6
Wet op de inlichtingen-en veiligheidsdiensten 20..

Aan de orde is de behandeling van:
- **het wetsvoorstel Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) (34588).**

De **voorzitter**:
De minister van Binnenlandse Zaken en Koninkrijksrelaties heb ik reeds welkom geheten in de Eerste Kamer. Ik heb eveneens in de Eerste Kamer welkom geheten de minister van Defensie. Zij heeft aangegeven dat zij in ieder geval tijdens de eerste termijn van de behandeling van dit wetsvoorstel in de Kamer aanwezig zal zijn.

De beraadslaging wordt geopend.

☐

De heer **Rombouts** (CDA):
Mevrouw de voorzitter. Het recht op veiligheid spreekt zo voor zich dat het niet in onze Grondwet staat. Veilig je kinderen op school achterlaten. Veilig met vrienden naar een festival gaan. Veilig kunnen bidden in de moskee. Veiligheid is een van de fundamenten van onze samenleving, die zo snel verandert. Hoe gaan we daarmee om, en hoever gaan we? Moet de AIVD (Algemene Inlichtingen- en Veiligheidsdienst) ieders WhatsApp-berichten kunnen lezen om eventuele aanslagen te voorkomen of gaan we juist alleen voor privacy en nemen we het risico van terreur voor lief? De CDA-fractie staat pal voor de veiligheid van alle Nederlanders, én voor de rechten van het individu. Zo heeft mijn fractie ook gekeken naar dit wetsvoorstel, dat gaat over de bevoegdheden en het toezicht op onze veiligheidsdiensten.

Allereerst de bevoegdheden. De Wet inlichtingen- en veiligheidsdiensten 2002 stamt uit het pre-iPhonetijdperk. Het zal niemand dus verbazen dat een herziening nodig is. Het is evident dat ook dataverkeer via de kabel nu met een specifieke onderzoeksopdracht mag worden onderzocht. Cruciale vragen zijn daarbij de volgende. Onder welke voorwaarden mag er afgetapt worden? Hoe wordt informatie geselecteerd? Hoelang blijven data bewaard? Wanneer mogen gegevens vernietigd worden? Op al deze vragen vindt mijn fractie dat het wetsvoorstel voldoet. Voordat er wordt afgetapt verleent de minister toestemming. Deze wordt daarbij gecontroleerd door de TIB (Toetsingscommissie Inzet Bevoegdheden). Het aftappen gaat volgens het "select while you collect"-principe, waardoor de minister verwacht dat tot 98% van de data in het begin van het proces wordt vernietigd.

Dat niet-vernietigde gegevens drie jaar bewaard worden, heeft met het oog op de bescherming van onze privacy tot grote kritiek geleid van de Raad van State, de Tweede Kamer en niet te vergeten de samenleving. Nog elk uur rollen de berichten op onze iPhones binnen. Mijn fractie heeft sympathie, begrip voor deze kritiek en ziet tegelijkertijd dat het voor effectieve historische data-analyses van de AIVD en de MIVD (Militaire Inlichtingen- en Veiligheidsdienst) essentieel is om de bewaartermijn niet te kort te maken. We staan hier voor een heus dilemma, een afweging van grote belangen. Hoe bestrijden we de georganiseerde criminaliteit, de ondermijning van onze rechtsstaat, en hoe voorkomen we terroristische aanslagen versus hoe beschermt de overheid de privacy van onschuldige burgers?

De bewaartermijn wordt in het wetsvoorstel begrensd. Niet-onderzochte gegevens worden na drie jaar verwijderd. Versleutelde gegevens mogen maximaal drie jaar bewaard worden om deze te ontsleutelen. Het geeft mijn fractie dan ook vertrouwen dat de minister verwacht dat minder dan 1 promille van de data aan het eind van het proces wordt bewaard. Door deze waarborgen is er voor de CDA-fractie een goede balans gevonden tussen effectiviteit en privacy, tussen het beschermen van de privacy van burgers en het beschermen van burgers tegen terroristische aanslagen.

Dan het stelsel van toezicht. Het bestaan van de veiligheidsdiensten staat niet ter discussie. Nederland beschikt over twee buitengewoon professionele en in het buitenland gerespecteerde organisaties. Het is wel zaak ook het toezicht mee te laten groeien met de uitbreiding van de bevoegdheden van de diensten. Het CDA kan zich vinden in het stelsel waarbij de TIB vooraf het besluit van de minister toetst en de CTIVD (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) tijdens en achteraf controleert. Mijn fractie hecht zeer aan de toezegging van de minister dat de ministeriële verantwoordelijkheid intact blijft. Zij zou van de minister hier vandaag nog wel een aanscherping van zijn schriftelijke antwoord willen horen. Immers, ziet mijn fractie het goed dat de TIB een hernieuwd verzoek van de minister om bijvoorbeeld af te mogen tappen, nog steeds kan afwijzen? Wat is in het geval van herhaalde afwijzing de ministeriële verantwoordelijkheid dan nog waard, versus het bindend advies?

De overige vragen die wij stelden naar aanleiding van de brief van de CTIVD over de vier drempels van toezicht zijn naar het oordeel van mijn fractie afdoende beantwoord. Wij kunnen ons vinden in de uitspraak van de minister dat de TIB en de CTIVD de expliciete taak hebben, de rechtseenheid te bevorderen. Daarnaast heeft de minister duidelijk uitgelegd dat er geen toezichthiaat is, omdat de CTIVD ook een onrechtmatigheidsoordeel over de toets van de TIB kan vellen. Ook de overgangstermijn van twee jaar voor de systematiek van het delen met buitenlandse diensten wordt ons inziens afdoende gerechtvaardigd. De toezichtdrempel dat relevantie te ruim gedefinieerd zou zijn, heeft de minister duidelijk kunnen weerleggen. Ook de keuze om de klachtenbehandeling niet bij de Nationale Ombudsman, maar bij een aparte afdeling van de CTIVD onder te brengen kan op de instemming van mijn fractie rekenen. Wel pleiten wij ervoor krachtige Chinese walls op de werkvloer te creëren, zodat de onpartijdigheid van de klachtbehandeling echt gegarandeerd wordt.

Het voorliggende wetsvoorstel is een complex stelsel, met op papier de juiste checks-and-balances. Omdat het stelsel niet alleen op papier moet werken, hecht het CDA veel waarde aan de evaluatie die binnen twee jaar na de inwerkingtreding van de wet zal plaatsvinden. Wij zijn dan ook blij met de toezegging van de minister om in de evaluatie het onderwerp "tijdig en correct vernietigen van data" toe te voegen en dit te laten checken door een onafhankelijke auditor.

Voor ons is het belangrijk dat er een goede balans is tussen de effectiviteit van de diensten en het toezicht op hun handelen. Deze balans blijkt naar het oordeel van mijn fractie in het wetsvoorstel gevonden. Resteert dus voor de CDA-fractie nog het punt van de ministeriële verantwoordelijkheid. Wij zien uit naar het antwoord van de bewindslieden in dezen.

De heer **Van Kappen** (VVD):
Voorzitter. Al in december 2013 constateerde de commissie-Dessens dat de huidige Wet op de Inlichtingen- en Veiligheidsdiensten, de Wiv 2002, verouderd was en hoognodig moest worden aangepast. Immers, de Wiv 2002 is eind jaren negentig opgesteld en de wetgever heeft toen niet voorzien wat de impact van de huidige technologische en maatschappelijke ontwikkelingen zou zijn. Een goed voorbeeld van de ongekende vlucht van de techniek is het feit dat er in 2002 slechts 600 miljoen internetgebruikers waren. Momenteel zijn dat er 3,2 miljard. Eind jaren negentig ging bovendien het grootste deel van de datastromen nog via de ether, inmiddels gaat echter 90% van alle datastromen via kabelnetwerken.

Op grond van de huidige wet mogen de inlichtingen- en veiligheidsdiensten gerichte interceptie uitvoeren van data die door de ether gaan, alsmede van data die via de kabel worden verzonden. Echter, ongerichte interceptie is op grond van de huidige wet alleen toegestaan van data die door de ether gaan. De diensten hebben dus op dit moment geen bevoegdheid om ongericht kabelgebonden datastromen te onderscheppen en te analyseren. Hierbij merk ik op dat de term "ongerichte interceptie" misleidend is, omdat ook ongerichte interceptie wel degelijk gericht is op specifieke datastromen die moeten passen binnen de onderzoeksopdracht. Vandaar dat er in het voorliggende wetsvoorstel wordt gesproken over onderzoekgerichte interceptie.

Gezien het feit dat 90% van alle data over de kabel wordt verstuurd, zijn onze veiligheidsdiensten dus grotendeels blind en doof geraakt. Immers, bestaande, maar niet gekende communicatie, van bekende maar zeker ook van onbekende "targets", blijft verborgen voor de diensten. In deze turbulente tijden is het onverantwoord dat onze diensten op de tast hun werk moeten doen. De huidige technologie stelt immers zowel staten als niet-statelijke actoren in staat om cyberaanvallen uit te voeren op onze hightechbedrijven, vitale infrastructuur en vitale overheidssectoren. Dat gebeurt momenteel op grote schaal. De massale cyberaanvallen op zondag 14 mei, waarbij 140 landen werden getroffen, en de cyberaanval op 27 juni hebben ons weer eens extra met onze neus op de feiten gedrukt. Ook de afschuwelijke aanslagen in Brussel, Parijs, Manchester, Londen et cetera liggen nog vers in ons geheugen.

De vervanging van de Wiv 2002 is dus hoognodig. Het voorliggende wetsvoorstel is daartoe bedoeld. Het wetsvoorstel is gezien de razendsnelle ontwikkeling van de techniek terecht techniekonafhankelijk geformuleerd. Onze buurlanden, waarmee onze diensten intensief samenwerken, hebben om dezelfde redenen eveneens techniekonafhankelijke wetgeving voor hun veiligheidsdiensten in werking laten treden. Om zeker te stellen dat de inzet van bevoegdheden te allen tijde rechtmatig plaatsvindt, zijn er stevige waarborgen opgenomen in de wet om onze grondrechten, waaronder het recht op bescherming van de persoonlijke levenssfeer, te waarborgen. Het toezicht op de diensten is dan ook verzwaard.

Hoewel de noodzaak om de Wiv te vernieuwen breed wordt gedragen, is en blijft het vinden van de juiste balans tussen enerzijds de verantwoordelijkheid van de regering om in deze turbulente tijden de veiligheid van de Staat en dus de veiligheid van de staatsburgers te garanderen, en anderzijds de verantwoordelijkheid van de regering om de persoonlijke levenssfeer van diezelfde staatsburgers te beschermen, een delicate zaak. Die taak vereist grote zorgvuldigheid. De regering is dan ook bij de totstandkoming van dit wetsvoorstel zeker niet over één nacht ijs gegaan. Na een uitgebreide internetconsultatie, nadat vervolgens de regering, de Raad van State en de Tweede Kamer hun werk hebben gedaan en na de beantwoording van de door deze Kamer tijdens het voorbereidend onderzoek gestelde vragen, is er meer dan genoeg informatie om een oordeel over dit wetsvoorstel te vellen. Dat neemt niet weg dat er nog een aantal aspecten zijn die voor mijn fractie onvoldoende duidelijk zijn of waar wij vraagtekens bij zetten.

Wat bij ons blijft schuren, is het feit dat het oordeel van de Toetsingscommissie Inzet Bevoegdheden, afgekort de TIB, bindend is voor zowel de minister als de CTIVD en er in feite geen beroep mogelijk is tegen een beslissing van de TIB om een bevoegdheid al of niet in te zetten. Hoe je het ook draait of keert, dit is een inbreuk op de ministeriële verantwoordelijkheid zoals we die in Nederland kennen. Het is immers de minister die verantwoording moet afleggen aan het parlement en niet de TIB. De leden van de TIB zijn immers niet gekozen maar benoemd.

De vraag rijst bij ons of deze inperking van de ministeriële verantwoordelijkheid niet in strijd is met de Grondwet. Het argument van de minister dat dit niet zo is omdat de minister immers de bevoegdheid heeft en houdt om met een nieuw besluit te komen in het geval dat de TIB de inzet van een bevoegdheid niet goedkeurt, vinden wij wat mager. In het geval van een negatief oordeel van de TIB zal in negen van de tien gevallen een aangepaste formulering van het verzoek om een bevoegdheid in te zetten, zodat de TIB wel akkoord kan gaan, een oplossing bieden; dat zien wij ook wel. Maar we moeten, zeker in deze Kamer, ook de mogelijkheid onder ogen zien dat de minister het fundamenteel oneens is en blijft met de TIB. Wat gebeurt er dan? De TIB is immers geen rechterlijke instantie. Dit is voor ons de kern van onze onvrede met de TIB in de voorgestelde vorm: een niet democratisch gekozen orgaan dat beslissingen neemt waartegen geen beroep mogelijk is.

Er leven bij ons echter ook nog veel andere vragen ten aanzien van het nut, de noodzaak en de werkwijze van de TIB. De TIB wordt volgens het wetsvoorstel voorzien van de noodzakelijke informatie om een oordeel te vellen, maar heeft geen toegang tot de systemen van de diensten en geen kennis en zicht op de uitvoeringspraktijk. Toch is het oordeel van de TIB bindend, ook voor de CTIVD. Wat gebeurt er als de CTIVD bijvoorbeeld achteraf tot de conclusie komt dat de onderbouwing van het besluit om een bevoegdheid in te zetten onvoldoende was? Of is het zo dat de CTIVD een dergelijk oordeel niet mag vellen? Als de CTIVD dat wel mag, wat gebeurt er dan? Wordt alle verzamelde informatie dan vernietigd?

Het eeuwenoude probleem — wie zal de wachters bewaken? — speelt hier in onverhulde vorm: wie controleert de TIB?

Bijkomende vragen zijn: welke waarborgen zijn er dat de leden van de TIB het inlichtingenwerk echt begrijpen? Hoe worden zij geselecteerd? Vormt de bureaucratie die de invoering van de TIB meebrengt niet een extra remmende factor bij het inlichtingenwerk, waardoor de diensten worden belemmerd om adequaat te reageren op de ontwikkelingen in deze tijd waarin de enige constante factor lijkt te zijn dat alles constant en in hoog tempo verandert?

Voor alle duidelijkheid: wij zijn niet tegen een toetsing vooraf, maar ondanks de uitgebreide reactie van de minister op onze schriftelijke vragen, is er wat ons betreft nog veel onduidelijk ten aanzien van de TIB. Maar goed, het heeft geen zin om tot een herhaling van zetten te komen. The proof of the pudding is immers in the eating. Het is naar ons oordeel dan ook beter om te bezien of en hoe de TIB in de praktijk functioneert. Wij vragen de minister dan ook om ons toe te zeggen dat het functioneren van de TIB, inclusief de constitutionele constructie, na twee jaar grondig wordt geëvalueerd. Misschien is het een idee om de evaluatie van de TIB te koppelen aan de evaluatie van de bewaartermijn van metagegevens, die door de minister, naar aanleiding van de motie-Recourt in de Tweede Kamer (34588, nr. 56), reeds is toegezegd.

Het woord "bewaartermijn" is gevallen. Ook daar hebben wij nog wel een opmerking en een vraag over. Voor gegevens die zijn verzameld door uitoefening van de bevoegdheid van onderzoeksopdrachtgericht aftappen, geldt een bewaartermijn van hoogstens drie jaren na verwerving of het ongedaan maken van de versleuteling. Gegevens die niet op hun relevantie zijn doorzocht, worden na afloop van deze termijn terstond vernietigd (artikel 48, lid 5).

Sommigen zijn van mening dat deze periode, uit het oogpunt van bescherming van de persoonlijke levenssfeer en verantwoorde databeperking, te lang is. Anderen zijn juist van mening dat deze periode te kort is, omdat het opsporen en volgen van slapende cellen en complexe ondergrondse terroristische netwerken door de AIVD zich vaak uitstrekt over tientallen jaren en omdat militaire operaties in conflictgebieden veelal langer duren dan drie jaar.

De heer **Köhler** (SP):
Kan de heer Van Kappen mij zeggen wie die "anderen" zijn? Het standpunt dat die bewaartermijn met drie jaar nog te kort is, heb ik bij de vele insprekers niet gehoord. Of is die "andere" misschien zijn eigen fractie?

De heer **Van Kappen** (VVD):
Ik denk dat u met andere insprekers te maken hebt gehad dan ik.

De heer **Köhler** (SP):
Dat zou kunnen als bepaalde insprekers zich alleen tot u wenden. Onder de insprekers die zich tot de hele Kamer hebben gewend, was er geen enkele die de bewaartermijn zou willen oprekken.

De heer **Van Kappen** (VVD):
Dat is mij ook opgevallen. Het is mij ook opgevallen dat er een soort internetcampagne is gevoerd, met een stortvloed van berichten gericht aan alle leden die het woord over de Wiv voeren. Dat is mij ook opgevallen en daar waren weinig reacties bij die om een langere termijn vroegen. Maar ík vraag erom.

Ik pak de draad weer op. De periode van drie jaar is naar de mening van mijn fractie dan ook arbitrair vastgesteld en ongetwijfeld het resultaat van een compromis; het is nu eenmaal geen wiskunde. De aangenomen motie-Recourt (34588, nr. 56) verzoekt de regering om "het verzoek van de Tweede Kamer aan de CTIVD over te brengen om binnen twee jaar na de inwerkingtreding van deze wet te rapporteren over hoe de bewaartermijn van drie jaar zich verhoudt tot de bescherming van de persoonlijke levenssfeer, waarbij wordt betrokken de vraag of de interceptie van gegevens zo gericht mogelijk is geschied en of de bewaartermijn en de bewaarde gegevens nodig zijn voor een goede taakuitoefening van de diensten".

Voor wat betreft dit laatste nemen wij aan dat ook wordt bezien of in bepaalde gevallen, waarbij sprake is van een inspanning van de diensten die zich per definitie uitstrekt over een langere periode dan drie jaar, de bewaartermijn niet te kort is voor een goede taakuitoefening van de diensten. Kan de minister dat toezeggen?

Een punt waar wij eveneens onze twijfels over hebben is de financiering van de beide toetsingscommissies en de invulling van de nieuwe bevoegdheden. Hiervoor is een extra budget toegewezen van 20 miljoen euro voor de uitvoering en 1 miljoen euro voor de TIB en de CTIVD. Het budget van 1 miljoen euro voor de bekostiging van de TIB en de CTIVD is weliswaar naar aanleiding van de motie-Schouten (34588, nr. 57) verhoogd, maar dat onderstreept alleen maar onze vrees dat het huidige budget van 20 miljoen euro voor de uitvoering eveneens te krap is begroot.

Het onderzoeksopdrachtgericht verwerven van kabelgebonden data en de daarvoor nodige apparatuur en het ontwikkelen van de noodzakelijke geautomatiseerde gegevensverwerkingsprocessen, zijn niet alleen kostbaar en technisch complex, maar vereisen ook organisatorische aanpassingen van de diensten. Wij zijn naar aanleiding van informatie uit open bronnen van mening dat de benodigde financiële middelen rond 150 miljoen euro zullen bedragen en misschien zelfs meer. Het verschil met het toegewezen budget van 20 miljoen euro is wel erg groot.

Wat wij willen voorkomen, is dat we straks worden geconfronteerd met nu al voorzienbare budgetoverschrijdingen die dan ad hoc moeten worden geaccommodeerd. Wij vragen ons dan ook af wat de onderbouwing is van het begrote bedrag van 20 miljoen euro. Graag een antwoord van de minister op deze vraag.

Dan hebben wij nog een vraag over de zogenaamde wegingsnotities. Om verantwoord te kunnen wegen of een buitenlandse dienst in aanmerking komt voor samenwerking, moeten de diensten een "wegingsnotitie" maken. Als gevolg van de opgelopen achterstand op dit gebied is er in artikel 166 van de wet een stukje overgangsrecht opgenomen waarin wordt gesteld dat de wegingsnotities pas over twee jaar vereist zijn. De termijn van twee jaar bevreemdt ons. De diensten hebben toch in het verleden ook een afweging moeten maken of er wel of niet verantwoord kon worden samengewerkt met een buitenlandse dienst? Die gegevens zijn toch ruim voorhanden? Waarom moet dit

allemaal zo lang duren? Dat moet toch veel sneller kunnen? Wat is de reden voor deze wel erg ruime overgangstermijn? Graag een antwoord van de minister op deze vraag.

In het verlengde hiervan vragen wij ons af hoe de samenwerking van de diensten binnen het Koninkrijk nu precies is geregeld. Ik doel hiermee op de samenwerking van de Nederlandse diensten en de veiligheidsdiensten van de Caribische landen van het Koninkrijk. Ook hierover hebben wij in de schriftelijke voorbereiding al een vraag gesteld, maar we zijn niet helemaal tevreden met het antwoord. Wij realiseren ons dat het hier gaat om een autonome bevoegdheid van de landen en wij begrijpen ook dat een wegingsnotitie over en weer voor de landen binnen het Koninkrijk om allerlei redenen niet wenselijk is. Dat de diensten op ad-hocbasis samenwerken zal ongetwijfeld zo zijn, maar is dat in deze tijden niet wat mager? Is het niet tijd voor een meer structurele samenwerking?

Het model van een zogenaamd "intelligence fusion centre" zou naar ons idee in deze meer structurele samenwerking kunnen voorzien. Deze constructie biedt een platform waarbij de diensten binnen het Koninkrijk kunnen aangeven wat hun inlichtingen- en informatiebehoefte is, om vervolgens te bezien in hoeverre men elkaar daarbij kan ondersteunen. Kan de minister op dit idee reflecteren?

Dan heb ik nog een specifieke vraag aan de minister van Defensie. Cyberspace wordt inmiddels terecht gezien als het vijfde domein voor de krijgsmacht, naast zee, land, lucht en ruimte. Bijna drie jaar geleden werd dan ook het Defensie Cyber Commando, het DCC, opgericht om offensieve operaties in cyberspace uit te voeren. Ik herhaal: offensieve operaties. Binnenkort zal het DCC operationeel worden verklaard. Het inbreken, spioneren en het plaatsen van malware in andermans netwerken is noodzakelijk om met succes gerichte offensieve cyberoperaties uit te kunnen voeren. Het probleem dat mijn fractie ziet, is dat het inbreken en spioneren in andermans netwerken door het DCC buiten oorlogstijd of zonder specifiek mandaat niet is toegestaan. Dat is voorbehouden aan de Joint Sigint Cyber Unit van de MIVD en de AIVD, die immers valt onder de werking van de Wiv. Operaties van het DCC vallen echter niet onder de werking van de Wiv en zijn bovendien onderworpen aan de geldende politieke besluitvormingsprocedures voor militaire operaties met de daarbij behorende parlementaire informatievoorziening; zorgvuldig dus, maar traag en daardoor niet een recept voor succes in het cyberdomein. Is de minister van Defensie dit met ons eens? Zo ja, is er dan een mogelijkheid om de capaciteit van het DCC ten behoeve van de diensten te ontsluiten, waarbij deze capaciteit wordt ingezet onder de werking van de Wiv en onder aansturing en verantwoordelijkheid van de MIVD? Als de minister het niet met ons eens is, horen wij graag een toelichting van haar: waar zit de fout in onze redenering?

Ons laatste punt betreft de samenwerking van de diensten met andere instanties die belast zijn met het opsporen van strafbare feiten. Artikel 60 van de huidige Wiv geeft daartoe aangewezen ambtenaren bijvoorbeeld bij de politie, de KMar en de inlichtingendienst Belastingdienst, die ontstaan is na het in elkaar schuiven van de ECD en de FIOD, de bevoegdheid om werkzaamheden te verrichten ten behoeve van de AIVD. Deze ambtenaren worden veelal aangeduid met "artikel 60-ambtenaren". In het voorliggende wetsvoorstel wordt artikel 60 overigens vervangen door artikel 79. Een probleem in het recente verleden was dat medewerkers van Regionale Inlichtingendiensten van de politie, de zogenaamde de RID's, naast hun werkzaamheden voor de AIVD en de MIVD ook belast waren met het verzamelen van inlichtingen in het kader van de openbare orde. Dit laatste gebeurde niet onder verantwoordelijkheid van de minister van BZK, maar onder de verantwoordelijkheid van de diverse burgemeesters.

De werkzaamheden door een politiefunctionaris als medewerker van de AIVD enerzijds en als ambtenaar van een regionaal politiekorps anderzijds waren niet altijd goed af te bakenen. Het lijkt erop dat met de invoering van de nationale politie in 2013 het probleem van de dubbele petten bij de RID's is opgelost. Uit het overzicht van de indeling van de regionale eenheden van de politie blijkt immers dat er nu aparte teams zijn die zich bezighouden met het verzamelen van inlichtingen in het kader van het handhaven van de openbare orde en dat de RID's zijn omgedoopt tot RID's-Wiv. Daarmee is dus een einde gekomen aan het probleem van de dubbele pet bij de opsporingsdiensten van de politie. In het verlengde hiervan vragen wij ons echter af of het probleem van de dubbele pet bij de KMar en de inlichtingendienst Belastingdienst eveneens is opgelost. Graag een antwoord van de minister op deze vraag.

Ik rond af. Per saldo is de VVD-fractie van oordeel dat dit wetsvoorstel een acceptabele balans heeft gevonden tussen enerzijds het belang van de staatsveiligheid en anderzijds de noodzakelijke staatsrechtelijke waarborgen. Dat neemt niet weg dat wij een duidelijk antwoord verwachten van de minister op onze vragen en suggesties.

Mevrouw **Beuving** (PvdA):
Voorzitter. Het wetsvoorstel dat wij hier vandaag bespreken is bedoeld om de Wet op de inlichtingen- en veiligheidsdiensten 2002, de Wiv 2002, te vervangen met het oog op de modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten en de herinrichting van het stelsel van toezicht. Een belangrijke kerntaak van de overheid is het garanderen van een veilig land waarin in vrijheid kan worden geleefd en de democratische rechtsorde is gewaarborgd. Inlichtingen- en veiligheidsdiensten zijn noodzakelijk in het kader van deze kerntaak van de overheid. De diensten verrichten onderzoek naar organisaties en personen die mogelijk een gevaar vormen voor de nationale en/of internationale veiligheid. Op die manier beschermen de diensten de democratische rechtsstaat en dragen zij bij aan het waarborgen van de grondrechten van de burgers.

Om effectief te kunnen zijn in het identificeren van gevaarlijke organisaties en personen dient het onderzoek van de diensten in het algemeen — althans in veel gevallen — heimelijk plaats te vinden, zonder dat betrokkenen daarvan afweten. De omvang van deze heimelijk uitgeoefende bevoegdheden moet corresponderen met de reële risico's waarmee de Nederlandse samenleving en de daarmee verbonden internationale rechtsorde tegenwoordig worden geconfronteerd. Die risico's zijn de afgelopen jaren sterk toegenomen. Denk daarbij aan terroristische dreigingen, aan cybercrimegevaren en aan veiligheidsrisico's die samenhangen met de vele brandhaarden in de wereld en destabilisatie aan de grenzen van Europa. Technologische

en maatschappelijke ontwikkelingen, zoals de snelle opkomst en mondiale verspreiding van digitale technologie en het internet, hebben vergaande gevolgen. Deze ontwikkelingen en het geschetste dreigingsbeeld maken volgens de regering modernisering en uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten noodzakelijk.

Voorzitter: Flierman

Mevrouw **Beuving** (PvdA):
Tegelijkertijd vergroot de uitbreiding van ingrijpende bevoegdheden van de diensten de inherente spanning tussen enerzijds de democratische rechtsstaat en de daarin beschermde grondrechten en anderzijds het bestaan en functioneren van de inlichtingen- en veiligheidsdiensten. Inlichtingen- en veiligheidsdiensten kunnen namelijk door gebruik te maken van hun ingrijpende bevoegdheden vergaande inbreuken maken op de grondrechten van burgers. Er moet dus een balans gevonden worden tussen enerzijds de bevoegdheden van de inlichtingen- en veiligheidsdiensten en anderzijds het waarborgen van grondrechten, inclusief daarop gericht toezicht. Uitbreiding van bevoegdheden van AIVD en MIVD moet gepaard gaan met een versterking van het waarborgen van grondrechten.

Het meest in het oog springende onderdeel van dit wetsvoorstel is het mogelijk maken van ongerichte interceptie van kabelgebonden telecommunicatie. Dit betekent dat AIVD en MIVD telecommunicatie kunnen verwerven, verwerken en analyseren als zij op zoek zijn naar personen, organisaties en dreigingen, maar door onvoldoende kennis niet of nog niet gericht te werk kunnen gaan. Dat kan alleen met vooraf geaccordeerde onderzoeksopdrachten. Ongerichte interceptie wordt in het kader van dit wetsvoorstel aangeduid als onderzoeksopdrachtgerichte interceptie. Daartegenover staat dat ook de controle op de diensten wordt versterkt. Er komt een Toetsingscommissie Inzet Bevoegdheden. Dat is een onafhankelijke commissie die bestaat uit drie leden. De TIB zal de door de minister verleende toestemming voor de uitoefening van bepaalde bijzondere bevoegdheden op rechtmatigheid toetsen voorafgaand aan de daadwerkelijke uitoefening van die bevoegdheid. Als de TIB tot het oordeel komt dat de toestemming niet rechtmatig is verleend, vervalt de toestemming van rechtswege. Het gaat hier dus om een bindende rechtmatigheidstoets.

Daarnaast hebben burgers de mogelijkheid een klacht in te dienen over het handelen van de AIVD en/of van de MIVD. Burgers die dat doen krijgen in het voorgestelde systeem een bindende uitspraak van de CTIVD. De minister is dus verplicht het oordeel van de CTIVD op te volgen.

In de huidige wet, de Wiv 2002, zijn de interceptiebevoegdheden techniekafhankelijk geformuleerd. Er is namelijk onderscheid gemaakt tussen communicatie via de ether, waarbij ongerichte interceptie is toegestaan, en communicatie via de kabel, waarbij ongerichte interceptie niet is toegestaan. De commissie-Dessens heeft er in het kader van de evaluatie van de Wiv 2002 in 2013 op gewezen dat dit onderscheid niet meer rijmt met de snel voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie. De thans voorgestelde opheffing van dit onderscheid vindt de PvdA-fractie op zichzelf begrijpelijk en legitiem.

Verstrekkende bevoegdheden, zoals ongerichte interceptie, vergen echter wel dat er ook adequate waarborgen en effectief toezicht zijn. In het kader van het voorbereidende onderzoek heeft de PvdA-fractie aan de regering een aantal vragen gesteld betreffende de voorgestelde waarborgen en het voorgestelde toezicht. De van de regering ontvangen antwoorden zijn op diverse onderdelen verhelderend en toereikend, maar dat geldt helaas niet voor alle antwoorden. Een enkele keer kreeg ik toch echt de indruk met een kluitje in het riet gestuurd te worden. Dat is jammer, maar de minister heeft vandaag een herkansing!

Eerst heb ik echter nog een vraag van meer technische aard, die ik nog niet eerder aan de orde heb gesteld. De PvdA-fractie vraagt zich af of er bij het aftappen van de kabel mogelijk zodanige fysieke inbreuk op de kabel wordt gemaakt, dat er kwetsbaarheden door kunnen ontstaan waarvan dan weer misbruik gemaakt zou kunnen worden door kwaadwillende derden.

Een onderwerp waar we wel al schriftelijke vragen over hebben gesteld, is de verantwoorde databeperking en de daarmee samenhangende toets op relevantie. In antwoord daarop heeft de regering uiteengezet dat de toets op relevantie bij onderzoeksopdrachtgerichte interceptie op andere wijze plaatsvindt dan bij gerichte interceptie. Bij gerichte interceptie is sprake van reeds onderkende targets, terwijl onderzoeksopdrachtgerichte interceptie zich ook richt op het onderkennen van netwerken en ongekende dreigingen en daarmee op nog niet geïdentificeerde targets. Gerichte interceptie dient gegevens over en van de specifieke target op te leveren, waarna de relevantie per verkregen gegeven kan worden bepaald. Onderzoeksopdrachtgerichte interceptie daarentegen levert een bredere dataset op. De relevantie van gegevens in die dataset wordt bepaald door de combinatie van het bepalen van de specifieke datastroom, de negatieve en positieve filtering alsmede tot slot de selectie van gegevens. Indien de selectie desalniettemin evident niet relevante gegevens oplevert, moeten deze conform artikel 48, lid 5 van het wetsvoorstel terstond worden vernietigd. Gegevens die niet op hun relevantie zijn onderzocht, moeten na afloop van een periode van drie jaar worden vernietigd.

De CTIVD heeft erop gewezen dat het voorgaande betekent dat bij onderzoeksopdrachtgerichte interceptie alle geselecteerde gegevens bewaard en gebruikt kunnen worden, zonder dat hieraan een inhoudelijke beoordeling op daadwerkelijke relevantie ten grondslag ligt. De CTIVD vindt dit om twee redenen problematisch. De eerste reden is dat dit vergeleken met de regeling voor de inzet van een gerichte bevoegdheid leidt tot een verschil in waarborgen op het punt van gegevensvernietiging en daarmee in de mate van rechtsbescherming voor de burger. De tweede reden is volgens de CTIVD dat het effectief toezicht in de weg staat. Namens mijn fractie vraag ik de minister om inhoudelijk in te gaan op deze door de CTIVD gesignaleerde bezwaren.

In het voorbereidend onderzoek hebben wij ook gevraagd of het klopt dat de diensten metadata mogen bewaren als deze niet op basis van negatieve filtering zijn uitgesloten, zonder dat hierop positieve filtering en selectie wordt toegepast. Het antwoord van de regering luidde dat dit inderdaad het geval is en dat de met de uitoefening van onderzoeksopdrachtgerichte interceptie verkregen metadata die resteren na negatieve filtering, ten hoogste drie jaar mogen

worden bewaard. Maar even verderop in de beantwoording staat te lezen, ik citeer: "Door de combinatie van het bepalen van de specifieke datastroom, de negatieve en positieve filtering alsmede tot slot de selectie van gegevens wordt gewaarborgd dat geen sprake is van het op grote schaal inbreuk maken op de privacy van personen die zelf geen onderwerp van onderzoek zijn. Voor metadata en inhoudsgegevens gelden dezelfde normen en is er dus geen sprake van een lagere selectiestandaard voor metadata."

Zonder nadere toelichting kan ik het laatste deel van het antwoord niet rijmen met het eerste deel van het antwoord. Aan de minister dus het verzoek om uiteen te zetten hoe dit nu precies zit. En voor het geval zijn antwoord er toch op neerkomt dat metadata mogen worden bewaard als deze niet op basis van negatieve filtering zijn uitgesloten, dus zonder dat hierop positieve filtering en selectie wordt toegepast, vraag ik nu de minister alvast waarom dit verschil tussen metadata en gegevens betreffende de inhoud van de communicatie wordt gemaakt. Voorts verneem ik in dat geval graag van de minister hoe wordt voorkomen dat metadata van grote groepen onschuldige burgers zullen worden bewaard, als enkel negatief wordt gefilterd, alvorens de metadata bewaard mogen worden.

De PvdA-fractie heeft ook nog een vervolgvraag over het voorgestelde artikel 39, waarin de bevoegdheid is geregeld voor de diensten om zich te wenden tot overheidsinstanties, bedrijven en andere derden met het verzoek om realtime en geautomatiseerd toegang te krijgen tot de gegevensbestanden van de betreffende derde. De regering stelt in de nadere memorie van antwoord dat het bij de bevoegdheid van artikel 39 gaat om het bevragen van reeds bij derden berustende gegevens, zij het dat die voor een ander doel zijn vergaard. Volgens de regering is het bevragen van gegevensbestanden bij derden dan ook — dan ook! — als minder ingrijpend middel te kenmerken dan wanneer deze gegevens via de inzet van een bijzondere bevoegdheid worden vergaard. De PvdA-fractie verzoekt de minister uit te leggen waarom dit voor de persoon waarop deze gegevens betrekking hebben, een minder ingrijpend middel is, waarvoor niet de extra waarborgen hoeven te gelden die wel gelden voor de inzet van bijzondere bevoegdheden.

Voorzitter, als laatste onderdeel van mijn inbreng in eerste termijn wil ik stilstaan bij de voorgestelde Toetsingscommissie Inzet Bevoegdheden, die een belangrijke waarborg moet vormen tegenover de uitbreiding van de bevoegdheden van de diensten. De PvdA-fractie is ingenomen met de zware benoemingsprocedure die in artikel 33 juncto artikel 99 van het wetsvoorstel is opgenomen. Minder zicht hebben we op de feitelijke inbedding van de TIB. Wordt de TIB ondergebracht bij of in de nabijheid van de CTIVD, of bij een andere toezichthoudend autoriteit?

Graag zouden we een beter beeld krijgen van de feitelijke omstandigheden waaronder de TIB haar belangrijke werk moet doen. Namens mijn fractie heb ik door het stellen van schriftelijke vragen ook inzicht proberen te krijgen in hoe de TIB, bestaande uit relatieve buitenstaanders en met een zeer beperkte inhoudelijke ondersteuning — blijkens de memorie van antwoord één secretaris en één plaatsvervangend secretaris — de noodzaak, proportionaliteit en subsidiariteit van de inzet van bijzondere bevoegdheden in het kader van mogelijk grootschalige, abstract aangeduide en technisch complexe operaties zodanig goed kan inschatten dat zij daadwerkelijk de rol kan vervullen die haar in het wetsvoorstel wordt toebedeeld.

De antwoorden van de regering hebben mij hierbij tot dusver nauwelijks verdergeholpen. In de nadere memorie van antwoord is vooral benadrukt wat er in de formulering van mijn vraag, die overigens aansloot bij een formulering van de Afdeling advisering van de Raad van State, niet klopte en is vooral uiteengezet wat niet tot de taak van de TIB behoort en voorts wordt verschillende keren herhaald dat de wettelijke rol van de TIB erin bestaat te toetsen op rechtmatigheid, namelijk van een door de minister verleende toestemming voor de uitoefening van een bijzondere bevoegdheid voorafgaand aan de daadwerkelijke uitoefening daarvan. Op de kern van mijn vraag, namelijk of de TIB wel voldoende is geëquipeerd om haar rol goed te vervullen en daarmee ook feitelijk de waarborg te zijn die zij wordt geacht te zijn, is de regering niet ingegaan. Ik vraag de minister dat vandaag alsnog te doen.

Wij zien de antwoorden van de minister met belangstelling tegemoet.

De heer **Lintmeijer** (GroenLinks):
Voorzitter. De gemiddelde leeftijd van de leden van onze Kamer is 67 jaar. Een doorsnee senator begon dus aan zijn werkende leven in de jaren tachtig, een tijd waarin het internet een vreemd en onbekend woord was en de eerste mobiele telefoon, voor de liefhebbers de Dynatac 8000X, die in 1983 op de markt kwam, een hebbedingetje was voor een kleine 4.000 dollar.

Hoe anders is het nu? Een dag zonder internet is haast niet geleefd en tegenwoordig weegt de mobiele telefoon met camera en andere vernuftigheden nog geen onsje. Anno 2017 is onze manier van werken en communiceren compleet getransformeerd. De digitale revolutie verandert onze manier van doen en denken fundamenteel. Het tempo van technologische ontwikkelingen op het gebied van communicatie is genadeloos. Mede om die reden namen we nog geen uur geleden in eerste termijn een herziening van artikel 13 van de Grondwet aan, die de onschendbaarheid, c.q. eerbiediging van het briefgeheim vat in een toekomstbestendige formulering.

En daarmee deden we ook iets anders. Deze Kamer stemde ermee in dat in artikel 13 het begrip "nationale veiligheid" wordt geïntroduceerd en dat we in dat geval het overall beschermingsniveau niet meer uitsluitend via de rechter opheffen, maar per onderliggende wet regelen. "Alles door de rechter laten toetsen zou wel een hoop werk zijn", zei de minister daarover vorige week.

Het wetsvoorstel dat nu voorligt, is niet het minste dat het beschermingsniveau goed moet regelen. Extra reden om daar goed naar te kijken en te zien of er sprake is van proportionaliteit. Wegen de middelen die deze wet inzet op tegen het doel van de wet, het moderniseren van de bevoegdheden van de veiligheidsdiensten?

Vooropgesteld, de fractie van GroenLinks begrijpt en ondersteunt de noodzaak tot het vernieuwen van de Wiv. De Nationaal Coördinator Terrorismebestrijding en Veiligheid Schoof constateerde recent dat Nederland elk jaar een

stukje verder achterloopt op internetcriminelen en vijandige staten wat digitale veiligheid betreft. Ook het bedrijfsleven dringt terecht aan op meer inzet op het gebied van digitale veiligheid. Recente digitale aanvallen herinneren ons nog maar eens aan de enorme groei in de ransomware, malware die je computer vergrendelt en pas weer ontgrendelt als je geld betaalt. Nederlandse bedrijven zijn hierin, net als andere, ook hard geraakt. Met dank overigens aan de NSA, die achterdeurtjes openliet waar ook criminele hackers dankbaar gebruik van maken.

Vooral ook de niet aflatende kans op terroristische aanslagen vergt een actief en scherp veiligheidsbeleid, op straat, in de wijken, bij de recherche en zeker ook in de digitale wereld. De memorie van toelichting bij deze wet benoemt de balans tussen de modernisering van de bevoegdheden en de grondrechtelijke waarborgen. In de woorden van mijn fractie: nemen we bij de bescherming van onze vrijheden die gewaarborgd zijn door onze rechtsstaat geen maatregelen die juist onze vrijheden en de rechtsstaat inperken?

Specifiek gaat het er wat mijn fractie betreft om of de taken, de bevoegdheden en de verantwoordelijkheden van de AIVD en de MIVD nauwkeurig worden vastgelegd in de wet en dat er voldoende waarborging is voor de individuele privacy. Dat vereist een ingewikkelde maar cruciale balans tussen vrijheid en veiligheid. Mijn fractie signaleert nog altijd twijfels of dit het geval is. De Raad van State, de Autoriteit Persoonsgegevens, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten zelf, het College voor de Rechten van de Mens, de Raad voor de rechtspraak, de Raad van Europa, tal van maatschappelijke organisaties op het gebied van de digitale privacy, op het gebied van journalistieke bronbescherming en op het gebied van medisch beroepsgeheim, hebben forse commentaren geuit. Het aantal aanpassingen op basis van de kritische commentaren bleef echter beperkt.

Een van de belangrijkste wetswijzigingen is het toestaan van bulkinterceptie, met een sleepnet door het dataverkeer gaan om te kijken of dat informatie oplevert. Het is alsof in vroeger tijden de BVD voor de zekerheid alle post openmaakt die vanuit laten we zeggen Amsterdam-Noord naar Brussel-Zuid wordt gestuurd, want je weet maar nooit of er iets tussen zit. Straks kan de veiligheidsdienst een flinke berg digitale brieven openmaken en er al dan niet met slimme algoritmes verdachte signalen uitfilteren. Daarmee kan bijvoorbeeld de AIVD — en dat is goed — in de gaten houden wat er binnen het internetverkeer tussen Nederland en Syrië gebeurt. Maar in het verzamelen van die gegevens komt de dienst ook bijzonder veel persoonlijke gegevens tegen die geen connectie hebben met een strafbare zaak en gegevens van burgers die überhaupt niets te maken hebben met enig strafrechtelijk onderzoek. Die algoritmes kunnen gemakkelijk tot onnodige of onlogische conclusies leiden. Een arts die met zijn patiënt een paar keer mailt over het wel of niet opnemen in een verslavingskliniek met een cc naar de betreffende kliniek. Alleen al op basis van metadata beschikken veiligheidsdiensten dan over een medisch dossier dat daar niet thuishoort. Bij mij thuis, om maar eens een voorbeeld te noemen, zijn we lid van Amnesty. Toevallig kennen we een paar mensen die daar werken. We zijn overigens ook lid van de Dierenbescherming om de balans goed te houden. Dus we mailen weleens heen en weer over geslaagde acties om iemand vrij te krijgen of gewoon privé over een weekje vakantie in Istanbul. Dan waarschuwen we elkaar voor verbranden in de hete zon of voor stakingen op het vliegveld of de lange wachtrijen bij de security op Schiphol. Die combinatie van trefwoorden in het sleepnet, zoals Amnesty, actie, security, Istanbul, verbranden en stakingen, in handen van de veiligheidsdienst van NATO-partner Turkije kan tot heel andere conclusies leiden dan u en ik zouden willen, zeker omdat dit wetsvoorstel niet verhindert dat een buitenlandse veiligheidsdienst zijn eigen evaluatie van gegevens kan maken.

De sleepnetbevoegdheid of, in de woorden van de minister, de onderzoeksgerichte interceptie is een van de belangrijkste wijzigingen die de wet introduceert. Het is dan ook belangrijk om helder te krijgen wat wel en niet mag en onder welke condities en welke waarborgen er zijn om te zorgen dat het medisch beroepsgeheim niet wordt geschonden, dat advocaten vertrouwelijk kunnen communiceren met hun cliënten, dat journalisten hun bronnen kunnen blijven beschermen en dat duidelijk is wanneer deze gegevens nu wel of niet met buitenlandse veiligheidsdiensten mogen worden gedeeld en wat die diensten er dan mee kunnen doen of niet.

De complexe manier waarop het toezicht is geregeld, roept vragen op bij mijn fractie. Effectief toezicht is cruciaal. Het wetsvoorstel voorziet in een systeem waarbij in beginsel alle besluiten tot het inzetten van bijzondere middelen vooraf getoetst worden. In specifieke gevallen, zoals bij journalisten en advocaten, gebeurt dat door een onafhankelijk rechter en meestal door de nieuwe toetsingscommissie, de TIB, waarover mevrouw Beuving een aantal vragen heeft gesteld die ik nu niet zal herhalen. Waarom die toetsende taak niet gewoon bij de bestaande CTIVD is belegd, blijft voor mijn fractie onduidelijk. Graag horen we dat nog eens helder uiteengezet door de minister. De taak van de CTIVD is nu vooral achteraf en op basis van klachtbehandeling. Zo heeft de wetgever, zoals ook de CTIVD zelf stelde, een gelaagd en complex stelsel geïntroduceerd door toetsing, toezicht en klachtbehandeling bij aparte instanties onder te brengen. Een vergelijking met het debat van vorige week drong zich even bij mij op, waarbij het kabinet ook even niet meer weet hoe het met het toezicht op de bouw verder moet, maar dat terzijde. Wat beoogt de minister met deze complexer gemaakte vorm van toezicht? De helderheid wordt niet gevoed door de wijze van rapporteren door de instanties. De toetsingen die aan de rechtbank zijn voorgelegd blijven, als we het goed begrijpen, altijd vertrouwelijk. TIB en CTIVD rapporteren alleen via de minister aan het parlement. Dat geheel leidt tot een aantal extra vragen. Waarom kiest de minister voor grotere complexiteit in het toezicht? Waarom houdt hij dat niet strak, streng en simpel? Waarom komt de rechterlijke toets maar in enkele gevallen, zoals bij de advocaten en journalisten, aan de orde? Ik verwijs net als vorige week bij het debat over artikel 13 nog een keer naar de jurisprudentie van het Europees Hof uit november 2012, waar het Hof feitelijk zegt dat als het schenden van de rechten van individuen gemakkelijk mogelijk is en de gevolgen heftig kunnen zijn, in principe de rechter zou moeten meekijken. Graag krijg ik nu wel een concrete reactie van de minister.

De CTIVD heeft bij meerdere gelegenheden aangegeven zich zorgen te maken of zij voldoende middelen ter beschikking heeft om haar taken uit te oefenen. Is de minister bereid om in gesprek te gaan over de financiën en, zo nee, om met een versnelde evaluatie te komen om te zien of de taken met de bestaande bezetting kunnen worden uitgevoerd? Is de minister tevens bereid een vol-

doende transparant, onafhankelijk en compleet stelsel van rapportages onverkort en onverwijld, eventueel vertrouwelijk, aan de Kamers te sturen om de Kamers inzicht te geven in de werking van het toezicht na inwerkingtreding van de wet?

De nieuwe techniekonafhankelijke formulering van interceptie was ook reden voor een reeks vragen in de schriftelijke behandeling. De CTIVD bepleitte dat het verzamelen en analyseren van data selectief, doelgericht en met zorg moet plaatsvinden. Het is belangrijk dat niet-relevante gegevens direct verwijderd worden, de zogenaamde nevenvangst. Uit de antwoorden van de minister maak ik op dat hij meent dat de "select while you collect"-handelwijze al nadrukkelijk genoeg verankerd is in de wet. GroenLinks heeft ook daar haar vragen bij. Is er bijvoorbeeld genoeg digitale ondersteuning en is er voldoende toezicht om deze handelwijze te realiseren? Zullen de diensten niet, tenzij er een sterke waarborg in de wet tegenover staat, altijd geneigd zijn om gegevens voor de zekerheid maar te bewaren, omdat er altijd een kleine kans is dat ze relevant zullen blijken in de nabije toekomst?

Gewone mensen willen veiligheid, maar ook de garantie dat ze ongehinderd hun mailtjes, sms'jes en whatsappjes kunnen sturen, zonder dat de overheid onnodig vaak en onnodig veel over hun schouder meekijkt. Het werk dat de veiligheidsdiensten doen, is een groot goed. Als zij dit werk kunnen blijven doen met het vertrouwen van de samenleving dat dit vakkundig, gericht en onder goede wettelijke waarborgen wordt gedaan, kan dat hun positie alleen maar versterken. In het maatschappelijk debat zien wij op dat punt echter bezorgdheid en erosie van draagvlak.

Daarom leg ik nog even een paar punten onder het vergrootglas. De minister stelde onder meer in de memorie van antwoord aan de Kamer dat voor het bepalen van de ernst van de inbreuk op de privacy gekeken wordt naar drie factoren: de vraag of het bij de inbreuk gaat om de inhoud van berichten of om metadata, de schaal waarop gegevens worden verzameld en hoe ingrijpend de gehanteerde ontsluitingssystematiek is. Dat vraagt, naar de mening van de fractie van GroenLinks, om een betere invulling van de criteria. Kan de minister nog eens uiteenzetten hoe hij in de praktijk concreet beoordeelt wat de impact is van de schaal waarop gegevens worden verzameld? Welke ontsluitingsmethodieken zijn in zijn ogen wel of niet aanvaardbaar? Waar ligt volgens de minister de grens waarbij een inbreuk op de privacy niet meer proportioneel is? Als alle mails van een stadswijk of buurt worden onderschept? Of mag dat wel? Als we iedereen met de naam Jansen — ik formuleer het bewust maar even met een neutrale naam — onder de loep nemen? Als we al het berichtenverkeer uit Rusland onderscheppen vanwege mogelijk hackgevaar? Waar ligt volgens de minister de grens van het toelaatbare? Ligt die grens voor de inhoud lager dan voor metadata? Is de toegepaste techniek van invloed? In de Tweede Kamer zei de minister dat het volgens het kabinet niet aannemelijk is dat bijvoorbeeld persoonlijke apparaten die mensen om medische redenen dragen, gehackt worden, maar dat staat niet in de wet. Waarom eigenlijk niet? Ook dat kun je techniekonafhankelijk formuleren. Het is van fundamenteel belang dat dit soort zaken helder en eenduidig geformuleerd is, ook om het draagvlak voor de veiligheidsdiensten zo groot mogelijk te houden.

Ik ga nog even kort in op de bewaartermijn. Ook daar is eerder over gesproken. Voorstellen om deze termijn terug te brengen naar twee of een jaar worden afgewezen door de minister, terwijl landen als het Verenigd Koninkrijk en Duitsland niet langer dan een halfjaar respectievelijk 90 dagen onbewerkte data bewaren. Waarom is de minister hierover zo halsstarrig? Hoe verhoudt de voorgestelde bewaartermijn zich tot de uitspraak van het Hof van Justitie uit 2014 over de Dataretentierichtlijn? De conclusie van het Hof van Justitie was destijds dat de bewaarplicht een disproportionele inbreuk vormt op het recht op privacy. In verband daarmee werd de Wet bewaarplicht telecommunicatiegegevens gezien als strijdig met het Handvest van de grondrechten van de Europese Unie, terwijl de bewaartermijn in die wet slechts een halfjaar bedroeg. Met welke argumenten kan deze bewaartermijn nu dan wel worden gelegitimeerd? Deze Kamer zou wat ons betreft geen wetsvoorstel moeten aannemen als er gerede twijfel is over de vraag of dit in strijd is met uitspraken van het Europese Hof. Ook recentelijk werd in Europees verband nog gesproken over de bewaartermijn van gegevens. Ik verwijs naar de brief van minister Blok over de JBZ-Raad van 3 juli 2017. Is er een advies van de juridische dienst van de Raad? Kan de minister dat bevestigen? Zo ja, kan de Kamer dat advies dan ontvangen, hetzij schriftelijk, hetzij mondeling, liefst vandaag nog?

Bestaande kwetsbaarheden in het digitale systeem zullen soms doelbewust worden opengelaten door de veiligheidsdiensten, om zo toegang te krijgen tot bepaalde gegevens. Wij vinden dat die achterdeurtjes zonder meer gemeld moeten worden. Hebben we niets geleerd van de recente malware? De minister spreekt van een richtlijn daarvoor. Hoe staat het met die richtlijn? Welke criteria worden daar dan in opgenomen? Graag krijg ik hierop een reactie van de minister.

De inzet van onze diensten om de veiligheid van Nederlanders te garanderen stopt niet bij de landsgrenzen. Het is ook belangrijk dat de Nederlandse diensten samenwerken met buitenlandse geheime diensten en in dat verband gegevens kunnen uitwisselen. Met deze wet wordt echter ook voorgesteld om in bepaalde gevallen niet-geëvalueerde data te delen. Dat wil zeggen dat buitenlandse diensten dan aan de slag kunnen met een complete set data waarvan geen analyse is gemaakt door onze veiligheidsdiensten. Dat is voor ons onaanvaardbaar. Als dat gebeurt, is het volstrekt onduidelijk wat een buitenlandse dienst uitspookt met gegevens van Nederlandse burgers, die niets anders hebben gedaan dan per ongeluk in het verkeerde sleepnet zitten. De gevolgen kunnen ernstig zijn voor mensen wier gegevens in handen komen van veiligheidsdiensten in landen waar bijvoorbeeld andere opvattingen over seksualiteit heersen. Welke zekerheid biedt dit wetsvoorstel volgens de minister dat data die gedeeld worden met buitenlandse diensten vooraf op enige wijze getoetst zijn op de gevolgen voor de positie van Nederlandse burgers?

Ik wil heel kort nog een paar puntjes aanstippen. Allereerst is er de waarborging van journalistieke vrijheden. Is de regeling die daarvoor is ingesteld in lijn met de eisen die het EVRM daaraan stelt? En geeft die klokkenluiders en journalisten voldoende ruimte om gevoelige informatie te delen met de media? Om mijn vraag uit de schriftelijke ronde nog eens te herhalen: is het voorstel nu zo ingericht dat er alleen een uitzondering gemaakt kan worden in gevallen waarin een rechter oordeelt dat het belang van de

diensten zwaarder weegt dan het belang van bronbescherming? Ik heb ook nog een puntje over het systeem van nummerherkenning. Is het overleg daarover met de Nederlandse orde van advocaten al in gang gezet? Wat is daarvan de stand van zaken?

Ik kom tot een afronding. Een wetsvoorstel dat in potentie dusdanig ingrijpt in de individuele vrijheid van de Nederlandse burger en dusdanig belangrijk is voor de nationale veiligheid vraagt om heldere afspraken over de vraag wanneer er op grote schaal getapt kan worden, om eenduidig toezicht en een rechterlijke toets, om uit te sluiten dat ongefilterde data van Nederlandse burgers zomaar naar het buitenland verdwijnen. Als daar geen sprake van is, dan ontstaan er onbehagen en bezorgdheid. Die zijn er nu nog te veel. Zo bereiken we niet de veiligheidsdoelen die we willen bereiken en ook niet het niveau van privacy en rechtsbescherming waar burgers op mogen rekenen. Wij zijn erg benieuwd naar de antwoorden van de minister.

☐

De heer **De Graaf** (D66):
Voorzitter. Ik val maar met de deur in huis: er bestaat nauwelijks een onderwerp dat lastiger te beoordelen is voor volksvertegenwoordigers — en al helemaal de deeltijdvariant daarvan — dan het noodzakelijk arsenaal van bevoegdheden waarover de inlichtingen- en veiligheidsdiensten zouden moeten beschikken. Als wij een diep wantrouwen zouden koesteren jegens onze inlichtingen- en veiligheidsdiensten, dan zou het wellicht nogal overzichtelijk zijn, maar dat wantrouwen is er niet. AIVD en MIVD kennen de laatste tientallen jaren een traditie van democratische inbedding en rechtsstatelijk waardenbesef, die eerder vertrouwen dan wantrouwen genereert. Daar past waardering voor de opeenvolgende diensthoofden. Hetzelfde geldt voor de eerstverantwoordelijke ministers van Binnenlandse Zaken, Defensie en Algemene Zaken.

Niettemin lopen wij met een lucifer in het donker. Wij kennen de omvang en de aard van de bedreigingen van onze veiligheid onvoldoende. Daarvoor zouden we diep moeten duiken in de door de diensten vergaarde informatie, waartoe we geen toegang hebben. Wij kennen de effectiviteit van de toepassing van de huidige bevoegdheden onvoldoende en kunnen daar dus ook moeizaam zelf over oordelen. Dat moeten we aan de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten overlaten en op afstand aan de commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer. En marge merk ik op dat de term "commissie-stiekem" buitengewoon ongelukkig is. Wij zijn bovendien onvoldoende thuis in de technische aspecten van verwerven, analyseren, bewaren, verwijderen en vernietigen van digitale gegevens — ik spreek nu vooral namens mijzelf — in het bijzonder waar het gaat om het op grote schaal verwerven van data door het internet af te tappen.

Toch moeten wij vandaag een oordeel vellen over een wetsvoorstel waarmee wordt beoogd een modernisering van het bevoegdhedencomplex van de inlichtingen- en veiligheidsdiensten en de toetsing en controle op de toepassing daarvan tot stand te brengen. Terzijde merk ik op dat een stevige grondwettelijke basis voor het onderhavige wetsvoorstel eigenlijk nog ontbreekt. Vandaag hebben wij in de Eerste Kamer immers pas in eerste lezing ingestemd met de modernisering van artikel 13 van de Grondwet.

Het is een lastige zoektocht in de spanningsrelatie die van oudsher bestaat tussen de bescherming van de nationale en internationale veiligheid enerzijds en de bescherming van de persoonlijke levenssfeer anderzijds. Het behoeft, hoop ik, geen betoog dat beide belangen voor mijn fractie van grote waarde zijn; het een is niet onder alle denkbare omstandigheden meer beschermingswaardig dan het andere. Juist daarin huist de complexiteit van onze afweging: onder welke omstandigheden kunnen veiligheid en privacy elkaar in evenwicht houden, wanneer rechtvaardigt de situatie dat privacy kan worden ingeperkt om de veiligheid te borgen en hoever moet die inperking dan gaan? En in welke gevallen moeten overheid en wetgever pal staan voor de persoonlijke levenssfeer, zelfs als daardoor de nationale veiligheid een zeker risico loopt? Daar is geen algemeen antwoord op, althans niet voor degene die platitudes of al te kortzichtige keuzes probeert te vermijden.

Zie daar het dilemma, dat overigens nog wordt verzwaard door het feit dat we niet alleen spreken over wat onze eigen nationale diensten doen met verworven data over mensen en hun communicatie, maar ook over het delen van deze informatie met diensten van meer en minder bevriende en meer en minder democratisch rechtsstatelijke landen. Is de uitwisseling van gegevens met de Verenigde Staten van Trump voor ons even vertrouwenwekkend als met hetzelfde land onder Obama? Kunnen inlichtingendiensten in NAVO-verband nog informatie delen met het Turkije van president Erdogan?

Ik beperk mij in mijn bijdrage tot een paar hoofdonderwerpen en ga achtereenvolgens in op de verwerving en het gebruik van bulkdata in het kader van de zogenaamde "onderzoeksopdrachtgerichte" gegevensverzameling, de samenwerking met buitenlandse diensten en het ontworpen toetsing- en toezichtsysteem, inclusief het klachtrecht.

Het grote verschil met de wet van 2002 is de uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten, die voorheen al grote informatiestromen via de ether konden aftappen, maar over de kabel alleen gerichte interceptie mochten toepassen. Nu is ook aftappen van bulkcommunicatie over internetkabels mogelijk. Het primaire door de wet beschreven criterium is dat het aftappen van internetkabels slechts "onderzoeksopdrachtgericht" mag plaatsvinden, dus niet buiten de onderzoeksopdracht. Dat sluit op zichzelf echter niet uit dat grote hoeveelheden data worden verzameld in het kader van de onderzoeksopdracht en dat dit ook van lange duur kan zijn. Ook sluit dit niet uit dat onder omstandigheden een hele buurt of wijk kan worden afgetapt omdat er aanwijzingen bestaan dat zich daar een potentiële terrorist of spion ophoudt. "Onderzoeksopdrachtgericht" kan zo snel ongericht worden en de vorm aannemen van wat in het spraakgebruik van critici wordt aangeduid met het "sleepnet": alles en iedereen wordt opgevist, ook wie en wat geen waarde heeft voor het specifieke onderzoek. Wordt dat op tijd weer verwijderd onder het motto: select while you collect? Blijft die onnodige informatie bewaard ook al is die verwijderd? Er bestaat immers een essentieel verschil tussen verwijderd en vernietigd. Heb ik goed begrepen dat verwijderde informatie niettemin nog kan worden teruggehaald lang nadat in het kader van het specifieke onderzoek de selectie heeft plaatsgevonden? Is dat wel in overeenstemming met de jurisprudentie van het EVRM? Ik wijs op de zaak Zakharov tegen Rusland van eind 2015. Het laatste CTIVD-rapport dat wijst op onvolkomenheden in de uitvoering van de vernie-

tigingsplicht en in meldingen aan de verantwoordelijke minister is wat mij betreft zorgelijk. Ik vraag de bewindslieden om een reactie.

Mijn fractie heeft grote aarzelingen bij de waarborgen die het wetsvoorstel biedt voor het zorgvuldig en verantwoord omgaan met grote informatiestromen die van internet worden afgetapt. En dan ga ik nog voorbij aan het zogenaamde chillingeffect dat dataverzameling via internet kan hebben op burgers en bedrijven, dat wil zeggen de terughoudendheid om te communiceren via het net omdat je nooit weet of die vertrouwelijke communicatie niet ooit tegen je wordt gebruikt of zelfs misbruikt. En ik ga ook voorbij aan de vraag hoe effectief het via internettaps zoeken van een speld in de hooiberg is als met die tap de hooiberg alleen maar groter wordt, een metafoor die de ministers vermoedelijk al vaker hebben gehoord, maar die nog steeds treffend is. De vraag is overigens wel zeer relevant voor de toets of toepassing van de bevoegdheid zinvol is, noodzakelijk is.

Vooralsnog meent mijn fractie dat de waarborgen voor een zo selectief mogelijke uitvoering van de onderzoeksopdracht en het voorkomen van een te grote beperking van de persoonlijke levenssfeer onvoldoende in het wetsvoorstel tot uitdrukking zijn gekomen. Ik richt mij daarbij in het bijzonder op de bevoegdheden van de artikelen 48, 49 en 50 in het wetsvoorstel. Laat ik vooropstellen dat mijn fractie de uitbreiding van de bevoegdheden in het kader van een goede uitoefening van de taken van de inlichtingen- en veiligheidsdiensten kan en wil billijken. Met de Afdeling advisering concluderen wij dat die uitbreiding legitiem en noodzakelijk is. Maar evenzeer meent mijn fractie dat een dergelijke uitbreiding alleen kan worden gerealiseerd als die gepaard gaat met duidelijke wettelijke waarborgen waarbinnen de diensten moeten werken en met de inrichting van een effectief stelsel van toezicht. De Afdeling advisering is in een buitengewoon heldere analyse van het EVRM en de jurisprudentie van het Europees Hof tot de slotsom gekomen dat het wetsvoorstel een aantal belangrijke waarborgen bevat die voldoen aan essentiële vereisten die door het Europees verdrag zijn gesteld. Dan gaat het om een deugdelijke wettelijke basis in het licht van kenbaarheid en voorzienbaarheid van inbreuken op grondrechten en een voldoende onderbouwing van de noodzaak om de bevoegdheid te scheppen tot ongerichte interceptie van kabelgebonden communicatie. De artikelen 18 en 26 van het wetsvoorstel geven in algemene zin de waarborgen bij de uitoefening van de in het voorstel opgenomen bevoegdheden van noodzakelijkheid, proportionaliteit en subsidiariteit. Dat is mooi, maar is het ook genoeg? De Afdeling advisering concludeerde dat voor de bevoegdheden tot interceptie van grote hoeveelheden data, en dus gegevens van een grote hoeveelheid mensen en instanties — soms nodig om uiteindelijk de beoogde selectie tot stand te brengen of een nog onbekende dreiging te ontdekken — onvoldoende scherpte in die waarborgen is aangebracht.

Mijn fractie had graag gezien dat in het bijzonder de bevoegdheden van de artikelen 48 tot en met 50 wettelijk waren voorzien van heldere, toegespitste criteria op het vlak van proportionaliteit en subsidiariteit, zo concreet mogelijk. Een amendement ter zake heeft het in de Tweede Kamer helaas niet gehaald. Dat amendement, op stuk nr. 34, formuleerde dat bij de inzet van een bijzondere bevoegdheid als hier bedoeld niet meer gegevens mogen worden verworven, verwerkt of geanalyseerd dan strikt noodzakelijk is voor het bereiken van het doel van de onderzoeksopdracht en dat de onderzoeksopdracht zo concreet mogelijk wordt geformuleerd en op zichzelf of tezamen met andere onderzoeksopdrachten niet leidt tot het stelselmatig op grote schaal collecteren en gebruiken van gegevens. Het ging hier natuurlijk om de combinatie "stelselmatig op grote schaal", om datgene wat in de wandelgangen al snel het sleepnet wordt genoemd. De regering ontraadde dit amendement, omdat het de essentie van het wetsvoorstel miskende, aldus minister Plasterk.

Moet ik daaruit afleiden dat de regering meent dat wel degelijk stelselmatig op grote schaal bulkdata kunnen worden verzameld, bewerkt, geanalyseerd en eventueel doorgegeven aan buitenlandse diensten? Ik vraag nadrukkelijk een reactie van de ministers. Is "stelselmatig op grote schaal" nog in overeenstemming met de eisen van proportionaliteit en subsidiariteit en gerichtheid, die de regering wil onderschrijven en die cruciaal zijn in de jurisprudentie van het Europees Hof voor de Rechten van de Mens? Ook hierop graag een reactie.

De overzijde, de Tweede Kamer, volstond met een buitengewoon mistige motie-Recourt waarin werd benadrukt dat de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit ook geïnterpreteerd en in de praktijk gebruikt moeten worden "als eisen die zullen leiden tot een zo gericht mogelijke inzet van bevoegdheden". Als ik het ietwat onaardig mag zeggen: een dooddoenende tekst om zowel de kool als de geit te sparen.

Ik zou zelfs een aanscherping van de wettelijke criteria op prijs stellen, al dan niet bij nadere wetgeving. Ik vind dat van het grootste belang om het vertrouwen van de bevolking in een zo zorgvuldig mogelijke toepassing van deze verreikende bevoegdheden te bewaren dan wel terug te winnen.

Een met deze zorgvuldigheid samenhangend ander punt is de vernietiging van gegevens. De regering vindt het van het grootste belang dat niet-onderzochte gegevens, dat wil zeggen uit bulkinterceptie verkregen gegevens die nog niet zijn verwerkt en geanalyseerd — voor een groot gedeelte zal dat dus vaak bijvangst zijn — in afwijking van de gewone termijn van een jaar, drie jaar bewaard mogen blijven. Voor versleutelde berichten kan dit zelfs oplopen tot een dubbele bewaartermijn van zes jaar, want na de decodering geldt ook weer de maximale bewaartermijn van drie jaar.

Deze lange termijn kan wellicht onder bijzondere omstandigheden dienstbaar zijn — ik zal dat niet ontkennen — maar strijdt naar het oordeel van de Afdeling advisering met artikel 8, lid 2, van het Europees Verdrag voor de Rechten van de Mens en de daarop gebaseerde jurisprudentie. De regering voelt niets voor verkorte bewaartermijnen en meent dat het wel los zal lopen met dat Europees Verdrag. Toch verzoek ik de ministers nog eens te reflecteren op de mogelijkheid om de bewaartermijnen te differentiëren naar de mogelijke toepassingen. Bijvoorbeeld een vernietiging binnen anderhalf of twee jaar, tenzij een ernstig nationaal veiligheidsbelang zich tegen deze termijn zou verzetten, hetgeen een eigenstandige toetsing vraagt. Voor versleutelde gegevens zou ten minste een termijn voor de ontsluiering in de wet zelf moeten worden opgenomen. Ook dat werd eerder door de Afdeling advisering gesuggereerd. Ook hierop hoor ik graag de reactie van het kabinet.

De samenwerking met het buitenland baart mijn fractie eveneens zorgen. De verstrekking van niet-geëvalueerde gegevens aan bevriende diensten is natuurlijk al een moeizaam vraagstuk op zich. De eindcontrole op wat ermee gebeurt, wordt uit handen gegeven en zo komen vele gegevens van mensen, instanties en hun communicatie in handen van diensten, die politieke regimes dienen die niet altijd een-op-een onze rechtsstatelijke principes wensen na te leven, ook al worden die vaak wel met de mond beleden. In het kader van de internationale samenwerking bij de bestrijding van ernstige vormen van staatsondermijning en terrorisme zou mijn fractie dit bij wijze van hoge uitzondering wel kunnen billijken, zij het dat ook hier de eisen van proportionaliteit en noodzakelijkheid vooropstaan.

Buitengewoon lastig vind ik het dat het vereiste van de wegingsnotities, waarin aan de criteria van rechtsstatelijkheid, democratie, wettelijk stelsel en waarborgen wordt getoetst, gedurende een overgangsperiode van twee jaar niet geldt. Dat betekent feitelijk dat zonder weging op grond van oude relaties van diensten niet geëvalueerde informatiestromen mogen worden overgedragen aan derde landen, zonder enige waarborg wat daarmee gebeurt. Ik heb drie vragen op dit punt aan de ministers. Waarom niet de werking van in ieder geval dit deel van de wet een of twee jaar uitstellen, zodat die wegingsnotities er gewoon zijn op het moment dat overdracht van internetinformatie aan de orde zou zijn? Waarom moet het überhaupt twee jaar duren? Wat is er dan gebeurd in de jaren hieraan voorafgaand? De wet was immers al enige tijd in voorbereiding. Hoe denken de ministers hun verantwoordelijkheid en die van hun opvolgers te kunnen waarmaken door toestemming te geven voor informatieoverdracht aan buitenlandse diensten, wanneer zijzelf niet een toetsbaar kader in de hand hebben? Zien zij de risico's die niet alleen zij zelf, maar vooral ook onschuldige burgers hierbij kunnen lopen? Graag vraag ik ook hoe juist hier de communicatie van journalisten en wetenschappers voldoende kan worden beschermd. Welke voorzieningen wil en kan de regering treffen om te voorkomen dat bronnen van journalisten en onderzoekers via deze overdracht van informatiestromen in landen van herkomst bekend worden en mogelijk bedreigd worden?

Ik ga over tot mijn laatste thema en dat is het toetsing- en toezichtsysteem. In het bijzonder dit stelsel van toezicht heeft op kritische beoordeling van de Afdeling advisering mogen rekenen, zulks tegen de achtergrond van de eisen die het Europees Hof voor de Rechten van de Mens in verband met artikel 13 van het verdrag aan het geheel van het juridisch kader en de feitelijke uitwerking stelt. Het oordeel is ongemeen scherp: het stelsel van toezicht is onvoldoende effectief en toetsing door de Toetsingscommissie Inzet Bevoegdheden zal in de praktijk slechts neerkomen op een marginale en abstracte rechtmatigheidstoets ex ante. Sterker nog, de verwachting is dat de toetsing van de TIB altijd positief zal uitvallen. De Afdeling advisering spreekt zelfs van een alibifunctie.

Mijn fractie begrijpt deze zorg, al voldoet de voorgestelde regeling formeel wel aan de vereisten van onafhankelijke toetsing. Een inbreuk op de ministeriële verantwoordelijkheid, zoals de Afdeling advisering ook nog stelde, zou onder omstandigheden inderdaad aan de orde kunnen zijn: de minister blijft weliswaar volledig verantwoordelijk, bijvoorbeeld als zou blijken dat zijn beslissing tot inzet en het rechtmatigheidsoordeel van de TIB op onjuiste gegevens zou berusten, maar hij is wel gebonden aan het rechtmatigheidsoordeel van de TIB in die zin dat als de TIB meent dat inzet onrechtmatig zou zijn, het besluit van de minister op grond van de wet van rechtswege vervalt. Dat is nogal wat. Misschien dat de voor de constitutie verantwoordelijke minister nog eens zijn licht hierop wil laten schijnen, zo vlak voor zijn eigen politiek verscheiden.

Maar de crux zit toch in de onvolkomenheid van het inzicht en de kennis van de TIB, terwijl de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten die op alle fronten wel heeft. Waarom de regering zo veel bezwaar heeft tegen een constructie waarin de CTIVD ook de rechtmatigheid ex ante beoordeelt, is mij tot op heden onvoldoende duidelijk geworden. De CTIVD wordt in deze constructie met de TIB in haar taak en verantwoordelijkheid beperkt doordat, ik citeer de minister, "de CTIVD de rechtmatigheid van het besluit in beginsel dient te respecteren". Ik acht dat overigens ten principale onjuist. De CTIVD moet immers in alle vrijheid zich een oordeel kunnen vormen over de aard, de omvang, de proportionaliteit en de noodzakelijkheid van de toepassing van de bevoegdheden en daarbij dus ook kunnen oordelen over de rechtmatigheid van de inzet, als het niet aan de voorkant mag, dan in ieder geval aan de achterkant. Dat is overigens ook in het belang van de parlementaire controle. Het is dan ook de vraag of de bewering van de minister dat de wet het rechtmatigheidsoordeel exclusief bij de TIB legt, juist is. De wet omvat immers geen beperking van de taak van de CTIVD; die heb ik er althans niet in kunnen lezen. De minister wil ook niet de rechtszekerheidstaak van beide commissies bevorderen door bijvoorbeeld een samenwerkingsprotocol te entameren. Dat is naar mijn oordeel een erg afhoudende houding, die weinig perspectief biedt op een goede positionering van beide commissies.

De wijze waarop de regering omgaat met het toezicht en de toetsing laat bij mijn fractie een wat ongemakkelijk gevoel achter. Voor de diensten is dit wellicht werkbaar, maar voor een gebalanceerd toezicht als onderdeel van rechtsstatelijke structuren is het toch onvolledig. Dat is voor mijn fractie een belangrijk punt van overweging.

Tot slot heb ik nog een vraag over het klachtrecht. De behandeling daarvan is, ondanks de bezwaren her en der, bij de CTIVD gelegd. De argumentatie van de regering dat er binnen het kader van art. 13 EVRM sprake moet zijn van een bindende klachtbehandeling, is voor mijn fractie overtuigend, maar onderbrenging bij de CTIVD niet, temeer niet omdat de schijn van partijdigheid kan ontstaan en een kleine eenheid zichzelf in tweeën moet gaan delen, inclusief Chinese walls. Ik wil de minister opnieuw uitnodigen om onderbrenging bij de Nationale ombudsman te overwegen. Ook dit zou bij nadere wetgeving kunnen worden geregeld. Het bindende karakter van een oordeel van de Nationale ombudsman, in afwijking van het reguliere stelsel, zou in dit geval kunnen worden gerechtvaardigd omdat toetsing en controle door de onafhankelijke rechter bij inlichtingen- en veiligheidsdiensten is uitgesloten.

De ministers begrijpen dat de kritische houding van mijn fractie instemming met dit wetsvoorstel niet gemakkelijk maakt, maar vanzelfsprekend wacht ik de reactie en mogelijke tegemoetkomingen van de zijde van de regering af alvorens een eindoordeel te geven.

Mevrouw **Beuving** (PvdA):
Ik heb als nabrander nog een kleine interruptie op een punt dat eerder is voorbijgekomen, namelijk de opmerking over de motie-Recourt. Ik kreeg helaas niet de gelegenheid om de spreektekst er nog even op na te slaan, maar ik meen de heer De Graaf te hebben horen zeggen dat dat een zeer vage motie is waar we eigenlijk heel weinig mee kunnen. Daardoor ben ik toch even in mijn eigen dossiertje ben gedoken, want ik meende mij te herinneren dat de CTIVD dat anders ziet. In de brief die we op 22 maart jongstleden allemaal hebben gehad, wordt de motie-Recourt onder het kopje "Handvatten voor effectief toezicht" prominent in het eerste punt genoemd. Vervolgens schrijft de CTIVD: "De CTIVD begrijpt dit aldus dat de diensten (telkens en uit zichzelf) de vraag of de inzet van bevoegdheden niet gerichter kan, gemotiveerd moeten beantwoorden in de verzoeken om toestemming voor die inzet." Het is al heel wat dat de CTIVD stelt dat dit haar voldoende handvatten voor het toezicht geeft en het is mooi dat de CTIVD zegt dat zij dit aldus begrijpt, maar ik wil heel graag van de regering horen dat de CTIVD dit goed ziet. Ik heb daar dus in twee rondes op doorgevraagd. In de nadere memorie van antwoord is daarop geantwoord dat bij die verzoeken om toestemming voor inzet van die bevoegdheden inderdaad beargumenteerd en gemotiveerd moet worden dat het zo gericht mogelijk is geschied. Ik wil daar heel graag een reactie op van de heer De Graaf.

De heer **De Graaf** (D66):
Zeker. Wat de minister zegt in antwoord op die motie en de CTIVD, kan ook uit de wet zelf worden afgeleid. Dat heeft de minister ook beweerd, ook in het debat met de Eerste Kamer. Dat zijn de eisen van proportionaliteit en subsidiariteit. Mijn verzoek was om het niet te houden bij één motie — die overigens geen rechtswaarde heeft, zoals u weet — maar een wettelijke nadere verbijzondering te geven van de eisen die aan de toepassing van artikelen 48, 49 en 50 kunnen worden gesteld. Ik zou willen dat dit verder werd toegespitst. Ik heb gewezen op een concreet amendement dat verder gaat dan de motie-Recourt, maar dat door de minister werd afgewezen omdat hij meent dat de diensten daardoor in hun taak zouden worden beperkt. Ik denk dat die beperking heel verstandig zou zijn.

Mevrouw **Beuving** (PvdA):
Ik realiseer mij wat de status van een motie is. Dat was voor mij mede de aanleiding om daarop door te vragen. We weten natuurlijk ook wat de status van onze Handelingen en de gehele parlementaire geschiedenis rond een wetsvoorstel is en hoe dat alles in de praktijk, in de rechtspraak et cetera kan doorwerken. In de memorie van antwoord kreeg ik een vaag geformuleerd antwoord van de regering, namelijk dat op enigerlei wijze zou moeten blijken dat de diensten bevoegdheden zo gericht mogelijk inzetten en dat daarmee aan de motie-Recourt in de praktijk genoegzaam uitvoering was gegeven. "Op enigerlei wijze" was voor mij veel te vaag en ik heb daarop doorgevraagd. In de nadere memorie krijg je uiteindelijk de bal op de stip of wat mij betreft in het doel: niet op enigerlei wijze, maar uit de verzoeken om toestemming aan de minister voor de inzet van een bijzondere bevoegdheid zal moeten blijken dat die zo gericht mogelijk wordt ingezet. Dat is toch een onderdeel van de parlementaire geschiedenis. Daarmee hebben we toch een behoorlijk concrete formulering. Ik zou daarop graag nog een reactie krijgen.

De heer **De Graaf** (D66):
Voorzitter, ik krijg de indruk dat mevrouw Beuving over uw en mijn hoofd vooral het debat met de regering verder voert. Dat is prima. Zij probeert, met veel geduld overigens, het uiterste uit die motie te peuren. Dat is mooi, maar ik heb liever dat het in de wet staat. In de wet zou ik veel concreter willen zijn. Nu zijn we afhankelijk van de interpretaties van de regering en van de Kamer over wat er niet in de wet staat. Dat vind ik een minder goede positie. Ik heb het ook betreurd dat aan de overzijde het amendement dat veel concretere criteria stelt en dus ook een zekere beperking invoert door onder meer de fractie van de Partij van de Arbeid niet werd gesteund. Dat was jammer, maar dat kan wat mij betreft altijd nog worden geredresseerd via nadere wetgeving. Ik hoop dat mevrouw Beuving die dan ook wil steunen.

Mevrouw **Bikker** (ChristenUnie):
Voorzitter. "De AIVD en de MIVD hebben gezien dat Nederlandse overheidsinstellingen het afgelopen jaar herhaaldelijk doelwit waren van omvangrijke en hardnekkige digitale spionageaanvallen. Zo zijn het ministerie van Buitenlandse Zaken en het ministerie van Defensie meerdere malen aangevallen, ook door landen die niet eerder zijn waargenomen als dreiging tegen Nederlandse overheidsnetwerken. De aanvallen geven blijk van omvangrijke en structurele interesse in de Nederlandse overheid", zo valt te lezen in het verslag van de Nationaal Coördinator Terrorismebestrijding en Veiligheid over de cybersecurity van Nederland in het afgelopen jaar. Sinds 2002, toen de vorige Wet op de inlichtingen- en veiligheidsdiensten tot stand kwam, zijn de technische mogelijkheden en middelen enorm gegroeid met alle gevolgen van dien. Dat laat ook het werk van onze inlichtingen- en veiligheidsdiensten niet onberoerd. Ik wil juist daarom beginnen met een compliment aan de vele mannen en vrouwen die dag en nacht in touw zijn om Nederland een veilig land te laten zijn. We zijn hen dankbaar.

Het wetsvoorstel dat wij vandaag bespreken, beoogt aan te sluiten bij de veiligheidsvraagstukken van deze tijd. Om onze rechtsorde en daarmee onze vrijheid en nationale veiligheid te beschermen, is het de taak van de wetgever om zorg te dragen voor een bij de tijd passend en effectief wettelijk kader voor de diensten. De ChristenUnie steunt het kabinet in die zoektocht, maar constateert tegelijkertijd wel dat er een spanningsveld is. Hoeveel vrijheid moet een burger inleveren om voor ons land te kunnen garanderen dat vrijheid en een stabiele rechtsorde de pijlers blijven? Als dat te veel wordt, dan wordt wat we beogen te beschermen ook uitgehold. Het komt aan op een zorgvuldig evenwicht en juist op dat punt heeft de fractie van de ChristenUnie op dit moment nog zorgen. Ik leg ze aan de ministers voor en geef hun vooraf mee dat de beantwoording voor ons zeer veel betekent voor ons uiteindelijke stemgedrag. Ik begin met het legaliteitsbeginsel. Het is zeer voorstelbaar dat opvolging wordt gegeven aan de aanbeveling van de commissie-Dessens om het onderscheid tussen kabel en ether bij interceptiebevoegdheden te laten vallen. Tegelijk vraagt dat wel om genoeg wettelijke waarborgen

om de proportionaliteit en de subsidiariteit te kunnen garanderen. Dessens heeft gepleit voor een techniekonafhankelijke formulering. Terugkijkend naar de Wiv 2002, zien we dat het is voorgekomen dat er bevoegdheden in stonden die door technologische ontwikkelingen een veel grotere reikwijdte kregen dan door de wetgever voorzien was. Neem bijvoorbeeld de analyse van grootschalig opgevangen ethergebonden telecommunicatie. Die was niet voorzien bij de wet in 2002 en kreeg een enorme vlucht. Dat schuurt met het legaliteitsbeginsel.

De nu gekozen techniekonafhankelijke formuleringen hebben als groot voordeel dat de diensten technisch bij kunnen blijven, maar voor mijn fractie is dit geen blanco cheque. Kan de minister toezeggen dat nieuwe technieken die worden toegepast of nieuwe technische hulpmiddelen die worden gebruikt die een andere of verdergaande inbreuk op de persoonlijke levenssfeer maken dan nu voorzien, een expliciet punt van aandacht worden van de vijfjaarlijkse evaluatie? Heb ik de minister goed begrepen dat de inzet van een bijzondere bevoegdheid nimmer het recht op de lichamelijke integriteit van personen zal schenden? Ik hoor dat graag straks nog eens expliciet. Al knikt de minister nu ja, voor de Handelingen is meer nodig.

Dan het sleepnet, zoals sommigen het noemen, of de onderzoeksopdrachtgerichte interceptie, zoals het in de wet staat. In de bezorgde mails die ik — ik begrijp inmiddels net zoals zo ongeveer deze hele Kamer — dagelijks in grote hoeveelheden ontvang, wordt het ook als de "sleepnetbevoegdheid" geduid. Bewaren de diensten niet te lang en te veel gegevens van burgers waar de diensten helemaal niks in te zoeken hebben? De minister heeft de motie-Recourt onderstreept waarin staat dat deze bevoegdheid zo gericht mogelijk wordt ingezet en dat bij een verzoek om toestemming voor de uitoefening van deze bevoegdheid nadrukkelijk de noodzakelijkheid, proportionaliteit, subsidiariteit aan de orde zijn. Bovendien vindt er na het oordeel van de minister nog een rechtmatigheidstoets plaats.

Mijn fractie heeft op twee punten zorgen bij dit wetsvoorstel. De ene ziet op de bewaartermijnen en de andere op de inrichting van het stelsel van toezicht en in het bijzonder de figuur van de toetsingscommissie. Allereerst de bewaartermijnen. Mijn fractie heeft moeite met de bewaartermijn van drie jaar voor gegevens die verzameld zijn door onderzoeksopdrachtgerichte interceptie. Artikel 48 geeft in het zesde lid voor versleutelde informatie bovendien nog de mogelijkheid dat het diensthoofd na de bewaartermijn van drie jaar verzoekt om verlenging en er zit geen slot op die deur. Wie of wat voorkomt nu dat informatie alsnog eindeloos bewaard wordt?

De voorbeelden in de memorie van toelichting die het nut moeten bewijzen van de driejaarstermijn gaan allen maximaal twee jaar terug in de tijd, niet verder. Bewaartermijnen van omliggende landen zijn volgens de minister op hoofdlijnen hetzelfde. Specifiek over de termijnen voor gegevens die voortkomen uit onderzoeksopdrachtgerichte interceptie wordt hij echter niet, ook niet in de bijlage die helemaal achterin die dikke memorie van toelichting zit. Kan hij de stelling dat de bewaartermijnen in de omliggende landen echt dezelfde zijn specifiek onderbouwen? Welke aanwijzingen heeft de minister bovendien dat Nederland hiermee stand kan houden bij het Europees Hof voor de Rechten van de Mens, mocht het tot een procedure komen? Is deze mogelijkheid ook niet strijdig met het advies in het privacy impact assessment om zo snel mogelijk de relevantie te beoordelen en de rest terstond te vernietigen? Deze gegevens kunnen namelijk gedurende de tijd dat ze bewaard worden ook aan andere diensten worden verstrekt. Hoe garandeert de minister dan dat de bewaartermijn op dat moment ook in stand blijft? Is dat een uitgangspunt bij de verstrekking aan andere diensten? Komt dat aan de orde of is dat überhaupt al een strijd waarvan de minister denkt dat hij die niet wint? Ik hoor daar graag meer over.

Dan de TIB, die eerder al is genoemd in dit debat, de Toetsingscommissie Inzet Bevoegdheden. Is dit nu de beste manier om vooraf onafhankelijk te toetsen? De Raad van State spreekt de vrees uit dat de toetsing zeer marginaal en slechts een abstracte rechtsmatigheidsbeoordeling zal zijn: de TIB als stempelmachine. Het ontbreekt aan rechtstreekse toegang tot gegevens en aan knowhow. Het beschikken over deze kennis en inzichten is echter onmisbaar om een weloverwogen oordeel over de noodzaak, proportionaliteit en subsidiariteit van de inzet van bijzondere bevoegdheden te vellen. Ik waardeer natuurlijk de uitbreiding van de financiële armslag en van de stevigheid ervan door de motie-Schouten, maar blijf de zorg houden dat het toezicht vooraf onvoldoende stevigheid kent. Wat gaat de minister doen met de TIB als meerdere malen blijkt dat het oordeel van de CTIVD na afloop anders uitvalt? Hoe informeert hij het parlement hierover? Al met al: waarom acht hij dit toezichtstelsel effectiever dan het voorstel dat de Raad van State deed? En hoe weet hij nu zeker dat deze constructie EHRM-bestendig is? De fractie van de ChristenUnie betwijfelt zeer of de TIB voor deze taak robuust genoeg is. Gaat de minister het toezichtstelsel trouwens ook kwalitatief evalueren, zodat duidelijk wordt of er voldoende kennis is en ruimte ervaren wordt om te oordelen dat een besluit onrechtmatig is? De fractie van de ChristenUnie deelt vooralsnog de overtuiging van de Raad van State dat toezicht over het geheel van activiteiten door de CTIVD effectiever zal zijn.

De Raad van State maakt bovendien terechte opmerkingen over de beperking van de politieke verantwoordelijkheid van de minister. De TIB geeft een soort alibi, terwijl de commissie alleen de juridische argumenten toetst en niet de politieke en internationale componenten. De Raad van State ontraadt deze keuze ernstig. Dat zijn stevige woorden. Het toevoegen van een lid met technische bagage, iets wat de regering heeft gedaan na het advies van de Raad van State, is dan onvoldoende. Naast ICT-deskundigheid is er ook expertise in veiligheidsvraagstukken nodig. Bovendien moet de expertise de eerste tijd worden opgebouwd in deze toetsingscommissie. Hoe ziet de minister die overgangstijd voor zich? Het moge duidelijk zijn: mijn fractie is nog niet overtuigd van de invulling van dit toezichtstelsel.

De fractie van de ChristenUnie zet bovendien vraagtekens bij de klachtenafhandeling en het verplaatsen van de behandeling van klachten over de veiligheidsdiensten van de Nationale ombudsman naar de CTIVD. Wij zetten die vraagtekens simpelweg omdat het in de weg staat aan de beleving van de burger dat dit een onafhankelijke klachtenbehandelaar is. De minister kan wijzen naar de Chinese muur die hij zal zetten tussen de afdelingen, maar de burger ziet dezelfde aftiteling als die van de toezichthouder als hij het gebouw in- of uitstapt. Bovendien is de CTIVD een onbekende voor veel burgers. Uit de schriftelijke behandeling bleek nog eens dat het om een handvol klachten gaat. Waarom voor de handvol klachten die het betreft, deze

rigoureuze wijziging? Is de burgerperceptie ook onderdeel van de evaluatie? Ik hoor de minister er graag over.

Ik kom tot mijn conclusie. Hoeveel vrijheid moet een burger inleveren om voor ons land te kunnen garanderen dat vrijheid en een stabiele rechtsorde de pijlers blijven? Het luistert heel nauw bij het bewaken van de balans tussen enerzijds de veiligheid en vrijheid die je krijgt, en anderzijds de privacy die je daarvoor moet opgeven. Het komt er voor de fractie van de ChristenUnie op aan dat er recht wordt gedaan aan het legaliteitsbeginsel, ook als de wet een opening blijkt te geven voor andere technieken dan op dit moment voorzien. We hebben zorgen bij de bewaartermijnen en de effectiviteit van het toezicht vooraf. En ten slotte vrezen we dat de klachtafhandeling niet meer als onafhankelijk wordt beleefd door de burger. Tegelijkertijd beseffen we dat de huidige wet nodig gemoderniseerd moet worden en dat de dreiging in deze tijd fors is. Juist daarom hoop ik dat de minister in zijn beantwoording recht weet te doen aan de moeite die we hebben met elementen uit dit voorstel.

☐

De heer **Van Hattem** (PVV):
Voorzitter. Onze inlichtingen- en veiligheidsdiensten zijn onmisbaar in de strijd voor onze nationale veiligheid, voor de veiligheid van onze bevolking. Islamitische terreuraanslagen zijn aan de orde van de dag. Onder andere Londen, Manchester, Brussel, Parijs, Berlijn, Nice en Stockholm zijn in de afgelopen tijd het bloedige toneel geweest van jihadistisch geweld tegen onze westerse samenleving. En deze week bleek dat net over de grens, in het Duitse Düsseldorf, een groot jihadistisch bloedbad verijdeld is. Islamitische terroristen die via de Balkanroute als vluchtelingen Duitsland waren binnengekomen en daar door de regering-Merkel waren opgevangen, wilden middels het zogenaamde Mumbaiscenario zo veel mogelijk slachtoffers maken in de binnenstad, de Altstadt van Düsseldorf. Net als bij de aanslagen op het hotel in Mumbai in 2008, waarbij 171 doden vielen, wilden zij eerst met zelfmoordaanslagen de mensenmassa paniek aanjagen, om de mensen vervolgens in de nauwe straatjes met machinegeweren massaal neer te schieten.

Dat dergelijke jihadistische terreur ook in Nederland kan plaatsvinden, is zeker niet ondenkbaar. Integendeel. In de afgelopen maand verscheen de publicatie Dreigingsbeeld Terrorisme Nederland van de NCTV. Hij stelt heel duidelijk dat een aanslag in Nederland, met name een jihadistische aanslag, reëel is en blijft. Met deze risico's is het van het grootste belang dat Nederland beschikt over een goed wettelijk kader voor de inlichtingen- en veiligheidsdiensten dat bij de tijd is.

De aanleiding tot het voorliggende wetsvoorstel komt mede voort uit de motie van het lid Elissen van de PVV-Tweede Kamerfractie, waarin werd opgeroepen tot een evaluatie van de Wet inlichtingen- en veiligheidsdiensten 2002 en goede toetsing van het toezicht bij deze wet.

De heer **Van Kappen** (VVD):
Ik heb een vraag aan de heer Van Hattem. Hij legt heel erg de nadruk op terroristische activiteiten van jihadisten, maar er is toch meer dan alleen jihadisme? De inlichtingen- en veiligheidsdiensten moeten ook in de gaten houden wat bijvoorbeeld het Rusland van mijnheer Poetin op dit moment doet, en zo zijn er nog wel een aantal andere voorbeelden. Is het niet wat eenzijdig om de activiteiten van de inlichtingendiensten uitsluitend te focussen op jihadistisch terrorisme?

De heer **Van Hattem** (PVV):
Het is zeker zo dat alle mogelijke bedreigingen voor onze nationale veiligheid gekanaliseerd moeten worden. Ik citeer alleen uit het Dreigingsbeeld Terrorisme Nederland van de NCTV, die heel nadrukkelijk stelt dat de jihadistische dreiging de meest bepalende dreiging voor Nederland is. Dus als we dan toch ergens de nadruk op moeten leggen, is het daarop. Het grootste risico is de jihadistische dreiging. Zo simpel is het. Zo stelt de NCTV het en daarop moeten we kunnen vertrouwen.

De heer **Van Kappen** (VVD):
De NCTV houdt zich natuurlijk bezig met terroristische activiteiten. Maar als ik praat over de activiteiten van Rusland of van andere landen die ons niet zo goed gezind zijn, zijn dat geen terroristische activiteiten. Dat is een dreiging van een heel andere orde. Maar ook daar zijn onze inlichtingendiensten natuurlijk voor bedoeld. Dat is het enige wat ik duidelijk wilde maken.

De heer **Van Hattem** (PVV):
Ik kan het alleen maar volledig eens zijn met de heer Van Kappen. Al die dreigingen moeten zeker in de gaten worden gehouden.

Voorzitter. Nadat de motie-Elissen in de Tweede Kamer was aangenomen, is de commissie-Dessens aan de slag gegaan. Die is tot de conclusies gekomen die uiteindelijk in dit wetsvoorstel zijn opgenomen. Dit wetsvoorstel behelst dat de AIVD en de MIVD de bevoegdheid krijgen om ook kabelgebonden telecommunicatie te onderzoeken, dat taken en diensten en de inzet van bevoegdheden van de AIVD en de MIVD nauwkeurig wettelijk worden vastgelegd, en dat voor een inzet van bevoegdheden toestemming van de minister en van de TIB nodig zijn, dat onafhankelijke toetsing vooraf ook voor de inzet van bestaande bijzondere bevoegdheden geldt en dat de CTIVD een zelfstandige klachtinstantie met bindende uitspraken wordt. Na uitvoerige afweging en bespreking is de Tweede Kamer met dit pakket uiteindelijk akkoord gegaan.

Vervolgens heeft de Eerste Kamer in haar voorbereiding een gesprek gehad met de CTIVD. Een van de punten die in dat gesprek naar voren kwam, is dat een aantal aspecten van deze wet voor de toepassing in de toetsing door de CTIVD nog verduidelijkt zouden kunnen worden. De vraag is daarom ook voorgelegd aan de minister om te zorgen dat dit zo veel mogelijk vanuit de bedoeling van de wetgever kan worden verduidelijkt, in plaats van dit in te vullen via rechtsvorming via de rechterlijke macht. De minister heeft op een aantal punten geantwoord. Alleen, op sommige onderdelen is er ook bewust gekozen om die invulling via de rechtsvorming te laten plaatsvinden. De vraag is hoe deze zal uitwerken.

Ten aanzien van dit wetsvoorstel zijn door burgers zorgen geuit over privacy en mogelijke aantasting van de persoon-

lijke levenssfeer. Uiteraard is het van fundamenteel belang deze aspecten te waarborgen. Daarmee is deze zorg niet onterecht. Desalniettemin zijn de nieuwe bevoegdheden in dit wetsvoorstel noodzakelijk.

Om de context van het onderzoeken van de kabelgebonden telecommunicatie te illustreren, het volgende voorbeeld. Bij de islamitische terreuraanslagen op een wijnbar in het Duits Ansbach vorig jaar en in een trein in Würzburg bleek communicatie via internet een cruciale rol te spelen. Deze jihadisten kregen via chatberichten direct commando's van een IS-commandant vanuit het Midden-Oosten. Toen bijvoorbeeld de jihadist in Ansbach een foto doorstuurde van het plein waar die avond een muziekfeest zou plaatsvinden met de mededeling dat het plein dan vol met mensen zou staan, was het jihadbevel per chat duidelijk. Ik citeer de Duitse media: "Töte sie alle." Töte sie alle; met zulke nietsontziende islamitische moordlust tegen de westerse samenleving is inlichtingenwerk bittere noodzaak, waarbij de diensten over geschikte middelen en bevoegdheden moeten beschikken om zulk soort internetchats te kunnen onderscheppen. De bevoegdheden tot het onderzoeken van kabelgebonden telecommunicatie kan de privacy van internetgebruikers raken, maar is wel met wettelijke waarborgen omkleed, zodat dit zo beperkt mogelijk blijft. Het niet meer veilig kunnen bezoeken van een muziekfeest, een wijnbar, een trein of een kerstmarkt is daarentegen een veel ernstigere aantasting van de persoonlijke levenssfeer, die onze vrijheid nog veel harder raakt.

Tegelijkertijd blijft cruciaal dat er ook voldoende focus is op de echte gevaren voor onze samenleving. Het is voor onze diensten nodig om bij het doen van onderzoek verbanden te kunnen signaleren die gevaren opleveren voor onze nationale veiligheid. Dan is het soms nodig om de context te kunnen verbreden. Doorgewinterde activisten en terroristen zijn immers getraind in het neutraliseren van statements, wetende dat ze getapt kunnen worden in hun communicatie. Ter illustratie hiervan een onderschept telefoongesprek tussen twee radicale dierenactivisten in januari 2002, waarbij de één zegt: "Fortuyn moet dood", waarop zijn gesprekspartner reageert met "Jongen, oppassen, monddood bedoel je." Juist om zulke gevaren goed in beeld te kunnen krijgen, moet rekening worden gehouden met zulke calculerende communicatie en zijn de nieuwe bevoegdheden van belang.

Bovendien is deze informatie alleen effectief en van waarde als vervolgens ook de verantwoordelijke instanties adequaat met deze informatie aan de slag gaan, bijvoorbeeld door een potentieel doelwit van een aanslag tijdig beveiligingsmaatregelen te bieden en door de mogelijke aanslagplegers tijdig aan te pakken. Nu zien we helaas nog te vaak dat de diensten informatie leveren, maar een verdachte vervolgens snel weer op vrije voeten is, bijvoorbeeld door een gebrek aan bewijs, zoals onlangs de "geradicaliseerde Amsterdammer", die in Eindhoven vermoedelijk mogelijkheden voor een jihadistische aanslag aan het verkennen was. Ook zolang we de grenzen wagenwijd openlaten, zullen inspanningen van onze diensten een gevecht tegen de bierkaai zijn.

De heer **Köhler** (SP):
Is het niet zo dat het oppakken van verdachten en het verder strafrechtelijk vervolgen een taak is van het Openbaar Ministerie? Dat zou toch geen taak van de veiligheidsdiensten moeten zijn?

De heer **Van Hattem** (PVV):
Dat zeg ik ook niet.

De heer **Köhler** (SP):
Dat suggereerde u wel, want u zei dat de diensten de verdachten adequaat zouden moeten aanpakken.

De heer **Van Hattem** (PVV):
Dan hebt u mij niet goed beluisterd. Ik heb gezegd: de verantwoordelijke instanties moeten adequater te werk gaan.

De heer **Köhler** (SP):
Ik ben blij dat u uw woorden nuanceert.

De heer **Van Hattem** (PVV):
Dat is geen nuance, het is wat ik letterlijk heb gezegd. Maar goed.

Zoals ik zei: zolang we onze grenzen wagenwijd openlaten, zullen de inspanningen van onze diensten een gevecht tegen de bierkaai zijn. Het gemak waarmee de aanslagpleger van Manchester vanuit IS-gebied ongestoord door Europa kon reizen, is hiervoor kenmerkend. Dat geldt evenzeer voor de vele andere islamitische terroristen die via de vluchtelingenstroom hierheen zijn gekomen. Grenzen dicht voor deze islamitische massa-immigratie is en blijft prioriteit nummer één.

Tot slot heb ik nog een vraag aan de minister. Volgens het wetsvoorstel zal de TIB bestaan uit drie leden, van wie ten minste twee rechters. Maar het derde lid kan ook een niet-rechter zijn, met andersoortige kennis en expertise. Kan de minister aangeven of hij bij de uitvoering van deze benoeming wil streven naar de benoeming van een niet-rechter als derde lid, zodat de expertise in de TIB diverser van aard zal zijn dan alleen vanuit de rechterlijke macht?

De heer **Köhler** (SP):
Voorzitter. Het recht op privacy is een grondrecht in onze democratische rechtsstaat. Dat is vastgelegd in artikel 10 lid 1 van de Grondwet: "Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer." De persoonlijke levenssfeer omvat onder meer communicatie via brieven, telefoon en internet. In het ook in Nederland van kracht zijnde Europees Verdrag voor de Rechten van de Mens staat in artikel 8, lid 1: "Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie". En in lid 2 staat: "Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid" enzovoorts. De genoemde artikelen in de Grondwet en het EVRM beschermen de burger tegen de overheid. Die bescherming is een van de belangrijkste kenmerken, zo niet het belangrijkste kenmerk,

van de democratische rechtsstaat. Natuurlijk is die bescherming niet absoluut. Zo mag de overheid om redenen van nationale veiligheid het communicatiegeheim schenden, maar dan wel met strikte wettelijke beperkingen. Kortom: alleen als dat noodzakelijk, proportioneel en subsidiair is.

Tegen die achtergrond heeft de SP-fractie het nu voorliggende voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten beoordeeld. Ons oordeel is dat de aantasting van de privacy in dit wetsvoorstel veel te ver gaat. Ik zal onze bezwaren op de volgende punten toelichten: het sleepnet, de uitwisseling van gegevens met buitenlandse diensten, het gebruik van zogenoemde kwetsbaarheden in software, de te beperkte bescherming van burgers bij realtimetoegang van gegevens van informanten en de onvoldoende bescherming van sommige beroepsgroepen.

Het wetsvoorstel opent de mogelijkheid dat de veiligheidsdiensten grote hoeveelheden elektronische communicatie van niet-verdachte burgers verzamelen, als was het met een sleepnet bijeenvegen, om daar later onderzoek naar te doen om te bezien of er misschien verdachte communicatie tussen zit. Dat is een ongerichte aantasting van de privacy van velen, die in deze wet wordt omschreven als "onderzoeksopdrachtgerichte interceptie". De vicevoorzitter van de Autoriteit Persoonsgegevens noemde dat in de hoorzitting van de Tweede Kamer terecht "het eufemisme van het jaar".

Mijn fractie ziet de noodzaak van dit soort verzameling van bulkgegevens niet. Waar dit al mogelijk is, in de Verenigde Staten van Amerika, is volgens onderzoek de effectiviteit ervan niet bewezen. Maar als het toch mogelijk wordt, zou het voor de rechtsbescherming van burgers nodig zijn om de noodzakelijkheid, de proportionaliteit en de subsidiariteit van een onderzoeksopdrachtgerichte interceptie van onze communicatie door een gespecialiseerde rechter te laten toetsen. Maar hier wil de minister, om ons niet-overtuigende redenen, niet aan. In plaats hiervan komt er, na de stroom van kritiek op de sleepnetbevoegdheid van de geheime diensten, een Toetsingscommissie Inzet Bevoegdheden, de TIB, die naast de minister toestemming voor zo'n operatie moet geven.

Mijn fractie vreest dat de TIB niet genoeg kennis en inzicht kan verwerven, onder meer door het ontbreken van onderzoeksbevoegdheden, om zo nodig tot een negatief oordeel te komen, temeer omdat de criteria waaraan een onderzoeksopdrachtgerichte interceptie moet voldoen, ontbreken en de minister weigert om die alsnog op te stellen. Vervolgens mogen de diensten de gegevens, na een eerste globale schifting, drie jaar bewaren om er verder onderzoek mee te doen. Met die zeer lange bewaartermijn van bulkgegevens komt het wetsvoorstel wel op heel gespannen voet te staan met het standpunt van het Europees Hof voor de Rechten van de Mens over artikel 8 van het EVRM. Kan de minister nog eens aangeven waarom hij zo ver wil gaan, anders dan dat het alleen een compromis is met de VVD, die de bewaartermijn eindeloos zou willen oprekken? Kan hij daarbij ook ingaan op artikel 48, vijfde lid van het wetsvoorstel, waarin staat dat deze bewaarde gegevens ook gebruikt mogen worden voor andere lopende onderzoeken? Dat betekent toch dat deze bulkgegevens ook niet-gericht, zelfs niet-onderzoeksopdrachtgericht, gebruikt mogen worden? En wordt de toets op de rechtmatigheid van het verzamelen van deze gegevens daarmee niet omzeild?

De nog niet onderzochte bulkgegevens mogen ook worden uitgewisseld met buitenlandse inlichtingen- en veiligheidsdiensten. En daarop is geen enkel voorafgaand toezicht. De SP-fractie is hier zonder meer tegen. Het kan grote gevaren inhouden voor onze burgers. Zeker als er geen restricties worden gesteld in het doel waarvoor en de tijdsduur dat deze gegevens gebruikt mogen worden. Er is dan geen enkele garantie ingebouwd dat die buitenlandse diensten die gegevens niet voor andere doelen zullen gebruiken dan waar ze in Nederland voor zijn verzameld.

Zo kan bijvoorbeeld de Turkse geheime dienst in bulkgegevens gaan zoeken naar de communicatie van vermeende Nederlandse Gülenaanhangers met mensen in Turkije. En zoals we weten kan dat in die falende rechtsstaat voldoende zijn om zonder proces gevangengezet te worden. Nu kan het zijn dat er met een land waar de democratische rechtsstaat verloren gaat, op een gegeven ogenblik dit soort bulkgegevens niet meer worden uitgewisseld, maar dat verhelpt dan niet dat gegevens die in het verleden zijn verstrekt, worden misbruikt.

Er zijn door de minister zogenoemde "wegingsnotities" toegezegd. Daarin wordt per land afgewogen of en in hoeverre er gegevens uitgewisseld mogen worden. Maar die notities zijn nog steeds niet af. Deze wet geeft de diensten toestemming om nog maximaal twee jaar zonder de eventuele beperkingen die in deze notities worden vastgelegd, gegevens met de bestaande samenwerkingspartners uit te wisselen. Mijn fractie vindt dit een onaanvaardbare gang van zaken.

Dit wetsvoorstel biedt de inlichtingendiensten expliciet de mogelijkheid om apparatuur van derden te hacken, om zich op die manier toegang te verschaffen tot apparatuur van concrete doelwitten. Hierbij kunnen veiligheidsdiensten gebruikmaken van zogenoemde kwetsbaarheden in software: foutjes in de software die nog niet zijn ontdekt door de fabrikant en daarom nog niet zijn verbeterd. In het kader van de nationale cybersecurity besteedt Nederland veel aandacht aan het zo snel mogelijk dichten van deze lekken in software, om te voorkomen dat kwaadwillenden er gebruik van maken en met hun aanvallen zelfs het hele land plat zouden kunnen leggen. Daarbij is het van groot belang dat onbekende kwetsbaarheden direct gemeld worden, waardoor de fabrikanten van de software het lek kunnen dichten. Maar de Nederlandse veiligheidsdiensten mogen deze onbekende kwetsbaarheden gebruiken om hun doelwitten in de gaten te houden, zonder dat ze deze hoeven te melden. Dat is een groot gevaar. Het is bekend dat het lek in Windows dat wordt misbruikt door zowel WannaCry als het onlangs opgedoken NotPetya, in handen was van de Amerikaanse veiligheidsdienst NSA en daar is uitgelekt.

Kan de minister nog eens uitleggen waarom hij het bewaren van deze mogelijkheden voor onze diensten om inlichtingen te verwerven, belangrijker vindt dan het bewaken van de cybersecurity, belangrijker dan de strijd tegen cybercriminaliteit in het algemeen? Wil hij ook uitleggen waarom er op het achterhouden van onbekende kwetsbaarheden door de diensten, met alle risico's van dien, geen enkele toetsing plaatsvindt, niet door de TIB, maar zelfs ook niet door de minister? Overigens is de minister wel bezig met een richtlijn voor het omgaan met onbekende kwetsbaarheden.

Wil hij deze richtlijn, desnoods vertrouwelijk, aan de Kamers voorleggen?

Ik kom bij enkele opmerkingen over het verkrijgen van realtimetoegang — excuses voor alle Engelse termen, maar ik citeer uit de wetgeving — door de diensten tot gegevensbestanden van informanten. Informanten zijn in dit verband bijvoorbeeld ziekenhuizen. De minister vindt dat minder ingrijpend dan het inzetten van een bijzondere bevoegdheid, omdat het bij realtimetoegang zou gaan om gegevens die reeds bij de informant voorhanden zijn. Maar de omstandigheid dat de gegevens al eerder met andere doeleinden zijn verzameld, maakt de inbreuk door de diensten op de rechten van burgers die hun gegevens aan deze instellingen hebben toevertrouwd, volgens ons niet kleiner.

Voor de burgers die het treft, maakt het immers niet uit op welke wijze de diensten deze gegevens vergaren: door de inzet van een bijzondere bevoegdheid of door realtimetoegang van een meewerkende partij. In beide gevallen vindt de gegevensvergaring heimelijk plaats. De burger heeft hier dus geen wetenschap van, laat staan zeggenschap over. Het enige verschil is dat bij de inzet van een bijzondere bevoegdheid een medewerkingsplicht voor de aangezochte partij geldt en bij de raadpleging van de aangezochte partij als informant niet. Dat verschil rechtvaardigt volgens mijn fractie niet waarom in het laatste geval een voorafgaande rechtmatigheidstoetsing door de TIB niet nodig zou zijn. Wil de minister nog eens uitleggen waarom waarborgen die wel gelden voor het vorderen van opgeslagen gegevens bij bijvoorbeeld een aanbieder van een communicatiedienst, niet van toepassing zijn bij het vergaren van dezelfde gegevens via de vrijwillige medewerking van dezelfde aanbieder?

Tot slot van mijn inbreng in eerste termijn nog enkele opmerkingen over de rechtsbescherming van een paar in het kader van deze wet bijzondere beroepsgroepen. Het wetsvoorstel bevat geen specifieke regels voor het verwerken en vernietigen van gegevens die door de inlichtingendiensten zijn verkregen door het uitoefenen van een bijzondere bevoegdheid en die betrekking hebben op de identiteit van een bron van een journalist. Die gegevens moeten volgens ons, net als de gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt, in principe terstond vernietigd worden. Waarom wil de minister dit niet in de wet opnemen?

In de wet heeft de rechter een rol bij de inzet van bevoegdheden tegen journalisten en advocaten. Wij vinden dat dat ook voor volksvertegenwoordigers moet gelden. Ook zij moeten hun werk vrijuit kunnen doen, tenzij er zeer zwaarwegende redenen zijn om hun communicatiegeheim te schenden. Waarom wil de minister het besluit om volksvertegenwoordigers te gaan bespioneren, niet aan de onafhankelijke rechter voorleggen?

De SP-fractie vindt het wetsvoorstel over de hele linie een te vergaande aantasting van de privacy van onze burgers. Maar ook voor de minister geldt: beter ten halve gekeerd dan ten hele gedwaald. Daarom zien we met belangstelling uit naar zijn reactie op onze opmerkingen en vragen.

☐

Mevrouw **Teunissen** (PvdD):
Voorzitter. Een overheid die luistert naar burgers. Wie wil dat niet? Maar als een overheid dat doet op een manier die zo groot en meeslepend is als we hier vandaag zien, moeten we ons ernstig afvragen of het middel niet veel erger is dan de kwaal. Zelden heb ik zo veel verontruste mails gekregen van bezorgde burgers als deze week. Dit zou zomaar ook het geval kunnen zijn voor heel wat collega's hier in de zaal die meer dienstjaren hebben in dit huis dan ik.

Het grootste bezwaar van mijn fractie is de bevoegdheid van het gebruiken van een sleepnet waarmee enorme hoeveelheden data van willekeurige burgers kunnen worden onderschept en opgeslagen. Waar diensten nu nog alleen gericht mogen aftappen, mogen ze straks werken met onderzoeksopdrachtgerichte interceptie. Daarmee kunnen de AIVD en de MIVD grote hoeveelheden informatie verzamelen over de kabel. Alle communicatie van grote groepen Nederlanders kan massaal worden onderschept door de geheime diensten. Alles wat je online doet, kan terechtkomen in het sleepnet van de geheime dienst.

Voor een goed draagvlak en voor controle moet er zo veel mogelijk transparantie zijn. Het wetsvoorstel regelt nauwelijks iets over de vraag welke informatie naar buiten kan worden gebracht of kan worden opgevraagd. Waarom is er zo veel onduidelijkheid over het delen van grote hoeveelheden gegevens? Hoe wordt voorkomen dat alle communicatie uit de buurt waar een verdacht persoon woont, kan worden getapt? Of dat alle Facebookberichten uit een bepaalde stad of wijk kunnen worden onderschept en jarenlang opgeslagen? Kortom, hoe wordt geborgd dat de onderzoeksopdrachten zo selectief mogelijk zijn? Aan welke criteria moeten de opdrachten voldoen? Ik verneem graag een reactie.

Het toezicht is ondergebracht bij verschillende instanties. Verschillende collega's refereerden daar al aan. Voorafgaand aan de inzet van bevoegdheden wordt getoetst op rechtmatigheid door de nieuwe TIB. Achteraf wordt de inzet van die bevoegdheden die voorafgaand door de minister of het hoofd van dienst zijn verleend, getoetst door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. Daarbij is de vraag wie wie controleert. Hoe weten we wat de toetsingscriteria zijn en of de toetsingskaders in de praktijk functioneren zoals in de wet staat? In de praktijk moet nog veel duidelijk worden over de werking van het toetsingskader. Het is dus zeer de vraag of de rechtmatigheid op losse schroeven wordt gezet voor aanvang van de praktijk. Ik krijg graag een reactie van de minister op dit punt.

Meer en meer informatie wordt gedeeld met buitenlandse diensten. Daarbij hoeft niet vooraf getoetst te worden of gegevens uitgewisseld mogen worden zonder dat de diensten die zelf geanalyseerd en getoetst hebben. Men weet niet precies waar de gegevens die aan het buitenland verstrekt worden over gaan. De gevolgen hiervan voor burgers op wie deze gegevens betrekking hebben, zijn momenteel niet te overzien. Waarom is een analyse voorafgaand aan het delen met buitenlandse diensten niet verplicht gesteld? Wat kunnen voor burgers de risico's zijn van het ongetoetst delen van informatie? Welke garantie kan de minister geven dat gegevens van burgers niet voor andere doeleinden

worden gebruikt dan waarvoor deze bedoeld waren? Ik krijg daarop graag een reactie.

Tot slot; ik houd het kort. In dit wetsvoorstel weegt volgens de fractie van de Partij voor de Dieren het doel, de modernisering van de inlichtingen- en veiligheidsdiensten, niet op tegen de risico's op inbreuk op de privacy. Mijn fractie kan niet instemmen met het voorstel dat nu voorligt, zo zeg ik tegen alle collega's en iedereen die meeluistert in welk kader dan ook, maar wacht met belangstelling de beantwoording door de ministers af. Mogelijk zal zij nog op basis daarvan haar oordeel herzien.

De **voorzitter**:
Dank u wel, mevrouw Teunissen.

De beraadslaging wordt geschorst.

De **voorzitter**:
Ik schors de vergadering in afwachting van de staatssecretaris van Onderwijs, Cultuur en Wetenschap. Er is inmiddels contact geweest met het ministerie van Onderwijs. We hebben begrepen dat de staatssecretaris om 16.20 uur hier aanwezig kan zijn.

De vergadering wordt van 15.57 uur tot 16.21 uur geschorst.

Voorzitter: **Broekers-Knol**