Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directie Europese en Internationale Zaken

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
DEIZ / 18306124

Uw kenmerk

Datum 3 december 2018
Betreft Aanvulling beantwoording schriftelijke vragen voor de Telecomraad op dinsdag 4 december 2018 te Brussel

Geachte Voorzitter,

Hierbij bied ik u zoals toegezegd in de beantwoording van het schriftelijk overleg over de Telecomraad[1] de reactie aan op de vragen over e-Privacy, die de VVD-fractie van uw Kamer heeft gesteld naar aanleiding van de bijeenkomst van de ministers verantwoordelijk voor Telecommunicatie op dinsdag 4 december in Brussel.

Hoogachtend,

mr. drs. M.C.G. Keijzer
Staatssecretaris van Economische Zaken en Klimaat

[1] https://www.rijksoverheid.nl/documenten/kamerstukken/2018/11/27/beantwoording-kamervragen-over-telecomraad-van-4-december-2018

De leden van de VVD-fractie danken de staatssecretaris voor haar reactie op de motie van het lid Wörsdörfer en haar bereidheid om met ondernemers in gesprek te gaan inzake de e-Privacyverordening.

De VVD is blij dat de besluitvorming bij Telecomraad over e-Privacy niet besluitvormend of concluderend zal zijn. Zorgvuldige en slimme wetgeving is belangrijker dan een snelle afronding, helemaal nadat het afgelopen jaar het bedrijfsleven al moeizaam worstelde met de implementatie van de AVG. De leden van de VVD-fractie begrijpen dat, met het oog op de concept e-Privacy verordening, met name de rechtsgronden om gegevens te kunnen verwerken de belangrijkste en meest bediscussieerde onderwerpen zijn waardoor het e-Privacy dossier in de Raad nog niet wordt afgerond.

Wat opvalt is dat de concept e-Privacy verordening andere definities hanteert dan de AVG en deels een andere wetgevingstechniek heeft, waarbij gebruik van persoonsgegevens voor specifieke processen wordt gereguleerd (rule-based). Dat is anders dan bij de AVG, die – overigens onder zeer strikte waarborgen – een aantal gronden bevat om gegevens te verwerken, zónder daarbij specifieke processen uit te sluiten of goed te keuren (technologieneutraal en principle-based). Daarmee is de AVG toekomstbestendige wetgeving, en is de concept e-Privacy verordening aanzienlijk minder flexibel.

Het kabinet schrijft dat Nederland van mening is dat er een afgewogen pakket ligt dat een goede balans geeft tussen privacybescherming en ruimte voor nieuwe dienstverlening. De VVD-leden menen evenwel dat er diverse knelpunten te identificeren zijn. Graag vragen zij het kabinet te reageren op het navolgende.

De leden van de VVD-fractie constateren dat de door de Tweede Kamer aangenomen motie Wörsdörfer om een goede vergelijkende toets tussen de concept e-Privacy verordening en de AVG, én om de gevolgen van deze wet voor innovatie en het mkb goed te toetsen vooralsnog niet volledig is uitgevoerd. Graag identificeren deze leden daarom zelf knelpunten met daarbij een aantal punten ter oplossing, op een wijze die het privacybelang sterk borgt én innovatie niet beperkt.

<u>Artikel 8, voeg 'plaatsen of uitlezen van informatie ter uitvoering van een overeenkomst' toe</u>
Artikel 8 van de concept e-Privacy verordening kent een lid 1(c), dat het mogelijk maakt om informatie te plaatsen of op te halen van gebruikersdevices, wanneer: "(c) it is necessary for providing an information society service requested by the end-user" Alhoewel dat lijkt op AVG artikel 6.1 " (b) necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" is dit net anders verwoord. De staatssecretaris heeft eerder al eens aangegeven dat de materiele betekenis tussen de twee artikelen niet wezenlijk verschilt, en dat deze grond in de concept e-Privacy verordening eigenlijk gelijk staat aan plaatsen of uitlezen van data ter uitvoering van het contract zoals in de AVG beschreven. De VVD-leden zijn echter van mening dat 'gevraagde dienst van de informatiesamenleving' wel degelijk een andere lading heeft dan 'uitvoering van een contract waar de betrokkene partij is'.

Zo vragen deze leden zich af of het noodzakelijke uitlezen en plaatsen van gegevens om een slim apparaat zoals een zelfrijdende auto te doen functioneren wel gedekt is onder een 'gevraagde dienst van de informatiesamenleving'? Indien de staatssecretaris meent dat precies hetzelfde beoogd wordt, dan is het volgens de leden van de VVD-fractie logisch dat zij er geen bezwaar tegen zou maken deze grond alsnog aan de concept e-Privacy verordening toe te voegen. Het toevoegen van de contractsgrond aan de concept e-Privacy verordening lijkt een no-regret-move voor de staatssecretaris waarmee ze die onduidelijkheid en rechtsonzekerheid bij ondernemingen weg kan halen. Is de staatssecretaris daartoe bereid?

De verwerkingsgrondslagen in de huidige e-Privacyrichtlijn alsmede in de voorgestelde e-Privacyverordening vormen deels een 'vertaling' en een nadere uitwerking van de verwerkingsgrondslagen in de Algemene verordening gegevensbescherming (AVG) naar de telecommunicatie-omgeving. Dat is logisch want de e-Privacyregels zien alleen op die omgeving. Deze omgeving wijkt in zoverre af van het regime van de AVG dat de specifieke processen wél van belang zijn. Er moet ook gereguleerd worden wat de partij mag die de communicatie verzorgt. Dit is anders dan in de AGV waar primair de verhouding tussen verwerkingsverantwoordelijke en betrokkene wordt gereguleerd. De grondslag "nodig voor uitvoering van een overeenkomst waarbij de betrokkene (het datasubject) partij is" uit de AVG 'vertaald' en verder gepreciseerd naar "nodig voor door de eindgebruiker verzochte levering van een dienst van de informatiemaatschappij" in de huidige e-Privacyrichtlijn en het voorstel hiervoor. Deze vertaling en nadere precisering is naar mijn opvatting volkomen correct. Bovendien is de aldus geformuleerde verwerkingsgrond niet nieuw. Deze komt ook in de huidige e-Privacyrichtlijn voor en wordt al jaren in de praktijk toegepast. Ik zie dan ook geen reden om in dit kader te pleiten voor een aanpassing van de voorgestelde verordening op dit punt.

Voor wat betreft de zelfrijdende auto merk ik het volgende op. Veel omtrent de zelfrijdende auto is nog niet duidelijk. Hoe maakt deze auto contact met zijn omgeving? Gaat dit rechtstreeks -dus zonder tussenkomst van een openbaar telecommunicatienetwerk- of gaat dit juist via een openbaar telecommunicatienetwerk of worden wellicht beide vormen benut? Als het gaat om rechtstreekse communicatie (een zender in de auto communiceert met een 'slim' verkeerslicht dat ook uitgerust is met een zender) dan is het e-Privacyregime niet van toepassing. Dat ziet immers alleen op apparaten indien (en voor zover) deze zijn aangesloten op een openbaar elektronisch communicatienetwerk. Vindt de communicatie plaats via een telecomnetwerk dan zal de eindgebruiker via dat openbare telecommunicatienetwerk een dienst van de informatiemaatschappij afnemen. In dat geval mogen gegevens worden verwerkt die noodzakelijk zijn voor de uitvoering van die dienst.

<u>Artikel 8, voeg een gecontroleerde vorm van gerechtvaardigd belang "de plusvariant" toe</u>
Artikel 8 van de concept e-Privacy verordening kent, anders dan de AVG, niet het zogeheten "gerechtvaardigd belang" voor een ondernemer: een ondernemer maakt dan zelf de weging of het plaatsen of uitlezen van informatie op gebruikers-devices gerechtvaardigd is, afgewogen tegen de privacybelangen van zijn klant, gebruiker of werknemer. Deze grond om persoonsgegevens te verwerken, kan hij volgens de AVG alleen inroepen indien er lage of te verwaarlozen privacy-risico's zijn voor de gebruiker. Anders mag het gewoonweg niet. Zo zouden cookies die slechts bedoeld zijn om de inhoud van een online winkelmandje bij te houden wel onder het gerechtvaardigd belang vallen, maar marketingcookies niet. Het is zeer strikt.

Het in de concept e-Privacy verordening ontbreken van dit gerechtvaardigde belang als grond voor bedrijven om gegevens te kunnen plaatsen of uitlezen in gevallen waar privacy vrijwel geen rol speelt, betekent dat bedrijven gebruikers veelal zullen moeten vragen om toestemming. Dat leidt ertoe dat consumenten met de komst van het Internet of Things – waarin steeds meer devices verbonden zijn – steeds vaker 'ja moeten klikken' – dus ook wanneer er geen noemenswaardig privacy-risico bestaat. Dit zal er in de ogen van de leden van de VVD-fractie in toenemende mate toe leiden dat gebruikers onverschillig 'ja' klikken', zonder daadwerkelijk goed gelezen te hebben wat de consequenties zijn. In jargon heet dit wel 'consent fatigue': er treedt een sleetsheid op bij het geven van toestemming waardoor uiteindelijk in de praktijk geen sprake meer van een bewuste wilsuiting van een individu, maar enkel van het wegklikken van hinderlijke pop-ups. Omgekeerd: een wetgever die ook voor niet privacygevoelige processen steeds toestemming voorschrijft, holt daarmee de facto de betekenis van toestemming als bewuste wilsuiting actief uit. Daarom is gerechtvaardigd belang ook een belangrijke grond: waar voor gebruikers geringe of geen privacy consequenties bestaan, is toestemming niet nodig.

Als het 1-op-1 overnemen van gerechtvaardigd belang in de e-Privacy verordening – zoals in de AVG – niet werkbaar is, zien de leden van de VVD-fractie twee mogelijke oplossingen die bovendien technologieneutraal en toekomstbestendig zijn.
<u>(1) gelimiteerd gerechtvaardigd belang:</u> het gerechtvaardigd belang wordt toegevoegd, maar met een aangehechte levende zwarte lijst van processen waarvoor dit gerechtvaardigde belang niet mag worden ingezet. Deze lijst wordt beheerd door de EDPB, het orgaan van gezamenlijke privacy-toezichthouders in Europa, dat ook expliciet de taak krijgt om voor dit gelimiteerde gerechtvaardigd belang in de EPR uitspraken te doen, of
(<u>2) een certified gerechtvaardigd belang,</u> waarbij door middel van een verplichte Privacy Impact Assessment (PIA) bij de toezichthouder of een certificerende instantie aangetoond wordt dat inderdaad sprake is van geringe privacy-consequenties en dat is uitgesloten dat bijzondere persoonsgegevens (een risicocategorie) worden verwerkt.
Op deze manier kunnen ook toekomstige bedrijfsprocessen die op dit moment nog onbekend zijn dynamisch gewogen worden op het moment dat zij zich manifesteren. Zo biedt de wet borging van privacy, maar wel technologieneutraal,

toekomstbestendig en biedt zij ruimte aan innovatie in plaats van slechts de ons nu bekende realiteit te stollen.

Graag vragen de leden van de VVD-fractie een reactie op bovengenoemde en vragen zij tevens of de staatssecretaris bereid is dit op te brengen in het vervolg van de onderhandelingen?

De leden van de VVD-fractie houden in hun vraag een pleidooi voor het introduceren van de grondslag gerechtvaardigd belang bij de toegang tot apparatuur van een eindgebruiker. In mijn brief van 26 oktober (Kamerstuk 32761, nr. 126) heb ik reeds aangegeven dat dat geen goed idee is. In de onderhandelingen in de Raad is eerder geconstateerd dat er geen enkel draagvlak is voor het opnemen van een dergelijke grondslag. Het uitgangspunt bij toegang tot een eindapparaat van een eindgebruiker moet mijns inziens zijn dat dit alleen is toegestaan als dat overeenstemt met de wil van die eindgebruiker. Het is zijn apparaat; hij beslist wie er informatie op zet of wie de informatie op het apparaat (*zijn* informatie) mag gebruiken. Ik trok daarbij al eerder de parallel met de toegang tot een woonhuis. Die wil van de eindgebruiker kan wat mij betreft allereerst blijken uit het feit dat de eindgebruiker heeft aangegeven een dienst te willen afnemen waarbij het nodig is om toegang tot het apparaat te krijgen. Als dat niet voor dat doel nodig is dan is het wat mij betreft vanzelfsprekend dat een bedrijf toestemming moeten vragen aan de eindgebruiker. Krijgt een bedrijf die toestemming niet dan mag het bedrijf geen gegevens op het eindapparaat verwerken ook al zou dat nuttig zijn voor dat bedrijf.

De leden van de VVD fractie merken verder op dat de in de verordening voorgestelde benadering -waarbij de grondslag gerechtvaardigd belang ontbreekt- leidt tot het telkens moeten geven van toestemming waardoor zogenaamde klikmoeheid ontstaat ('consent fatigue') waardoor de eindgebruiker zonder daarbij na denken akkoord gaat. Ik deel deze opvatting niet. Allereerst is het zo dat veel (nieuwe) IoT (Internet of Things) toepassingen tot gevolg hebben dat eindgebruikers (nieuwe) diensten gaan afnemen. Als het bij die diensten nodig is om gegevens op het eindapparaat te verwerken dan wordt dit gedekt door de grondslag "nodig voor de levering van een door de eindgebruiker gevraagde dienst van de informatiemaatschappij". Met andere woorden: in veel gevallen zal er geen toestemming hoeven te worden verleend. Mijns inziens is de e-Privacy verordening dan ook niet zozeer 'consent based' als wel wat men 'service based' zou kunnen noemen. Toestemming speelt vooral in de context van het plaatsen van trackingcookies voor reclame doeleinden. Daarbij ontstaat inderdaad klikmoeheid. Dit komt door meerdere oorzaken. Allereerst zijn er helaas bedrijven die hun website zo inrichten dat onnodig veel toestemming wordt gevraagd. Daarnaast speelt een belangrijke rol dat de eindgebruiker vaak geen echte keuze heeft bij trackingcookies. Immers als hij niet instemt wordt de toegang tot de website hem ontzegd. Daarom pleit Nederland in lijn met de motie Verhoeven (nr. 35000-XIII-43) voor een verbod op deze zogenoemde cookiewalls. Als een eindgebruiker echte keuze heeft zal hij immers minder snel 'klik moe' worden.

In de AVG mogen partijen gegevens verwerken indien zij daartoe wettelijk verplicht zijn. Dat ontbreekt nog in artikelen 6 en 8 van de concept e-Privacy verordening. Dat zou bijvoorbeeld moeten gelden voor alle data die vanuit maatschappelijke veiligheid verplicht moeten worden verzameld door fabrikanten (denk bijvoorbeeld aan veiligheid van zelfrijdende auto's). Vanwege de veiligheid moeten deze gegevens, rekening houdend met de eisen van privacy-by-design, zonder toestemming kunnen worden verzameld. Artikel 11 van de concept e-Privacy verordening biedt daarvoor een te smalle basis. Deelt de staatssecretaris deze mening en is zij bereid dit in te brengen in het vervolg van de onderhandelingen over de concept verordening?

Zoals de leden van de VVD-fractie zelf aangeven geeft artikel 11 van de voorgestelde e-Privacyverordening de mogelijkheid om in nationale wetgeving van de regels in die verordening af te wijken. Deze mogelijkheid bestaat voor een aantal in de verordening genoemde doelen. In de raadsversie zijn daar naar aanleiding van de bespreking in de raad diverse doelen aan toegevoegd, zoals "de bescherming van de betrokkene en de rechten en vrijheden van anderen". Naar mijn opvatting bieden de aldus verruimde mogelijkheden voor nationale wetgeving voldoende ruimte om bijvoorbeeld uitzonderingen te maken voor de verkeersveiligheid van de betrokkenen en de andere verkeersdeelnemers. Ik laat daarbij in het midden of het in toekomst nodig is van uit het oogpunt van verkeersveiligheid te regelen dat fabrikanten van auto's deze auto's op afstand zouden moeten kunnen aflezen.

Tot slot hebben de leden van de VVD-fractie nog de volgende vragen over de concept verordening. In verschillende versies van de Raadsstukken duikt in artikel 6 van de concept e-Privacy verordening een vreemde stijlfiguur op. Er is daar weliswaar een soort grond 'uitvoering van het contract' zoals in de AVG opgenomen, maar alsnog dient extra toestemming van de gebruiker te worden verkregen (zelfs als het expliciet om de uitvoering van een overeenkomst gaat, binnen die tijd en binnen het gevraagde). Dit is dubbelop en bovendien innerlijk strijdig Want indien iemand dan toestemming terugtrekt, geldt dan het contract nog wel? Vindt de staatssecretaris dit ook vreemd en zou zij dit willen amenderen?

De leden van de VVD-fractie merken dit terecht op. Ik heb dit eerder ook al zelf vastgesteld en naar voren gebracht in de raadswerkgroepen. Helaas is er tot nu toe door het voorzitterschap geen gevolg gegeven aan mijn wens de concept-verordeningstekst op dit punt aan te passen. Ik zal dit punt in de verdere onderhandelingen nogmaals naar voren brengen.

Hoe ziet de staatssecretaris de verhouding tussen de concept e-Privacy verordening en haar wens om kunstmatige intelligentie in Nederland stevig te versnellen? Kunstmatige intelligentie heeft behoefte aan grote hoeveelheden goed georganiseerde (daar heeft zo begrijpen we de AVG een positief effect) data zonder bias (dus geen gedeeltelijke datasets). Steeds vaker zullen deze ook uit verbonden devices gaan komen. In hoeverre is het regime op grond van de concept verordening ondersteunend aan het verkrijgen van deze grote hoeveelheden onge-bias-te data? Aanvullend begrijpen de voornoemde leden dat slimme foto-herkenningstechnologieën die pro-actief kinder-pornografisch materiaal opsporen, maar ook gebruikt worden om terroristisch materiaal te

traceren niet expliciet toegestaan zijn onder het nieuwe e-privacy regime van artikel 6. De leden verzoeken een reactie van de staatssecretaris, met daarbij het verzoek om expliciet dit artikel mee te nemen: https://www.telegraph.co.uk/news/2018/10/14/european-commission-putting-paedophiles-privacy-ahead-fighting/

Bij kunstmatige intelligentie is toegang tot data inderdaad belangrijk. Daarmee is echter niet gezegd dat aan deze toegang tot data geen grenzen zitten. Deze grenzen worden wat mij betreft gevormd door het communicatiegeheim - bedrijven mogen geen data verzamelen door communicatie af te luisteren zonder toestemming van de communicerende partijen- en het recht van de eindgebruiker om zelf te mogen beslissen wie toegang heeft tot de informatie op zijn eindapparaat. Voor wat betreft het proactief opsporen van kinderpornografisch materiaal merk ik het volgende op. De e-Privacyregels staan er niet aan in de weg dat er opsporing wordt verricht door de bevoegde autoriteiten naar stafbare feiten. Wat echter niet mag is dat telecommunicatie-aanbieders deze rol op zich nemen door, bijvoorbeeld, door middel van deep packet inspection al het internetverkeer te bekijken. De telecommunicatie-aanbieders hebben zich, mijn inziens terecht, te houden aan het communicatiegeheim. Dit is ook mijn reactie op het door de leden van de VVD-fractie bedoelde Engelstalige artikel. Het is niet de taak van, bijvoorbeeld, Facebook om communicatie tussen zijn gebruikers af te luisteren om strafbare feiten te voorkomen. De nieuwe e-Privacyverordening zorgt ervoor dat partijen zoals Facebook wat dat betreft onder dezelfde regels vallen, waar de klassieke telecommunicatiepartijen al sinds jaar en dag onder vallen.

De leden van de VVD-fractie zien mogelijkheden in een verwerkingsgrond als 'ten behoeve van de integriteit van een dienst'. Is de staatssecretaris bereid dit in te brengen in het vervolg van de onderhandelingen over de concept verordening?

Ik kan de insteek van de leden van de VVD-fractie goed volgen maar denk dat, zij het in andere bewoordingen, een dergelijke verwerkingsgrond al in de meest recente raadsversie van de e-Privacyverordening is opgenomen. Zo bevat artikel 6 (uitzondering op het communicatiegeheim) de volgende verwerkingsgrondslag: verwerking is toegestaan "if it is necessary to maintain or restore the security of electronic communications networks and services, or to detect faults and/or errors and/or security risks and/or attacks in the transmission of electronic communications, for the duration necessary for that purpose" en bevat artikel 8 (verwerken gegevens eindapparaten) de grondslag "it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose".

De leden vragen zich in de vergelijking tussen AVG en e-Privacy af of de staatssecretaris in meer detail kan ingaan op de volgende constateringen: in veel gevallen zijn elektronische communicatiegegevens tegelijkertijd weer persoonsgegevens, waardoor de AVG eveneens (deels) van toepassing is.

De constatering is juist maar dat levert geen probleem op. De e-Privacyverordening bevat grondslagen voor verwerking van zowel persoonsgegevens als niet-persoonsgegevens.

De e-Privacyverordening kent ook grondslagen die niet zijn terug te vinden in de AVG. De e-Privacy verordening doet dit vanuit andere grondrechten (communicatiegeheim, persoonlijke levenssfeer) dan het grondrecht dat de AVG beoogd te beschermen (recht op bescherming persoonsgegevens). Voor de gegevens die zijn te kwalificeren als persoonsgegevens geldt dat - afgezien van de grondslagen - alle andere regels met betrekking tot persoonsgegevens van de AVG van toepassing zijn. Bijvoorbeeld: als een telecommunicatie-aanbieder met toestemming van de communicerende partijen een gesprek afluistert en hij daarbij kennis krijgt van persoonsgegevens, dan hebben de communicerende partijen op basis van de AVG recht op inzage in de (persoons)gegevens die de telecommunicatie-aanbieder verwerkt.

Hoe verhouden de richtlijnen die bepalen wanneer een organisatie conform de AVG een verplichte PIA moeten doen – komend vanuit de privacy-toezichthouders en de Europese koepel EDPR (waarbij voor elektronische communicatiedata, metadata, IoT data en gegevens voor online behavioral targeting expliciet is bepaald dat voor verwerking eerst een verplichte PIA nodig is) zich tot de verbijzondering die de e-Privacy verordening bepaalt en is de laatste daarmee niet toch overbodig?

Zoals hiervoor al aangegeven geeft de e-Privacyverordening voor zover hier van belang afwijkende verwerkingsgrondslagen. Dat neemt niet weg dat, als het om persoonsgegevens gaat een bedrijf dat een dergelijke grondslag gebruikt en daarbij persoonsgegevens verwerkt, in sommige gevallen eerst een PIA (Privacy Impact Assessment) moet doen. Ik zie daarin geen spanning of tegenstrijdigheid maar juist consistentie in de toepassing van de regels.

Uit onderzoek van het Oxford Reuters Institute blijkt dat EU nieuwssites 22 procent minder cookies plaatsen sinds de AVG. Daarnaast hebben verschillende nieuwssites uit de VS hun site ontoegankelijk gemaakt voor EU gebruikers omdat het cookiebeleid niet conform de bepalingen uit de AVG zou zijn. De AVG blijkt daarmee door te werken in het domein van e-Privacy.

Wat is de analyse van de staatssecretaris over de doorwerking van de AVG op een fenomeen als tracking cookies en noopt dit tot een eventuele heroverweging op elementen uit de concept verordening?

Het onderzoek waarnaar de leden van de VVD-fractie verwijzen is mij niet bekend. Ik heb er dan ook geen oordeel over. Maar aannemende dat de bevinding juist is dat de AVG feitelijk doorwerking heeft bij de plaatsing van tracking cookies zie ik dat als positief. Ik zie er echter geen grond in om wijziging aan te brengen in de e-Privacyregels. De verwerkingsgrondslagen van de e-Privacyverordening en de (overige) regels van de AVG vullen elkaar goed aan.

In de reactie op de eerder genoemde motie Wörsdörfer stelt de staatssecretaris dat de e-Privacy verordening nodig is om te voorkomen dat bedrijven mogen kijken in e-mails. De voornoemde leden vragen zich af hoe zich dat verhoudt tot de AVG die dergelijke toegang ook niet toestaat. Het Europese Hof van Justitie oordeelt immers in de Digital Rights Ireland zaak uit 2014 dat toegang tot metagegevens en inhoud een buitengewoon ernstige inbreuk op grondrechten is, zeker als dit profilering mogelijk maakt.

Kan de staatssecretaris nader toelichten hoe AVG en e-Privacy zich in dit kader tot elkaar verhouden?

De jurisprudentie waar de leden van de VVD-fractie naar verwijzen is zowel op het Handvest voor de grondrechten van de Europese Unie gebaseerd alsmede op de uitwerking van het daarin opgenomen grondrecht op bescherming van het privéleven in richtlijn 2002/58/EG, de huidige e-Privacyrichtlijn. De e-Privacyrichtlijn is op zijn beurt weer uitgewerkt in hoofdstuk 11 van de Telecommunicatiewet.

Net als in de e-Privacyrichtlijn richt het communicatiegeheim in hoofdstuk 11 van de Telecommunicatiewet zich tot de klassieke aanbieders van telecommunicatiediensten. Dan gaat het dus om aanbieders die zelf elektronisch transport verzorgen, derhalve aanbieders als KPN en Ziggo. Het communicatiegeheim geldt niet voor partijen die communicatie verzorgen over een door een andere partij geleverde internetverbinding (Skype, Facebook Messenger, WhatsApp). De nieuwe e-Privacyregels brengen hier verandering in. Maar, zo begrijp ik de vraag van de leden van de VVD-fractie, is dit wel nodig en kan een eindgebruiker jegens zijn (over-de-top) communicatie-aanbieder niet rechtstreeks een beroep doen op het Handvest voor de grondrechten van de Europese Unie? De heersende opvatting omtrent het antwoord op deze vraag is dat dat niet mogelijk is. Met andere woorden: de grondrechten in het Handvest kennen geen rechtstreekse horizontale werking. Dit betekent dat zolang de e-Privacyregels niet zijn aangepast, partijen als Facebook en WhatsApp zonder toestemming van de communicerende partijen kennis mogen nemen van de inhoud van de door hen verzorgde communicatie. Dit is een van de voornaamste redenen dat het van belang is dat de nieuwe regels spoedig komen.