Consultatie van het voorontwerp voor een

Wet op de inlichtingen- en veiligheidsdiensten 20..

Reactie van KPN

KPN
Contactpersonen: drs. ing. G.J.C. Wabeke / mr. P.C. Knol
Postbus 30 000
2500 GA Den Haag
gert.wabeke@kpn.com / paul.knol@kpn.com

Kenmerk: GCO/15/U/058

31 augustus 2015

Inleiding

KPN heeft kennisgenomen van het voorontwerp voor een 'Wet op de inlichtingen- en veiligheidsdiensten 20..'. Dat voorontwerp betreft een herziening van de inrichting en bevoegdheden van de veiligheidsdiensten. KPN zal zich in deze reactie beperken tot die aspecten van de wet waar KPN, voornamelijk in de hoedanigheid van aanbieder van elektronische communicatiediensten, mee te maken heeft. Het voorontwerp heeft vergaande gevolgen voor de manier waarop KPN betrokken raakt bij de werkzaamheden van de veiligheidsdiensten.

Voor KPN is het belangrijkste punt dat het voorontwerp voorziet in een verregaande uitbreiding van bevoegdheden en van medewerkingsplichten voor een groot aantal marktpartijen. Tegelijk wordt daarmee de principiële uitbreiding van de betrokkenheid van het bedrijfsleven bij het werk van de diensten gemaskeerd. De investeringen en kosten voor de uitvoering van die uitbreiding van bevoegdheden worden voor het belangrijkste deel bij die marktpartijen, dus ook bij KPN, gelegd, zonder dat enige reële mogelijkheid is ingebouwd om invloed op die kosten uit te oefenen.

In het uitgewerkte stelsel van medewerkingsplichten op kosten van het bedrijfsleven wordt bovendien een belangrijk deel van het inzicht, de effectiviteit en de proportionaliteit van (de inzet) van de nieuwe bevoegdheden aan politieke en rechterlijke controle onttrokken. Dat is volgens KPN een fundamentele weeffout in het voorgestelde stelsel, dat dan ook heroverwogen moet worden.

In het voorontwerp zijn de negatieve gevolgen van deze uitbreiding van bevoegdheden en medewerkingsplichten voor de Nederlandse ICT- en telecommunicatiesector niet onderzocht. In het regeringsbeleid wordt erkend dat die markten voor de Nederlandse economie van cruciaal belang zijn. Een uitvoerige analyse van de effecten van de voorgestelde regels op de betrokken markten, die steeds meer internationaal zijn, is dan ook noodzakelijk. Zonder die afweging van de economische effecten kan het voorontwerp volgens KPN niet in behandeling worden genomen. Dat geldt zowel voor de directe effecten (kosten) als voor de meer indirecte effecten (vestigingsklimaat).

Vanuit de grondwettelijk gewaarborgde vrijheden – waaronder de communicatievrijheid – gelden voor aanbieders van openbare telecommunicatiediensten strenge regels. Niet naleving van die regels kan zelfs leiden tot strafrechtelijke sancties tegen betrokken personeel. KPN is zich er van bewust dat zij in haar bedrijfsvoering een belangrijke rol vervult om die grondwettelijk gewaarborgde rechten na te leven. De Wiv biedt – naast het Wetboek van Strafvordering – van oudsher de wettelijke grondslag voor de in de Grondwet toegestane inbreuken op die grondrechten. KPN heeft – sinds 1989 als zelfstandige onderneming – jarenlange ervaring met het balanceren tussen de twee tegengestelde instructies die zij uit dat kader krijgt: zowel het waarborgen van het communicatiegeheim als het medewerking verlenen aan bevoegde inbreuken daarop. Dat stelsel is gebaseerd op een nauw gedefinieerd kader en vormt – als het goed is – een evenwicht met voldoende 'checks and balances'. Aanbieders van communicatiediensten kunnen nooit in staat zijn om inhoudelijk de bevoegdheden van de diensten (en opsporing) te beoordelen, maar hooguit of er in algemene zin een wettelijke bevoegdheid (en daartegenover staande medewerkingsplicht) bestaat. De noodzakelijke controle op de uitoefening van die bevoegdheden moet dus elders worden geregeld.

KPN zal deze punten in deze reactie nader uitwerken.

Inhoud

1. De nieuwe bevoegdheden ten aanzien van telecommunicatie

KPN zal in deze reactie vooral ingaan op de bevoegdheden die in het voorontwerp zijn neergelegd voor de diensten om medewerking op te dragen voor aftappen van en gegevensverstrekking over telecommunicatie (vooral paragraaf 3.2.2.7). In de huidige Wiv 2002 bestaan dergelijke bevoegdheden al voor het gericht (op benoemde personen of aansluitingen) aftappen en gegevensvergaring. Daarnaast biedt de Wiv 2002 de mogelijkheid dat de diensten 'de ether scannen' en daarmee ongerichte draadloze communicatie kunnen vergaren. Zoals eerder al als kabinetsvoornemen geuit[1], is één van de belangrijkste redenen voor het voorontwerp de uitbreiding van deze bevoegdheden tot ongericht aftappen van kabelgebonden communicatie te realiseren. Daarnaast verbreedt het voorontwerp de bevoegdheid van aftappen en gegevensvergaring tot telecommunicatie met gebruikmaking van voorheen buiten die bevoegdheid vallende diensten en netwerken. Daarmee wordt de plicht tot medewerking aan aftappen en gegevensvergaring uitgebreid naar niet-openbare diensten en naar andere dan traditionele telecommunicatiediensten.

De wens van de diensten tot uitbreiding is deels al eerder in het parlement aan de orde geweest. In wetsvoorstel 30553 ('Wijziging Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede enkele andere wijzigingen') werd voorgesteld door aanpassing van de art. 28 en 29 WivD 2002 ook aanbieders van niet openbare communicatiediensten verplicht te stellen de daar bedoelde gegevens te verstrekken, waarmee het nooit in werking getreden artikel 13.7 voor de gegevensverstrekking van de art. 13.2a en 13.4 de facto toch zou zijn ingevoerd. Na grote bezwaren vanuit de Eerste Kamer is dit wetsvoorstel destijds ingetrokken.

> **De redenen om zonder beperking ook besloten communicatie te onderwerpen aan alle bevoegdheden die in het voorontwerp worden opgenomen zijn onvoldoende onderbouwd.**

Bij de onderbouwing van de noodzaak van de nieuwe bevoegdheden worden de verschillende redenen (terrorisme, tegengaan spionage, beschermen tegen digitale aanvallen, inzicht in bedreigingen, doorgronden intenties van een aantal landen, zicht op capaciteitsontwikkelingen van risicolanden) over één kam geschoren. Hieraan wordt de conclusie verbonden dat hiervoor adequate toegang tot telecommunicatie nodig is. De reden waarvoor toegang tot telecommunicatie nodig zou kunnen zijn zou echter moeten worden opgesplitst in defensieve- (C) en inlichtingen- (A) taken (zoals in artikel 10 van de WiV omschreven). Per taak of doel zou de wetgever extra restricties moeten opleggen.

Voor het onderzoek naar digitale aanvallen voor defensieve redenen (C-taak) kan misschien toegang tot infrastructuur nodig zijn. Deze toegang zou zich dan wel moeten beperken tot het signaleren van de aanval. Hiervoor is ongerichte ('bulk') interceptie niet nodig maar kan men zich beperken tot het gericht detecteren/signaleren van de aanval. Hierna kunnen met getroffen en betrokken partijen (zoals telecombedrijven) defensieve maatregelen genomen worden. Daarvoor is nauwe samenwerking nodig tussen de dienst en bedrijven en zouden de diensten niet alleen zelfstandig moeten opereren. In deze samenwerking zouden de diensten ook gebruik kunnen maken van de mogelijkheid om bedrijven zelf de aanvallen te signaleren door de *signatures* te delen binnen een vertrouwd netwerk. Ten aanzien van het

[1] Brief Minister BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 21 november 2014 bevattende het Kabinetsstandpunt herziening interceptiestelsel Wiv 2002.

beschermen tegen digitale aanvallen wordt impliciet verondersteld dat de diensten daadwerkelijk zouden kunnen ingrijpen in netwerkverkeer. Zoals nader zal worden aangegeven (par. 13) is dit zeer onwenselijk. Aanbieders dienen hun (mede wettelijk opgedragen) taken om continuïteit en veiligheid van communicatie te garanderen zonder directe technische inmenging te kunnen uitvoeren. Voor de inlichtingentaak (A) geldt dat aanbieders onvoldoende bekend zijn met wat er op dit vlak allemaal speelt om te kunnen beoordelen in hoeverre ongerichte interceptie noodzakelijk is en of niet gerichte interceptie evenzeer de doelstellingen dient. Het zou beter gemotiveerd moeten worden waarom gerichte interceptie niet de beoogde doelden kan dienen. Als al ongerichte interceptie noodzakelijk is dient in elk duidelijk te worden gemaakt dat de verantwoordelijkheid van aanbieders centraal staat en de diensten niet actief kunnen ingrijpen op het verkeer.

Bij de definiëring van bevoegdheden tot ongerichte interceptie wordt te weinig onderscheiden naar de verschillende taken van de diensten. Door daarin wel duidelijker te differentiëren kunnen bevoegdheden meer doelgericht en proportioneel worden geformuleerd en kunnen medewerkingsplichten beter worden beschreven,

2. Noodzaak tot adequate toetsing aan juridisch kader

De belangenafweging tussen waarborging van het grondwettelijke communicatiegeheim en de noodzaak om ter waarborging van de nationale veiligheid daarop inbreuken toe te staan is de kern van de bepalingen over het onderzoek van elektronische communicatie. Die belangenafweging is in belangrijke mate een politieke afweging, maar kan niet geïsoleerd van het bestaande juridische kader worden bekeken. Nederland is door verdragen gebonden aan de waarborging van persoonlijke vrijheden. In recente rechterlijke uitspraken is aangetoond dat die verdragsrechtelijke regels beperkingen stellen die verder gaan dan waarmee politieke besluitvorming rekening houdt. Een belangrijk voorbeeld daarvan is de onverbindend verklaring van de Richtlijn bewaarplicht[2] en de daarop volgende buitenwerkingstelling van de Nederlandse implementatie daarvan.[3] Hoewel aanbieders de investeringen voor de voorzieningen die nodig waren om de daaruit voortvloeiende regels na te leven voor eigen rekening hebben moeten nemen, blijkt achteraf dat daarvoor geen legitieme grondslag bestond.

Ten aanzien van dit voorontwerp doet zich hetzelfde risico voor. In een recente studie hebben Eskens, Van Daalen en Van Eijk een uitvoerige analyse van de toepasselijke juridische kaders gepubliceerd, specifiek gericht op het toezicht op nationale veiligheidsdiensten.[4] De 'tien standaarden' van de studie geven invulling aan het noodzakelijke systeem van *checks and balances* dat volgens het geldende internationale recht noodzakelijk is. KPN volstaat er hier mee naar die studie te verwijzen, maar gaat ervan uit dat die bij de verdere behandeling van het voorontwerp zal worden betrokken.

Voorkomen moet worden dat opnieuw onverbindende regels worden ingevoerd die leiden tot lasten voor het bedrijfsleven.

---

[2] De Richtlijn bewaarplicht (2006/24/EG) werd door HvJ EU 8 april 2014 (C-293/12 en C-594/12) onverbindend verklaard, omdat die onvoldoende waarborgen bevatte om de werking van de bewaarplicht te beperken tot voldoende ernstige situaties en om de beveiliging van de gegevens en het onbevoegd gebruik daarvan tegen te gaan.

[3] Rb. Den Haag (vzr.) 11 maart 2015 (ECLI:NL:RBDHA:2015:2498).

[4] *Ten standards for oversight and transparancy of national intelligence services*, Sarah Eskens, ot van Daalen en Nico van Eijk, IViR, juli 2015.

3. Proportionaliteit nieuwe bevoegdheden onvoldoende onderbouwd

Zowel bij het creëren van bevoegdheden – en daartegenover staande medewerkingsplichten voor ondernemingen – als bij de toepassing daarvan dient de proportionaliteit van het instrument te worden afgewogen tegen het daarmee gemoeide belang. Lezing van het voorontwerp leert dat die afweging niet kan plaatsvinden op basis van de verstrekte zeer algemene informatie. Op de noodzaak van de zeer brede bevoegdheid tot ongericht aftappen wordt slechts in algemene bewoordingen ingegaan. Daarbij wordt een beroep gedaan op het zeer vertrouwelijke karakter van inlichtingenwerk. Dat argument is in veel discussies – en in de praktische uitvoering van de taplasten – het enige dat naar voren wordt gebracht, maar is gezien de geldende juridische kaders onvoldoende om de verregaande inbreuk te rechtvaardigen.

> **Tijdens de parlementaire behandeling zal er noodzakelijkerwijs een modus moeten worden gevonden om het parlement wel een veel diepgaander analyse van nut en noodzaak van de bevoegdheden te kunnen laten maken.**

Voor wat betreft de proportionaliteit van de op te leggen medewerkingsplichten is het voorontwerp eveneens vaag. Er wordt aangegeven dat dit 'onderwerp van overleg met betrokken marktpartijen' zal zijn. Daarmee onttrekt een beoordeling van de daadwerkelijke gevolgen zich echter aan de voorafgaande democratische controle. En toetsing achteraf is praktisch ook lastig. De medewerkingsplicht voor ondernemingen is voorzien van vergaande geheimhoudingsplichten en onttrekt zich – zoals de ervaring leert – aan enige mate van adequate rechtsbescherming. Zodra een bevoegdheid in de wet is neergelegd dienen aanbieders de facto de door de diensten aangegeven invulling daarvan na te leven, omdat de – strafrechtelijk gesanctioneerde – geheimhoudingsplicht zich ertegen verzet dat een aanbieder in een openbare discussie of juridische procedure inzicht zou geven in de aard en omvang van de aangegeven invulling. Bij concreet gedefinieerde wettelijke medewerkingsplichten kan de parlementaire behandeling een waarborg van de proportionaliteit zijn, maar hoe breder de omschreven de medewerkingsverplichting is, des te minder controle en toezicht er in de praktijk is. Hoe algemener de bevoegdheid en de medewerkingsplicht is, hoe hoger de bewijslast zou moeten zijn voor wetgever van de noodzaak. Maar juist hierin schiet het voorgelegde voorontwerp tekort.

> **Volgens KPN kan het voorontwerp zonder adequate analyse van de gevolgen van de uitbreiding van de medewerkingsplichten voor aftappen en gegevensvergaring niet in behandeling worden genomen in het parlement. De effecten van die uitbreiding op de bedrijfsvoering van betrokken ondernemingen, op de algemene betrouwbaarheid en veiligheid van de communicatiediensten, op het vestigingsklimaat in Nederland en op de ontwikkeling van de 'interneteconomie' zijn onvoldoende onderzocht.**

4. 'Techniekonafhankelijkheid' als misleidende etikettering

Op vele plaatsen wordt in de toelichting aangegeven dat de uitbreiding van bevoegdheden van de diensten een logische en technisch noodzakelijke stap is om de bevoegdheden 'techniekonafhankelijk' te maken. De beperking van de bevoegdheid tot ongerichte interceptie van 'alleen' draadloze communicatie wordt als een achterhaalde technische beperking gepresenteerd.

Met deze presentatie wordt versluierd dat de uitbreiding van bevoegdheden een zeer wezenlijke verandering meebrengt in de rol van vele private ondernemingen bij het werk van de diensten. De bestaande wettelijke bevoegdheden tot het ongericht aftappen van draadloze communicatie leidt niet tot enige medewerkingsplicht of verantwoordelijkheid van aanbieders van de betrokken mobiele diensten. Die bestaande bevoegdheid maakt gebruik van de technische mogelijkheid om draadloze communicatie zonder medewerking te kunnen onderscheppen. De diensten zullen die onderschepte informatie zonder medewerking van die aanbieders moeten trachten te herleiden tot begrijpelijke informatie.

De veronderstelde 'logische uitbreiding' van de bevoegdheid om ook kabelgebonden infrastructuur ongericht te kunnen aftappen leidt echter tot verregaande nieuwe medewerkingsplichten van betrokken aanbieders. Niet alleen worden daarbij de technische middelen opgerekt, maar ook wordt de kring van diensten en dienstaanbieders die worden onderworpen aan deze nieuwe medewerkingsverplichting uitgebreid. Alle aanbieders van besloten en openbare netwerken en besloten of openbare telecommunicatiediensten en van internetapplicaties waarmee gecommuniceerd kan worden vallen onder het voorontwerp. Ook voor mobiele netwerken gaat een medewerkingsplicht gelden, waar die nu niet bestaat.

Op die uitbreiding van medewerkingsplichten wordt volstrekt onvoldoende ingegaan in de toelichting. Misschien dat voor de wensen van de diensten de uitbreiding slechts een kleine stap is, maar door daarvoor – anders dan voorheen – medewerking nodig te hebben van een onbenoemd groot aantal bedrijven wordt een principieel nieuw kader geschapen. Daaraan zitten veel verschillende aspecten, waarvan KPN in het navolgende een aantal belangrijke aspecten zal aanstippen, zoals de proportionaliteitstoetsing, de gevolgen voor de geheimhouding en de potentiële gevolgen voor het vestigingsklimaat en de marktwerking.

> **Volgens KPN verdient de principiële uitbreiding van de medewerkingsplicht van een groot aantal bedrijven een aparte afweging. Anders dan voorheen wordt ten aanzien van het aftappen van ongerichte communicatie een vergaande inbreuk op de bedrijfsvoering opgelegd, zonder voldoende afweging en inzicht in de feitelijke gevolgen voor betrokken marktpartijen.**

5. Betrokken aanbieders met medewerkingsplichten

In artikel 31 wordt ervoor gekozen om voor de definitie van de 'aanbieder van een communicatiedienst' voor wie medewerkingsplichten gelden aan te sluiten bij de definitie van het Cybercrimeverdrag (die ook wordt gebruikt in artikel 126la Strafvordering) en niet bij de definities van de Telecommunicatiewet. Volgens de toelichting vallen onder deze definitie '*niet alleen de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten als hiervoor aangegeven, maar ook die van de besloten netwerken en diensten (...) aanbieders van webhostingdiensten en beheerders van websites*' (p. 57). Het voorontwerp geeft de diensten bevoegdheid om de diensten van die aanbieders af te tappen en gegevens van hen te vergaren en rekt daarmee de bevoegdheid tot aftappen en het vragen om gebruikers- en gebruiksgegevens op tot ver buiten de huidige grenzen. Nu de beperking van 'openbaarheid' is vervallen geldt dat naar de letter voor alle diensten, ook als die besloten gebruikersgroepen, zoals bedrijfsnetwerken betreffen. Daarnaast wordt ook de kring van traditionele telecommunicatie ver uitgebreid door ook webhosting en beheer van websites als communicatiedienst te benoemen.

KPN herkent dat ontwikkeling van de markt meebrengt dat ook anderen dan de traditionele telecommunicatiedienstaanbieders vergelijkbare diensten aanbieden en deelt de conclusie dat gelijke behandeling van vergelijkbare diensten noodzakelijk is. Maar de oprekking van het voorontwerp tot alle openbare of besloten vormen van communicatie via geautomatiseerde werken en zelfs tot daarmee verband houdende diensten als webhosting en het beheer van websites is disproportioneel.

Het uitgangpunt van het huidige wettelijke kader – waarin de bevoegdheid van de diensten is geregeld in de Wiv 2002 en de verplichting tot medewerking van aanbieders van openbare telecommunicatiediensten daarop aansluitend in de Telecommunicatiewet – wordt (deels) verlaten. Enerzijds brengen de nieuwe bevoegdheden in het voorontwerp een beperking mee, doordat alleen aanbieders van netwerken en diensten die via een 'geautomatiseerd werk' diensten aanbieden worden gereguleerd. Aanbieders van passieve kabel (*dark fiber*) vallen daarmee buiten de definitie. Dat zij nog wel binnen de medewerkingsplichten van de Telecommunicatiewet vallen doet niet ter zake, omdat alleen als zowel de bevoegdheid als de medewerkingsverplichting een wettelijke grondslag heeft medewerking aan aftappen mag plaatsvinden.

Anderzijds betreft de bevoegdheid een grote groep aanbieders aan wie in de Telecommunicatiewet geen medewerkingsplicht is opgelegd. Het voorontwerp lost dat probleem op door in het voorstel zelf op verschillende plaatsen de medewerkingsplichten op te leggen aan aanbieders waarvoor dat niet reeds op grond van de Telecommunicatiewet geldt (zie artikelen 32 lid 7, 37 lid 6 en 39 lid 4). Daarnaast worden in de artikelen 36 lid 4 en 38 lid 4 nog voor alle aanbieders geldende medewerkingsplichten opgelegd (waarvan het laatste geval voor de aanbieders van openbare telecommunicatienetwerken en –diensten overigens ook al een verplichting bevat)

Daarmee wordt het stelsel dat *bevoegdheden* tot aftappen en gegevensvergaring in de Wiv of Wetboek van Strafvordering worden neergelegd en de daarmee samenhangende *verplichtingen* die op ondernemingen in de Telecommunicatiewet verlaten. Omdat die verplichtingen regels zijn die activiteiten van aanbieders van diensten in de betrokken sector van de interne markt zijn en geen regeling van de activiteiten van de overheid voor wetshandhaving bevatten (vergelijk HvJ EU 10 februari 2009 (C-301/06)) is het nodig al die verplichtingen in de Telecommunicatiewet neer te leggen. Dat is de wet die de activiteiten van marktpartijen regelt en de verplichtingen die zij hebben. De voorgestelde verspreide regeling verhindert niet alleen de transparantie over de ondernemingen die medewerkingsplichten opgelegd krijgen, maar is ook wet systematisch onwenselijk. Daarmee wordt ook de eenheid van toezicht door het Agentschap Telecom op de naleving van die verplichtingen (hoofdstuk 15 Telecommunicatiewet) doorbroken. De noodzaak om artikel 13.6 te pas en te onpas van overeenkomstige toepassing te verklaren (zie hierna par. 12) is dan ook overbodig.

De noodzaak deze medewerkingsplichten goed te regelen vloeit ook voort uit Europese regels. De Machtigingsrichtlijn (2002/20/EG) staat weliswaar toe dat aan ondernemingen 'met een algemene machtiging' (in Nederland: de registratie bij ACM) verplichtingen worden opgelegd, onder meer in het kader van aftappen,[5] maar wel met inachtneming van de artikelen 5, 6 7 8 en 9 Kaderrichtlijn (2002/21/EG). Dat leidt ertoe dat bij het opleggen van verplichtingen aan ondernemingen de toets op de uitgangspunten van artikel 8 Kaderricht-

[5] Zie Bijlage A onder 11 van de Richtlijn, met inachtneming van de e-Privacyrichtlijn 2002/58/EG en de algemene Privacyrichtlijn 95/46/EG.

lijn moet worden uitgevoerd. Daarmee is ook een toets op de proportionaliteit van de verplichtingen en de consistentie en concurrentie op Europese schaal voorgeschreven. Het toezicht op de verplichtingen behoort te zijn opgedragen aan een onafhankelijke Nationale regelgevende instantie (artikel 3 Kaderrichtlijn) en tegen besluiten van een NRI dient beroep open te staan (artikel 4 Kaderrichtlijn). De waarborging van die bepalingen van de Europese regelgeving is in Nederland in de Telecommunicatiewet neergelegd met het stelsel van hoofdstuk 15 (en beroep op grond van de Awb) en de verantwoordelijkheid is belegd bij het Ministerie van Economische Zaken. De naleving van de Europese regels en de controle daarop door dat Ministerie kan niet plaatsvinden als een deel van de verplichtingen en het toezicht daarop zich aan de Telecommunicatiewet onttrekt.

De werking van de wet ten aanzien van de medewerkingsplichten dient noodzakelijkerwijs tot Nederland te worden beperkt. Nu de communicatiedienstverlening steeds internationaler wordt zullen veel aanbieders delen van hun activiteiten buiten Nederland uitvoeren. Het moet uitgesloten worden geacht dat de medewerkingsplichten zo ver zouden gaan dat aanbieders door handelen in andere landen tot strijd met de daar geldende wetgeving zou kunnen worden gedwongen. Met opneming van de verplichtingen in de Telecommunicatiewet is dat door het daarin veronderstelde territorialiteitsbeginsel gewaarborgd.

> **Het huidige stelsel, waarin de Wiv de bevoegdheden van de diensten regelt en de Telecommunicatiewet de daartegenover staande medewerkingsplichten voor ondernemingen, moet worden gehandhaafd, mede om de uit het Europees regelgevend kader voortvloeiende regels inzake verplichtingen op ondernemingen, het toezicht daarop en de beroepsmogelijkheden tegen dat toezicht na te leven.**

6. ‘Bijzondere bevoegdheden’ vergen bijzondere controle

Aanbieders van wie medewerking wordt verlangd hebben geen mogelijkheden om te controleren of een opdracht valt onder de in artikel 23 lid 1 geformuleerde bevoegdheid. Dat is terecht, omdat het om uiterst gevoelige informatie gaat. De keerzijde daarvan is dat aanbieders slechts op procedurele aspecten kunnen toetsen en die moeten dan ook goed geregeld zijn. De inhoudelijke toetsing op de gerechtvaardigdheid van de verregaande inbreuk op de grondrechten moet in de voorfase plaatsvinden; met het aftappen en vergaren van gegevens is immers de inbreuk al gepleegd en toezicht achteraf kan hooguit preventief werken voor toekomstige situaties, maar niet een eventuele onrechtmatige inbreuk op de grondrechten achteraf corrigeren. De cruciale vraag is of het gezien de ernst van de inbreuk gerechtvaardigd is dat de voorafgaande toetsing alleen berust bij de betrokken minister. De analyse in het in voetnoot 1 genoemde rapport leert dat een vorm van onafhankelijk toezicht op zulke vergaand ingrijpende bevoegdheden noodzakelijk is. De betrokken ministers zijn in dat opzicht vermoedelijk onvoldoende onafhankelijk.

Het voorontwerp geeft weinig overtuigende argumenten om niet, net als in artikel 24 lid 4 (journalisten) en artikel 29 (brieven), rechterlijke toetsing voorafgaand aan het opleggen van deze vergaande bevoegdheden te vereisen. De rechter is in staat om te beoordelen of de reden voor aftappen verband houdt met de gronden van artikel 23 lid 1.

> **Onvoldoende is gemotiveerd waarom rechterlijke toetsing op de uitoefening van bevoegdheden die inbreuk maken op het communicatiegeheim niet nodig of mogelijk zou zijn.**

Maar indien die keuze toch zou worden gemaakt is in elk geval een basale vorm van procedureel toezicht nodig. Volgens het voorontwerp is voor het uitoefenen van de ‘bijzondere

bevoegdheden' tot het gericht aftappen van communicatie de toestemming van de verantwoordelijke minister aan het hoofd van de betrokken dienst noodzakelijk. Uit de formulering van artikelen 32 lid 2 en 37 lid 2 ('is verleend') wordt duidelijk dat de toestemming tevoren moet zijn gegeven. Naar valt aan te nemen kunnen aanbieders tot wie medewerkingsbevelen zijn gericht dan ook afgaan op een schriftelijke te tonen toestemming alvorens zij tot die medewerking mogen overgaan.

> **Om een minimale controle van een verleende bevoegdheid tot (ongericht) aftappen mogelijk te maken is het wenselijk in de wet op te nemen dat de toestemming van de minister schriftelijk wordt verleend en (daarmee) aan de aanbieder van wie medewerking wordt verlangd kan worden getoond.**

Volgens artikel 32 lid 9 is voor militair telecommunicatieverkeer met oorsprong of bestemming in andere landen zelfs helemaal geen toestemming nodig. In de toelichting wordt aangegeven dat dit onder huidige Wiv 2002 al geldt voor draadloze communicatie en dit nu eenvoudig wordt uitgebreid naar kabelgebonden interceptie. Ook hier wordt er aan voorbijgegaan dat anders dan bij het onderscheppen van verkeer uit de ether er daarbij de zeer brede medewerkingsplichten gelden. De regeling zou meebrengen dat er in die gevallen geheel geen controle bestaat voor aanbieders om te verifiëren of hun medewerking gebaseerd is op een rechtmatige inbreuk op het grondwettelijk gewaarborgd communicatiegeheim. Zij moeten – om het plastisch te zeggen – louter afgaan op het militair gezag. Bij verdergaande samenwerking van de diensten op het gebied van operationele aftapfaciliteiten ontbreekt daarmee iedere vorm van waarborg voor de legitimiteit van aftappen.

> **Het is noodzakelijk om voor alle opdrachten tot medewerking aan tapverzoeken een toestemming van de minister verplicht te stellen; artikel 32 lid 9 dient te worden geschrapt (of beperkt tot aftappen waarvoor geen medewerking van een aanbieder nodig is).**

Het valt op dat in artikel 32 de toestemming tot aftappen niet aan een termijn is gebonden. Er is geen goede reden om hier af te wijken van het uitgangspunt van artikel 24 lid 3 dat de toestemming voor een (verlengbare) periode van maximaal drie maanden mag worden gegeven.

> **De toestemming van artikel 32 moet aan een termijn worden gebonden.**

7. Medewerking aan ongericht aftappen (in het licht van technologische ontwikkelingen)

De belangrijkste vernieuwing van het voorontwerp is de regeling van de 'ongerichte interceptie van kabelgebonden infrastructuur' in de artikelen 33-40. De noodzaak tot die uitbreiding wordt in de toelichting (p. 63-64) onderbouwd met algemene opmerkingen over de groei van communicatie (lees: data) verkeer en de stelling dat 'inmiddels ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt'. Dat de hoeveelheid dataverkeer strek groeit is juist, maar dat het allergrootste deel daarvan via vaste betwerken verloopt is nooit anders geweest. Sterker: mobiel internet is relatief recent pas tot ontwikkeling gekomen en de groei ervan verloopt inmiddels veel sneller dan die via vaste netwerken. Voor de stelling dat het 'in bulk intercepteren in het kabelgebonden domein (…) onmisbaar' is wordt geen feitelijkbewijs geleverd.

Zoals al aangegeven is het grootste – en principiële – verschil tussen aftappen 'in bulk' van verkeer uit de ether en van verkeer via kabelgebonden infrastructuur dat het laatste altijd

betekent dat de diensten ingrijpen in bedrijfsmiddelen van aanbieders. Weliswaar gaat het voorontwerp ervan uit dat dit geschiedt op basis van opgelegde 'medewerking' van die aanbieder, maar het betekent wel dat aan de brede categorie van ondernemingen (zie hierboven, par. 5) zo'n medewerkingsplicht wordt opgelegd. De toelichting bagatelliseert het effect daarvan:

> *Voor de uitoefening van de bevoegdheid tot interceptie van kabelgebonden telecommunicatie zal in de praktijk de medewerking vereist zijn van de desbetreffende aanbieder van de communicatiedienst (in casu de netwerkaanbieder). Deze medewerking is zowel vereist bij het verkrijgen van informatie van relevante aanbieders met het oog op het in kaart brengen van het zogeheten communicatielandschap (in brede zin) als de concrete formulering van de inhoud van het verzoek om medewerking (de last); zie artikel 36 van het wetsvoorstel. Voorts is medewerking vereist bij de uitvoering van de last, zij het dat daartoe niet eerder wordt overgegaan dan nadat ter zake met de desbetreffende aanbieder overleg is gevoerd; zie artikel 37 van het wetsvoorstel. (p. 64).*

De realiteit in de ontwikkeling van de telecommunicatie is dat verkeer steeds moeilijker is te onderscheiden naar gebruiker, bestemming, netwerk, gebruikte netwerkelementen, etc. Het traditionele telefoonverkeer – met nog enigszins (maar ook al snel steeds minder) te volgen routes – wordt vervangen door transport op IP basis, waarbij ontwikkelingen als netwerkvirtualisering, versleuteling van gegevens en dergelijke het steeds onmogelijker zullen maken om bepaald verkeersstromen te definiëren en op te sporen.

In de toelichting wordt niet op deze ontwikkelingen ingegaan. Er wordt geen inzicht gegeven in de steeds groter wordende complexiteit om bepaalde verkeersstromen te onderscheiden. De effectiviteit van het aftappen van verkeer op bepaalde punten wordt daarmee uitgehold. Alleen door alle verkeer – langs vele wegen en aanbieders – te onderscheppen en analyseren zou een concrete verkeersstroom of patroon in kaart kunnen worden gebracht. Er wordt geen inzicht gegeven in de vraag of de diensten met de bestaande middelen en kennis überhaupt daartoe in staat zijn.

> **Het wetsvoorstel geeft een veel te simpel beeld van de mogelijkheden om met de snelle technologische ontwikkelingen de in de toelichting beoogde doelen uit te voeren. Het is voor een goede beoordeling van de effectiviteit van de bevoegdheden en medewerkingsplichten noodzakelijk om een veel diepgaander inzicht te geven in de complexiteit en in de mogelijkheden (en kosten) voor de diensten om met die complexiteit om te gaan.**

Wel geeft de toelichting aan dat een 'voordeel' van de techniekonafhankelijke medewerkingsplicht is dat ook aanbieders van mobiele netwerken – op wie voorheen geen medewerkingsplicht rustte – nu onder de werking van artikel 36 en 37 vallen (p. 79). Waar voorheen de diensten zonder hun medewerking (en kosten) bevoegd waren om draadloze communicatie ongericht te kunnen aftappen, kunnen ze dat nu ook opdragen aan de mobiele aanbieders. De stelling dat het alleen gaat om een uitbreiding in het kabelgebonden domein wordt daarmee nog verder geweld aangedaan.

Het grote gevaar van de regeling is dan ook dat aanbieders op basis van artikel 36 consultancy moeten bieden om de diensten inzicht te geven in de manier waarop bepaalde verkeerstromen (kunnen) lopen en hun rol daarin en vervolgens op basis van artikel 37 voorzieningen moeten aanleggen teneinde in voorkomende gevallen in staat te zijn om daadwerkelijk ongericht af te tappen als daar een concreet verzoek toe komt. Het allergrootste deel van deze consultancy en voorbereidingshandelingen dient te geschieden voor rekening van de aanbieders, maar aannemelijk is dat niet of nauwelijks van de voorzieningen

gebruik zal worden gemaakt omdat de gegevens ofwel te omvangrijk zijn om redelijkerwijs te kunnen verwerken, ofwel niet volledig genoeg omdat slechts beperkte delen van verkeer in kaart kan worden gebracht. Het is niet aanvaardbaar dat dit pas door 'trial and error' duidelijk wordt en intussen de markt die trial and error heeft moeten (mee) financieren. Met dit stelsel is iedere proportionaliteitstoets verdwenen. Lasten worden afgeschoven op het bedrijfsleven en daarmee buiten de controle op de diensten gelaten.

De zorg van KPN hierover is mede gebaseerd op ervaringen in de veel concretere huidige praktijk van aftappen onder de geldende wettelijke regeling. Volgens het stelsel van de Telecommunicatiewet mogen telecommunicatiediensten pas worden aangeboden als ze aftapbaar zijn (artikel 13.1 Telecommunicatiewet) en moet de aanbieder op basis van die voorbereiding concrete tapverzoeken van behoeftestellers naleven (artikel 13.2 Telecommunicatiewet). Voor de 'standaardtaps' zijn in het Besluit aftappen openbare telecommunicatienetwerken en –diensten en de daarop gebaseerde Regeling aftappen openbare telecommunicatienetwerken en – diensten, nadere specificaties en eisen gesteld. Daarmee kunnen aanbieders daarop zijn voorbereid. Dat geldt niet voor de minder vaak voorkomende typen taps, zoals bijv. een tap voor uitgaand e-mailverkeer. Daarvoor zijn geen specificaties en kan lastig tevoren worden beoordeeld of de aanbieder aan de concrete eisen van individuele tapverzoeken kan voldoen.

> In een proefprocedure op verzoek van behoeftestellers heeft het Agentschap Telecom in 2009 aan KPN een last onder dwangsom opgelegd voor het niet voldoen aan verzoeken tot het plaatsen van een tap voor 'uitgaande e-mail'. Het verweer van KPN dat daarvoor geen specificatie was vastgesteld of overeengekomen en KPN dus in onzekerheid verkeerde over de manier waarop zij aan een dergelijke last kon voldoen werd verworpen door Rechtbank Rotterdam 6 januari 2011, ECLI:NL:RBROT:2011:BP0012. Volgens de rechtbank was het ontbreken van overeengekomen specificaties geen grond om een last niet uit te voeren: '*De rechtbank merkt daarbij op dat door KPN niet is betwist dat, na enige investeringen, het technisch mogelijk is om uitgaande e-mail te tappen. Om aan zo'n last te kunnen voldoen, zo stelt KPN in haar beroep, zou zij op haar servers specifieke daarop ingerichte filters moeten plaatsen. Door het plaatsen van dergelijke filters is KPN derhalve in staat om aan de bijzondere taplasten te voldoen.'* Dat KPN alvorens een technische implementatie te realiseren waarvan voldoende zekerheid bestond dat die ook door behoeftestellers zou worden geaccepteerd, zodat niet bij een iets ander geformuleerd verzoek iets anders zou worden verlangd wordt door de rechtbank eveneens verworpen: '*De stelling van KPN, dat een termijn van twee weken om aan de last te voldoen niet haalbaar is, ziet niet zozeer op de technische realiteit doch in de omstandigheid dat KPN, alvorens over te gaan tot niet geringe investeringen, van de behoeftestellers wenst te vernemen voor welke technische optie gekozen moet worden om de specifieke voorzieningen in het netwerk te bouwen (eenduidige implementatie). KPN heeft in dit kader gesteld dat zij al enige jaren bezig is om van de behoeftestellers meer duidelijkheid te verkrijgen op welke wijze zij het beste haar netwerk kan inrichten om uitvoering te geven aan een e-mailtap, en dat de termijn van twee weken haar geen enkele ruimte laat voor het streven naar overeenstemming op dit punt. Wat hier ook van zij, uit het dossier blijkt dat tot op heden ondanks diverse bijeenkomsten en workshops nog steeds geen (hernieuwd) protocol voor de wijze waarop het aftappen van e-mailverkeer dient plaats te vinden, is vastgesteld. Derhalve zou ook een langere begunstigingstermijn niet het door KPN gewenste resultaat hebben gehad.'* Dat een aanbieder daarmee voor niet in de lagere regelgeving beschreven vormen van aftappen in grote onzekerheid verkeert ten aanzien van de vraag wanneer zij voldoet aan de verplichting tot 'aftapbaarheid' is voor de rechtbank geen grond om te veronderstellen dat geen last onder dwangsom kan worden opgelegd totdat die duidelijkheid er is: '*De rechtbank stelt vast dat de Regeling aftappen geen regels bevat die van toepassing zijn op de dienst e-mail, zodat uitsluitend de al-*

gemene regels uit de Tw en het Besluit gelden. (...) Dit betekent dat de formulering van de last leidend is voor de omvang van de verplichting die op de aanbieder rust tot medewerking aan de uitvoering van een bevoegd gegeven taplast. Het bevel tot het opnemen van (alle) communicatie via het in de bijzondere last genoemde e-mailadres is dus voldoende om zowel het ingaande als uitgaande e-mail te verkrijgen. Hieruit volgt dat de van KPN gevraagde medewerking niet treedt buiten de wettelijke verplichtingen die uit artikel 13.1 en 13.2 van de Tw voortvloeien.'

In het vervolg op deze zaak heeft KPN exact [GEHEIM] tapopdrachten moeten uitvoeren als in de last onder dwangsom van het AT omschreven. In het woord 'geheim' in de vorige zin zit precies het probleem voor aanbieders om tot een redelijke invulling te komen: zij mogen informatie hieromtrent niet openbaar maken, de Ministers doen het zelf ook niet voldoende en dus kan besluitvorming en wetgeving niet worden gebaseerd op daadwerkelijke informatie. De Ministers weten als het goed is wel welk cijfer achter het woord 'geheim' schuil gaat en zouden dat op verzoek van het parlement zonder probleem van KPN mogen onthullen. Dat zou meer inzicht kunnen geven in het proportionaliteit van te maken kosten.

Teneinde meer inzicht te geven in de proportionaliteit van de op te leggen medewerkingsplichten zou meer inzicht moeten worden gegeven in de huidige praktijk van taplasten op verschillende typen taps en de daarmee voor aanbieders gemoeide kosten. Dat kan zonder inzicht te geven in de redenen voor behoeftestellers om taplasten te geven.

De grote zorg die KPN heeft op grond van haar ervaringen is dat de nieuwe bevoegdheid ertoe zal leiden dat het bedoelde 'overleg' met aanbieders zal leiden tot aanpassingen in netwerken en diensten om concrete ongerichte tapverzoeken te kunnen doen, terwijl volstrekt onduidelijk is of daar wel gebruik van zal worden gemaakt. De toelichting erkent dat het hier om 'maatwerk' zal gaan (p. 82), wat in de praktijk vaak tot bijzondere, operationeel complexe en ingrijpende oplossingen, leidt. Weliswaar geeft artikel 37 lid 6 de 'geruststelling' dat voorzieningen 'slechts' 12 maanden na de periode waarvoor toestemming is verleend in stand behoeven te worden gelaten, maar geenszins wordt uitgesloten dat een nieuwe toestemming zal volgen. Eenmaal gebouwd (op eigen kosten; zie par. 12) zal een voorziening daarom niet snel afgebroken kunnen worden ter besparing van meermalige investeringen. Ook veronderstelt de toelichting bij voorbaat reeds (p. 84) dat eenmaal opgedragen medewerkingsplichten 'bijvoorbeeld als gevolg van wijzigingen in de onderzoeksopdrachten van de diensten' aangepast kunnen worden. Ook dat is jegens aanbieders die daaraan medewerking moeten verlenen meer een dreigement van nutteloos te maken kosten dan een geruststelling.

Op p. 83 van de toelichting wordt aangegeven dat voor de medewerking van de in artikel 33 lid 1 neergelegde bevoegdheid 'een beperkt aantal – en dus niet alle – aanbieders in aanmerking' komt. Het is niet duidelijk waarop die geruststelling ziet. Artikelen 36 en 37 kennen geen beperking. Voor zover wordt bedoeld dat de diensten – ook al geldt de bevoegdheid alle communicatiedienstaanbieders – in de praktijk slechts voornemens zijn om alleen een door hen geselecteerd aantal aanbieders opdrachten te verlenen is deze opmerking voor KPN echter eerder zorgelijk dan geruststellend. Dat zou betekenen dat die diensten vermoedelijk 'de grote vijf' (KPN, Ziggo, Vodafone, T-Mobile en Tele2) op het oog hebben, alsmede enkele grote spelers in de verdere waardeketen als AMS-IX, Google, Facebook (Whatsapp) en Microsoft (Skype). Dat zou betekenen dat ook bij gelijke verplichtingen die partijen de lasten van de medewerkingsplicht dragen en zij in concurrentie met andere partijen een verder kostennadeel krijgen opgelegd (zie ook par. 12).

Het wetsvoorstel laat daarmee zeer veel onduidelijkheid bestaan over de reikwijdte van de medewerkingsplichten. Voor de aanbieders die vallen onder artikel 13.1 Telecommunicatiewet – dat ongewijzigd blijft – zou de invoering van de artikelen 36 en 37 van het voorontwerp in theorie betekenen dat zij elke denkbare vorm van 'ongericht aftappen' in hun netwerken en diensten voorbereid zouden moeten hebben. Hopelijk is dat een niet bedoelde consequentie van het wetsvoorstel, maar in elk geval is die conclusie niet realistisch.

> **In het voorontwerp dient het uitgangspunt dat telecommunicatienetwerken 'aftapbaar' moeten zijn voor nog allerlei onbekende vormen van ongericht aftappen expliciet te worden aangepast. Van aanbieders kan niet worden verwacht dat zij zich voorbereiden op technische eisen waarvan de diensten zelf nog niet kunnen aangeven welke dat zijn.**

Er lijkt daarnaast in artikel 36 te worden gevraagd naar een 'communicatie matrix'. Dit zal in de praktijk vaak redelijkerwijs niet opgeleverd kunnen worden. In toenemende mate wordt data getransporteerd over een veelheid van netwerken en in verschillende vormen. Een concrete vraag kan wellicht gericht beantwoord worden, aanbieders zijn veelal niet (c.q. ook nog steeds minder) in staat verdergaande algemene onderzoeken te doen. Dit geldt zowel voor internationale als nationale netwerken.

Tot slot dient hier nog te worden opgemerkt dat – indien al bevoegdheden en medewerkingsplichten ter zake van ongericht aftappen worden opgenomen – in elk geval moet worden bewaakt dat aanbieders niet gedwongen kunnen worden tot wijzen van uitvoering waarbij hen de mogelijkheid wordt ontnomen om te kiezen voor de minst ingrijpende manier van medewerking. Het wetsvoorstel bevat ter zake geen enkele waarborg. Het stelsel van de artikelen 36 en 37 van het voorontwerp roepen zoveel vragen op dat KPN in deze fase nog niet op alle mogelijke gevolgen kan reageren. Het is aan de diensten om in de wetgevingsfase daarover meer inzicht te geven. Pas daarna kunnen marktpartijen adequaat reageren op wat dit in concreto voor hen kan betekenen.

8. Medewerking aan decryptie

Een medewerkingsplicht van iets andere aard in neergelegd in artikel 41 van het voorontwerp. Iedereen die kennis draagt van 'de wijze van versleuteling' van elektronische communicatie dient desgevraagd de diensten te ondersteunen. Ook al is toestemming van de Minister nodig, toch is de bepaling opvallend in de ongeclausuleerdheid van de bevoegdheid. Het lijkt een 'risk-free' activiteit voor de diensten om derden-deskundigen in te schakelen voor de decryptie van communicatie; geheimhouding is opgelegd en in een vergoedingsregeling van de deskundige is niet voorzien. Er wordt niet vereist dat er enig verband is tussen de persoon en de gebruikte sleutels. Ietwat gechargeerd gezegd: het wetsvoorstel geeft geen positieve incentive voor onafhankelijk cryptografie onderzoek en expertise in Nederland.

De kans is aannemelijk dat de diensten in concrete gevallen geen inzicht hebben in de toepassing van versleuteling en door wie die is aangebracht. Het kan gaan om versleuteling als onderdeel van een communicatiedienst, maar ook om versleuteling die door aanbieders van websites of end-to-end diensten, of op basis van beschikbare software door bepaalde (besloten) gebruikersgroepen worden aangebracht. Het risico bestaat dat de diensten eenvoudigweg slechts enkele partijen tot medewerking aanspreken en dat zonder vergoeding. Daarmee wordt verdere onevenredigheid bereikt, doordat zulke partijen medewerking wordt opgedragen ten behoeve van mede buiten hun domein liggende versleutelingen.

Aanbieders van openbare telecommunicatiediensten worden vanuit hun zorgplicht voor veiligheid en privacy zelf al gedwongen zo veel en veilig mogelijk te versleutelen en ook andere partijen hebben deze noodzaak. Hierin wordt veel geld geïnvesteerd. Een veilige versleuteling betreft in veel gevallen sterk wisselende sleutels, die niet zonder complexe handelingen uit communicatie systemen kunnen worden verkregen. Als het vrijmaken van de sleutel al mogelijk is brengt dit hoge kosten met zich mee die alle partijen zelf dragen. Dus hoe beter aanbieders hun 'goed huisvaderschap' (cybersecurity, privacy, bedrijfscontinuïteit) waarmaken en daarvoor hoge kosten maken, des te groter lijkt het risico dat ze aan een opdracht tot verplichte medewerking van de diensten ontsleuteling te voldoen. Indien de kosten bij de aanbieders liggen – zeker voor wat betreft (naar komt vast te staan) ziet door henzelf toegepaste sleutels – ontstaat daarmee een prikkel om zo min mogelijk of zo simpel mogelijk te versleutelen. Alleen volledige kosten vergoeding maakt het acceptabel, en zal ook de juiste terugkoppelingen naar de overheid tot gevolg hebben die nodig zijn om alleen de juiste vragen aan de juiste partij te stellen.

> **De bevoegdheid voor de diensten om medewerking op te dragen aan personen die kunnen bijdragen aan het doorbreken van aangebrachte cryptografie dient beperkt te worden tot personen die in hun functie of bedrijfsvoering betrokken zijn bij het aanbrengen of verwijderen van de desbetreffende cryptografie. Buiten die beperktere medewerkingsplicht dient een redelijke vergoeding voor de in te schakelen derden te worden geregeld.**

Voor aanbieders van communicatiediensten geldt daarenboven dat hun bijzondere rol bij het mogelijk maken van beveiligde communicatie volgens de eisen van de techniek nog aanvullende beperkingen mee behoort te brengen. Daarop wordt hierna in par. 13 nader ingegaan.

9. Effecten op de bedrijfsvoering

Uit paragraaf 7 bleek al dat KPN op basis van de ervaringen met de huidige verplichting om voorbereid te zijn op en medewerking te verlenen aan verzoeken tot het gericht aftappen, grote zorgen heeft over de gevolgen voor haar bedrijfsvoering van de nog veel onduidelijker en potentieel verdergaande vormen van ongericht aftappen.

Voor de belangrijkste vormen van gericht aftappen (telefonie, IP-tap) zijn er – ook internationale – standaarden beschikbaar, maar voor de voorgestelde vormen van tappen en medewerking niet. Mogelijk dat telecomaanbieders in andere landen daar ervaring mee hebben, maar omdat die – net zoals in Nederland – aan geheimhouding zijn onderworpen kunnen Nederlandse aanbieders daarover geen inzicht krijgen. Evenmin is duidelijk in welke omvang de diensten van de nieuwe bevoegdheden gebruik zullen gaan maken.

Dat betekent dat bij eventuele invoering van de bevoegdheden er onduidelijke en onzekere effecten voor de bedrijfsvoering van een groot aantal ondernemingen zal zijn. Het gaat daarbij niet alleen om het voeren van het in de artikelen 36 en 37 van het voorontwerp bedoelde overleg en de implementatie van concrete voorzieningen die daaruit voortvloeien, maar ook om voorzieningen die aanbieders moeten treffen om bijkomende verplichtingen als geheimhouding in hun organisatie te realiseren, om de impact op andere processen en systemen in kaart te brengen en te bewaken, etc. Al in de huidige praktijk constateert KPN dat de medewerkingsplichten leiden tot inflexibiliteit voor de aanbieder (extra eisen in netwerk- en dienstarchitectuur wijzigingen, etc.). Met de nog niet ingevulde eisen ten aan-

zien van de veel bredere medewerkingsplichten zal de inflexibiliteit en zelfs mogelijke rem op innovatie nog worden versterkt.

Een inhoudelijke reactie op de praktische consequenties voor aanbieders vergt een veel diepgaander inzicht in de concrete invulling van medewerkingsplichten, waarbij rekenschap wordt gegeven van de snelle technologische ontwikkelingen. Het voorontwerp kan pas worden behandeld als dat inzicht wordt gegeven en aanbieders daarop in meer detail hebben kunnen reageren. Zonder dat dit gebeurt schrijft het wetsvoorstel in wezen een blanco cheque uit ten laste van de markt, wat in strijd is met het Europees regelgevend kader.

> **Het wetsvoorstel bagatelliseert de gevolgen voor de bedrijfsvoering van aanbieders en kan zonder nader onderzoek op dat punt en nadere motivering niet (door het parlement) op proportionaliteit worden getoetst.**

10. Markteffecten niet voldoende onderzocht

Naast de directe effecten op de bedrijfsprocessen voor betrokken ondernemingen zijn er meer indirecte effecten die in het wetsvoorstel onderbelicht blijven. Zo ontstond onlangs commotie, naar aanleiding van geruchten dat internationale verbindingen van KPN in Duitsland zouden zijn afgetapt ten behoeve van de NSA. Dit noopte KPN tot complex onderzoek, zonder dat KPN daarvoor de middelen en bevoegdheden heeft om daadwerkelijk alle feiten te achterhalen.[6] Ondernemingen komen op die manier buiten hun verantwoordelijkheid in een negatief daglicht, met mogelijke effecten voor de keuze van klanten en de afwegingen voor ondernemingen om zich al of niet in Nederland te vestigen (vestigingsklimaat).

Juist voor Nederland met een voortrekkersrol in de EU voor wat betreft de internetdienstverlening zijn er hier grote risico's, die in het wetsvoorstel niet worden onderzocht. Nederland heeft een grote rol als 'mainport' voor internettoegang voor bedrijven uit allerhande sectoren. Die bedrijven kunnen kiezen uit alle landen om toegang te krijgen, afhankelijk van het daar bestaande 'internet-eco-systeem'. Weliswaar wordt vaak als argument tegen dit vestigingsklimaat argument gebruikt 'dat alle landen om ons heen allang ongericht aftappen', maar bewijs voor deze stelling is niet geleverd. De – op zich terechte – Nederlandse transparantie met dit wetsvoorstel zorgt ervoor dat in elk geval Nederland duidelijkheid daarover geeft, maar wel op een manier die (ook al zou van die bevoegdheid slechts beperkt gebruik worden gemaakt) grote afschrikwekkende werking zal hebben.

Het rapport Dessens zegt min of meer dat Nederland in staat moet zijn te doen wat andere landen allang doen. De onthullingen over hetgeen andere landen doen met hun bevoegdheid heeft aanwijzingen gegeven over o.a. bedrijfsspionage. Weliswaar wordt in het wetsvoorstel een verbeterd (achteraf) toezicht in het vooruit gesteld, maar een analyse t.b.v. vestigingsklimaat voor grote en kleine internationale bedrijven in Nederland ontbreekt. KPN is als nationale en internationale aanbieder van online diensten afhankelijk van een aantrekkelijk/betrouwbaar vestigingsklimaat. Andere aanbieders zijn veelal internationaler en kunnen makkelijker keuzes maken om Nederland te vermijden of verlaten. Het bedoelde 'internet eco systeeem' bestaat niet alleen uit mondiale spelers op het gebied van telecom-, content (zoals Googles datacenter in Groningen) en e-commerce, maar evenzeer uit kleine innovatieve bedrijven. Het wegvallen of beperken van die economische activiteit zou nadelige gevolgen hebben voor de Nederlandse economie. Zonder onderzoek daarnaar en in-

[6] Zie http://nos.nl/artikel/2038166-kpn-onderzoekt-aftappen-verbindingen-door-duitsers.html.

zicht daarin kan niet worden beoordeeld of het veronderstelde nut van de uitbreiding van bevoegdheden daartegen opweegt.

> **Aan het wetsvoorstel dient een goed onderzoek naar de gevolgen van het vestigingsklimaat en de verdere economische gevolgen ten grondslag te worden gelegd.**

11. Bewaartermijnen communicatie

Artikel 32 lid 10 bepaalt voor gegevens die uit (gericht) aftappen zijn verkregen slechts dat die binnen 12 maanden *nadat* is vastgesteld dat ze voor het onderzoek niet relevant zijn moeten zijn vernietigd. Daarmee lijkt gezegd dat (i) voor wel relevante gegevens er kennelijk geen bewaartermijn geldt (ii) het weggooien van vastgesteld niet relevante gegevens maar liefst een jaar mag worden uitgesteld. Dit uitgangspunt is een te grote inbreuk op de grondwettelijke bescherming van het communicatiegeheim. Volgens artikel 33 lid 5 geldt voor door ongericht aftappen verkregen gegevens zelfs dat die drie jaar mogen worden bewaard en (pas) nadien hoeven te worden vernietigd als ze voor het onderzoek niet relevant zijn. Die termijn wordt – als KPN het goed interpreteert – in artikel 33 lid 6 nog onbeperkt verlengd voor zover de gegevens door encryptie niet kunnen worden ontsleuteld. Daarmee ontstaan bewaartermijnen, niet alleen voor de verkeersgegevens, maar ook voor de inhoud van de communicatie, die in het licht van andere discussies over bewaartermijnen van persoonsgegevens onverdedigbaar lang zijn.

In de toelichting op de artikel 33 tot en met 35 wordt uitvoerig ingegaan op alle mogelijkheden die ongericht geïntercepteerd en opgeslagen telecomverkeer kan hebben voor de diensten. Het is aannemelijk dat inderdaad met volledige toegang tot de inhoud alle getapte communicatiestromen inlichtingen kunnen worden verkregen, mits de diensten voldoende technische kennis, financiële middelen en technische kennis daarvoor beschikbaar krijgen. De inbreuk op het grondwettelijk beschermde communicatiegeheim wordt daarmee evenwel ook navenant groter. Op p. 71 van de toelichting staat beschreven dat analyse van gegevens m.b.v. DPI kan geschieden. In een viertal rapporten heeft het CBP in 2013 diepgaand de mogelijke inspectietechnieken beschreven en daar zeer restrictieve conclusies aan verbonden voor zover die technieken door aanbieders zouden worden verricht. Duidelijk is dus dat die niet betrokken kunnen worden bij de inhoudelijke analyse en selectie van af te tappen gegevens. Dat betekent dat de diensten alle informatie van de aanbieders zullen moeten doorkrijgen en opvangen en bewerken om de bedoelde analyses uit te voeren. Er zit geen beperkingsmogelijkheid in het feit dat de gegevens niet bij hen berusten (zoals bij de bewaarplicht het geval was). Daarmee gaat de inbreuk op het communicatiegeheim heel veel verder dan bij de onverbindend verklaarde bewaarplicht.

> **Het is noodzakelijk dat het wetsvoorstel – mede door de Raad van State – wordt beoordeeld op de vraag of de toets van het EVRM en het Handvest van de Grondrechten van de EU wordt doorstaan. Anders is het risico groot dat – net als bij de bewaarplicht – grote lasten ontstaan zonder legitieme grondslag. Telecomaanbieders hebben bij die bewaarplicht grote kosten moeten maken om zowel de bewaarplicht mogelijk te maken, uit te voeren als later weer af te breken.**[7]

[7] Zie de op 21 juli 2015 aan de Tweede Kamer aangeboden Factsheet Buitenwerkingstelling Wet bewaarplicht telecommunicatiegegevens, van het Agentschap Telecom.

12. Kosten en investeringen als controlemiddel: de overheid moet vergoeden

In het voorgaande is kritisch ingegaan op de brede medewerkingsplichten die in het voorontwerp aan marktpartijen worden opgelegd. De achtergrond daarvan is niet in het minst de regeling inzake vergoeding van kosten van artikel 13.6 Telecommunicatiewet, die overal waar dat enigszins denkbaar is van overeenkomstige toepassing wordt verklaard (artikelen 31 lid 8, 36 lid 6, 37 lid 7, 38 lid 6, 39 lid 6 en 40 lid 7), om zeker te stellen dat de investeringen voor de voorzieningen die noodzakelijk zijn – voor een groot deel – door het bedrijfsleven worden gedragen. KPN heeft hiertegen twee belangrijke bezwaren:

- De oorspronkelijke grondslag van de kostenverdeling van artikel 13.6 is niet van toepassing op deze uitbreiding;
- De belangrijkste mogelijkheid van parlementaire controle op de proportionaliteit van de activiteiten van de diensten (het 'budgetrecht') wordt de facto verstoord doordat een belangrijk deel van de kosten op deze manier 'uitbesteed' wordt aan de markt.

Ten aanzien van het eerste punt is van belang dat de kostenverdeling – zoals thans neergelegd in artikel 13.6 Tw – destijds is ingevoerd met de Wijziging van de Wet op de telecommunicatievoorzieningen in verband het aftappen van GSM, Stb. 2004, 594. Daarbij werd de volgende motivering gegeven:

> *'De verplichting tot betaling is vooralsnog beperkt tot GSM, omdat voor dit systeem ten eerste momenteel al een inschatting gemaakt kan worden van de kosten voor het aftapbaar maken. Ten tweede gaat het om een in Europees verband gestandaardiseerd telecommunicatiesysteem. Tenslotte lijkt de verwachting gerechtvaardigd dat (als gevolg van de technische karakteristieken; digitaal signaal dat gecodeerd door de ether gaat) er door de georganiseerde misdaad veel gebruik gemaakt zal worden van dit systeem.' (*Nota naar aanleiding van het verslag *(Kamerstukken II* 1994–1995, 24 108, nr. 5 p. 2).

Het is juist dat in de GSM standaard, mede dankzij internationale standaardisatie, de specificaties voor het aftappen van telefoniediensten qua kosten relatief overzichtelijk en voorspelbaar waren. Bij de introductie van die aanpassing van het voorheen geldende systeem – waarin de overheid de voorzieningen bekostigde – speelde dat een belangrijke rol. Met de introductie van de telecommunicatiewet werd die regel per 15 december 1998 verbreed naar alle toen bestaande telecommunicatiediensten. Volgend de toelichting was de reden daarvan:

> *'Bijkomend voordeel is dat zodoende een prikkel wordt ingebouwd om op de meest voordelige wijze de aftapbaarheid te realiseren, zodat een kostprijsverhogend effect van de te treffen voorzieningen beperkt kan blijven. Het verdisconteren van de gemaakte kosten in de bedrijfsvoering is verder een ondernemersverantwoordelijkheid. Bij de wet van 23 november 1995 tot wijziging van de Wet op de telecommunicatievoorzieningen in verband met het aftappen van GSM is de WTV in die zin gewijzigd dat de investeringskosten alsmede de jaarlijkse onderhouds- en exploitatiekosten, die verband houden met het aftappen, ten laste komen van de GSM-vergunninghouders. Bij de behandeling van dat wetsvoorstel heeft ondergetekende aangekondigd dat de voor GSM ingezette lijn op dit punt zal worden doorgetrokken naar alle openbare telecommunicatienetwerken en -diensten in Nederland. In het eerste lid van het onderhavige artikel wordt deze verplichting vormgegeven en wordt tevens geregeld dat ook de technische inspanningen die gedaan moeten worden ten behoeve van het verstrekken van informatie en ten behoeve van de beveiliging voor rekening van de hier bedoelde aanbieders hieronder vallen. Het beleid met betrekking tot de financiering van het aftappen van GSM wordt hiermee*

ook op andere telecommunicatiesystemen in Nederland van toepassing verklaard.' (Kamerstukken II 1996–1997, 25 533, nr. 3, p. 126).

De strekking van de regeling is daarmee mede geënt op het bereiken van de meest efficiënte manier van implementatie. In de standaarddienstverlening zoals die in die tijd (voornamelijk voor telefonie) bestond is het misschien logisch de prikkel daartoe op die manier bij aanbieders te leggen. Maar bij de steeds verder uitbreidende verplichtingen rondom het aftappen van internet en datadiensten blijkt steeds meer dat (i) er geen internationale standaardisatie voorhanden is, (ii) de mogelijkheid voor aanbieders om tevoren exact te weten op welke manier ze 'aftapbaar moeten zijn steeds moeilijker voorspelbaar is en (iii) er daarmee steeds meer 'maatwerk' nodig is. Zoals al eerder geconstateerd gaat het voorontwerp daarop door en legt het medewerkingsplichten op die geheel ongespecificeerd zijn. Daarmee is de grondslag voor het efficiënt en via gestandaardiseerde oplossingen kunnen implementeren van tapvoorzieningen af aanwezig. Het is dan ook niet gepast om het stelsel van artikel 13.6 zonder nadere motivering op die nieuwe verplichtingen van toepassing te verklaren.

Met de nieuwe situatie dat 'maatwerk' uitgangspunt is wordt het van steeds groter belang dat de proportionaliteit van de benodigde investeringen wordt afgewogen. Met de uitbesteding van die investeringen aan aanbieders is er voor de diensten geen enkele prikkel om de bedrijfseconomisch meest efficiënte oplossing op te dragen, ook zonder dat er een afweging tegenover de potentiële opbrengsten in inlichtingenperspectief tegenover staat. De controle op de proportionaliteit is daarmee uit het systeem van toezicht op de diensten goeddeels verdwenen. Aanbieders mogen op grond van de hen opgelegde geheimhouding niet aangegeven welke plichten en lasten hen worden opgelegd en het parlement ontbeert de normale mogelijkheden om via de goedkeuring van begrotingen toezicht te houden op de maatschappelijke lasten van overheidsoptreden.

> **Het is dringend noodzakelijk dat in het wetsvoorstel wordt afgestapt van het systeem van artikel 13.6 Telecommunicatiewet, waarin alle investeringen in en kosten van voorzieningen van ongerichte interceptie voor rekening van marktpartijen worden gebracht. Alleen door die kosten voor rekening van de algemene middelen – en dus de begroting van de diensten – te laten lopen kan enig toezicht op de proportionaliteit en inzet van deze uiterst ver strekkende bevoegdheden in het systeem worden geïncorporeerd.**

Het is daartoe nodig dat in de artikelen 36 en 37 verplichtingen voor aanbieders worden opgenomen om binnen een redelijke termijn na een verzoek daartoe offertes uit te brengen aan die diensten, waarop deze kunnen besluiten door acceptatie van die offertes de voorzieningen te laten aanbrengen.

13. Netwerkbeveiliging versus medewerkingsplichten

Het uitgangspunt van het voorontwerp is de (mede in par. 8 hierboven al besproken) medewerkingsplicht tot ontsleuteling en/of de methode te delen van versleuteling. Deze medewerkingsplicht is voor aanbieders van communicatiediensten niet goed na te leven en zeker niet zonder hun overige verplichtingen ten aanzien van de beveiliging van netwerken, diensten en persoonsgegevens, die zij hebben 'naar de stand van de techniek'. De medewerkingsplichten maken de mogelijkheden om hieraan te voldoen onmogelijk of onredelijk complex. Daarmee wordt het primaire doel van telecommunicatiediensten ten behoeve van de economische voortuitgang en de ontwikkeling naar een te vertrouwen '*e-economy*' ge-

weld aangedaan. Het wetsvoorstel lijkt de 'veiligheidsfunctie' van communicatienetwerken te zeer boven de primaire functie ervan te stellen.

Dit geldt ook voor de taak die wordt aangegeven voor de diensten tot het beschermen tegen digitale aanvallen. Zoals in par. 1 al aangegeven kan hierin worden gelezen dat de diensten bij aanvallen daadwerkelijk zouden mogen ingrijpen in netwerkverkeer. Technische toegang tot kabelgebonden telecommunicatie zou echter op zo'n manier moeten gebeuren zodat de diensten geen mogelijkheid hebben op welke manier dan ook om het verkeer te kunnen manipuleren of daarop zelf in te grijpen. De verantwoordelijkheid van de telecom aanbieders mag niet beïnvloed worden, om te voorkomen dat buiten hun invloed om zij niet meer de kwaliteit en continuïteit van hun dienstverlening zelf kunnen garanderen.

Hiervoor gelden mede technische redenen die zich als volgt laten samenvatten.

(a) Voor transportsleutels is de informatie onmogelijk op te leveren:

- Transportsleutels zijn per definitie sessie-gebonden en in veel gevallen vluchtige informatie die enkel tijdelijk in het geheugen leven van de end-to-end oplossing. Daarna zijn ze weg. Dit is de moderne internationale standaard hiervoor (Elliptic Curve) Diffie-Hellman Key Exchange met Emphimeral (=vluchtige) sleutels.
- Oudere transport versleuteltechnieken (RSA key exchange) kunnen met een capture van de data worden teruggerekend te samen met de private key van het certificaat.
    - Dit veronderstelt dat er een volledige unsampled capture bestaat van een sessie en dat de private key opgeleverd kan worden. Deze captures kunnen alleen op selectieve momenten gemaakt worden om het netwerk te debuggen. Er is geen enkele voorziening getroffen om hier meer mee te doen.
    - Dit vereist dat er selectieve specifieke nieuwe oplossingen gemaakt worden, omdat er geen enkele noodzaak is voor de aanbieder van communicatiediensten om hierin te moeten voorzien. Dit zou betekenen dat alle netwerkverkeer opgeslagen moet worden. De kosten hiervoor zijn buiten proportioneel hoog en in strijd met de wettelijke regels voor de verwerking van persoonsgegevens.
- Private keys delen, in welke vorm van door, is volgens de internationale standaarden per definitie gelijk aan een 'key-compromise'.
    - Appliances met en zonder Hardware Security Module (HSM) oplossingen bieden geen private key exportfunctie, maar alleen importfuncties. Dit is een veel voorkomende bescherming. Bij een HSM oplossing is een private key zelfs 'tamper-proof' opgeslagen en zijn er buiten dit systeem enkel mogelijkheden om de key's te vervangen, niet te exporteren.
    - Operationeel gericht beleid eist dat een beheerder in een appliance, HSM en op het uiteindelijke doelsysteem de sleutels aanmaakt en nergens anders. Transport van een private key wordt hiermee uitgesloten om de privacy, security en soevereiniteit van de aanbieder te kunnen handhaven.

(b) Storage gerelateerde keys:

- Er zijn sleutels voor systemen en gebruikers die betrekking hebben op disk-volumes, databases, tabellen in databases, rijen en data-velden.
    - De keys zijn van verschillende typen, omvang, techniek, en hebben betrekking op uiteenlopende toepassingen.
    - Er is geen peil op te trekken hoe alle verschillende oplossingen op verschillende deelgebieden en verschillende implementaties met sleutels werken en in welke

vorm. Aanbieders pentesten per oplossing of dit goed gebeurt en letten op de certificeringen wanneer het interne systemen/back-end systemen zijn. Dit zijn de waarborgen die aangeven hoe de status van de beveiliging is. De oplevering van een key is in al deze kwesties geen onderdeel van de vraagstelling geweest, behalve dan hoe te voorkomen dat anderen bij de sleutels zouden kunnen. Dit is in het belang van de soevereiniteit van de aanbieder.

(c) Algemene toevoegingen ten aanzien van geheime sleutels, zoals private keys of andere geheime sleutels:

- Het delen van een private key zou de privacy en security zorgplicht van aanbieders schenden. Het delen van een private key staat gelijk het delen van de identiteit van de aanbieder met de partij die de key heeft. De partij die de private key krijgt kan zich voordoen als de aanbieder. Dit is een aanvalsscenario van hackers en cyber-criminelen om ongezien *man-in-the-middle* attacks uit te voeren. Zoals in de volgende par. nader uitgewerkt acht KPN het uiterst onwenselijk dat de diensten deze rol zou kunnen vervullen zonder transparantie naar de aanbieders toe.
- Als *collateral damage* zou het mogelijk moeten maken van het delen van de private key betekenen dat alle beheerders moeten worden geïnstrueerd om met cryptografisch materiaal te moeten omgaan. Dit is specialistisch werk en het cryptografisch materiaal moet met diverse waarborgen worden getransporteerd. Iedere beheerder binnen een aanbieder zal een key ceremonie cursus moeten krijgen om dit te kunnen uitvoeren.
    - Het mogelijk maken van de oplevering van cryptografisch materiaal, zelfs tussen afdelingen binnen een aanbieder, zorgt ervoor dat de security en privacy zorgplicht wordt ondermijnd.

(d) Algemene toevoeging voor 'one-way' encryptie technieken:

Volgens *industry-best practices* zijn er vele one-way encryptie technieken om bijvoorbeeld wachtwoorden op te slaan. Deze zijn nooit meer terug te halen, omdat er alleen een hash/digest wordt gemaakt van een wachtwoord en deze wordt dan vaak nog een aantal malen complexer opgeslagen om decryptie door aanvallers die de gehele database of harddisk zouden stelen te kunnen voorkomen.

- Deze techniek wordt ook gebruikt om data te anonimiseren.
- Deze techniek wordt ook gebruikt om cryptografische bewijslasten te vormen wanneer er challenge-response technieken of digitale handtekeningen moeten worden gezet.
- Het gebruik van deze techniek is fundamenteel voor onze digitale samenleving.
- In lekentermen betekent dat simpelweg: 'wij (de aanbieder) weten meestal ook niet wat het wachtwoord is en wat er als data staat opgeslagen'. Dit is volledig aan de verantwoordelijkheid van de eindgebruikers overgelaten.

De conclusie hieruit is dat de primaire functie van adequaat beveiligde communicatiediensten in alle gevallen zonder inbreuk in stand moet blijven. Daarbij past het niet om aan aanbieders van die diensten verplichtingen op te leggen die daaraan afbreuk zouden kunnen doen. Als het gaat om doorbreken van beveiligde communicatie dient dat veelal niet gezocht te worden bij de aanbieders van de communicatiediensten, maar bij aan de zijde

van de gebruikers zelf, omdat die veelal aan zet zijn, zowel wanneer data versleuteld is als voor het ontsleutelen hun wachtwoorden.

> **De bevoegdheden van de diensten dienen dan ook primair gericht te worden op de doorbreking van de beveiliging op het niveau van te onderzoeken eindgebruikers en niet op die van de diensten waarvan ook talloze 'niet targets' beveiligd gebruik maken. Alleen in zoverre in het kader van het bevoegd gerichte aftappen ontsleutelde communicatie kan worden geleverd zouden aanbieders daartoe gehouden moeten zijn, maar dat is in het huidige wettelijke kader al geregeld.**

14. Binnendringen in geautomatiseerde werken

Artikel 30 lid 1 onderdeel a geeft een verregaande bevoegdheid aan de diensten om technische kenmerken van geautomatiseerde werken te verkennen. De bevoegdheid is beperkt tot geautomatiseerde werken 'die op een communicatienetwerk zijn aangesloten'. Hoewel het begrip communicatienetwerk niet is gedefinieerd, zou uit de context moeten worden aangenomen dat het gaat om elektronische communicatienetwerken waarover de (alleen voor paragraaf 3.2.2.7 van de wet) gedefinieerde 'aanbieder van een communicatiedienst' zijn elektronische diensten aanbiedt. Daarmee is er in de lezing van KPN – geheel terecht – geen bevoegdheid om verkenningen van telecommunicatienetwerken uit te voeren.

Een vergelijkbare beperking ontbreekt echter in onderdeel b van dat lid, waardoor het lijkt dat de diensten wel met technische ingrepen, valse signalen en valse hoedanigheden in de geautomatiseerde werken die een telecomnetwerk ook zijn (volgens de definitie van artikel 31) kunnen binnendringen. Dit is een uiterst onwenselijke regeling. Het gehele nationale en Europese beleid is erop gericht om digitale infrastructuren – die het hart van de toekomstige *e-economie* zijn – te beveiligen en te beschermen tegen ingrijpen van buiten. In dat kader worden steeds verdergaande continuïteits- en beveiligingsverplichtingen aan aanbieders opgelegd. Daarbij past nooit een tegenovergestelde bevoegdheid van de diensten om op eigen initiatief binnen te dringen in die netwerken. Een digitale bewapeningswetloop tussen de beveiliging van de netwerken en de hackbevoegdheden van de diensten zou daarvan slechts het maatschappelijk uiterst onwenselijke gevolg zijn.

Op p. 51 van de toelichting staat aangegeven dat het voor de diensten soms '*niet mogelijk is het bij een onderzoekssubject in gebruik zijnde geautomatiseerde werk direct binnen te dringen, maar dat deze mogelijkheid wel kan worden gecreëerd door gebruikmaking van een onderkende zwakheid in een ander geautomatiseerd werk'*. Voor zover daarmee ook gedoeld zou worden op het communicatienetwerk via welke de diensten proberen een aangesloten geautomatiseerd werk binnen te dringen zou daarvan de perverse prikkel voor de diensten uitgaan om een door hen herkende zwakte in de beveiliging van netwerken stil te houden in plaats van de aanbieder in staat te stellen die te verbeteren.

Vervolgens wordt aangegeven dat '*het vanuit operationeel belang wenselijk technische voorzieningen in een geautomatiseerd werk aan te kunnen brengen ter ondersteuning van de uitvoering van andere bijzondere bevoegdheden' (eveneens p. 51).* Het moet binnen het systeem van de wet uitgesloten worden geacht dan de diensten buiten aanbieders om enige voorziening in beveiligde telecomnetwerken zouden mogen aanbrengen. Anders zou het mogelijk zijn dat die netwerkingen aanpassingen ondergaan die hen buiten hun wil en buiten hun macht in overtreding brengen ten aanzien van verschillende zorgplichten (privacy, cybersecurity). Ook zou het onderzoeksubject de betrokken aanbieders van communicatiediensten mogelijk aanspreken op de niet naleving van die normen als gevolg van door

veiligheidsdiensten verrichte technische voorzieningen. Een ander niet uit te sluiten risico is dat andere partijen de 'voorzieningen' kwaadwillig gaan misbruiken die de diensten hebben aangelegd. Zelfs als de aanbieder op de hoogte is van de voorzieningen verzet de geheimhoudingsplicht van de aanbieder om zich hiertegen effectief te verdedigen.

Voor zover het gaat om het weerstand bieden aan cyber aanvallen is coördinatie tussen de diensten en de netwerkaanbieders een betere manier.

> **Het is noodzakelijk om de bevoegdheid van artikel 30 tot het verkennen van en binnendringen in geautomatiseerde werken in lid 1, zowel voor de bevoegdheid onder a, als de bevoegdheid onder b, te beperken tot geautomatiseerde werken die zijn aangesloten op communicatienetwerken en die netwerken zelf daarvan expliciet uit te sluiten.**

15. Coördinatie aan de zijde behoeftestellers

In de praktijk is een toenemende operationele samenwerking op het terrein van het elektronische inlichtingenwerk – waaronder aftappen en gegevensverstrekking – tussen de diensten waar te nemen. Het voorontwerp laat echter in het midden in hoeverre de diensten als één entiteit optreden in de richting van marktpartijen, of nog met eigen aanvullende of afwijkende invulling van hun bevoegdheden kunnen komen. Dat is onwenselijk.

In de snel toenemende complexiteit van het aftappen van datacommunicatie en internet gerelateerde dienstverlening is het voor een goed functioneren van de telecommunicatiemarkt noodzakelijk dat alle behoeftestellers – inclusief openbaar ministerie/politie in het kader van strafvordering – op uniforme wijze medewerking van aanbieders verlangen. Het zou wenselijk zijn de coördinatie daarvan aan overheidszijde ook wettelijk te waarborgen. Bij voorkeur zouden aanbieders contact hebben met één entiteit, zodat ook de afstand tussen hun activiteiten en de concrete doelen van aftappen en gegevensverstrekking voor hen nog verder onduidelijk zijn en geheimhouding ten aanzien van specifieke situaties nog beter is te realiseren. Het is ongewenst dat aanbieders de complexiteit van twee diensten te accommoderen.

> **Van de gelegenheid moet gebruik worden gemaakt om in het wetsvoorstel een sterkere coördinatie binnen de overheid te realiseren, zodat het steeds grotere aantal betrokken ondernemingen op eenduidige manier invulling kan geven aan wettelijke medewerkingsplichten.**

16. Samenwerking toezichthouders

Artikel 49 van het voorontwerp regelt de bevoegdheid voor de diensten om van verwerkte gegevens mededeling te doen aan een relatief brede kring van andere instanties, waaronder 'bestuursorganen'. De wet maakt niet duidelijk of daaronder ook zelfstandige bestuursorganen worden verstaan, maar dat wordt niet uitgesloten. Dat zou meebrengen dat informatie die de diensten verkrijgen door toepassing van 'bijzondere bevoegdheden' die diep ingrijpen in de grondrechten van burgers gedeeld mogen worden met toezichthouders die zelf niet op legitieme manier aan die informatie hadden kunnen komen. Hoezeer het wenselijk is spam te bestrijden, of bepaalde financiële transacties tegen te gaan, of bepaalde zorg te verlenen, het moet toch niet mogelijk worden geacht dat de diensten informatie die zij – hetzij uit doelgericht onderzoek, hetzij als bijproduct – vergaren in het kader van inlichtingen taken verstekken aan ACM ten behoeve van spambestrijding, AFM ten behoeve

van financieel toezicht of de NZA ten behoeve van toezicht op de zorgsector. Dit klemt temeer nu bevoegdheden als (gericht of ongericht) aftappen zich volgens het voorontwerp ook richten op besloten communicatienetwerken.

Het verdient aanbeveling de mogelijkheid om door de dienst verwerkte gegevens te delen met andere bestuursorganen of andere personen of instanties te beperken tot informatie die dergelijke instanties ook op grond van hun eigen bevoegdheden hadden kunnen verkrijgen. De rechtvaardiging van de bijzondere en diep ingrijpende bevoegdheden van de diensten zou anders geweld worden aangedaan.

17. Uitbesteding van overheidstaken en de vertrouwelijkheid

In het voorgaande is de verregaande medewerkingsplicht als ietwat schertsend aangeduid als 'uitbesteding van overheidstaken'. Hoewel daar in formele zin geen sprake van is, leidt het wettelijk stelsel er wel toe dat private ondernemingen en hun personeel en ingeschakelde derden steeds meer betrokken worden bij het werk van de inlichtingendiensten. De traditioneel – in het Wetboek van Strafrecht gesanctioneerde – geheimhoudingsplichten zijn daarmee steeds moeilijker te garanderen. In de snel ontwikkelende technologische markten van de elektronische communicatie en internet is er een steeds kleiner aantal bedrijven dat zelf in staat is de eigen bedrijfsprocessen geheel binnenshuis te realiseren. Leveranciers van (gestandaardiseerde) telecommunicatie-apparatuur is er in Nederland niet meer en netwerkaanbieders zijn aangewezen op de wereldmarkt (veelal VS, Azië). Aanpassingen in netwerken en bedrijfssystemen kunnen dan ook niet binnen de organisaties van de aanbieders blijven, maar moeten om geïmplementeerd te worden gedeeld worden met een – potentieel groot aantal – toeleveranciers. De meeste daarvan vallen niet direct onder Nederlands toezicht. De praktijk van veiligheidsdiensten heeft in het 'post-Snowdon-tijdperk' al veel illustratie opgeleverd dat ook wettelijke geheimhoudingsplichten niet daadwerkelijk het door en in opdracht gedane werk van veiligheidsdiensten geheim kunnen houden. Van aanbieders kan niet meer worden verlangd dan dat zij contractueel geheimhouding opleggen ten behoeve van het werk voor de diensten, maar een verdergaande vorm van garantie – zoals in het verleden werd verondersteld – is niet meer mogelijk.

Het is belangrijk dat het wetsvoorstel zich er rekenschap van geeft dat de in artikel 124 herhaalde geheimhoudingsplicht steeds vaker niet geëffectueerd zal kunnen worden, mede omdat in de internationale context van telecom- en internetdienstverlening een groot deel van betrokken natuurlijke personen niet onder de Nederlandse rechtsorde valt.

18. Overige opmerkingen

In de toelichting op p. 23 wordt ten aanzien van artikel 19 lid 3 opgemerkt dat de Minister van BZK onderscheidenlijk de Minister van Defensie wordt aangewezen als zorgdrager voor de bij de artikel 79 onderscheidenlijk 80 berustende archiefbescheiden, voor zover die nog niet naar een rijksarchiefbewaarplaats zijn overgedragen. Dat zou nader uitgewerkt moeten worden voor wat betreft de vertrouwelijkheid, integriteit en beschikbaarheid.