

Vergaderjaar 2011–2012

32 549

Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen

32 403

Wijziging van de Wegenverkeerswet 1994 op een aantal punten van uiteenlopende aard, van de Wet personenvervoer 2000 ten aanzien van het openbaar-vervoerverbod en enkele technische wijzigingen, van de Wet advies en overleg verkeer en waterstaat in verband met wijzigingen in de vorm waarin betrokkenen en organisaties bij het beleidsproces worden betrokken, wijziging van de Wet op de economische delicten, de Wet luchtvaart, de Binnenvaartwet, de Wet capaciteitsbeheersing binnenvaartvloot, de Wet belastingen op milieugrondslag, de Waterwet, de Invoeringswet Waterwet, de Waterschapswet en de Crisis- en herstelwet op enkele punten van technische aard, alsmede van de Telecommunicatiewet ter herstel van een abuis (Verzamelwet Verkeer en Waterstaat 2010)

G¹

NADERE MEMORIE VAN ANTWOORD

Ontvangen 17 februari 2012

Met belangstelling heb ik kennis genomen van de vragen van de leden van de fracties van het CDA en de VVD in het nader voorlopig verslag. Bij de beantwoording van de vragen hanteer ik de in het nader voorlopig verslag gebruikte indeling op onderwerp.

Cookies

Het voorgestelde artikel 11.7a strekt tot implementatie van het gewijzigde artikel 5, derde lid, van de Bijzondere privacyrichtlijn. De leden van de fracties van het CDA en de VVD hebben hierover vragen gesteld in het nader voorlopig verslag. De leden van de VVD-fractie hebben signalen ontvangen dat in enkele EU-lidstaten de instellingen van de huidige browsers voldoende worden geacht om toestemming voor het plaatsen en lezen van cookies te veronderstellen. Deze leden vragen of het juist is dat andere lidstaten van de EU de richtlijnbevestiging zo implementeren of interpreteren dat zij minder zware eisen stellen om te voldoen aan het

¹ De letter G heeft alleen betrekking op wetsvoorstel 32 549.

toestemmingsvereiste. Deze leden vragen tevens naar de gevolgen voor de concurrentiepositie van Nederland en voor de concurrentiepositie van Nederlandse ondernemingen.

Ik wil vooropstellen dat het van het allergrootste belang is dat binnen de Europese Unie geen interpretatieverschillen bestaan over de richtlijnbe-
paling. Interpretatieverschillen zijn natuurlijk altijd al ongewenst als er voor bepaalde diensten geharmoniseerde regels gelden. Maar voor een dienst als internet, die naar zijn aard geen landsgrenzen kent, geldt dat misschien nog wel sterker. En juist daarom is te betreuren dat over de interpretatie van deze bepaling in de Bijzondere privacyrichtlijn nog zoveel discussie gaande is. Maar we kunnen in verband met de implementatie-termijn de uitkomst van die discussie niet afwachten, en daar vraag ik de leden van de Eerste Kamer begrip voor. Van mijn kant begrijp ik de zorgen die er leven.

De regering heeft er daarom voor gekozen om met de tekst van artikel 11.7a zo dicht mogelijk bij de richtlijntekst te blijven, om te voorkomen dat de Nederlandse wettekst afwijkt van de Europese regelgeving op dit punt. Helaas bestaat er, zoals de leden van de fractie van de VVD ook aangeven, geen communis opinio binnen de EU over de precieze uitleg van artikel 5, derde lid, van de Bijzondere privacyrichtlijn. In de lidstaten is in het bijzonder nog onduidelijkheid over hoe in de praktijk de vereiste toestemming zou moeten worden verkregen. De actuele stand van zaken ten aanzien van de manier waarop artikel 5, derde lid, van de Bijzondere privacyrichtlijn in de verschillende lidstaten is of wordt geïmplementeerd is onlangs in kaart gebracht door de Europese Commissie. Uit deze inventarisatie blijkt dat de meeste lidstaten, net als Nederland, de letterlijke tekst van de richtlijnbe-
paling volgen in hun implementatie. De meeste lidstaten geven geen expliciete toelichting op hoe de vereiste toestemming zou moeten en kunnen worden verkregen. Er zijn wel landen die uitdrukkelijk wijzen op de in overweging 66 bij de Richtlijn Burgerrechten genoemde mogelijkheid om, indien technisch mogelijk en doeltreffend, de vereiste toestemming via de browser te verkrijgen. Maar dit betekent niet dat deze lidstaten beweren dat de huidige browsers al geschikt zijn om op de door de richtlijn vereiste manier toestemming te verkrijgen, of dat deze lidstaten een eenduidige opvatting hebben over hoe in de praktijk uitvoering kan worden gegeven aan het toestemmings-
vereiste. Nederland wijkt hierin dus niet af van de meeste lidstaten. Er lijken echter ook enkele lidstaten te zijn, waarin voor bepaalde soorten cookies (cookies die niet voor persoonsgerichte reclame worden gebruikt) een opt-outmogelijkheid voldoende zou zijn. Echter, gelet op de tekst van de richtlijnbe-
paling is het bieden van een mogelijkheid het gebruik van cookies te weigeren onvoldoende, zoals bevestigd is door de Artikel 29-werkgroep in haar Opinion van 22 juni 2010¹, en door Europees Commissaris voor de Digitale Agenda Neelie Kroes in haar blog². Over het algemeen bevestigt de door de Commissie verzamelde informatie mijn indruk dat in de verschillende lidstaten de discussie over de toepassingspraktijk nog volop gaande is. Hoopgevend is dat de Europese Commissie alles in het werk stelt om samen met het bedrijfsleven (makers van browsers en partijen die cookies gebruiken) te komen tot een gebruiksvriendelijke oplossing, die voldoet aan de eisen in de richtlijn. OPTA zal er in haar toezicht op letten dat zij niet afwijkt van de uitleg die in de andere lidstaten aan de richtlijnbe-
paling gegeven wordt. Ik geef toe dat deze aanpak niet de schoonheidsprijs verdient. Natuurlijk zou het beter zijn geweest als de Europese discussie bij de totstandkoming van de Richtlijn Burgerrechten volledig zou zijn afgerond. Maar deze constatering doet niet af aan het feit dat die Europese wetgeving wel zo snel mogelijk moet worden geïmplementeerd.

Tegen deze achtergrond stel ik voor dat OPTA, zolang binnen de EU geen consensus is bereikt over de precieze interpretatie van de Bijzondere privacyrichtlijn, terughoudend toezicht houdt en er daarbij zorg voor

¹ Article 29 Data Protection Working Party, Opinion 2/2010 on Online Behavioural Advertising, zie: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

² «Why we need a sound Do-Not-Track standard for privacy online», Eurocommissaris Neelie Kroes (Digitale Agenda), 20 januari 2012, zie: <http://blogs.ec.europa.eu/neelie-kroes/donottrack/>

draagt dat Nederland niet uit de pas loopt met de overige EU-landen. Zodra die consensus er wel is, kan de OPTA zo nodig met beleidsregels een nadere invulling geven. Ook kan er nadere regelgeving komen op grond van het vierde lid van het voorgestelde artikel 11.7a.

De leden van de VVD-fractie vragen de regering of verwacht wordt dat nieuwe browsers, waarbij de gebruiker zelf moet aangeven of hij al dan niet cookies wil laten plaatsen op zijn apparatuur, wel geschikt zijn om te voldoen aan het toestemmingsvereiste.

De richtlijn eist dat voor het mogen plaatsen of lezen van een cookie de gebruiker geïnformeerde toestemming moet hebben gegeven. Veel hangt af van welke keuzemogelijkheden via browsers kunnen worden aangeboden, en de informatie die de gebruiker wordt aangeboden om een bewuste en geïnformeerde keuze te kunnen maken. De Artikel 29-werkgroep in haar Opinion van 8 december 2011¹, en Europees Commissaris Kroes in haar reeds aangehaalde blog² beschrijven dat de mogelijkheden die op dit moment in bestaande browsers worden geboden nog niet toereikend zijn. De huidige browsers staan standaard ingesteld op «cookies accepteren». In die situatie kan iemand die cookies wil plaatsen of lezen er niet vanuit gaan dat de gebruiker door het enkele feit dat cookies niet worden tegengehouden door de browser, toestemming heeft gegeven. Maar het is wel de verwachting dat uiteindelijk de vereiste toestemming via de browserinstellingen zal kunnen worden verkregen. Hierbij wordt gewezen op de door de Europese Commissie aangemoedigde inspanningen van aanbieders van internetbrowsers om hun browsers op dit punt te verbeteren (zie bijvoorbeeld de activiteiten van het World Wide Web Consortium: www.w3c.org/TR/tracking-dnt/).

De leden van de fractie van de VVD vragen of het op alternatieve wijze, althans anders dan via browserinstellingen, vragen van toestemming inherent (technische) kosten met zich meebrengt. Voor een partij die cookies wil plaatsen kan het vragen om toestemming inderdaad extra kosten met zich meebrengen. Het kan namelijk nodig zijn om de website en de achterliggende software hiervoor aan te passen. Ik zou ook het liefst zien dat via de browserinstellingen toestemming zou kunnen worden gevraagd op de manier die de richtlijn voorschrijft. Dit vergroot niet alleen het gebruiksgemak, maar leidt ook tot kostenbesparing voor partijen die gebruik willen maken van cookies waarvoor informatieverstrekking en toestemming vereist is.

De leden van de CDA-fractie vragen naar de visie van de regering omtrent de door de Artikel 29-Werkgroep in haar Opinion 16/2011 voorgestelde praktische oplossingen om een goed nalevingsniveau van de richtlijn te verenigen met de ervaringen van gebruikers.

Zoals gezegd wil ik niet te veel vooruitlopen op de discussie over wat nog wel en wat niet meer aan de richtlijn voldoet, maar de door de Artikel 29-Werkgroep voorgestelde oplossingen lijken in ieder geval wel te voldoen aan de eisen die de richtlijn stelt aan het plaatsen en lezen van cookies. In de praktijk zal moeten blijken of de oplossingen bruikbaar zijn, of dat er door bijvoorbeeld ontwikkelaars van browsers gebruiksvriendelijkere oplossingen kunnen worden bedacht die aan de richtlijneisen voldoen.

De leden van de VVD-fractie vragen welke gevolgen de cookiebepaling heeft op het gelijke speelveld tussen internetondernemingen onderling. Het klopt dat grote partijen als Google een schaalvoordeel kunnen hebben bij het vragen om toestemming voor het plaatsen en lezen van cookies. Maar bij economische activiteiten is het ook niet ongebruikelijk dat grote partijen schaalvoordelen kunnen bereiken. Ik merk hierbij op dat kleinere

¹ Article 29 Data Protection Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, zie: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

² Zie voetnoot 2.

partijen zich zouden kunnen organiseren en door samenwerking ook van schaalvoordelen kunnen profiteren.

De leden van de VVD-fractie vragen welke gevolgen de cookiebepaling heeft op het gelijke speelveld tussen internetondernemingen en andere mediabedrijven. De leden van de VVD- en de CDA-fractie gaan er vanuit dat andere mediabedrijven wel in staat zijn om zonder toestemming het gedrag van gebruikers te volgen, bijvoorbeeld door het kijkgedrag van hun klanten te volgen en daarop afgestemde advertenties aan te bieden. Artikel 11.7a is niet alleen van toepassing op het plaatsen en lezen van cookies op computers van internetgebruikers: de informatieverplichting en het toestemmingsvereiste gelden voor alle gegevens die door middel van elektronische communicatienetwerken worden opgeslagen in of gelezen van alle soorten randapparatuur van een gebruiker. Stel dat een aanbieder van (digitale) kabeltelevisie, zoals Ziggo of UPC, het kijkgedrag van kabeltelevisie-abonnees vastlegt. De kennis van dat kijkgedrag zou de kabelexploitant dan in staat stellen om individuele abonnees aanbeidingen te doen die passen bij zijn kijkgedrag, of om een abonnee specifiek op hem gerichte reclame of informatie aan te bieden. Als dat gebeurt door informatie uit te lezen die is vastgelegd in randapparatuur (zoals de digitale decoder), dan is artikel 11.7a gewoon van toepassing. Het is dan ook niet nodig hierover een soortgelijke bepaling in de Mediawet op te nemen, zoals de leden van de fractie van het CDA voorstellen.

De leden van de VVD-fractie verwijzen naar de brief van de Staatssecretaris van Veiligheid en Justitie aan de Tweede Kamer d.d. 20 december 2011. Zij vragen of de argumenten van de Staatssecretaris van Veiligheid en Justitie om de verwerking van persoonsgegevens via wifi-routers niet afhankelijk te maken van uitdrukkelijke toestemming, naar analogie zouden moeten gelden voor de cookiebepaling of de uitleg daarvan. Zoals de genoemde brief vermeldt, wordt in geen enkel ander land in de EU vaststelling van een wettelijke toestemmingseis voor het gebruik van wifi-routergegevens overwogen. Ten aanzien van het plaatsen en lezen van gegevens op randapparatuur van gebruikers is wel Europees bepaald dat hiervoor geïnformeerde toestemming vereist is. Het verwerken van statische wifi-routergegevens vormt ook een veel minder grote inbreuk op de persoonlijke levenssfeer dan het plaatsen of lezen van gegevens op de computer van een internetgebruiker, al helemaal als daarbij het surfgedrag wordt gevolgd.

De leden van de VVD-fractie vragen op welke wijze de persoon die een cookie plaatst, kan bewijzen dat de internetgebruiker hiervoor toestemming heeft gegeven.

Het is primair aan OPTA als toezichthouder om in een concreet geval te bepalen hoe degene die cookies heeft geplaatst moet bewijzen dat hij daarvoor de vereiste toestemming van de gebruiker heeft verkregen. OPTA kan hierbij aansluiting zoeken bij het geldende bewijsrecht en de ervaring die is opgedaan met het toestemmingsvereiste in de Wet bescherming persoonsgegevens (hierna: Wbp).

De leden van de CDA-fractie achten het aannemelijk dat Nederland met het door de Tweede Kamer geamendeerde artikel 11.7a vermoedelijk enigszins verder gaat dan veel andere lidstaten. Zij wijzen erop dat buitenlandse toezichthouders immers alleen toezicht kunnen houden op de in hun nationale recht neergelegde implementatie van de richtlijn-bepaling en niet op basis van de Nederlandse interpretatie. Daar waar de Nederlandse interpretatie tot strengere toepassing leidt, zal bij websites die vanuit andere landen worden aangeboden dan ook materieel anders toezicht worden gehouden.

In de memorie van antwoord is betoogd dat de uiteindelijke tekst van artikel 11.7a, zoals dat luidt na aanneming van de aangepaste versie van het amendement, materieel niet afwijkt van de Europese wetgeving. De tekst van artikel 11.7a geeft dan ook geen aanleiding voor een afwijkende, strengere, interpretatie van artikel 5, derde lid, van de Bijzondere privacyrichtlijn. Ook de verwijzing naar de Wbp (het hieronder besproken rechtsvermoeden) maakt niet dat een strenger regime van toepassing is dan in andere landen, omdat in de andere lidstaten ook de in de Wbp geïmplementeerde Algemene privacyrichtlijn geldt. Ik verwacht daarom niet dat artikel 11.7a, ook met het rechtsvermoeden dat hier in is opgenomen, in de praktijk zal leiden tot verschillen tussen Nederland en de andere lidstaten. Hier ga ik in het antwoord op de volgende vraag nog dieper op in.

De leden van de CDA-fractie vragen in verband met dit rechtsvermoeden wat de gevolgen zijn voor het gebruik van analytics cookies. Zoals ik in de memorie van antwoord al aangaf zal dit per geval verschillen. Wanneer van het gebruik van analytics cookies in een bepaald geval gezegd kan worden dat dit noodzakelijk is voor het goed kunnen functioneren van de door de gebruiker bezochte site, valt dit gebruik van analytics cookies onder de uitzondering in het derde lid van artikel 11.7a. Het toestemmingsvereiste en het rechtsvermoeden in het eerste lid zijn in dat geval niet van toepassing. In gevallen die niet onder de uitzondering vallen, geldt het vermoeden dat met het gebruik van analytics cookies persoonsgegevens worden verwerkt alleen wanneer de cookies het surfgedrag over *meerdere* sites volgen. Benadrukt wordt dat dit slechts een rechtsvermoeden is. Het is niet zo dat analytics cookies in Nederland eerder onder het regime van de Wbp vallen dan in de overige lidstaten, die dit rechtsvermoeden naar mijn weten niet kennen. Immers, als de gebruiker van analytics cookies, als hij hierop wordt aangesproken door de toezichthouder, kan aantonen dat hij geen persoonsgegevens verwerkt, valt hij net als in andere lidstaten niet onder de Wbp. Verwerkt hij daarentegen wél persoonsgegevens, dan is in alle lidstaten de Wbp of een buitenlandse equivalent op deze verwerking van toepassing. Het rechtsvermoeden zorgt er dus niet voor dat Nederland een zwaarder regime hanteert.

De leden van de CDA-fractie vragen hoe ten aanzien van *device fingerprinting* met de cookiebepaling moet worden omgegaan. *Device fingerprinting* kan worden gebruikt om het surfgedrag van individuele internetgebruikers te volgen. Als met een computer of mobiele telefoon een website wordt bezocht, geeft de browser bepaalde instellingen en kenmerken van het apparaat (computer, mobiele telefoon) door aan die website. Te denken valt aan het type besturingssysteem, de browserinstellingen, geïnstalleerde plug-ins, tijdzone en beeldschermgrootte en dergelijke. Deze combinatie van instellingen en kenmerken (de «device fingerprint») is zo specifiek, dat een adverteerder die via verschillende sites dezelfde fingerprint aantreft, er met redelijke mate van zekerheid vanuit kan gaan dat het gaat om dezelfde computer, en dus dezelfde internetgebruiker. Als deze adverteerder bijvoorbeeld op verschillende sites advertentiebanner plaatst, kan hij de fingerprints van de computers waarmee die sites zijn bezocht verzamelen. Door die gegevens te analyseren kan hij afleiden welke sites de (verder ongeïdentificeerde) bezoeker achter een bepaalde fingerprint heeft bezocht. Hierbij wordt dus surfgedrag gevolgd aan de hand van informatie die wordt gelezen van de computer van een gebruiker. Artikel 11.7a is niet alleen van toepassing op het plaatsen van gegevens op de randapparatuur van een gebruiker, maar ook op het verkrijgen van toegang tot gegevens die

zijn opgeslagen in de randapparatuur van een gebruiker. Ook het gebruik van device fingerprinting valt daarom onder artikel 11.7a. Deze conclusie wordt overigens gedeeld door de Artikel 29-werkgroep in Opinion 16/2011¹. Het lezen van de combinatie van instellingen en kenmerken van het apparaat met als uitsluitend doel de met dat apparaat opgevraagde dienst te leveren (bijvoorbeeld om de bezochte website goed te kunnen weergeven) valt onder de uitzondering in het derde lid. Het lezen van deze informatie om het surfgedrag van de gebruiker van het apparaat te volgen valt niet onder de uitzondering. Hiervoor is dan ook geïnformeerde toestemming van de gebruiker vereist.

Netneutraliteit

De leden van de CDA-fractie stellen dat het systeem van white-listing, waarin blokkeren of vertragen altijd verboden is, behalve als het onder een in de wet genoemde uitzondering valt, het grote gevaar in zich heeft dat nu nog onvoorziene ontwikkelingen in de toekomst worden belemmerd. Zo zou vooral bij mobiele datadiensten de bepaling over netneutraliteit met zich mee kunnen brengen dat diensten die elders in Europa ontwikkeld worden in Nederland mogelijk in strijd zijn met de wet. Met het voorgestelde artikel 7.4a wordt het beginsel van netneutraliteit stevig in de wet verankerd. Het artikel is inderdaad geformuleerd als algemeen verbod, waarop alleen een uitzondering kan worden gemaakt in de bij wet genoemde gevallen. In de uitzonderingen is aangeduid in welke situaties belemmering of vertraging van verkeer door de aanbieder geen bezwaar oplevert gezien de belangen die netneutraliteit beoogt te beschermen. De uitzonderingen zijn techniekneutraal en daarmee toekomstvast geformuleerd. Met de gekozen formulering (volgens het systeem van white-listing) wordt voorkomen dat nu nog onvoorziene ontwikkelingen in de toekomst ertoe kunnen leiden dat het verbod om verkeer te belemmeren of vertragen wordt omzeild. Het verlies van netneutraliteit zou afbreuk doen aan de grote waarde van internet voor de maatschappij en economische groei in Nederland, zoals toegelicht in mijn memorie van antwoord van 13 december 2011. Om dit belang te borgen is door de indieners gekozen voor een restrictief systeem van white-listing. Het is inderdaad niet uit te sluiten dat abonnementsvormen die elders in Europa ontwikkeld worden, in Nederland in strijd zijn met de wet. Een bestaand voorbeeld daarvan zijn de in andere landen toegestane mobiele abonnementen waarin het gebruik van internetdiensten als Skype en WhatsApp worden geblokkeerd. In Nederland wordt deze abonnementsvorm met onderhavig wetsvoorstel verboden. Dit zorgt er juist voor dat deze diensten, terwijl ze in het buitenland door aanbieders worden geblokkeerd, in Nederland beschikbaar blijven voor alle internetgebruikers.

De leden van de CDA-fractie informeren naar de gevolgen van artikel 7.4a voor «diensten waar bepaalde verkeersstromen prioriteit krijgen, bijvoorbeeld voor publieke veiligheidsdiensten». De wet en de toelichting staan, zo menen de leden van de CD-fractie, naar de letter alleen «proportioneel» hogere prioriteit toe voor abonnementen met hogere bandbreedtes, maar niet voor specifieke toepassingen die een gewone (of misschien zelfs lagere) bandbreedte vragen.

Voor de duidelijkheid maak ik hier onderscheid tussen a) zogenoemde «managed services lanes», waarbij een bepaalde bandbreedte voor IP-gebaseerde diensten (bijvoorbeeld televisie) wordt gereserveerd, b) gevallen waarin een niet-internetdienst (bijvoorbeeld mobiele telefonie) bij congestie altijd voorrang krijgt boven een (mobiele) internetdienst die van hetzelfde (mobiele) netwerk gebruik maakt, en c) een internettoegangsdienst waarbij bepaald verkeer bij congestie prioriteit krijgt boven ander verkeer. Artikel 7.4a zegt alleen iets over de prioritering onder c. In

¹ Article 29 Data Protection Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, p. 8.

situaties waarin voor de onderlinge communicatie van publieke veiligheidsdiensten hoge eisen aan de kwaliteit en betrouwbaarheid van de verbinding moeten worden gesteld, wordt geen gebruik gemaakt van de onder c bedoelde internettoegangsdienst.

De prioritering waar artikel 7.4a op ziet, het toekennen van verschillende prioriteiten bij het afwickelen van verkeer in verband met een internettoegangsdienst, is slechts relevant wanneer congestie optreedt. Congestie betreft een vermindering van de kwaliteit van diensten en toepassingen die merkbaar is voor de eindgebruiker en veroorzaakt wordt door een tijdelijk gebrek aan capaciteit. In hoeverre een eindgebruiker last heeft van congestie wordt in sterke mate bepaald door de dienst of toepassing die hij of zij gebruikt en het congestiebeleid dat de aanbieder hanteert. Spraak- of videotoe toepassingen hebben eerder last van vertraging dan bijvoorbeeld e-mail. Artikel 7.4, eerste lid, aanhef en onderdeel a, stelt dat bij congestie gelijksoortige diensten of toepassingen gelijk moeten worden behandeld. Netwerkaanbieders zijn vrij om beleid te maken ten aanzien van congestiemanagement, waarbij zij rekening houden met de karakteristieken van (gelijksoortige) diensten of toepassingen, bijvoorbeeld de gevoeligheid voor vertraging. Zo kan een aanbieder er bijvoorbeeld voor kiezen om spraak- of videotoe toepassingen bij congestie voorrang te geven boven e-mailverkeer. Als een abonnee het belangrijk vindt dat bepaalde diensten of toepassingen die hij vaak over het internet gebruikt, ook beschikbaar zijn als er congestie optreedt, kan hij aldus kiezen voor een aanbieder die bij congestie prioriteit geeft aan die typen diensten of toepassingen. Een abonnee kan er daarnaast voor kiezen om een abonnement met een hogere bandbreedte te nemen, want aanbieders van internettoegangsdiensten mogen bij congestie ook prioriteit geven aan verkeer ten behoeve van deze abonnees boven verkeer ten behoeve van abonnees die een abonnement met een lagere bandbreedte hebben, zoals de leden ook al noemden.

Volgens de leden van de CDA-fractie zou het bij mobiele netwerken moeilijk zijn om bij congestie daadwerkelijk te garanderen dat gelijke soorten verkeer gelijk worden behandeld, zoals artikel 7.4a, eerste lid, onderdeel a, voorschrijft. Zij gaan er daarbij vanuit dat dit voorschrift betekent dat als in het mobiele netwerk een cel «vol» zit, alle klanten in het bereik van de cel alsnog dezelfde diensten via het mobiele netwerk moeten kunnen afnemen.

Zo moet het voorschrift echter niet geïnterpreteerd worden. Het voorschrift dat gelijke soorten verkeer gelijk moeten worden behandeld is alleen van belang indien de aanbieder, om de gevolgen van congestie te beperken, diensten of toepassingen op het internet belemmert of vertraagt. Het voorschrift ziet niet op het niet kunnen bieden van toegang tot een cel van het mobiele netwerk omdat deze cel «vol» zit. Het voorschrift zegt met andere woorden niets over toegang van abonnees tot het mobiele netwerk of de beschikbaarheid van internettoegang (al dan niet bij congestie).

De leden van de CDA-fractie vragen voorts of de internationaal overeengekomen standaarden voor mobiele diensten (de zgn. 3GPP-standaarden) gelet op artikel 7.4a in Nederland nog ongewijzigd kunnen worden gebruikt.

Dat is inderdaad het geval. Artikel 7.4a schrijft voor dat bij het belemmeren of vertragen van verkeer om de gevolgen van congestie te beperken, gelijke soorten verkeer gelijk moeten worden behandeld. De technische standaarden, waaronder 3GPP, ondersteunen deze manier van netwerkmanagement. Zij definiëren verschillende klassen van mobiel dataverkeer. Aan elke klasse kan een aanbieder van internettoegang een verschillende prioriteit qua verkeersafhandeling geven om de gevolgen van congestie te beperken. Zo kan bij (dreiging van) congestie een klasse

met tijdkritisch verkeer voorrang krijgen boven minder tijdkritisch verkeer. Binnen zo'n klasse wordt echter geen onderscheid gemaakt tussen bijvoorbeeld eigen diensten en diensten van een concurrent. Artikel 7.4a staat dan ook niet aan toepassing van de 3GPP-standaarden in de weg.

De leden van de CDA-fractie informeren daarnaast naar de mogelijkheid om, gezien artikel 7.4a «goedkope mobiele internetabonnementen met beperkte diensten (bijvoorbeeld met alleen toegang tot Facebook, Twitter en andere sociale media)» aan te bieden.

Hierbij draait het om de definitie van de term «internettoegangsdienst», omdat de reikwijdte van artikel 7.4a daartoe beperkt is. De toelichting bij het netneutraliteitsamendement¹ zegt hierover dat de term internettoegangsdienst breed moet worden uitgelegd, om te voorkomen dat artikel 7.4a wordt omzeild. Het door de leden van de CDA-fractie genoemde voorbeeld wordt in de toelichting op het amendement besproken: *«Indien toegang tot websites, meerdere diensten of toepassingen, zoals apps, wordt aangeboden is er in ieder geval sprake van een internettoegangsdienst. Het is op grond van dit artikel dan ook in ieder geval niet toegestaan om een dienst, bestaande uit toegang tot (bepaalde) webpagina's, diensten of toepassingen, aan te bieden, waarbij het gebruik van bepaalde toepassingen of diensten wordt geblokkeerd of apart wordt getarifeerd.»* Aanbieders mogen wel losse diensten via het internet aanbieden, bijvoorbeeld de dienst «mobiel bellen via VolP», chat-only of een dienst die uitsluitend bestaat uit internetradio of -tv of on demand muziek of video via het internet, als het maar geen dienst is die bedoeld is om toegang tot internet te verlenen. Via sociale mediadiensten als Facebook en Twitter bevelen gebruikers elkaar vaak (informatie op) andere internetsites aan, waarbij een link naar die andere site wordt geplaatst. In dat opzicht functioneren deze diensten als een soort toegangspoort naar de rest van het internet. Deze diensten moeten om die reden worden gezien als internettoegangsdiensten in de ruime betekenis die artikel 7.4a aan dit begrip toedicht. Het is daarom niet toegestaan om dergelijke diensten los aan te bieden als daarbij de toegang tot een deel van het internet wordt geblokkeerd.

De leden van de CDA-fractie merken op dat effectieve bestrijding van spam vaak alleen werkt als generiek bepaalde bronnen worden afgesloten. Dit zou aldus niet alleen gedaan kunnen worden voor de groep eindgebruikers die daarvoor toestemming hebben gegeven. Een aanbieder kan onder de uitzondering van artikel 7.4a, eerste lid, onderdeel b, uitgaande spam (spam die bewust of onbewust door zijn eigen klanten wordt verstuurd) blokkeren. Daarnaast kan het generiek filteren van inkomende spam nuttig zijn omdat klanten dit op prijs stellen en omdat het onnodige belasting van netwerken en systemen voorkomt. Artikel 7.4a, eerste lid, onderdeel c, stelt hiervoor wel als voorwaarde dat de abonnee toestemming heeft gegeven. De aanbieder die alleen generiek op spam wil filteren, zou ervoor kunnen kiezen om bij het afsluiten van een overeenkomst te wijzen op het nut van een spamfilter en het geven van toestemming als voorwaarde voor het sluiten van de overeenkomst te stellen.

Levering van de internettoegangsdienst

De leden van de CDA-fractie hebben vragen gesteld over het bij amendement ingevoegde artikel 7.6a, dat bepaalt dat het slechts in de limitatief in dat artikel opgesomde gevallen is toegestaan de levering van een internettoegangsdienst aan een eindgebruiker geheel of gedeeltelijk te beëindigen of op te schorten. Over deze bepaling heb ik in de memorie van antwoord gezegd dat er andere dan de in artikel 7.6a omschreven gevallen denkbaar zijn waarbij de overeenkomst volgens het Burgerlijk

¹ Kamerstukken 32 549, 29, p. 2 ev.

Wetboek rechtmatig kan worden beëindigd door de aanbieder. Als een ontbindende voorwaarde afwijkt van de in artikel 7.6a omschreven gevallen, dan kan die ontbindende voorwaarde civielrechtelijk misschien wel leiden tot een ontbinding van de overeenkomst, maar blijft de aanbieder publiekrechtelijk verplicht te leveren. De ontbinding dient dan de facto geen doel. In artikel 7.6a zijn de privaatrechtelijke gevolgen van de publiekrechtelijke leveringsverplichting niet beschreven. De indieners hebben zich geconcentreerd op het via het publiekrecht (de Telecommunicatiewet) voorkomen van een situatie waarin een abonnee te lichtvaardig van internet wordt afgesloten¹, of dat nu civielrechtelijk rechtmatig zou zijn of niet. Daarmee hebben de indieners ook willen voorkomen dat de aanbieder met het opnemen van allerlei ontbindende voorwaarden in de overeenkomst kan bepalen of een abonnee toegang heeft tot het internet of niet. Daarvoor vinden de indieners het belang van een burger om toegang te kunnen hebben tot internet te zwaar wegen².

De leden van de CDA-fractie vragen of de bepaling kan worden geïnterpreteerd als een regeling die alleen geldt «zodra en zolang er een bestaande verbintenis tot levering bestaat».

Gezien de uit de toelichting blijkende intentie van de indieners en gelet op onderdeel d van het artikel, is deze interpretatie niet juist. Artikel 7.6a ziet niet alleen op het opschorten tijdens het contract. Het artikel bepaalt in onderdeel d bijvoorbeeld dat, ook al is een contract van bepaalde duur afgelopen, de levering niet mag worden beëindigd zonder instemming van de abonnee met het niet-verlengen of niet-vernieuwen van het contract. Het Burgerlijk Wetboek stelt voor de beëindiging van een dergelijke overeenkomst «instemming van de abonnee met het niet-verlengen of niet-vernieuwen van het contract» niet als voorwaarde. Civielrechtelijk bestaat dan ook zonder instemming van de abonnee geen verbintenis tot levering meer, terwijl artikel 7.6a in dat geval beëindiging van de levering alleen toestaat als de abonnee ermee instemt dat de overeenkomst niet wordt verlengd of vernieuwd.

Ondanks dat het artikel geen helderheid biedt over de civielrechtelijke gevolgen van het verbod de levering op te schorten of te beëindigen is het duidelijk wat de indieners hebben willen regelen. Ik denk dat de praktijk hiermee ook prima uit de voeten kan. Zoals ik in de memorie van antwoord probeerde aan te geven is de discussie over hoe de civielrechtelijke situatie er precies uitziet als de aanbieder volgens het Burgerlijk Wetboek rechtmatig opzegt, maar op grond van artikel 7.6a toch verplicht blijft tot levering, een theoretische discussie. In de praktijk zal een aanbieder van een internettoegangsdienst er, vanwege artikel 7.6a, geen belang bij hebben de overeenkomst met de abonnee te ontbinden in andere dan de in artikel 7.6a genoemde gevallen. Dat zal dus niet snel voorkomen. Ik verwacht dan ook geen problemen met de toepassing van dit artikel in de praktijk.

¹ Kamerstukken 32 549, 40, p. 2: «Op dit moment kunnen internetproviders volgens hun algemene voorwaarden om talloze redenen de internettoegang van gebruikers beperken of afsluiten.»

² Kamerstukken 32 549, 40, p. 2: «Gelet op het belang van internettoegang in Nederland, is het noodzakelijk om de omstandigheden waaronder een aanbieder internettoegang mag beëindigen of opschorten, limitatief te omschrijven.»

³ Kamerstukken 32 549, 40, p. 2: «Voor alle duidelijkheid ziet dit nieuwe artikel niet op webhosting. Conform de wettelijke bepalingen en de Notice and Takedown-procedure die de sector zelf heeft opgesteld, kunnen websites offline gehaald worden als sprake is van onmiskenbaar onrechtmatige of strafbare zaken.»

De leden van de fractie van het CDA vragen of het amendement aan de toepassing van notice-and-take-downprocedures in de weg staat. Dat is niet het geval. In de toelichting op het amendement is benadrukt dat dit artikel niet ziet op webhosting³, maar op aanbieders van internettoegangsdiensten. De notice-and-takedownprocedure zoals die is opgenomen in de Gedragscode ziet alleen op webhosts die onmiskenbaar strafbaar of onrechtmatig materiaal offline kunnen halen. (Het beëindigen van) de hosting van een website is iets anders dan (het opschorten of beëindigen van) de levering van een internettoegangsdienst, waar artikel 7.6a op ziet.

De leden van de CDA-fractie wijzen erop dat artikel 7.6a niet het in het Burgerlijk Wetboek gebruikte «toerekenbare tekortkoming in de nakoming» noemt als criterium, maar in plaats daarvan specifieke soorten toerekenbare tekortkomingen in de nakoming noemt.

Artikel 7.6a geeft een uitzondering op het verbod de levering van de internettoegangsdienst op te schorten of beëindigen bij de volgende «vormen» van tekortkoming in de nakoming door de abonnee: het niet nakomen van een betalingsverplichting, faillissement, en bedrog. In de door artikel 7.6a besproken contractsituaties zullen dit naar mijn inschatting ook de enige mogelijke tekortkomingen aan de zijde van de abonnee kunnen zijn, nu de contractuele verplichting van de abonnee in die gevallen over het algemeen uitsluitend bestaat uit een betalingsverplichting.

De leden van de CDA-fractie vragen tot slot of opschorting mogelijk zou moeten zijn als de veiligheid of integriteit van het netwerk of de dienstverlening in het geding is. Zij wijzen op het verschil op dit punt met artikel 7.4a, tweede lid.

In de toelichting op het amendement¹ wordt de verhouding tussen artikel 7.6a en artikel 7.4a beschreven. Op basis van artikel 7.4a kan de aanbieder het uitgaande verkeer afkomstig van een bepaalde internetverbinding blokkeren teneinde de veiligheid en integriteit van het netwerk te garanderen. Het artikel geeft bewust geen grond voor de aanbieder om de levering van de internettoegangsdienst aan een abonnee wiens computer is geïnfecteerd en wordt ingezet in een botnet in dat geval te beëindigen of op te schorten. De indieners lichten toe dat zij het om deze reden afsluiten van deze abonnee van de toegang tot het internet disproportioneel vinden.

Termijn instemmingsbesluit graafwerkzaamheden

De leden van de fractie van de VVD verzoeken de regering om artikel 5.4, tweede lid, pas in werking te laten treden bij de eerstvolgende gelegenheid waarbij de Telecommunicatiewet wordt aangepast om zo mogelijke problemen in de tussenliggende periode te voorkomen. De leden van de fractie van het CDA merken op dat het zeer onwenselijk is dat een bepaling in werking treedt waarvan de wetgever eigenlijk toegeeft dat die niet correct is, maar het herstel daarvan onbestemd is en lang kan duren. Het is juist dat het enige tijd zal duren voordat artikel 5.4, tweede lid, is aangepast. Zoals beide fracties aangeven kan bij inwerkingtreding van de thans voorgestelde bepaling onduidelijkheid optreden omtrent de termijn waarbinnen een instemmingsbesluit moet worden genomen. Om deze onduidelijkheid en de daaruit voortvloeiende onzekerheid weg te nemen is de regering bereid het voorgestelde artikel 5.4, tweede lid, niet in werking te laten treden.

Toegang tot de kabel c.q. wederverkoopverplichting programma-diensten

De leden van de fractie van het CDA verzoeken de regering advies te vragen aan de Raad van State over de juridische houdbaarheid van de met amendementen 18 en 28 in het wetsvoorstel opgenomen bepalingen met betrekking tot toegang tot de kabel. Ook vragen zij de regering pas na het verkrijgen van dat advies over de inwerkingtreding van deze bepalingen te beslissen.

In de memorie van antwoord is aangegeven dat het voor het antwoord op de vraag, of de voorgestelde bepalingen zich verdragen met het Europese recht, nodig is te weten of de programmadiensten waarop beide amendementen zien, zijn te beschouwen als elektronische communicatiediensten in de zin van de Europese richtlijnen. Een belangrijke vraag daarbij is of de door de kabelmaatschappijen geboden dienst moet worden gezien als één dienst die hoofdzakelijk bestaat uit programma's en voor een ondergeschikt deel uit het transport van die programma's. Als dit zo is dan is er geen sprake van een elektronische communicatiedienst en

¹ Kamerstukken 32 549, 40, p. 3.

wordt deze dienstverlening niet beheerst door de Europese regels op het terrein van elektronische communicatie. Zoals in de memorie van antwoord is aangegeven wordt er verschillend gedacht over het antwoord op de vraag of de hier bedoelde programmadienst te beschouwen is als een elektronische communicatiedienst. Het uiteindelijke antwoord op deze vraag kan alleen worden gegeven door het Europese Hof van Justitie. Advisering door de Raad van State kan die duidelijkheid niet geven en lijkt daarom niet de meest aangewezen weg.

Gezien het belang van een uitspraak van het Hof van Justitie merk ik op dat prejudiciële vragen zijn gesteld door het Gerechtshof Amsterdam in een geschil tussen de gemeente Hilversum en kabelmaatschappij UPC (geregistreerd onder zaaknummer C-518/11). Eén van de aan het Europese Hof voorgelegde vragen betreft de vraag of de door UPC geboden programmadienst onder de werking van het Europese telecommunicatiekader valt. De Nederlandse regering heeft in deze zaak schriftelijke opmerkingen gemaakt. De kern van deze opmerkingen is dat Nederland van opvatting is dat de door UPC geboden programmadienst niet is te beschouwen als een elektronische communicatiedienst waardoor het Europese kader voor elektronische communicatie niet van toepassing is. Voor wat betreft het al dan niet uitstellen van de inwerkingtreding van de hier aan de orde zijnde bepalingen merk ik het volgende op. De voorgestelde bepalingen komen, zoals bekend, voort uit twee amendementen. Deze amendementen geven uitdrukking aan een reeds geruime tijd bij een meerderheid van de Tweede Kamer sterk levende wens om te komen tot toegang tot de kabel. Ik heb eerder beleidsmatige bedenkingen geuit tegen een wettelijke regeling van de toegang tot de kabel. Ook heb ik gewezen op de juridische risico's. Niettemin ben ik van mening dat er argumenten zijn om aan te nemen dat de betreffende bepalingen juridisch houdbaar zijn. Om die reden en omdat ik het besluit van de Tweede Kamer, als medewetgever, respecteer, ben ik voornemens de bepalingen met betrekking tot toegang tot de kabel direct in werking te laten treden. Mocht in de toekomst onverhoopt blijken dat er sprake is van strijd met het Europese recht dan zal ik alsdan met een wetsvoorstel komen om de betreffende bepalingen uit de Telecommunicatiewet te schrappen.

De minister van Economische Zaken, Landbouw en Innovatie,
M. J. M. Verhagen