BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank NL32ABNA0554706512
KvK 34 12 12 86

M +31 6 13380036
E ton.siedsma@bof.nl
W https://www.bof.nl

Dr. R.H.A. Plasterk
Minister van Binnenlandse Zaken en
Koninkrijksrelaties
Turfmarkt 157
2511 DP Den Haag

Betreft
Reactie op consultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX

Amsterdam
1 september 2015

Geachte minister Plasterk,

Bij dezen wil Bits of Freedom graag reageren op het wetsvoorstel op de inlichtingen- en veiligheidsdiensten 20XX dat u ter consultatie hebt aangeboden.

Het is een onderwerp dat leeft: ruim 500 burgers, belangenorganisaties en bedrijven hebben op de consultatie gereageerd. Bits of Freedom hoopt dat het ministerie de in al deze reacties geuite zorgen ter harte neemt.

Het wetsvoorstel beoogt een nieuwe balans te vinden tussen nieuwe bevoegdheden en versterkte waarborgen. Bits of Freedom is van mening dat voor zowel het geheel van de wet als voor een aantal specifieke bevoegdheden die balans wordt gemist.

Door de voortschrijdende digitalisering van communicatie hebben de inlichtingen- en veiligheidsdiensten nog nooit eerder in de geschiedenis de beschikking gehad over zoveel gegevens. Ook met gelijkblijvende bevoegdheden zal de informatiestroom naar verwachting alleen maar toenemen. Nu wordt voorgesteld die bevoegdheden nog verder uit te breiden, waardoor de hoeveelheid verzamelde gegevens alleen maar groter wordt. Het is niet zeker of dat ook zinvol is. In zijn algemeenheid ontbreekt in de Memorie van Toelichting aandacht voor de huidige effectiviteit van de inlichtingen- en veiligheidsdiensten en de effectiviteit en noodzaak van voorgestelde bevoegdheden.

Bits of Freedom zal hieronder uitgebreid op de bezwaren van het wetsvoorstel ingaan. Vooropgesteld zijn de belangrijkste punten voor Bits of Freedom:

- Introduceer geen nieuwe bevoegdheden zonder onderbouwing van de noodzaak;
- Schrap de sleepnetbevoegdheid;
- Beperk de uitwisseling van gegevens met buitenlandse diensten;
- Introduceer bindend toezicht op de inlichtingen- en veiligheidsdiensten.

Uiteraard zijn wij graag bereid om onze reactie nader toe te lichten, mocht daaraan behoefte bestaan.

Met vriendelijke groet,

Ton Siedsma

1. Minimumwaarborgen zijn niet goed genoeg voor Nederland

De voorliggende integrale herziening van de wet op de inlichtingen- en veiligheidsdiensten is een uitgelezen kans om de bescherming van grondrechten van burgers bij het uitoefenen van de bevoegdheden van inlichtingen- en veiligheidsdiensten voor het komende decennium goed te regelen.

Eén van de redenen om de wet te wijzigen is, zoals in de Memorie van Toelichting (MvT) wordt gesteld, dat de huidige wet niet meer voldoet aan de huidige eisen van het EHRM.[1] Een andere reden om de wet aan te passen is om de bevoegdheden in de wet aan te passen.[2] Ten slotte is het de bedoeling om de waarborgen in een nieuwe balans te brengen met de voorgestelde nieuwe bevoegdheden.

Ook zonder de invoering van nieuwe bevoegdheden is het nodig om de huidige bevoegdheden in balans te brengen met nieuwe waarborgen. Dat is zeker zo wanneer daarbij in aanmerking wordt genomen dat, door technologische ontwikkelingen, met de inzet van de huidige bevoegdheden een grotere inbreuk gemaakt kan worden op grondrechten dan werd voorzien bij de invoering van de Wiv2002.[3]

Het aanpassen van de waarborgen van bijzondere bevoegdheden gebeurt, blijkens de toelichting, naar de ondergrens van de waarborgen van het EHRM: ¨De door het EHRM geformuleerde minimum waarborgen zijn onder meer bij de uitwerking van de nieuwe regeling inzake de bijzondere bevoegdheden geïmplementeerd.¨[4] Dat is om twee redenen een teleurstellende keuze.

1.2 Nederland moet het goede voorbeeld geven

Ten eerste gaat het om de minimum waarborgen van het EHRM. Dat is een absolute ondergrens voor alle landen die bij het EVRM zijn aangesloten. Door die ondergrens te kiezen worden de mensenrechtelijke kantjes er vanaf gelopen.

Nederland moet juist in dit verband het goede voorbeeld geven. Dat is niet alleen een morele verplichting die de Nederlandse regering naar haar burgers heeft, maar ook een mogelijkheid om in Europa – en in de rest van de wereld – een positief voorbeeld te geven hoe een overheid kan omgaan met de grondrechten van haar burgers.

1 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 28.
2 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 5.
3 Zie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Commissie Dessens, p. 78.
4 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 30.

1.3 Voorkom een snelle herziening

Ten tweede is de wet op de inlichtingen- en veiligheidsdiensten al eerder aangepast omdat de waarborgen in de wet onder de ondergrens van het EHRM zaten.[5] Als de voorgestelde waarborgen in lijn zouden zijn met de minimumvereisten van het EHRM, dan is het denkbaar dat de nieuwe waarborgen ook in de toekomst onder de ondergrens van het EHRM vallen. Dat zou niet alleen betekenen dat de wet weer zou moeten worden aangepast, wat veel tijd, geld en energie zou kosten, maar dan zouden dus ook de grondrechten van de Nederlandse burger – net als nu – onvoldoende beschermd worden. Dat is onnodig.

Het zou beter zijn om op toekomstige ontwikkelingen te anticiperen en de wet zodanig ´Straatsburg-proof´ te maken dat er ook voor de toekomst voldaan wordt aan de vereisten van het EHRM.

In die context is het teleurstellend dat er bij de inbreuk die de inzet van deze bevoegdheden op grondrechten oplevert niet alleen summier getoetst wordt op het recht op privacy en het briefgeheim, maar dat er zelfs helemaal geen afweging gemaakt wordt ten opzichte van andere grondrechten, zoals de *chilling effects* die deze bevoegdheden kunnen hebben op de vrijheid van meningsuiting.[6]

2. Trek de bevoegdheid voor een sleepnet in

De minister stelt voor om de bevoegdheid in te voeren om niet-kabelgebonden communicatieverkeer ongericht te kunnen onderscheppen.

Bits of Freedom is van mening dat het voorstel om deze bevoegdheid in te voeren ingetrokken moet worden. Ten eerste wordt ten onrechte geen afweging gemaakt tussen de grondrechten van burgers en de inbreuk die het invoeren van deze bevoegdheid op die grondrechten oplevert. Daarnaast ontbreekt de noodzaak om deze bevoegdheid in te voeren. Ten derde is deze bevoegdheid niet proportioneel ten opzichte van de inbreuk die de bevoegdheid veroorzaakt. Tot slot wordt niet aangetoond dat deze bevoegdheid effectiever zal zijn dan andere, minder inbreukmakende, bevoegdheden.

2.1 De overheid moet een fundamentele vraag beantwoorden

De regering gaat ten onrechte een principieel debat over de bescherming van grondrechten uit de weg. De Toelichting gaat nu alleen in op de redenen waarom de diensten deze bevoegdheid moeten hebben. Maar er is ook een fundamentele keerzijde: wat die bevoegdheden betekenen voor de grondrechten

5 Memorie van Toelichting wiv2002, p. 1.
6 Zie bijvoorbeeld het rapport van de Human Rights Watch en de ACLU: https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

van burgers en voor de wijze waarop die burgers beschermd worden tegen overheidsingrijpen.

Veel barrières die van oudsher een belemmering vormden tegen het op grote schaal kunnen volgen van burgers zijn vervaagd. Anders gezegd: zelfs als de Nederlandse overheid in het verleden alle communicatie van burgers had willen onderscheppen, was dat niet mogelijk geweest omdat de technologie niet bestond, het te duur was en het analyseren van die communicatie teveel mankracht zou kosten.

Technologische ontwikkelingen hebben het mogelijk gemaakt om (vrijwel) elke vorm van communicatie tussen personen, bedrijven en overheden te onderscheppen. Daarnaast is het nu ook mogelijk om dat tegen geringe kosten arbeidsextensief te doen: onderschepte communicatie kan automatisch gefilterd, geselecteerd en doorzocht worden.

Dat betekent dat de fundamentele vraag die eerder niet aan de orde was nu wel aan de orde is: moeten de Nederlandse inlichtingen- en veiligheidsdiensten de mogelijkheid hebben om de communicatie van élke burger en masse te onderscheppen zonder dat die burger daarvoor enige aanleiding heeft gegeven? De regering moet deze vraag in de Memorie van Toelichting beantwoorden.

2.2 Artikel 33 is een ongerichte bevoegdheid, dat moet uit de wet blijken

Het woord ´ongericht´ staat niet in artikel 33, maar het is wel degelijk een ongerichte bevoegdheid.

Immers, artikel 32 luidt: *De diensten zijn bevoegd tot het met een technisch hulpmiddel* ***gericht*** *aftappen, ontvangen, opnemen en afluisteren van elke vorm van* ***gesprek****, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt.*

Artikel 33 luidt: *´De diensten zijn bevoegd tot het met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk ongeacht waar een en ander plaatsvindt* ***in andere gevallen dan bedoeld in artikel 32´***,

Er zijn twee verschillen tussen deze twee artikelen. In artikel 32 komen de woorden ¨gesprek¨ en ¨gericht¨ voor en in artikel 33 niet. Artikel 33 betreft ¨in andere gevallen dan bedoeld in artikel 32¨. Artikel 32 betreft gericht onderscheppen, artikel 33 betreft dus het in andere gevallen dan gericht onderscheppen, oftewel ongericht onderscheppen.

Het gaat dus om een ongerichte bevoegdheid. De vaagheid van het artikel maakt de gevolgen niet voorzienbaar voor de burger.

2.3 Zonder aangetoonde noodzaak geen nieuwe bevoegdheid

In de Toelichting wordt niet aannemelijk gemaakt dat er een noodzaak is om de inlichtingen- en veiligheidsdiensten toe te staan in bulk ongericht kabelgebonden communicatie van (Nederlandse) burgers te onderscheppen.

De overheid moet, nog voordat er kan worden gesproken over de wijze waarop een dergelijke bevoegdheid invulling zou moeten krijgen, aantonen waarom de bevoegdheid noodzakelijk is. Zelfs de sterkste waarborg bij de individuele inzet van een bevoegdheid kan een ontbrekende noodzaak voor het invoeren van een bevoegdheid niet rechtvaardigen.

De Toelichting voert aan dat een hoogwaardige zelfstandige informatiepositie noodzakelijk is voor de geheime diensten[7] én dat tegenwoordig 90% van de communicatie over de kabel verloopt en dat de diensten geen toegang hebben tot die communicatie.[8]

Ten eerste hebben de diensten nu al toegang tot kabelgebonden communicatie. Ze kunnen onder meer gericht de kabel aftappen van personen, groepen of organisaties die zij in het vizier hebben, ze kunnen ook vorderingen tot aanbieders van communicatie richten, geautomatiseerde werken hacken, onderzoek doen op sociale media; ook als die informatie via de kabel verzonden wordt.

Ten tweede blijkt niet uit de Toelichting dat de informatiepositie van de diensten daadwerkelijk een risico loopt. De diensten hebben tal van bevoegdheden tot hun beschikking om informatie te verzamelen. Nergens blijkt dat de bestaande bevoegdheden onvoldoende effectief zijn om de informatiepositie op peil te houden.

Daarnaast is het feit dat iets technisch mogelijk is geen reden om dat ook te doen. Zoals ook de CTIVD in het jaarverslag 2014-2015 aangeeft, is het feit dat communicatie via de kabel plaatsvindt en niet meer via de ether onvoldoende reden om vervolgens dan ook die communicatie in bulk te onderscheppen.[9]

2.4 Proportionaliteit en subsidiariteit bevoegdheid niet aangetoond

Er is in de Toelichting geen afweging gemaakt waarom de bevoegdheid proportioneel zou zijn ten opzichte van de inbreuk die de bevoegdheid veroorzaakt. Zoals hierboven al beschreven, levert het in bulk onderscheppen van communicatie een enorme inbreuk op de grondrechten van de burgers wiens communicatie onderschept wordt. De regering moet aantonen dat deze bevoegdheid proportioneel is.

7 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 63.
8 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 63.
9 Jaarverslag CTIVD 2014-2015, p. 28.

Ook de subsidiariteit van de bevoegdheid wordt onvoldoende aangetoond. Ten eerste toont de Memorie van Toelichting niet aan dat is onderzocht of de bestaande bevoegdheden onvoldoende effectief zijn. Daarnaast blijkt nergens dat er onderzoek is gedaan naar andere bevoegdheden die hetzelfde resultaat zouden bereiken met een geringere inbreuk op de grondrechten van burgers.

De Toelichting gaat wél in op de proportionaliteit en subsidiariteit bij de specifieke inzet van de bevoegdheid.[10] Maar als in zijn algemeenheid de proportionaliteit en subsidiariteit van de bevoegdheid niet aangetoond is, dan is de proportionaliteits- en subsidiariteitstoets bij de specifieke inzet van deze bevoegdheid een wassen neus.

2.5 De voorgestelde waarborgen zijn ondermaats

In het wetsvoorstel zijn tal van waarborgen opgenomen die op papier robuust ogen, maar dat in de praktijk niet zijn. Het vereiste van ´doelgerichtheid´ is te vaag, de termijnen voor interceptie en opslag zijn te ruim, er zijn geen beperkingen in de cumulatieve inzet, de combinatie-lasten ondermijnen waarborgen en tot slot zijn de toestemmingsvereisten voor de tweede en derde fase minder zwaarwegend dan ze beogen te zijn.

2.5.1 Ook interceptie en opslag levert een grote inbreuk op

Dat de privacy-inbreuk in de interceptiefase beperkt is, is onjuist.[11] Zelfs als in het stadium na het intercepteren van communicatie de te doorzoeken communicatie tot een summiere groep personen beperkt zou worden, wil dat niet zeggen dat de inbreuk op de grondrechten van alle personen wiens gegevens in de eerste fase zijn onderschept niet groot is. Het feit dat hun communicatie niet verder geanalyseerd of bekeken wordt, doet daar niets aan af: de inbreuk die het opvangen en opslaan van communicatie veroorzaakt is al ontstaan.[12] De lange bewaartermijn maakt die inbreuk nog groter.

2.5.2 Doelgericht blijft ongericht

De reikwijdte van de bevoegdheid om ongericht communicatie te onderscheppen wordt in het voorgestelde artikel 33 niet ingeperkt. Volgens de Toelichting wordt de ongerichte interceptie beperkt doordat de inzet van de bevoegdheid doelgericht dient te zijn. De minister heeft in het eerder aangehaalde Kamerdebat over deze bevoegdheid in februari 2015 herhaaldelijk aangeven er sprake zou zijn van een ´doelgerichte´ bevoegdheid. De Memorie van Toelichting spreekt over een ´doelgerichte inzet´ en ´doelgerichte verwerving´.

10 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 68.
11 Anders dus dan in de concept-memorie van toelichting wordt beweerd, zie p. 68.
12 Zie *Opinion 04/2014 on electronic communications for intelligence and national security purposes* 2014, p. 27.

Doelgerichte interceptie moet een waarborg zijn die het ongerichte karakter van de interceptie inperkt. Maar uit de Memorie van Toelichting blijkt niet wat precies onder ´doelgericht´ moet worden verstaan. Artikel 24 van het voorstel is van toepassing op artikel 33. Het artikel geeft een specificatie van eisen waaraan een verzoek voor de inzet van de bevoegdheid uit artikel 33 moet voldoen, maar ook de toelichting op artikel 24 maakt niet goed duidelijk hoe precies het ´doel´ omschreven moet worden. Het enige voorbeeld dat gegeven wordt is dat ¨onderzoek naar terrorismedreiging¨[13] te vaag omschreven is om bevoegdheden in te mogen zetten, maar dat zegt nog niets over hoe precies een omschrijving wel zou moeten zijn.

Datzelfde geldt ook voor de soorten communicatie die onderschept mogen worden; er wordt weliswaar vereist dat deze afgebakend dienen te worden, maar in praktijk zal het blijven gaan om grote hoeveelheden gegevens die onderschept worden. Al het spraakverkeer tussen een buurt in Nederland en een land in het buitenland is weliswaar beperkter dan al het spraakverkeer van en naar Nederland onderscheppen, maar dat wil niet zeggen dat het niet ongericht is. Daarmee blijft te vaag hoe ongericht de bevoegdheid in zijn uitvoering precies zal zijn.

2.5.3 Lange duur inzet en opslag maakt inzet nog meer ongericht

De combinatie van de lange duur van de inzet van de bevoegdheid en de opslagtermijn maakt de inbreuk van de bevoegdheid nog groter.

Het kan niet zo zijn dat een ongerichte bevoegdheid die een grote inbreuk maakt op de gehele groep burgers wiens communicatie onderschept wordt veel langer ingezet kan worden dan een bevoegdheid die gericht wordt ingezet. Toch stelt de minister dat voor.

De inzet van de interceptiebevoegdheid maakt het mogelijk om voor een periode van maximaal 12 maanden de bevoegdheid uit te oefenen, waarbij die periode telkens voor de periode van maximaal 12 maanden verlengd kan worden. Dat is een periode die, zoals ook de minister zelf zegt, afwijkt van de normale termijn van drie maanden.[14] Volgens de minister is dat mogelijk omdat de ¨indringendheid van de privacy-inbreuk in deze fase beperkt is en voorts de onderzoeksopdrachten voor een periode van een jaar worden vastgelegd¨[15].

Waarom het uitoefenen van deze bevoegdheid vereist dat een individuele inzet één jaar zou moeten duren, wordt niet aangegeven. Onderzoeksopdrachten worden voor een jaar vastgesteld, maar dat is nog geen reden om specifieke inzetten van bevoegdheden dan ook voor die periode in te voeren. Het is niet ondenkbaar dat die onderzoeksopdrachten tamelijk generiek worden opgesteld.

13 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 36.
14 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 68.
15 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 68.

De inzet van bevoegdheden zijn dienend aan die onderzoeksopdrachten, maar zullen dan specifieker omschreven moeten worden.

Onderschepte communicatie mag drie jaar worden bewaard – en versleuteld mogelijk zelfs langer. De onderbouwing van de periode van drie jaar wordt niet verder onderbouwd dan dat de periode van één jaar op dit moment als een knelpunt wordt ervaren.[16] Ook stelt de minister dat uit voorbeelden uit de praktijk van de diensten blijkt dat de termijn van drie jaar de diensten in ¨voldoende mate in staat stelt de toebedeelde onderzoeksopdrachten op verantwoorde wijze in te vullen.¨[17] Dat is opmerkelijk, want niet alleen worden de onderzoeksopdrachten voor één jaar vastgesteld, maar daarnaast is de huidige bewaartermijnen voor ongerichte interceptie één jaar.[18] De aangehaalde voorbeelden lijken dus of fictief en daarmee niet bruikbaar, of de diensten hebben zich blijkbaar niet aan de bestaande wettelijke opslagtermijn gehouden.

2.5.4 Cumulatie van inzetten maakt de bevoegdheid nog meer ongericht

De cumulatieve individuele inzetten van de bevoegdheid ex artikel 33 kan in de praktijk tot een nog breder sleepnetmiddel leiden. Dat is zeker het geval gezien de hierboven beschreven lange duur van de inzet en opslagtermijn.

In de Toelichting is niets opgenomen over de verwachte hoeveelheid inzetten per jaar. Het is denkbaar dat er meerdere inzetten tegelijkertijd plaats zullen vinden. Bovendien kunnen die inzetten allemaal meerdere jaren duren. De combinatie van die inzetten zal dan in de praktijk op een nog meer ongerichte gegevensverzameling neerkomen.

2.5.5 Combinatie-lasten verlagen waarborgen

Volgens de Toelichting zal in de praktijk vaak gebruikt gemaakt worden van de zogenaamde combinatie-last, waarbij gelijktijdig toestemming wordt gegeven voor artikel 33 en artikel 34. De Toelichting zegt daarover dat dat niet betekent dat beide verzoeken niet zorgvuldig voorbereid dienen te worden. In de praktijk zal het zwaartepunt van de ministeriële toestemming waarschijnlijk liggen bij artikel 33. Dat is ook logisch, want dat is het artikel waarmee daadwerkelijk communicatie onderschept kan worden.

Op het moment dat die hobbel genomen is en de communicatie verzameld is, is het logisch dat er ook iets met die communicatie gedaan wordt. De neiging om in te stemmen met een verzoek om iets te doen met de al verzamelde communicatie zal dan ook logischerwijs groot zijn. Het is daarom sterk de vraag of de toestemming voor artikel 34 en in (mindere mate) voor artikel 35 wel een fundamentele extra waarborg is, als in de praktijk toch standaard of vrijwel standaard toestemming zal worden gegeven.

16 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 68.
17 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 75.
18 Zie artikel 27 lid 9 van de Wiv2002.

2.5.6 Reikwijdte van bevoegdheid moet uit wet blijken, niet uit praktijk

De daadwerkelijke reikwijdte van deze ongerichte bevoegdheid zal pas in de praktijk duidelijk worden. Een bevoegdheid moet zoveel mogelijk worden ingeperkt, via de wet, maar ook via de toelichting. Hoe vager een bevoegdheid, hoe meer ruimte er is om de bevoegdheid ruim te interpreteren. Dat gaat ten koste van de rechtszekerheid.

Daarnaast maken vage bevoegdheden het toezicht lastig. Door een vage omschrijving legt het een extra zware druk op de toezichthouder om de uitoefening nader te toetsen en in te kaderen. Een helder kader maakt het toetsen eenvoudiger.

In het voorgestelde systeem waarin niet de CTIVD maar de CIVD het laatste woord heeft over de rechtmatigheid van de inzet van bevoegdheden, betekent het dat de reikwijdte van de ongerichtheid een politieke afweging wordt, maar zonder dat daar een publiek debat over wordt gevoerd. Dat is onwenselijk. Simpel gezegd: of het aftappen van communicatie tussen Amsterdam-Oost en Land-X wel doelgericht genoeg is en het aftappen van communicatie tussen Amsterdam – Land-X niet, is niet een beslissing die door de CIVD genomen zou moeten worden.

2.6 Artikel 33 is techniekafhankelijk geformuleerd

Gesprekken mogen volgens het wetsvoorstel niet ongericht worden onderschept. Maar of dit een fundamentele keuze is, of een overweging op praktische gronden om gesprekken niet te onderscheppen blijft onduidelijk.

Op grond van artikel 32 kunnen gesprekken gericht worden opgenomen. Voor artikel 33 geldt dat gesprekken niet ongericht mogen worden verzameld. Dat gesprek moet dan kennelijk een gesprek zijn dat niet via telecommunicatie of gegevensoverdracht plaatsvindt, aangezien de Memorie van Toelichting het in het kader van artikel 33 ook over het onderscheppen van spraakverkeer via satellieten heeft.[19] Dat is – voor een technologieonafhankelijke – bepaling opmerkelijk.

Volgens de regering is dus het ene soort gesprekken het beschermen tegen ongerichte verzameling wél waard en het andere soort gesprekken niet. Een reden geeft de Toelichting niet. Als er al een onderscheid gemaakt zou moeten worden, dan zou het onderscheid moeten liggen in het vertrouwelijke karakter van die gesprekken, niet in het kader of er wel of niet technologie voor is gebruikt. Immers, de mate waarin mensen vertrouwen dat persoonlijke e-mails, sms-berichten, niet-publieke berichten via Facebook en dergelijke niet worden bekeken, kan groter zijn dan het vertrouwen dat gesprekken in een bar, op een terras of op straat niet zal worden afgeluisterd door een derde. Het lezen van e-

19 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 67.

mail kan eenzelfde inbreuk opleveren als het doorlezen van een brief.

2.7 ´Cyberbevoegdheid´ moet een zelfstandige bevoegdheid zijn

Artikel 34, eerste lid, aanhef en onder a, geeft volgens de Memorie van Toelichting, de inlichtingen- en veiligheidsdiensten de bevoegdheid om aan netwerkmonitoring en netwerkdetectie te doen. Het is de bedoeling dat het mogelijk wordt om *real time* het dataverkeer te analyseren.

Alleen al voor de rechtszekerheid zou een dergelijke bevoegdheid een zelfstandige bevoegdheid moeten zijn en niet ondergebracht moeten worden onder artikel 34, eerste lid, aanhef en onder a.

De bevoegdheid om zulke monitoring en detectie uit te voeren, lijkt op deze manier weggemoffeld te zijn: uit een lezing van de wetstekst zou nooit duidelijk worden dat een dergelijke bevoegdheid onder het artikel kan worden verstaan. Belangrijker nog is dat het fundamenteel een andersoortige bevoegdheid is dan artikel 34, eerste lid, aanhef en onder a lijkt te suggereren: namelijk een voorbewerking ten dienste van artikel 33 en ten dienste van artikel 35.

2.7.1 Invulling ´cyberbevoegdheid´ is onduidelijk

Het is niet duidelijk hoe deze bevoegdheid zich verhoudt tot het nationaal detectienetwerk van het NCSC en op welke wijze deze bevoegdheid daarop een aanvulling zal zijn en of het ook nodig is om daar een aanvulling op te hebben. Of het bijvoorbeeld voor de diensten wenselijk is om zelfstandig internetverkeer te kunnen onderscheppen om te analyseren en niet afhankelijk te hoeven zijn van het samenwerkingsverband bij het Nationaal Detectie Netwerk (NDN) wordt niet in de Toelichting beantwoord.

Daarnaast is het niet duidelijk op welke wijze met aangetroffen zwakheden, malware en virussen zal worden omgegaan. Zullen deze worden gemeld aan de getroffen organisaties en burgers? Is het een bevoegdheid die alleen wordt ingezet vanuit een defensief perspectief of zal de hiermee verkregen kennis ook gebruikt worden voor offensieve activiteiten?

3. Hackbevoegdheid

Sinds de invoering van de Wiv2002 is het de inlichtingen- en veiligheidsdiensten toegestaan om geautomatiseerde werken (op afstand) te betreden; de hackbevoegdheid. De minister stelt voor om de hackbevoegdheid uit te breiden naar het hacken van derden. Het wordt echter niet duidelijk waarom die uitbreiding noodzakelijk is. Daarnaast wordt er ten onrechte geen aandacht besteedt aan een aantal cruciale vraagstukken over de aankoop en het gebruik van zwakheden en de aankoop en het gebruik van malware.

3.1 Hacken maakt de maatschappij onveiliger

De Memorie van Toelichting moet stilstaan bij de risico´s van het hacken maar doet dat ten onrechte niet.

Bij de invoering van de hackbevoegdheid is er in het parlementaire debat betrekkelijk weinig aandacht geweest voor de hackbevoegdheid[20] De motivering voor de noodzaak van de bevoegdheid was met ¨het is gewenst dat zij – indien daartoe de noodzaak bestaat – ook computervredebreuk als hier bedoeld kunnen plegen¨[21] niet afdoende onderbouwd. In 1998 was wellicht niet duidelijk wat de reikwijdte van deze bevoegdheid was en hoe het verstrekkende karakter van de inbreuk die door het hacken van apparaten van burgers zou zijn. In de afgelopen 13 jaar is op dat gebied veel veranderd.

De manier waarop burgers, bedrijven en overheden met elkaar communiceren is vrijwel volledig gedigitaliseerd. Datzelfde geldt ook voor de opslag van die communicatie en voor de opslag van documenten, foto´s, filmpjes en andere gegevens die in meer of mindere mate een weerslag vormen van ons leven. Die informatie kunnen inzien, verwijderen, kopiëren of manipuleren levert een grote inbreuk op de grondrechten van de burger. Het hacken van een geautomatiseerd werk is nu een grotere inbreuk dan in 1998 voorzien werd. Het is goed dat de waarborgen voor deze bevoegdheid worden verstevigd.[22]

In essentie maakt het gebruik van zwakheden in software om een geautomatiseerd werk te hacken iedereen onveiliger die gebruik maakt van dezelfde software. De onveiligheid in de software van het target geldt immers niet alleen voor het target, maar ook voor alle andere gebruikers van die software. Ook criminelen of diensten van andere overheden maken gebruik van die zwakheden. Uiteindelijk is er dus in technisch opzicht niet zoveel verschil tussen de crimineel die een burger hackt en begluurt en de overheid die datzelfde doet bij een target. Dat betekent ook dat als de Nederlandse geheime diensten denkt dat ze de enige zijn die beschikking hebben over een zwakheid in software, dat niet per se waar is.[23]

3.2. Nederland moet verantwoord omgaan met kwetsbaarheden

Wanneer de overheid van een zwakheid weet en daarvan profiteert maar dat niet communiceert naar de burger en het bedrijfsleven blijven zij kwetsbaar. Daarmee draagt de overheid bij aan de onveiligheid van haar burgers. Die verantwoordelijkheid moet zwaar wegen op de schouders van de overheid. Dat blijkt niet uit de Memorie van Toelichting. Dat is opmerkelijk, want in reactie op diverse rapporten heeft de regering wel blijk gegeven van het feit dat internet niet alleen een vitale rol heeft, maar ook beschermd dient te worden.[24]

20 Kamerstukken 1997/1998 25 877, nr 3, p. 39 en 40.
21 Kamerstukken 1997/1998 25 877, nr 3, p. 39.
22 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 53 en 54.
23 Zie bijvoorbeeld: http://www.wired.com/2014/09/eppb-icloud/.
24 Zie bijvoorbeeld toe toespraak van minister Koenders bij de ontvangst van het WRR rapport ´De

De toelichting moet dan ook de vraag beantwoorden hoe de overheid zijn rol gaat nemen bij het verbeteren van de (digitale) veiligheid van hun burger. Van burgers en het bedrijfsleven wordt verwacht dat zij hun best doen om hun systemen zo veilig mogelijk houden. Publiekscampagne na publiekscampagne is erop gericht de burger ´digibewust´ te maken en ervoor te zorgen dat zij niet in de val van criminelen stappen. Meldplichten moeten – al dan niet met sancties – garanderen dat bedrijven ervoor zorgen dat hun systemen zo veilig mogelijk zijn. De overheid moet die veiligheid niet verzwakken, maar juist versterken.

Het is niet de vraag óf, maar wanneer geconstateerde zwakheden gemeld moeten worden. Dat melden zou plaats kunnen vinden via het NCSC.

Uit de toelichting wordt eveneens niet duidelijk op welke wijze de geheime diensten kennis krijgen van zwakheden in software. Dat kan via de inzet van eigen bevoegdheden. onder meer bij de via artikel 30 lid a of 34 lid 1 onder a in te zetten bevoegdheid. Deze kennis zou ook – bijvoorbeeld middels het NCSC – kunnen worden verkregen dankzij door bedrijfsleven en overheid gedeelde zwakheden. Dat kan ook via andere geheime diensten of door aankoop van kennis over die zwakheden.

Er moet een regeling komen voor het verkrijgen, het gebruiken en het delen van zwakheden door de inlichtingen- en veiligheidsdiensten. De Memorie van Toelichting moet hier richtlijnen voor geven. Daarbij moet rekening worden gehouden met het zwaarwegende maatschappelijke belang om zwakheden openbaar te maken en met de risico´s van het aankopen van exploits en malware, het gebruik en de inzet daarvan (zie hieronder).

3.3 Risico´s mensenrechten bij aankoop exploits en malware

Als de Nederlandse overheid zaken doet met bedrijven die handelen in zwakheden en exploits, dan draagt zij (vaak) bij aan een markt waarbij de handelaren profiteren van de onveiligheid van de burger. Het is onwenselijk dat de Nederlandse overheid zich inlaat op zulke markten.

3.3.1 Inkopen kan mensenrechten in het buitenland ondermijnen

Sommige aanbieders van malware en exploits doen zaken met overheden en criminelen die het niet zo nauw nemen met grondrechten. Als de overheid met zulke aanbieders zaken zou doet, dan draagt zij bij aan het voortbestaan van zulke bedrijven, legitimeert zij het handelen van deze bedrijven, maar nog belangrijker: ze draagt indirect bij aan het mogelijk maken van het schenden van burgerrechten in andere landen.

publieke kern van het internet´: https://www.rijksoverheid.nl/documenten/toespraken/2015/03/30/wrr-rapport-de-publieke-kern-van-het-internet.

3.3.2 Gebruik malware moet worden ingekaderd

Tot slot moet er in de Memorie van Toelichting ingegaan worden op het gebruik, en de controleerbaarheid van het gebruik van eerder genoemde malware. Daarbij moeten de volgende vragen worden meegenomen: Kan de Nederlandse overheid de broncode inzien van de gebruikte malware? Kan de Nederlandse overheid garanderen dat het bedrijf dat de malware levert op geen enkele wijze inzicht kan krijgen in de door de geheime dienst verkregen informatie?

3.4 Hackbevoegdheid krijgt een steeds meer ongericht karakter

De Toelichting zou ook aandacht moeten besteden aan de reikwijdte van de hackbevoegdheid. Artikel 24 (oud) en artikel 30 (nieuw), noch de respectievelijke toelichtingen vereisen dat het geautomatiseerd werk in het bezit is van de verdachte. Dat maakt het mogelijk om een ruimere kring van geautomatiseerde werken te hacken, wat in de praktijk ook gebeurd is. Blijkens onthullingen van Edward Snowden en rapporten van de CTIVD is de hackbevoegdheid van de geheime diensten allang niet meer gericht op individuele targets. Zo worden servers overgenomen die niet alleen in gebruik zijn bij het target en webfora zijn (onterecht) overgenomen die meer gebruikers hadden dan alleen het target.[25]

In 2002 was het niet voorzienbaar dat de geheime diensten de hackbevoegdheid ruimer zouden inzetten dan alleen op het geautomatiseerde werk van het target. De CTIVD heeft deze ruimere reikwijdte in zijn algemeenheid weliswaar geaccordeerd, maar dat neemt niet weg dat ook de Memorie van Toelichting op de wenselijkheid en reikwijdte hiervan in zou moeten gaan.

3.4.1 Reikwijdte geautomatiseerd werk wordt steeds uitgebreider

Het begrip geautomatiseerd werk is erg breed. In het wetsvoorstel computercriminaliteit III wordt voorgesteld om het begrip nog verder uit te breiden. Met het oog op technologische ontwikkelingen is het in ieder geval aannemelijk dat er meer en meer apparaten onder het begrip geautomatiseerd werk zullen vallen, zelfs als de uitbreiding van het begrip niet door zou gaan.

Met the internet of things wordt het aantal apparaten dat de geheime diensten zou mogen hacken steeds groter. De hoeveelheid informatie die daarmee wordt verzameld wordt ook steeds groter. Dat betekent dat het bereik en de reikwijdte van de hackbevoegdheid steeds groter wordt en de inbreuk op grondrechten steeds indringender. In de toelichting wordt op deze ontwikkelingen volstrekt niet ingegaan.

Het feit dat je door te hacken steeds dichter op, of zelfs ín de mens kunt kijken is eveneens een ontwikkeling waarbij de Toelichting ten onrechte niet stilstaat. De toelichting zou in ieder geval aan moeten geven óf en zo ja waar er voor de inlichtingen- en veiligheidsdiensten grenzen zijn voor het hacken van

25 Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (CTIVD nr 38), 2014, p. 23.

geautomatiseerde werken.

3.5 Uitbreiding hackbevoegdheid naar derde zeer riskant

De minister stelt in artikel 30 lid b voor de geheime diensten toe te staan om ´derden´ te hacken. De mogelijkheid om een derde te kunnen hacken is een uitbreiding die zonder precedent is in Nederlandse wetgeving. Uit niets blijkt uit de Toelichting dat er rekening is gehouden met de consequenties van het hacken van derden, terwijl die groot kunnen zijn. De Toelichting moet hier aandacht aan besteden.

Bij het hacken van een derde, puur om het target te bereiken, wordt een actieve handeling verricht die een grote inbreuk oplevert voor de derde dan wanneer passief en noodgedwongen communicatie van de derde wordt onderschept.

Die handeling heeft namelijk tot gevolg dat niet alleen kortstondig de communicatie opgevangen kan worden tussen het target en de derde, maar dat de geheime diensten volledig toegang krijgen tot het systeem van de derde. Daarbij kunnen alle gegevens bekeken worden, kan alle communicatie bekeken worden en kan het systeem gemanipuleerd worden. Dit levert een grote inbreuk op de grondrechten van de derde op en dat alles zonder dat hij ergens van verdacht wordt. Het enige dat hij misdaan heeft is nodig zijn om het target te bereiken.

3.5.1 Categorie derden is te onbegrensd

De Memorie van Toelichting en de wet zijn onduidelijk over de definitie van een ´derde´. Om te voorkomen dat in de toekomst de ´derde´ door inlichtingen- en veiligheidsdiensten steeds uitgebreider wordt opgevat, dient de Toelichting een scherpe definitie van de ´ derde´ te bevatten.

Er wordt in de Memorie van Toelichting gesproken over het kunnen benutten van zwakheden bij ´technische randgebruikers´. Het blijft in het midden om welke derde(n) het dan zou kunnen gaan. Er wordt slechts één voorbeeld gegeven in de Toelichting; namelijk die van de medehuurder van een server. Dat laat zien dat in zulke gevallen de enkele omstandigheid dat er een technische relatie is tussen target en onverdachte burger voldoende is om die onverdachte burger te hacken. Ze hoeven elkaar dus niet te kennen.

Het hacken van derden is niet beperkt tot de mede-huurders van een bepaalde server. De wetgever spreekt over ¨dergelijke situaties¨[26]. Dat roept de vraag op tot in hoeverre de derde slechts een technische randgebruiker dient te zijn en tot hoever het zijn van een technisch randgebruiker strekt.

Er zijn immers ook andere relaties die de derde relevant maken om gehackt te

26 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 53.

worden. Een familielid, verre vriend of buur die minder goed beveiligd is, zou ook gehackt kunnen worden om vervolgens vanuit diens geautomatiseerde werk het geautomatiseerde werk van de target te hacken, door bijvoorbeeld geïnfecteerde e-mails. Het zou ook de werkgever van het bedrijf van het target kunnen zijn, die een geïnfecteerde mail stuurt en vervolgens het target besmet, of een bedrijf van wiens diensten het target gebruikt maakt en vervolgens besmet raakt. Ook een medewerker wiens beveiliging minder goed op orde is en via wiens geautomatiseerde werk – al dan niet via de servers van het bedrijf – het target gehackt wordt zou een technische randgebruiker kunnen zijn.

3.5.2 Hacken voor derde niet voorzienbaar en niet proportioneel

De mogelijkheid om een derde te hacken maakt het ook voor burgers, bedrijven en organisaties nauwelijks voorzienbaar dat zij gehackt zouden kunnen worden door de inlichtingen- en veiligheidsdiensten. Zij hebben immers niets gedaan, anders dan hun *operational security* niet voldoende op orde hebben.

Via een derde een target hacken levert dus eigenlijk alleen maar extra inbreuken op. Niet alleen de inbreuk op de grondrechten van het target, maar ook op de grondrechten van de derde. Tegenover die extra inbreuken staan niet méér waarborgen ten opzichte van het hacken van ´alleen´ het target. Dat moet door de regering worden aangepast.

Het blijkt ook niet uit de Toelichting of er andere methoden ingezet kunnen worden die hetzelfde resultaat zouden kunnen bereiken. Zelfs als dat een grotere inbreuk op de grondrechten van het target zou opleveren, dan betekent dat in ieder geval dat er geen inbreuk op de – onverdachte – derde plaatsvindt. Een gerichtere inbreuk is over het algemeen te prefereren boven een meer ongerichte inbreuk.

Uit de Toelichting blijkt niet dat er is nagedacht over de consequenties en de mensenrechtelijke aspecten van de uitbreiding. De Toelichting noemt alleen dat het ¨in het belang van de bescherming van de nationale veiligheid noodzakelijk¨[27] kan zijn derden te hacken, omdat targets over het algemeen te veiligheidsbewust zijn om zich te laten hacken.

Dat is een argumentatie waarbij het doel het middel lijkt te heiligen. Maar omdat iets het makkelijker maakt betekent dat nog niet dat het opweegt tegen de inbreuk die wordt veroorzaakt.

Ook veel andere vragen blijven onbeantwoord: Op welk punt gaat de derde genotificeerd worden dat zijn geautomatiseerde werk is betreden? Als het een bedrijf of organisatie is die gehackt is om zo het target om de tuin te leiden, wordt die dan ook genotificeerd? Is het überhaupt mogelijk om het

27 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 53.

geautomatiseerde werk weer in oude de staat achter te laten?

3.5.3 Hacken derde levert grote risico´s op voor derde

Ook zijn er risico´s voor de gehackte derde waaraan de Memorie van Toelichting voorbij gaat.

Ten eerste het risico van (strafrechtelijke) aansprakelijkheid. Stel dat de derde en het target een server delen. Vervolgens wordt de derde gehackt door de AIVD en de AIVD probeert vervolgens het target te hacken. Het target, een (buitenlandse) overheidsdienst of het bedrijf dat de server beheert kan merken dat er gehackt is of een poging daartoe wordt ondernomen. Op dat moment lijkt de derde zich schuldig te maken aan (een poging tot) computervredebreuk.

Stel dat het bedrijf aangifte doet van (poging tot) computervredebreuk. Hoe wordt de derde dan beschermd? Zal de AIVD in zulke gevallen de derde beschermen tegen (strafrechtelijke) procedures en eventuele aansprakelijkheid?

Daarnaast is er nog ander risico: Stel dat het target zelf geen aangifte doet maar besluit tot meer rigoureuze actie, door bijvoorbeeld het hacken van de derde, hoe wordt de derde dan beschermd? Hij wordt op dat moment blootgesteld aan risico´s die hij kon, noch hoefde te voorzien. Het is daarbij lang niet zeker dat de geheime diensten op het moment dat het target doorkrijgt dat hij gehackt is via een derde beiden nog in hun vizier hebben. Ook dan zijn er (grote) risico´s voor de derde.

Bits of Freedom is van mening dat zolang de Nederlandse regering dergelijke risico´s niet ondervangt de bevoegdheid ook niet zou moeten worden ingevoerd.

4. Beperk de reikwijdte van het mogen verzoeken om gegevens

Het is zorgelijk dat een bevoegdheid die eerder al door de Eerste Kamer als onnodig en een te zware inbreuk op de privacy werd bestempeld nu opnieuw wordt voorgesteld, maar nu met minder zware waarborgen, in de vorm van artikel 22 lid 3. De bevoegdheid moet daarom – opnieuw – moet worden ingetrokken.

4.1. Diensten moeten vorderen, niet vragen

Voor opsporingsdiensten geldt het adagium dat zij niet mogen vragen, maar moeten vorderen. Er is geen reden om dat niet ook voor inlichtingen- en veiligheidsdiensten te laten gelden. Dat is belangrijk om twee redenen: ten eerste zijn er waarborgen bij vorderingen die er niet bij verzoeken zijn. Dat zorgt ervoor dat verzoeken niet te snel of ten onrechte worden gedaan, maar dat er een extra toets plaatsvindt of er een noodzaak is om bepaalde informatie te

verkrijgen. Ten tweede zorgt een vordering voor duidelijkheid voor de ontvangende partij: het voorkomt dat de verzochte een druk voelt om te voldoen aan een verzoek zonder dat daar een verplichting voor is.

4.2 Schrap artikel 22 lid 3

Bovenstaande geldt nog sterker bij verzoeken als bedoeld in artikel 22 lid 3, door het ruime karakter van het verzoek. Artikel 22 lid 3 zou de inlichtingen- en veiligheidsdiensten ¨rechtstreekse geautomatiseerde toegang aan de dienst tot de desbetreffende gegevens dan wel door het verstrekken van geautomatiseerde gegevensbestanden¨ moeten geven. Dat zou¨online en real time¨ moeten kunnen gebeuren.[28] Zonder een onderbouwing van de noodzaak en nadere inkadering kan deze bevoegdheid niet worden ingevoerd.

De noodzaak is onvoldoende onderbouwd, daarnaast wordt de reikwijdte in de Toelichting niet toegelicht of beperkt. En dat terwijl de potentiële inbreuk die deze bevoegdheid oplevert enorm is. De Memorie van Toelichting noemt alleen de CT infobox, maar de bevoegdheid is dermate ruim opgesteld dat toegang tot álle verzamelde gegevens, overal, mogelijk is. Het verzoek kan gericht worden tot eenieder, van een burger tot de Belastingdienst tot grote communicatieaanbieders, van de lokale voetbalclub tot de grootste bank en van de snackbar tot de NS.

De grootste beperking zou dan in het feit zitten dat het hier gaat om een verzoek, niet een verplichting. Maar het feit dat het een verzoek is, maakt de inbreuk die het overhandigen van of toegang geven tot grote hoeveelheden gegevens oplevert niet kleiner.

De inzet van een dergelijk zware bevoegdheid moet niet afhankelijk zijn van de mate van publiek-private samenwerking. Er is de afgelopen jaren veel kritiek geweest op private aanbieders van (tele)communicatie die, al dan niet vrijwillig, op grote schaal hebben meegewerkt met de Amerikaanse NSA. Deze voorgestelde ´algemene´ bevoegdheid zou dezelfde problematische situatie op kunnen leveren.

Tot slot is het toezicht op een dergelijke vorm van samenwerking lastig omdat de normale procedures voor de inzet van bijzondere bevoegdheden niet toegepast worden.

5. Versterk het toezicht van de CTIVD

Het toezicht op de inlichtingen- en veiligheidsdiensten is een cruciaal onderdeel van goed functionerende regelgeving voor de inlichtingen- en veiligheidsdiensten. De diensten moeten zich immers verantwoorden aan de

28 Concept-memorie van Toelichting bij het conceptwetsvoorstel, p. 27.

maatschappij. Zonder mechanismen om het naleven van de regels te waarborgen kunnen regels lege hulzen blijken. Daar is een aantal instrumenten essentieel bij: zinvolle transparantie naar de burger, bedrijfsleven en parlementsleden en volwaardig, onafhankelijk, bindend toezicht.

5.1 Zinvolle transparantie

Transparantie is een belangrijke voorwaarde voor controle op overheidshandelen en een middel om onrechtmatig overheidshandelen te voorkomen. Daarom moet zoveel mogelijk informatie over wat de overheid doet openbaar zijn. Voor de inlichtingen- en veiligheidsdiensten geldt eveneens dat transparantie het uitgangspunt zou moeten zijn. Soms zijn er gevallen waarin terecht informatie niet (direct) publiek beschikbaar wordt. Maar er zijn ook gevallen zijn waarin ten onrechte wordt gekozen voor geheimhouding, zoals bij de publicatie van tapstatistieken. Dat ondergraaft de mogelijkheid om publiekelijk overheidshandelen te controleren en ondermijnt het vertrouwen van het publiek in een rechtmatig handelen door dat overheidsorgaan.[29]

Om te achterhalen of terecht of onterecht informatie achter is gehouden, is toetsing door een derde essentieel. De ervaring in de praktijk met de openbaarheid van de inlichtingen- en veiligheidsdiensten heeft Bits of Freedom geleerd dat onterecht informatie geheim gehouden wordt. Ook de CTIVD komt tot een gelijkluidende conclusie. Zij waarschuwen in het jaarverslag 2014-2015 voor een ¨geheimhoudingscultuur¨ bij de AIVD. Dat is zorgelijk omdat openbaarheid juist controle op de diensten en vertrouwen in het rechtmatige handelen van de diensten ten goede komt.

5.1.1 Schrap in artikel 101 lid 3 de verwijzing naar artikel 12 lid 3.

Wanneer de rechter of de CTIVD van oordeel is dat informatie openbaar mag worden, dan moeten zowel de inlichtingen- en veiligheidsdiensten als de verantwoordelijke ministers zich daar naar voegen. Het past hen dan niet om geheimhouding te forceren. De conclusie van de toezichthouder dat dergelijk handelen geen schoonheidsprijs verdient[30] is dan ook een understatement.

De CTIVD is als toezichthouder uitstekend geschikt om te beoordelen of informatie openbaar gemaakt kan worden. Om te voorkomen dat informatie die volgens de CTIVD wel degelijk openbaar gemaakt moet worden toch geheim blijft, is het nodig om in artikel 101 lid 3 de verwijzing naar artikel 12, derde lid te schrappen.

In het eerste lid van artikel 101 dient de CTIVD al een afweging te maken of gegevens onder artikel 12 , lid 3 vallen. Op het moment dat zij besluiten dat dat gegevens daar niet onder vallen en openbaar gemaakt kunnen worden, dan

29 Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Commissie Dessens, p. 133.
30 CTIVD-jaarverslag 2014/2015, p. 32.

wordt de minister in lid 2 in de mogelijkheid gesteld om te reageren op het rapport. Als de minister van mening is dat informatie onder artikel 12 lid 3 valt, dan kan de CTIVD een heroverweging toepassen. Vanuit de rol die de CTIVD heeft is het onacceptabel dat de minister vervolgens het oordeel van de CTIVD zelfstandig aan kan passen.

5.2 Bindende toetsing

Toetsing op de uitoefening van diensten moet voorafgaand aan de inzet van bevoegdheden plaatsvinden en die toetsing moet bindend zijn. Het is goed dat de regering het toezicht op de inlichtingen- en veiligheidsdiensten wil versterken. Maar de voorgestelde wijzigingen dragen onvoldoende bij aan die doelstellingen.

5.2.1 Voorkom onrechtmatige inzet

Voorkomen is beter dan genezen. Bindend – vooraf – toetsen levert een bijdrage aan het voorkomen dat ten onrechte een inbreuk op grondrechten plaatsvindt. Een stelsel waarbij een onafhankelijke toetsing plaatsvindt voorafgaand aan de inzet van bevoegdheden zorgt ervoor dat de kwaliteit van de verzoeken toeneemt, de kwaliteit van de genomen beslissing groeit en daardoor de grondrechten van de burger beter beschermd worden.

Anders dan de Commissie Dessens, vindt de regering dat voor de uitoefening van bevoegdheden geen onafhankelijk bindend toezicht dient te zijn, maar een stelsel met een heroverwegingsplicht voor de minister. Een heroverwegingsplicht zou de minister de mogelijkheid geven om de beslissing van de toezichthouder naast zich neer te leggen. Daarmee wordt een onrechtmatige beslissing doorgezet, waardoor ten onrechte een inbreuk op grondrechten wordt gemaakt.

Het is voor het individu belangrijk dat een dergelijk toetsingsmoment vooraf plaatsvindt. Het is voor het individu namelijk heel erg lastig, zo niet onmogelijk, om te achterhalen of er een inbreuk heeft plaatsgevonden. Pas na vijf jaar kan de burger achterhalen – hetzij door notificatie, hetzij door zelf een verzoek in te dienen – of een bevoegdheid jegens hem is ingezet. Als vervolgens een klachtprocedure wordt gestart kan het nog geruime tijd duren voor blijkt of een bevoegdheid (onterecht) is ingezet. Het is vervolgens lastig een onterechte inbreuk op grondrechten te repareren: de inbreuk heeft immers al plaatsgevonden.

Daarbij geldt dat een onafhankelijke toetsing – vooraf – geen unicum is: Over het openen van brieven moet bijvoorbeeld nu al de rechtbank Den Haag zich uitlaten. Een dergelijke constructie kan prima uitgebreid worden naar alle (zware) bevoegdheden van de inlichtingen- en veiligheidsdiensten. Ook in een aantal andere landen is sprake van onafhankelijke bindende toetsing.

5.2.2 Maak oordeel rechtmatigheid individuele inzet niet politiek

Als de minister het oordeel van de toezichthouder naast zich neer kan leggen, dan ontstaat het risico dat de (politieke) wenselijkheid het wint van rechtmatig inzetten van bevoegdheden. Het kan immers politiek opportuun zijn om daadkrachtiger te zijn dan noodzakelijk. Dat mag nooit een maatstaf zijn voor het inzetten van bevoegdheden.

Het is onwenselijk dat de uiteindelijke toetsing van rechtmatigheid van de inzet van specifieke bevoegdheden bij de CIVD komt te liggen. Door de CIVD het laatste woord te geven over de rechtmatigheid van specifieke bevoegdheden wordt die beslissing nodeloos politiek.

De CIVD moet het functioneren van de minister en van de inlichtingen- en veiligheidsdiensten beoordelen. Het wordt problematisch als de CIVD ook moet beoordelen of een specifieke bevoegdheid terecht of onterecht is ingezet. Daar is de CIVD niet voor gekwalificeerd en belangrijker nog: die toetsing moet bij onafhankelijke experts liggen, niet bij politici. Het is aan de politici om vervolgens consequenties te verbinden aan de bevindingen van de toezichthouder.

5.2.3 Gebrek aan publieke verantwoording

Het is belangrijk dat verantwoording over het functioneren van de minister en de inlichtingen- en veiligheidsdiensten zoveel mogelijk publiekelijk plaatsvindt. Toetsing bij het heroverwegingsstelsel zal niet publiekelijk plaatsvinden. In de 1.8-miljoen-metadata-affaire is duidelijk gebleken dat in de verantwoording van de minister naar de CIVD en naar het publieke debat in de Tweede Kamer grote problemen op kunnen treden over wat wel en wat niet publiekelijk besproken kan en mag worden. Daardoor werd het publieke debat ernstig beperkt.

Deze onwenselijke situatie zal bij de invoering van dit stelsel toenemen. Dat betekent dat als er naar het oordeel van de CIVD ten onrechte een bevoegdheid in is gezet, dit niet gedeeld of gecommuniceerd kan worden. Dat is op zich niet onbegrijpelijk, maar dat levert wel een probleem op als de CIVD een verregaande consequentie verbindt aan het onterecht handelen van de minister. Als de CIVD van mening zou zijn dat de minister moet opstappen, dan zou dat moeten gebeuren zonder dat er een fatsoenlijk en openbaar politiek gebat over gevoerd kan worden. Het enige dat immers in het openbaar gezegd kan worden is dat de minister moet opstappen omdat hij iets heeft gedaan of heeft toegestaan dat zó ernstig is dat hij niet langer aan kan blijven.

Ook bij de CIVD zal de rechtmatigheid van inzetten van bevoegdheden worden gekoppeld aan de wenselijkheid. De CIVD kan van mening kan zijn dat de inzet weliswaar onrechtmatig was, maar wel degelijk wenselijk. Ook in dit geval geldt

dat die ´wenselijkheid´ onvoldoende reden is om een bevoegdheid in te zetten. De CIVD kan ook besluiten dat de inzet zowel onrechtmatig als onwenselijk was, maar er geen consequenties aan verbinden omdat het ofwel niet serieus genoeg is voor het aftreden van de minister of niet opportuun is om de minister tot aftreden te dwingen. Dat is vanzelfsprekend een politiek oordeel, maar het moet niet tot onzuiverheid leiden in de besluitvorming of een inzet wel of niet onrechtmatig was.

5.2.4 Bindend toetsen maakt slagkracht niet kleiner

Het door de CTIVD afwijzen van inzet van bevoegdheden zal een uitzondering zijn. Onderzoek van de CTIVD laat structureel zien dat de diensten zich over het algemeen aan de wet houden en dat bevoegdheden rechtmatig zijn ingezet. Dat betekent eveneens dat de minister terecht tot de beslissing is gekomen om een bevoegdheid in te zetten. Ervan uitgaande dat diezelfde zorgvuldigheid in acht zal worden genomen in de toekomst, zal het overgrote deel van de beslissingen van de minister rechtmatig zijn. De minister hoeft zich dus weinig zorgen te maken over de slagkracht van de inlichtingen- en veiligheidsdiensten, maar er is hiermee wel een stok achter de deur om onrechtmatig genomen beslissingen te voorkomen.

6. Samenwerking met buitenlandse geheime diensten

In het wetsvoorstel wordt het stelsel voor internationale samenwerking herzien. Die herziening schiet op een aantal punten tekort. Er moet een beperking komen voor de bevoegdheden die namens een buitenlandse dienst door de inlichtingen- en veiligheidsdiensten kunnen worden ingezet. Daarnaast mogen ongeëvalueerde gegevens niet aan buitenlandse diensten worden overgedragen.

6.1 Beperk de namens buitenlandse diensten in te zetten bevoegdheden

Op grond van artikel 77 lid 4 kunnen de Nederlandse inlichtingen- en veiligheidsdiensten bevoegdheden inzetten voor buitenlandse diensten. Voor een goede internationale samenwerking en om te voorkomen dat buitenlandse diensten op eigen houtje actie in Nederland ondernemen is een dergelijke regeling belangrijk. Maar er moeten beperkingen zijn voor de bevoegdheden die de Nederlandse diensten in mag zetten voor buitenlandse diensten.

6.1.1 Voorkom inzet ongerichte bevoegdheden voor buitenlandse diensten

Een buitenlands verzoek voor de inzet van bevoegdheden moet voldoende specifiek zijn. Er moet een concrete aanleiding zijn voor het verzoek. Dan moet er ook sprake zijn van een inzet van gerichte bevoegdheden. Nederland moet eventuele ongerichte bevoegdheden waarmee gegevens van onverdachte burgers ongericht wordt onderschept dan ook niet inzetten voor buitenlandse diensten.

6.1.2 Alleen inzet bevoegdheden die door land zelf ingezet mogen worden

Nederland moet alleen bevoegdheden inzetten die de verzoekende dienst ook in mag zetten. Stel dat een ander land een bevoegdheid niet heeft en Nederland wel, dan zou Nederland die bevoegdheid voor dat land in kunnen zetten. Dat kan in potentie U-bochtconstructies opleveren waaraan Nederland geen medewerking zou moeten verlenen.

Andersom heeft Nederland het wel goed geregeld; artikel 78 vijfde lid verbiedt de Nederlands inlichtingen- en veiligheidsdiensten bevoegdheden in het buitenland in te zetten die in Nederland niet ingezet mogen worden. Er is geen reden om die regeling niet gelijk te trekken voor verzoeken van buitenlandse diensten.

6.2 Stop uitwisseling van ongeëvalueerde gegevens

Volgens de Memorie van Toelichting is het delen van gegevens essentieel voor de internationale samenwerking met buitenlandse diensten en voor de slagkracht van de Nederlandse inlichtingen- en veiligheidsdienst.

Maar dat wil niet zeggen dat Nederland zelf ongebreideld informatie moet verzamelen en overdragen, puur als wisselgeld zonder dat de consequenties van die overdracht kunnen worden overzien. Nederland heeft als leverende of ontvangende partij een verantwoordelijkheid naar haar burgers die in het huidige wetsvoorstel onvoldoende wordt belicht. Als Nederlands alleen geëvalueerde gegevens overdraagt is het veel duidelijker wat de wenselijkheid en noodzakelijkheid van de overdracht en het gebruik van die informatie is. Bij overdracht van ongeëvalueerde gegevens is daarnaast ook voor burgers niet voorzienbaar wat de consequentie van overdracht zullen zijn.

Bij het (internationaal) uitwisselen van gegevens staan mensenrechten onder druk, mede omdat het niet duidelijk is hoe die gegevens zijn verkregen of wat er met de geleverde gegevens gaat gebeuren. Deze rechten staan extra onder druk als het gaat om gegevens die ongericht zijn verzameld en ongeëvalueerd zijn, omdat er gegevens van onverdachte burgers tussen zitten die veel over hen prijsgeven.

Het is bijvoorbeeld niet ondenkbaar dat seksuele voorkeur kan worden gedestilleerd na analyse van verzamelde data. Als ongeëvalueerde gegevens waar dit uit gedestilleerd wordt gedeeld met een land waar homoseksuelen vervolgd worden dan kan dit grote problemen opleveren voor homoseksuelen.