



17/NL

WP 247

**Advies 01/2017 over  
het voorstel voor een verordening ter vervanging van de e-privacyrichtlijn (2002/58/EG)**

**Goedgekeurd op 4 april 2017**

De Groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij is het onafhankelijke EU-adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer. De taken van de Groep zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door de Europese Commissie, directoraat-generaal Justitie en Consumentenzaken, directoraat C (Grondrechten en Rechtsstaat), B-1049 Brussel, België, kantoor nr. MO-59 05/035.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING  
VAN PERSOONSgegevens**

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien artikelen 29 en 30 van die richtlijn,

Gezien het reglement van orde van de Groep,

**HEEFT HET VOLGENDE ADVIES GOEDGEKEURD:**

## SAMENVATTING

De Groep juicht het voorstel toe van de Europese Commissie van 10 januari 2017 voor een e-privacyverordening. Dat als regelgevend instrument een **verordening** wordt voorgesteld, is volgens haar een goede keuze, want een verordening zorgt voor uniforme regels in de gehele EU en creëert duidelijkheid voor toezichthoudende autoriteiten en organisaties. In dit geval verzekert een verordening ook samenhang met de algemene verordening gegevensbescherming. Die samenhang wordt versterkt door de keuze om de **autoriteit die de naleving van de algemene verordening gegevensbescherming moet controleren**, ook verantwoordelijk te maken voor de handhaving van de e-privacyregels.

De keuze voor (het behoud van) een **aanvullend rechtsinstrument** is tegelijk positief. De algemene verordening gegevensbescherming bevat immers geen bepalingen over de bescherming van vertrouwelijke communicatie en eindapparatuur. Door de bijzondere kenmerken van deze diensten zijn er aanvullende bepalingen nodig om een passende bescherming van het grondrecht op privéleven en op vertrouwelijkheid van communicatie, met inbegrip van vertrouwelijkheid van eindapparatuur, te verzekeren. In dat verband is de Groep duidelijk voorstander van de **beginselen van brede verboden en enge uitzonderingen** waarop de Commissie de voorgestelde verordening heeft gebaseerd en **de gerichte toepassing van het begrip toestemming**.

De Groep is blij dat het toepassingsgebied van de voorgestelde verordening is uitgebreid en nu ook **over-the-topcommunicatiediensten (hierna "OTT's" genoemd)** omvat. Dat zijn diensten die functioneel gelijkwaardig zijn aan de meer traditionele communicatiemiddelen en die bijgevolg een soortgelijk effect kunnen hebben op de privacy en het recht op geheimhouding van communicatie van mensen in de EU. Het is ook een goede zaak dat de voorgestelde verordening duidelijk betrekking heeft op **inhoud en bijbehorende metagegevens** en erkent dat **uit metagegevens zeer gevoelige informatie aan het licht kan komen**.

De Groep stelt echter ook vier **ernstige punten van zorg** vast. Zo zou de voorgestelde verordening ten opzichte van de algemene verordening gegevensbescherming minder bescherming bieden op het gebied van het **traceren van de locatie van eindapparatuur, de omstandigheden waaronder inhoud en metagegevens mogen worden geanalyseerd, de standaardinstellingen van eindapparatuur en software** en **"tracking walls"**. In dit advies doet de Groep specifieke voorstellen om ervoor te zorgen dat de e-privacyverordening hetzelfde of, afhankelijk van de gevoelige aard van de communicatiegegevens (zowel inhoud als metagegevens), een hoger beschermingsniveau zal waarborgen.

Wat **wifitracking** betreft, moet volgens de algemene verordening gegevensbescherming waarschijnlijk toestemming worden gevraagd voor de tracking of mag de tracking enkel worden uitgevoerd als de verzamelde gegevens anoniem worden gemaakt, afhankelijk van de omstandigheden en de doeleinden van gegevensverzameling. In het laatste geval moet aan de volgende vier voorwaarden zijn voldaan: het doel van de verzameling van gegevens uit eindapparatuur wordt beperkt tot louter statistisch tellen, het volgen is beperkt in tijd en ruimte tot hetgeen voor dit doeleinde strikt noodzakelijk is, onmiddellijk nadat het doeleinde is bereikt, worden de gegevens verwijderd of anoniem gemaakt, en er zijn daadwerkelijke opt-outmogelijkheden. De Europese Commissie wordt verzocht aan te sporen tot een

technische norm die ervoor zorgt dat mobiele apparaten automatisch een signaal geven wanneer de gebruiker niet akkoord gaat met een dergelijke tracking.

Wat de **analyse van inhoud en metagegevens** betreft, moet ervan worden uitgegaan dat geen communicatiegegevens mogen worden verwerkt als niet alle eindgebruikers (verzenders en ontvangers) hun toestemming hebben gegeven. Om aanbieders de mogelijkheid te geven diensten te verlenen die de gebruiker uitdrukkelijk heeft aangevraagd, zoals zoek- en indexeringsfuncties of tekst-naar-spraakdiensten, moet er een uitzondering voor huishoudelijk gebruik komen voor de verwerking van inhoud en metagegevens voor de zuiver persoonlijke doeleinden van de gebruiker zelf.

Wat **toestemming voor tracking** betreft, verzoekt de Groep de "tracking walls" uitdrukkelijk te verbieden. "Tracking walls" zijn alles-of-nietskeuzes die gebruikers dwingen toestemming te verlenen om getraceerd te worden als ze toegang tot de desbetreffende dienst willen.

Tot slot beveelt de Groep aan dat eindapparatuur en software **standaardinstellingen moeten aanbieden die de privacy beschermen** en de gebruikers duidelijke opties moeten bieden om deze standaardinstellingen tijdens de installatie te bevestigen of wijzigen. Deze instellingen moeten tijdens het gebruik gemakkelijk toegankelijk zijn. Gebruikers moeten via hun browserinstellingen hun specifieke toestemming kenbaar kunnen maken. Privacyvoorkeuren mogen niet worden beperkt tot interferentie door derden of tot cookies. De Groep beveelt sterk aan de naleving van de volg-me-nietnorm verplicht te stellen.

De Groep heeft ook nog andere punten van zorg vastgesteld, die betrekking hebben op bijvoorbeeld het toepassingsgebied, de bescherming van eindapparatuur en direct marketing. Tot slot heeft de Groep punten vastgesteld die moeten worden verduidelijkt om eindgebruikers beter te beschermen en meer rechtszekerheid te creëren voor alle betrokken belanghebbenden.

## INHOUDSOPGAVE

<b>1. INLEIDING .....</b>	<b>6</b>
<b>2. POSITIEVE ASPECTEN VAN DE VOORGESTELDE VERORDENING.....</b>	<b>6</b>
<i>EU-brede harmonisering, afstemming van boetes en exclusieve handhaving door gegevensbeschermingsautoriteiten .....</i>	
	<i>6</i>
<i>Uitbreiding van het toepassingsgebied ten opzichte van de e-privacyrichtlijn.....</i>	
	<i>8</i>
<i>Gerichte toepassing van het concept toestemming .....</i>	
	<i>11</i>
<b>3. ERNSTIGE PUNTEN VAN ZORG .....</b>	<b>11</b>
<i>De bescherming die de algemene verordening gegevensbescherming biedt, wordt door de voorgestelde verordening ondermijnd .....</i>	
	<i>11</i>
<b>4. ANDERE PUNTEN VAN ZORG .....</b>	<b>19</b>
<i>Het territoriale en materiële toepassingsgebied moet worden uitgebreid.....</i>	
	<i>19</i>
<i>Eindapparatuur moet beter worden beschermd.....</i>	
	<i>20</i>
<i>Direct marketing.....</i>	
	<i>24</i>
<i>Tijdschema.....</i>	
	<i>27</i>
<i>Andere punten van zorg .....</i>	
	<i>27</i>
<b>5. VOORSTELLEN VOOR VERDUIDELIJKING OM RECHTSZEKERHEID TE WAARBORGEN.....</b>	<b>31</b>
<i>Verduidelijking van het toepassingsgebied.....</i>	
	<i>31</i>
<i>Verduidelijkingen betreffende het begrip toestemming en de toepassing ervan .....</i>	
	<i>34</i>
<i>Verduidelijkingen betreffende locatie- en andere metagegevens.....</i>	
	<i>35</i>
<i>Verduidelijking met betrekking tot ongewenste communicatie .....</i>	
	<i>37</i>
<i>Verduidelijkingen betreffende de toepassing van grondrechteninstrumenten .....</i>	
	<i>38</i>
<i>Andere verduidelijkingen .....</i>	
	<i>39</i>

## 1. INLEIDING

1. De Groep gegevensbescherming artikel 29 (hierna "de Groep" of "WP29" genoemd) is verheugd over het voorstel van de Europese Commissie voor een e-privacyverordening (hierna "de voorgestelde verordening" of "e-privacyverordening" genoemd)<sup>1</sup>, die de e-privacyrichtlijn moet vervangen<sup>2</sup>.
2. De voorgestelde verordening is in veel opzichten positief en de Europese Commissie heeft hiermee een belangrijke stap gezet. Ze is echter nog voor verbetering vatbaar, niet alleen om de eindgebruikers beter te beschermen, maar ook om meer rechtszekerheid te creëren voor alle betrokken belanghebbenden.
3. De Groep heeft dan ook meerdere punten van zorg aangestipt en aanbevelingen voor verduidelijking geformuleerd, die het Europees Parlement en de Raad van ministers in overweging kunnen nemen wanneer ze de voorgestelde verordening bespreken. In dit advies zullen eerst de positieve aspecten van de voorgestelde verordening worden besproken, en daarna de punten van zorg en de punten die verduidelijking behoeven.

## 2. POSITIEVE ASPECTEN VAN DE VOORGESTELDE VERORDENING

*EU-BREDE HARMONISERING, AFSTEMMING VAN BOETES EN EXCLUSIEVE HANDHAVING DOOR GEGEVENSBSCHERMINGSAUTORITEITEN*

4. De Groep is verheugd dat als **regelgevend instrument een verordening is gekozen**, want een verordening zorgt voor uniforme regels in de gehele EU (op enkele uitzonderingen na, die hieronder worden besproken) en creëert duidelijkheid voor toezichthoudende autoriteiten en organisaties. Bovendien wordt door de belangrijke rol die de algemene verordening gegevensbescherming<sup>3</sup> in de voorgestelde verordening speelt, de samenhang tussen beide instrumenten verzekerd. **De keuze voor (het behoud van) een aanvullend rechtsinstrument** is tegelijk positief. De algemene verordening gegevensbescherming bevat immers geen bepalingen over de bescherming van vertrouwelijke communicatie en eindapparatuur. Door de bijzondere

<sup>1</sup> Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), 2017/0003 (COD), beschikbaar op: <http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017PC0010&qid=1510169587008&from=NL>.

<sup>2</sup> 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. 37-47), beschikbaar op: <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32002L0058>.

<sup>3</sup> Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PB L 119 van 4.5.2016, blz. 1-88, beschikbaar op: <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679>.

kenmerken van deze diensten zijn er aanvullende bepalingen nodig om een passende bescherming van dat grondrecht te verzekeren. In dat verband **ondersteunt de Groep ook de beginselen van brede verboden en enge uitzonderingen die in de voorgestelde verordening zijn toegepast** en is ze van mening dat de onbegrensde uitzonderingen die mogelijk worden gemaakt door artikel 6 van de algemene verordening gegevensbescherming, en met name artikel 6, lid 1, onder f), hiervan (om redenen van gerechtvaardigd belang), moeten worden vermeden.

5. De **handhaving van die regels door dezelfde autoriteit die verantwoordelijk is voor de controle van de naleving van de algemene verordening gegevensbescherming** zal de samenhang tussen de twee instrumenten versterken. Gezien het verband tussen de bescherming van persoonsgegevens en de bescherming van vertrouwelijke communicatie en eindapparatuur, is het nuttig dat de handhaving van de bepalingen van de voorgestelde verordening wordt toevertrouwd aan dezelfde toezichthoudende autoriteit die belast is met de handhaving van de algemene verordening gegevensbescherming (overweging 38 en art. 18 van de voorgestelde verordening). Daarnaast wordt in de rechtspraak van het Hof van Justitie van de Europese Unie (hierna "HvJ-EU" of "het Hof" genoemd)<sup>4</sup> bevestigd dat de toezichthoudende autoriteit onafhankelijk moet zijn, zoals is bepaald in artikel 7 van het Handvest. Praktisch gezien zou dit echter leiden tot een veel grotere werklast voor de gegevensbeschermingsautoriteiten en is er geen garantie dat de nodige taken worden uitgevoerd als er geen aanvullende financiële middelen worden toegekend. De gegevensbeschermingsautoriteiten zijn dan ook verheugd over overweging 38 van de voorgestelde verordening, waarin wordt benadrukt dat elke toezichthoudende autoriteit dient te beschikken over de bijkomende financiële en personele middelen, dienstruimten en infrastructuur die nodig zijn om haar taken uit hoofde van deze verordening doeltreffend uit te voeren. Het is ook een goede zaak dat in artikel 18, lid 2, de rechtsgrondslag wordt vastgesteld voor samenwerking tussen de toezichthoudende autoriteiten van de voorgestelde verordening en de nationale regelgevende autoriteiten van de voorgestelde richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie<sup>5</sup>.
6. Gezien het sterke verband tussen de voorgestelde verordening en de algemene verordening gegevensbescherming, is het ook positief dat **de boetes onder de voorgestelde verordening zijn afgestemd op die van de algemene verordening gegevensbescherming**. De activiteiten waarop de voorgestelde verordening van toepassing is, zijn best wel gevoelig omdat ze onder andere gepaard gaan met interferentie in vertrouwelijke communicatie en met eindapparatuur. De hoogte van de boetes moet evenredig zijn met die gevoelige context. De gevoeligheid van de context is ook de reden waarom harmonisering in de gehele EU belangrijk is. Op die manier wordt immers hetzelfde hoge niveau van bescherming in de gehele regio

---

<sup>4</sup> Zie bv. arrest van 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punt 41 en arrest van 21 december 2016, Tele2 Sverige, C-203/15 en C-698/15, EU:C:2016:970, punt 123.

<sup>5</sup> Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking), 2016/0288 (COD), 12.10.2016, beschikbaar op: [http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=comnat:COM_2016_0590_FIN).

gewaarborgd. In artikel 23 van de voorgestelde verordening worden doeltreffende boetes voor inbreuken op de verordening vastgesteld. De hoogte ervan ligt in de lijn van de boetes die zijn vastgesteld voor schending van de regels van de algemene verordening gegevensbescherming, uitgezonderd enkele punten (zie opmerking 38).

7. Een ander pluspunt is dat de voorgestelde verordening **geen specifieke regels meer bevat voor het melden van inbreuken in verband met persoonsgegevens**. Op die manier wordt immers een onnodige overlapping vermeden met de gegevensinbreukvereisten van de algemene verordening gegevensbescherming.
8. Het is ook **goed dat de nadruk nu ligt op het waarborgen van een gelijk beschermingsniveau voor alle eindgebruikers**. In de voorgestelde verordening wordt er immers geen onderscheid meer gemaakt tussen "abonnees" en andere gebruikers van elektronischecomunicatiediensten.

#### *UITBREIDING VAN HET TOEPASSINGSGEBIED TEN OPZICHTE VAN DE E-PRIVACYRICHTLIJN*

9. De Groep is blij dat **het toepassingsgebied van de voorgestelde verordening is uitgebreid en nu ook over-the-topcommunicatiediensten (hierna "OTT's" genoemd) omvat**. Dat zijn diensten die functioneel gelijkwaardig zijn aan de meer traditionele communicatiemiddelen en die bijgevolg een soortgelijk effect kunnen hebben op de privacy en het recht op geheimhouding van communicatie van EU-burgers. De Groep is in het bijzonder verheugd over het feit dat alle OTT-categorieën (OTT0, OTT1 en sommige OTT2's)<sup>6</sup> nu tot het toepassingsgebied van de verordening behoren, want de verordening heeft niet alleen betrekking op traditionele communicatiemiddelen (OTT0), maar ook functioneel gelijkwaardige diensten (OTT1), zoals vermeld in artikel 8, lid 1, onder c), van de voorgestelde verordening. Het is ook positief dat, naast de definities in het Europees wetboek voor elektronische communicatie, sommige OTT2's in het toepassingsgebied zijn opgenomen, met name wanneer dergelijke diensten als bijkomstig kenmerk persoonlijke en interactieve communicatie mogelijk maken die onlosmakelijk is verbonden met de dienst, zoals in spellen, dating-apps of beoordelingssites (art. 4, lid 2, van de voorgestelde verordening). Zo is het bovendien een goede zaak dat er wordt **verduidelijkt dat de bescherming ook geldt voor interactie tussen machines**. In overweging 12 wordt er duidelijk gesteld dat de bescherming uit hoofde van de voorgestelde verordening ook van toepassing is op apparaten die met elkaar communiceren. Dat is wenselijk, want dergelijke communicatie bevat vaak informatie die is beschermd door de regels inzake het recht op privacy. De toepasselijkheid moet echter worden verduidelijkt (zie opmerking 40h).

---

<sup>6</sup> Voor een verklaring van deze termen, zie BEREC, *Report on OTT Services*, BoR (16) 35, 29 januari 2016, blz. 15 en 16, beschikbaar op: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). Merk ook op dat er in het verslag op wordt gewezen dat de categorieën louter een hulp zijn voor het debat over de evaluatie en niet mogen worden opgevat als juridische begrippen.



10. Daarnaast is het positief dat de **voorgestelde verordening duidelijk betrekking heeft op inhoud en bijbehorende metagegevens**. In overweging 14 wordt duidelijk gesteld dat de definitie van "elektronischecomunicatiegegevens" in art. 4, lid 3, onder a), voldoende ruim is opgevat om te slaan op *alle* inhoud en de bijbehorende metagegevens, ongeacht hoe bijvoorbeeld de signalen worden overgebracht. De Groep merkt echter in opmerking 39 als punt van zorg op dat de huidige definitie van "elektronischecomunicatiegegevens" nog ter discussie staat. De Groep vindt dat, in lijn met de uitbreiding van het toepassingsgebied, **de erkenning dat via metagegevens ook zeer gevoelige gegevens aan het licht kunnen komen** (zie par. 2.2 van de toelichting en overweging 2) een belangrijke toevoeging. De Groep is verheugd over het feit dat de Europese Commissie hiermee de overwegingen van het Hof in de arresten *Digital Rights Ireland* en *Tele2 Sverige* in acht neemt. WP29 is ook blij met de **erkenning dat de analyse van inhoud een vorm van zeer risicovolle gegevensverwerking is**. In overweging 19 en art. 6, lid 3, onder b), wordt het logisch wettelijk vermoeden vastgesteld dat het scannen van inhoud een zeer risicovolle vorm van verwerking is op grond van artikel 35 van de algemene verordening gegevensbescherming en, blijkbaar ongeacht of er een hoog restrisico bestaat, altijd een voorafgaande raadpleging van de (leidende) gegevensbeschermingsautoriteit vereist. Tegelijk is de Groep bezorgd over de reikwijdte van de definitie van "metagegevens" en het feit dat de verplichte effectbeoordeling inzake gegevensbescherming niet geldt voor de analyse van metagegevens (zie opmerkingen 33 en 46).
11. Dat in de voorgestelde verordening opnieuw **het belang van het anoniem maken van gegevens wordt erkend**, moet ook worden toegejuicht. Anonimiseringsmaatregelen speelden in de e-privacyrichtlijn al een rol bij het waarborgen van de verenigbaarheid (zo wordt in art. 6, lid 1, van de e-privacyrichtlijn bepaald dat verkeersgegevens, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, moeten worden gewist of anoniem gemaakt). Op grond van art. 6, lid 2, onder c), en art. 6, lid 3, onder b), van de voorgestelde verordening is een uitzondering op het verbod op de verwerking van metagegevens en inhoud toegestaan, op voorwaarde dat de gebruikers toestemming hebben gegeven en de betrokken doeleinden "niet kunnen worden bereikt door verwerking van anoniem gemaakte gegevens". Door niet alleen de toestemming van de gebruikers, maar ook dergelijke privacybeschermende maatregelen te eisen, worden deze gebruikers beschermd tegen ongewettigde verwerking. De Groep is tegelijk echter ernstig bezorgd dat dergelijke anonimiseringstechnieken niet zouden hoeven te worden toegepast wanneer de locatie van gebruikers wordt getraceerd aan de hand van hun mobiele apparatuur (zie opmerking 17). En zelfs wanneer anonimiseringsmaatregelen moeten worden toegepast, moeten aanbieders altijd een gegevensbeschermingseffectbeoordeling uitvoeren (zie opmerkingen 33 en 46). Tot slot verzoekt de Groep een aanvullende verplichting in te stellen om de manier waarop gegevens anoniem worden gemaakt en geaggregeerd bekend te maken (zie opmerking 42b).
12. Nog een positief punt is de **brede formulering van de bescherming van eindapparatuur**. In overweging 20 en art. 8 is vastgesteld dat het niet uitmaakt met welke technologieën toegang tot de eindapparatuur wordt verkregen: voor elke

interferentie met de eindapparatuur, met inbegrip van het gebruik van de verwerkingscapaciteit van het apparaat, is de toestemming van de eindgebruiker vereist (er zijn wel enkele uitzonderingen). De Europese Commissie heeft nu gelukkig verduidelijkt dat "vingerafdrukkeuze" onder deze bepaling valt. Daarnaast is de Groep blij dat de eerbiediging van de voorkeuren die een persoon kenbaar maakt in zijn **browserinstellingen ten aanzien van derden kunnen worden afgedwongen**, zoals beschreven in overweging 22. Dat is nuttig in situaties waarin een derde (bv. een reclamenetwerk) geen rekening houdt met die instellingen. Er moet in de voorgestelde verordening echter ook een bepaling worden opgenomen die deze afdwingbaarheid vaststelt.

13. Tot slot moet worden toegevoegd dat **in het toepassingsgebied van de voorgestelde verordening weer rechtspersonen zijn opgenomen** (zie par. 2.2 van de toelichting, overwegingen 3, 33 en 42, artikelen 1 en 15 en artikel 16, lid 5). Dat is al het geval onder de e-privacyrichtlijn, maar aangezien de gegevensbeschermingsautoriteiten ook zullen worden belast met de handhaving van de nieuwe regels, is het nuttig dat specifiek te benadrukken. Op die manier kunnen gegevensbeschermingsautoriteiten optreden wanneer rechtspersonen het slachtoffer zijn van een inbreuk, bijvoorbeeld wanneer ondernemingen spam ontvangen of wanneer hun communicatie heimelijk wordt gemonitord. De Groep merkt echter als punt van zorg op dat het niet duidelijk is hoe rechtspersonen hun toestemming moeten geven (zie opmerking 41a) en evenmin wat er wordt bedoeld met "het rechtmatig belang" van rechtspersonen in het geval van direct marketing (zie opmerking 43c).

14. De Groep is tevreden met nog een andere categorie van verbeteringen, met name met betrekking tot de toepassing en uitlegging van het begrip toestemming. Ten eerste is het een goede zaak dat er **wordt verduidelijkt dat internettoegang en (mobiele) telefonie essentiële diensten zijn en dat de aanbieders van deze diensten hun klanten niet kunnen "dwingen" om toestemming te verlenen voor de verwerking van gegevens die niet nodig zijn voor de verlening van de essentiële dienst zelf**. In met name overweging 18 wordt opgemerkt dat basistoegang tot breedbandinternet en spraakcommunicatiediensten moeten worden beschouwd als essentiële diensten. Bijgevolg kan, gezien de afhankelijkheid van personen om toegang tot deze diensten te krijgen, de toestemming voor de verwerking van hun communicatiegegevens voor aanvullende doeleinden (bv. verwerking voor reclame- of marketingdoeleinden) niet geldig zijn. De Groep is tegelijk bezorgd dat deze verduidelijking niet ver genoeg gaat. Diensten van bepaalde aanbieders van OTT-diensten kunnen ook worden beschouwd als essentiële diensten, en de e-privacyverordening moet ook alles-of-nietskeuzes in andere omstandigheden specifiek verbieden (zie opmerking 20).
15. Daarnaast is het positief dat de **vereiste toestemming voor opname van persoonsgegevens van natuurlijke personen in telefoongidsen is geharmoniseerd**. Op grond van art. 15 van de voorgestelde verordening is de verwerking van gegevens in algemeen beschikbare telefoongidsen slechts toegestaan met toestemming van natuurlijke personen en hebben rechtspersonen de mogelijkheid om bezwaar te maken. Dat wordt verder uitgewerkt in overweging 31, waarin is bepaald dat deze toestemming specifiek moet worden verleend voor specifieke categorieën in het repertorium op te nemen persoonsgegevens. De Groep merkt echter als punt van zorg op dat de voorgestelde verordening onvoldoende duidelijk is over het feit dat een afzonderlijke toestemming zal zijn vereist voor zoek- en omgekeerde zoekfuncties (zie opmerking 37).
16. **De nieuw gerichte uitzondering voor interferentie met eindapparatuur waarbij de privacy niet wordt aangetast** wordt ook positief onthaald. WP29 vindt het nuttig dat de voorgestelde verordening verduidelijkt dat het verbod niet van toepassing is op het meten van het bezoekersverkeer op een website (met als welomschreven uitzondering dat deze meting door de aanbieder van de door de eindgebruiker aangevraagde dienst van de informatiemaatschappij wordt verricht, zie art. 8, lid 1, onder d), van de voorgestelde verordening). Zie ook overweging 21. De Groep stelt echter voor een meer technologieneutrale definitie te gebruiken en de toepasselijkheid van deze uitzondering te verduidelijken (zie opmerking 25).

### 3. ERNSTIGE PUNTEN VAN ZORG

*DE BESCHERMING DIE DE ALGEMENE VERORDENING GEGEVENSBESCHERMING BIEDT, WORDT DOOR DE VOORGESTELDE VERORDENING ONDERMIJND*

Zoals hierboven uitgelegd, bevat de voorgestelde verordening enkele belangrijke verbeteringen. Er zijn echter ook punten van zorg, het ene al ernstiger dan het andere. In dit hoofdstuk bespreekt de Groep de vier punten waarover **zij zeer bezorgd** is. Deze

punten betreffen **bepalingen die het niveau van bescherming dat door de algemene verordening gegevensbescherming is gewaarborgd, ondermijnen.**

17. **De verplichtingen in de verordening met betrekking tot het traceren van de locatie van eindapparatuur moeten in overeenstemming zijn met de vereisten in de algemene verordening gegevensbescherming.** Op grond van art. 8, lid 2, onder b), hoeft slechts een bericht te worden aangebracht en beveiligingsmaatregelen te worden genomen voor de verzameling van gegevens uit de eindapparatuur. Voorts wordt in art. 8, lid 2, onder b), opgemerkt dat de persoon die verantwoordelijk is voor de verzameling van de gegevens de maatregelen moet vermelden die de eindgebruikers kunnen nemen om het verzamelen van gegevens te beperken of te beëindigen. Art. 8, lid 2, onder b), geeft hierdoor de indruk dat organisaties gegevens uit eindapparatuur mogen verzamelen om de fysieke bewegingen van personen te traceren (zoals wifitracking of bluetoothtracking) zonder toestemming van de betrokkene. De partij die de gegevens verzamelt, zou blijkbaar aan de regels kunnen voldoen door een bericht te laten verschijnen waarin de gebruikers wordt gevraagd hun apparatuur uit te schakelen als ze niet getraceerd willen worden. Een dergelijke benadering zou in strijd zijn met de basisdoelstelling van het telecommunicatiebeleid van de Europese Commissie, met name het verstrekken van grensoverschrijdende mobiele hogesnelheidsinternetverbindingen met een hoge bescherming van de privacy tegen lage kosten voor alle Europeanen.

Daarnaast bevat de voorgestelde verordening geen duidelijke beperking met betrekking tot het toepassingsgebied van de gegevensverzameling of de daarop volgende verwerkingsactiviteiten. In die context moet worden opgemerkt dat MAC-adressen persoonsgegevens zijn, zelfs na het nemen van beveiligingsmaatregelen zoals hashing. Aangezien er geen verdere vereisten of beperkingen worden opgelegd, is het niveau van bescherming van deze persoonsgegevens op grond van de voorgestelde verordening aanzienlijk lager dan op grond van de algemene verordening gegevensbescherming, waarin is bepaald dat deze vorm van traceren behoorlijk, rechtmatig en transparant dient te geschieden. In overweging 25 wordt ook gezegd dat sommige van de wifitrackingfuncties geen hoge risico's voor de persoonlijke levenssfeer inhouden, terwijl andere – die bijvoorbeeld personen in de tijd traceren – dat wel doen. Dat is een nutteloze opmerking. De Groep is wel tevreden met de erkenning dat de laatste categorie functies hoge risico's voor de persoonlijke levenssfeer inhouden, maar vindt het nutteloos en voorbarig om te beslissen dat bepaalde andere functies geen risico's inhouden, zonder een beoordeling van de omstandigheden en de evenredigheid van de verwerking. Een dergelijke beoordeling moet worden uitgevoerd met inachtneming van de volgende voorwaarden betreffende niet-geanonimiseerde wifitracking.

Afhankelijk van de omstandigheden en het doeleinde van de gegevensverzameling, moet voor het traceren op grond van de algemene verordening gegevensbescherming toestemming worden verkregen of mag slechts worden getraceerd als de verzamelde persoonsgegevens anoniem worden gemaakt, bij voorkeur onmiddellijk na de verzameling. Als de gegevens niet onmiddellijk anoniem kunnen worden gemaakt in het licht van het doeleinde waarvoor de gegevens zijn verzameld, mogen deze gegevens slechts gedurende een bepaalde periode in niet-anonieme vorm worden verwerkt als aan de volgende voorwaarden is voldaan: i) het doeleinde van de gegevensverwerking moet zijn beperkt tot louter statistisch tellen (zie de voorbeelden hieronder), ii) het volgen is beperkt in tijd en ruimte tot hetgeen voor dit doeleinde

strikt noodzakelijk is, iii) onmiddellijk nadat het doeleinde is bereikt, worden de gegevens verwijderd of anoniem gemaakt, en iv) er zijn daadwerkelijke opt-outmogelijkheden. De verwerkingsverantwoordelijke moet uiteraard in alle omstandigheden voldoen aan de vereiste inzake het verstrekken van passende informatie.

De Groep is bezorgd dat als elke organisatie die dergelijke gegevens verzamelt een eigen opt-outmogelijkheid biedt aan gebruikers, de burgers met een onaanvaardbare last zullen worden geconfronteerd omdat het gebruik van dergelijke tracerings technologieën door zowel privé- als overheidsorganisaties toeneemt. De Groep roept dan ook de Europese wetgever op om de ontwikkeling van technische normen te bevorderen die ervoor zorgen dat apparaten automatisch een signaal geven wanneer de gebruiker bezwaar maakt tegen een dergelijke tracering, en ervoor te zorgen dat het eerbiedigen van een dergelijk signaal afdwingbaar is.

Toestemming op grond van de algemene verordening gegevensbescherming is bijvoorbeeld wellicht nodig wanneer een verwerkingsverantwoordelijke (via wifi of bluetooth) de indirect identificeerbare MAC-adressen van apparaten verzamelt en opslaat en de locatie van de gebruiker berekent om de locatie van de gebruiker in de loop van de tijd, bijvoorbeeld wanneer hij meerdere winkels bezoekt, te traceren. Een dergelijke toestemming is voornamelijk vereist wanneer de tracering plaatsvindt op openbare plaatsen waar MAC-adressen van voorbijgangers worden verzameld, omdat gebruikers een gerechtvaardigde verwachting hebben dat ze nog niet worden geïdentificeerd of getraceerd. De toestemming van de gebruikers kan worden verkregen via bijvoorbeeld een app die gebruikers uitnodigt de tracering van hun locatie in specifieke zones toe te laten in ruil voor commerciële aanbiedingen, via check-inpunten op bepaalde locaties of via een toestemmingsmodule in wifihotspots.

Slechts in een beperkt aantal omstandigheden mogen verwerkingsverantwoordelijken zonder de toestemming van de betrokkene gegevens uit eindapparatuur verwerken om de fysieke bewegingen van de betrokkene te traceren. Voorbeelden van dergelijke omstandigheden zijn het tellen van het aantal klanten op een bepaalde locatie of het verzamelen van gegevens van eindapparatuur aan beide zijden van een controlepost om de wachttijd weer te geven. In beide voorbeelden moeten de gegevens echter onmiddellijk na het verwezenlijken van het statistische doeleinde worden verwijderd of anoniem worden gemaakt. Dat impliceert dat de MAC-adressen van de apparatuur van de bezoekers op een specifieke locatie, zoals in een winkel, onmiddellijk na de verzameling ervan anoniem moeten worden gemaakt en dat ze niet permanent mogen worden opgeslagen. Hierbij moet in elk geval worden gewaarborgd dat het later technisch onmogelijk is de bezoekers opnieuw te identificeren. In het geval van de berekening van de wachttijd, moeten de MAC-adressen worden verwijderd of anoniem worden gemaakt zodra de gegevens niet meer relevant zijn voor de berekening van de wachttijd (bijvoorbeeld omdat de bezoeker zich aan de andere kant van de controlepost bevindt of de wachtrij heeft verlaten).

Daarnaast moet de verwerkingsverantwoordelijke voldoen aan de vereisten betreffende minimale gegevensverwerking (bijvoorbeeld niet 24 uur per dag traceren wanneer het doeleinde is beperkt tot de openingstijden van de winkel en/of tot het nemen van steekproeven met tussenpozen). Verwerkingsverantwoordelijken moeten

ook andere verzachtende maatregelen nemen om te waarborgen dat het effect op de privacyrechten van gebruikers heel klein of onbestaande is en om bijvoorbeeld de privacy van de mensen die in de buurt van een verzamelpunt wonen te beschermen.

De keuze in art. 8, lid 2, van de voorgestelde verordening voor het louter aanbrengen van een bericht is des te opvallender omdat in overweging 20 is geconcludeerd dat informatie met betrekking tot de uitrusting van de eindgebruiker ook op afstand kan worden verzameld met het oog op identificatie en traceeractiviteit, en dat een dergelijke verwerking – volgens de voorgestelde verordening – kan leiden tot ernstige inbreuken op de persoonlijke levenssfeer van deze eindgebruikers. Bovendien reikt deze verplichting niet verder dan de informatieverplichting die al is opgenomen in artikelen 13 en 14 van de algemene verordening gegevensbescherming. De "ernstige inbreuk op de persoonlijke levenssfeer" door de tracering wordt nog versterkt door de mogelijke toegang door anderen tot de verzamelde gegevens, zoals de mogelijkheid voor wetshandhavingsdiensten om eindgebruikers te identificeren op basis van de opgeslagen MAC-adressen die door hun mobiele apparatuur worden uitgezonden.

#### **18. De voorwaarden voor het analyseren van inhoud en metagegevens moeten worden uitgewerkt**

In artikel 6 van de voorgestelde verordening worden verschillende niveaus van bescherming vastgesteld voor metagegevens en inhoud. WP29 gaat hiermee niet akkoord, omdat beide categorieën zeer gevoelige gegevens betreffen. Aan metagegevens en inhoud moet bijgevolg hetzelfde hoge niveau van bescherming worden toegekend. Het uitgangspunt moet dus zijn dat het verboden is zowel metagegevens als inhoud te verwerken zonder de toestemming van alle eindgebruikers (d.w.z. zender en ontvanger).

Afhankelijk van de doeleinden mogen bepaalde vormen van verwerking wel zonder toestemming worden uitgevoerd, indien dit strikt noodzakelijk is voor die doeleinden:

- Aanbieders mogen voor de in artikel 6, lid 1, onder a) en b), en artikel 6, lid 2, onder a) en b), van de voorgestelde verordening vermelde doeleinden elektronischecomunicatiegegevens verwerken<sup>7</sup>.
- Er moet worden verduidelijkt dat bepaalde technieken voor het opsporen en filteren van spam en het remmen van botnets ook kunnen worden beschouwd als strikt noodzakelijk voor de opsporing of de beëindiging van frauduleus of onrechtmatig gebruik van elektronischecomunicatiediensten (art. 6, lid 2, onder b)). Eindgebruikers die spam ontvangen, moeten gedetailleerde opt-outmogelijkheden hebben indien dit technisch mogelijk is.

---

<sup>7</sup> Voor de noodzaak te voldoen aan dwingende eisen inzake kwaliteit van de dienstverlening, zoals beschreven in artikel 6, lid 2, onder a), van de voorgestelde verordening, moeten de aanbieders rekening houden met de voorwaarden die zijn beschreven in Verordening (EU) 2015/2120, met name in artikel 3 en overwegingen 10 en 13 tot en met 15. Aanbieders kunnen op basis van deze bepaling verplicht zijn om communicatiegegevens te verwerken om malware en spyware op te sporen en te filteren, en hebben de mogelijkheid tot gegevenscompressie.

- Er moet worden verduidelijkt dat de analyse van elektronischecommunicatiegegevens met het oog op de dienstverlening aan klanten ook kan vallen onder de uitzondering van "noodzakelijk ten behoeve van de facturering" (art. 6, lid 2, onder b)). De desbetreffende metagegevens kunnen worden bewaard tot het einde van de termijn waarbinnen de rekening in rechte kan worden bestreden of de betaling overeenkomstig de nationale wetgeving kan worden gevorderd. De desbetreffende gegevens (zoals internetadressen) mogen uitsluitend worden bewaard op verzoek van de eindgebruiker, en ook slechts gedurende de periode die strikt noodzakelijk is om een geschil over een rekening op te lossen (wat dus impliceert dat art. 7, lid 3, moet worden gewijzigd).
- Elektronischecommunicatiegegevens moeten kunnen worden verwerkt met het oog op de verlening van diensten die een eindgebruiker uitdrukkelijk heeft aangevraagd, zoals zoekfuncties en functies voor indexerings op basis van sleutelwoorden, virtuele ondersteuning en tekst-naar-spraakfuncties en vertaaldiensten. Dat vereist dat een uitzondering wordt ingevoerd voor de analyse van dergelijke gegevens voor zuiver individueel (huishoudelijk) gebruik en voor individueel werkgerelateerd gebruik<sup>8</sup>. Op die manier hoeven niet alle eindgebruikers hun toestemming te verlenen, maar is wel nog de toestemming nodig van de eindgebruiker die de dienst aanvraagt. Door een dergelijke specifieke toestemming wordt ook voorkomen dat de aanbieder deze gegevens gebruikt voor andere doeleinden.

Dat impliceert dat er voor de analyse van inhoud en/of metagegevens voor alle andere doeleinden, zoals analyses, profilering, reclame maken op basis van surfgedrag of andere doeleinden die de aanbieder (commerciële) voordelen brengen, toestemming is vereist van alle eindgebruikers van wie de gegevens zouden worden verwerkt. Voor deze situaties moet in de voorgestelde verordening worden uitgelegd dat het louter verzenden van een e-mail of een andere vorm van persoonlijke communicatie van een andere dienst aan een eindgebruiker die persoonlijk zijn toestemming heeft gegeven voor de verwerking van zijn of haar inhoud en metagegevens (bijvoorbeeld bij het abonneren op een e-maillidienst), niet impliceert dat de verzender op een geldige wijze zijn toestemming heeft gegeven.

Tot slot moet worden verduidelijkt dat de verwerking van gegevens van andere betrokken personen dan de eindgebruikers (bv. de foto of beschrijving van een derde persoon bij een uitwisseling tussen twee personen) ook moet voldoen aan alle desbetreffende bepalingen van de algemene verordening gegevensbescherming.

## 19. Eindapparatuur en software moeten *standaard zo zijn ingesteld dat ze onwettige interferentie ontmoedigen, voorkomen en verbieden en informatie verstrekken*

---

<sup>8</sup> Hoewel volgens overweging 13 van de voorgestelde verordening bedrijfsnetwerken uitdrukkelijk van het toepassingsgebied van de verordening zijn uitgesloten, kan deze nieuwe uitzondering voor individueel gebruik ook worden toegepast op het gebruik van clouddiensten door werknemers voor werkgerelateerd gebruik, zoals het zoeken in e-mails.



**over de opties** Hoewel softwareaanbieders die elektronische communicatie mogelijk maken op grond van de voorgestelde verordening "de optie moeten bieden" om een beperkte vorm van interferentie met eindapparatuur te voorkomen en zij verplicht zijn de eindgebruiker bij de installatie te vragen een instelling te aanvaarden (artikel 10, leden 1 en 2), staat dit niet gelijk aan de "bescherming van de privacy door standaardinstellingen". Bovendien bestaat momenteel de "optie" om een bepaalde vorm van interferentie te voorkomen al en heeft dit nog niet geleid tot een toereikende oplossing voor ongewenste tractering. Om deze reden werd in de algemene verordening gegevensbescherming de bewuste beleidskeuze gemaakt om de beginselen van gegevensbescherming en privacy door ontwerp en door standaardinstellingen in te voeren (art. 25 van de algemene verordening gegevensbescherming). De voorgestelde verordening ondermijnt deze beginselen voor communicatie- en apparaatgegevens. In de richtlijn radioapparatuur (Richtlijn 2014/53/EU)<sup>9</sup> (waarvan sprake is in overweging 10) is intussen slechts een zeer beperkte beveiligingsverplichting opgenomen, met name door te vereisen dat radioapparatuur "beveiligingen [bevat] om de bescherming van de persoonsgegevens en de privacy van de gebruiker en de abonnee te waarborgen" (art. 3, lid 3, onder e)). Deze bepaling is geen vervanging voor specifieke bepalingen op het gebied van privacy door standaardinstellingen in het kader van de voorgestelde verordening. In dat verband moet ook worden opgemerkt dat in het Eurobarometeronderzoek over e-privacy dat in december 2016 is bekendgemaakt, wordt opgemerkt dat bijna zeven op de tien ondervraagden (69 %) het er volledig mee eens zijn dat hun browser standaard zo moet worden ingesteld dat hun informatie niet meer wordt gedeeld<sup>10</sup>. Voor de Groep zijn browserinstellingen en de definitie van "derden" een afzonderlijk punt van zorg. Zie opmerking 24. Bovendien mag niet worden vergeten dat die bepaling niet alleen betrekking heeft op browsers op computers, maar ook op andere soorten software die communicatie mogelijk maken (waaronder besturingssystemen, apps en software-interfaces voor apparaten die zijn aangesloten op het internet van dingen). Samengevat moeten eindapparatuur en software standaard instellingen bieden die de privacy beschermen en gebruikers bij de installatie door configuratiemenu's leiden zodat ze van deze standaardinstellingen kunnen afwijken. Die configuratiemenu's moeten tijdens het gebruik altijd gemakkelijk toegankelijk zijn. De Groep moedigt de Europese wetgevers aan op basis hiervan het toepassingsgebied van artikel 10 te verduidelijken.

20. **De e-privacyverordening moet tracking walls uitdrukkelijk verbieden.** "Tracking walls" zijn een praktijk waarbij de toegang tot een dienst wordt geweigerd indien de betrokkene niet akkoord gaat om te worden getraceerd op andere websites of bij andere diensten. Zoals de Groep reeds heeft opgemerkt in eerdere adviezen over de e-privacyrichtlijn<sup>11</sup>, zijn dergelijke "alles-of-niets"-benaderingen zelden gewettigd<sup>12</sup>.

<sup>9</sup> Richtlijn radioapparatuur (Richtlijn 2014/53/EU).

<sup>10</sup> Zie Flash Eurobarometer 443, *Report e-Privacy* (bekendgemaakt in december 2016), blz. 5.

<sup>11</sup> Zie bv. WP 240 (evaluatie e-privacy), blz. 16; WP 208 (uitzondering voor toestemming), blz. 5.

<sup>12</sup> Dat standpunt doet geen afbreuk aan artikel 7, lid 4, van de algemene verordening gegevensbescherming, op grond waarvan in andere situaties ook, indien nodig, "alles-of-niets"-keuzes kunnen worden uitgesloten.

Wanneer door het gebruik van verwerkings- en opslagcapaciteit van eindapparatuur en het verzamelen van gegevens uit eindapparatuur van eindgebruikers de activiteiten van de gebruiker in de loop van de tijd of over verschillende diensten heen (bv. verschillende websites of apps) kunnen worden getraceerd, kunnen dergelijke verwerkingsactiviteiten leiden tot ernstige inbreuken op de persoonlijke levenssfeer van deze eindgebruikers. Gezien het feit dat internet fundamenteel belangrijk is voor het uitoefenen van het grondrecht van vrijheid van meningsuiting, met inbegrip van het recht op toegang tot informatie, mag de mogelijkheid van personen om online inhoud te raadplegen niet afhankelijk worden gemaakt van het aanvaarden van het traceren van zijn of haar activiteiten op verschillende apparaten en via verschillende websites/apps. In de toekomstige e-privacyverordening moet bijgevolg worden verduidelijkt dat toegang tot inhoud op bijvoorbeeld websites en apps niet voorwaardelijk mag worden gemaakt aan de aanvaarding van dergelijke verwerkingsactiviteiten die de privacy aantasten, ongeacht welke traceringstechnologie er wordt gebruikt (cookies, vingerafdruklezing, gebruik van unieke identificatoren of andere controletechnieken). Dat een dergelijke verplichting noodzakelijk is, blijkt duidelijk uit het recente Eurobarometeronderzoek over e-privacy, waarin wordt opgemerkt dat bijna twee derde van de ondervraagden (64 %) zegt dat het onaanvaardbaar is dat hun onlineactiviteiten worden gecontroleerd in ruil voor een onbeperkte toegang tot een bepaalde website.

21. Op basis van de vier bovenvermelde punten kan samenvattend worden gesteld dat ervoor moet worden gezorgd dat **de voorgestelde verordening een minstens even hoog niveau van bescherming biedt als de algemene verordening gegevensbescherming**. Die belofte is trouwens opgenomen in overweging 5, waarin wordt opgemerkt dat de voorgestelde verordening niet leidt tot een lager niveau van bescherming dan in de algemene verordening gegevensbescherming. De voorgestelde verordening voldoet in haar huidige formulering echter hier niet aan, met name voor wat het traceren van apparatuur (opmerking 17), het ontbrekende beginsel van privacy door standaardinstellingen (opmerking 19) en toestemming (opmerking 18) betreft. Dat is met name van belang omdat in dezelfde overweging wordt opgemerkt dat de voorgestelde verordening "een *lex specialis* bij de algemene verordening gegevensbescherming [zal zijn] en zal voorzien in de nadere omschrijving en de aanvulling daarvan voor elektronischecommunicatiegegevens die als persoonsgegevens worden aangemerkt". De Groep stelt voor dat in de e-privacyverordening ten minste wordt verduidelijkt dat:

- i) de verboden in de e-privacyverordening voorrang krijgen op de toelatingen in de algemene verordening gegevensbescherming (dat bv. het verbod op interferentie op grond van art. 5 in de e-privacyverordening voorrang krijgt op de rechten van aanbieders van elektronischecommunicatiediensten om persoonsgegevens verder te verwerken op grond van art. 5, lid 1, onder b), en art. 6, lid 4, van de algemene verordening gegevensbescherming);
- ii) wanneer verwerking is toegestaan op grond van een uitzondering (met inbegrip van toestemming) op de verboden in de e-privacyverordening, deze verwerking, indien ze persoonsgegevens betreft, nog steeds moet voldoen aan alle desbetreffende bepalingen in de algemene verordening gegevensbescherming;

iii) wanneer verwerking is toegestaan op grond van een uitzondering op de verboden in de e-privacyverordening, andere verwerking op grond van de algemene verordening gegevensbescherming is verboden, met inbegrip van verwerking voor een ander doel op grond van art. 6, lid 4, van de algemene verordening gegevensbescherming. Verwerkingsverantwoordelijken kunnen nog steeds een aparte toestemming vragen voor nieuwe verwerkingsactiviteiten. Ook behouden de wetgevers de mogelijkheid om aanvullende, beperkte en specifieke uitzonderingen op de e-privacyverordening vast te stellen om bijvoorbeeld de verwerking voor wetenschappelijke of statistische doeleinden op grond van art. 89 van de algemene verordening gegevensbescherming mogelijk te maken of om de "vitale belangen" van de personen overeenkomstig art. 6, lid 1, onder d), van de algemene verordening gegevensbescherming te beschermen.

Bovendien moet de e-privacyverordening zo worden uitgelegd dat ze ten minste hetzelfde en indien van toepassing een hoger niveau van bescherming biedt dan de algemene verordening gegevensbescherming.

#### **4. ANDERE PUNTEN VAN ZORG**

In verband met de hierboven genoemde punten is Groep artikel 29 **bezorgd** over de volgende punten.

#### *HET TERRITORIALE EN MATERIËLE TOEPASSINGSGEBIED MOET WORDEN UITGEBREID*

22. **De term "metagegevens" is te eng omschreven.** Metagegevens worden nu in art. 4, lid 3, onder c), omschreven als "gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, distributie of de uitwisseling van inhoud van elektronische communicatie" (nadruk toegevoegd). Het gebruik van het woord "netwerk" lijkt te suggereren dat alleen gegevens die bij de verlening van diensten in de "onderste" laag van het netwerk worden gegenereerd, zouden worden aangemerkt als "metagegevens". Bijgevolg zouden gegevens die bij de verlening van OTT-diensten worden gegenereerd, niet onder "metagegevens" vallen. Dat zou ongewenst zijn, en is wellicht niet de bedoeling aangezien de voorgestelde verordening ertoe strekt het toepassingsgebied uit te breiden naar OTT-dienstverleners. De Groep stelt dan ook voor om de definitie van "elektronischecommunicatiemetagegevens" zo te wijzigen dat alle gegevens die worden verwerkt met het oog op de transmissie, distributie of uitwisseling van inhoud van elektronische communicatie eronder vallen.

23. Het is ook een punt van zorg dat het **territoriale toepassingsgebied van de voorgestelde verordening met betrekking tot organisaties die geen vestiging in de EU hebben, slechts de aanbieders van elektronischecommunicatiediensten omvat**. Volgens de voorgestelde verordening wijst de aanbieder van een elektronischecommunicatiedienst die niet in de Unie is gevestigd, schriftelijk een vertegenwoordiger in de Unie aan (art. 3, lid 2). In overweging 9 wordt ook gezegd dat de verordening van toepassing moet zijn op verwerking door aanbieders van elektronischecommunicatiediensten, ongeacht waar de verwerking plaatsvindt. De

Groep is blij met deze verduidelijking. Aangezien er echter uitsluitend wordt gesproken over aanbieders van elektronische communicatiediensten, is het niet zeker in welke mate dat territoriaal toepassingsgebied van toepassing is op andere soorten derden (bijvoorbeeld partijen die interfereren met gegevens uit eindapparatuur van eindgebruikers of deze verzamelen, zie art. 3, lid 1, onder c), samen te lezen met art. 8 van de voorgestelde verordening). Bijgevolg stelt de Groep voor om art. 3, leden 2 en 5, zo te wijzigen dat ook aanbieders van algemeen beschikbare telefoongidsen, aanbieders van software voor elektronische communicatie en personen die commerciële boodschappen van direct marketing verzenden of (andere) informatie verzamelen die verbonden is aan of opgeslagen is in eindapparatuur van eindgebruikers op te nemen in het territoriale toepassingsgebied wanneer hun activiteiten gericht zijn op gebruikers in de EU (zie overweging 8 van de voorgestelde verordening)<sup>13</sup>.

#### *EINDAPPARATUUR MOET BETER WORDEN BESCHERMD*

Een ander punt van zorg heeft betrekking op de ontoereikende bescherming van eindapparatuur in de voorgestelde verordening.

24. Ten eerste **wordt er in de voorgestelde verordening ten onrechte gesuggereerd dat een geldige toestemming kan worden verleend via niet-specifieke browserinstellingen**. De Groep erkent de overweging dat eindgebruikers momenteel te maken hebben met een overvloed aan verzoeken om toestemming te geven (overweging 22). Browserinstellingen (en vergelijkbare software-instellingen) kunnen dit probleem verhelpen. Aangezien algemene browserinstellingen echter niet zijn bedoeld om in afzonderlijke gevallen te worden geconfigureerd op basis van de gebruikte tracerings technologie, zijn ze niet geschikt om op grond van artikel 7 en overweging 32 van de algemene verordening gegevensbescherming toestemming te verlenen (omdat de toestemming niet geïnformeerd en specifiek genoeg is).

De eindgebruiker moet per website of app afzonderlijk toestemming kunnen geven voor de tracering voor verschillende doeleinden (zoals het delen of reclame maken via sociale media). Een verwerkingsverantwoordelijke die belast is met meerdere websites of apps mag ook toestemming vragen voor alle andere websites of apps die hij beheert, op voorwaarde dat hij deze toestemming voor elke afzonderlijke website of app vraagt.

Daarnaast moet de verwerkingsverantwoordelijke voldoen aan alle andere verplichtingen met betrekking tot toestemming, met inbegrip van de verplichting om gebruikers passende informatie te verstrekken. Het volstaat bijgevolg niet dat browsers en verwerkingsverantwoordelijken een optie "aanvaarden van alle cookies"

---

<sup>13</sup> Zie artikel 3, lid 2, van de algemene verordening gegevensbescherming: *Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met: a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt. Deze verplichting kan ook uitzonderingen omvatten die zijn vastgesteld in art. 27, lid 2, van de algemene verordening gegevensbescherming.*

aanbieden, aangezien de gebruikers op die manier niet de vereiste gedetailleerde toestemming kunnen geven. Browsers moeten echter wel gebruikers de mogelijkheid kunnen geven om geïnformeerd en bewust ervoor te kiezen alle cookies te aanvaarden, zodat ze geen afzonderlijke toestemmingen meer moeten geven voor andere websites die ze raadplegen.

De Groep beveelt sterk aan dat in de e-privacyverordening de verplichting wordt opgenomen voor browsers om technische mechanismen op te nemen zoals de volg-me-nietnorm, om ervoor te zorgen dat gebruikers echt kunnen beslissen over de inferentie met hun apparatuur en deze kunnen beheren<sup>14</sup>.

Het is zelfs des te belangrijker dat de e-privacyverordening ervoor zorgt dat zowel de keuze met betrekking tot de opslag van informatie in het apparaat als een volg-me-nietsignaal van de browser worden aanvaard als een wettelijk bindende aanwijzing van toestemming of weigering door alle verwerkingsverantwoordelijken. Dat doet geen afbreuk aan de richtsnoeren die de Groep zal uitvaardigen met betrekking tot de naleving van de volg-me-nietnorm, met onder andere het beginsel inzake doelbinding, wanneer de norm zal zijn voltooid (gepland voor einde 2017).

Impliciete vormen van "toestemming", zoals het klikken of scrollen op de website, zijn ondergeschikt aan keuzes met betrekking tot opslag en het volg-me-nietsignaal. Een belangrijk voordeel van het gebruik van deze norm is dat ze niet is beperkt tot de traceertechnologie van cookies, maar ook betrekking heeft op andere vormen van tracering, zoals vingerafdrukkezing.

Door de naleving van deze norm wettelijk bindend te maken, wordt ook een ander probleem opgelost in verband met het huidige gebruik in artikel 10 van de term "derden". Een website of app bestaat in het algemeen uit meerdere elementen, die zowel van de website of app zelf afkomstig zijn, als een externe oorsprong hebben. Er kan ook een externe code lopen in de back-end van de geraadpleegde website, die gegevens doorstuurt naar de server van een derde. Een eerste partij kan traceren aan de hand van een cookie wanneer een gebruiker bijvoorbeeld een socialenetwerksite bezoekt. Die socialenetwerksite kan ook een derde zijn wanneer die gebruiker een andere website raadpleegt die met die socialenetwerksite interageert. In al deze gevallen maakt het niet uit of informatie in het apparaat van de eindgebruiker wordt geraadpleegd of opgeslagen: er is sprake van interferentie met het apparaat en er is dus toestemming nodig (tenzij er een uitzondering van toepassing is). In de volg-me-nietnorm worden hiervoor de termen "voor de gehele website" en "voor het gehele web" gebruikt. Om meer rechtszekerheid voor alle belanghebbenden te creëren moet bijgevolg de verwijzing in de e-privacyverordening naar "derden" opnieuw worden geformuleerd, zodat alle entiteiten worden opgenomen met wie een apparaat interageert (omdat ze informatie in het apparaat opslaan of raadplegen).

Om de volg-me-nietnorm in overeenstemming te brengen met het in het Handvest vastgestelde hoge niveau van bescherming van de vertrouwelijkheid van communicatie en gegevensbescherming, moet in de e-privacyverordening worden verduidelijkt dat de verzoeken voor het traceren op het gehele web, tegenover het

---

<sup>14</sup> Zie <https://www.w3.org/TR/tracking-compliance/>. Onder punt 7 worden het uitzonderingsmodel en het onderscheid tussen uitzonderingen voor de gehele website en uitzonderingen voor het gehele web uitgelegd. Punt 6 bevat de machineleesbare informatie die verwerkingsverantwoordelijken kunnen verstrekken in het kader van de informatievereiste voor het verkrijgen van toestemming.

traceren op de gehele website, afzonderlijk moeten worden aangeboden en dat gebruikers de vrijheid moeten hebben om dergelijke verzoeken te aanvaarden of weigeren. Om gebruikers te beschermen tegen frequente toestemmingsverzoeken, moet de e-privacyverordening er bovendien voor zorgen dat, nadat een verzoek om toestemming van een specifieke organisatie voor het traceren op het gehele web is geweigerd (via de volg-me-nietnorm of een afzonderlijke zwarte lijst), deze organisatie gedurende ten minste de volgende zes maanden geen nieuwe toestemmingsverzoeken meer kan verzenden. Die regel sluit niet uit dat de organisatie de gebruiker, als hij of zij rechtstreeks de website van de organisatie raadpleegt (en dus de organisatie de eerste partij is), toestemming kan vragen voor haar eigen website (m.a.w. een verzoek om toestemming voor de gehele website). In de praktijk betekent dat bijvoorbeeld dat een videostreamingwebsite die gebruikmaakt van traceercookies de gebruiker om toestemming mag vragen wanneer hij of zij de videostreamingwebsite raadpleegt, maar niet opnieuw om toestemming mag vragen gedurende zes maanden wanneer die gebruiker toestemming heeft geweigerd en andere websites bezoekt die video's van die streamingwebsite aanbiedt.

25. Daarnaast is **de uitzondering voor "het meten van de omvang van het publiek van een website" onnauwkeurig verwoord**. In art. 8, lid 1, onder d), van de voorgestelde verordening is een uitzondering opgenomen voor het meten van de omvang van het publiek van een website. Het eerste punt van zorg is dat die term niet is omschreven en kan worden verward met profilering van gebruikers. Uit de definitie moet blijken dat deze uitzondering niet kan worden gebruikt voor profileringsdoeleinden. De uitzondering mag alleen worden gebruikt voor gebruiksanalyses die nodig zijn om de prestaties van de door de gebruiker aangevraagde dienst te analyseren, maar niet voor gebruikersanalyses (m.a.w. niet voor de analyse van het gedrag van identificeerbare gebruikers van een website, app of apparaat). Bijgevolg mag er geen beroep worden gedaan op de uitzondering wanneer de gegevens in verband kunnen worden gebracht met identificeerbare gebruikersgegevens die door de aanbieder of andere verwerkingsverantwoordelijken worden verwerkt. Bovendien schuilt er achter de omschrijving van de term een zeer technologiespecifieke applicatie. De term "het meten van de omvang van het publiek van een website" moet bijgevolg opnieuw worden omschreven, en op een technologieneutrale manier, zodat ook gelijksoortige analytische gebruiksinformatie van apps, wearables en internet-van-de-dingenapparatuur eronder vallen.

De Groep stelt voor inspiratie te halen uit de uitzondering die in Nederland van toepassing is indien strikt noodzakelijk – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij (zie art. 11.7a, lid 3, onder b), van de Nederlandse Telecommunicatiewet). Deze uitzondering houdt er rekening mee dat de meeste gegevens die via web- of appanalyses worden verzameld, nog altijd persoonsgegevens zijn en dat met andere woorden voor de verwerking ervan de algemene verordening gegevensbescherming moet worden toegepast. Dat impliceert bijvoorbeeld dat gebruiksanalyses ook kunnen worden uitgevoerd door een externe organisatie, maar alleen als:

- i) die organisatie handelt als verwerkingsverantwoordelijke;

- ii) er een verwerkingsovereenkomst is gesloten die voldoet aan de bepalingen in de algemene verordening gegevensbescherming;
- iii) de gebruikte analysetechnologie re-identificatie niet mogelijk maakt, onder andere door IP-adressen van gebruikers anoniem te maken;
- iv) de specifieke cookie(s) of andere gegevens die worden gebruikt voor de analyses alleen kunnen worden gebruikt voor die specifieke website, app of wearable en niet kunnen worden gekoppeld aan andere identificeerbare gegevens;
- v) gebruikers een opt-outrecht hebben (zie ook opmerkingen 17 en 50 van dit advies).

Hoewel toestemming niet is vereist als aan deze voorwaarden is voldaan, moeten verwerkingsverantwoordelijken nog altijd passende informatie aan de gebruikers verstrekken, bijvoorbeeld via de velden in de volg-me-nietnorm waarin de traceerstatus is weergegeven<sup>15</sup>.

26. In de e-privacyverordening **moeten de uitzonderingen op de toestemmingsvereisten eng en nauwkeurig worden omschreven**. De uitzondering op de toestemmingsvereiste voor interferentie met apparatuur in art. 8, lid 1, onder c), is bijna op dezelfde manier geformuleerd als in artikel 5, lid 3, van de e-privacyrichtlijn, waarin de formulering "strikt noodzakelijk voor de levering van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij" wordt gebruikt, maar net het belangrijke woordje "strikt" is zonder enige toelichting weggelaten. Dat is om twee redenen een punt van zorg. Ten eerste heeft de bepaling in de e-privacyrichtlijn al tot heel wat discussies geleid over het toepassingsgebied ervan tussen de toezichthoudende autoriteiten en organisaties en zal de weglating van het woord "strikt" de rechtsonzekerheid alleen maar doen toenemen. Bovendien heeft de Groep al richtsnoeren uitgevaardigd over de uitlegging van de term "strikt" in deze context. De Groep heeft de volgende verduidelijking in het advies over ontheffing van de toestemmingsverplichting voor cookies (WP 194) voorgesteld:

het cookie is strikt noodzakelijk om de gebruiker (of abonnee) een specifieke functie te bieden: als cookies zijn gedeactiveerd, is de functie niet beschikbaar en de functie is door de gebruiker (of abonnee) uitdrukkelijk gevraagd in het kader van een dienst van de informatiemaatschappij.<sup>16</sup>

Daarnaast heeft de Groep het volgende verduidelijkt:

"cookies van derden" zijn bovendien doorgaans niet "strikt noodzakelijk" voor het bezoek aan de website, aangezien dergelijke cookies doorgaans verband houden met een andere dienst dan die waarom de gebruiker "uitdrukkelijk heeft gevraagd"<sup>17</sup>.

---

<sup>15</sup> Zie: Tracking Preference Expression (DNT), Editor's draft, 7 maart 2016.

<sup>16</sup> Groep artikel 29, WP 294, Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies, goedgekeurd op 7 juni 2012, beschikbaar op: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_nl.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_nl.pdf).

<sup>17</sup> Ibidem.

De Groep voegde eraan toe dat het gebruik van sociale plug-ins voor niet-gebruikers van een platform of website evenmin zou worden beschouwd als strikt noodzakelijk.

Bovendien is op grond van artikel 6, lid 1, onder b), van de voorgestelde verordening de verwerking van elektronische communicatiegegevens toegestaan indien dit "noodzakelijk" is voor de veiligheid, terwijl dit volgens overweging 49 van de algemene verordening gegevensbescherming "strikt noodzakelijk" moet zijn. Het woord "strikt" is misschien niet opzettelijk weggelaten, aangezien in overweging 21 van de voorgestelde verordening wel is vermeld dat geen toestemming voor interferentie hoeft te worden gevraagd wanneer dit "strikt" noodzakelijk is. De voorgestelde verordening is echter een gelegenheid om te verduidelijken dat de noodzakelijkheidstoets in het kader van deze verordening nauw moet worden uitgelegd ten aanzien van alle uitzonderingen. De Groep stelt bijgevolg voor ten aanzien van alle uitzonderingen in art. 6 en art. 8, lid 1, van de voorgestelde verordening het woord "strikt" in te voegen voor "noodzakelijk".

Anderzijds moet de e-privacyverordening interferentie met apparatuur uitdrukkelijk toestaan voor de installatie van beveiligingsupdates. De installatie van beveiligingsupdates op de meeste apparatuur van eindgebruikers gebeurt bij voorkeur door het verzenden van beveiligingsupdates via internet. De installatie van updates wordt beschouwd als interferentie met eindapparatuur. Er is een gerechtvaardigd belang in het waarborgen dat de veiligheid van deze apparatuur steeds is bijgewerkt. Een aanbieder van beveiligingspatches moet bijgevolg in het algemeen de strikt noodzakelijke beveiligingspatches kunnen installeren zonder toestemming van de eindgebruiker. Het is echter onduidelijk of ook voor deze vorm van interferentie kan worden gebruikgemaakt van de "informatiemaatschappij"-uitzondering op het interferentieverbod (art. 8, lid 1, onder c)). Er moet worden verduidelijkt dat de installatie van beveiligingsupdates is toegestaan onder deze uitzondering, maar uitsluitend indien i) de beveiligingsupdates discreet zijn verpakt en op geen enkele wijze de functies van de software op het apparaat wijzigen (met inbegrip van de interactie met andere software of instellingen die de gebruiker heeft gekozen), ii) de eindgebruiker telkens vooraf op de hoogte wordt gebracht dat een update wordt geïnstalleerd, en iii) de eindgebruiker de mogelijkheid heeft om de automatische installatie van deze updates uit te schakelen.

## *DIRECT MARKETING*

Een ander punt van zorg betreft de gebrekkige bescherming tegen direct marketing.

27. Ten eerste is **het toepassingsgebied van direct marketing te eng**. In art. 4, lid 3, onder f), van de voorgestelde verordening worden "directmarketingberichten" gedefinieerd als "elke vorm van reclame, zowel geschreven als mondeling, gericht aan één of meer geïdentificeerde of identificeerbare eindgebruikers van elektronische communicatiediensten". Het gebruik van de woorden "gericht aan één of meer geïdentificeerde of identificeerbare eindgebruikers" impliceert het gebruik van technologische communicatiemiddelen die noodzakelijkerwijs het overdragen van een boodschap moeten omvatten, terwijl de meeste vormen van reclame via het web



(op sociale media of websites) strikt gezien geen advertenties "overdragen". Dit wordt verder benadrukt in de voorbeelden die in het vervolg van deze definitie (sms, e-mail) en in overweging 33 zijn aangehaald. Deze voorbeelden verwijzen naar de vrij traditionele vormen van marketingberichten, en zelfs voor het gebruik van – vrij traditionele – oproepsystemen staat het niet vast dat het binnen het toepassingsgebied valt. Het artikel en de overweging moeten worden gewijzigd zodat het duidelijk is dat de definitie van toepassing is op alle advertenties die worden *verzonden naar of gericht of gepresenteerd aan één* of meer geïdentificeerde of identificeerbare eindgebruikers. Daarnaast moet ervoor worden gezorgd dat op surfgedrag gebaseerde advertenties (d.w.z. gebaseerd op de profielen van eindgebruikers) ook worden beschouwd als directmarketingberichten gericht aan "één of meer geïdentificeerde of identificeerbare eindgebruikers" (aangezien dergelijke advertenties zijn gericht aan specifieke, identificeerbare gebruikers).

Daarnaast zou op grond van het voorgestelde toepassingsgebied van "directmarketingberichten" de bescherming van art. 16, lid 1, beperkt zijn tot berichten die reclamemateriaal bevatten en zouden personen niet zijn beschermd tegen andere berichten die naar hen worden verzonden of aan hen zijn gericht of gepresenteerd voor marketingdoeleinden (zoals leadgeneratieberichten waarin om toestemming wordt verzocht, bevordering van politieke standpunten of stemvoorkeuren, bevordering van liefdadigheidsorganisaties of vzw's of algemene branding van een organisatie). Bovendien worden nog steeds directmarketingberichten via faxtoestellen verzonden, wat niet in de definitie is opgenomen. Bijgevolg moet artikel 4, lid 3, onder f), alle vormen van reclame maken, klantenwerving of bevordering, ook door vzw's, omvatten en moeten faxtoestellen uitdrukkelijk worden opgenomen naast e-mail en sms (zie ook het voorstel voor verduidelijking in opmerking 43, onder a)). Tot slot staat in overweging 32 dat berichten die politieke partijen zenden om hun partij te promoten ook onder direct marketing vallen. Dat moet worden uitgebreid met politici en verkiezingskandidaten die campagne voeren.

28. Ten tweede **kan de toestemming voor direct marketing niet kosteloos en even gemakkelijk als het geven van toestemming worden ingetrokken**. De optie in de voorgestelde verordening om toestemming in te trekken moet worden verduidelijkt om samenhang te verzekeren en ontvangers beter te beschermen. In art. 16, lid 6, van de voorgestelde verordening staat momenteel dat de ontvangers van direct marketing "de nodige informatie [moeten ontvangen] om het recht tot intrekking van hun toestemming voor verdere ontvangst van marketingberichten op eenvoudige wijze uit te oefenen" (nadruk toegevoegd). Dat wordt bevestigd in overweging 34. Uit overweging 70 van de algemene verordening gegevensbescherming blijkt echter dat betrokkenen op grond van de algemene verordening gegevensbescherming niet alleen het recht moeten hebben om op eenvoudige wijze bezwaar te maken tegen verwerking ten behoeve direct marketing, maar dat ze dat ook "kosteloos" moeten kunnen doen. Die term wordt ook gebruikt in artikel 16, lid 2, van de voorgestelde verordening, maar alleen met betrekking tot de opt-out voor direct marketing op basis van contactgegevens die in het kader van een verkoop zijn verkregen.

In art. 7, lid 3, van de algemene verordening gegevensbescherming staat dat het intrekken van de toestemming even eenvoudig is als het geven ervan en dat betrokkenen te allen tijde hun toestemming moeten kunnen intrekken. Daarnaast erkende de Groep al in haar Advies 4/2010 over FEDMA (WP 174) het belang van het aanbieden van "afmeldingsmogelijkheden waarmee een ontvanger van commerciële boodschappen op een eenvoudige, kosteloze, rechtstreekse en gemakkelijk toegankelijke wijze te kennen kan geven geen [directmarketingboodschappen] meer te willen ontvangen"<sup>18</sup>. Die norm voor het intrekken van toestemming moet worden opgenomen in de regels voor direct marketing in de voorgestelde verordening. Hetzelfde geldt voor de vereiste in art. 7, lid 3, van de algemene verordening gegevensbescherming dat het intrekken van de toestemming even eenvoudig moet zijn als het geven ervan.

29. In dit verband **moet worden verduidelijkt hoe de toestemming kan worden ingetrokken of van directmarketingoproepen kan worden afgezien**. Op basis van artikel 16, lid 4, van de voorgestelde verordening kunnen lidstaten een opt-outregeling vaststellen voor spraakoproepen voor direct marketing. In de e-privacyverordening moeten de regelingen worden vermeld voor de intrekking van de toestemming en de opt-out voor marketingoproepen. In overweging 36 staat dat de lidstaten "de mogelijkheid moeten hebben" om nationale opt-outsysteem in te stellen of te handhaven. Op basis van deze bepaling kunnen lidstaten dus een situatie toelaten waarin een gebruiker bij elke communicatieaanbieder afzonderlijk zijn wil voor opt-out kenbaar moet maken. Dergelijke situatie doet afbreuk aan de bescherming van gebruikers tegen de overlast van ongewenste communicatie<sup>19</sup> en biedt hen geen mechanisme waarmee ze overeenkomstig de algemene verordening gegevensbescherming hun toestemming op eenvoudige wijze en te allen tijde kunnen intrekken. Bijgevolg moet in de verordening uitdrukkelijk de verplichting worden opgenomen voor lidstaten om een nationaal bel-me-niet-register aan te leggen. Daarnaast moet in de verordening worden gespecificeerd dat de ontvangers van spraakoproepen twee opties moeten krijgen om hun toestemming in te trekken: voor nieuwe oproepen van die onderneming of organisatie en de mogelijkheid om tijdens deze oproepen zich te laten opnemen in een nationaal bel-me-niet-register.
30. Een ander punt van zorg is dat **het gebruik van valse identiteiten voor het verzenden van directmarketingberichten niet uitdrukkelijk is verboden**. In overweging 34 wordt opgemerkt dat "het afschermen van de identiteit en het gebruiken van valse identiteiten, valse terugzendadressen of nummers bij verzending van ongevraagde commerciële communicatie van direct marketing" verboden is. In art. 16, lid 4, staat echter gewoon dat de eindgebruikers worden geïnformeerd over

---

<sup>18</sup> Groep artikel 29, WP 174, Advies 4/2010 over de Europese gedragscode van FEDMA voor het gebruik van persoonsgegevens in het kader van direct marketing, goedgekeurd op 13 juli 2010, beschikbaar op: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_nl.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_nl.pdf)

<sup>19</sup> Zo heeft de telecomoperator BT in het Verenigd Koninkrijk 31 miljoen ongewenste oproepen in één week tijd geregistreerd. Zie <http://www.bbc.com/news/business-38635921>

"de identiteit van de natuurlijke of rechtspersoon namens wie de communicatie wordt verzonden". Deze verplichting om ontvangers te informeren over de identiteit moet worden aangevuld met een duidelijk verbod op het gebruik van afgeschermd of valse contactadressen voor directmarketingdoeleinden.

31. Dat houdt verband met een ander punt van zorg: de **kengetalvereiste voor directmarketingoproepen wordt voorgesteld als een alternatief voor de vereiste inzake de identificatie van de oproepende lijn**. Directmarketingoproepen zijn op grond van art. 16, lid 3, toegestaan indien de oproeper i) de identiteit verstrekt van een lijn waarop contact kan worden opgenomen met de natuurlijke of rechtspersoon die de oproep doet (art. 16, lid 3, onder a)), of ii) een specifieke code of kengetal gebruikt waaruit blijkt dat de oproep een marketingoproep is (art. 16, lid 3, onder b)). Hoewel de Groep blij is met de verplichting in art. 16, lid 3, onder b), om een kengetal te gebruiken, vindt zij dat deze vereiste niet op hetzelfde probleem betrekking heeft als waaraan de verplichting inzake de identificatie van de oproepende lijn in art. 16, lid 3, onder a), tegemoetkomt. Terwijl de kengetalvereiste moet dienen om het de ontvanger mogelijk te maken een oproep vooraf te identificeren als een marketingoproep (en maatregelen te nemen om deze oproepen te blokkeren), is de vereiste inzake de identificatie van de oproepende lijn bedoeld om ontvangers (en toezichthoudende autoriteiten) de middelen te verstrekken om de initiatiefnemer van de marketing te identificeren en ermee contact op te nemen. Dat is met name relevant voor geautomatiseerde oproepen, waarbij er een groot onevenwicht is tussen de mogelijkheden voor de marketeer om ongewenste oproepen te verzenden en de mogelijkheden van de ontvanger om deze oproepen te vermijden. De vereisten mogen dus niet als alternatieven worden beschouwd, maar moeten elkaar aanvullen.

#### *TIJDSHEMA*

32. De Groep artikel 29 looft het feit dat de Europese Commissie erkent dat de voorgestelde verordening samen met de algemene verordening gegevensbescherming in mei 2018 in werking moet treden om inconsistenties tussen de twee wetshandelingen te vermijden. Dat is volgens haar echter een ambitieuze termijn, die ook vereist dat het ontwerp van het Europees wetboek voor elektronische communicatie wordt voltooid. WP29 verzoekt daarom alle belanghebbenden bij het wetgevingsproces de uiterste termijn van mei 2018 na te leven.

#### *ANDERE PUNTEN VAN ZORG*

In dit deel worden een aantal aanvullende punten van zorg besproken.

33. Ten eerste is WP29 bezorgd over **de suggestie dat niet-doelgerichte gegevensbewaringsmaatregelen worden aanvaard**. In de toelichting wordt opgemerkt dat het op grond van de voorgestelde verordening de lidstaten vrijstaat een nationaal kader voor gegevensbewaring te behouden of te creëren dat onder meer

voorziet in doelgerichte bewaringsmaatregelen (paragraaf 1.3). Sinds het arrest *Tele2 Sverige*<sup>20</sup> is het duidelijk dat op grond van het Handvest kaders voor gegevensbewaring die andere vormen van gegevensbewaring dan doelgerichte gegevensbewaring regelen, niet zijn toegestaan (en zelfs dan moeten voldoen aan belangrijke voorwaarden zoals toezicht), en dat algemene toegang tot metagegevens op dezelfde manier als algemene toegang tot de inhoud van elektronische communicatie moet worden beschouwd als een inbreuk op de grondgedachte van art. 7 (zie arrest Schrems van het Hof en overweging 94). De formulering van die zin laat dus vermoeden dat de lidstaten een zekere vrijheid hebben voor wat gegevensbewaringsmaatregelen betreft, wat eigenlijk niet zo is. In verband hiermee moet worden opgemerkt dat **metagegevens in de voorgestelde verordening een onvoldoende niveau van bescherming krijgen**. Zoals verklaard in opmerking 10, is de Groep artikel 29 blij met de erkenning dat via metagegevens zeer gevoelige gegevens aan het licht kunnen komen. Metagegevens krijgen in de voorgestelde verordening echter niet de bescherming die bij dergelijke erkenning hoort. Gezien de gevoeligheid van metagegevens moet met name, vóór een analyse op grond van art. 6, lid 2, onder c), een gegevensbeschermingseffectbeoordeling worden uitgevoerd (zie ook opmerking 46).

34. Ten tweede **zou de voorgestelde verordening de mogelijkheden om gegevens te bewaren uitbreiden, wat niet wenselijk is**. In artikel 11 van de voorgestelde verordening wordt verwezen naar artikel 23, lid 1, onder a) tot en met e), van de algemene verordening gegevensbescherming door de doeleinden te beschrijven waarvoor de lidstaten de verplichtingen en rechten waarin de artikelen 5 tot en met 8 van de verordening voorzien, kunnen beperken. De algemene verordening gegevensbescherming voorziet, gezien de hoge risico's voor betrokkenen, niet in dergelijke beperkingen ten aanzien van bijzondere categorieën gegevens. Art. 15 van de e-privacyrichtlijn staat momenteel een gelijksoortige beperking wel toe, maar met meer beperkte doeleinden. Op grond van de nieuwe voorgestelde verordening zouden nieuwe beperkingen mogelijk zijn ten behoeve van "de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen voor de openbare veiligheid" (art. 23, lid 1, onder d), van de algemene verordening gegevensbescherming) en "andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid" (art. 23, lid 1, onder e), van de algemene verordening gegevensbescherming). Die doeleinden zijn niet alleen nieuw ten opzichte van de e-privacyrichtlijn, maar, voor wat het laatste doeleinde van art. 23, lid 1, onder d), en het volledige doeleinde van art. 123, lid 1, onder e), betreft, ook veel te ruim geformuleerd. Bijgevolg wordt voorgesteld om de verwijzing naar artikel 23, lid 1, onder a) tot en met e), van de algemene verordening gegevensbescherming te schrappen en in plaats daarvan alleen de doeleinden te vermelden die momenteel in art. 15 van de e-privacyrichtlijn zijn opgenomen.

<sup>20</sup> ECLI:EU:C:2016:970, beschikbaar op: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

35. **De verplichting om gebruikers te informeren over veiligheidsrisico's heeft een minimalistisch toepassingsgebied.** De Groep is blij met het feit dat dienstverleners gebruikers moeten informeren over de veiligheidsrisico's en de maatregelen, zoals encryptie, om deze risico's aan te pakken (art. 17 en overweging 37). De titel van de desbetreffende bepaling luidt echter: "Informatie over geconstateerde veiligheidsrisico's". Het feit dat de titel verwijst naar geconstateerde risico's, suggereert dat deze bepaling uitsluitend betrekking heeft op (mogelijke) beveiligingsinbreuken, terwijl de formulering van de bepaling en de overweging meer een algemene voorlichting van eindgebruikers suggereert. Indien bijvoorbeeld een aanbieder constateert dat het apparaat van een gebruiker is besmet met malware en een onderdeel van een botnet is geworden, blijkt de aanbieder op grond van deze bepaling rechtstreeks verplicht te zijn om de gebruiker te informeren over de hieruit voortvloeiende risico's. Het toepassingsgebied van deze bepaling kan echter worden verduidelijkt en mag niet worden beperkt tot dat specifieke scenario. De bepaling moet ten minste betrekking hebben op geconstateerde veiligheidsrisico's in alle apparatuur die de aanbieder aan de eindgebruiker verstrekt in het kader van een abonnement, zoals routers en mobiele apparatuur, en moet voorlichting omvatten over de risico's van het wijzigen van instellingen die volgens het beginsel van privacy door ontwerp op privacybeschermend zijn ingesteld.

De Groep beveelt aan het toepassingsgebied uit te breiden tot aanbieders van software voor elektronische communicatie (zie overweging 8) en mogelijk ook tot een nieuwe categorie: aanbieders, andere dan aanbieders van een elektronische communicatiedienst, van technologie die nodig is om communicatie te beveiligen (bv. aanbieders van encryptietechnologie). In het laatste geval moet ervoor worden gezorgd dat die verplichting niet overlapt met de verplichtingen inzake de melding van beveiligingsinbreuken in andere instrumenten zoals de NIS-richtlijn<sup>21</sup> en andere rechtsinstrumenten betreffende certificaatverstrekkers. Aangezien de laatste categorie, die van de technologie-aanbieders, doorgaans geen rechtstreeks contact heeft met eindgebruikers, moet ook worden toegelicht hoe deze aanbieders kunnen voldoen aan hun informatieverplichting uit hoofde van deze bepaling.

36. De Groep is blij met de bepalingen van artikelen 2 en 13 die van toepassing zullen zijn op nummergebaseerde persoonlijke communicatiediensten. Het is echter niet onmiddellijk duidelijk waarom een **gelijksoortig niveau van privacybescherming ook niet van toepassing zou kunnen zijn op OTT-oproepdiensten met gelijksoortige functies.**
37. De Groep is ook bezorgd over het **gebrek aan duidelijkheid over de gedetailleerde toestemming voor omgekeerde zoekfuncties in telefoongidsen.** Aanbieders moeten op grond van art. 15, lid 2, van de voorgestelde verordening toestemming verkrijgen van eindgebruikers voordat zij zoekfuncties in verband met gegevens mogelijk maken

---

<sup>21</sup> Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB L 194 van 19.7.2016, blz. 1-30, beschikbaar op: <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016L1148&from=NL>

(zie ook overweging 31). De Groep is blij met de harmonisering van de toestemmingsvereiste met betrekking tot de opname in telefoongidsen, maar betreurt het feit dat er voor de gedetailleerdheid van de toestemming geen onderscheid wordt gemaakt tussen de verschillende soorten zoekopdrachten. De lidstaten mogen op grond van artikel 12, lid 3, van de huidige e-privacyrichtlijn een aparte toestemmingsvereiste verlangen voor omgekeerde zoekfuncties. In dat artikel staat het volgende: "De lidstaten kunnen verlangen dat de aparte toestemming van de abonnees ook verkregen moet worden voor andere doeleinden van een openbare abonneelijst dan het zoeken van contactgegevens van een persoon op basis van zijn naam en, in voorkomend geval, een minimumaantal andere identificatiegegevens." Op basis van deze bepaling is in veel lidstaten een afzonderlijke toestemming vereist voor omgekeerde zoekfuncties op basis van de verschillende niveaus van identificeerbaarheid en dus de mate waarin de twee functies de privacy aantasten.

38. Een ander formeel punt is dat **het niveau van de boetes niet geharmoniseerd is voor alle inbreuken in de verordening**. De lidstaten stellen op grond van de voorgestelde verordening de regels inzake de sancties voor inbreuken op artikel 23, leden 4 en 6, en artikel 24 van de voorgestelde verordening vast. Het komt de samenhang meer ten goede als een dergelijke bepaling ook wordt opgenomen in de e-privacyverordening zelf.
39. Tot slot **is de voorgestelde verordening gebaseerd op definities die nog kunnen veranderen**. Voor een aantal kernbegrippen verwijst de voorgestelde verordening naar een ander rechtsinstrument dat momenteel nog in de ontwerpfase zit, met name het Europees wetboek voor elektronische communicatie (zie bijvoorbeeld art. 4, lid 1, onder b)). Twee belangrijke voorbeelden hiervan zijn de definitie van "eindgebruiker", die momenteel natuurlijke en rechtspersonen omvat, en de definities van "elektronischecomunicatiedienst" en "persoonlijke communicatiedienst", waarvan sprake is in art. 4, lid 1, onder b), van de voorgestelde verordening en waarvoor, in het geval van de laatste definitie, in art. 4, lid 2, verder wordt uitgelegd dat de definitie ook soorten diensten omvat die specifiek zijn uitgesloten in het Europees wetboek voor elektronische communicatie.<sup>22</sup> Dit advies is gebaseerd op de huidige definities, maar het is zeer waarschijnlijk dat het voorgestelde Europees wetboek voor elektronische communicatie en/of de kernbegrippen ervan zullen wijzigen. Dat zou ook rechtstreekse gevolgen hebben op de e-privacyverordening. In het ideale geval zouden alle termen die van het Europees wetboek voor elektronische communicatie zijn overgenomen, op onafhankelijke wijze in de e-privacyverordening moeten worden gedefinieerd, of zou ten minste in de voorgestelde verordening moeten worden verduidelijkt welke termen een andere definitie hebben dan die in het Europees wetboek voor elektronische communicatie (bv. de reeds genoemde opname van "bijkomstige diensten" in de definitie van "persoonlijke communicatiedienst").

<sup>22</sup> Zo staat er in art. 4, lid 2, van de voorgestelde verordening dat een persoonlijke communicatiedienst "diensten [omvat] die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst", terwijl in art. 2, lid 5, van het Europees wetboek voor elektronische communicatie dergelijke diensten uitdrukkelijk van die definitie worden uitgesloten. (In het Europees wetboek voor elektronische communicatie wordt "persoonlijke communicatiedienst" opgenomen in de ruimere categorie van "elektronischecomunicatiedienst" in art. 2, lid 4.)

Indien dat niet mogelijk is, zou de Groep echter alle partijen die betrokken zijn bij het wetgevingsproces willen voorstellen om de voorgestelde verordening en het Europees wetboek voor elektronische communicatie tegelijk te bespreken en stemmen, zodat de belanghebbenden het toepassingsgebied en de gevolgen van de nieuwe instrumenten correct kunnen beoordelen.

## **5. VOORSTELLEN VOOR VERDUIDELIJKING OM RECHTSZEKERHEID TE WAARBORGEN**

Naast de hierboven besproken punten, wenst de Groep enkele bepalingen in de voorgestelde verordening te benadrukken die het best zouden worden verduidelijkt. Dergelijke verduidelijkingen geven alle belanghebbenden meer rechtszekerheid dat de e-privacyverordening in de gehele EU op een uniforme manier zal worden begrepen en toegepast.

### *VERDUIDELIJKING VAN HET TOEPASSINGSGEBIED*

40. WP29 stelt met betrekking tot het toepassingsgebied van de voorgestelde verordening de volgende verduidelijkingen voor:

- a. **De term "eindgebruiker" moet alle individuele gebruikers omvatten.** In art. 2, lid 14, van het Europees wetboek voor elektronische communicatie wordt "eindgebruiker" gedefinieerd als een gebruiker die geen openbaar communicatienetwerk of openbare elektronischecommunicatiediensten aanbiedt. Er moet worden verduidelijkt dat personen die bijdragen aan netwerken, bijvoorbeeld aan vermaasde netwerken met hun wifirouter, niet zijn uitgesloten van het toepassingsgebied van de bescherming die de voorgestelde verordening biedt.
- b. **Er moet worden verduidelijkt dat het territoriale toepassingsgebied alle eindgebruikers in de Unie omvat.** In art. 3, lid 1, onder a), is bepaald dat de voorgestelde verordening van toepassing is op het aanbieden van elektronischecommunicatiediensten aan eindgebruikers "in de Unie", terwijl in art. 3, lid 1, onder c), is bepaald dat de voorgestelde verordening van toepassing is op de bescherming van eindapparatuur van eindgebruikers "die zich in de Unie bevinden" (nadruk toegevoegd). Er zijn verschillen tussen de vertalingen. In de Duitse vertaling wordt dat onderscheid niet gemaakt, terwijl er in andere vertalingen, zoals de Franse, Spaanse en Nederlandse, wel een onderscheid is. Uit overweging 9 blijkt duidelijk dat het territoriale toepassingsgebied breed moet worden opgevat en dat het niet uitmaakt of de diensten binnen of buiten de Unie worden aangeboden en of de verwerking in de Unie plaatsvindt. Er wordt bijgevolg voorgesteld de term "die zich in de Unie bevinden" in art. 3, lid 1, onder c), te vervangen door "in de Unie" om dat breed toepassingsgebied te benadrukken.
- c. **De voorgestelde verordening blijkt slechts vertrouwelijke communicatie in doorvoer te beschermen, en geen opgeslagen communicatie.** De huidige aanpak van de voorgestelde verordening is voornamelijk gericht op de bescherming van de transmissie van communicatie. Zie bijvoorbeeld overweging 15, waarin staat dat het verbod op interceptie van

communicatiegegevens moet gelden tijdens de overdracht ervan, met andere woorden totdat de inhoud van de elektronische communicatie door de beoogde geadresseerde is ontvangen. Het toepassingsgebied van deze bescherming is gebaseerd op een verouderd conceptueel kader van communicatie. De meeste communicatiegegevens worden, zelfs na ontvangst, door de dienstverlener bijgehouden. Er moet worden gezorgd dat de vertrouwelijkheid van die gegevens beschermd blijft. Bovendien is er bij communicatie tussen abonnees van dezelfde cloudgebaseerde diensten (bijvoorbeeld webmailaanbieders) vaak slechts in zeer beperkte mate sprake van overdracht: het verzenden van een e-mail zal ten hoogste zichtbaar zijn in de gegevensbank van de aanbieder en niet echt het verzenden van berichten tussen twee partijen inhouden. Het argument dat dit al aan bod zou komen in de algemene verordening gegevensbescherming is niet overtuigend: de bedoeling van de voorgestelde verordening is net het beschermen van alle vertrouwelijke communicatie, ongeacht de technische middelen die voor de communicatie zijn gebruikt. Het is mogelijk dat dit gewoon een fout in het ontwerp betreft, want het verbod in artikel 5 heeft betrekking op "opslaan" en "verwerken".

- d. **Alle openbare draadloze internethotspots moeten onder het toepassingsgebied vallen.** Aangezien het gebruik van draadloze hotspots gangbaar is, is het niet meer dan logisch dat er geen twijfel mag bestaan over de bescherming van de vertrouwelijkheid van communicatie die via dergelijke hotspots wordt overgedragen. De poging om dat in de verordening te verduidelijken, is echter mislukt, aangezien uitsluitend netwerken die worden verleend aan een "onbepaalde groep van eindgebruikers" onder het toepassingsgebied vallen (overweging 13). De termen "onbepaalde groep van eindgebruikers" en "gesloten groep eindgebruikers" moeten worden gedefinieerd. Er moet met name worden verduidelijkt dat beveiligde draadloze netwerken (d.w.z. met een wachtwoord) ook binnen het toepassingsgebied vallen als dit wachtwoord wordt verstrekt aan een theoretisch ongelimiteerde groep gebruikers waarvan de identiteit vooraf niet kan worden vastgesteld (bv. klanten van een café, bezoekers van een luchthaven). Het onderliggende beginsel in dat verband is dat, in overeenstemming met het eerdere advies van WP29 inzake de evaluatie van de e-privacyrichtlijn, alleen diensten die in een officiële of arbeidssituatie plaatsvinden voor werkgerelateerde of officiële doeleinden, of technische communicatie tussen niet-overheidsorganen of overheidsorganen uitsluitend om werk- of bedrijfsprocessen te beheren, alsook het gebruik van diensten voor uitsluitend huishoudelijke doeleinden kunnen worden vrijgesteld van het e-privacyinstrument (blz. 8).
- e. **Gegevens die zijn verzameld bij het aanbieden van digitale omroepdiensten moeten onder de voorgestelde verordening vallen.** Gezien de gevoelige aard van kijkgedrag, waaruit de persoonlijke interesses en kenmerken van de kijkers kunnen worden afgeleid, moet in de e-privacyverordening worden verduidelijkt (misschien in een overweging) dat de uitsluiting van diensten waarbij "met behulp van elektronische-communicatienetwerken overgebrachte inhoud" wordt geleverd, van de definitie van "elektronischecomunicatiedienst", niet impliceert dat



dienstverleners die zowel elektronischecommunicatiediensten als inhoudsdiensten aanbieden buiten het toepassingsgebied vallen van de bepalingen van de e-privacyverordening die gericht zijn op de aanbieders elektronischecommunicatiediensten. Dat is met name van belang omdat het verlenen van diensten waarbij "met behulp van elektronischecommunicatienetwerken overgebrachte inhoud" wordt geleverd, uitgesloten is van de definitie van "elektronischecommunicatiedienst" in het voorgestelde Europees wetboek voor elektronische communicatie (art. 2, lid 4).

- f. **Communicatiegegevens zijn in het algemeen persoonsgegevens.** In overweging 4 wordt opgemerkt dat communicatiegegevens persoonsgegevens kunnen omvatten. De meeste communicatiegegevens zijn echter persoonsgegevens<sup>23</sup> die meestal intiem en gevoelig van aard zijn. De overweging moet dus worden gewijzigd en vermelden dat de gegevens in het algemeen persoonsgegevens zijn.
- g. **Ook berichten binnen hetzelfde platform vallen onder vertrouwelijke communicatie.** In overweging 1 wordt uitgelegd dat het beginsel van vertrouwelijkheid van toepassing is op "huidige en toekomstige communicatiemiddelen". In die overweging wordt vervolgens een lijst van voorbeelden van dergelijke middelen gegeven, zoals "persoonlijke berichten die via de sociale media worden verzonden". Hiermee worden wellicht ook privéberichten tussen gebruikers van een sociaal netwerk bedoeld (bv. Facebook of Twitter) of berichten die op een tijdslijn worden gepost en die toegankelijk zijn voor een eindig aantal personen. De formulering is echter niet duidelijk genoeg.
- h. **Hoe de e-privacyverordening van toepassing is op de communicatie tussen machines.** Zoals gezegd in paragraaf 9, is de Groep blij met de uitbreiding van de bescherming tot de communicatie tussen machines. Hiervan wordt echter uitsluitend melding gemaakt in overweging 12 en niet in een dienovereenkomstig artikel. Die bescherming is wenselijk, want dergelijke communicatie bevat vaak informatie die is beschermd door de regels inzake het recht op privacy. Anderzijds moet een beperkte categorie van zuivere communicatie tussen machines worden vrijgesteld indien er geen gevolgen zijn voor de privacy of de vertrouwelijkheid van communicatie, bijvoorbeeld in het geval waarin wordt gecommuniceerd over de activiteitsstatus in het kader van een transmissieprotocol tussen netwerkelementen (bv. servers, switches).

Een specifieke context waarvoor de toepassing van de e-privacyverordening moet worden verduidelijkt, is het gebied van intelligente vervoerssystemen. Voertuigen in dergelijke systemen zullen voortdurend gegevens met een identificatiecode via de radio doorzenden. Zonder de aanvullende

---

<sup>23</sup> Zie bijvoorbeeld HvJ-EU 6 november 2003, C-101/01, punt 24 (met betrekking tot een telefoonnummer), HvJ-EU 19 oktober 2016, C-582/14 (*Breyer*), punt 49 (met betrekking tot dynamische IP-adressen) en HvJ-EU 8 april 2014, C-239/12 en C-594/12 (*Digital Rights Ireland*), punten 26-27 (met betrekking tot de gevoeligheid van metagegevens).

bescherming in de e-privacyverordening betreffende communicatiegegevens zou dit kunnen leiden tot een voortdurende tracering van de rijgewoonten, routes en snelheid van de chauffeurs. In artikel 2, lid 1, van het Europees wetboek voor elektronische communicatie is echter een nieuwe, uitgebreide definitie van communicatienetwerken opgenomen. Volgens deze definitie zijn transmissiesystemen die geen gecentraliseerde beheerscapaciteit hebben en die het mogelijk maken signalen over te brengen via radiogolven ook communicatienetwerken. In overweging 14 van de e-privacyverordening staat dat dergelijke gegevens elektronischecommunicatiegegevens zijn. Overeenkomstig artikel 5 van de voorgestelde verordening is het onderscheppen, controleren en opslaan van deze communicatiegegevens verboden, tenzij een uitzondering van toepassing is. Er is echter een belang bij het verwerken van gegevens op basis waarvan voorwerpen, zoals zelfrijdende auto's en apparatuur, elkaar kunnen waarschuwen voor hun nabijheid of andere risico's. De vraag is dan welke uitzondering in dat geval van toepassing is. Toestemming van eindgebruikers is geen haalbare uitzondering omdat het nodig kan zijn om te allen tijde deze gegevens te kunnen verwerken. Aanbieders moeten bijgevolg een beroep kunnen doen op een specifieke uitzondering op basis waarvan voorwerpen, zoals zelfrijdende auto's en apparatuur, elkaar kunnen waarschuwen voor hun nabijheid of andere risico's.

#### *VERDUIDELIJKINGEN BETREFFENDE HET BEGRIIP TOESTEMMING EN DE TOEPASSING ERVAN*

41. WP29 stelt met betrekking tot het begrip toestemming en de toepassing ervan in de huidige voorgestelde verordening de volgende verduidelijkingen voor:

- a. **Hoe "toestemming" moet worden toegepast in de context van rechtspersonen.** In overweging 3 wordt opgemerkt dat de verordening ervoor moet zorgen dat de bepalingen van de algemene verordening gegevensbescherming eveneens toegepast worden op eindgebruikers die rechtspersonen zijn. Volgens de overweging valt de definitie van toestemming krachtens de algemene verordening gegevensbescherming hieronder (zie ook overweging 18). Zoals reeds gezegd in opmerking 13, is de Groep blij met de uitdrukkelijke opname van rechtspersonen in het toepassingsgebied van de verordening. De praktische toepassing van dit beginsel is echter niet duidelijk. Volgens de definitie van "toestemming" in de algemene verordening gegevensbescherming moet de toestemming "geïnformeerd" zijn en de wilsuiting van de betrokkene moet gebeuren via "een verklaring of een ondubbelzinnige actieve handeling" (art. 4, lid 11, van de algemene verordening gegevensbescherming). Er moet worden verduidelijkt wanneer een rechtspersoon in de praktijk als "geïnformeerd" kan worden beschouwd en wanneer een rechtspersoon een dergelijke wilsuiting bekendmaakt.
- b. In dat verband is het nuttig op te merken dat werkgevers in de meeste omstandigheden geen toestemming kunnen geven namens hun werknemers omdat, indien een werkgever toestemming vraagt aan een werknemer en, gezien de ongelijke machtsverhouding, er een werkelijk of mogelijk nadelig

effect is als de toestemming wordt geweigerd, dergelijke toestemming niet geldig is omdat deze niet vrij is gegeven<sup>24</sup>. Voor **bedrijven die apparatuur verstrekken aan personen voorziet de voorgestelde verordening niet in een (passende) uitzondering** op het interferentieverbod. Een eerste voorbeeld is wanneer een werkgever de software van een bedrijfstelefoon wil bijwerken. Een tweede voorbeeld is wanneer een werkgever werknemers een leaseauto aanbiedt en om administratieve redenen een derde locatiegegevens via een boordcomputer in de auto laat verzamelen. In beide gevallen heeft de werkgever belang bij de interferentie met die apparatuur.

Die vorm van interferentie kan niet worden beschouwd als noodzakelijk voor het aanbieden van een dienst van de informatiemaatschappij (art. 8, lid 1, onder c)), of noodzakelijk om de omvang van het publiek te meten (art. 8, lid 1, onder d)). Dat probleem kan worden opgelost door een nieuwe uitzondering in te voeren, die betrekking heeft op een situatie waarin i) de werkgever bepaalde apparatuur verstrekt in het kader van een arbeidsverhouding, ii) de werknemer de gebruiker van deze apparatuur is, en iii) interferentie strikt noodzakelijk is voor de werking van de uitrusting die de werknemer gebruikt (wat impliceert dat de beginselen inzake evenredigheid en subsidiariteit moeten worden toegepast voor het verzamelen van gegevens). Alleen als aan deze voorwaarden is voldaan, moet interferentie met de apparatuur van de eindgebruikers voor de werkgever mogelijk zijn.

- c. **Betere controle over de beëindiging van automatische doorschakeling van oproepen.** Artikel 14 voorziet in een belangrijke beheersmaatregel op basis waarvan eindgebruikers automatische doorschakeling van oproepen kunnen beëindigen. Deze bescherming kan worden verbeterd door in de eerste plaats ook de toestemming van de eindgebruiker te vereisen voor het tot stand brengen van de doorschakeling van oproepen.

#### *VERDUIDELIJKINGEN BETREFFENDE LOCATIE- EN ANDERE METAGEGEVENS*

- 42. De Groep stelt voor het volgende te verduidelijken met betrekking tot locatie- en andere metagegevens:

- a. De betekenis van **"locatiegegevens die in een andere context dan bij het aanbieden van elektronische-communicatiediensten worden gegenereerd" in overweging 17 moet worden verduidelijkt.** Het is onduidelijk of dat betrekking heeft op locatiegegevens die zijn verzameld via bijvoorbeeld apps die gebruikmaken van de gegevens van de gps-functie in slimme apparaten en/of die locatiegegevens genereren op basis van wifirouters in de buurt, en/of locatiegegevens die zijn verzameld met navigatieondersteuning aan boord en/of andere manieren om locatiegegevens te genereren. Door deze onduidelijkheid is er rechtsonzekerheid over de

---

<sup>24</sup> Zie Advies 15/2011 over de definitie van "toestemming" (WP 187), Advies 8/2001 betreffende de verwerking van persoonsgegevens in het kader van de arbeidsverhouding (WP 48) en het nieuwe advies over gegevensverwerking op het werk (dat samen met dit advies wordt goedgekeurd).

reikwijdte van de verplichting. Locatiegegevens van de eindapparatuur van een natuurlijk persoon zijn in elk geval persoonsgegevens en dus moet voor de verwerking van deze gegevens aan de verplichtingen in de algemene verordening gegevensverwerking worden voldaan.

- b. Er moet worden verduidelijkt dat er **voor de meeste gewettigde verwerking van locatiegegevens en andere metagegevens geen identificatiecodes zijn vereist**. In overweging 17 worden heatmaps genoemd als voorbeeld van commercieel gebruik van elektronischecomunicatiemetagegegevens door aanbieders van elektronischecomunicatiediensten. Om een basisheatmap aan te maken zijn echter geen identificatiecodes nodig, maar gewoon gegevens van een statistische telling. Een ander voorbeeld uit die overweging, met name het gebruik van en de druk op infrastructuur, kan ook worden gemeten door middel van bepaalde meetpunten, bijvoorbeeld door statistieken over het gebruik van verkeerstorens samen te voegen om een indicatie te hebben van de druk op een bepaald moment op een bepaalde locatie, zonder dat de identiteit van de verbonden personen moet worden vastgesteld.

Daarnaast wordt in de overweging als voorbeeld het weergeven genoemd van verkeersbewegingen in bepaalde richtingen gedurende een bepaalde periode, waarbij een identificatiecode nodig zou zijn om de posities van individuele personen op bepaalde tijdstippen met elkaar te verbinden. Uit dit voorbeeld blijkt dat de overweging een verdere verwerking van die gegevens ter ondersteuning van "big data"-analyses wettigt. De enige voorwaarde die in de voorgestelde verordening voor dat soort verwerking wordt gesteld, is de verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren indien de verwerking "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen". Die voorwaarde is ontoereikend en in strijd met de verplichting in art. 6, op grond waarvan een dergelijke verwerking alleen kan plaatsvinden wanneer de gebruikers hun toestemming hebben gegeven en de gegevens niet anoniem kunnen worden gemaakt, d.w.z. geen identificatiecode bevatten. Gebruikers kunnen vaak de verzameling van hun geolocatiegegevens door de aanbieders van elektronischecomunicatiediensten niet weigeren, omdat een dergelijke verzameling technisch noodzakelijk kan zijn om communicatie over te brengen naar de gebruiker of omdat een dergelijke verzameling noodzakelijk is om de gevraagde dienst (bijvoorbeeld navigatie) te verlenen. In vorige adviezen heeft de Groep geconcludeerd dat dergelijke locatiegegevens van slimme apparatuur gevoelige persoonsgegevens zijn en dat de voordelen van het analyseren van deze gegevens niet opwegen tegen de rechten van de gebruikers op bescherming van de vertrouwelijkheid van de metagegegevens van hun communicatie, noch tegen hun algemene rechten op gegevensbescherming op grond van de algemene verordening gegevensbescherming. Bijgevolg moet in de overweging op zijn minst worden verduidelijkt dat aanbieders moeten voldoen aan de verplichtingen in art. 25 van de algemene verordening gegevensbescherming indien ze locatiegegevens of andere metagegegevens verder verwerken. Hiertoe dienen ten minste de volgende maatregelen te worden genomen:

- i) het gebruik van tijdelijke pseudoniemen;
- ii) het wissen van omgekeerde opzoektabelen tussen deze pseudoniemen en de originele identificerende gegevens;
- iii) aggregeren van gegevens tot een niveau waarop de individuele gebruikers niet meer kunnen worden geïdentificeerd aan de hand van hun specifieke routes;
- iv) het wissen van uitschieters die nog altijd zouden kunnen worden geïdentificeerd (alle maatregelen moeten samen worden toegepast).

Tot slot moet de e-privacyverordening de verplichting bevatten voor de partijen die betrokken zijn bij de verwerking van locatie- en andere metagegevens om hun methoden voor het anoniem maken en verder aggregeren van de gegevens bekend te maken, zonder echter afbreuk te doen aan het bij wet beschermde recht op geheimhouding. Op die manier kunnen de toezichthoudende autoriteiten en het brede publiek gemakkelijk nagaan of de gekozen methode passend is.

#### *VERDUIDELIJKING MET BETREKKING TOT ONGEWENSTE COMMUNICATIE*

43. De Groep stelt voor het volgende te verduidelijken met betrekking tot ongewenste communicatie:

a. **De formulering van het verbod op direct marketing zonder toestemming.**

In art. 16, lid 1, van de voorgestelde verordening wordt nu opgemerkt dat elektronischecomunicatiediensten "kunnen" worden gebruikt voor de verzending van directmarketingberichten (met toestemming), maar er is in dat artikel geen uitdrukkelijk verbod opgenomen op het verzenden (of richten aan of presenteren) van direct marketing zonder toestemming. Dat staat in contrast met de benadering in de andere bepalingen, waar eerst een verbod wordt geformuleerd, en vervolgens bepaalde specifieke uitzonderingen. De huidige formulering wijst op een meer soepele benadering, wat wellicht niet de bedoeling is. De Groep stelt voor om de formulering van het huidige art. 16, lid 1, van de e-privacyrichtlijn licht aan te passen: "Het gebruik door natuurlijke of rechtspersonen van elektronischecomunicatiediensten, met inbegrip van spraakoproepen, automatische oproep- en communicatiesystemen, met inbegrip van halfautomatische systemen die de opgeroepen persoon verbindt met een persoon, faxtoestellen, elektronische post of andere gebruiken van elektronischecomunicatiediensten, om directmarketingberichten aan eindgebruikers te verstrekken mag uitsluitend worden toegestaan indien de eindgebruikers voorafgaand hun toestemming hebben gegeven."

b. **Het toepassingsgebied van de bepalingen inzake marketingberichten en -oproepen aan bestaande contacten.**

In artikel 16, lid 2, is bepaald dat wanneer een persoon van een bestaande klant elektronische contactgegevens voor elektronische post heeft verkregen, hij deze gegevens mag gebruiken voor verdere direct marketing van eigen producten en diensten indien de klant op het tijdstip van de gegevensverzameling en telkens wanneer een bericht wordt verzonden duidelijk in de gelegenheid wordt gesteld om kosteloos en op gemakkelijke wijze bezwaar te maken. Dat is momenteel

beperkt tot handelscontacten "in het kader van de verkoop van een product of een dienst" en voor verdere commerciële marketing van soortgelijke eigen producten en diensten. Aangezien de bepalingen inzake direct marketing in gelijke mate van toepassing zijn op niet-commerciële promotieactiviteiten (van bijvoorbeeld liefdadigheidsorganisaties of politieke partijen), moet deze bepaling zo worden gewijzigd dat ze in gelijke mate van toepassing is op niet-commerciële organisaties die zich voor de promotie van soortgelijke eigen doelstellingen of idealen willen richten tot vroegere aanhangers, en moet hetzelfde recht op bezwaar maken gelden voor directmarketingoproepen. Daarnaast moet een termijn worden vastgesteld voor de geldigheid van "bestaande klantencontacten" in elektronische communicatie voor commerciële, liefdadigheids- of politieke doeleinden. Die termijn moet ook gelden voor directmarketingoproepen. In lidstaten waar een systeem bestaat om bezwaar te maken tegen spraakoproepen door bijvoorbeeld registratie in een bel-me-niet-register, is deze ondergeschikt aan de aanwezigheid van "contactgegevens van een bestaande klant". In die omstandigheden hebben eindgebruikers geen doeltreffende mogelijkheid om ongewenste oproepen te voorkomen van bedrijven of organisaties waarmee ze ooit contact hebben gehad, maar niets meer mee te maken willen hebben. Daarom moet, als vuistregel en overeenkomstig de gerechtvaardigde verwachtingen van de betrokken eindgebruikers, in de verordening een geldigheidstermijn worden vastgesteld voor deze uitzondering van "bestaande klant", bijvoorbeeld een of twee jaar.

- c. **De toepassing van directmarketingregels op rechtspersonen.** In art. 16, lid 5, van de voorgestelde verordening staat dat de lidstaten ervoor zorgen dat de rechtmatige belangen van eindgebruikers die rechtspersonen zijn, met betrekking tot ongewenste communicatie, voldoende worden beschermd. In art. 13, lid 5, van de huidige e-privacyrichtlijn zijn de rechtmatige belangen van andere abonnees dan natuurlijke personen beschreven. Het is onduidelijk welke gevolgen deze andere formulering met zich meebrengt. Het moet in de overwegingen worden verduidelijkt dat het niet de bedoeling is om met deze wijziging het beschermingsniveau te verlagen. In verband hiermee moet worden opgemerkt dat het verbod op direct marketing zonder toestemming betrekking heeft op "eindgebruikers die natuurlijke personen zijn, die hun toestemming hebben gegeven" (nadruk toegevoegd). Er moet worden verduidelijkt dat dit natuurlijke personen omvat die *in dienst zijn van* rechtspersonen. Anderzijds zou toestemming niet vereist zijn om rechtspersonen te benaderen via algemene contactgegevens die ze voor dit doeleinde hebben bekendgemaakt (zoals "info@bedrijfsnaam.eu").
- d. **De toepassing van directmarketingregels op personen in een (politiek) vertegenwoordigende hoedanigheid:** Het huidige ontwerp van artikel 16 kan voorkomen dat sommige berichten naar verkozen vertegenwoordigers worden verzonden als er commerciële belangen mee gepaard gaan. Er moet worden verduidelijkt dat de verordening dat niet doet.

44. **De toepassing van het Handvest en het EHRM op nationale gegevensbewaringswetten** moet worden verduidelijkt. In overweging 26 staat dat maatregelen van lidstaten ter bescherming van openbare belangen, zoals wettelijk toegestane interceptiemaatregelen, in overeenstemming moeten zijn met het Handvest (en met het EHRM). Dat is wenselijk, want volgens de redenering in *Tele2 Sverige* moeten nationale uitzonderingen op de EU-wetgeving inzake bescherming bij gegevensverwerking in overeenstemming zijn met het Handvest (en kunnen inbreuken via nationale wetten dus voor het Hof van Justitie van de EU worden gebracht). In artikel 11 van de voorgestelde verordening wordt echter gewoon vermeld dat beperkingen van het toepassingsgebied van art. 5 tot en met 8 van de voorgestelde verordening in overeenstemming moeten zijn met de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en een noodzakelijke, passende en evenredige maatregel moeten zijn. Een uitdrukkelijke verwijzing naar het Handvest en het EHRM moet hier worden ingevoegd.
45. **Dat de vertrouwelijkheid van communicatie ook is beschermd op grond van art. 8 EHRM.** In paragraaf 1.1 van de toelichting en in overweging 1 wordt uitgelegd dat de voorgestelde verordening uitvoering geeft aan art. 7 van het Handvest. Dat wordt herhaald in overweging 19. Het grondrecht inzake vertrouwelijke communicatie wordt echter niet alleen in die bepaling beschermd, maar ook in art. 8 EHRM. Door een uitdrukkelijke verwijzing op te nemen in een artikel van de voorgestelde verordening zou nogmaals worden bevestigd dat bij de beoordeling van de (definitieve) verordening ook moet worden rekening gehouden met desbetreffende rechtspraak van het Europees Hof voor de Rechten van de Mens. Die verwijzing is eigenlijk al opgenomen in overweging 20 (met betrekking tot eindapparatuur) en overweging 26 (met betrekking tot wettelijk toegestane interceptie) en verder ondersteund door de overwegingen in par. 2.1 van de toelichting (over het verband tussen het Handvest en het EHRM voor rechtspersonen), maar niet in een desbetreffend artikel, zoals artikel 11, lid 1.

#### ANDERE VERDUIDELIJKINGEN

46. Er moet worden verduidelijkt dat **de verplichtingen op grond van de algemene verordening gegevensbescherming, zoals inzake de regeling voor inbreuken in verband met persoonsgegevens en gegevensbeschermingseffectbeoordelingen, van toepassing blijven** wanneer partijen persoonsgegevens verwerken in het kader van elektronischecomunicatiegegevens. Aangezien in overweging 5 wordt opgemerkt dat de voorgestelde verordening een *lex specialis* is bij de algemene verordening gegevensbescherming en dat de verwerking van elektronischecomunicatiegegevens alleen mag worden toegestaan in overeenstemming met de voorgestelde verordening, kan de vraag worden gesteld of bepaalde verplichtingen in de algemene verordening gegevensbescherming ook van toepassing zijn in de context van de voorgestelde verordening. Dat is voornamelijk het geval wanneer de voorgestelde verordening zou voorzien in een bepaalde verplichting waarin ook de algemene verordening gegevensbescherming voorziet. Een paar voorbeelden ter illustratie:

- (i) in de voorgestelde verordening is een meldingsverplichting opgenomen voor "geconstateerde" veiligheidsrisico's (art. 17) (zie ook opmerking 35), maar de algemene verordening gegevensbescherming bevat een meldingsregeling voor inbreuken in verband met persoonsgegevens (art. 33 en 34);
- (ii) in de voorgestelde verordening staat dat de verrichting van een effectbeoordeling inzake gegevensbescherming en de raadpleging van de toezichthoudende autoriteit overeenkomstig de algemene verordening gegevensbescherming verplicht is in bepaalde omstandigheden (overwegingen 17 en 19 en art. 6, lid 3, onder b)), terwijl in de algemene verordening gegevensbescherming al is vastgesteld wanneer een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd en wanneer raadpleging is vereist (art. 35 en 36);
- (iii) het is niet duidelijk vermeld dat indien wordt voldaan aan de noodzakelijke voorwaarden van een uitzondering op de verwerkingsverplichting in art. 5 van de voorgestelde verordening, ook nog moet worden voldaan aan alle desbetreffende verplichtingen in de algemene verordening gegevensbescherming in het geval van verwerking van persoonsgegevens en wanneer andere vormen van verwerking op grond van de algemene verordening gegevensbescherming zijn verboden. Er moet worden verduidelijkt dat de verenigbaarheidstest die is vastgesteld in art. 6, lid 4, van de algemene verordening gegevensbescherming bijgevolg niet van toepassing is;
- (iv) de voorgestelde e-privacyverordening voorziet niet in soortgelijke certificeringsmechanismen als die in artikelen 42 en 43 van de algemene verordening gegevensbescherming. Aangezien het toepassingsgebied van artikel 42 van de algemene verordening gegevensbescherming strikt genomen beperkt is tot de invoering van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens waarmee kan worden aangetoond dat aan de algemene verordening gegevensbescherming is voldaan, moet worden nagegaan of geen vergelijkbare bepaling kan worden ingevoerd zodat verwerkingsactiviteiten, -normen, -producten of -diensten kunnen worden gecertificeerd met betrekking tot hun overeenstemming met de e-privacyverordening.

Om te vermijden dat deze onduidelijkheid wordt gebruikt als argument om het niveau van bescherming op grond van de voorgestelde verordening te verlagen, moet worden verduidelijkt dat verwerkingsverantwoordelijken in al die gevallen ook moeten voldoen aan de algemene verordening gegevensbescherming.

47. Er moet ook worden verduidelijkt dat **de vereiste voor de intrekking van toestemming ook van toepassing is in het kader van interferentie met eindapparatuur**. In art. 8, lid 1, onder b), van de voorgestelde verordening is de mogelijkheid opgenomen voor interferentie met de eindapparatuur van eindgebruikers mits zij toestemming hebben gegeven. In art. 9, lid 3, wordt vereist dat eindgebruikers in de gelegenheid worden gesteld om hun toestemming te allen tijde in te trekken, maar deze vereiste is slechts van toepassing op toestemming voor de analyse van metagegevens en inhoud. Er moet worden verduidelijkt dat deze verplichting ook geldt voor interferentie met eindapparatuur.



48. In verband hiermee moet worden verduidelijkt dat **de andere mogelijkheden om toestemming in te trekken ook van toepassing zijn op toestemming via browserinstellingen**. Art. 9, lid 3, bevat de vereiste dat eindgebruikers periodiek om de zes maanden worden herinnerd aan de mogelijkheid om hun toestemming te allen tijde in te trekken. Hoewel de algemene instellingen van browsers en andere software, met inbegrip van besturingssystemen, apps en software-interfaces voor apparaten die zijn aangesloten op het internet van de dingen (die niet zijn gebaseerd op specifieke, gedetailleerde controle), volgens de Groep niet als een geldige maatregel voor het verlenen van toestemming kan worden beschouwd, aangezien algemene instellingen niet geschikt zijn om specifiek toestemming te geven voor specifieke scenario's (zie opmerking 24), is zij van mening dat standaardinstellingen gebruiksvriendelijk moeten zijn (zie opmerking 19). *Als* die bepaling in de voorgestelde verordening blijft, moeten de instellingen gedetailleerd genoeg zijn zodat alle vormen van gegevensverwerking waarmee de gebruiker toestemt, kunnen worden gecontroleerd, en alle functies van de apparatuur omvatten die tot gegevensverwerking zouden kunnen leiden. Daarnaast moet de eindgebruiker ten minste periodiek om de zes maanden worden herinnerd aan de mogelijkheid om deze instellingen te wijzigen.
49. Het is positief dat op grond van de voorgestelde verordening voor de software die al in de handel is de eindgebruiker moet worden geïnformeerd over de privacyinstellingen van die software (art. 10). **Het is echter onduidelijk hoe dat doeltreffend kan worden toegepast op bestaande producten** en andere die niet langer worden ondersteund. Bovendien moet worden verduidelijkt hoe deze verplichting van toepassing zal zijn op opensourcesoftware, die is ontwikkeld om op een open, gedecentraliseerde manier te worden beheerd.
50. Er moet worden verduidelijkt dat **het aanbieden van de mogelijkheid om cookies (van derden) te blokkeren op grond van art. 10 van de voorgestelde verordening voorrang krijgt op de uitzondering betreffende het meten van de omvang van het publiek** op grond van art. 8, lid 1, onder d). Een website die via analyses de omvang van het publiek meet op grond van art. 8, lid 1, onder d), moet met andere woorden de gebruikers nog steeds het recht verlenen om deze traceertechnologieën in hun browser te blokkeren.
51. De **definitie van (half)automatische oproep- en communicatiesystemen moet worden verduidelijkt**. De definitie van deze term in art. 4, lid 3, onder h), van de voorgestelde verordening bevat in het tweede deel van de zin een verwijzing naar de term zelf ("met inbegrip van oproepen waarbij gebruik wordt gemaakt van automatische oproep- en communicatiesystemen die de opgeroepen persoon in verbinding stellen met een persoon"). Er wordt voorgesteld deze laatste zin uit de definitie te schrappen en in de definitie in art. 4, lid 3, onder g), de oproepen op te nemen die tot stand komen met behulp van halfautomatische communicatiesystemen, zoals automatische dialers, die de opgeroepen persoon in verbinding stellen met een persoon.
52. De **informatie "die deel uitmaakt van de inschrijving op de dienst" moet worden verduidelijkt**. In overweging 14 wordt vermeld dat tot de elektronischecommunicatiemetagegevens "ook de informatie [kan] worden gerekend

die deel uitmaakt van de inschrijving op de dienst, wanneer deze informatie verwerkt wordt met het oog op de transmissie, de distributie of de uitwisseling van elektronischecommunicatie-inhoud". Het is niet duidelijk wat met deze formulering wordt bedoeld.

53. **De toepasselijkheid van de mechanismen voor samenwerking en coherentie** moet worden verduidelijkt. In overweging 38 wordt opgemerkt dat de voorgestelde verordening berust op het coherentiemechanisme van de algemene verordening gegevensbescherming. Daarnaast is in art. 18, lid 1, bepaald dat hoofdstukken VI en VII van de algemene verordening gegevensbescherming mutatis mutandis van toepassing zijn. In art. 19 wordt ook opgemerkt dat het Europees Comité voor gegevensbescherming de taken uitoefent die zijn vastgesteld in art. 70 van de algemene verordening gegevensbescherming. Hoewel de toepassing van deze bepalingen relatief duidelijk is, kan niet worden uitgesloten dat er vragen zullen rijzen over de uitlegging van de kernbegrippen "mechanismen voor samenwerking en coherentie" op grond van de algemene verordening gegevensbescherming. Zo is het mechanisme van de leidende toezichthoudende autoriteit van toepassing in het geval van "grensoverschrijdende verwerking" (art. 56, lid 1, van de algemene verordening gegevensbescherming), maar is het onzeker hoe dit van toepassing is in het geval van interferentie met eindapparatuur of analyse van inhoud en metagegevens op grond van de voorgestelde verordening. Het is bijgevolg raadzaam om de toepassing van deze kernbegrippen te verduidelijken in een overweging en te benadrukken dat overige problemen met betrekking tot de toepasselijkheid van deze hoofdstukken van de algemene verordening gegevensbescherming in het kader van de voorgestelde verordening moeten worden opgelost door de bepalingen van deze hoofdstukken uit te leggen in samenhang met hun bedoeling. Daarnaast is het raadzaam om te verduidelijken dat art. 70 mutatis mutandis van toepassing is op het Europees Comité voor gegevensbescherming in het kader van de voorgestelde verordening (dit ontbreekt nu in de overweging).

\* \* \*