2004) en de programma's Veiliger internet plus (2005-2008).

3. Het programma omvat de volgende punten:

   — reduceren van illegale online-inhoud en aanpakken van schadelijk onlinegedrag;

   — bevordering van een veiliger onlineomgeving;

   — bewustmaking van het publiek;

   — oprichten van een kennisbasis.

4. Het programma vormt een samenhangend geheel en is een aanvulling op andere communautaire beleidsmaatregelen, programma's en acties ter zake. Gezien het aantal bestaande regelgevende maatregelen op het gebied van de bescherming van kinderen in verband met nieuwe technologieën concentreert het zich meer op actie dan op regelgeving. Het accent ligt vooral op de doeltreffendheid en de doelmatigheid van mogelijke initiatieven alsook op de aanpassing aan de ontwikkeling van nieuwe technologieën. Hiertoe beoogt het programma de uitwisseling van informatie en goede praktijken te bevorderen.

5. Als kaderinstrument gaat het programma niet gedetailleerd in op de te ondernemen actie, maar voorziet het in uitnodigingen tot het indienen van voorstellen en in aanbestedingen met betrekking tot de vier vastgestelde punten.

Invalshoek van het advies

6. Het programma is in het algemeen gericht, op de bescherming van kinderen die het internet en andere communicatietechnologieën gebruiken, zonder dat het veel aandacht besteedt aan de privacyaspecten van de kwestie ([3]). Alhoewel de EDPS de doelstelling van het voorstel steunt, wil hij in dit advies toch op de privacyaspecten wijzen.

([1]) PB L 281 van 23.11.1995, blz. 31.
([2]) PB L 8 van 12.1.2001, blz. 1.

([3]) In de effectbeoordeling staan enkele verwijzingen naar privacy (3.2. Specifieke risico's: de openbaarmaking van persoonsgegevens; 3.3. Doelgroepen; 5.2. Analyse van de impact van de beleidsopties), maar deze zijn niet bijzonder uitgebreid.

7. De EDPS acht het van essentieel belang dat de geplande initiatieven in overeenstemming zijn met de bestaande wetgeving zoals genoemd in het voorstel ([1]), met name Richtlijn 2000/31/EG inzake e-handel, Richtlijn 2002/58/EG inzake e-privacy, en Richtlijn 95/46/EG inzake gegevensbescherming ([2]).

8. Er moet rekening worden gehouden met de bescherming van persoonsgegevens die de verschillende bij het programma betrokken aspecten en actoren betreffen. Het beschermen van persoonsgegevens van kinderen is uiteraard de belangrijkste aangelegenheid, maar niet de enige: er dient namelijk ook rekening te worden gehouden met persoonsgegevens en met online-inhoud die met oog op de bescherming van kinderen onder toezicht staat.

9. Deze aangelegenheden zullen in dit advies als volgt nader worden toegelicht:

   — in hoofdstuk II zal nader worden ingegaan op het verband tussen gegevensbescherming en de veiligheid van kinderen, waarbij het feit wordt belicht dat de bescherming van persoonsgegevens van kinderen een onontbeerlijke stap is in de richting van meer veiligheid en het voorkomen van misbruik;

   — in hoofdstuk III wordt beklemtoond dat het verwerken van persoonsgegevens ook inherent is aan het rapporteren, filteren of afschermen van verdachte inhoud of personen op het internet:

      — in eerste instantie zal de vraag betreffende het rapporteren van verdachte feiten of personen vanuit het oogpunt van gegevensbescherming worden onderzocht;

      — het tweede gedeelte zal zich voornamelijk concentreren op de rol van technische instrumenten;

      — ten slotte komt de verantwoordelijkheid van het bedrijfsleven in verband met zijn controle over gebruikersdata en inhoudsdata aan de orde.

II. **BESCHERMING VAN PERSOONSGEGEVENS EN VEILIGHEID VAN KINDEREN**

10. De EDPS steunt ten volle de doelstelling van het programma alsook de voor de verbeterde bescherming van kinderen in de onlineomgeving gedefinieerde richtsnoeren. Met name dienen beslissende maatregelen zoals de bewustmaking van kinderen en andere betrokken actoren en het beteugelen van illegale of schadelijke inhoud verder te worden uitgewerkt.

11. De EDPS wenst er tevens opnieuw op te wijzen dat een passende bescherming van de persoonsgegevens van het kind een hoogst belangrijke voorbereidende stap vormt voor het garanderen van een veilige onlineomgeving. Dit verband tussen de privacy en de veiligheid van het kind staat uitdrukkelijk vermeld in de recente verklaring van het Comité van ministers (Europaraad) betreffende de bescherming van de waardigheid, de zekerheid en het privéleven van kinderen die het internet gebruiken ([3]). De verklaring herinnert aan het recht van kinderen op de *waardigheid, de speciale bescherming en de zorg die nodig zijn voor hun welzijn, alsook aan hun recht op bescherming tegen alle vormen van discriminatie of willekeurige of onwettige inmenging in hun privéleven en tegen onwettige aanvallen op hun eer en reputatie.*

12. Als voorbeeld van de risico's die nauw met het beschermen van het privéleven van kinderen samenhangen, noemt de verklaring de traceerbaarheid van activiteiten van minderjarigen die hen aan criminele activiteiten kunnen blootstellen, zoals het zoeken van toenadering met seksuele bedoelingen (kinderlokkerij) of andere illegale activiteiten. Het weergeven of bewaren van persoonsgegevens die het internetgebruik van minderjarigen betreffen kan eveneens een potentieel risico van misbruik met zich meebrengen, bijvoorbeeld gebruik voor commerciële doeleinden of voor zoekacties door onderwijsinstellingen of mogelijke werkgevers. De verklaring verlangt derhalve het wissen of verwijderen binnen een redelijk korte termijn van de online-inhoud die door kinderen wordt achtergelaten, en roept op tot het ontwikkelen en verspreiden van informatie die aan kinderen dient te worden verstrekt, met name betreffende het bevoegde gebruik van instrumenten die toegang tot informatie verschaffen (zoekmachines), het ontwikkelen van een kritische analyse van online-inhoud en het verwerven van passende communicatievaardigheden.

13. De EDPS steunt deze bevindingen. Met name acht de EDPS het belangrijk kinderen meer bewust te maken van de risico's die aan een spontane mededeling van persoonsgegevens zoals naam, leeftijd en woonplaats verbonden zijn.

14. Punt 3 van de door het meerjarenprogramma voorgelegde maatregelen ([4]) is speciaal gewijd aan de „Bewustmaking van het publiek" door middel van tot kinderen, ouders, voogden en opvoeders gerichte bewustmakingsacties betreffende de kansen en risico's die verband houden met het gebruik van onlinetechnologieën en „middelen om veilig online te kunnen gaan". De in het voorstel genoemde instrumenten omvatten onder andere het verspreiden van relevante informatie en het instellen van contactpunten waar ouders en kinderen antwoord kunnen krijgen op vragen over veilig online gaan. Deze twee nuttige instrumenten dienen uitdrukkelijk een rol te spelen bij het beschermen van de persoonsgegevens van minderjarigen.

15. De EDPS wil duidelijk beklemtonen dat gegevensbeschermingsautoriteiten in dit kader relevante gesprekspartners zijn. Zij dienen dus apart in het voorstel vermeld te worden, met name waar sprake is van de bevordering van samenwerking en uitwisseling van informatie, ervaringen en goede praktijken op zowel nationaal als Europees niveau ([5]).

([1]) Toelichting, 2.1. Het regelgevingskader; Samenvatting van de effectbeoordeling, 1.2. Stand van zaken: wetgeving.

([2]) — Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („Richtlijn inzake elektronische handel") (PB L 178 van 17.7.2000, blz. 1);
— 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 (Richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37);
— 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 (PB L 281 van 23.11.1995, blz. 31).

([3]) Verklaring door het Comité van Ministers goedgekeurd op 20 februari 2008 op de 1018ste bijeenkomst van de afgevaardigden van de ministers, beschikbaar op de volgende website: „wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001".

([4]) Bijlage 1, Acties, punt 3.

([5]) Bijlage 1, Acties, punt 1.

16. In dit opzicht kunnen verschillende initiatieven als illustratie van onlangs door EU-lidstaten of EER-lidstaten genomen acties worden genoemd. Zo heeft de Zweedse gegevensbeschermingsautoriteit een jaarlijks onderzoek gestart over de houding van jongeren ten opzichte van internet en toezicht, terwijl de gegevensbeschermingsautoriteit van het Verenigd Koninkrijk ([1]) een onderzoek heeft uitgevoerd onder 2000 kinderen tussen de 14 en 21 jaar. In januari 2007 heeft de Noorse gegevensbeschermingsautoriteit in samenwerking met het ministerie van Onderwijs een tot scholen gerichte informatiecampagne gelanceerd ([2]). In Portugal werd tussen de gegevensbeschermingsautoriteit en het ministerie van Onderwijs een protocol ter bevordering van een „gegevensbeschermingscultuur" met betrekking tot het internet en met name tot sociale netwerken ondertekend ([3]). Ingevolge dit project hebben Portugese sociale netwerken een interface alsook een mascotte voor kinderen tussen 10 en 15 jaar opgenomen/geïntegreerd.

17. Deze voorbeelden illustreren de actieve en beslissende rol van de gegevensbeschermingsautoriteiten op gebied van de bescherming van kinderen online, alsook de noodzaak om deze actoren expliciet als gesprekspartners in het meerjarenprogramma op te nemen.

III. BESCHERMING VAN PERSOONSGEGEVENS EN RECHTEN VAN ANDERE BELANGHEBBENDEN

I. *Registers en uitwisseling van gegevens*

18. In het eerste punt van het voorstel (reduceren van illegale online-inhoud en aanpakken van schadelijk onlinegedrag ([4])) staat de instelling van contactpunten waar illegale online-inhoud en schadelijk onlinegedrag kan worden gemeld centraal. Onbetwistbaar is dat illegale online-inhoud en schadelijk onlinegedrag ter kennis van de competente autoriteiten dient te worden gebracht om op doelmatige wijze te worden bestreden. In verband met de bescherming van kinderen maar bijvoorbeeld ook in het kader van de bestrijding van spam werden reeds contactpunten opgezet ([5]).

19. De EDPS neemt er niettemin nota van dat het begrip „schadelijke inhoud" onduidelijk blijft. Er wordt namelijk niets gezegd over wie verantwoordelijk is voor het definiëren van schadelijke inhoud en op basis van welke criteria deze aldus kan worden beschouwd. Dit is des te zorgwekkender gezien de gevolgen van het rapporteren van dergelijke inhoud.

20. Zoals reeds hierboven vermeld, gaat het in het kader van het huidige programma bovendien niet alleen om de persoonsgegevens van kinderen, maar ook om de persoonsgegevens van personen die op enigerlei wijze betrokken zijn bij de informatie die op het netwerk circuleert. Het kan daarbij bijvoorbeeld gaan om de persoon die van onrechtmatig gedrag wordt verdacht en als verdacht wordt gemeld, maar ook om de persoon die dergelijk onlinegedrag of verdachte online-inhoud rapporteert, of om het slachtoffer van het misbruik. Hoewel deze informatie voor een efficiënt meldingssysteem noodzakelijk is, acht de EDPS het van belang eraan te herinneren dat deze informatie altijd in overeenstemming met de gegevensbeschermingsbeginselen dient te worden verwerkt.

21. Het kan zelfs voorkomen dat bepaalde gegevens specifieke bescherming behoeven, indien ze als gevoelige gegevens in de zin van artikel 8 van Richtlijn 95/46/EG kunnen worden beschouwd. Dit kan bijvoorbeeld het geval zijn voor data die plegers van inbreuken of slachtoffers van misbruik betreffen, met name op het gebied van kinderpornografie. Er zij op gewezen dat op nationaal niveau sommige meldingssystemen een aanpassing van de wetgeving inzake gegevensbescherming hebben vereist om het verwerken van juridische data betreffende verdachten of slachtoffers mogelijk te maken ([6]). De EDPS wijst er met klem op dat eventuele op te zetten meldingssystemen rekening moeten houden met het bestaande wettelijke kader voor gegevensbescherming. Het aantonen van een algemeen belang alsook het bestaan van garanties ten aanzien van het — in principe door rechtshandhavingsautoriteiten uitgevoerde — systeemtoezicht zijn voorwaarden om aan dit kader te voldoen.

II. *De rol van technische instrumenten vanuit privacyoogpunt*

22. Het gebruik van technische instrumenten wordt aangemoedigd als één van de oplossingen om illegale online-inhoud en schadelijk onlinegedrag aan te pakken ([7]). Voorbeelden van dergelijke instrumenten staan in de effectbeoordeling ([8]) en omvatten leeftijdsherkenning, gezichtsherkenning (voor het identificeren van slachtoffers door rechtshandhavingautoriteiten) en filtertechnologieën. Volgens het voorstel zouden deze instrumenten beter aan praktische behoeften moeten worden aangepast en voor relevante belanghebbenden toegankelijk moeten zijn.

23. De EDPS heeft zich reeds duidelijk uitgesproken ([9]) voor het gebruik van nieuwe technologieën om de bescherming van individuele rechten te verbeteren. De EDPS is van oordeel dat het beginsel „ingebouwde privacy" vooropgesteld moet worden bij de technologische ontwikkeling die het verwerken van persoonsgegevens impliceert. Derhalve moedigt de EDPS het opzetten van projecten die dergelijke technologieën ontwikkelen, ten zeerste aan.

24. Het is van groot belang systemen te ontwikkelen die het prijsgeven van de persoonsgegevens van kinderen zo veel mogelijk beperken en kinderen zowel betrouwbare bescherming bieden als de gelegenheid om de nieuwe instrumenten van de Informatiemaatschappij, zoals sociale netwerken, op een veiliger manier te gebruiken.

([1]) Zie volgende website: „www.ico.gov.uk/youngpeople".
([2]) Zie volgende website: „www.dubestemmer.no".
([3]) Zie „dadus.cnpd.pt/".
([4]) Bijlage 1 bij het voorstel.
([5]) Zie bv. de voor deze doeleinden door de Belgische autoriteiten ingerichte website: www.ecops.be
([6]) Zie de Belgische gegevensbeschermingswetgeving van 8 december 1992, artikel 3, lid 6, met betrekking tot de verwerking van gegevens door het Centrum voor sexueel misbruikte en verdwenen kinderen.
([7]) Bijlage 1, Acties, punt 1.
([8]) Effectbeoordeling, punt 3.1.
([9]) EDPS jaarverslag 2006, deel 3.5.1. Technologische Ontwikkelingen.

25. Gememoreerd zij niettemin dat technologische instrumenten, afhankelijk van de manier waarop ze worden gebruikt, zeer uiteenlopende gevolgen voor personen kunnen hebben. Als ze worden gebruikt om informatie te filteren of af te schermen, kunnen ze de toegang van minderjarigen tot potentieel schadelijke inhoud stoppen, maar ook iemand beletten toegang tot legitieme informatie te krijgen.

26. Hoewel hier het meeste gewicht wordt toegekend aan de vrije toegang tot informatie, zijn er ook consequenties voor de privacy. In het kader van de meest recente ontwikkelingen op het gebied van filtertechnieken met behulp van identiteitsbeheer, kan het filteren van informatie op basis van bepaalde criteria gebeuren, met inbegrip van persoonsgegevens, zoals de leeftijd van de op internet aangesloten persoon (om te voorkomen dat volwassenen of kinderen toegang hebben tot specifieke inhoud), de informatie-inhoud zelf alsook de verkeersgegevens die aan die identiteit van de auteur van de informatie gekoppeld zijn. Afhankelijk van de manier waarop deze persoonsgegevens — automatisch — worden verwerkt, kunnen de betreffende personen met gevolgen worden geconfronteerd die betrekking hebben op hun recht op onlinecommunicatie.

27. Filter- en afscherminstrumenten om de toegang tot netwerken te controleren moeten derhalve voorzichtig worden ingezet, en er dient rekening te worden gehouden met mogelijke negatieve effecten. Ook moeten de privacyversterkende mogelijkheden die de technologie te bieden heeft, maximaal worden benut.

28. De EDPS is ingenomen met de precisering in de effectbeoordeling ([1]) dat geen van de voorgestelde opties afbreuk mag doen aan het recht op eerbiediging van het privéleven of aan de vrijheid van meningsuiting. Hij sluit zich eveneens aan bij het standpunt dat „user empowerment" (overdracht van de beslissingsbevoegdheid aan de gebruiker) een van de hoofddoelen vormt, namelijk het in staat stellen van de gebruiker betere keuzes te maken en op passende wijze te handelen om kinderen te beschermen ([2]).

III. *De verantwoordelijkheid van dienstverleners*

29. De samenwerking van alle belanghebbenden wordt in het voorstel als een noodzakelijk element beschouwd om de bescherming van kinderen die communicatietechnologieën gebruiken, te verbeteren. Tot deze belanghebbenden rekent het voorstel ([3]) ook het bedrijfsleven, dat in het bijzonder via zelfregulering dient deel te nemen.

30. Als verantwoordelijke voor het verlenen van telecommunicatie- en inhoudsdiensten zou het bedrijfsleven op dit gebied enige invloed kunnen uitoefenen op het rapporteren, filteren en afschermen van verdacht of schadelijk geachte online-inhoud. De vraag in hoeverre het bedrijfsleven een dergelijke taak kan worden toevertrouwd, zou vanuit juridisch oogpunt niettemin tot discussie kunnen leiden.

31. De medewerking van het bedrijfsleven met oog op een betere bewustmaking van kinderen en andere betrokkenen zoals ouders en opvoeders, is uiteraard welkom. Het opzetten van alarmsystemen en moderatoren op websites die ongepaste inhoud uitsluiten, vormt een wezenlijk aspect van de verantwoordelijkheid van de aanbieders van inhoud.

32. Wat de aanbieders van *telecommunicatie*diensten betreft, is het toezicht op de telecommunicatie — gericht op de controle van hetzij door intellectuele-eigendomsrechten beschermde inhoud, hetzij andere illegale inhoud — echter een omstreden kwestie. Deze aangelegenheid werpt de vraag op of een commerciële instelling die een specifieke (telecommunicatie)dienst verleent, moet kunnen ingrijpen op een gebied waar deze in principe niet verwacht wordt in te grijpen, namelijk de controle op de inhoud van de telecommunicatie. De EDPS herinnert eraan dat een dergelijk toezicht principieel niet door dienstverleners wordt uitgeoefend, en zeker niet systematisch. Indien een dergelijk toezicht in specifieke omstandigheden noodzakelijk blijkt, zou dit in principe een taak zijn van de wetshandhavingautoriteiten.

33. In haar advies van 18 januari 2005 wijst de bij artikel 29 van Richtlijn 95/46/EG opgerichte Groep er in verband met deze kwestie ([4]) op dat internetaanbieders geen stelselmatige toezichts- of samenwerkingsverplichting krachtens artikel 15 van Richtlijn 2000/31/EG inzake elektronische handel kan worden opgelegd. (…) Zoals in artikel 8 van de richtlijn gegevensbescherming is bepaald, kunnen data inzake strafbare feiten, strafrechtelijke veroordelingen of veiligheidsmaatregelen alleen worden verwerkt onder de strikte voorwaarden die door lidstaten worden toegepast. 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 uitvoerig 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.

34. Op een gebied waar de vrijheid van meningsuiting, de toegang tot informatie, de privacy en andere grondrechten op het spel staan, werpt het optreden van particuliere actoren de vraag op of de gebruikte middelen wel proportioneel zijn. Het Europees Parlement heeft onlangs een resolutie aangenomen die de noodzaak van een de individuele grondrechten ([5]) eerbiedigende oplossing benadrukt. Volgens punt 23 van deze resolutie is „het internet een breed platform voor culturele expressie toegang tot kennis en democratische participatie in de Europese creativiteit, dat generaties samenbrengt in de informatiemaatschappij. Het Parlement roept de lidstaten en de Commissie op geen maatregelen te nemen die strijdig zijn met de burgerlijke vrijheden en de mensenrechten alsmede de beginselen van evenredigheid, doelmatigheid en ontradende werking, zoals onderbreking van de internettoegang".

([1]) Effectbeoordeling, punt 5.2.

([2]) In die zin zouden filters door de ouders moeten kunnen worden geïnitialiseerd en gedesactiveerd, zodat de volwassene volledige controle behoudt over het filteren.

([3]) Overweging 8 van de preambule; bijlage 1, punt 1.4; Samenvatting van de effectbeoordeling, punt 3.1.

([4]) Werkdocument van de Groep artikel 29 betreffende gegevensbeschermingsvraagstukken in verband met intellectuele-eigendomsrechten, WP 104.

([5]) Resolutie van het Europees Parlement van 10 april 2008 over de culturele industrieën in Europa (2007/2153(INI)), punt 23.

35. De EDPS is van mening dat een evenwicht moet worden gevonden tussen het legitieme doel illegale inhoud te bestrijden en het geschikte karakter van de gebruikte middelen. Hij herinnert eraan dat elke vorm van toezicht op telecommunicatienetwerken, wanneer dit in specifieke gevallen noodzakelijk is, de taak is van rechtshandhavingsautoriteiten.

IV. **CONCLUSIE**

36. De EDPS steunt het voorstel voor een meerjarenprogramma betreffende de bescherming van kinderen die het internet en andere communicatietechnologieën gebruiken. Hij is ingenomen met het feit dat het programma voornemens is de aandacht te richten op het ontwikkelen van nieuwe technologieën en op het vaststellen van concrete acties die de bescherming van kinderen in de onlineomgeving verbeteren.

37. De EDPS memoreert dat de bescherming van persoonsgegevens een wezenlijke voorwaarde voor de veiligheid van kinderen online is. Misbruik van persoonsgegevens van de kinderen dient te worden voorkomen door het aanwenden van de in het programma voorgelegde richtsnoeren, met name de volgende:

   — versterken van het bewustzijn van kinderen en andere belanghebbenden, zoals ouders en opvoeders;

   — bevorderen van beste praktijken in de industrie;

   — bevorderen van privacyeerbiedigende technologische instrumenten;

   — bevorderen van de uitwisseling van goede praktijken en praktische ervaring tussen de autoriteiten op het bewuste gebied, met inbegrip van de gegevensbeschermingsautoriteiten.

38. Deze acties moeten worden ontwikkeld zonder dat uit het oog wordt verloren dat de bescherming van kinderen plaatsvindt in een omgeving waar de rechten van anderen op spel kunnen staan. Elk initiatief dat het verzamelen, rapporteren of afschermen van informatie inhoudt, zou alleen dan moeten worden genomen indien het de grondrechten van alle betrokkenen eerbiedigt en in overeenstemming is met het wettelijke kader voor gegevensbescherming. Met name herinnert de EDPS eraan dat elke vorm van toezicht op telecommunicatienetwerken — wanneer in specifieke gevallen noodzakelijk —, de taak van rechtshandhavingsautoriteiten is.

39. De EDPS neemt er nota van dat dit programma een algemeen kader vormt voor verdere concrete acties. De EDPS is van mening dat sommige van de in dit advies gemaakte opmerkingen een eerste stap vormen, en dat zij op een praktische manier en in overeenstemming met de richtsnoeren van het programma verder kunnen worden uitgewerkt. Hij beveelt aan dat de gegevensbeschermingsautoriteiten te zijner tijd nauw betrokken worden bij de definitie van deze praktische projecten. Hij verwijst tevens naar de werkzaamheden van de Groep artikel 29, met name naar het huidige werk van de Groep betreffende sociale netwerken ([1]).

Gedaan te Brussel, 23 juni 2008.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming

([1]) Zie werkdocument 1/2008 van 18 februari 2008 betreffende de bescherming van persoonsgegevens van kinderen, WP 147, en voor een algemener inzicht het werkprogramma 2008-2009 van de Groep, met inbegrip van sociale netwerken, op: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm