I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese toezichthouder voor gegevensbescherming inzake het vergroten van het vertrouwen in de informatiemaatschappij door de bevordering van gegevensbescherming en privacy

(2010/C 280/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

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 7 en 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. Informatie- en communicatietechnologieën (ICT) bieden enorme mogelijkheden in vrijwel elk aspect van ons leven: werk, spel, sociale omgang en onderwijs. Ze zijn van essentieel belang voor de huidige informatie-economie en voor de samenleving in het algemeen.

2. De Europese Unie is een wereldmacht op het gebied van geavanceerde ICT en wil dat ook blijven. Om deze uitdaging aan te gaan zal de Europese Commissie naar verwachting weldra een nieuwe Europese digitale agenda vaststellen. Commissaris Kroes heeft bevestigd dat dit voor haar een prioriteit is ([4]).

3. De Europese Toezichthouder voor gegevensbescherming (EDPS) erkent de voordelen van ICT en is het ermee eens dat de EU haar uiterste best moet doen om de ontwikkeling en het wijdverspreid gebruik ervan te stimuleren. Hij staat ook volledig achter het standpunt van de commissarissen Kroes en Reding dat het individu centraal moet staan in deze nieuwe omgeving ([5]). Individuele burgers moeten erop kunnen vertrouwen dat ICT in staat zijn hun informatie veilig te houden en het gebruik ervan te controleren, en moeten er zeker van kunnen zijn dat hun recht op privacy en gegevensbescherming wordt geëerbiedigd in de digitale ruimte. De eerbiediging van dit recht is een essentiële voorwaarde om het vertrouwen van de consumenten te winnen. En dat vertrouwen is van cruciaal belang opdat de burgers nieuwe diensten aanvaarden ([6]).

([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.

([4]) Antwoorden op de vragenlijst van het Europees Parlement voor commissaris Neelie Kroes in de context van de EP-hoorzittingen die voorafgingen aan de benoeming van de commissaris.
([5]) Antwoorden op de vragenlijst van het Europees Parlement voor commissaris Neelie Kroes in de context van de EP-hoorzittingen die voorafgingen aan de benoeming van de commissaris; toespraak van commissaris Viviane Reding over „een Europese digitale agenda voor de nieuwe digitale consument", gehouden op het multistakeholderforum van het BEUC over de privacy van consumenten en onlinemarketing: „Market Trends and Policy Perspectives", Brussel, 12 november 2009.
([6]) Zie bijvoorbeeld „Trust in the Information Society", een verslag van de adviesraad RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society). Beschikbaar op http://www.think-trust.eu/general/news-events/riseptis-report.html Zie ook: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. De EU heeft een sterk rechtskader voor gegevensbescherming en privacy, waarvan de beginselen hun volledige relevantie behouden in het digitale tijdperk. Dat mag echter niet leiden tot zelfvoldaanheid. In veel gevallen doen ICT nieuwe vragen rijzen die buiten het bestaande kader vallen. Daarom moet actie worden ondernomen om ervoor te zorgen dat de in de EU-wetgeving vastgelegde individuele rechten doeltreffende bescherming blijven bieden in deze nieuwe omgeving.

5. In dit advies wordt besproken welke maatregelen de Europese Unie kan nemen of bevorderen om de persoonlijke levenssfeer en de bescherming van persoonsgegevens te waarborgen in een geglobaliseerde wereld die door technologie gestuurd zal blijven. Er worden zowel wetgevende als niet-wetgevende instrumenten besproken.

6. Het advies geeft eerst een overzicht van ICT als een nieuwe ontwikkeling die mogelijkheden maar ook risico's schept, en bespreekt dan de noodzaak om gegevensbescherming en privacy vanaf het eerste begin op een praktisch niveau te integreren in nieuwe informatie- en communicatietechnologieën (het zgn. beginsel van ingebouwde privacy of „privacy by design"). Om de naleving van dit beginsel af te dwingen moet volgens het advies het beginsel van ingebouwde privacy op minstens twee verschillende manieren worden voorzien in het rechtskader voor gegevensbescherming. Ten eerste door het erin op te nemen als een bindend algemeen beginsel en ten tweede door het erin op te nemen voor bepaalde ICT-gebieden met specifieke risico's inzake gegevensbescherming en privacy die kunnen worden voorkomen door een aangepaste technische architectuur en een aangepast ontwerp. Deze gebieden zijn radiofrequentie-identificatie (RFID), applicaties voor sociale netwerken en browserapplicaties. Tot slot bevat het advies voorstellen betreffende andere hulpmiddelen en beginselen ter bescherming van de persoonlijke levenssfeer en de persoonsgegevens in de ICT-sector.

7. Met het oog op het bovenstaande gaat het advies nader in op de opmerkingen die de Werkgroep artikel 29 formuleert in zijn bijdrage aan de openbare raadpleging over de toekomst van privacy ([1]). Daarnaast wordt voortgebouwd op eerdere adviezen van de EDPS, zoals het advies van 25 juli 2007 over de toepassing van de gegevensbeschermingsrichtlijn, het advies van 20 december 2007 over RFID en twee adviezen over de e-privacyrichtlijn ([2]).

II. ICT BIEDEN NIEUWE MOGELIJKHEDEN MAAR HOUDEN OOK NIEUWE RISICO'S IN

8. ICT zijn al vergeleken met andere belangrijke uitvindingen uit het verleden, zoals elektriciteit. Hoewel het wellicht nog te vroeg is om hun werkelijke historische impact te beoordelen, bestaat er een duidelijk verband tussen ICT en economische groei in de ontwikkelde landen. ICT hebben werkgelegenheid geschapen, economische voordelen voortgebracht en bijgedragen aan de algemene welvaart. De impact van ICT gaat verder dan het louter economische, aangezien ze ook een belangrijke rol hebben gespeeld in het stimuleren van innovatie en creativiteit.

9. Bovendien hebben ICT de manier waarop mensen werken en met elkaar omgaan veranderd. Ze zijn bijvoorbeeld steeds meer afhankelijk van ICT voor hun sociale en economische interacties. Burgers kunnen gebruik maken van een brede waaier van nieuwe ICT-toepassingen zoals e-gezondheid, e-transport en e-overheid, en van innovatieve interactieve systemen voor amusement en onderwijs.

10. In het licht van deze voordelen hebben alle Europese instellingen toegezegd om ICT te ondersteunen als een noodzakelijk hulpmiddel om het concurrentievermogen van de Europese industrie te verbeteren en het economische herstel van Europa te bespoedigen. In augustus 2009 keurde de Commissie het verslag over het digitale concurrentievermogen van Europa ([3]) goed en startte ze een openbare raadpleging over geschikte toekomststrategieën om het gebruik van ICT te stimuleren. Op 7 december 2009 presenteerde de Raad een bijdrage aan deze raadpleging onder de titel „Post-i2010-strategie — Naar een open, groene en concurrerende kennismaatschappij" ([4]). Het Europees Parlement heeft onlangs een verslag

([1]) Advies 168 van de Werkgroep artikel 29 over de toekomst van privacy, gezamenlijke bijdrage aan de raadpleging van de Europese Commissie inzake het rechtskader voor het grondrecht op de bescherming van persoonsgegevens, goedgekeurd op 1 december 2009.

([2]) Advies van 25 juli 2007 inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming, PB C 255, 27.10.2007, blz. 1; advies van 20 december 2007 inzake de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over radiofrequentie-identificatie (RFID) in Europa: maatregelen met het oog op een beleidskader (COM(2007) 96), PB C 101, 23.4.2008, blz. 1; advies van 10 april 2008 inzake het voorstel voor een richtlijn tot wijziging van, onder andere, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PB C 181, 18.7.2008, blz. 1; tweede advies van 9 januari 2009 over de herziening van Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

([3]) Verslag over het digitale concurrentievermogen van Europa — Voornaamste successen van de i2010-strategie 2005-2009 (SEC (2009) 1060).

([4]) Conclusies van de Raad „Post-i2010-strategie — Naar een open, groene en concurrerende kennismaatschappij" (17107/09), goedgekeurd op 18.12.2009.

goedgekeurd dat bedoeld is om de Commissie te helpen bij het vaststellen van een digitale agenda [1].

11. De mogelijkheden en voordelen die de ontwikkeling van ICT biedt, gaan gepaard met nieuwe risico's, inzonderheid voor de persoonlijke levenssfeer en de bescherming van persoonsgegevens. ICT leiden vaak tot een toename (vaak zonder dat de gebruikers precies weten hoe) van de hoeveelheid informatie die wordt verzameld, gesorteerd, gefilterd, overgedragen of bewaard, waardoor deze gegevens blootstaan aan meer risico's.

12. Zo is er het voorbeeld van de RFID-chips, die de streepjescodes op (sommige) verbruiksartikelen vervangen. Doordat het nieuwe systeem de informatiestroom in de toeleveringsketen verbetert (en aldus de behoefte aan „veiligheidsvoorraden" vermindert, juistere prognoses mogelijk maakt, enz.), zou het zowel bedrijven als consumenten ten goede moeten komen. Maar tegelijk ontstaat de verontrustende mogelijkheid dat mensen worden gevolgd, voor andere doeleinden en door andere entiteiten, via hun van een tag voorziene persoonlijke bezittingen.

13. Een ander voorbeeld is „cloud computing", waarbij gehoste applicatiediensten voor consumenten en niet-consumenten worden aangeboden via het internet. Het betreft hier fotobibliotheken, kalenders, webmail en klantendatabanken, maar ook meer complexe bedrijfsgerelateerde diensten. De voordelen voor zowel bedrijven als particulieren zijn duidelijk: het systeem is goedkoper (de kosten zijn marginaal), niet locatiegebonden (gemakkelijke toegang tot informatie overal in de wereld), geautomatiseerd (geen specifieke IT-bronnen en geen softwareupdates nodig), enz. Daartegenover staan de zeer reële risico's van veiligheidsstoringen en hacking. Verder bestaat het gevaar dat gebruikers de toegang tot en de controle over hun eigen gegevens verliezen.

14. Ook op andere gebieden waarbij gebruik wordt gemaakt van ICT-toepassingen is gebleken dat voordelen en risico's samengaan. E-gezondheid, bijvoorbeeld, kan de doeltreffendheid bevorderen, de kosten verminderen, de toegankelijkheid vergroten en in het algemeen de kwaliteit van gezondheidszorgdiensten verbeteren. Maar e-gezondheid doet ook vaak vragen rijzen over de wettigheid van het secundaire gebruik van e-gezondheidsinformatie, zodat een grondige analyse van de doeleinden van elk potentieel secundair gebruik vereist is [2]. Doordat bovendien steeds meer gebruik wordt gemaakt van elektronische gezondheidsdossiers, worden de systemen zelf geplaagd door schandalen waarbij veel gevallen van gekraakte elektronische gezondheidsdossiers aan het licht zijn gekomen.

15. Samengevat kan worden gesteld dat er wellicht altijd een zeker risico zal blijven bestaan, ook nadat de juiste beoordelingen zijn gemaakt en de nodige maatregelen zijn toegepast. Nulrisico bestaat niet. Toch kunnen en moeten, zoals hieronder verder wordt besproken, maatregelen ten uitvoer worden gelegd om het risico zoveel mogelijk te beperken.

III. INGEBOUWDE PRIVACY ALS ESSENTIEEL HULPMIDDEL OM VERTROUWEN IN ICT TE WEKKEN BIJ DE GEBRUIKERS

16. De potentiële voordelen van ICT zullen alleen in de praktijk kunnen worden genoten als zij erin slagen vertrouwen te wekken, m.a.w. als de gebruikers bereid worden gevonden zich op ICT te verlaten wegens de kenmerken en voordelen die ze hebben. Dat vertrouwen kan alleen worden gewekt als de gebruikers ICT zien als betrouwbaar, veilig en onder hun controle, en als de bescherming van hun persoonsgegevens en privacy gewaarborgd is.

17. Er is gerede kans dat algemeen voorkomende risico's en gebreken zoals hierboven beschreven het vertrouwen van de gebruikers in de informatiemaatschappij aantasten, inzonderheid wanneer hun privacy wordt blootgelegd door misbruik of schending van persoonsgegevens. Dat kan de ontwikkeling en de mogelijke voordelen van ICT ernstig in gevaar brengen.

18. Deze risico's voor de privacy en gegevensbescherming kunnen echter niet worden opgelost door het gebruik of de bevordering van ICT uit te sluiten of af te wijzen. Dat zou niet doenbaar en niet realistisch zijn; het zou verhinderen dat mensen voordeel halen van ICT en het zou de mogelijke algemene voordelen ernstig beperken.

19. De EDPS meent dat een positievere oplossing zou zijn dat ICT zo worden ontworpen en ontwikkeld, dat de privacy en gegevensbescherming worden geëerbiedigd. Het is daarom van essentieel belang dat privacy en gegevensbescherming worden geïntegreerd in de gehele levenscyclus van deze technologieën, van het vroegste ontwerpstadium tot de toepassing, het gebruik en de afdanking. Dat wordt gewoonlijk ingebouwde privacy („privacy by design") genoemd en hieronder nader besproken.

20. Ingebouwde privacy kan verschillende maatregelen met zich meebrengen naargelang het specifieke geval of de specifieke toepassing. Zo kan het in sommige gevallen nodig zijn om persoonsgegevens te verwijderen/beperken of een onnodige en/of ongewenste verwerking ervan te voorkomen. In andere gevallen kunnen hulpmiddelen worden aangereikt om de gebruikers meer controle over hun persoonsgegevens te bieden. Zulke maatregelen dienen te worden overwogen wanneer normen en/of beste praktijken worden vastgesteld. Ze kunnen ook worden

[1] Verslag over de vaststelling van een nieuwe digitale agenda voor Europa: van i2010 naar digital.eu (2009/2225 (INI)), goedgekeurd op 18.3.2010.

[2] Er zou bijvoorbeeld zorgvuldig moeten worden onderzocht of gezondheidsinformatie die is verzameld met het oog op het verstrekken van een behandeling mag worden verkocht of gebruikt om vestigingsplaatsen voor satellietziekenhuizen te kiezen, ambulante operatiecentra op te richten of andere toekomstige activiteiten met financiële implicaties te plannen.

opgenomen in de architectuur van informatie- en communicatiesystemen of in de structurele organisatie van de entiteiten die persoonsgegevens verwerken.

III.1. **Beginsel van ingebouwde privacy toepasbaar op verschillende ICT-omgevingen en -effecten**

21. De behoefte aan ingebouwde privacy bestaat in veel verschillende ICT-omgevingen. De sector van de gezondheidszorg, bijvoorbeeld, steunt steeds meer op ICT-infrastructuren waarbij gezondheidsinformatie over patiënten vaak centraal wordt opgeslagen. Om het beginsel van ingebouwde privacy in de gezondheidssector toe te passen, zou de geschiktheid van verschillende maatregelen moeten worden beoordeeld: het aantal centraal opgeslagen gegevens tot een minimum herleiden of beperken tot een index, gebruik maken van versleutelingsmethoden, toegangsrechten uitsluitend toekennen op basis van het beginsel van kennisnemingsbehoefte, gegevens anoniem maken zodra ze niet meer nodig zijn, enz.

22. Ook vervoerssystemen worden in toenemende mate standaard geleverd met geavanceerde ICT-toepassingen die met het voertuig en zijn omgeving in wisselwerking staan voor verschillende doeleinden en functies. Zo zijn auto's steeds vaker uitgerust met nieuwe ICT-functies (gps, gsm, sensornetwerk, enz.) die niet alleen hun positie direct weergeven, maar ook hun technische toestand. Deze informatie zou bijvoorbeeld kunnen worden gebruikt om het bestaande wegenbelastingssysteem te vervangen door een gebruiksafhankelijke tolheffing. De toepassing van ingebouwde privacy op het architectuurontwerp van zulke systemen zou ertoe moeten leiden dat zo weinig mogelijk persoonsgegevens worden verwerkt of verder worden overgedragen ([1]). In overeenstemming met dit beginsel zouden gedecentraliseerde of semi-gedecentraliseerde architecturen die de bekendmaking van positiegegevens aan een centraal punt beperken te verkiezen zijn boven gecentraliseerde architecturen.

23. Uit de bovenstaande voorbeelden blijkt dat, wanneer informatie- en communicatietechnologieën worden gemaakt volgens het beginsel van ingebouwde privacy, de risico's voor de privacy en gegevensbescherming aanzienlijk kunnen worden beperkt.

III.2. **Onvoldoende toepassing van ingebouwde privacy in ICT**

24. Een belangrijke vraag is of de economische deelnemers, de ICT-fabrikanten en -aanbieders en de voor de verwerking verantwoordelijken geïnteresseerd zijn in het in de handel brengen en toepassen van ingebouwde privacy in ICT. In deze context is het ook belangrijk om te beoordelen hoe groot de vraag naar ingebouwde privacy is bij de gebruikers.

25. In 2007 publiceerde de Commissie een mededeling waarin bedrijven werden verzocht hun innovatievermogen te gebruiken om technologieën ter bevordering van de persoonlijke levenssfeer te ontwerpen en toe te passen teneinde de bescherming van de privacy en persoonsgegevens te verbeteren vanaf het eerste begin van de ontwikkelingscyclus ([2]).

26. Uit het thans beschikbare bewijsmateriaal blijkt evenwel dat de ICT-fabrikanten noch de voor de verwerking verantwoordelijken (in de particuliere en de openbare sector) erin zijn geslaagd om ingebouwde privacy op consistente wijze toe te passen of in de handel te brengen. Hiervoor worden verschillende redenen aangevoerd, zoals een gebrek aan economische stimulansen of institutionele steun, onvoldoende vraag, enz. ([3])

27. Tegelijkertijd is er bij de gebruikers vrij weinig vraag naar ingebouwde privacy. De gebruikers van ICT-producten en -diensten gaan er terecht van uit dat hun privacy en persoonsgegevens *de facto* beschermd zijn, in veel gevallen zijn ze dat echter niet. In sommige gevallen zijn de gebruikers gewoon niet bij machte de nodige veiligheidsmaatregelen te nemen om hun eigen persoonsgegevens of die van anderen te beschermen. Vaak komt dit doordat ze de risico's niet of slechts gedeeltelijk kennen. Jongeren, bijvoorbeeld, slaan in het algemeen geen acht op de privacyrisico's die het plaatsen van persoonlijke informatie op sociale netwerken met zich meebrengt en hebben dikwijls geen aandacht voor privacyinstellingen. Andere gebruikers zijn zich wel bewust van de risico's, maar beschikken niet over de nodige technische deskundigheid om technologieën toe te passen die, bijvoorbeeld, hun internetverbinding beveiligen of om hun browserinstellingen zo aan te passen dat de profilering op basis van hun surfactiviteiten tot een minimum wordt beperkt.

28. Toch zijn de risico's voor de privacy en gegevensbescherming heel reëel. Als niet vanaf het begin rekening wordt gehouden met de privacy en gegevensbescherming, is het daarna vaak te laat en economisch te lastig om de systemen bij te stellen en te laat om de reeds aangerichte schade te herstellen. Het toenemende aantal inbreuken in verband met persoonsgegevens van de voorbije jaren

([1]) Zie het advies van de Europese Toezichthouder voor gegevensbescherming van 22 juli 2009 betreffende de mededeling van de Commissie over een actieplan voor de invoering van intelligente vervoerssystemen in Europa en het bijbehorende voorstel voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van het kader voor het toepassen van intelligente vervoerssystemen op het gebied van wegvervoer en voor raakvlakken met andere vervoerswijzen, beschikbaar op: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_NL.pdf

([2]) Mededeling COM(2007) 228 definitief van de Commissie aan het Europees Parlement van 2 mei 2007 inzake de verbetering van de gegevensbescherming door technologieën ter bevordering van de persoonlijke levenssfeer.

([3]) Studie over de economische voordelen van technologieën ter bevordering van de persoonlijke levenssfeer, JLS/2008/D4/036.

toont duidelijk aan dat er wel degelijk een probleem is en dat ingebouwde privacy een dringende noodzaak is.

29. Het bovenstaande impliceert dat de fabrikanten en aanbieders van ICT die ontworpen zijn om persoonsgegevens te verwerken, de verantwoordelijkheid hebben, samen met de voor de verwerking verantwoordelijken, om deze technologieën te ontwerpen met ingebouwde waarborgen voor de privacy en gegevensbescherming. In veel gevallen zou dit betekenen dat de standaardinstellingen maximale privacy bieden („privacy by default").

30. Tegen deze achtergrond moeten we onderzoeken welke stappen de beleidsmakers moeten ondernemen om ingebouwde privacy bij de ontwikkeling van ICT te bevorderen. Een eerste vraag hierbij is of het bestaande rechtskader voor gegevensbescherming toereikende bepalingen bevat om het beginsel van ingebouwde privacy te laten toepassen door de voor de verwerking verantwoordelijken en de fabrikanten en ontwikkelaars. Een tweede vraag is wat er in de context van de Europese digitale agenda moet worden gedaan opdat de consumenten vertrouwen krijgen in de ICT-sector.

IV. INTEGRATIE VAN HET BEGINSEL VAN INGEBOUWDE PRIVACY IN HET EU-RECHT EN -BELEID

IV.1. Het huidige rechtskader voor gegevensbescherming en privacy

31. De EU heeft een stevig kader voor gegevensbescherming en privacy neergelegd in Richtlijn 95/46/EG ([1]), Richtlijn 2002/58/EG ([2]) en de jurisprudentie van het Europees Hof voor de Rechten van de Mens ([3]) en het Hof van Justitie.

32. De gegevensbeschermingsrichtlijn is van toepassing op „elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens" (verzamelen, bewaren, verstrekken, enz.). Hij legt de naleving van bepaalde beginselen en verplichtingen op aan hen die persoonsgegevens verwerken („voor de verwerking verantwoordelijken"). Hij voorziet in individuele rechten, zoals het recht van toegang tot persoonlijke informatie. De e-privacyrichtlijn handelt uitdrukkelijk over de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie. ([4]).

33. De huidige gegevensbeschermingsrichtlijn schrijft ingebouwde privacy niet uitdrukkelijk voor. Wel bevat hij bepalingen die onrechtstreeks, in verschillende situaties, de toepassing van het beginsel van ingebouwde privacy kunnen eisen. Met name artikel 17 bepaalt dat de voor de verwerking verantwoordelijken passende technische en organisatorische maatregelen ten uitvoer dienen te leggen om persoonsgegevens te beveiligen tegen onwettige verwerking ([5]). Ingebouwde privacy wordt bijgevolg op heel algemene wijze behandeld. Bovendien hebben de bepalingen van de richtlijn vooral betrekking op de voor de verwerking verantwoordelijken en op hun verwerking van persoonsgegevens. Ze schrijven niet uitdrukkelijk voor dat de informatie- en communicatietechnologieën moeten voldoen aan de voorschriften inzake privacy en gegevensbescherming; hiervoor zouden ze ook betrekking moeten hebben op de ICT-ontwerpers en -fabrikanten en op de werkzaamheden in het stadium van de normalisatie.

34. De e-privacyrichtlijn is explicieter. Artikel 14.3 bepaalt het volgende: „Zo nodig kunnen maatregelen worden goedgekeurd om ervoor te zorgen dat de eindapparatuur gebouwd is op een wijze die verenigbaar is met het recht van gebruikers om het gebruik van hun persoonsgegevens te beschermen en te controleren, in overeenstemming met Richtlijn 1995/5/EG en met Beschikking 87/95/EEG van de Raad van 22 december 1986 betreffende de normalisatie op het gebied van de informatietechnologieën en de telecommunicatie." Deze bepaling is evenwel nog nooit toegepast ([6]).

35. Hoewel de bovengenoemde bepalingen van de twee richtlijnen nuttig zijn voor het bevorderen van ingebouwde privacy, zijn zij in de praktijk ontoereikend gebleken om ervoor te zorgen dat privacy wordt ingebouwd in ICT.

36. Als gevolg van deze situatie schrijft de wet niet voldoende nauwkeurig voor dat ICT moeten worden ontworpen in overeenstemming met het beginsel van ingebouwde privacy. Ook beschikken de gegevensbeschermingsinstanties over onvoldoende bevoegdheden om ervoor te zorgen dat privacy wordt ingebouwd. Dat leidt tot ondoeltreffendheid. De gegevensbeschermingsinstanties kunnen bijvoorbeeld straffen opleggen indien niet wordt ingegaan op toegangsverzoeken van gebruikers en zij hebben de bevoegdheid om de toepassing van bepaalde maatregelen ter

([1]) Richtlijn 95/46/EG van het Europees Parlement en de Raad (hierna: gegevensbeschermingsrichtlijn).

([2]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad (hierna: e-privacyrichtlijn).

([3]) Door uitlegging van de belangrijkste elementen en voorwaarden van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), ondertekend in Rome op 4 november 1950.

([4]) Het Verdrag van Lissabon heeft deze bescherming versterkt door de eerbiediging van het privéleven en de bescherming van persoonsgegevens te erkennen als afzonderlijke grondrechten in artikel 7 en 8 van het EU-handvest van de grondrechten. Het EU-handvest van de grondrechten werd bindend toen het Verdrag van Lissabon in werking trad.

([5]) Artikel 17 luidt als volgt: „De Lid-Staten bepalen dat de voor de verwerking verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer dient te leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.". Overweging 46 vult dit aan: „Overwegende dat de bescherming van de rechten en vrijheden van de betrokkenen in verband met de verwerking van persoonsgegevens zowel bij het ontwerpen als bij de uitvoering van de verwerking passende technische maatregelen vergt, in het bijzonder om de veiligheid te waarborgen en zodoende elke ongeoorloofde verwerking te verhinderen."

([6]) De Commissie heeft haar voornemen bekendgemaakt om Richtlijn 1999/5/EG bij te werken tegen het einde van 2010.

voorkoming van onwettige gegevensverwerking te eisen. Het is echter niet altijd voldoende duidelijk of ze ook de bevoegdheid hebben om voor te schrijven dat een systeem zo ontworpen wordt, dat het de rechten inzake de bescherming van persoonsgegevens faciliteert [1]. Het is bijvoorbeeld onduidelijk of, op basis van de bestaande wettelijke bepalingen, kan worden geëist dat de architectuur van een informatiesysteem zo ontworpen wordt, dat bedrijven gemakkelijker kunnen reageren op toegangsverzoeken van gebruikers, zodat deze verzoeken automatisch en sneller kunnen worden afgehandeld. Bovendien kunnen latere pogingen om de technologie te wijzigen nadat ze is ontwikkeld of ingevoerd, resulteren in een lappendeken van halve oplossingen die ook nog duur zijn.

37. Naar de mening van de EDPS, die wordt gedeeld door de Werkgroep artikel 29 [2], laat het huidige rechtskader ruimte voor een meer expliciete bevestiging van het beginsel van ingebouwde privacy.

IV.2. **Integratie van ingebouwde privacy op verschillende niveaus**

38. In het licht van het bovenstaande raadt de EDPS de Commissie aan vier actielijnen te volgen:

a) voorstellen om een algemene bepaling over ingebouwde privacy op te nemen in het rechtskader voor gegevensbescherming;

b) deze algemene bepaling uitwerken in specifieke bepalingen wanneer specifieke rechtsinstrumenten in verschillende sectoren worden voorgesteld. Deze specifieke bepalingen zouden nu al kunnen worden opgenomen in rechtsinstrumenten op basis van artikel 17 van de gegevensbeschermingsrichtlijn (en andere bestaande wetgeving);

c) ingebouwde privacy als leidend beginsel opnemen in de Europese digitale agenda;

d) ingebouwde privacy als beginsel invoeren in andere EU-initiatieven (vooral niet-wetgevende).

Een algemene bepaling over ingebouwde privacy

39. De EDPS stelt voor om het beginsel van ingebouwde privacy ondubbelzinnig en uitdrukkelijk op te nemen in het bestaande regelgevende kader voor gegevensbescherming. Dat zou het beginsel van ingebouwde privacy sterker en explicieter maken en de effectieve toepassing ervan afdwingen. Het zou de handhavingsinstanties ook meer legitimiteit geven om de feitelijke toepassing ervan in de praktijk te eisen. In het licht van de hierboven beschreven feiten is dit des te noodzakelijker, gezien het belang van het beginsel zelf als middel om vertrouwen te wekken, maar ook als stimulans voor de belanghebbenden om ingebouwde privacy in te voeren en de door het bestaande rechtskader geboden waarborgen te versterken.

40. Dit voorstel steunt op de aanbeveling van de Werkgroep artikel 29 om het beginsel van ingebouwde privacy als een algemeen beginsel op te nemen in het rechtskader voor gegevensbescherming en inzonderheid in de gegevensbeschermingsrichtlijn. De Werkgroep artikel 29 stelt het als volgt: „Dit beginsel zou bindend moeten zijn voor de technologieontwerpers en -producenten en de voor de verwerking verantwoordelijken die moeten beslissen over de aankoop en het gebruik van ICT. Zij zouden moeten worden verplicht om reeds in het planningsstadium van informatietechnologieprocedures en -systemen rekening te houden met de technologische gegevensbescherming. De aanbieders van deze systemen of diensten en de voor de verwerking verantwoordelijken zouden moeten aantonen dat ze alle nodige maatregelen hebben genomen om te voldoen aan deze eisen.”.

41. De EDPS neemt ook met instemming kennis van de bevestiging van het beginsel van ingebouwde privacy door commissaris Viviane Reding bij haar aankondiging van de herbeoordeling van de gegevensbeschermingsrichtlijn [3].

42. Dit brengt ons tot de inhoud van een dergelijke regelgeving. In de eerste plaats moet een algemeen beginsel van ingebouwde privacy technologisch neutraal zijn. Het beginsel mag niet proberen de technologie te reguleren, d.w.z. het mag geen specifieke technische oplossingen voorschrijven. Wel moet het verplicht stellen dat de bestaande beginsels van privacy en gegevensbescherming worden geïntegreerd in ICT-systemen en -oplossingen. Hierdoor kunnen de belanghebbenden — fabrikanten, voor de verwerking verantwoordelijken en gegevensbeschermingsinstanties — de betekenis van het beginsel

[1] Zie het verslag van het Britse Information Commissioner's Office: „Privacy by Design”, gepubliceerd in november 2008.

[2] Zie advies 168 van de Werkgroep artikel 29 over de toekomst van privacy, een gezamenlijke bijdrage aan de raadpleging van de Europese Commissie inzake het rechtskader voor het grondrecht op de bescherming van persoonsgegevens, goedgekeurd op 1 december 2009.

[3] „Ingebouwde privacy is een beginsel waar zowel particulieren als bedrijven belang bij hebben. Ingebouwde privacy zal leiden tot een betere bescherming van de burgers en ook tot vertrouwen in nieuwe diensten en producten, wat op zijn beurt een positief effect op de economie zal hebben. Er bestaan al bemoedigende voorbeelden, maar er moet nog veel meer worden gedaan.” Thematoespraak op de Dag van de gegevensbescherming, 28 januari 2010, Europees Parlement, Brussel.

interpreteren naargelang van elk individueel geval. In de tweede plaats moet de naleving van het beginsel verplicht zijn in verschillende stadia, van de vaststelling van de normen en het ontwerp van de architectuur tot de toepassing ervan door de voor de verwerking verantwoordelijke.

Bepalingen in specifieke rechtsinstrumenten

43. Het beginsel van ingebouwde privacy moet in de huidige en toekomstige wetgevende instrumenten worden geïntegreerd op basis van het bestaande rechtskader en, na aanneming van de hierboven voorgestelde algemene bepaling, op basis van deze bepaling. Volgens de huidige initiatieven in verband met intelligente vervoerssystemen, bijvoorbeeld, zal de Commissie een specifieke eerste verantwoordelijkheid dragen bij de vaststelling van maatregelen, normalisatie-initiatieven, procedures en beste praktijken. Bij de uitvoering van deze taken zou ingebouwde privacy een leidend beginsel moeten zijn.

44. De EDPS merkt verder op dat het beginsel van ingebouwde privacy ook van specifiek belang is op het gebied van vrijheid, veiligheid en recht, inzonderheid met betrekking tot de in het programma van Stockholm vervatte doelstellingen van de informatiebeheersstrategie ([1]). In zijn advies over het programma van Stockholm benadrukte de EDPS dat de architectuur voor informatie-uitwisseling gebaseerd moet zijn op „ingebouwde privacy" ([2]): „Dat houdt meer concreet in dat informatiesystemen die ten behoeve van de openbare veiligheid worden ontworpen, steevast volgens het beginsel van „privacy by design" moeten worden aangelegd."

45. Het advies van de Werkgroep artikel 29 over de toekomst van privacy ([3]) stelt nog duidelijker dat de eisen betreffende ingebouwde privacy dwingend moeten worden gemaakt op het gebied van vrijheid, veiligheid en recht, waar de overheidsinstanties de belangrijkste actoren zijn en waar maatregelen ter verbetering van het toezicht een rechtstreeks effect op de grondrechten inzake privacy en gegevensbescherming hebben. Door hun informatiesystemen te laten voldoen aan deze eisen zouden de overheden de toepassing van ingebouwde privacy ook stimuleren als eerste gebruikers.

Ingebouwde privacy als leidend beginsel in de Europese digitale agenda

46. Informatie- en communicatietechnologieën worden steeds complexer en brengen grotere privacy- en gegevensbeschermingsrisico's met zich mee. In het algemeen staat gedigitaliseerde informatie, die toegankelijker is en gemakkelijker kan worden gekopieerd en doorgegeven, bloot aan veel hogere risico's dan informatie op papier. Naarmate we meer evolueren naar netwerken van onderling gekoppelde objecten, zullen de risico's nog toenemen. Hoe groter de privacy- en gegevensbeschermingsrisico's zijn, hoe groter de vraag wordt naar betere waarborgen inzake gegevensbescherming en privacy. Daarom zijn de motiveringen voor de noodzaak om ingebouwde privacy toe te passen dwingender in de ICT-sector. Bovendien zullen, zoals hierboven gezegd, de burgers deze nieuwe diensten maar aanvaarden als ze vertrouwen hebben in ICT, en privacy en gegevensbescherming zijn essentiële elementen van dit vertrouwen.

47. Het bovenstaande onderstreept dat een strategie voor de ontwikkeling van ICT moet inhouden dat deze technologieën worden ontworpen met een inherent element van privacy en gegevensbescherming, d.w.z. rekening houdend met het beginsel van ingebouwde privacy.

48. Daarom zou de Europese digitale agenda het beginsel van ingebouwde privacy expliciet moeten bevestigen als noodzakelijk element om bij de burgers vertrouwen in ICT en onlinediensten te wekken. Hij zou dienen te erkennen dat privacy en vertrouwen hand in hand gaan, en dat ingebouwde privacy een leidend beginsel hoort te zijn bij de ontwikkeling van een betrouwbare ICT-sector.

Ingebouwde privacy als beginsel in andere EU-initiatieven

49. Ingebouwde privacy zou voor de Commissie een leidend beginsel moeten zijn bij de tenuitvoerlegging van beleidsmaatregelen, activiteiten en initiatieven in specifieke ICT-sectoren zoals e-gezondheid, e-aanbesteding, e-sociale zekerheid, e-leren, enz. Veel van deze initiatieven zullen actiepunten zijn in de Europese digitale agenda.

50. Dat betekent, bijvoorbeeld, dat initiatieven om overheidsapplicaties efficiënter en moderner te maken zodat de burgers kunnen interageren met overheidsdiensten, zouden moeten inhouden dat deze applicaties dienen te worden ontworpen en gebruikt in overeenstemming met het beginsel van ingebouwde privacy. Hetzelfde geldt voor beleidsmaatregelen en activiteiten van de Commissie die gericht zijn op een sneller internet, digitale inhoud of een algemene bevordering van vaste en draadloze communicatie en datatransmissie.

([1]) Het programma van Stockholm — Een open en veilig Europa ten dienste en ter bescherming van de burger, goedgekeurd door de Europese Raad in december 2009.

([2]) Advies van 10 juli 2009 over de mededeling van de Commissie aan het Europees Parlement en de Raad betreffende een ruimte van vrijheid, veiligheid en recht ten dienste van de burger, PB C 276, van 17.11.2009, blz. 8, punt 60.

([3]) Advies 168 van de Werkgroep artikel 29 over de toekomst van privacy, gezamenlijke bijdrage aan de raadpleging van de Europese Commissie inzake het rechtskader voor het grondrecht op de bescherming van persoonsgegevens, goedgekeurd op 1 december 2009.

51. Het bovenstaande heeft ook betrekking op die gebieden waar de Commissie verantwoordelijk is voor grootschalige IT-systemen als SIS en VIS, en op die gevallen waar de verantwoordelijkheid van de Commissie beperkt blijft tot de ontwikkeling en het onderhoud van de gemeenschappelijke infrastructuur van een systeem als het Europees Strafregisterinformatiesysteem (ECRIS).

52. Hoe het beginsel van ingebouwde privacy precies wordt ontwikkeld, hangt af van elke specifieke sector en situatie. Wanneer bijvoorbeeld initiatieven van de Commissie vergezeld gaan van wetgevende voorstellen betreffende een bepaalde ICT-sector, dient in veel gevallen uitdrukkelijk te worden gesteld dat het begrip ingebouwde privacy moet worden toegepast op het ontwerp van de specifieke ICT-toepassing of het specifieke ICT-systeem. Als actieplannen worden opgesteld voor een specifiek gebied zouden zij er systematisch voor moeten zorgen dat het rechtskader wordt toegepast en meer specifiek moeten garanderen dat de relevante ICT-technologie wordt ontwikkeld met ingebouwde privacy in gedachten.

53. Wat onderzoek betreft, zouden het zevende kaderprogramma en de volgende kaderprogramma's moeten worden gebruikt als een hulpmiddel om projecten te ondersteunen die gericht zijn op de analyse van normen, ICT-technologieën en ICT-architecturen waarin beter rekening wordt gehouden met de privacy en inzonderheid met het beginsel van ingebouwde privacy. Daarnaast zou ingebouwde privacy ook als een noodzakelijk element moeten worden beschouwd voor ruimere ICT-projecten die gericht zijn op de verwerking van persoonsgegevens.

Bijzondere aandachtsgebieden

54. In sommige gevallen kan het, wegens de bijzondere risico's voor de persoonlijke levenssfeer en de bescherming van persoonsgegevens of wegens andere factoren (weerstand van bedrijven om producten met ingebouwde privacy te verstrekken, vraag van de consumenten, enz.), nodig zijn om, al dan niet in wetgevende instrumenten, explicietere en specifiekere maatregelen betreffende ingebouwde privacy vast te stellen, die moeten werden geïntegreerd in bepaalde ICT-producten of -technologieën.

55. De EDPS heeft verschillende gebieden vastgesteld (RFID, sociale netwerken en browserapplicaties) die volgens hem in dit stadium door de Commissie zorgvuldig moeten worden bestudeerd en in aanmerking komen voor de hierboven aanbevolen praktijkgerichtere benadering. Deze drie gebieden worden hieronder nader besproken.

V. **RADIOFREQUENTIE-IDENTIFICATIE (RFID)**

56. RFID-tags kunnen worden ingebouwd in voorwerpen, dieren en mensen. Ze kunnen worden gebruikt om persoonsgegevens zoals medische dossiers te verzamelen en op te slaan, om de bewegingen van personen te volgen of om een profiel van hun gedrag op te stellen voor verschillende doeleinden. Dat kan gebeuren zonder medeweten van de betrokkene ([1]).

57. Doeltreffende waarborgen betreffende gegevensbescherming, privacy en alle hiermee verbonden morele dimensies zijn van cruciaal belang om het vertrouwen van het publiek in RFID en een toekomstig internet der dingen te winnen. Alleen dan kan de technologie haar talrijke economische en maatschappelijke baten opleveren.

V.1. **Hiaten van het toepasselijke rechtskader voor gegevensbescherming**

58. De gegevensbeschermingsrichtlijn en de e-privacyrichtlijn zijn van toepassing op het verzamelen van gegevens door middel van RFID-toepassingen ([2]). Ze schrijven onder andere voor dat moet worden voorzien in passende privacywaarborgen bij het gebruik van RFID-toepassingen ([3]).

59. Dit rechtskader biedt evenwel geen oplossing voor alle problemen inzake gegevensbescherming en privacy die deze technologie met zich meebrengt. Dat komt doordat

([1]) RFID staat voor radiofrequentie-identificatie. De belangrijkste onderdelen van de RFID-technologie of -infrastructuur zijn een tag (d.i. een microchip), een lezer en een applicatie die via middleware gekoppeld is aan de tags en lezers en die de gegenereerde gegevens verwerkt. De tag bestaat uit een elektronische schakeling die gegevens opslaat en een antenne die de gegevens via radiogolven verzendt. De lezer is uitgerust met een antenne en een demodulator die de via de radioverbinding ontvangen analoge informatie omzet in digitale gegevens. De informatie kan dan over netwerken worden verstuurd naar databanken en servers om te worden verwerkt door een computer.

([2]) De e-privacyrichtlijn verwijst in artikel 3 naar RFID: „Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.". Dit wordt aangevuld door overweging 56: „De technologische vooruitgang maakt de ontwikkeling mogelijk van nieuwe toepassingen die zijn gebaseerd op systemen voor gegevensverzameling en identificatie, zoals contactloze radiofrequentiesystemen. RFID-systemen (Radio Frequency Identification Devices) bijvoorbeeld maken gebruik van radiofrequenties om gegevens op te vangen van op unieke wijze geïdentificeerde RFI-chips, gegevens die vervolgens kunnen worden verstuurd over bestaande communicatienetwerken. Een breed gebruik van dergelijke technologieën kan aanzienlijke economische en maatschappelijke baten opleveren en kan dus een krachtige bijdrage leveren voor de interne markt, op voorwaarde dat hun gebruik aanvaardbaar is voor de burger. Om dat doel te bewerkstelligen, is het noodzakelijk al de fundamentele rechten van het individu, inclusief het recht op privacy en gegevensbescherming, te waarborgen. Wanneer dergelijke systemen aan openbare elektronischecommunicatienetwerken worden gekoppeld of gebruikmaken van elektronischecommunicatiediensten als basisinfrastructuur gelden de relevante bepalingen van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), inclusief die in verband met veiligheids-, verkeers- en locatiegegevens en vertrouwelijkheid.".

([3]) Artikel 17 van de gegevensbeschermingsrichtlijn, bijvoorbeeld, legt de verplichting op passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, of niet-toegelaten verspreiding.

de richtlijnen niet voldoende preciseren in welk soort waarborgen moet worden voorzien in RFID-toepassingen. De bestaande voorschriften dienen te worden aangevuld met regels die specifieke waarborgen opleggen en inzonderheid de integratie van technische oplossingen (ingebouwde privacy) in de RFID-technologie verplicht stellen. Meer bepaald zouden tags die persoonlijke informatie opslaan uitschakelbevelen moeten bevatten en zou cryptografie moeten worden gebruikt bij tags die bepaalde categorieën van persoonsgegevens opslaan.

V.2. **Zelfregulering als eerste stap**

60. In maart 2007 heeft de Commissie een mededeling [1] goedgekeurd waarin onder andere wordt gesteld dat er gedetailleerde richtsnoeren nodig zijn voor de praktische toepassing van RFID en dat de vaststelling van ontwerpcriteria wenselijk is om privacy- en veiligheidsrisico's te voorkomen.

61. Om deze doelstellingen te verwezenlijken heeft de Commissie in mei 2009 een aanbeveling over de tenuitvoerlegging van de beginselen inzake privacy en gegevensbescherming in RFID-toepassingen goedgekeurd [2]. Deze aanbeveling schrijft voor dat de tags bij RFID-toepassingen voor de kleinhandel moeten worden gedeactiveerd op de plaats van verkoop, tenzij de consument toestemming verleent. Dit voorschrift is niet van toepassing indien uit een effectenbeoordeling blijkt dat de tags geen aannemelijke bedreiging vormen voor de persoonlijke levenssfeer of de bescherming van persoonsgegevens; in dat geval blijven ze operationeel na de verkoop, tenzij de consument wil dat ze — kosteloos — worden gedeactiveerd.

62. De EDPS is het eens met de aanpak van de Commissie om zelfreguleringsinstrumenten te gebruiken. Het is evenwel, zoals hieronder beschreven, best denkbaar dat zelfregulering niet de verwachte resultaten oplevert. Daarom roept hij de Commissie op bereid te zijn om alternatieve maatregelen aan te nemen.

V.3. **Zorgpunten en mogelijke aanvullende maatregelen indien zelfregulering niet werkt**

63. De EDPS vreest dat organisaties die werken met RFID-toepassingen in de kleinhandelsector de mogelijkheid over het hoofd kunnen zien dat RFID-tags worden gevolgd door ongewenste derden. Hierdoor zouden eventueel in de tag opgeslagen persoonsgegevens bekend kunnen worden, maar het zou een derde ook in staat kunnen stellen om iemand in de tijd te volgen of te herkennen aan de hand van de unieke identificatiecodes in één of meer tags die hij of zij draagt, en dit zelfs in een omgeving die buiten het operationele bereik van de RFID-toepassing valt. Hij is ook bezorgd dat gebruikers van RFID-toepassingen in de verleiding kunnen komen om van de uitzondering de regel te maken en de tags operationeel te laten na de verkoop.

64. Als het bovenstaande zich voordoet, kan het te laat zijn om de risico's voor de misschien reeds aangetaste privacy en gegevensbescherming af te wenden. Gezien de aard van zelfregulering kunnen de nationale handhavingsinstanties bovendien in een zwakkere positie staan wanneer ze eisen dat organisaties die werken met RFID-toepassingen specifieke maatregelen betreffende ingebouwde privacy toepassen.

65. Daarom roept de EDPS de Commissie op bereid te zijn om wetgevende instrumenten voor te stellen die de belangrijkste aspecten van RFID-gebruik regelen ingeval de effectieve tenuitvoerlegging van het bestaande rechtskader mislukt. De beoordeling van de Commissie mag niet te lang worden uitgesteld; dat zou individuele personen immers blootstellen aan risico's en het zou ook een averechtse uitwerking hebben op de bedrijven omdat de rechtsonzekerheid te groot is en het wellicht moeilijker en duurder is om diepgewortelde problemen te verhelpen.

66. Als een van de maatregelen die zouden moeten worden voorgesteld beveelt de EDPS de toepassing van het beginsel van uitdrukkelijke toestemming op het punt van verkoop („opt-in") aan; volgens dit beginsel worden alle aan verbruiksproducten bevestigde RFID-tags gedeactiveerd op het punt van verkoop behoudens toestemming van de consument. Het is waarschijnlijk niet nodig of passend dat de Commissie specificeert welke concrete technologie moet worden gebruikt. Het EU-recht moet daarentegen wel de wettelijke verplichting tot het verkrijgen van toestemming creëren en de gebruikers van RFID-toepassingen zelf laten beslissen hoe ze aan deze eis voldoen.

V.4. **Verdere overwegingen: beheer van het internet der dingen**

67. De informatie die wordt gegenereerd door RFID-tags, productinformatie bijvoorbeeld, zou uiteindelijk onderling kunnen worden gekoppeld in een algemeen netwerk van communicatie-infrastructuur. Dat wordt gewoonlijk het „internet der dingen" genoemd en doet vragen inzake gegevensbescherming en privacy rijzen, omdat voorwerpen uit de reële wereld kunnen worden geïdentificeerd door RFID-tags die naast productinformatie ook persoonsgegevens kunnen bevatten.

68. Er zijn nog veel vragen onbeantwoord: wie zal de opslag van informatie afkomstig van voorwerpen met tags beheren? Hoe zal deze opslag worden georganiseerd? Wie krijgt toegang tot de informatie? In juni 2009 keurde de Commissie een mededeling over het internet der dingen goed [3] waarin expliciet wordt aangegeven met welke problemen inzake gegevensbescherming en privacy dit verschijnsel gepaard kan gaan.

---

[1] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 15 maart 2007 betreffende radiofrequentie-identificatie (RFID) in Europa: maatregelen met het oog op een beleidskader, COM(2007) 96 definitief.

[2] Aanbeveling van de Commissie van 12 mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen, C(2009) 3200 definitief.

[3] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio' van 18 juni 2009 betreffende het internet van de dingen — Een actieplan voor Europa, COM(2009) 278 definitief.

69. De EDPS wil graag wijzen op een aantal door de Commissie naar voren gebrachte punten die volgens hem nadere aandacht verdienen naarmate het internet der dingen zich verder ontwikkelt. Ten eerste zou een gedecentraliseerde architectuur de verantwoording en afdwingbaarheid van het EU-rechtskader kunnen vergemakkelijken. Ten tweede moet het recht van het individu om niet te worden gevolgd zoveel mogelijk worden gehandhaafd. Dat betekent dat personen slechts in zeer beperkte gevallen via RFID-tags mogen worden gevolgd zonder hun toestemming. Die toestemming moet uitdrukkelijk worden gegeven. Dat wordt gewoonlijk het recht op „stilzwijgen van de chips" genoemd, of het recht om met rust te worden gelaten. Ten slotte moet ingebouwde privacy een leidend beginsel zijn bij het ontwerpen van het internet der dingen. Dat zou bijvoorbeeld inhouden dat concrete RFID-toepassingen met ingebouwde mechanismen die de gebruikers controle verschaffen, zo worden ontworpen dat de standaardinstellingen maximale privacy bieden.

70. De EDPS verwacht te worden geraadpleegd wanneer de Commissie de in de mededeling beoogde acties ten uitvoer legt, in het bijzonder wanneer ze de mededeling over privacy en vertrouwen in de alomtegenwoordige informatiemaatschappij opstelt.

VI. **SOCIALE NETWERKEN EN DE BEHOEFTE AAN STANDAARDPRIVACYINSTELLINGEN**

71. Sociale netwerken zijn „in". Ze lijken nog populairder te zijn geworden dan e-mails. Ze brengen mensen met dezelfde interesses en/of activiteiten in verbinding met elkaar. Mensen kunnen hun profiel online plaatsen en mediabestanden als video's, foto's, muziek en hun loopbaanprofielen delen.

72. Jongeren waren snel gewonnen voor de sociale netwerken en deze trend zet zich door. De gemiddelde leeftijd van de internetgebruikers in Europa is de voorbije jaren gedaald: 9- en 10-jarigen zitten verscheidene keren per week op het internet, 12- tot 14-jarigen gaan dagelijks online, vaak gedurende één tot drie uur.

VI.1. **Sociale netwerken en het toepasselijke rechtskader voor gegevensbescherming en privacy**

73. De ontwikkeling van de sociale netwerken heeft de gebruikers in staat gesteld informatie over zichzelf en anderen naar het internet te uploaden. Door dit te doen, aldus de Werkgroep artikel 29 ([1]), treden de internetgebruikers voor de gegevens die ze uploaden op als voor de verwerking verantwoordelijken zoals bedoeld in artikel 2, onder d), van de gegevensbeschermingsrichtlijn ([2]). In de meeste gevallen echter valt deze verwerking onder de gangbare uitzondering bedoeld in artikel 3, lid 2, van de richtlijn. Tegelijkertijd worden ook de socialenetwerkdiensten beschouwd als voor de verwerking verantwoordelijken in zover zij de middelen voor de verwerking van gebruikersgegevens aanreiken en alle basisdiensten in verband met gebruikersbeheer (bv. registratie en schrapping van accounts) verstrekken.

74. In rechtstermen betekent dit dat de internetgebruikers en socialenetwerkdiensten samen verantwoordelijk zijn voor de verwerking van persoonsgegevens als „voor de verwerking verantwoordelijken" zoals bedoeld in artikel 2, onder d), van de richtlijn, zij het in verschillende mate en met verschillende reeksen verplichtingen.

75. De gebruikers dienen bijgevolg te weten en te begrijpen dat zij, door hun persoonsgegevens en die van anderen te verwerken, vallen onder de bepalingen van de EU-wetgeving over gegevensbescherming, die onder andere voorschrijft dat toestemming met kennis van zaken moet worden verkregen van degenen wier informatie wordt geüpload en dat aan de betrokkenen een recht op correctie, bezwaar, enz. moet worden verleend. Zo ook moeten de socialenetwerkdiensten onder andere passende technische en organisatorische maatregelen ten uitvoer leggen om ongeoorloofde verwerking te verhinderen, rekening houdend met de risico's die de verwerking en de aard van de gegevens met zich meebrengen. Dat betekent tevens dat de socialenetwerkdiensten moeten voorzien in privacyvriendelijke standaardinstellingen, met inbegrip van instellingen die de toegang tot gebruikersprofielen beperken tot de door de gebruiker zelf geselecteerde contacten. Deze instellingen moeten ook dusdanig zijn, dat de toestemming van de gebruiker vereist is voordat een profiel toegankelijk wordt gemaakt voor derden, en de beperkt toegankelijke profielen mogen niet kunnen worden ontdekt door interne zoekmachines.

76. Helaas bestaat er een kloof tussen de wettelijke voorschriften en de feitelijke naleving ervan. Hoewel internetgebruikers juridisch gezien worden beschouwd als voor de verwerking verantwoordelijken en gebonden zijn door het EU-rechtskader voor gegevensbescherming en privacy, zijn ze zich in werkelijkheid vaak niet bewust van deze rol. Algemeen gesproken beseffen zij niet goed dat ze persoonsgegevens verwerken en dat het publiceren van dergelijke informatie risico's inhoudt voor de privacy en gegevensbescherming. Vooral jongeren plaatsen informatie online en onderschatten de gevolgen ervan voor zichzelf en voor anderen, bijvoorbeeld in de context van inschrijvingen in onderwijsinstellingen of sollicitaties naar betrekkingen.

([1]) Zie advies 163, 5/2009 van de Werkgroep artikel 29 over sociale netwerken op het internet, goedgekeurd op 12 juni 2009.

([2]) Onder „voor de verwerking verantwoordelijke" wordt verstaan de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen.

77. De aanbieders van sociale netwerken, van hun kant, selecteren vaak vooraf standaardinstellingen die gebaseerd zijn op stilzwijgende toestemming, waardoor de bekendmaking van persoonlijke informatie wordt vergemakkelijkt. Sommige aanbieders maken profielen standaard beschikbaar voor gewone zoekmachines. Dat doet vragen rijzen over het feit of de betrokken personen daadwerkelijk toestemming hebben verleend voor de bekendmaking en of de sociale netwerken voldoen aan artikel 17 van de richtlijn (zie boven), dat voorschrijft dat ze passende technische en organisatorische maatregelen ten uitvoer moeten leggen om ongeoorloofde verwerking te verhinderen.

VI.2. **Risico's voortvloeiend uit sociale netwerken en voorgestelde maatregelen om ze te verminderen**

78. Het bovenstaande leidt tot een verhoogd risico voor de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Het stelt de internetgebruikers en degenen wier gegevens zijn geüpload bloot aan flagrante schendingen van hun privacy en gegevensbescherming.

79. De vraag die de Commissie tegen deze achtergrond moet beantwoorden is: wat kan en moet er worden gedaan om deze situatie te verhelpen? Dit advies biedt geen alomvattend antwoord op die vraag, maar presenteert een aantal voorstellen ter overweging.

Investeren in de voorlichting van internetgebruikers

80. Het eerste voorstel is te investeren in de voorlichting van de internetgebruikers. De EU-instellingen en de nationale overheden zouden moet investeren in de voorlichting en bewustmaking inzake de gevaren van socialenetwerksites. Het DG Informatiemaatschappij, bijvoorbeeld, heeft het programma Veiliger Internet lopen, dat erop gericht is de positie van kinderen en jongeren te versterken en hen te beschermen door middel van, onder andere, bewustmakingsactiviteiten ([1]). Onlangs gingen de EU-instellingen van start met de campagne „Denk na voor je iets online zet", om jongeren bewust te maken van de risico's die het delen van persoonlijke informatie met vreemden inhoudt.

81. De EDPS moedigt de Commissie aan zulke activiteiten te blijven steunen. Maar ook de aanbieders van sociale netwerken moeten een actieve rol spelen, aangezien zij de juridische en sociale verantwoordelijkheid hebben om de gebruikers te leren hoe ze hun diensten op een veilige en privacyvriendelijke manier kunnen gebruiken.

82. Zoals hierboven beschreven, kan de informatie die op sociale netwerken wordt geplaatst op diverse wijzen standaard beschikbaar worden gesteld. Informatie kan bijvoorbeeld beschikbaar zijn voor het algemene publiek, met inbegrip van zoekmachines, die ze kunnen indexeren en er directe koppelingen naar kunnen aanbieden. Daarnaast kan informatie ook worden beperkt tot „geselecteerde vrienden" of volledig privé worden gehouden. Uiteraard verschillen de toegangstoestemmingen voor profielen en de gebruikte terminologie van site tot site.

83. Zoals hierboven uiteengezet, weten echter slechts weinig gebruikers van socialenetwerkdiensten hoe ze de toegang tot de door hen geplaatste informatie kunnen controleren, laat staan hoe ze de standaardprivacyinstellingen kunnen wijzigen. Privacyinstellingen blijven gewoonlijk ongewijzigd omdat de gebruikers zich niet bewust zijn van de implicaties als ze ze niet veranderen of niet weten hoe ze ze moeten veranderen. Het feit dat gebruikers de privacyinstellingen niet wijzigen, betekent dus meestal niet dat ze met kennis van zaken hebben beslist om te aanvaarden dat hun informatie wordt gedeeld. In deze context is het des te belangrijker dat derden zoals zoekmachines geen koppelingen naar individuele profielen aanbieden, in de veronderstelling dat de gebruikers ermee hebben ingestemd (door de privacyinstellingen niet te wijzigen) dat de informatie onbeperkt beschikbaar wordt gesteld.

84. Deze situatie kan mede worden verholpen door de gebruikers voor te lichten, maar dat alleen volstaat niet. Zoals de Werkgroep artikel 29 aanbeveelt in zijn advies over sociale netwerken, zouden de aanbieders van sociale netwerken kosteloos privacyvriendelijke standaardprivacyinstellingen moeten aanbieden. Dat zou de gebruikers bewuster maken van wat ze doen en hen in staat stellen om betere keuzes te maken met betrekking tot het al dan niet delen van informatie en met wie.

Rol van zelfregulering

85. De Commissie heeft met twintig aanbieders van sociale netwerken de overeenkomst „Safer Social Networking Principles for the EU" (beginselen van veiligere sociale netwerken voor de EU) gesloten ([2]). Deze overeenkomst heeft tot doel de veiligheid van minderjarigen bij het gebruik van socialenetwerksites in Europa te verbeteren. De beginselen bevatten veel eisen die afgeleid zijn van de toepassing van het hierboven beschreven rechtskader voor gegevensbescherming. Bijvoorbeeld de eis om gebruikers via hulpmiddelen en technologie in staat te stellen om het gebruik en de verspreiding van hun persoonlijke informatie te controleren. Ze bevatten ook de eis dat standaardprivacyinstellingen moeten worden aangeboden.

86. Begin januari 2010 maakte de Commissie de bevindingen van een evaluatieverslag over de toepassing van de beginselen bekend ([3]). De EDPS is bezorgd over het feit dat uit dit verslag blijkt dat sommige stappen zijn ondernomen, maar veel andere niet. Zo wordt in het verslag vastgesteld dat er problemen waren betreffende het meedelen van op de sites beschikbare veiligheidsmaatregelen en -hulpmiddelen. Er wordt ook vastgesteld dat minder dan de helft

([1]) Informatie over dit programma is beschikbaar op: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Deze beginselen zijn beschikbaar op: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Verslag over de beoordeling van de toepassing van de beginselen van veiligere sociale netwerken voor de EU, beschikbaar op: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

van de ondertekenaars van de overeenkomst de toegang tot de profielen van minderjarigen beperkt tot alleen hun vrienden.

Verplichtstelling van standaardprivacyinstellingen

87. In deze context is de fundamentele vraag of er aanvullende beleidsmaatregelen nodig zijn om ervoor te zorgen dat de sociale netwerken hun diensten aanbieden met standaardprivacyinstellingen. Deze vraag is opgeworpen door Viviane Reding, de EU-commissaris bevoegd voor de informatiemaatschappij, die aangaf dat een wetgeving ter zake nodig zou kunnen zijn ([1]). In dezelfde zin stelde het Europees Economisch en Sociaal Comité dat er naast zelfregulering ook minimale beschermingsnormen door de wet zouden moeten worden opgelegd ([2]).

88. Zoals hierboven opgemerkt, kan de verplichting voor aanbieders van sociale netwerken om standaardprivacyinstellingen toe te passen, indirect worden afgeleid uit artikel 17 van de gegevensbeschermingsrichtlijn ([3]), die de voor de verwerking verantwoordelijken verplicht om passende technische en organisatorische maatregelen te nemen („zowel bij het ontwerpen als bij de uitvoering van de verwerking") om de veiligheid te waarborgen en elke ongeoorloofde verwerking te verhinderen, rekening houdend met de risico's die de verwerking en de aard van de gegevens met zich meebrengen.

89. Dat artikel is evenwel veel te algemeen en te weinig specifiek, ook in deze context. Het verduidelijkt niet wat er wordt bedoeld met passende technische en organisatorische maatregelen in de context van sociale netwerken. De huidige situatie is er dus een van rechtsonzekerheid, wat problemen veroorzaakt voor zowel de regelgevende instanties als de personen wier privacy en persoonsgegevens niet volledig beschermd zijn.

90. In het licht van het bovenstaande dringt de EDPS er bij de Commissie op aan een wetgeving op te stellen die minstens een algemene eis voor verplichte privacyinstellingen bevat, naast andere, meer precieze eisen:

a) er moet worden voorzien in instellingen die de toegang tot gebruikersprofielen beperkt tot de door de gebruiker zelf geselecteerde contacten. De instellingen moeten ook dusdanig zijn, dat de toestemming van de gebruiker vereist is voordat een profiel toegankelijk wordt gemaakt voor derden;

b) de beperkt toegankelijke profielen mogen niet kunnen worden ontdekt door interne of externe zoekmachines.

91. De vraag blijft bestaan of er, naast de verplichte standaardprivacyinstellingen nog aanvullende specifieke gegevensbeschermingsmaatregelen of andere maatregelen (bijvoorbeeld met betrekking tot de bescherming van minderjarigen) nodig zijn. Hierdoor rijst de ruimere vraag of het passend zou zijn om voor dit soort diensten een specifiek kader te scheppen dat niet alleen verplichte privacyinstellingen oplegt, maar ook andere aspecten regelt. De EDPS verzoekt de Commissie om dit te bestuderen.

VII. **STANDAARDPRIVACYINSTELLINGEN IN BROWSERS OM TOESTEMMING MET KENNIS VAN ZAKEN TE WAARBORGEN VOOR HET ONTVANGEN VAN ADVERTENTIES**

92. Aanbieders van advertentienetwerken gebruiken cookies en andere middelen om het surfgedrag van individuele gebruikers op het internet te volgen teneinde hun interesses te catalogiseren en profielen samen te stellen. Deze informatie wordt dan gebruikt om gerichte advertenties naar hen te sturen ([4]).

VII.1. **Resterende uitdagingen en risico's van het huidige rechtskader voor gegevensbescherming en privacy**

93. Deze verwerking valt onder de gegevensbeschermingsrichtlijn (wanneer het gaat om persoonsgegevens) en onder artikel 5.3 van de e-privacyrichtlijn. Dit artikel schrijft meer specifiek voor dat de gebruiker moet worden geïnformeerd en de kans moet krijgen om te reageren door al dan niet in te stemmen met de opslag van cookies en dergelijke op zijn computer of een ander apparaat ([5]).

94. Tot op heden gebruikten de aanbieders van advertentienetwerken browserinstellingen en een privacybeleid om de gebruikers te informeren en hen in staat te stellen al dan niet in te stemmen met cookies. In het privacybeleid van de uitgever legden zij uit hoe de gebruikers ervoor konden kiezen om helemaal geen cookies te ontvangen of om geval per geval te beslissen of ze er wilden ontvangen.

([1]) Viviane Reding, lid van de Europese Commissie bevoegd voor de informatiemaatschappij en media: Denk na voor je iets online zet! Hoe socialenetwerksites veiliger maken voor kinderen en tieners? Safer Internet Day, Straatsburg, 9 februari 2010.

([2]) Advies van het Europees Economisch en Sociaal Comité over de impact van sociale netwerksites op burgers/consumenten, 4 november 2009.

([3]) Ook nader beschreven in punt 33 van dit document.

([4]) Traceercookies zijn kleine tekstbestanden met een unieke identificatiecode. Aanbieders van advertentienetwerken (en ook websitebeheerders of -uitgevers) plaatsen cookies op de harde schijf van de bezoekers, met name in de browser van internetgebruikers, wanneer de gebruikers voor het eerst websites bezoeken die advertenties bevatten welke deel uitmaken van hun netwerk. Dankzij de cookie kan de aanbieder van het advertentienetwerk een vroegere bezoeker herkennen wanneer die terugkeert naar dezelfde website of een partnerwebsite van het advertentienetwerk bezoekt. Aan de hand van zulke herhaalde bezoeken kan de aanbieder van het advertentienetwerk een profiel van de bezoeker samenstellen.

([5]) Artikel 5, lid 3, van de e-privacyrichtlijn werd onlangs gewijzigd om gebruikers nog beter te beschermen tegen het onderscheppen van hun communicatie door middel van, bijvoorbeeld, spyware en cookies die op de computer of een ander apparaat van de gebruiker worden opgeslagen. Krachtens de nieuwe richtlijn moeten de gebruikers beter worden geïnformeerd en gemakkelijker kunnen aangeven of ze willen dat cookies worden opgeslagen op hun eindapparatuur.

Op die manier wilden ze voldoen aan hun verplichting om de gebruikers het recht te bieden cookies te weigeren.

95. Hoewel deze methode (via de browser) in theorie inderdaad zou kunnen leiden tot een met kennis van zaken gegeven toestemming, is de werkelijkheid heel anders. In het algemeen ontbreekt het de gebruikers aan een fundamenteel inzicht in het verzamelen van gegevens, met name van derden, in de waarde van zulke gegevens, in het gebruik ervan en in de werking van de technologie; inzonderheid weten ze vaak niet hoe en waar ze advertenties kunnen weigeren. De stappen die een gebruiker moeten ondernemen om zijn toestemming in te trekken lijken niet alleen gecompliceerd maar ook excessief (eerst moet hij zijn browser zo instellen, dat hij cookies aanvaardt, en dan moet hij de optie „niet aanvaarden" („opt-out") kiezen).

96. In de praktijk betekent dit dat heel weinig mensen de optie „niet aanvaarden" kiezen: niet omdat ze met kennis van zaken hebben besloten om advertenties op basis van zoekgedrag te aanvaarden, maar veeleer omdat ze niet beseffen dat ze door de optie „niet aanvaarden" niet te kiezen, de advertenties in feite aanvaarden.

97. Hoewel artikel 5, lid 3, van de e-privacyrichtlijn juridisch gezien doeltreffende rechtsbescherming biedt, is het in de praktijk zo, dat internetgebruikers worden geacht ermee in te stemmen dat ze worden gevolgd met het oog op de verzending van advertenties op basis van zoekgedrag, terwijl ze zich er vaak, om niet te zeggen meestal, totaal niet van bewust zijn dat ze worden gevolgd.

98. De Werkgroep artikel 29 werkt aan een advies om duidelijkheid te scheppen over de juridische eisen die moeten worden gesteld aan het adverteren op basis van zoekgedrag, en dat is een goede zaak. Maar uitlegging zal op zich wellicht niet volstaan om deze situatie op te lossen en het kan nodig zijn dat de Europese Unie aanvullende maatregelen neemt.

VII.2. **Behoefte aan verdere maatregelen, met name om standaardprivacyinstellingen verplicht te stellen**

99. Zoals hierboven beschreven verlenen webbrowsers in het algemeen een zekere controle over bepaalde soorten cookies. Momenteel aanvaarden de standaardinstellingen van de meeste webbrowsers alle cookies. Met andere woorden, de browsers zijn standaard ingesteld om alle cookies te aanvaarden, ongeacht het doel van de cookie. Alleen indien de gebruiker de instellingen van zijn browserapplicatie wijzigt om cookies te weigeren, wat, zoals hierboven gezegd, heel weinig gebruikers doen, zal hij geen cookies ontvangen. Bovendien verschijnt er geen privacywizard wanneer de browserapplicaties worden geïnstalleerd of geüpdatet.

100. Dit probleem zou kunnen worden opgelost als de browsers standaardprivacyinstellingen hadden. Anders gezegd, als ze een instelling hadden die het mogelijk maakt om cookies van derden niet te aanvaarden. Om dit aan te vullen en doeltreffender te maken, zouden de browsers de gebruikers een privacywizard moeten laten doorlopen wanneer ze de browser installeren of updaten. Er is behoefte aan meer verfijning en duidelijke informatie over de verschillende soorten cookies en het nut van sommige ervan. Gebruikers die willen worden gevolgd om advertenties te ontvangen, zullen naar behoren worden geïnformeerd en dienen de browserinstellingen te veranderen. Hierdoor hebben ze meer controle over hun persoonsgegevens en privacy. Dat zou, naar de mening van de EDPS, een doeltreffende manier zijn om ervoor te zorgen dat de toestemming van de gebruikers geëerbiedigd en gewaarborgd wordt ([1]).

101. Rekening houdend met, enerzijds, de wijdverbreidheid van het probleem, d.w.z. het aantal internetgebruikers dat thans wordt gevolgd op basis van een denkbeeldige toestemming, en, anderzijds, de omvang van de belangen die op het spel staan, worden aanvullende waarborgen steeds dringender. De toepassing van het beginsel van ingebouwde privacy in webbrowserapplicaties zou de gebruikers veel meer controle bieden over de gegevensverzamelingsmethoden die worden gebruikt voor reclamedoeleinden.

102. Daarom dringt de EDPS er bij de Commissie op aan juridische maatregelen te overwegen die standaardprivacyinstellingen in browsers en het verstrekken van relevante informatie verplicht stellen.

VIII. **ANDERE BEGINSELEN TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER EN PERSOONSGEGEVENS**

103. Het beginsel van ingebouwde privacy biedt grote mogelijkheden om de bescherming van de persoonlijke levenssfeer en persoonsgegevens te verbeteren, maar daarnaast moeten aanvullende beginselen worden ontwikkeld en omgezet in wetgeving om ervoor te zorgen dat de consumenten vertrouwen krijgen in ICT. Tegen deze achtergrond gaat de EDPS dieper in op het aansprakelijkheidsbeginsel en op de opstelling van een bindend kader voor inbreuken op de beveiliging dat toepasselijk is op alle sectoren.

VIII.1. **Het aansprakelijkheidsbeginsel om de naleving van het beginsel van ingebouwde privacy te waarborgen**

104. In zijn nota „The Future of Privacy" ([2]) beveelt de Werkgroep artikel 29 aan om het aansprakelijkheidsbeginsel op te nemen in de gegevensbeschermingsrichtlijn. Volgens dit

([1]) Tergelijkertijd is de EDPS zich er bewust van dat dit het probleem niet volledig zou oplossen, aangezien er cookies zijn die niet via de browser kunnen worden gecontroleerd, bijvoorbeeld de zogenaamde flashcookies. Hiervoor zouden de ontwikkelaars van browsers flashcontroles moeten integreren in de standaardcookiecontroles van hun nieuwe browserversies.

([2]) Advies 168 van de Werkgroep artikel 29 over de toekomst van privacy, gezamenlijke bijdrage aan de raadpleging van de Europese Commissie inzake het rechtskader voor het grondrecht op de bescherming van persoonsgegevens, goedgekeurd op 1 december 2009.

beginsel, dat wordt erkend in sommige multinationale gegevensbeschermingsinstrumenten ([1]), moeten organisaties processen toepassen om bestaande wetten na te leven en methoden opzetten om de naleving van de wet en andere bindende instrumenten te beoordelen en aan te tonen.

105. De EDPS staat volledig achter de aanbeveling van de Werkgroep artikel 29. Hij is van oordeel dat dit beginsel uiterst relevant zal zijn om de effectieve toepassing van de gegevensbeschermingsbeginselen en -verplichtingen te bevorderen. Aansprakelijkheid vereist dat de voor de verwerking verantwoordelijken aantonen dat ze het mechanisme hebben opgezet dat nodig is om de toepasselijke wetgeving inzake gegevensbescherming na te leven. Dat zal waarschijnlijk bijdragen tot de effectieve toepassing van ingebouwde privacy in ICT als een bijzonder geschikt element om blijk te geven van aansprakelijkheid.

106. Om aansprakelijkheid te meten en aan te tonen kunnen de voor de verwerking verantwoordelijken interne procedures gebruiken of een beroep doen op derden om audits of andere controles te laten uitvoeren die kunnen leiden tot de toekenning van keurmerken of prijzen. In deze context dringt de EDPS er bij de Commissie op aan te overwegen of het niet nuttig zou kunnen zijn om, naast een algemeen aansprakelijkheidsbeginsel, een wet in te voeren die specifieke aansprakelijkheidsmaatregelen voorschrijft, zoals de verplichting om de effecten op de privacy en gegevensbescherming te beoordelen en onder welke omstandigheden.

VIII.2. **Inbreuken op de beveiliging: voltooiing van het rechtskader**

107. Krachtens de vorig jaar in de e-privacyrichtlijn aangebrachte wijzigingen moeten inbreuken in verband met persoonsgegevens worden gemeld aan de betrokken personen en aan de bevoegde instanties. Een inbreuk in verband met persoonsgegevens wordt ruim gedefinieerd als elke inbreuk die resulteert in de vernietiging, het verlies, de vrijgave, enz. van persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de dienst. De betrokken personen moeten in kennis worden gesteld indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonsgegevens of persoonlijke levenssfeer. Dat zou het geval kunnen zijn wanneer de inbreuk kan resulteren in identiteitsdiefstal, ernstige vernedering of aantasting van de reputatie. De bevoegde instanties moeten in kennis worden gesteld van elke inbreuk in verband met persoonsgegevens, ongeacht of ze een risico voor personen inhoudt.

Toepassing van verplichtingen inzake inbreuken in alle sectoren

108. Helaas geldt deze verplichting alleen voor de aanbieders van voor het publiek beschikbaar gestelde elektronischecommunicatiediensten, zoals telefoonbedrijven, aanbieders van internettoegang, aanbieders van webmail, enz. De EDPS dringt er bij de Commissie op aan voorstellen inzake inbreuken op de beveiliging te doen die in alle sectoren van toepassing zijn. Wat de inhoud van een dergelijk kader betreft, oordeelt de EDPS dat het in de e-privacyrichtlijn vastgestelde rechtskader voor inbreuken op de beveiliging zorgt voor een goed evenwicht tussen de bescherming van de rechten van natuurlijke personen, met inbegrip van hun recht op gegevensbescherming en persoonlijke levenssfeer, en de verplichtingen die worden opgelegd aan de betrokken entiteiten. Tegelijkertijd is het een kader met echte „tanden", aangezien het wordt ondersteund door zinvolle handhavingsbepalingen die de autoriteiten voldoende bevoegdheden verlenen om te onderzoeken en te straffen in geval van niet-naleving.

109. Bijgevolg dringt de EDPS er bij de Commissie op aan een wetsvoorstel aan te nemen dat dit kader in alle sectoren toepast, eventueel met de nodige aanpassingen. Dat zou er bovendien voor zorgen dat in alle sectoren dezelfde normen en procedures worden toegepast.

Het in de e-privacyrichtlijn ingebouwde rechtskader voltooien via comitologie

110. De herziene e-privacyrichtlijn machtigt de Commissie om technische handhavingsmaatregelen, d.w.z. gedetailleerde maatregelen inzake de kennisgeving van inbreuken op de beveiliging, aan te nemen via een comitologieprocedure ([2]). Deze machtiging is gerechtvaardigd met het oog op een consistente tenuitvoerlegging en toepassing van het rechtskader voor inbreuken op de beveiliging. Een consistente tenuitvoerlegging moet erop gericht zijn een even hoog beschermingsniveau te bieden aan alle burgers in de Gemeenschap en ervoor te zorgen dat de betrokken entiteiten niet worden belast met uiteenlopende kennisgevingsvoorschriften.

111. De e-privacyrichtlijn is goedgekeurd in november 2009. Er lijkt geen enkele reden te zijn om niet meteen te beginnen werken aan de aanneming van de technische tenuitvoerleggingsmaatregelen. De EDPS heeft twee seminars georganiseerd met het oogmerk ervaringen inzake de kennisgeving van inbreuken in verband met persoonsgegevens te delen en te verzamelen. Hij is bereid om de resultaten van deze seminars te delen en verheugt zich erop om met de Commissie en andere belanghebbenden samen te werken aan de verfijning van het algemeen rechtskader voor inbreuken in verband met persoonsgegevens.

112. De EDPS dringt er bij de Commissie op aan snel de nodige stappen te ondernemen. Alvorens technische tenuitvoerleggingsmaatregelen aan te nemen moet de Commissie overgaan tot een brede raadpleging met onder andere ENISA, de EDPS en de Werkgroep artikel 29. Ze dient ook andere „relevante belanghebbenden" te raadplegen, inzonderheid om zich te informeren over de beste beschikbare technische en economische tenuitvoerleggingsmiddelen.

([1]) OESO-richtsnoeren van 1980 inzake de bescherming van privacy en grensoverschrijdend verkeer van persoonsgegevens; privacyverklaring van Madrid van 3 november 2009 over wereldwijde privacynormen voor een geglobaliseerde wereld.

([2]) Comitologie behelst dat technische tenuitvoerleggingsmaatregelen worden aangenomen via een comité bestaande uit vertegenwoordigers van de lidstaten en voorgezeten door de Commissie. Voor de e-privacyrichtlijn is de zogenaamde regelgevingsprocedure met toetsing van toepassing, wat betekent dat het Europees Parlement en de Raad zich kunnen verzetten tegen door de Commissie voorgestelde maatregelen. Zie verder http://europa.eu/scadplus/glossary/comitology_nl.htm

IX. **CONCLUSIES**

113. Vertrouwen, of liever het gebrek eraan, blijkt een essentieel onderwerp te zijn in de opkomst en succesvolle toepassing van de informatie- en communicatietechnologieën. Als de mensen geen vertrouwen hebben in ICT, is de kans groot dat deze technologieën mislukken. Het vertrouwen in ICT hangt af van verschillende factoren. Een van de belangrijkste is, dat wordt gewaarborgd dat deze technologieën de grondrechten van natuurlijke personen inzake de persoonlijke levenssfeer en de bescherming van persoonsgegevens niet aantasten.

114. Met het oog op een verdere versterking van het rechtskader voor gegevensbescherming en privacy, waarvan de beginselen hun volledige relevantie behouden in de informatiemaatschappij, stelt de EDPS aan de Commissie voor om ingebouwde privacy te integreren op verschillende niveaus van het EU-recht en -beleid.

115. Hij beveelt de Commissie aan de volgende vier actielijnen te volgen:

a) voorstellen om een algemene bepaling over ingebouwde privacy op te nemen in het rechtskader voor gegevensbescherming. Deze bepaling moet technologisch neutraal zijn en de naleving ervan moet verplicht worden gesteld in verschillende stadia;

b) deze algemene bepaling uitwerken in specifieke bepalingen wanneer specifieke rechtsinstrumenten in verschillende sectoren worden voorgesteld. Deze specifieke bepalingen zouden nu al kunnen worden opgenomen in rechtsinstrumenten op basis van artikel 17 van de gegevensbeschermingsrichtlijn (en andere bestaande wetgeving);

c) ingebouwde privacy als leidend beginsel opnemen in de Europese digitale agenda;

d) ingebouwde privacy als beginsel invoeren in andere EU-initiatieven (vooral niet-wetgevende).

116. Op drie aangeduide ICT-gebieden beveelt de EDPS de Commissie aan te beoordelen in hoever ze voorstellen dient te presenteren die het beginsel van ingebouwde privacy op specifieke wijze toepassen:

a) met betrekking tot RFID, wetgevende maatregelen voorstellen die de belangrijkste aspecten van het gebruik van RFID regelen ingeval de effectieve tenuitvoerlegging van het bestaande rechtskader via zelfregulering mislukt. Inzonderheid voorzien in het beginsel van uitdrukkelijke toestemming op het punt van verkoop („opt-in"), volgens hetwelk alle op verbruiksproducten aangebrachte RFID-tags worden gedeactiveerd op het punt van verkoop;

b) met betrekking tot sociale netwerken, een wetgeving opstellen die minstens een algemene eis voor verplichte privacyinstellingen bevat, naast de meer specifieke eisen dat de toegang tot gebruikersprofielen moet worden beperkt tot de door de gebruiker zelf geselecteerde contacten en dat de beperkt toegankelijke profielen niet ontdekt mogen kunnen worden door interne of externe zoekmachines;

c) met betrekking tot gerichte advertenties, een wetgeving overwegen die verplicht stelt dat de browserinstellingen standaard geen cookies van derden aanvaarden en dat de gebruikers een privacywizard moeten doorlopen wanneer ze de browser installeren of updaten.

117. Tot slot stelt de EDPS voor dat de Commissie:

a) overweegt om het aansprakelijkheidsbeginsel toe te passen in de bestaande gegevensbeschermingsrichtlijn, en

b) een kader van voorschriften en procedures ontwikkelt om de bepalingen van de e-privacyrichtlijn betreffende de kennisgeving van inbreuken op de beveiliging ten uitvoer te leggen en algemeen toepasselijk te maken voor alle voor de verwerking verantwoordelijken.

Gedaan te Brussel, 18 maart 2010.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming