NEDERLAND ICT

Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties
De heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA DEN HAAG

Woerden, 31 augustus 2015

Betreft : Reactie Nederland ICT op consultatie wetsvoorstel Wiv
Kenmerk : 40289/LdB/AdJ/JB

Geachte heer Plasterk,

Nederland ICT is de brancheverenigingvan ruim 550 ICT-bedrijven in Nederland. Met een achterban die bijna € 30 miljard omzet en meer dan 250.000 medewerkers telt, is Nederland ICT de belangenbehartiger en vertegenwoordiger van de Nederlandse ICT-sector.

De inzet van ICT draagt bij aan 60 procent van de economische groei in Nederland. 70 procent van alle innovaties is ICT-gerelateerd. Nederland is een aantrekkelijk vestigingsland vanwege haar hoge ICT dichtheid en sterke digitale infrastructuur. Netwerkeffecten zorgen ervoor dat wereldwijd een relatief klein aantal landen een disproportioneel aandeel in de digitale infrastructuur heeft. Nederland heeft daardoor naast de mainports Schiphol en Rotterdam ook twee internet mainports: 's werelds nummer twee internet exchange en 's werelds nummer negen[1]. Nederland profileert zich als vestigingsland mede daardoor terecht als Europese koploper en Digital Gateway to Europe[2]. Het sterke en open Nederlandse digitale ecosysteem heeft een aanzuigende werking op innovatieve bedrijven en zorgt daarmee voor een uitstekende uitgangspositie voor Nederland in de transitie naar vergaande digitalisering van de wereldeconomie.

Deze economische groei wordt mede mogelijk gemaakt door flankerend beleid van de overheid. De overheid richt zich op het stellen van randvoorwaarden en ordenen van deze markt opdat digitale innovatie en groei over de volle breedte van de Nederlandse economie kan plaatsvinden. Belangrijke randvoorwaarden voor de overheid zijn[3]:

- Voldoende concurrentie in de markt zodat een dynamiek van continue investeringen en innovaties blijft bestaan;
- Vrijheid, waaronder hier wordt verstaan keuzevrijheid voor gebruikers, vrij van oneigenlijke invloed van overheden, bedrijven en overige belangengroepen;
- Betrouwbaarheid van netwerken en diensten, in het bijzonder integriteit (juistheid van informatie, geen veiligheidsinbreuken), continuïteit (geen storingen of uitval) en bescherming van persoonsgegevens.

[1] https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size
[2] http://investinholland.com/infrastructure/broadband/
[3] Voortgangsrapportage uitwerking visie op Telecom, internet en media. Kamerstuk, 26643 nr. 345

Borging van deze randvoorwaarden zorgen voor een aantrekkelijk ondernemingsklimaat en vertrouwen onder burgers en bedrijven. Hierdoor kunnen we blijvend profiteren van de toegevoegde waarde van ICT en blijft Nederland een aantrekkelijke vestigingsplaats. Om onze koploperspositie te behouden is het van belang als overheid terughoudend te zijn met het doen van voorstellen die nadelig zijn voor het vertrouwen van burgers en bedrijven, het ondernemingsklimaat en daarmee voor de positie van Nederland als ICT vestigingsland.

Het voorstel van de herziening van de Wet op de inlichtingen- en veiligheidsdiensten is naar de mening van Nederland ICT zo'n voorstel. Het voorstel gaat voorbij aan het beoogde doel van 'technologie onafhankelijk maken van de interceptie', tast de betrouwbaarheid van netwerken en diensten aan, en beperkt de hierboven genoemde vrijheid.

Reactie Nederland ICT op Wiv

Nederland ICT maakt zich ernstige zorgen over de gevolgen van het voorstel voor de nieuwe Wet op de Inlichtingen en Veiligheidsdiensten (Wiv). De nieuwe wet geeft de inlichtingen- en veiligheidsdiensten de bevoegdheid tot massale interceptie van kabelgebonden communicatie.

Nederland ICT heeft grote twijfels over het nut en noodzaak, de transparantie en proportionaliteit, de reikwijdte en toerekening van kosten, de praktische uitvoerbaarheid en het juridisch toetsingskader van de nieuwe bevoegdheden en daarmee het draagvlak voor een dergelijk ingrijpend wetsvoorstel.

De door de wet opgelegde eisen aan een groot aantal bedrijven zullen resulteren in een verlies aan vertrouwen van burgers en bedrijven, in toegenomen onzekerheid en financiële druk voor het bedrijfsleven, minder innovatie, risico's voor de betrouwbaarheid en integriteit van dienstverlening en verslechtering van het internationale imago van Nederlandse als Digital Gateway to Europe.

Belangrijkste bezwaren

De reikwijdte van de nieuwe bevoegdheden is erg groot: in essentie valt elke aanbieder van een dienst die over het internet gegevens uitwisselt, wat voor gegevens dan ook, binnen het kader van de wet.

Het voorgestelde systeem voldoet volgens Nederland ICT niet aan minimale maatschappelijke en rechtsstatelijke verantwoording en toetsing die nodig is om zo'n ingrijpend middel, rechtmatig, te kunnen invoeren. Ook de benodigde transparantie om nut en noodzaak van de programma's van de diensten te kunnen beoordelen ontbreekt voor het huidige voorstel.

Het voorstel geeft geen technische details over de manier waarop de integriteit, beschikbaarheid en vertrouwelijkheid van de getapte data gewaarborgd wordt. Aanbieders krijgen geen compensatie voor schade of verstoring dienstverlening aan gebruikers naar aanleiding van handelen van inlichtingen- en veiligheidsdiensten. Bovendien is, door de geheimhoudingsplicht, de toegankelijkheid van toetsing door een rechter bij een mogelijk bezwaar voor aanbieders in het geding.

Het voorstel is verder onduidelijk over de vraag of het ontsleutelbevel (aanbieders worden geacht mee te werken aan ontsleuteling van versleutelde informatie) het inbouwen van backdoors mogelijk

maakt. Gezien de weerstand die in de nasleep van de onthullingen van Snowden wereldwijd heerst tegen dit soort bevoegdheden zou dit funest zijn voor het vertrouwen van burgers en bedrijven in de integriteit van hun data en daarmee het internet, en zodoende voor de positie van Nederland als aantrekkelijke ICT-vestigingsplaats. De economische schade door het verlies aan vertrouwen in digitale diensten was in de VS groot. Het is zeer onwaarschijnlijk dat dit in Nederland anders zal zijn.

De huidige infrastructuur is niet toegerust op massale interceptie van gegevens. Om te voldoen aan de last voor bulk interceptie zal een kostbare nieuwe interceptie-infrastructuur ontworpen, ontwikkeld, gebouwd en getest moeten worden specifiek voor elk bedrijf.

Het voorstel legt alle kosten bij private partijen, waarbij het in veel gevallen onduidelijk blijft wanneer en hoe bedrijven investeringen moeten doen om de last tot aftappen te faciliteren. Dit heeft een grote remmende werking op de innovatiekracht en de groeipotentie van met name kleine dienstverleners en startups. Uit het wetsvoorstel blijkt dat er zodoende binnen de diensten geen noodzaak is tot het doen van een effectieve proportionaliteitstoets. Een tap dagen langer laten lopen, of het aansluiten van verschillende taps in de hoop op een hit kost de AIVD of de MIVD niets. Het gevaar van '*overreach*' is dan ook prominent aanwezig.

Concluderend
Nederland ICT vraagt de minister het voorstel in de huidige bewoordingen te heroverwegen en samen met de sector na te denken over een wetsvoorstel dat op meer draagvlak bij burgers en bedrijven kan rekenen.

Nederland ICT pleit er voor om bij het opleggen van dergelijke verplichtingen voor het bedrijfsleven altijd de kosten via de Rijksbegroting te laten lopen. Niet alleen is er zodoende democratisch toezicht op de kosten, ook worden de diensten er door financiële overwegingen toe gedwongen hun activiteiten scherp en doelgericht in te zetten. De proportionaliteit is hierdoor beter geborgd.

Meer specifiek vraagt Nederland ICT de minister, in overleg met zijn collega's van Veiligheid en Justitie en Economische Zaken, om:

- Een gedegen onderbouwing van nut en noodzaak van een dergelijk ingrijpend wetsvoorstel.
- Een voorstel hoe in de toekomst op een transparante wijze inzicht gegeven wordt in de reikwijdte van de bevoegdheden van inlichtingen- en veiligheidsdiensten en de wijze waarop deze hun taak uitoefenen. Dit teneinde het vertrouwen van burgers en bedrijven in de integriteit van hun data, het internet en daarmee de digitale economie als geheel te waarborgen.
- Een analyse van het effect dat het wetsvoorstel zal hebben op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

Nederland ICT bedankt u voor de mogelijkheid om te reageren op het voorontwerp voor het wetsvoorstel Wiv. Als u naar aanleiding van deze opmerkingen vragen heeft, ben ik natuurlijk graag bereid een nadere toelichting te geven.

In de bijgesloten bijlage treft u een nadere reactie aan op specifieke onderdelen van het voorstel.

Met vriendelijke groet,
Nederland ICT

Lotte de Bruijn,
directeur.

bijlage: 1

BIJLAGE 1.

Nederland ICT vindt het huidige voorstel juridisch problematisch en vaak niet duidelijk. In onderstaande tekst staan de punten die voor Nederland ICT primair onduidelijk zijn. Zonder nadere toelichting is het voor Nederland ICT niet mogelijk het voorstel en de implicaties er van volledig te kunnen inschatten en afdoende te wegen. We vragen de minister daarom bij elk van deze punten een nadere toelichting:

1. Kabelgebonden telecommunicatie:
Ongerichte interceptie was ingevolge artikel 27 Wiv 2002 alleen mogelijk bij niet-kabelgebonden telecommunicatie. In het onderliggende voorstel komt het onderscheid tussen kabel- en niet-kabelgebonden telecommunicatie te vervallen. Met de motivering '*[dat] de basis van het onderscheid tussen de ether en de kabel niet meer te rijmen valt met de voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie*' gaat men voorbij aan de reden waarom de Wiv 2002 alleen niet-kabelgebonden telecommunicatie toestaat.

Ingevolge artikel 10 EVRM bestaat er een 'ontvangstvrijheid' die door de AIVD en de MIVD wordt gebruikt om via het adagium '*de ether is vrij*', Inmarsat- dan wel andere satellietcommunicatie op te vangen en te verwerken. Dit kan door in de naaste omgeving van bijvoorbeeld een Inmarsat basisstation een schotel van de AIVD en/of MIVD te zetten. Alle gegevens komen zo, zonder medewerking of medeweten van de satellietprovider beschikbaar.

Voor het aftappen van kabelgebonden communicatie is een ingreep in de fysieke infrastructuur nodig. Hulp van de netwerkbeheerder is daarbij noodzakelijk, omdat de gegevens niet simpel voor een ieder zijn op te vangen. Het voorstel breidt het adagium '*de ether is vrij*' zonder onderbouwde nut en noodzaak analyse, en zonder een doeltreffend toetsingskader, uit tot '*alle communicatie is vrij*'.

Nederland ICT verzoekt de minister nut en noodzaak nader toe te lichten.

2. Reikwijdte:
Het voorgestelde artikel 31 onder a. geeft een eerste inzicht tot de groep van bedrijven die door deze wet aangesproken kunnen worden: **een aanbieder van een communicatiedienst** wordt gedefinieerd als elke (rechts-)persoon die aan de gebruik van zijn dienst '*de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens opslaat ten behoeve van een zodanige dienst, of de gebruikers van die dienst*.' Het begrip 'communicatiedienst' plaatst niet alleen de huidige openbare elektronische communicatiediensten en –netwerken zoals gedefinieerd in de Telecomwet onder de reikwijdte van het voorstel, maar breidt deze uit tot besloten netwerken en –diensten (oa. Surfnet en interne bedrijfsnetwerken), maar verder vallen ook aanbieders van webhostingdiensten, beheerders van websites en aanbieders van online opslag, email of spraakdiensten onder deze nieuwe definitie. Maar zelfs 'zelfrijdende voertuigen' en ' connected cars' kunnen door het voorstel binnen deze definitie vallen en in dat geval 'in bulk' gevolgd worden. Deze nieuwe toepassingen maken namelijk inherent gebruik van communicatienetwerken en bieden ook communicatiefuncties voor mensen onderling. Niet alleen communicatie tussen mensen en tussen mensen en on-line diensten worden nu bulk aftapbaar, maar ook alles wat in de wereld van '*Internet of Things*' gaat komen. In essentie valt **elke** aanbieder van een dienst die over het internet

gegevens, wat voor gegevens dan ook, uitwisselt onder de reikwijdte van het voorstel. Gegevens thuis, in de auto, in het ziekenhuis, echt alles wat een verbinding met het internet heeft, of is aangesloten op een eigen netwerk.

Het voorgestelde artikel 32 eerste lid geeft een tweede aanduiding van de omvang van de reikwijdte van dit voorstel. De te onderscheppen gegevens zijn '*elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk*'. Alle output van geautomatiseerde werken is blijkbaar potentieel interessant voor de diensten en kan op deze manier ontsloten worden.

Het voorgestelde artikel 33 ten slotte komt in de plaats van de vroegere artikelen 25, 26 en 27, Wiv 2002, waarbij verkennen door middel van ongerichte interceptie van de niet-kabelgebonden telecommunicatie geoorloofd was, mits deze communicatie zijn oorsprong of bestemming in andere landen had. In het onderliggende voorstel is deze laatste beperking, voor AIVD en/of de MIVD, zonder verdere motivatie komen te vervallen.

Nederland ICT verzoekt de minister bovengenoemde keuzes nader te motiveren.

3. Bulk interceptie (digitaal sleepnet):
Het voorgestelde artikel 33 lid 1 van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) legt verplichtingen op over 'bulk interceptie'. Men spreekt van "*elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk*". Het gaat hier om niet gerichte interceptie.

Artikel 4 van het Besluit aftappen openbare telecommunicatienetwerken en –diensten stelt "*Bij ministeriële regeling kunnen nadere regels inzake technische aftapbaarheid worden gesteld met betrekking tot de bij die regeling aan te wijzen openbare telecommunicatienetwerken en openbare telecommunicatiediensten*."

In de Regeling aftappen openbare telecommunicatienetwerken en –diensten, wordt in art. 8 de aftapbaarheid van internettoegang dan wel diensten beperkt tot :
1°. de accountnaam van de gebruiker dan wel een ander identificerend nummer, dat door de aanbieder ten behoeve van de dienstverlening aan de gebruiker wordt gehanteerd, of
2°. het adres voor elektronische post dat door de aanbieder ten behoeve van de dienstverlening aan de gebruiker wordt gehanteerd.

In het onderliggende voorstel zal, volgens de Memorie van Toelichting, bij een last tot bulk intercept '*nader aangegeven dienen te worden welk deel van de kabelinfrastructuur het betreft en wat voor soort verkeer [er] dient te worden geïntercepteerd*'. De huidige interceptie infrastructuur ziet niet op 'bulk interceptie'. Het is derhalve niet mogelijk om de huidige infrastructuur een-op-een te gebruiken voor deze bulk-interceptie. Om te voldoen aan een last voor bulk interceptie zal een kostbare nieuwe unieke interceptie infrastructuur ontworpen, ontwikkeld, gebouwd en getest moeten worden voor elk specifiek bedrijf. Waarbij er grote kans is dat kosten en werkzaamheden gedupliceerd worden aangezien er een geheimhouding rust op het ontvangen van een last.

Nederland ICT verzoekt de minister meer informatie te geven over de wijze waarop de last tot bulk interceptie technisch dient te worden uitgevoerd door *alle* communicatiedienstaanbieders en welke

kosten hier naar verwachting mee zijn gemoeid. Ook vraagt Nederland ICT de minister deze kosten te vergelijken met soortgelijke nalevingskosten voor bedrijven in andere EU-landen.

4. Deep Packet Inspectie:
Artikel 33 eerste lid geeft tevens de mogelijkheid om netwerkmonitoring of netwerkdetectie activiteiten te ontplooien door middel van *Deep Packet Inspection (DPI)- apparatuur*[4]. Onduidelijk is hoe de netwerkdetectie zich verhoudt tot het Nationaal Detectie Netwerk van de NCSC waar de AIVD en de MIVD ook bij zijn aangesloten. Tevens is onduidelijk of de detectie voor defensieve en/of offensieve doeleinden wordt gebruikt.

Het voorstel maakt tevens niet duidelijk of netwerkmonitoring en –detectie een activiteit is die de diensten als aangeboden dienst van de aanbieder kunnen eisen, of dat deze activiteit door de AIVD en/of de MIVD zelf opgezet en uitgevoerd wordt op data die door middel van bulk intercept aan hen geleverd wordt. De memorie van toelichting spreekt van een combinatie-last. Dit lijkt erop te duiden dat netwerkmonitoring en –detectie door de aanbieder opgezet en uitgevoerd dient te worden.

Nederland ICT vraagt om een verduidelijking op dit onderdeel.

5. Wanneer aftapbaar zijn ?
Uit het voorstel blijkt niet dat men analoog aan Tw 13.1 lid 1, aanbieders van communicatiediensten verplicht hun communicatiediensten uitsluitend beschikbaar te stellen aan gebruikers indien deze aftapbaar zijn. Dit duidt erop dat de medewerkingsplicht, en de daar aan gekoppelde investeringen pas dienen te worden gedaan op het moment dat deze aanbieder met een last geconfronteerd wordt.

Nederland ICT vraagt een verduidelijking op dit onderdeel.

6. Hoe aftapbaar te zijn ?
Het voorstel geeft geen technische details over de manier waarop de integriteit, beschikbaarheid en vertrouwelijkheid van de getapte data gewaarborgd wordt. De ETSI-specificatie Transport of Intercepted IP Traffic (TIIT) v1.2.0 geeft technische details hoe aanbieders van openbare telecommunicatienetwerken en –diensten kunnen voldoen aan 13.1 Tw. Infrastructuuraanbieders dienen gebruik te maken van standaarden om interoperabiliteit te kunnen garanderen, het aftappen kan daardoor ook via een standaard (ETSI/TIIT) gereguleerd worden. Nu de scope wijzigt naar **elke** aanbieder van een communicatiedienst kan geen aansluiting gezocht worden bij een standaard, immers niet elke communicatiedienst ziet op interoperabiliteit, een groot aantal diensten (apps) voorziet in communicatie binnen het eigen ecosysteem. Het is niet duidelijk op welke wijze deze aanbieders moeten en kunnen voldoen aan de Wiv.

Onduidelijk blijft derhalve wat en wanneer men dient te investeren. Vooral voor kleinere innovatieve communicatiediensten aanbieders (start-ups) kan een verplichte investering, net als haar product populair wordt (binnen een doelgroep of land dat een aandachtsgebied van de AIVD en/of de MIVD is, dan wel is opgenomen in het (geheime) aanwijzingsbesluit) funest zijn voor verdere doorontwikkeling. Voor Nederland als start-up land is zo'n dreigende verplichte investering suboptimaal.

[4] idem, p.71

Nederland ICT vraagt de minister om een nadere toelichting.

7. Hoelang aftapbaar?

Het voorstel geeft aan dat een aanbieder nog 12 maanden na de beëindiging van de last zijn infrastructuur aftapbaar moeten houden (art. 37 lid 3 WIV). Dit is disproportioneel, aangezien deze taplasten, door de diensten, gemotiveerd beëindigd dienen te worden. Enige motivering dan wel een kosten/baten afwegingskader ontbreekt volledig.

Nederland ICT vraagt de minister om een nadere motivering.

8. Aansprakelijkheid?

In het voorstel ontbreekt tevens enig aansprakelijkheidsregime ten aanzien van vergoeding van schade door het directe of indirecte handelen of nalaten van de inlichtingen- en veiligheidsdiensten. Het installeren van een interceptievoorziening kan leiden tot een verstoring van de dienstverlening aan klanten. Het nemen van financiële verantwoordelijkheid voor haar eigen handelingen zou een goede afweging over wel of niet ingrijpen moeten ondersteunen.

Een extra moeilijkheid is de geheimhouding die rust op een last tot meewerken. Rechtspraak wijst uit dat op de overheid een zware aansprakelijkheid rust voor haar publiekrechtelijke (rechts)handelingen. Door de geheimhouding is de toegang tot de rechter voor een aanbieder van communicatiediensten in het geding.

Nederland ICT verzoekt om een eenduidige aansprakelijkheidsregeling en een eenduidige regeling waarbij toegang tot de rechter, vooraf, verzekerd is.

9. Toezicht:

Zoals uit het voorgaande blijkt, is Nederland ICT van mening dat bevoegdheden die zo diep ingrijpen op de Nederlandse burger en het bedrijfsleven omgeven moeten zijn met een uitermate stringent system van checks en balances. Alleen artikel 29 voorziet in een systeem van onafhankelijke bindende toetsing. Pas bij een contentieuze procedure, waarbij er analoog aan de Amerikaanse FISA procedure sprake is van een '*Public Advocate*'[5] kan het toetsingssysteem als adequaat worden aangemerkt. Het voorgestelde systeem voor de overige bepalingen voldoet volgens Nederland ICT niet aan minimale maatschappelijke en rechtsstatelijke verantwoording die nodig is om zo'n ingrijpend middel, rechtmatig, te kunnen invoeren.

Nederland ICT vraagt de minister alsnog een adequaat toetsingssysteem in het wetsvoorstel op te nemen.

10. Transparantie:

Naast toezicht is transparantie een belangrijke voorwaarde voor acceptatie van verregaande bevoegdheden. Het WRR rapport "*De publieke kern van het Internet. Naar een buitenlands internetbeleid.*[6]" geeft aan dat '*transparantie op een –noodzakelijkerwijs- hoog niveau zou kunnen helpen om nut en noodzaak van bepaalde programma's van de diensten op nationaal niveau te beoordelen [..]*'[7]. Nederland ICT sluit zich graag aan bij deze conclusie. Transparantie zoals in België

[5] http://illinoislawreview.org/wp-content/ilr-content/articles/2015/3/Poorbaugh.pdf , p.1391
[6] http://www.wrr.nl/publicaties/publicatie/article/de-publieke-kern-van-het-internet-1/
[7] WRR. De publieke kern van het Internet. Naar een buitenlands internetbeleid, p.108

door de BIM commissie[8] of de G-10-Kommission[9] in Duitsland maakt dat nut en noodzaak duidelijk gemaakt kunnen worden en er draagvlak ontstaat. Iets dat nu ontbreekt voor het huidige voorstel.

Nederland ICT vraagt de minister nader uit te werken hoe meer transparantie kan worden geboden over nut en noodzaak van bulkinterceptie en de wijze waarop communicatiedienstaanbieders hierover kunnen communiceren met hun klanten.

11. Technologie onafhankelijk:
Een van de genoemde doelstellingen is om de wet technologie onafhankelijk te maken. Er geldt echter ingevolge artikel 29 van het voorstel een specifieke regeling voor analoge communicatie (briefgeheim) die niet geldt voor elektronische communicatie. In gevolge het briefgeheim dient de rechtbank Den Haag, op verzoek van het hoofd van de dienst, een last af te geven. Nederland ICT is van mening dat deze toetsing vooraf ook voor de interceptie van alle overige communicatie dient te worden toegepast, zeker gezien de diverse voorstellen om elektronische communicatie onder artikel 13 van de Grondwet te brengen.

Door onderscheid te maken tussen 'papier' en 'digitaal' sluit het voorstel ook niet aan bij de Archiefwet.

Uit het voorstel blijkt ook niet hoe er met Voice over IP (VoIP) data uit de sleepnet taps dient te worden omgegaan. Niet duidelijk wordt of dergelijke data onder het grondwettelijke telefoongeheim vallen. Ingevolge artikel 13 Gw, lid 2 bestaat er een telefoongeheim. Klaarblijkelijk wordt dat geheim, zonder verdere motivering, in dit voorstel afgeschaft.

Nederland ICT vraagt de minister om een nadere motivering.

12. Encryptie:
Het hiervoor genoemde WRR rapport geeft ook aan[10] dat encryptie van het dataverkeer, zowel van data in transit als van opgeslagen data, grootschalige onderschepping van data door inlichtingen- en veiligheidsdiensten zowel veel moeilijker als veel duurder maakt. Nu biedt het voorstel de mogelijkheid om een aanbieder te dwingen de communicatie te ontsleutelen, echter dat zal niet in alle gevallen zomaar kunnen.

Ter illustratie, Perfect Forward Secrecy[11] bewaart geen encryptiesleutels. Het is daardoor voor de aanbieder niet mogelijk om deze communicatiestroom ontsleuteld uit te leveren aan de diensten. In het voorstel is het onduidelijk of de zogenaamde ontsleutelbevel ook het inbouwen of (gedeeltelijk) uitschakelen van essentiële encryptiemethoden verplicht maakt voor leveranciers. Het inbouwen van zogenaamde '*backdoors*' waar alleen diensten toegang tot hebben is een illusie. Bruce Schneier, een bekende internetveiligheidsexpert stelt: "*You can't build a backdoor that only the good guys can walk through*"[12]. De onthullingen gedaan door Snowden laten zien op welke wijze inlichtingen- en veiligheidsdiensten proberen de omgeving naar hun hand te zetten. Zo werd doelbewust een encryptiealgoritme verzwakt[13].

[8] http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2013.pdf
[9] http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf
[10] idem, p.90
[11] https://nl.wikipedia.org/wiki/Perfect_forward_secrecy
[12] https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html
[13] https://www.lawfareblog.com/nsas-subversion-nists-algorithm

De onthullingen van Snowden hebben een enorme economische impact op Amerikaanse technologiebedrijven. Dit heeft ertoe geleid dat Obama het beleid heeft gewijzigd: '*the mass collection of phone data will be sharply curtailed*'[14]. Gezien de algehele weerstand tegen deze mogelijke bevoegdheden wereldwijd en zeker in de V.S. zou introductie van deze bevoegdheid in Nederland funest zijn voor Nederland als ICT standplaats. In dit licht is het vreemd dat Nederland nu juist de mogelijkheden voor massasurveillance, zonder verdere inhoudelijke motivatie introduceert. De economische gevolgen zullen niet anders zijn dan in Amerika[15].

Saillant is de conclusie "*The biggest difference between initial worst-case projections in 2013 of revenue loss of $180 billion and the current $47 billion projection is that customers took encryption into their own hands, said Forrester*." De opbrengsten van bulk interceptie kunnen derhalve door het en masse gebruik van encryptie door eindgebruikers naar verwachting niet opwegen tegen de kosten. Door de encryptie bij gebruikers te laten, kan een dienstenaanbieder niet voldoen aan de ontsleutelplicht. Het is immers alleen de klant die de encryptiesleutel heeft.

Nederland ICT vraagt de minister in te gaan op de gevolgen van toenemende encryptie door de eindgebruiker voor dit wetsvoorstel, en nader te onderbouwen wat het effect van het wetsvoorstel zal zijn op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

13. Proportionaliteitstoets:
Het voorstel geeft in de artikelen 43 en 44 een afwegingskader voor noodzakelijkheid, proportionaliteit en subsidiariteit met betrekking tot het uitoefenen van de bevoegdheden. Zo'n afwegingskader is een papieren werkelijkheid. Om het afwegingskader handen en voeten te geven pleit Nederland ICT ervoor om het kader in te bedden in een budgettair model. Dit zorgt er voor dat, door de simpele beperking van een vooraf vastgesteld of flexibel budget voor de kosten van interceptie, financiële overwegingen voor de diensten de proportionaliteitstoets mede inkleuren. Het dwingt de diensten ertoe om hun activiteiten veel scherper en doelgerichter op- en in te zetten.

Dit geeft de diensten een betere *Return-on-Investment* bij haar onderzoeken. Tevens zorgt het voor een democratische controle op de kosten van interceptie omdat het benodigde budget via de Rijksbegroting inzichtelijk is. Naast deze efficiëntere afhandeling en effectieve proportionaliteits-toetsing dient er zich nog een belangrijk economisch voordeel aan. Bedrijven kunnen blijven investeren in innovatie, en daarmee de groei van de BV Nederland faciliteren.

Nederland ICT vraagt de minister aan te geven wat de te verwachten kosten voor de verschillende communicatiedienstaanbieders zijn en waarom er voor is gekozen deze kosten bij de private partijen neer te leggen.

14. Vergoeding kosten:
Uit artikel 13.2 van de Telecomwet (Tw) volgt dat aanbieders van openbare telecommunicatienetwerken en –diensten, verplicht zijn hun netwerk aftapbaar te maken. Deze aftapbaarheid kan worden gebruikt door zowel de opsporings- alsmede de inlichtingen- en

[14] http://blogs.wsj.com/cio/2014/01/17/obama-addresses-economic-damage-caused-by-snowden-nsa-leaks/
[15] http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/

veiligheidsdiensten. De aftapbaarheid ziet toe op een geïndividualiseerd subject. Er is daarom sprake van gerichte interceptie. De 'geïndividualiseerde' aftapbaarheid van de huidige infrastructuur is geregeld bij Besluit aftappen openbare Telecommunicatienetwerken en –diensten. De capex[16] kosten komen voor rekening van de bedrijven (Tw 13.6 lid 1). Alleen de directe opex[17] kosten voor het uitvoeren van een taplast komen voor vergoeding in aanmerking (Tw 13.6 lid 2). Artikel 32, lid 8 van het voorstel verklaart deze regeling van overeenkomstige toepassing. De Memorie van Toelichting zegt: "*Er bestaat geen aanleiding om voor deze aanbieders een (deels) afwijkende regeling te treffen*"[18].

De Telecomwet maakt onderscheid tussen communicatiediensten en –netwerken en openbare communicatiediensten en –netwerken. Het onderliggende voorstel maakt dat onderscheid niet. Alleen de openbare communicatienetwerken en –diensten vallen onder de werking van artikel 13.2 Tw. Voor de overige, niet openbare communicatienetwerken en –diensten gelden slechts de verplichtingen om mee te werken uit het Wetboek van Strafvordering en niet die uit de Telecomwet. Er bestaat voor deze groep geen verplichting om haar netwerk of dienst a priori aftapbaar te maken, tevens geeft de systematiek van strafvordering de mogelijkheid om redelijke kosten bij het Openbaar Ministerie te claimen.

De kosten van het nakomen van een vordering tot het verstrekken van gegevens, tot het medewerking verlenen aan het ontsleutelen of het bewaren en beschikbaar houden van gegevens komen op grond van het Wetboek van Strafvordering wel voor vergoeding in aanmerking.

Een zeer beperkte groep van (openbare) communicatiediensten aanbieders valt onder de Telecomwet de overige aanbieders van communicatiediensten zou onder art. 592 Wetboek van Strafvordering wel in aanmerking komen voor vergoeding van kosten. Dat onder het voorstel deze grotere groep van aanbieders hun recht op vergoeding zal worden afgenomen wordt in het geheel niet onderbouwd.

Nederland ICT vraagt de minister deze onderbouwing alsnog te leveren.

15. Capaciteit:

In het voorgaande hebben we bekeken wat de hernieuwde Wiv inhoudt voor aanbieders van communicatiediensten. Alle getapte communicatie zal door de AIVD en/of de MIVD verwerkt moeten worden.

Ongeveer 90% van alle communicatie verloopt via kabelnetwerken, terwijl de hoeveelheid gegevens elke twee tot drie jaar verdubbelt. De hoeveelheid data die de AIVD en/of de MIVD in het nieuwe voorstel moeten verwerken zal dan ook naar verwachting meer dan vertienvoudigen. Mocht het voorstel medio 2017 inwerking treden dan zou dat zelfs een vertwintigvoudiging kunnen zijn. Het is onduidelijk op welke wijze de AIVD met de huidige en voor 2017 geprognosticeerde personele capaciteit deze nieuwe stroom aan gegevens inhoudelijk op een zinvolle wijze kan analyseren. In het licht van het voorstel en de te verwachten explosie van te verwerken gegevens zal de personele capaciteit sterk dienen te worden uitgebreid met de daartoe benodigde specialistische kennis. Over

[16] https://en.wikipedia.org/wiki/Capital_expenditure
[17] https://en.wikipedia.org/wiki/Operating_expense
[18] idem, p.61

de daartoe beschikbare middelen wordt in het wetsvoorstel niet gesproken, ook wordt niet aangegeven op welke termijn de diensten denken de benodigde aanvullende specialistische kennis operationeel in te kunnen zetten. De komende Rijksbegroting zal wellicht meer inzicht geven.

Een ander scenario is dat de AIVD en/of MIVD niet geïnteresseerd zijn in het verwerken van de communicatie, maar dat ze de ruwe data als handelswaar zien. Artikel 77 lid 2 van het voorstel maakt deze zgn. bulkdata uitwisselbaar. Daarvoor is slechts eenmalig ministeriële toestemming nodig.

Onder ruwe data, ofwel ongeëvalueerde gegevens, valt bijvoorbeeld een kopie van een complete website en de in het kader van artikel 33 ontvangen en opgenomen gegevens waarop nog geen selectie is toegepast als bedoeld in artikel 35, eerste lid, van het wetsvoorstel. Overigens wordt opgemerkt dat de toestemming ook betrekking kan hebben op meerdere opeenvolgende verstrekkingen van vergelijkbare aard, zonder dat dit per geval dient te worden verleend.

Nederland ICT vraagt de minister nader toe te lichten hoe men de bulkdata, ook bij de verwachte toename, op een zinvolle manier denkt te kunnen verwerken.

Resumerend

Onder het mom van '*technologie onafhankelijk maken van de interceptie*' wordt volgens Nederland ICT onvoldoende gemotiveerd fundamentele wijzigingen aangebracht in de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze fundamentele wijzigingen worden niet gecompenseerd door enige vorm van onafhankelijk toezicht vooraf.

Nederland ICT heeft grote twijfels over het nut en noodzaak, de transparantie en proportionaliteit, de reikwijdte en toerekening van kosten, de praktische uitvoerbaarheid en het juridisch toetsingskader van de nieuwe bevoegdheden en daarmee het draagvlak voor een dergelijk ingrijpend wetsvoorstel.

Door de kosten geheel op de aanbieder af te wentelen, creëert de overheid geen geïnternaliseerd *incentive* bij de inlichtingen- en veiligheidsdiensten om *overreach* tegen te gaan.

"*In prior generations, the cost of surveillance and data acquisition constituted a useful buffer between state surveillance and privacy; resource constraints forced law enforcement to focus on a limited number of targets on a scale where judicial oversight was a practical – if imperfect- deterrent against overreach*"[19].

De door de wet opgelegde eisen aan een groot aantal bedrijven zal resulteren in een verlies aan vertrouwen van burgers en bedrijven, in toegenomen onzekerheid en financiële druk voor het bedrijfsleven, minder innovatie, risico's voor de betrouwbaarheid en integriteit van dienstverlening en verslechtering van het internationale imago van Nederlandse als Digital Gateway to Europe.

Nederland ICT pleit er voor om bij het opleggen van dergelijke verplichtingen voor het bedrijfsleven altijd de kosten via de Rijksbegroting te laten lopen. Niet alleen is er zodoende democratisch toezicht

[19] Governments as Actors, Faris and Gasser, Internetmonitor 2013, Reflections on the digital world, p.21 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840)

op de kosten, ook worden de diensten er door financiële overwegingen toe gedwongen hun activiteiten scherp en doelgericht in te zetten. De proportionaliteit is hierdoor beter geborgd.

Meer specifiek vraagt Nederland ICT de minister, in overleg met zijn collega's van Veiligheid en Justitie en Economische Zaken, om:

- Een gedegen onderbouwing van nut en noodzaak van een dergelijk ingrijpend wetsvoorstel.
- Een voorstel hoe in de toekomst op een transparante wijze inzicht gegeven wordt in de reikwijdte van de bevoegdheden van inlichtingen- en veiligheidsdiensten en de wijze waarop deze hun taak uitoefenen. Dit teneinde het vertrouwen van burgers en bedrijven in de integriteit van hun data, het internet en daarmee de digitale economie als geheel te waarborgen.
- Een analyse van het effect dat het wetsvoorstel zal hebben op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@nederlandict.nl
www.nederlandict.nl

ING Bank
IBAN: NL 53 ING B 0662 590546
KvK 30174840