9
Privacy en toezicht op de inlichtingen- en veiligheidsdiensten

Aan de orde is **het beleidsdebat over de rol van de overheid bij digitale dataverwerking en –uitwisseling II; privacy en toezicht op de inlichtingen- en veiligheidsdiensten (CVIII)**.

De **voorzitter**:
De minister van Binnenlandse Zaken en Koninkrijksrelaties heb ik al eerder verwelkomd. De minister van Defensie heeft gevraagd of ik haar wil excuseren wegens zeer dringende verplichtingen elders. De voorzitter van de commissie voor Veiligheid en Justitie en de woordvoerders bij het beleidsdebat hebben daar gehoor aan gegeven en dat verzoek geaccordeerd. De minister van Defensie is derhalve niet aanwezig bij dit debat.

De beraadslaging wordt geopend.

□

De heer **Franken** (CDA):
Voorzitter. Bij het begin van dit debat wil ik graag de naam van onze helaas inmiddels oud-collega Willem Witteveen noemen. Hij was een van de initiatiefnemers voor het debat dat vandaag plaatsvindt. Ik heb het voorrecht gehad om Willem ook in mijn universitaire functies als collega te mogen meemaken. In onze overeenkomstige leeropdrachten op het terrein van de rechtstheorie hielden wij met overtuiging een gezamenlijke lijn aan, waaraan hij door zijn belezenheid en eruditie extra kleur heeft gegeven. Ik ben hem dankbaar voor de stimulerende contacten.

In de tweede plaats wil ik graag de medewerkers van het Rathenau Instituut en de staf van I&A en JBZ van onze Eerste Kamer bedanken voor hun actieve ondersteuning bij de voorbereiding van dit debat.

Op 5 juni vorig jaar publiceerden The Washington Post en The Guardian een geheim bevel van de Amerikaanse overheid waarin aan telefoonmaatschappij Verizon werd opgelegd om aan de National Security Agency (NSA) gegevens te verstrekken van alle Amerikaanse nationale en internationale telefoongesprekken "on an ongoing basis". Op 6 juni openbaarden deze kranten het bestaan van het NSA-programma onder de codenaam PRISM, waardoor de NSA vrijelijk kan grasduinen in gegevens van burgers die zijn opgeslagen bij bedrijven als Microsoft, Google, YouTube, Facebook, Yahoo en Skype. Drie dagen later verscheen een interview met Edward Snowden; uit door hem geopenbaarde documenten bleek vervolgens dat de NSA op grote schaal telecommunicatie van Europese bondgenoten onderschepte. In Nederland zouden in december 2012 1,8 miljoen sets metadata zijn verzameld. Uit een door de staf van het EU-parlement opgesteld overzicht blijkt dat ook al bij reeds langer actieve programma's — ik denk dan in het bijzonder aan ECHELON — de fundamentele rechten van niet-Amerikanen volstrekt worden genegeerd.

Nu is de surveillance van bepaalde volken of bevolkingsgroepen, ook door liberale regimes, niet iets heel nieuws. Wel is de schaalgrootte van de datasurveillance vele malen groter dan voorheen voor mogelijk werd gehouden. De technologische ontwikkelingen van de telecommunicatie, inclusief mobiele telefoons, internet, satellieten en meer in het algemeen alle data die kunnen worden gedigitaliseerd en geïntegreerd in "platforms", hebben geleid tot de mogelijkheid om een volstrekt onvoorziene hoeveelheid data te verzamelen, te bewaren, te ordenen en te doorzoeken. Een hoeveelheid die miljoenen malen groter is dan het Stasi-archief ooit is geweest.

Verder zien we dat de nieuwe technologieën er zijn en dat zij "daarom" worden gebruikt — zoals dat ook vaak met nieuwe wapens het geval is — zelfs om de leiders en diplomatieke vertegenwoordigingen van de meest trouwe bondgenoten af te luisteren. De Duitse minister van buitenlandse zaken heb ik dan ook horen zeggen dat de Amerikaanse overheid hiermee het vertrouwen van haar beste bondgenoot heeft verspeeld. De heer Steinmeier gebruikte weliswaar het woord "eroded", maar hij kan dat niet anders dan in deze zin hebben bedoeld. Het blijkt dat de Amerikaanse overheid een verschil maakt tussen eigen onderdanen en instituties en niet-Amerikaanse personen en instituties. Voor een dergelijk onderscheid zouden volgens de Amerikaanse wetgeving nog wel redenen kunnen worden aangevoerd, maar inmiddels hebben wij gelezen dat ook de communicatiesystemen van de eigen senatoren door de CIA of de NSA zijn gehackt. Het is overduidelijk dat ook wij in een surveillancemaatschappij leven.

De laatste constatering heeft niet alleen consequenties voor de privacy van burgers; daarmee wordt ook bevestigd dat er schade wordt geleden wegens industriële spionage — onlangs door minister Plasterk geschat op zeker 2 miljard euro voor de Nederlandse industrie — en dat onze kwetsbare infrastructuur wordt bedreigd.

Nu kan ik mij voorstellen dat nieuwe of andersoortige bedreigingen voor onze veiligheid leiden tot nieuwe of andersoortige beveiligingsmaatregelen en daaraan aangepaste bevoegdheden. Dat is op zich niet nieuw. Spionnen oefenen, zoals wel wordt gezegd, het op een na oudste beroep van de wereld uit. En het is nodig nieuwe technieken te gebruiken om inlichtingen over potentiële vijanden te vergaren. Wij kunnen niet meer volstaan met "een vent onder een bed of een man met een gleufhoed" en ook niet meer met het in beperkte mate onderscheppen van het berichtenverkeer. Wij zullen ook data en het dataverkeer moeten analyseren. De vraag is echter: wat is nog verantwoord en wat is eigenlijk effectief?

De extreme toename van het dataverkeer heeft geleid tot ongeveer 10 biljoen sms'jes per dag en tot enige tientallen miljarden e-mails die dagelijks worden verzonden. Daarvan kan men er wel veel bewaren, maar het is onmogelijk die hoeveelheden adequaat te verwerken. Het schijnt dat de NSA ongeveer 20 miljoen e-mails, oftewel 6 miljard metadata per dag, opslaat, maar niet meer dan 0,01% van het opgeslagen verkeer kan analyseren. En dat voor een organisatie met een — naar de deskundigen ons zeggen — jaarlijks budget van $52 miljard. Zoeken in deze massa is het zoeken van een druppel in de oceaan. Het levert dus bar weinig op. In de VS zijn maar enkele voorbeelden genoemd van zaken die met behulp van de verzamelde metadata zouden zijn opgelost en deze voorbeelden zijn volgens een door ons gehoorde deskundige ook nog onjuist. Ik beschik over literatuur waarin dit wordt bevestigd. Ik ben benieuwd of de minister naar aanleiding van de door de

regering steeds sterk aangeprezen dataretentie Nederlandse voorbeelden kan noemen.

Een tweede probleem met betrekking tot de opsporing betreft de convergentie van de infrastructuren. Telefoon, tv, e-mail en Twitter vormen een steeds groter wordende massale berg, waarbij burgers door middel van diverse IP-nummers tegelijk met behulp van verschillende netwerken kunnen communiceren, en dus in feite verschillende namen hanteren. Opsporingsacties zijn dus gemakkelijk te omzeilen.

Een volgend punt is dat overheden, en ook de Nederlandse overheid, altijd de kritiek op het grootschalig bewaren van metadata hebben getracht te sussen door te zeggen dat zij niet kijken naar de inhoud, de content, maar dat alleen de verkeersgegevens worden bewaard. In het rapport van Koops en Smits is duidelijk aangetoond dat verkeersgegevens wel degelijk vallen onder "vertrouwelijke informatie" zoals bedoeld in artikel 13 van de Grondwet en dus als persoonsgegevens moeten worden beschouwd. Het is tegenwoordig ook wel algemeen aanvaard dat de digitale enveloppe meer bevat dan alleen de namen van de afzender en de geadresseerde, maar ook te zien geeft waar en op welk moment zij zich ergens bevinden, wat hun bewegingspatronen zijn, wat hun positie in sociale netwerken is, enzovoorts. Daarom kunnen metadata zeer privacygevoelig zijn. Het maken van profielen blijkt een voor de burger zeer bedreigende bezigheid. Iemand kan een identiteit opgelegd krijgen die in werkelijkheid niet bij hem hoort en waardoor hij ten onrechte onder een bepaalde verdenking kan vallen.

Ten slotte merk ik in dit verband op dat het vergaren van data meer zal worden bemoeilijkt door het toepassen van privébeveiligingsmethoden en encryptietechnieken. Natuurlijk zijn er ook mensen die een modern nudistenbestaan leiden door hun hele hebben en houden op bijvoorbeeld Facebook te plaatsen, maar zij doen dat op eigen risico. Er zijn ook anderen, niet alleen overheden maar vooral ook bedrijven, die graag willen dat alleen de door hen uitgekozen geadresseerde hun bericht leest. En dan is daar weer een valkuil, want de leverancier van het encryptieprogramma kan aan de grote klant Google of de overheid een achterdeurtje aanbieden om in het beveiligde systeem van de burger binnen te komen. Uw geheim is dus maar schijn!

We zien dus dat de effectiviteit van de verzamelwoede van overheidsdiensten en bepaalde bedrijven helemaal niet is aangetoond en ook dat de techniek van het maken van profielen buitengewoon gevaarlijk is, omdat daarmee bepaalde identiteiten aan personen worden toegedeeld, die daarvan niet op de hoogte zijn. Bovendien zijn de diensten machtig en ongevoelig voor enigerlei controle, zoals ook het Amerikaanse voorbeeld van het door de CIA/NSA hacken van de systemen van "eigen" senatoren aangeeft. Zij vormen inmiddels "een staat in de staat".

Nu zou men zich kunnen afvragen of het nog wel zin heeft om je tegen zo'n overmacht te verzetten. Ik citeer een uitspraak van de executive chairman van Google, Eric Schmidt, uit 2013: "There's been spying for years, there's been surveillance for years, and so forth, I'm not going to pass judgement on that, it's the nature of our society". Is de "nature of our society" inderdaad zo veranderd dat we moeten accepteren dat we leven in een surveillancestaat of zelfs een controlestaat? De technologie bestaat en het gebruik daarvan is een feit en we zijn als Nederlanders naïef als we die niet gebruiken, is dan de stelling. En de overheden doen het allemaal voor onze veiligheid. Maar, zo vraag ik mij dan af, hoe veilig willen wij zijn? Ik spreek Rousseau na wanneer ik zeg: het is pas echt veilig als we allemaal alleen in een kerker zitten.

Dat soort veiligheid kunnen we bewerkstelligen met een orwelliaans Ministry of Love, waarin het hoofdkwartier van de gevreesde Thought Police is gevestigd. Ik geef met mijn fractie echter de voorkeur aan een uitspraak van de beroemde chef van de CIA uit de jaren vijftig en zestig, Allen Dulles: "Our government in its very nature, and our open society in all its instinct, under the Constitution and the Bill of Rights automatically outlaws intelligence organizations of the kind that have developed in police states."

Wij erkennen in het "vrije Westen", en dan denk ik maar aan de EU, nog steeds het fundamentele recht van de burger op vrije meningsuiting, op bescherming van de persoonlijke levenssfeer en op de mogelijkheid van vertrouwelijke communicatie. Deze rechten zijn verworven in een lang historisch proces. Ik denk aan de Magna Charta, Verenigd Koninkrijk 1215, de Declaration of Independence, Verenigde Staten 1776, en de Déclaration des droits de l'homme et du citoyen, Frankrijk 1789. Bij deze verklaringen is het uitgangspunt dat burgers rechten hebben en dat zij vervolgens de overheid toestaan op deze rechten beperkingen toe te passen als dat nuttig en noodzakelijk is voor het gemeenschappelijk belang.

Wij zullen dus een plaats moeten bepalen op een continuüm waarbij het ene uiterste de kerker is, dus absolute veiligheid met totale onvrijheid, en het andere uiterste een letterlijk vogelvrij bestaan. Voor het maken van een keuze tussen deze twee grootheden speelt een derde begrip een rol: vertrouwen. In een politiestaat wantrouwt de overheid de burger en vice versa. Wanneer wij, zoals Dulles, willen leven onder een constitutie waarin respect voor mensenrechten is opgenomen, zal de burger een beperking van zijn vrijheid ten behoeve van een grotere veiligheid accepteren. De overheid zal het daaraan ten grondslag liggende vertrouwen echter niet krijgen wanneer onder het mom van terrorismebestrijding die vrijheid zonder meer wordt beperkt door met name uitgebreide surveillance met programma's van datamining en profilering. Wanneer zulke programma's zonder nadere motivering worden gehanteerd, kunnen we ook niet meer spreken van een balans tussen veiligheid en privacy, maar tasten de veiligheidsmaatregelen de democratie aan. De behoefte aan veiligheid is niet hetzelfde als de instemming van de burger met het ongemotiveerd beperken van zijn grondrechten. Veiligheidsmaatregelen dienen daarom te worden gelegitimeerd met behulp van een verantwoordingsplicht van de overheid. Zij moeten zijn gebaseerd op een formele wet en een motivering waarmee nut, noodzaak en proportionaliteit worden aangetoond. Maar we zijn het overzicht en de controle verloren en we hebben, nog afgezien van de rechtmatigheidsvraag, geen publieke discussie over de doelmatigheid en proportionaliteit van het ongebreidelde datagraaien dat nu plaatsvindt.

Ook de politieke aansturing is onduidelijk. Het Europees Parlementslid Claude Moraes bepleit in een LIBE-rapport een "Digitale Habeas Corpus", met instrumenten die ervoor moeten zorgen dat de burger enigszins de controle op de verzameling van zijn persoonlijke data terugkrijgt. Daarbij zou Europa een onafhankelijke IT-strategie moeten ontwik-

kelen. Het land waar de servers staan, heeft immers de macht in handen. Ik ben benieuwd naar de visie van de regering daaromtrent. Ook de VN High Commissioner for Human Rights, Navi Pillay, heeft eind juni 2014 een rapport uitgebracht over massasurveillance. Graag verneem ik het commentaar van de ministers ook op dit rapport.

Wanneer we ons nu, in verband met de beperkte spreektijd, beperken tot de Nederlandse situatie, heb ik nog een aantal concrete vragen. Let wel: een goed werkende intelligence service acht mijn fractie een must, maar dat wil zeggen een intelligence service die dienstbaar is aan een democratische samenleving, dus een intelligence service die is geplaatst onder de checks-and-balances van een parlementaire en justitiële controle.

Gelukkig kunnen wij, voor zover we dat nu kunnen beoordelen, over onze Nederlandse diensten tevreden zijn. Het is niet gebleken dat zij zich niet aan de wet houden. Toch zullen wij een nieuwe Wiv nodig hebben, nu de wet uit 2002 door de techniek is achterhaald. Dat betekent een Wiv die bestaat uit techniekonafhankelijke formuleringen, omdat hij niet meer verwijst naar instrumenten die snel obsoleet zullen raken, maar is gericht op het gebruik van diverse middelen en technieken en de bevoegdheden van de gebruiker.

Hierbij past meteen de vraag: wat is de opvatting van de bewindslieden over het idee van professor Jacobs om ongericht zoeken zowel via satelliet als kabel mogelijk te maken, waarbij alleen bepaalde gegevens volgens transparante criteria worden geselecteerd en voor een bepaalde periode worden bewaard, terwijl de rest ongemoeid wordt gelaten? Dit is dus ruimer dan gericht zoeken, zoals dat nu mogelijk is, maar meer beperkt dan geheel ongericht zoeken. Het komt mijn fractie overigens ongewenst voor wanneer ISP'ers door de overheid zouden worden gedwongen om gegevens om andere dan strikt bedrijfsmatige redenen te bewaren. Ik verwijs hiervoor naar het rapport van de VN-rapporteur Navi Pillay en naar de uitspraak van het Hof van Justitie van de EU over de dataretentie. Ik verbaas mij er nog steeds over dat de regering een onrechtmatig verklaarde wet handhaaft. Ik wil graag horen waarom dat het geval is.

Kan de minister verder aangeven wanneer er in de huidige situatie sprake is van notificatie van zoekactiviteiten? Is hij het ermee eens dat notificatie van een toe te passen surveillance als uiting van transparantie zal bijdragen aan het vertrouwen van de burger in de overheid?

Volgens het huidige artikel 24 Wiv is gericht hacken, met last, toegestaan. In hoeverre is dit "gericht zijn" beperkt? Komt ook grootschalig verspreiden van malware door de diensten voor en, zo ja, onder welke voorwaarden gebeurt dit? In hoeverre is een vergelijking met undercoveractiviteiten juist? Is de minister bereid om te stimuleren dat de inlichtingendiensten kwetsbaarheden in de systemen van burgers of bedrijven aan de betrokkenen melden, wanneer zij daarop zijn gestuit? Ik zou een verhaal kunnen houden over de zero-day-exploits, maar dat zal ik nu achterwege laten. Misschien kan ik dat na het antwoord nog debiteren.

Democratische controle op onze inlichtingen- en veiligheidsdiensten vindt plaats door een onafhankelijke toezichthouder, de CTIVD, en door het parlement, waarbij de zogenaamde commissie-stiekem een belangrijke rol speelt. Mijn fractie schaart zich in grote lijnen achter de voorstellen, die de commissie-Dessens met betrekking tot dit onderwerp doet. Het verdient aanbeveling voor de bemensing van de commissie-stiekem de expertise van de leden als doorslaggevend criterium te hanteren en ook eens aandacht te geven aan de situatie in het Verenigd Koninkrijk en Duitsland, waar parlementariërs worden toegelaten tot controle op het operationele niveau van de diensten, waarmee zo veel mogelijk publieke verantwoording wordt afgelegd.

Ten aanzien van de CTIVD onderschrijft de CDA-fractie van harte het voorstel dat de rechtmatigheidstoetsing, die is gericht op het voldoen aan wet, proportionaliteit en subsidiariteit, moet worden uitgebreid met een toetsing van de doelmatigheid van de acties van de diensten. Immers, nut en effectiviteit van een maatregel kunnen pas dan werkelijk worden beoordeeld wanneer de actie in volle omvang door de toetsende instantie kan worden bezien. Juist ook voor maatregelen die preventief kunnen werken — te denken valt aan "privacy enhancing technologies" en "human rights by design" — is een volle toetsing onontbeerlijk.

Met betrekking tot het werk van de CTIVD wil ik er nog nadrukkelijk op wijzen dat afspraken met buitenlandse organisaties ook toetsbaar moeten zijn. Wij willen immers dat Nederlandse waarden worden gerespecteerd. Dit moet contractueel worden vastgelegd.

Naast de parlementaire controle dient ook er een "judicial review" mogelijk te zijn — ik verwijs naar het rapport van de Venice Commission uit 2007 — waardoor de burger zich kan verweren tegen onterechte verdenkingen. Ik wijs hier op de "blacklisting" activiteiten, die op mondiale en Europese schaal plaatsvinden. Graag hoor ik het commentaar van de minister hierop en een vermelding van de bestaande mogelijkheden van beroep.

Sprekend over toezicht moeten we overigens de inlichtingen- en veiligheidsdiensten niet alleen als doelgroep zien. Ook de Nationale Politie, oftewel "de grootste tapper van Nederland", die met betrekking tot telefoontaps zelfs de VS ver achter zich laat, de FIOD en de Belastingdienst zijn grote verzamelaars van persoonsgegevens. Hoe stelt de regering zich hier op? Daarbij denk ik in het bijzonder aan het feit dat de CIOT-database ongecontroleerd wordt gebruikt. Er wordt geen "loglisting" bijgehouden, zodat niet bekend is wat de politie met deze gegevens doet. Daarover wordt al jaren geklaagd, evenwel zonder resultaat. Gaarne vandaag een antwoord van de bewindspersoon op mijn vraag hoe de situatie is.

Ten slotte een opmerking over de wetstechniek. Het gaat om een belangrijk en gevoelig onderwerp, waarbij technologie is betrokken die aan snelle en ingrijpende veranderingen onderhevig is. Daarom moeten beide Nederlandse inlichtingen- en veiligheidsdiensten worden geïntegreerd en is een nieuwe Wiv noodzakelijk. Deze nieuwe wet zal rigoureuze horizonbepalingen moeten bevatten, rigoureus, omdat de uitoefening van bevoegdheden wordt gekoppeld aan een bepaald, beperkt budget. Voor enkele onderwerpen zal met een korte evaluatietermijn moeten worden gewerkt. De maatregelen, of ze nu op technisch, organisatorisch of juridisch niveau plaatsvinden, dienen aan transparante procedures te voldoen. Wij willen immers een "open society", waarin democratische controle mogelijk is en niet de technologie onze handelingen bepaalt. Wij willen dat de technologie op een redelijke manier wordt gebruikt, met

de rule of law als fundament voor het handelen van de overheid. Wij willen dat ons parlement beoordeelt of de vorm, de schaal en de diepgang van de surveillance past in onze democratie. Daarbij zullen we onze grondwettelijke rechten als basis nemen en de onschuldpresumptie blijven hanteren. Verdenking dient te worden gerelateerd aan een specifieke delictsomschrijving en niet aan een toevallige gedraging of leefstijl. Naast de vraag wat kan, zullen wijzelf moeten bepalen hoe de overheid deze kennis en kunde dient te gebruiken. Voor onze veiligheid zullen wij offers moeten brengen, maar wij kiezen voor een plaats op de balans waarbij we onze vrijheid niet tegen elke prijs zullen verkopen.

Mevrouw **Gerkens** (SP):
Voorzitter. Ik zou ook willen beginnen met een herinnering aan Willem Witteveen, eigenlijk de aanstichter van dit debat. Toen ik de stukken gisteren nog een keer las, kwam ik een aantal van zijn opmerkingen tegen. Wij missen hem vandaag zeer.

Privacy, wat is het nu eigenlijk en wat is het waard? Privacy is een woord dat een gedevalueerde betekenis heeft. Vaak wordt privacy verbonden met strijders voor het recht van vrijheid van meningsuiting en mensen die vinden dat niemand iets over ze mag weten. Een betrekkelijk kleine groep mensen lijkt zich druk te maken over de privacy en daarmee voelt menig dataverzamelende organisatie zich gelegitimeerd zo veel mogelijk informatie over mensen te verzamelen.

Op 3 september nam ik deel aan de "privacy as innovation workshop" op het Internet Governance Forum 2014. Aan deze workshop namen ook jongeren deel die voorbeelden noemden van goede privacybeschermende diensten. Vol vreugde werd Facebook genoemd, want daar kon je instellen naar wie je wat wilde sturen, en Messenger, de nieuwe app van Facebook, evenals WhatsApp. Dit waren jongeren die zich van te voren hadden voorbereid op de workshop en dus geacht werden meer te weten van privacyaspecten dan andere jongeren. Facebook, dat bijhoudt op welke websites je nog meer geweest bent en dat je door middel van datamining specifieke reclame aanbiedt. Messenger en Whatsapp, ze hebben toegang tot al je data op je telefoon, je wifiverbinding, je foto's, je camera. Kortom, ze kunnen je hele mobiele telefoon compleet overnemen. De eerst wat geschrokken jongeren haalden even later hun schouders op, want wat maakt het eigenlijk uit dat Facebook alles van mij kan zien? Wat maakt het uit?

Dat is de vraag die het privacydebat overheerst. Wat maakt het uit dat ze wat van mij weten? Ik heb niets te verbergen. Ik zie de staatssecretaris knikken. Hebben we onze privacy dan opgegeven in deze samenleving? Is de privacy iets van oude tijden? Worden wij te oud en maken we ons druk om onzinnige zaken? Heeft de komst van internet gezorgd voor het verdwijnen van onze privacy en moeten we dat gewoon maar gaan accepteren? Naar mijn mening hebben velen de privacy al eerder opgegeven. Met de komst van shows als Big Brother, The Kardashians en De Grote Donorshow op tv gingen we op zoek naar de grens van wat we liever achter de gordijnen wilden houden. Niet omdat wij iets te verbergen hebben, maar omdat we heel benieuwd zijn naar wat anderen te verbergen hebben. Het laten varen van privacy op internet is de nieuwe manier van roddelen geworden. Tegelijkertijd gaf ons dit de kans tot een nieuw soort openheid, namelijk laten zien hoe leuk, fijn, gelukkig, netjes en gezellig het leven wel niet is, door ons leven te posten op internet. De jeugd begint te beseffen dat het hebben van dronkenschapsfoto's op internet in hun generatie juist heel normaal is en dat het dus, wanneer ze een baan zouden gaan zoeken, eerder vreemd dan normaal gevonden wordt wanneer er niet zo'n uitspatting op internet te vinden is.

Het "niets te verbergen"-adagium gaat er vanuit dat het fout is wanneer je wél iets te verbergen hebt. Ik heb niets te verbergen wat niet mag van de overheid, ik ben geen crimineel of terrorist, dus deze beker gaat aan mij voorbij. Dit wordt uitstekend geëtaleerd door de website GeenStijl, waarop de volgende zinsnede is opgenomen in een artikel over het plaatsen van foto's van jongeren die zwanen hadden gemolesteerd. Ik citeer: "Potentieel gajes zou nu toch wel kunnen weten: een camera is nooit ver weg. Een paar miljoen mensen lopen met een mobiel NSA/B-device (doorkruisen naar voorkeur) in hun broekzak/bh/hoofddoek rond. Privacy schmivacy, in dit geval moet je maar geen zwanen pesten."

Die stelling is pertinent fout en ik wil deze hier met alle kracht weerleggen. Heeft de jongen die een relatie heeft met een andere jongen, maar het zijn ouders nog niet durft te vertellen, recht op zijn proces om uit de kast te komen? Ja. Heeft hij zolang recht op privacy als hij zelf wil? Ja. Heeft de vrouw die mishandeld wordt door haar man en stiekem geld spaart om bij hem weg te gaan, recht op privacy? Ja. Heeft de man die solliciteert naar een andere baan en dat nog niet verteld heeft aan zijn baas om de werkverhouding niet te verstoren, recht op privacy? Ja. Hebben deze mensen iets te verbergen? Inderdaad. Maar verkeerd is het niet.

Ik ga een stap verder. Heeft The Guardian het recht om zijn bronnen te verbergen, zodat klokkenluiders misstanden aan de kaak kunnen stellen? Heeft de politieke dissident iets te verbergen wanneer hij zijn vrije mening uit om een totalitair systeem aan te pakken? Heeft de homoseksueel iets te verbergen in een land waar dit met de doodstraf bestraft wordt? Heeft een bedrijf het recht, zijn nieuwste uitvinding te verbergen wanneer het nog geen patent heeft kunnen aanvragen? Heeft een organisatie het recht, haar offerte te verbergen bij een aanbesteding? Doen zij iets verkeerd?

De bescherming van privacy is een grondrecht. In artikel 10 van de Grondwet staat dit recht geschreven en ik loop echt niet op de discussie vooruit wanneer ik zeg dat de overheid hier schromelijk faalt, deels verwijtbaar en deels niet-verwijtbaar. Niemand kon twintig jaar geleden voorzien hoe enorm internet op ons privéleven zou inbreken. Nog minder konden we weten dat burgers op zo eenvoudige wijze informatie zouden weggeven, maar het feit dat die informatie op dusdanige wijze gebruikt zou worden dat de aangeboden dienst al weet dat je in verwachting bent voordat je het zelf weet, enkel en alleen door het analyseren van jouw patroon op internet, dat wisten we al helemaal niet. In plaats van dit een halt toe te roepen, in te grijpen en het een serieuze aanpak te gunnen, zag de overheid een nieuwe kans, want wat Google, Facebook, Microsoft et cetera kunnen, dat kan de overheid ook.

Informatie- en communicatietechnologieën zoals het internet zijn binnen een relatief kort tijdsbestek het zenuwstelsel van onze moderne economie, cultuur en maatschappij

geworden. Bijna alle facetten van onze samenleving worden via het internet geregeld. In toenemende mate maakt ook de overheid gebruik van de digitale mogelijkheden. In 2016 moeten alle overheidsdiensten digitaal worden aangeboden. In toenemende mate zijn diensten van de overheid alleen nog digitaal te bereiken. Dat vraagt een enorme inspanning van de zijde van de overheid om deze data goed te beschermen. Dat vraagt ook een enorme inspanning van de overheid om de privacy te beschermen van degene van wie zij data heeft.

Kan de regering deze Kamer ervan verzekeren dat zij haar taak zoals gesteld in artikel 10 van de Grondwet kan waarmaken? Ik denk het niet. Sterker nog, ik weet van niet. Bij de invoering van de Wmo en de Jeugdwet komen mij verontrustende geluiden ter ore. Een minister die zegt: we ontwerpen de privacy gaande het proces. Een gemeente die aan de cliënt vraagt om haar huisarts te vragen, even haar hele medische dossier toe te sturen, want dat is makkelijker. Gevoelige, zeer gevoelige informatie in het kader van deze twee wetten wordt straks beheerd door gemeenteambtenaren zonder geheimhoudingsverplichting. Het is naïef te veronderstellen dat de gemeentes nu überhaupt nog de tijd hebben om deze gemeenteambtenaar op te leiden voor die nieuwe taak. Mijn fractie maakt zich dan ook grote zorgen over de bescherming van de privacy op dit terrein.

Het gebrek aan echte aandacht voor de privacy van de burger is eigenlijk stuitend te noemen. Techniek kan veel en maakt inderdaad vele processen lichter en makkelijker. De digitale ontwikkeling gaat snel, zo snel dat deze menselijkerwijs haast niet bij te houden is. Heidegger zei: de mensheid zal aan techniek ten onder gaan. Wordt het geen tijd dat we een pas op de plaats maken en de prioriteiten anders gaan stellen? Wordt het geen tijd ons eens te bezinnen voordat er grote ongelukken gaan gebeuren? Ik vraag dit omdat de grootste impact van de digitale wereld ons nog te wachten staat, namelijk die van The Internet of Things. Straks is alles via het internet met elkaar verbonden. 30 miljard devices in 2020. Straks is ons hele leven digitaal te traceren. Dat is misschien onvoorstelbaar, maar straks is ons hele leven nog beter te traceren dan nu al het geval is.

Wat doet de overheid dan met de beschikbare data? Wij spreken hier vandaag over de veiligheidsdiensten, maar hoe zit het met de politie, de FIOD, de sociale dienst? De FIOD vraagt voor het gemak alle gegevens op van mensen die via een app hun parkeerplek betalen. Pas wanneer een van deze aanbieders zichzelf de vraag stelt of dit wel mag, komt het naar buiten. De rest heeft het waarschijnlijk allang gewoon gedaan. Hoe ver mag de overheid gaan met het opvragen van informatie van de aanbieders van diensten die digitaal traceerbaar zijn? Gaat de sociale dienst straks alle gegevens opvragen van mensen die een bijstandsuitkering of AOW hebben, om te zien of zij niet bovengemiddeld energie verbruiken, omdat dit zou kunnen aantonen dat er illegaal samengewoond wordt? Of vraagt de overheid van Siemens door te geven wat er in diezelfde huishoudens in de koelkast staat? En bewijst dan de aanwezigheid van een paar flessen dure witte wijn dat de persoon bijverdient?

In de zaak van de parkeerapp oordeelde de rechter uiteindelijk dat het algemeen belang boven het persoonlijk belang gaat en dat door het opvragen van gegevens fraude met leaseauto's kan worden voorkomen. Inderdaad. Door deze technieken kunnen we iets wat we vroeger niet konden, zonder iemand voor de deur te posten, de man met de gleufhoed van de heer Franken. Maar wat voor samenleving creëren we hiermee? Is dit de samenleving die wij voor ogen hebben? En zijdelings is het ook frappant dat vaak de partijen ter rechterzijde van het politieke spectrum hier minder moeite mee hebben dan de partijen aan de linkerkant van het spectrum. Het adagium "minder overheid" gaat kennelijk niet op wanneer het gaat om de controle van de burger.

Het opvragen van gegevens door andere overheidsdiensten dan de veiligheidsdiensten dient wat de SP-fractie betreft onder de loep genomen te worden. Kan de regering vertellen welke diensten digitale informatie opvragen over burgers, welke voorwaarden hieraan verbonden zijn en op welke wijze hier toezicht op wordt gehouden? Omdat zoveel facetten van onze samenleving tegenwoordig via internet lopen, heeft het een groot effect op de maatschappij als de overheid al deze data heimelijk aftapt en voor onbepaalde tijd (waarschijnlijk voor altijd) opslaat. Toezicht op het aftappen van geheime diensten is tot op heden vooral een toets op wettelijke naleving, of legal compliance. Gezien de compleet nieuwe technieken om data die alle facetten van het moderne leven onthullen, af te tappen, op te slaan en voor onbepaalde tijd te gebruiken — waarmee ook een omkering van de bewijslast wordt verwezenlijkt — zou het toezicht breder dan slechts juridisch en technisch moeten zijn. Bovendien wordt er nauwelijks op doelmatigheid getoetst.

De overheid in de Verenigde Staten kon niet aantonen of de surveillancepraktijken daadwerkelijk effectief zijn. Sterker nog, de overheid loog over het aantal terroristische dreigingen die zijn tegengehouden. Uiteindelijk bleek dat slechts in één enkel geval een bedrag van een aantal duizend US-dollars van een Somalische taxichauffeur is tegengehouden, dat was bestemd voor zijn piratenvrienden in Somalië. Door de complexiteit en de onbeheersbare hoeveelheid data zijn er wel verschillende personen als gevolg van "false positives" de dupe geweest van analyses, en zijn de voorbereidingen van meerdere aanslagen niet waargenomen. Het gebrek aan resultaat en de gigantische begrotingen van de geheime dataverzameling en -analyse geven blijk van een verhulling van het daadwerkelijke doel van deze informatieverzameling.

Kan de overheid het nut van het gebruik van de apparatuur voor terrorismebestrijding concreet aantonen? Indien niet, wat is volgens deze regering dan het doel van die informatieverzameling? Een aantal sprekers op de hoorzittingen gaf aan, een raambepaling wenselijk te vinden in de wetten over de digitale verzameling en opslag van informatie. Mijn fractie vindt dat een interessante gedachtegang. Een dergelijke afspraak zou ons als overheid dwingen om de doelmatigheid ook daadwerkelijk aan te tonen na een aantal jaar. Graag hierop een reactie van het kabinet. Andere relevante analytische invalshoeken voor het toezicht zijn bijvoorbeeld de sociale psychologie (het effect op de vrijheid van meningsuiting, zelfcensuur en vrijheidsgevoel), de economie (het effect op de technische sector), de ethiek en het sociaal-juridische aspect.

Het verzamelen van metadata door overheid en bedrijven geeft kans op zelfcensuur, en niet alleen op het internet. Met de komst van het verleggen van de taken van de Wmo en de Jeugdwet naar de gemeentes, zal het gebeuren dat

cliënten voorzichtiger zijn met het delen van persoonlijke informatie, wetende dat alles opgeslagen wordt en bekeken kan worden. Een cliënt zal de afweging maken tussen relevantie en privacy. Hierdoor wordt de verzamelde informatie onbetrouwbaarder, juist in de gevallen waar de juistheid van informatie van belang is.

Wat er digitaal mogelijk is en wat we al dan niet moeten toestaan, is hiermee dan ook het domein van de ethiek binnengedrongen. Ik wil de vergelijking trekken met de discussie rondom bijvoorbeeld stamcelonderzoek. Wat technisch mogelijk is, kan onwenselijke kanten hebben. De afwegingen rondom medisch-ethische kwesties worden veel indringender bekeken dan de afwegingen rondom het gebruik van software die ons leven in kaart brengt. Mijn fractie vindt een ethische benadering van de onderzoeksmogelijkheden van de hedendaagse software en het opslaan, bewaren en gebruiken van metadata een ethische discussie waard.

De heer **Van Boxtel** (D66):
Ik wil mevrouw Gesthuizen — excuses: mevrouw Gerkens — complimenteren dat zij het op deze manier aansnijdt, want dit element raakte echt helemaal uit beeld. In de medische ethiek bestaat er ook nog zoiets als de leer van het recht op niet-weten. Dat schijnt in dit debat echt totaal zoek te zijn. Ik vind dat de overheid bijna de lead moet nemen om dat fier te verdedigen. Als dat bij de suggesties gevoegd kan worden, ben ik benieuwd naar het antwoord van de bewindslieden.

Mevrouw **Gerkens** (SP):
Ik begrijp dat dit een interruptie aan het kabinet is.

De heer **Van Boxtel** (D66):
Nou ja, ook bijval.

Mevrouw **Gerkens** (SP):
Goed. Inderdaad. De vraag die ik wilde gaan stellen, is of de regering bereid is om een ethische commissie samen te stellen die de discussie op dit punt kan voeden.

Voorzitter. Verder wordt de burger zwakker in deze informatieherschikking van de machtsbalans tussen burger en staat. Hoe gaat de overheid het toezicht aanpassen aan en uitbreiden naar het moderne leven, om de werkelijkheid te weerspiegelen? Wordt dat toezicht dan ook transparanter?

De regering geeft aan dat de veiligheidsdiensten binnen de grenzen van de wet opereren. Wel hoorden we van de veiligheidsdiensten dat wanneer zij om informatie vragen aan andere landen over een persoon, zij niet weten of het verzamelen van de informatie binnen de door onze wet aangegeven ruimte is gegaan of dat de Nederlandse wet overtreden is door de buitenlandse dienst. Zou het niet juister zijn om die diensten aan te geven dat we alleen informatie willen die op een door de Nederlandse wet gelegitimeerde wijze is verzameld?

De AIVD stelt in zijn jaarverslag over 2013 dat internationale samenwerking een vereiste zou zijn om goed te functioneren en dat het delen van kennis en middelen daarvoor noodzakelijk is. In hoeverre is de aangekondigde bevoegdheid tot het aftappen van kabelgebonden communicatie daarvoor bedoeld? Is de bevoegdheid ook voor andere doelen noodzakelijk? Kan de regering mij vertellen of de Nederlandse diensten toegang hebben tot of gebruikmaken van het programma XKeyscore?

In Nederland is er in mijn ogen te weinig ophef over de onthullingen van Snowden. We denken allemaal dat wat we op Facebook posten, via Google delen, skypen of whatsappen te onbelangrijk is om door de NSA opgemerkt te worden. Zelfs wanneer de NSA weet dat we homoseksueel zijn, geld sparen of een andere baan zoeken, zullen ze toch nog niet de betrokkenen inlichten. En verder zijn we niet extremistisch of enig gevaar voor de Amerikaanse overheid, dus we hebben niets te vrezen. Ik denk dat veel burgers daar gelijk in hebben. De NSA zal niet snel achter de gewone burger aangaan. De NSA niet. Maar misschien een van hun honderden medewerkers wél, wanneer die een persoonlijk belang heeft. Dat zou een goed script zijn voor een film. Snowden lekte de informatie van de NSA op een kinderlijk gemakkelijke wijze. Als Snowden dat kan in het algemeen belang, wat kan iemand dan wel niet voor zijn persoonlijk belang ...

Wanneer we data verzamelen van mensen omdat het kan, omdat we de mogelijkheden hebben, omdat ze beschikbaar zijn, en niet omdat we iemand verdacht vinden of aanwijzingen hebben om iemand nader te onderzoeken, hoe staat dat dan in verhouding tot artikel 10 van de Grondwet? Uit onderzoek blijkt sterk dat metadata van communicatie en internetgedrag persoonsgegevens zijn en net zo onthullend zijn als de inhoud van communicatieverkeer en dat de analyse ervan nog meer blootlegt dan een analyse van de inhoud. Op welke grond blijft de overheid vasthouden aan het idee dat het geen privacyinbreuk is wanneer zij metadata verzamelt en analyseert?

Ik kom bij de rol van de inlichtingendiensten en de technische ontwikkelingen. Laat ik vooropstellen dat inlichtingendiensten altijd nodig zullen zijn. Spionage is van alle tijden en heeft ook een functie waar het gaat om de nationale veiligheid. Echter, in de ogen van de SP is het buitenproportioneel om 100% van de mensen in de gaten te houden terwijl een veel kleiner deel van onze bevolking daadwerkelijk in de gaten gehouden dient te worden. Van groot belang is en blijft dat het doorzoeken van data onder democratische controle dient te staan en te blijven, en gelegitimeerd dient te worden door de wet. Het voorbeeld van de parkeerapp geeft aan dat die legitimatie vaak pas achteraf gebeurt, als die al gebeurt.

Inmiddels is de spionagesoftwarelobby druk doende om de mooiste software aan overheden te verkopen. Inspelend op de natuurlijke drang van onderzoekers om meer informatie te vergaren en deze snel te kunnen analyseren, verleiden zij de overheid met hun producten. De heimelijke procedures en het gebrek aan technische kennis van toezichtcommissies hebben ertoe geleid dat zogenaamde cybersecuritylobbyisten en -verkopers eenvoudig, zonder publiekelijke of geïnformeerde toets, ingrijpende apparatuur konden verkopen onder de dekmantel van terrorismebestrijding. In de Verenigde Staten nemen ambtenaren van de NSA en vergelijkbare organisaties in toenemende mate zeer goedbetaalde functies aan bij de leveranciers van zulke apparatuur. Dit geeft bijna blijk van corruptie. Hoe gaat de overheid de aanschaf van apparatuur toetsen aan een pro-

portionaliteitstoets? Hoe gaat de overheid de inmiddels aangeschafte apparatuur aan een proportionaliteitstoetsing onderwerpen?

De onthullingen over de praktijken van geheime diensten leiden tot een potentieel maatschappelijk verlies van vertrouwen in technologie. De Nederlandse maatschappij wordt steeds meer een informatiemaatschappij, die wordt ondersteund door deze gecompromitteerde technologie. Hoe gaat de overheid het cruciale vertrouwen in deze kritieke informatie-infrastructuur herstellen?

De wetten die afluisterpraktijken reguleren, zijn gebaseerd op oude technieken en praktijken. Om deze technieken gelijk te stellen met het internet is een gevaarlijke misvatting, omdat het internet afluisterpraktijken technisch en economisch exponentieel eenvoudiger maakt en de schaal in meerdere ordes van grootte uitbreidt. Gaat de overheid uit proportioneel oogpunt de toepassing van hoofdstuk 13 van de Telecommunicatiewet evalueren?

De NSA zag en ziet veel bedrijfsinformatie. De NSA kent dus ook de overwegingen van een aanbesteding, de strategieën van oliebedrijven in het buitenland en de nieuwste ontwikkelingen bij Philips, vandaag heel actueel. Bedrijfsspionage is op dit moment een van de grootste vormen van internetcriminaliteit. De JSF wordt nu al in China nagemaakt. De vraag rijst of we wel voldoende zijn toegerust om onze eigen staatsgeheimen te bewaren. Hoe waarschijnlijk is een inbreuk op onze eigen servers? Of moeten we die gedachte maar helemaal laten varen? Is er nog wel een veilige haven, voor de overheid, het bedrijfsleven of het individu? Wat weten we eigenlijk van onze netwerken? De glasvezelsnelwegen zijn aangelegd door buitenlandse bedrijven. Hoe weten we zeker dat deze niet getapt worden? Houdt de overheid hier toezicht op?

Ik kom bij de conclusie van mijn betoog. Alle seinen staan op rood. De overheid kan haar verantwoordelijkheid ten opzichte van artikel 10 van de Grondwet niet alleen niet waarmaken, zij gaat er zelf slordig mee om. Ik bedoel hiermee de implementatie van de Jeugdwet en de Wmo evenals het lukraak verzamelen van data door FIOD, sociale dienst en andere overheidsorganisaties.

In de toekomst kan er nog veel meer. Tijdens de hoorzitting werd al verwezen naar het inbreken op Google Glass of medische systemen. In de wet nemen we voorwaarden op als proportionaliteit en doelmatigheid, maar het is de vraag wat er doelmatig is aan het feit dat mijn kenteken wordt doorgegeven aan de Belastingdienst wanneer ik in Amsterdam parkeer. Gezien alle toekomstige toepassingen die mogelijk zijn, wil ik het kabinet vragen om met een nota te komen waarin het zijn visie uiteenzet op de vraag hoe de overheid in de toekomst omgaat met de door diverse organisaties verzamelde data. Wat doet de overheid met die gegevens? Hoe bewaart zij deze? Op welke wijze wordt er doorzocht? Hoe ver mogen de opsporingsdiensten gaan? Ik heb het dan niet alleen over de AIVD en de MIVD — ik geloof eigenlijk dat juist deze instellingen het meeste nadenken over de vraag wat ze met de data doen — maar juist over de FIOD, de inspectie SZW en dergelijke. Wie houdt het toezicht daarop? Mijn fractie zou het een goed idee vinden wanneer deze organisaties en hun werkwijze periodiek gescreend worden door het CBP. Zou het bovendien, gezien alle opgaves op het gebied van privacy die naar ons toekomen, niet juist zijn om de capaciteit van het CBP een keer uit te breiden?

Mevrouw **Duthler** (VVD):
Ik deel de zorgen van de SP-fractie over de manier waarop wordt omgegaan met de Wmo, Jeugdwet, de rol van de politie, inlichtingen, FIOD, Belastingdienst en wat er allemaal gebeurt met onze persoonsgegevens. Ik mis in uw zienswijze echter de rol van bedrijven en organisaties zelf. U belicht heel erg de rol van de overheid en de rol van de burger, om wiens gegevens het gaat. Dat is terecht, maar zouden die bedrijven en organisaties zelf ook geen verantwoordelijkheid moeten krijgen om heel zorgvuldig met de persoonsgegevens om te gaan? U vraagt nu om een visie. Mogen die bedrijven en organisaties daarin ook een plek krijgen?

Mevrouw **Gerkens** (SP):
U bedoelt dat zij meeschrijven?

Mevrouw **Duthler** (VVD):
Ik bedoel dat zij in het object van het onderzoek betrokken worden.

Mevrouw **Gerkens** (SP):
Ja, heel graag zelfs. Ik had daarop aan het einde nog even willen terugkomen. De moeilijkheid is dat veel van die bedrijven komen uit Silicon Valley. Dat is een van de grootste privacyopgaves die wij hebben. De beste manier om onze privacy te verbeteren, is ervoor zorgen dat wij zelf zulke bedrijven krijgen en dat wij het op onze eigen grond kunnen doen. Ik weet wel dat veel Nederlandse bedrijven ook echt moeite hebben met de privacy. Ik heb dat zelf op allerlei manieren ervaren. Het zou dus heel goed zijn als de overheid ook een visie hierop meegaf.

Mevrouw **Duthler** (VVD):
U bedoelt dus niet alleen de leveranciers van software of andere ICT-hulpmiddelen, maar ook de gebruikers en de afnemers. Begrijp ik u zo goed?

Mevrouw **Gerkens** (SP):
Ja.

Voorzitter. Als laatste vraag ik de regering dus om veel meer te doen aan awareness. Heel veel mensen beseffen niet wat zij vrijgeven en wat de gevolgen zijn. Een jaarlijkse campagne is niet genoeg. Er moet structureel en intensief informatie worden gegeven over het beschermen van je privacy, het recht daarop en de techniek daarvoor. De scholen zijn de eerste plek waar dit moet gebeuren. Ik begrijp dan ook niet dat het ministerie van OCW op dit terrein nog steeds heel erg stil is.

Ik rond af. Wij hebben wel degelijk wat te verbergen. Wat de NSA doet, is wel degelijk een bedreiging voor onze samenleving, onze gehele samenleving. Ook al hebben wij geen bedrijfsgeheimen en geen geheime spaarrekening en ook al maken wij geen JSF, dan nog moeten wij principieel staan voor diegenen die om terechte redenen hun privacy

wel willen beschermen. Wanneer wij zeggen dat wij niets te verbergen hebben, worden degenen die dat om terechte redenen wel hebben, vogelvrij. Door zorgvuldig om te gaan met onze privacy maken wij het mogelijk dat anderen hun privacy kunnen hebben. Wanneer wij onze privacy opgeven, geven wij de privacy van anderen op. Als samenleving kunnen en mogen wij dat niet laten gebeuren. Daarin dienen wij als overheid het voorbeeld te geven.

□

De heer **De Vries** (PvdA):
Mevrouw de voorzitter. Ik heb de verdrietige taak om in dit debat de plaats in te nemen van Willem Witteveen.

Een aantal commissies uit deze Kamer heeft zich gedurende het afgelopen jaar beziggehouden met aspecten van veiligheid, of eigenlijk onveiligheid, van datacommunicatie. De gebruikelijke belangstelling van de Kamer voor dit onderwerp werd in belangrijke mate gestimuleerd door Edward Snowden, die met de kracht van een mokerslag alle illusies over de veiligheid van dataverkeer aan diggelen sloeg en alle vermoedens over onveiligheid bevestigde. Met veel dank aan alle deskundigen die ons hebben voorgelicht, wil ik de regering een aantal vragen voorleggen. Daarbij ontleen ik veel aan wat tijdens de hoorzittingen is gezegd.

Internet heeft zich de afgelopen 25 jaar uit het niets ontwikkeld tot de belangrijkste communicatiestructuur ter wereld. Iedereen maakt er gebruik van. We verschaffen informatie, we zoeken informatie, we bankieren, kopen en verkopen en we communiceren via de sociale media. We kunnen niet meer zonder en we hopen dat het goed gaat, want iedere gebruiker kan dagelijks vaststellen dat je op internet voortdurend wordt bedreigd door grote en kleine criminelen. Banken worden platgelegd door hackers, DigiNotar wordt gekraakt, particulieren worden bestolen en bedrijven worden op grote schaal bespioneerd. Elk groot bedrijf in Nederland schijnt er rekening mee te houden dat er Chinezen in zijn netwerk zitten.

Experts schetsten tijdens de hoorzitting een onthutsend beeld. De heer Prins vergeleek de IT-infrastructuur met een oude roestige auto, vol met gaten. Hij vertelde dat er in Nederland heel grote botnets gevonden zijn, met tienduizenden en soms honderdduizenden computers die in feite openstaan voor misbruik. De heer Arnbak, een andere gehoorde deskundige, legde de Kamer een aantal waarnemingen voor die ik in hoge mate verontrustend vond. Ik ontleen aan zijn inbreng ook een aantal voorbeelden.

Veel van de onveiligheid op internet is niet het gevolg van onvolkomen techniek, maar wordt moedwillig veroorzaakt. De Internet Engineering Taskforce, de GSM Association, het National Institute of Standards and Technology en andere sleutelorganisaties die het grondwerk doen voor de standaardisering van de beveiligingsprotocollen, worden al jaren op heel systematische wijze gemanipuleerd. De techniek is dus ondermijnd. Het vertrouwen in de Verenigde Staten in de mensen die van dag tot dag internet veilig moeten houden, is onherstelbaar beschadigd. Soms worden zelfs beveiligingsupdates van Microsoft gebruikt om het mogelijk te maken systemen te hacken. Het gezond en up-to-date houden van hard- en software vormt nu in zichzelf een beveiligingsrisico. De Amerikaanse veiligheidsdiensten hebben sinds 2007 140.000 botnets gecoöpteerd om mee te liften met cybercriminelen. Wereldwijd zijn 100.000 internetrouters op kritieke netwerknodes alvast gehackt om later surveillance mogelijk te maken. Het is geen wonder dat de conclusie van de heer Arnbak luidde dat het vertrouwen in die collectieve hallucinatie die internet was, absoluut is ondermijnd. Internet is volgens hem een volstrekte surveillanceomgeving geworden.

Dit leidt tot een drietal vragen. Is de regering het met die conclusies en observaties eens? Was de regering op de hoogte van deze moedwillige ondermijning van de veiligheid van internet en zo niet, acht zij dit schokkend? Het allerbelangrijkste is natuurlijk: hoe kan hieraan tegenwicht worden geboden? Je zou verwachten dat men in internationaal verband hard aan de bel zou trekken en degenen die zich hieraan schuldig maken, krachtig zou aanspreken. Is Europa, is Nederland niet veel te slap en onderdanig als dit in en door de Verenigde Staten gebeurt? Uit tal van documenten, laatstelijk uit de zeer leesbare nota Vrijheid en veiligheid in de digitale samenleving, blijkt dat de onveiligheid op internet door het kabinet serieus wordt genomen. Er zijn tal van fora gecreëerd waarin de overheid, instellingen en bedrijven samenwerken.

De heer **Van Boxtel** (D66):
Ik deel helemaal de analyse waarmee u gestart bent, maar ik vind wel iets frappant. Wij kunnen ons — gelukkig! — enorm opwinden over alles wat in de Verenigde Staten misgaat, maar dat komt in ieder geval nog een keer naar buiten. Laten wij echter ook de Chinezen eens noemen. Het is bekend dat zij megaveel op internet manipuleren. Ik wijs ook op de Iraniërs. Het gaat dus niet alleen om de Amerikanen.

De heer **De Vries** (PvdA):
Nee, ik heb de Chinezen ook al genoemd. Ik heb hun al de eervolle plaats gegeven dat zij in elk groot netwerk in Nederland actief zijn. Als u zegt dat de Iraniërs daar ook zitten, geef ik ze daarvoor graag de credits. Misschien hebt u nog een lijst van landen die niet deugen; anders wil ik u wel een suggestie doen. Ik mag nu natuurlijk niet interrumperen, maar ik zou de heer Van Boxtel weleens willen vragen waarom hij denkt dat hier alleen de Verenigde Staten te kijk worden gezet. Is dat een bijzondere gevoeligheid van hem?

De heer **Van Boxtel** (D66):
Nee, absoluut niet! Ik heb uw opmerking over de Chinezen blijkbaar gemist, maar het viel mij gewoon op, ook in de betogen van de heer Franken en mevrouw Gerkens. Wij zijn heel veel te weten gekomen door wat via Snowden allemaal naar buiten is gekomen over NSA en PRISM, maar van anderen weten wij eigenlijk niks, behalve dat bij DigiNotar ook andere staten een bemoeienis hadden. Ik wil alleen maar de balans overeind houden dat er veel meer mensen, staten en overheden actief zijn.

De heer **De Vries** (PvdA):
Maar het is een grote verdienste van de Verenigde Staten dat ze ons de heer Snowden hebben gegeven.

De heer **Franken** (CDA):
Een kleine aanvulling: de Engelse inlichtingendienst heeft dezelfde dingen gedaan waaraan we hier een bepaalde kwalificatie kunnen geven. Belgacom is gekraakt. We hoeven dus niet eens zo ver van huis.

De heer **De Vries** (PvdA):
Nee, je hoeft maar in de kabel bij Katwijk te kruipen en in Engeland boven water te komen, bij wijze van spreken.

In de nota Vrijheid en veiligheid wordt gesteld dat alle partijen, dus overheid, maatschappelijke organisaties en bedrijfsleven, betrokken moeten worden als het om cybersecurity gaat. Dat klinkt goed, maar de oproep tot een constante open dialoog tussen burgers, bedrijfsleven en overheid, zowel nationaal als internationaal, is natuurlijk voor de burgers niet navolgbaar. Het spreekt vanzelf dat iedere gebruiker het zijne moet doen om het gebruik veilig te maken. Ook op de weg moet elke verkeersdeelnemer goed opletten. Maar individuele gebruikers, die miljarden burgers en die miljoenen bedrijven die internet gebruiken, staan natuurlijk machteloos tegenover het structurele geweld waarmee internet blijkt te worden ondermijnd. Daar moet men op de overheid kunnen rekenen.

De analogie met het wegverkeer trek ik nog even door. Daar speelt de overheid op bijna alle terreinen een cruciale rol. Dat gaat van het stellen van gedetailleerde eisen aan de kwaliteit van de weg en van de vervoermiddelen tot het actief bestrijden van wegpiraten. Merkwaardigerwijs lijkt het alsof de overheid de onveiligheid op internet anders ziet en zelfs soms bestendigt.

Mevrouw **Duthler** (VVD):
Begrijp ik het goed dat de PvdA-fractie vraagt om meer en duidelijkere spelregels en om handhaving en naleving van de spelregels?

De heer **De Vries** (PvdA):
Op zijn minst. Ik zou nog meer willen vragen, maar dat moet ik dan heel zorgvuldig formuleren. Ik vraag op zijn minst om het handhaven van de spelregels.

Tijdens de hoorzittingen van deze Kamer bracht de heer Jacobs naar voren dat op internet door veiligheids- en inlichtingendiensten kwetsbaarheden worden gesignaleerd die met opzet niet worden bekendgemaakt, omdat de diensten zelf ook graag van die kwetsbaarheden gebruik willen blijven maken. Willem Witteveen merkte daarover op dat het algemeen belang om die kwetsbaarheid te kennen en te verhelpen toch zwaarder zou moeten wegen dan het belang van de diensten. Het antwoord dat hij daarop kreeg, was ontwijkend. Er zou naar een balans moeten worden gezocht tussen het publieke belang en dat van de diensten. Wat vindt de regering daarvan? Vindt zij ook niet dat het belang van de burgers hier richtinggevend moet zijn en dat we dat niet mogen neutraliseren met een sofistische redenering dat het belang van diensten ook altijd het belang van de burgers is? Het lijkt mij een bijna principiële keuze. Is de regering het daarmee eens?

De vraag is hoe de onveiligheid van internet te verbeteren valt. Wat vindt de regering daarbij de belangrijkste methode? Moet het van regelgeving komen, van het opvoeren van verdediging tegen machtige vijanden of van het intrinsiek veiliger maken van de infrastructuur en de hardware en software? En als het alle drie is, wat doet de regering dan concreet op het laatste gebied? Arnbak wijst op jurisprudentie in Duitsland waarin een nieuw grondrecht op de vertrouwelijkheid en integriteit van IT-systemen is ontwikkeld. Wat is de visie van de regering daarop?

Dezelfde deskundige wees er ook op dat voor een land als Nederland op verdedigend vlak enorm veel te winnen valt, als we ons kunnen profileren als een land waar data veilig zijn en waar goed wordt nagedacht over kwetsbaarheden in software. De wereld staat echt te springen om zo'n plek, zo zei hij, maar het huidige toezichtinstrumentarium is daar totaal niet op ingericht. Wat vindt de regering daarvan?

Tot slot wat dit deel betreft, heb ik een vraag over de governance. Op veel plaatsen in ons land zijn overheidsdiensten actief bezig met IT-onveiligheid. Zijn deze activiteiten voldoende op elkaar afgestemd om een optimaal resultaat te kunnen bereiken? Wie verzorgt die afstemming? Wordt de beperkte deskundigheid optimaal ingezet? Dezer dagen wordt een nieuw cybercommando opgericht bij het ministerie van Defensie. Wat gaat dat precies doen? "Cyberwarfare" zult u zeggen, maar wat is dat? Het beveiligen van vitale infrastructuur? Maar daar waren toch al voorzieningen voor getroffen? Hoe is het toezicht op die nieuwe activiteiten geregeld? Wat is de relatie met de SIGINT-activiteiten van de MIVD? Houdt de coördinerend minister ook oog op deze activiteiten van dit cyberwarfarecommando?

Ik kom bij mijn tweede onderwerp. Snowden heeft duidelijk gemaakt dat overheden niet alleen gebruikmaken van de onveiligheid van internet, maar daaraan ook een grote bijdrage leveren. Zijn constatering betrof niet de overheden van China of Rusland, maar van landen die westerse waarden zeggen te verdedigen. China en Rusland hebben we zojuist al geïdentificeerd als waardige concurrenten. De minister van Binnenlandse Zaken deelde deze Kamer desgevraagd mede dat de onthullingen van Snowden voor hem een verrassing inhielden. Ik neem aan dat hij dat niet persoonlijk bedoelde, maar dat het ook een verrassing was voor de onder hem ressorterende diensten. Kan hij dat bevestigen? Hadden de diensten hier werkelijk geen idee van? Wisten ze niet wat de collega's van de NSA en van de Britse diensten in hun kolossale gebouwen uitspookten? Het is moeilijk te geloven.

Voor de minister die de grondrechten moet beschermen, moet het een grote schok geweest zijn dat de persoonlijke levenssfeer van de burgers zo lek is als een mandje. Op de hoorzitting werd ons voorgehouden dat de verzameling gegevens die de NSA over personen heeft verzameld, heel Europa zou vullen met archiefkasten, indien al die gegevens geprint moesten worden. De heer Franken maakte al een vergelijking met de Stasi, die zijn spullen nog in één huizenblok kon onderbrengen. Alle dataverkeer wordt door onze bondgenoten afgeluisterd en getapt, geanalyseerd en opgeslagen. Wat onze vijanden allemaal doen, zal niet veel beter zijn. De onthullingen van Snowden hebben niet alleen het vertrouwen in internet, maar ook in overheden ernstig aangetast. De keizer heeft al te vaak geen kleren aan. Gelukkig houden onze eigen inlichtingen- en veiligheidsdiensten zich volgens de regering aan de wet, maar volgens

de CTIVD gaan ze toch regelmatig over de schreef. Bovendien leveren ze massaal gegevens aan veiligheidsdiensten van andere landen die zich niet door onze wet gebonden weten. "Metadata", zegt de minister. Hij zei er niet bij hoe privacygevoelig die kunnen zijn.

De surveillance van alle burgers, die kennelijk in de ogen van sommige overheden allemaal potentiële verdachten zijn, wordt gerechtvaardigd door de claim dat hiermee onze veiligheid gediend is, met name tegen terroristen. Er is net al gewezen op een officieel onderzoek in de Verenigde Staten waaruit bleek dat in geen enkel geval een terrorist geïdentificeerd was met behulp van de verzamelde gegevens. Ook de heer Wiebes wees tijdens de hoorzittingen daarop. Wat is de visie van de regering daarop? Als al dat verzamelen niet echt helpt tegen terroristen, waar is het dan wel goed voor? Mevrouw Gerkens stelde deze vraag zeer terecht. Waar wordt al dat geld voor uitgegeven, vroeg de heer Franken. Mogen we misschien een indicatie krijgen van wat het nut is van die investeringen die door de NSA en door de Britse geheime diensten worden gedaan en die natuurlijk ook in Nederland op een bepaalde wijze worden gedaan? Wat levert dit op? Waar is men mee bezig? Is dat economische spionage of is het iets anders? Ik zou dat graag van de regering horen.

Het perspectief waarbij iedereen besurveilleerd wordt en als verdachte wordt beschouwd, is veel te dominant in alles wat ik lees over internet. Komt dat ook omdat het coördinerend ministerschap bij het departement van Veiligheid en Justitie is belegd, waar men natuurlijk eerder geneigd is om mensen als verdachte te behandelen? Zou een grotere verantwoordelijkheid van de minister van BZK de bescherming van de grondrechten van de burger niet meer centraal stellen? Ziet de minister van BZK een taak voor zichzelf om de positie van de burger in deze internetomgeving te beveiligen? Beschikt hij over de deskundigheid daartoe, niet alleen bij zijn geheime diensten, maar ook binnen het normale departement?

Het heeft mij verbaasd hoe beleefd en terughoudend de Nederlandse regering, anders dan de Duitse, op de onthullingen van de heer Snowden heeft gereageerd. Minister Timmermans heeft er een keer met de heer Kerry over gesproken en minister Plasterk overlegde met een hoge Amerikaanse ambtenaar. Hebben wij boter op het hoofd zoals Duitsland, waar de inlichtingendiensten ook buitenlandse politici bleken af te luisteren, of durven we de Amerikanen op dit punt niet echt aan te spreken? Alle publieke verontrusting heeft alleen geleid tot het instellen van een aantal werkgroepen in EU-verband waarin samen met de VS de problematiek wordt besproken. Dat schiet niet op, zou je zeggen. Of misschien wel? Hoe staat het ermee? Zijn er al resultaten bekend of zijn de Verenigde Staten daarin niet geïnteresseerd? Wordt ook met de regering van Groot-Brittannië besproken hoe ze erbij komt om alle dataverkeer dat per kabel Nederland verlaat, in Engeland af te tappen? Voor welke doeleinden worden die gegevens dan gebruikt? Wat vindt de regering van het feit dat de Amerikaanse regering met betrekking tot niet-Amerikaanse burgers praktijken toelaatbaar acht die ze niet op de eigen burgers mag toepassen? Is de inzet van de regering in Europees verband om de eigen burgers hiertegen te beschermen duidelijk genoeg?

Ik heb nog een enkele opmerking over het toezicht op de inlichtingen- en veiligheidsdiensten in ons land. De in de Wiv geïntroduceerde CTIVD, die op de rechtmatigheid van de diensten toezicht houdt, doet naar ik meen voortreffelijk werk. De commissie-Dessens beveelt aan dat de verantwoordelijke ministers zichzelf beter uitrusten om toezicht te houden. Dat lijkt mij niet overbodig. Het gaat niet eens alleen om het houden van toezicht, maar, in elk geval bij Binnenlandse Zaken, ook om het direct leiding geven aan het directoraat-generaal dat in wording is.

Wat de controle door het parlement betreft, via de commissie voor de Inlichtingen- en Veiligheidsdiensten, lijkt enige professionalisering ook geen overbodige luxe. De Tweede Kamer beraadt zich hierop naar aanleiding van de rapportage van de commissie-Dessens. Ook iedere televisiekijker in Nederland zal echter de indruk hebben dat het wel iets beter kan dan we tot nu toe hebben gezien, zeker in het afgelopen halfjaar. De commissie van de Kamer zou niet noodzakelijkerwijs uit fractievoorzitters moeten bestaan, maar uit Kamerleden die zich ter zake specialiseren, zo is ons gezegd. Een kleine permanente ambtelijke ondersteuning is toch het minste dat vereist is. Toezicht moet nu eenmaal aan zware methodische eisen voldoen wil men er vertrouwen in kunnen hebben. Hoe denkt de regering daarover?

Zou het geen goed idee zijn als de commissie die de inlichtingendiensten moet controleren, althans die de ministers die verantwoordelijk zijn voor de inlichtingendiensten moet controleren waar het gaat om vertrouwelijke dossiers, een gezamenlijke commissie zou zijn en zou bestaan uit leden van de Tweede en de Eerste Kamer? De controle van inlichtingendiensten is een verantwoordelijkheid die op het ogenblik in de Eerste Kamer helemaal niet wordt waargemaakt. We lopen daar met een boog omheen, omdat we denken dat de collega's in de Tweede Kamer dat wel goed doen. Als die indruk niet overtuigend wordt bevestigd, is er misschien alle aanleiding om eens na te denken over de vraag of wij daarin ook een verantwoordelijkheid moeten nemen. Het lijkt er in elk geval op alsof het parlementair toezicht op deze diensten de afgelopen jaren enige achterstand heeft opgelopen.

Inmiddels heeft klokkenluider Snowden, die het bespioneren van de burgers aan de kaak stelde en die en passant ook licht wierp op het vertrouwen van bondgenoten in elkaar, zijn toevlucht moeten zoeken in het Rusland van de heer Poetin, of all places. In het vrije Westen loopt hij het gevaar te worden uitgeleverd aan de Verenigde Staten, hetgeen hem meteen in de gevangenis zal doen belanden. Wat vindt de minister van BZK, die in ons land klokkenluiders die kwalijke praktijken blootleggen bescherming wil bieden, hier eigenlijk van?

Dit zijn vele vragen en ik kijk zeer uit naar de beantwoording ervan.

De **voorzitter**:
Dank u wel, mijnheer De Vries. Ik geef het woord aan mevrouw Duthler van de fractie van de VVD.

Mevrouw **Duthler** (VVD):
Voorzitter. Op diverse momenten hebben we reeds stilgestaan bij het tragische verlies van onze zeer gewaardeerde collega Willem Witteveen. Andere collega's zijn mij daarin voorgegaan. Ook vandaag is zo'n moment dat we daar aan worden herinnerd. Hij was immers een van de initiatiefnemers van dit debat. Ook nam hij aan de commissie deel die dit debat, onder meer met een openbare deskundigenbijeenkomst, heeft voorbereid. De VVD-fractie is dankbaar voor zijn sterk inhoudelijke, bijdragen, ook aan andere debatten. Het gemis doet zich op een dag als vandaag extra sterk voelen. Voordat ik de inbreng van de VVD-fractie verwoord, wilde ik dit gezegd hebben.

De inbreng van de VVD-fractie is langs drie lijnen opgebouwd. De maatschappelijke betekenis van cyberintelligence en bestrijding van cybercrime, de economische betekenis en de juridische vraagstukken.

Ik begin met de maatschappelijke betekenis. Het is inmiddels alweer meer dan een jaar geleden dat Snowden met zijn onthullingen over de NSA-afluisterpraktijken wereldwijde aandacht trok voor de praktijk van cyberintelligence, het belang van dataprotectie of privacybescherming en daarmee inherent het belang van informatiebeveiliging. In het afgelopen jaar, en met name in de afgelopen maanden, is er in de wereld veel veranderd. MH17 heeft ons diep geraakt en bracht de oorlog in de Oekraïne dichtbij. Ook op andere plekken in de wereld breidden brandhaarden zich uit. Het Midden-Oosten, Noord-Afrika en Oekraïne zijn oorlogsgebieden. Grote vluchtelingenstromen komen op gang. Europa wordt omringd door een gordel van toenemende instabiliteit, een instabiliteit die volgens alle analyses voor langere duur zal zijn.

Deze veranderende geopolitieke omstandigheden dwingen ons tot aanpassingen. De vraag of wij daartoe in staat zijn, is niet aan de orde. Wij zijn daartoe in staat. De vraag is aan de orde welke rol cyberintelligence daarbij kan of moet spelen, onder welke randvoorwaarden dat moet gebeuren en welke rol de wetgever daar dan in heeft. Hoe gaan wij om met de bescherming van de persoonlijke levenssfeer van onze burgers? Hoe zorgen we ervoor dat de informatiebeveiliging, die onlosmakelijk verbonden is met privacybescherming alsook met cyberintelligence, op een adequaat niveau wordt gebracht? De kernwaarden van de democratische rechtsstaat vormen voor mijn fractie de toetssteen waaraan antwoorden op deze vragen beoordeeld zullen moeten worden.

Ik ga nu eerst terug naar de onthullingen van Snowden. Een belangrijke vraag die mijn fractie bezighoudt, is wat we daar nu eigenlijk mee zijn opgeschoten. Er was een hoop verontwaardiging. Het mobieltje van Merkel was onderwerp van gesprek. De persoonsgegevens van miljoenen nietverdachte burgers werden zonder dat zij dat wisten afgetapt, gekopieerd of anderszins onderschept door Amerikaanse inlichtingen- en veiligheidsdiensten. Dat worden zij nog steeds. Er werden werkgroepen ingesteld in Europees verband die van alles moesten uitzoeken en de onderhandelingen over het vrijhandelsakkoord kwamen op scherp te staan. De grote vraag van mijn fractie is wat wij ermee zijn opgeschoten. Welke acties heeft de regering ondernomen? Is de rechtsbescherming van de burger inmiddels verbeterd? Ik kom straks toe aan concretere vragen die ik aan de regering wil voorleggen, maar ik vraag haar om hier eens op te reflecteren.

Voordat ik nader inga op cyberintelligence, wil ik eerst iets zeggen over de bestrijding van cybercrime. Van groot belang voor de bestrijding van cybercrime is de cyberbeveiliging. De regering is betrokken bij vele initiatieven om een hoger beveiligingsbewustzijn bij bedrijven en instellingen te creëren, zodat ze het tot in hun haarvaten normaal gaan vinden dat ze hun systemen, bedrijfsinformatie en persoonsgegevens beschermen tegen aanvallen van buiten en tegen diefstal. In de praktijk gaat het nogal eens mis. In de afgelopen zomer was de spoedeisende hulp van een academisch ziekenhuis een hele dag dicht vanwege een computerstoring. Artsen konden niet bij patiëntgegevens. Russische hackers verzamelden meer dan 1,2 miljard usernamepasswordcombinaties en meer dan 500 miljoen e-mailadressen. Het securitybedrijf dat dit ontdekte, verkocht deze data terug aan de betrokkenen, zonder blikken of blozen.

De VVD-fractie is blij met initiatieven als The Hague Security Delta en het Nationaal Cyber Security Centrum (NCSC), waar overheid en bedrijfsleven nauw met elkaar samenwerken. Behalve programma's die het bewustzijn van het belang van een adequate beveiliging bevorderen, kan ook wetgeving een belangrijke stok achter de deur zijn om beveiliging op orde te krijgen. De Wet computercriminaliteit III, althans het wetsvoorstel daartoe, en het wetsvoorstel Meldplicht datalekken zijn belangrijke voorbeelden daarvan. Kan de regering aangeven wat de status is van deze wetsvoorstellen? Dit zijn voorbeelden van spelregels waarop ik zonet doelde.

Het wetsvoorstel Computercriminaliteit III is inmiddels geaccordeerd door de ministerraad, zo heb ik op de site van het ministerie van V en J gelezen. De internetconsultatie was reeds op 1 juli 2013 afgesloten. Wanneer verwacht de minister dat het wetsvoorstel kan worden aangeboden aan de Tweede Kamer? Het CBP heeft in een mededeling van februari dit jaar de regering geadviseerd, het wetsvoorstel niet aldus in te dienen. Hackbevoegdheden van politie en opsporingsdiensten zijn naar de mening van het CBP te ruim geformuleerd. Een te grote groep kan bij een te grote hoeveelheid data. Niet alleen huidige gegevens, maar ook historische en toekomstige gegevens. Niet alleen van verdachten, maar ook van grote groepen tot wie een verdenking zich niet richt. De dringende noodzaak hiertoe is door de regering onvoldoende onderbouwd. Heeft de regering het wetsvoorstel nog aangepast aan het advies van het CBP?

Kan de regering daarnaast nog iets zeggen over de status van het wetsvoorstel Meldplicht datalekken, de voorgestelde Europese privacyverordening, waarin het recht op vergeten is geïncorporeerd — dat zeg ik met een blik naar de heer Van Boxtel — en de implementatie van de NIB-richtlijn? In mijn eigen dagelijkse praktijk — zoals bekend maken privacybescherming en informatiebeveiliging daarvan deel uit — kom ik nogal eens information security officers tegen die nog steeds moeite hebben om het belang van de informatiebeveiliging bij hun bestuurders onder de aandacht te brengen. Zij geven mij aan dat dergelijke wetgeving hen enorm zou helpen. Daarnaast merk ik zelf bij bestuurders dat een aanstaande wettelijke meldplicht en vooral de hoogte van boetes — ik ben toe aan de handhaving — een belangrijke stok achter de deur kunnen zijn om informatiebeveiliging en privacybescherming heel serieus te nemen.

Dit onderstreept voor mij nog eens de rol die wetgeving kan spelen bij het op orde krijgen van beveiliging en het vergroten van het bewustzijn. Ik hoor zoals gezegd graag van de regering wat de status is.

Ik kom toe aan de economische betekenis van cyberintelligence en bestrijding van cybercrime. De jaarlijkse economische schade als gevolg van cybercrime is voor het United Kingdom berekend op 27 miljard pond in 2011. Bij mijn weten zijn voor Nederland geen vergelijkbare cijfers bekend. Wel zijn cijfers bekend over schade als gevolg van identiteitsfraude. ID-fraude kost het Nederlandse bedrijfsleven miljarden euro's per jaar, terwijl de pakkans nog geen 5% is. De Nederlandse overheid zit bepaald niet stil. Dat mag ook wel eens gezegd worden. Nederland speelt in Europa een voortrekkersrol als het gaat om cybersecurity en de aanpak van cybercrime. De bestrijding van identiteitsfraude kan echter beter. Met behulp van DigiD, waarvoor de minister van BZK verantwoordelijk is, kunnen veel burgers hun identiteit bewijzen om gebruik te kunnen maken van overheidsdiensten. Ook aanbieders van kritieke infrastructuren, zoals ziekenhuizen, maken steeds meer gebruik van DigiD. DigiD ligt er echter nogal eens uit en de betrouwbaarheid schiet nog wel eens te kort. Wat gaat de regering hieraan doen? En hoe gebruikt ze de resultaten van de onderzoeken die uitgevoerd zijn naar de DigiNotar-zaak? Wordt de werking van beveiligingsmaatregelen daadwerkelijk betrokken bij de jaarlijkse auditonderzoeken? En neemt de regering geen genoegen met een goedkeuringsverklaring over de opzet en bestaan? Beveiligingsbeleid en beveiligingsplannen zijn prachtig, maar hoe weten we zeker dat ze ook worden nageleefd?

Mijn fractie begrijpt verder dat de minister van BZK overweegt om het rijbewijs geschikt te maken als elektronisch identificatiemiddel. Waarom niet gebruikmaken van de identificatiemiddelen van banken? Bijna alle Nederlanders hebben er één. De betrouwbaarheid is hoog. De gebruiksvriendelijkheid goed. Op die manier kunnen de banken ook wat terug geven aan burgers en bedrijven die hen overeind hebben gehouden.

Dit was de defensieve kant van cybercrime. Nederland is niet alleen het land van de dominee, maar ook het land van de koopman. Nederland is in staat bedreigingen om te buigen naar kansen. Kansen om veiligheid, vrijheid en maatschappelijke groei op het hoogste niveau samen te laten gaan. Nederland zou bijvoorbeeld een voortrekkersrol kunnen spelen als het gaat om bestrijding van cybercrime. The Hague Security Delta zou een mooi platform kunnen zijn om zo'n voortrekkersrol in te vullen. Maar ook daarbuiten zou Nederland zich kunnen profileren als land waar je gegevens veilig zijn. Nederland als aantrekkelijk land waar buitenlandse bedrijven graag investeren. Dat levert economische bedrijvigheid op en daarmee economische groei. Dan is het wel nodig dat de Nederlandse overheid streng optreedt tegen bedrijven die hun beveiliging niet op orde hebben; dat zij streng optreedt tegen bedrijven die persoonsgegevens uitwisselen met derde landen terwijl zij niet voldoen aan de wettelijke randvoorwaarden die daaraan worden gesteld; en dat de Nederlandse overheid streng optreedt tegen bedrijven die te gemakkelijk persoonsgegevens aan derden verstrekken terwijl een juridische grondslag daarvoor ontbreekt. Is de Nederlandse regering voornemens dan wel bereid om dergelijk optreden te versterken? En deelt de regering de gedachte dat Nederland zich zou moeten profileren als land waar gegevens veilig staan, en zo ja, is zij bereid deze gedachte nader uit te werken en internationaal uit te dragen?

In dit verband wenst mijn fractie de regering vragen te stellen over de Patriot Act. Veel bedrijven en instellingen zijn een beetje de weg kwijt als het gaat om de toepassing van de Patriot Act. Er is veel onduidelijkheid over de mogelijkheden en kansen dat Amerikaanse overheden met een beroep op de Patriot Act gevoelige gegevens opvragen bij deze bedrijven en instellingen. Als dat inderdaad mogelijk is, hoe groot zijn de kansen hier dan op?

Ik kom toe aan de juridische betekenis. We hebben in de aanloop naar dit debat een expertmeeting georganiseerd en diverse deskundigen gehoord. Een aantal onderwerpen en vragen is opengebleven. Enkele vragen wenst mijn fractie de regering voor te leggen. Om te beginnen toegang tot de kabel door onze inlichtingendiensten. De Wet op de inlichtingen- en veiligheidsdiensten (Wiv) legt in tegenstelling tot communicatieverkeer via de ether beperkingen op om toegang te krijgen tot verkeer dat via de kabel loopt. Alleen gerichte interceptie is mogelijk, met toestemming van de minister. Ongerichte interceptie op de kabel is niet toegestaan. Het meeste gegevensverkeer, 90%, loopt echter via glasvezelkabels. Onze inlichtingendiensten hebben zo beperkter zicht op cyberbedreigingen, bedrijfsspionage en terroristische activiteiten dan volgens mijn fractie gewenst is.

Aanpassing van de Wiv lijkt dan ook nodig. De commissie-Dessens, die een evaluatieonderzoek uitvoerde naar de Wiv 2002, was van mening "dat een verruiming van bevoegdheden gepaard zal moeten gaan met een kwalitatief hoogstaand systeem van waarborgen om disproportionele aantasting van democratische beginselen en grondrechten te voorkomen." De commissie vervolgt: "De diensten moeten bij de inzet van deze bevoegdheden gebonden zijn aan een helder juridisch kader dat meer inzicht geeft in de voorwaarden waaronder en de manieren waarop deze bevoegdheden ingezet mogen worden. Naarmate de inbreuk op de grondrechten van privacy en communicatiegeheim indringender is, moeten de toestemmingsprocedure en het toezicht ook sterker ingebed zijn."

Hoe kijkt de regering aan tegen deze aanbevelingen? Heeft zij inmiddels een begin gemaakt met de uitwerking daarvan? Als we het controlemechanisme willen versterken, hoe kan dat in de praktijk worden geoperationaliseerd? Welke ideeën heeft de regering daarover?

Ten aanzien van het toestemmingsvereiste heb ik nog twee vragen. Om invulling te geven aan het toestemmingsvereiste moeten de diensten inzicht geven in de gemaakte afwegingen omtrent noodzakelijkheid, proportionaliteit en subsidiariteit. Worden de diensten hierin getraind? Hoe toetst de minister de gemaakte afwegingen?

Ik ga nog even terug naar de Wiv. De Wiv is alleen in Nederland van toepassing. Voor militair optreden in het buitenland geldt het criterium dat dit zo veel mogelijk in overeenstemming moet zijn met de Wiv. Maar hoe zit het met elektronische oorlogsvoering? Valt die ook onder de Wiv? Het gaat dan over het afluisteren van gesprekken, het aftappen van data en het verstoren van signalen. Hoe zit het met de opslag van die gegevens? In onze globaliserende samenleving worden gegevens lang niet altijd meer opgeslagen op servers op Nederlands grondgebied. Gegevens

van inlichtingendiensten kunnen ook op servers in bijvoorbeeld Pakistan of India staan. Daar geldt niet onze Wiv, maar de Wiv van de betreffende landen. Dat betekent dat de lokale inlichtingen- en veiligheidsdiensten van die landen bij de gegevens kunnen. Kan de regering aangeven of er een kans is dat gegevens van inlichtingendiensten op servers worden opgeslagen die zich niet op Nederlandse grondgebied bevinden? Hoe beoordeelt de regering het uitgangspunt dat gegevens van inlichtingendiensten altijd op Nederlandse servers en op Nederlands grondgebied zouden moeten staan?

Dan het toezicht op de inlichtingendiensten door de CTIVD. De CTIVD toetst de activiteiten van de inlichtingendiensten alleen op rechtmatigheid en niet op doelmatigheid.

De heer **Van Boxtel** (D66):
Mevrouw Duthler heeft het over de gegevens van Nederlandse veiligheidsdiensten die in Nederlandse centra op Nederlandse bodem worden opgeslagen, maar ze formuleerde dit niet direct als een vraag. Heeft zij aanleiding om te veronderstellen dat deze gegevens niet in Nederland worden opgeslagen?

Mevrouw **Duthler** (VVD):
Ja, die aanleiding heb ik.

De heer **Van Boxtel** (D66):
Dus dan maken we de vraag aan het kabinet scherper om zekerheid te krijgen over het feit dat het zo is.

Mevrouw **Duthler** (VVD):
Ja, mijn laatste zin was geformuleerd als een vraag, maar het is goed dat de heer Van Boxtel het nog eens onderstreept. Het is een heel concrete vraag aan het kabinet.

Ik was bij de doelmatigheid gebleven. Nu de inlichtingendiensten zo veel toegang krijgen tot zo veel gegevens, is de verleiding groot om te gaan grasduinen in de grote hoeveelheden gegevens. Het zou goed zijn als de commissie niet alleen toezicht houdt op de rechtmatigheid, maar ook op de doelmatigheid van de uitoefening van hun bevoegdheden. Hoe denkt het kabinet hierover? Overweegt het kabinet om de taken en bevoegdheden van de CTIVD hiertoe uit te breiden? Moet de samenstelling van de CTIVD worden aangepast omdat hiervoor andere kennis en competenties nodig zijn? In dit verband is het relevant om te wijzen op de onrechtmatigheid van de Europese dataretentierichtlijn. De heer Franken noemde deze al. De richtlijn is door het Europese Hof van Justitie in Luxemburg onrechtmatig verklaard. Is het kabinet voornemens om de Wet bewaarplicht telecommunicatiegegevens, die daarop is gebaseerd, in te trekken dan wel aan te passen?

Bij het toezicht op de inlichtingendiensten door de CTIVD hoort ook het toezicht door de zogenaamde commissiestiekem van de Tweede Kamer. Voor de vragen over dit onderwerp sluit ik aan bij de vragen van de PvdA-fractie om te voorkomen dat ik bijna hetzelfde ga zeggen in andere bewoordingen. Dat bespaart weer tijd.

Ik kom bij het onderwerp rechtsbescherming. Rechtsbescherming van de burger houdt onder meer in dat hij het recht heeft op inzage in de gegevens die de AIVD of MIVD over hem of haar verwerkt, alsook het recht op verbetering of vernietiging van deze gegevens. De huidige Wiv biedt burgers de mogelijkheid om eigen gegevens of die van een overleden direct familielid in te zien als deze gegevens ouder zijn dan vijf jaar, of als ze onderdeel hebben uitgemaakt van een onderzoek dat langer dan vijf jaar geleden is afgerond. Burgers hebben echter geen mogelijkheid om hun gegevens te corrigeren of te vernietigen. In de praktijk blijkt dat de diensten formalistisch, terughoudend en inconsistent reageren op inzageverzoeken. De commissie-Dessens beveelt daarom aan om een leidraad op te stellen, waarin duidelijk wordt aangegeven hoe een verzoekschrift moet worden geformuleerd om op een effectieve manier de gewenste gegevens te kunnen opvragen en op basis van welke criteria inzageverzoeken getoetst worden. Dan kan ook tegemoetgekomen worden aan de kritiek dat er niet altijd een duidelijke lijn ontwaard kan worden in de inzagebeslissingen. Tevens beveelt de commissie-Dessens aan om in de Wiv te regelen dat personen die inzage hebben gekregen, gemotiveerd moeten kunnen verzoeken om herstel, aanvulling, verwijdering of vernietiging van de gegevens. De leden van de VVD-fractie onderschrijven deze aanbevelingen van harte. Is het kabinet voornemens om ze op te volgen?

Gegevens van de inlichtingendiensten worden soms gebruikt in zaken die niet direct de staatsveiligheid raken, maar wel grote consequenties kunnen hebben voor de betrokkenen. Ik refereer aan het voorbeeld van een korpschef in Zeeland, die moest vertrekken op grond van informatie van de AIVD, maar zelf niet kon verifiëren op grond van welke informatie dat precies was. Vijf jaar wachten op het mogen inzien van je dossier duurt echt te lang. Daar heeft de betrokkene niets meer aan. Is de regering bereid om het inzagerecht te differentiëren naar gevallen waarin sprake is van directe of aantoonbare risico's voor de staatsveiligheid, en gevallen waarin daar geen sprake van is, en voor de laatste categorieën het inzagerecht in beginsel toe te staan?

Ik kom aan het slot van mijn betoog. Er is zo veel te zeggen over cyberintelligence, privacybescherming en cybercrime. De belangrijkste onderwerpen en vragen heb ik benoemd en gesteld namens mijn fractie. Mijn fractie wacht nu eerst met belangstelling een reactie van het kabinet af.

Mevrouw **Strik** (GroenLinks):
Voorzitter. Dit debat vormt het vervolg op een aantal expertbijeenkomsten over de ontwikkelingen in de cyberintelligence. In navolging van mijn collega De Vries wil ik de experts hartelijk danken voor hun inbreng. Ik herinner mij nog goed dat Willem Witteveen dit onderwerp als eerste te berde bracht in de commissie voor Veiligheid en Justitie naar aanleiding van het Snowden-schandaal. Bescherming van burgerrechten lag hem altijd na aan het hart. Wat is het wrang en verdrietig om dit debat nu zonder hem te moeten voeren.

Eind jaren negentig werden Nederland en de rest van Europa opgeschrikt door een NSA-schandaal: ECHELON. De onthullingen over de grootschalige afluisterpraktijk van radio- en satellietverkeer door de zogenaamde five eyes schudden overheden en burgers wakker. Ze zorgden voor

discussies over de rol van de Europese overheden bij dit programma en over de vraag hoe burgers gewapend konden worden tegen dergelijke bemoeienis en privacyschending. De Nederlandse regering reageerde destijds lauw. Ze vond het niet nodig om medewerking te verlenen aan hoorzittingen over ECHELON, achtte een eigen onderzoek naar ECHELON niet nodig en vond het evenmin opportuun om het Verenigd Koninkrijk aan te spreken op deelname aan ECHELON. "Een relevante dreiging op het gebied van grootschalig afluisteren waartegen de Nederlandse inlichtingen- en veiligheidsdiensten actie kunnen voeren is thans niet aan de orde", zo schreef minister De Grave aan de Tweede Kamer. De toenmalige minister van Binnenlandse Zaken schreef aan het parlement dat op internet al voldoende praktische en relatief goedkope middelen voorhanden waren voor burgers om zichzelf te beschermen tegen dergelijke praktijken. "Het daadwerkelijk aanwenden van deze middelen is vooral een eigen verantwoordelijkheid van burgers, bedrijven en instellingen", zo schreef destijds minister De Vries. De minister toonde zich wel bereid om een bewustwordingscampagne op te zetten over een veilig internetgebruik. En zo gingen we allemaal gerustgesteld weer slapen.

Wat is er sinds die schok gebeurd? De NSA heeft zijn programma's verder uitgebreid, en vergaart sinds 2007 met PRISM inlichtingen uit persoonsgegevens via een reeks grote Amerikaanse internetbedrijven. Sinds de onthullingen van Snowden weten we hoe verstrekkend die praktijken zijn. Inmiddels weten we ook dat niet alleen de VS metagegevens verzamelt voor inlichtingenwerk en dat inlichtingendiensten op grote schaal samenwerken en daarmee de nationale privacywetgeving ontduiken. Wat was anno 2013 de reactie van de Nederlandse regering? Was deze meer adequaat, beschermend en transparant dan twaalf jaar daarvoor? Nou, nee. Er was sprake van tegenstrijdige berichtgeving en ontkenningen, en de VS wordt de schuld in de schoenen geschoven voor de verzameling van 1,8 miljoen telefoontjes. We maakten geen beste beurt. We zijn weer even wakker. Burgers beseffen nu des te meer dat constituties en verdragen niet afdoende zijn om hun persoonlijke levenssfeer te beschermen. De praktijk is veel lastiger te beteugelen. De vraag is nu of we wakker zullen blijven.

In dit debat wil mijn fractie stilstaan bij de bescherming van burgers en met name bij de vraag of ons wettelijk kader nationaal en internationaal wel is toegesneden op de huidige technologie en praktijk. Wat mijn fractie betreft staan vandaag daarom twee vragen centraal. Aan welke criteria willen wij het verzamelen en uitwisselen van data door inlichtingen- en veiligheidsdiensten verbinden? En welke aanpassingen aan wet- en regelgeving zijn nodig om naleving van die criteria te waarborgen?

Ik zal ingaan op de doelmatigheid van het verzamelen van data, het juridisch kader versus de technologische ontwikkelingen, het toezicht op de diensten en ten slotte op het probleem van de valspositieven.

De hoeveelheid data groeit ons volkomen boven het hoofd. Tegelijkertijd wordt de bewaarduur alleen maar langer. Vanwaar die informatiehonger? Wat willen we ermee bereiken? En lukt dat ook? Tot nu toe blijkt uit onderzoek steeds dat er nauwelijks een aanslag mee verijdeld wordt. De NSA gaf laatst toe dat er geen enkele aanslag is verijdeld door massasurveillance. Er zouden hooguit dertien terrorist events gevonden zijn. Deze bekentenissen roepen ook meteen vragen op over het jaarverslag van 2013 van de CTIVD, waarin de commissie meldt dat PRISM in 2013 26 aanslagen wist te verijdelen. Ik hoor hierop graag de reactie van het kabinet.

Dergelijke verwaarloosbare resultaten stroken ook met andere onderzoeken, bijvoorbeeld naar de effectiviteit van PNR-gegevens. De vraag lijkt gerechtvaardigd of de groei van de hooiberg het inlichtingenwerk niet juist minder effectief maakt. Al die energie en middelen gaan ten koste van de klassieke recherche, en zelfs ook van een integrale preventieve aanpak van terrorisme. Denk daarbij aan onderwijs, diplomatie, ontwikkelingssamenwerking en dergelijke. Wanneer vormen deze schamele resultaten nu een aanleiding voor kritische reflectie op onze verzamelwoede? Graag hoor ik daarop een reactie van de bewindslieden. Het volstaat immers niet om te zeggen "baat het niet, dan schaadt het niet". Deze praktijken schaden namelijk wel. Ze schaden de persoonlijke levenssfeer van mensen en vergroten het risico op onterechte weigeringen aan de grens, blokkades van rekeningen of strafrechtelijke vervolgingen. Hoeveel schade mag massasurveillance opleveren? En wie bepaalt dat? Hoe kun je misbruik van informatie en onnodige lange retentieduur voorkomen?

Tot nu toe lijkt het adagium te gelden dat het vooral de stand van de techniek zelf is die bepaalt wat we verzamelen en voor hoelang. Dat zou naar de mening van mijn fractie moeten worden omgedraaid. Bovendien lopen wetgeving en technologie bijna nooit synchroon. De klassieke indeling in methodieken van verzamelen — kabel versus ether — in gerichte en ongerichte interceptie is inmiddels achterhaald. Ook het onderscheid tussen metadata en data is minder functioneel, omdat ook uit metadata veel persoonlijke informatie te destilleren is. Dat is vandaag al eerder geconstateerd.

Wat betekent dit voor het onderscheid dat we maken tussen het toelaten van surveillance op kabel enerzijds en ether anderzijds? De evaluatiecommissie van de Wiv beveelt aan om ongerichte kabelgebonden interceptie toe te staan, maar dan wel gekoppeld aan steviger wettelijke waarborgen van toestemming en toezicht. De commissie onderbouwt dit met het uitgangspunt dat hoe groter de inbreuk op de privacy is, hoe hoger de eisen aan toezicht en toestemming moeten zijn. Wij steunen de aanbeveling om niet langer de techniek, maar de mate van indringendheid van de inbreuk op de privacy leidend te laten zijn voor deze waarborgen. Als aan die voorwaarden is voldaan, zou kabelgebonden interceptie eventueel acceptabel zijn, omdat het meeste verkeer daar op te halen is.

Daar is echter wel een aantal vragen aan verbonden. Hoe kan dit zodanig beperkt worden dat we niet onnodig veel toestaan? Kunnen we bijvoorbeeld volstaan met het toestaan van gerichte interceptie, zodat ongericht zoeken niet te verleidelijk wordt? Of zou je hier een strenger criterium aan moeten verbinden? Een voorbeeld is een direct gevaar voor lijf en leden, zoals dat in de Duitse wetgeving is opgenomen.

Een ander idee, tijdens de expertmeeting geuit door professor Jacobs, is om data wel breed binnen te halen, maar deze bulkdata slechts enkele minuten vast te houden en meteen in te zoomen op de verdachte gegevens. Graag hoor ik de visie van het kabinet op dit punt. In maart van

dit jaar gaf het kabinet namelijk aan er nog niet uit te zijn wat betreft een reactie op deze aanbeveling. Als het kabinet kabelgebonden interceptie zou willen toestaan, is het dan ook bereid om het toestemmingsvereiste en de rechtmatigheidstoets door de CTIVD te laten verstrekken? En zo ja, op welke wijze?

Inlichtingendiensten hebben de naam genegen te zijn om zo veel mogelijk te willen weten. Je weet tenslotte maar nooit waarvoor je informatie gebruiken kunt. Bovendien kunnen individuele medewerkers het soms te interessant vinden om in bestanden te zoeken naar de achtergrond van hun buren of schoonzoon. In de Snowden files is hiervoor bewijs gevonden, onder meer in LOVEINT.

Het NSA-debacle maakte voor het eerst ook de omvangrijke en vergaande inbreuk van IVD-bevoegdheden in de digitale wereld op de persoonlijke levenssfeer duidelijk. De CTIVD heeft geconstateerd dat ook bij de Nederlandse diensten grenzen worden overschreden. Denk aan de disproportionele toepassing van bevoegdheden bij het hacken van algemene internetfora. De heer Arnbak, een van de experts, gaf aan dat dit soort praktijken al voorafgaan aan de daadwerkelijke inbreuk op de privacy. De grondrechten bieden daarbij dus geen bescherming. Dat is een punt van zorg. Welke bescherming kunnen we daar dan toch tegenoverstellen?

Kortom: al dit soort vragen maken het naar de mening van onze fractie duidelijk dat er een onderzoek zou moeten komen naar de effectiviteit van die praktijk, in samenhang met de impact op de persoonlijke vrijheden. Alleen zo kunnen we analyseren of onze onderzoeksbevoegdheden wel in balans zijn. We hebben nu een heel mooie evaluatie van de Wiv, waar heel veel dingen in staan. De evaluatie gaat echter niet over de effectiviteit in samenhang met de impact op de privacy.

Een baanbrekend arrest van het Hof van Justitie over de bewaarplicht heeft ook gevolgen voor de wetgeving en de werkwijze van inlichtingendiensten. Blanket retention, de grootschalige opslag van metadata van onverdachte personen, is in strijd bevonden met artikel 7 en 8 van het Handvest van de Grondrechten. Mijn collega Van Tongeren heeft daarom in de Tweede Kamer het initiatiefwetsvoorstel ingediend om de Wet bewaarplicht voor telecommunicatiegegevens in te trekken. Wij wachten nog op een reactie van het kabinet op dit arrest. De eerste reactie van staatssecretaris Teeven was weinig hoopgevend, moet ik zeggen. Zou het kabinet in deze reactie ook kunnen meenemen of naast wettelijke aanpassing ook de Grondwet zou moeten worden aangepast?

Verder is de vraag of we naast wetgeving niet vooral de techniek zouden moeten aanpassen om zelfbeperking te garanderen. Zo zouden we meer kunnen investeren en regelen om bijvoorbeeld encryptie aan burgers te kunnen aanbieden. Ook door meer regels te stellen via privacy by design kan de overheid ervoor zorgen dat alleen wordt opgevangen wat noodzakelijk en toegestaan is.

Een andere mogelijkheid waaraan gedacht kan worden, is om de inlichtingen- en veiligheidsdiensten zo in te richten dat het niet te verleidelijk is om misbruik te maken van bevoegdheden en mogelijkheden. De diensten zouden bijvoorbeeld alleen bevoegd kunnen worden gemaakt voor de analyses zelf, waarbij ze de gegevens laten vergaren door een andere organisatie. De verzoeken van de diensten zouden dan worden geregistreerd en gekoppeld aan een specifiek onderzoeksproject. Daarnaast zou een ruimere klokkenluidersregeling helpen om ambtenaren die misbruik constateren het te laten aandurven om dit misbruik ook te melden. Graag hoor ik een reactie op deze suggesties.

Ik heb nog een aantal opmerkingen over het toezicht. De controle op het handelen van de inlichtingen- en veiligheidsdiensten is onbevredigend. Dat geldt voor zowel de rechtmatigheidstoets van de CTIVD als de parlementaire doelmatigheidstoets. De CTIVD toetst alleen achteraf. De evaluatiecommissie heeft de aanbeveling gedaan voor een onmiddellijke toets door de CTIVD bij de uitoefening van bijzondere bevoegdheden. Hoe denkt het kabinet hierover? Dat zou de rechtmatigheidstoets meer naar voren halen in de procedure, waardoor onrechtmatige handelingen sneller kunnen worden gestaakt. Mijn fractie juicht dit toe. Het kabinet is in elk geval geen voorstander van een bindend rechtmatigheidsoordeel van de CTIVD, omdat dit tot de eindverantwoordelijkheid van de politiek zou behoren. Het is de vraag of dit ook bij een rechtmatigheidstoets zou moeten gelden. De CTIVD toetst aan de normen in de wetgeving. Ik ga ervan uit dat de minister of de Kamer een onrechtmatige actie toch nooit zou willen goedkeuren. Waarom zou deze commissie van toezicht dit niet op een bindende wijze kunnen doen?

Een ander punt is of de CTIVD ook een doelmatigheidstoets zou moeten uitvoeren. Mijn fractie ervaart het als een groot gemis dat die toets eigenlijk nergens goed extern is belegd. Deelt het kabinet dit en, zo ja, welke oplossingen ziet het hiervoor? Wellicht zou de Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, de commissie-stiekem, daarvoor toegerust moeten worden, of zou deze Kamercommissie duidelijker criteria moeten vaststellen voor de doelmatigheid, aan de hand waarvan de CTIVD zou kunnen toetsen.

In elk geval lijkt er nu wel consensus over te bestaan dat de huidige politieke controle via de commissie-stiekem gebrekkig is, onder andere vanwege het grote kennisverschil tussen het ministerie en de diensten enerzijds en de fractievoorzitters anderzijds. De Kamercommissie zou moeten worden uitgebreid met een fractiespecialist en een deskundige staf die in staat is om informatie te analyseren en de juiste vragen te formuleren. Wat onze fractie betreft zouden wij niet alleen moeten denken aan extra griffie, maar bijvoorbeeld ook aan het inhuren van experts, mits zij garant kunnen staan voor de vertrouwelijkheid. Alleen op die manier zou het parlement de analyses van de diensten kunnen doorgronden en beoordelen en zelf meer sturing kunnen geven aan de doelmatigheid van het werk van de diensten.

Tevens moeten wij ons de vraag stellen of ook andere overheidsdiensten dan de inlichtingen- en veiligheidsdiensten wellicht zoveel doen aan interceptie en opslag van gegevens dat ook voor hen een toezichthoudende commissie noodzakelijk zou moeten zijn. Ik denk aan de FIOD, de IND — die als het aan de evaluatiecommissie ligt nog vaker moet worden betrokken — en de Nationale Politie. Graag ontvangen wij op dit punt een reactie.

Het toezicht van de burgers zelf vormt een interessante dimensie. In artikel 29 van de Data Protection Working Party wordt gepleit voor meer transparantie voor burgers over

de werkwijze van surveillanceprogramma's. Wij hadden al een aantal expertmeetings nodig om te doorgronden hoe het werkt, dus men kan nagaan hoe het voor andere burgers is. Op die manier zouden de burgers meer inzicht kunnen krijgen in de wijze waarop een en ander werkt en zich daarvan meer bewust kunnen worden, en hebben zij ook meer mogelijkheid om zich te mengen in discussies over wat nog gelegitimeerd is en wat niet. Op die manier kunnen de surveillanceprogramma's meer democratisch worden ingebed. Tenslotte is het ook voor de veiligheid van de burgers dat wij de rechten van de burgers soms schenden en daar inbreuk op maken.

Vervolgens enkele opmerkingen over het probleem van de omzeiling. Mijn fractie ziet op een drietal punten het gevaar dat het wettelijk kader dat wij hebben relatief gemakkelijk kan worden omzeild. Ik loop de drie punten even langs.

Ten eerste gelden de waarborgen voor de verifieerbaarheid van bewijsmiddelen in het strafrecht en de privacywaarborgen bij de uitvoering door overheidsorganisaties doorgaans niet voor de meer schimmige praktijk van de inlichtingen- en veiligheidsdiensten. Gegevens die via inlichtingen- en veiligheidsdiensten worden verzameld, kunnen vrij gemakkelijk worden "witgewassen" en vervolgens een rol spelen in strafrechtelijke procedures. Burgers die verdacht worden, worden daarmee op achterstand gezet. Zouden strafrechters en advocaten niet meer inzicht moeten hebben in deze gegevens, om de gelijkwaardigheid tussen partijen terug te brengen?

Ten tweede staan diensten onder de beperking van hun nationale wetgeving, maar mogen zij data van hun collegadiensten gebruiken zonder dat die aan de nationale criteria hoeven te voldoen. Dit zorgt voor het gevaar van uitruil van data, zelfs van verzoeken aan internationale collega's om data te verzamelen in een ander land. Al dan niet intentioneel wordt nationale wetgeving hiermee ontdoken. Dit vraagt van de diensten waarmee de Nederlandse diensten samenwerken om transparante minimumeisen waaraan de nationale wetgeving moet voldoen. Uiteraard gelden er al minimumeisen voor de samenwerking met landen, maar de vraag is of die voldoen. Moeten die niet, behalve op meer algemene voorwaarden, ook zien op wetgeving?

De **voorzitter**:
Mevrouw Strik, kunt u langzamerhand afronden?

Mevrouw **Strik** (GroenLinks):
Ja.

Een voorbeeld is de VS. Dit land sluit Unieburgers uit van de grondwettelijke bescherming waar Amerikaanse burgers zich wel op kunnen beroepen. Internetproviders en andere bedrijven die hun hoofdzetel in de VS hebben, worden op grond van de Patriot Act gedwongen om gegevens af te staan aan de VS. Op deze manier wordt nationale en zelfs Europese bescherming van onze privacy ondermijnd. Zou de EU zich op dit punt niet krachtiger moeten kunnen opstellen? De lidstaten van de Unie hebben de Unie nadrukkelijk uitgesloten van bevoegdheid op het gebied van inlichtingen- en veiligheidsdiensten. In de Europese ontwerprichtlijn en -verordening inzake privacy wordt daarom niet veel geregeld over inlichtingen- en veiligheidsdiensten. Wel staat als gevolg van Snowden een nieuwe bepaling in de verordening dat bedrijven worden verboden om gegevens van Unieburgers over te dragen aan veiligheidsdiensten van niet-EU-landen. Dit brengt de bedrijven in de VS in een spagaat. Hopelijk leidt dit ertoe dat bedrijven druk gaan uitoefenen op de VS om uit die spagaat te komen. Zou echter ook de EU zelf niet in de onderhandelingen over het TTIP-vrijhandelsverdrag, of andere verdragen inzake dataoverdracht met de VS en Safe Harbour, moeten eisen dat ook de data van Unieburgers onder de Amerikaanse bescherming vallen?

Ten slotte nog één punt, te weten het probleem van de valspositieven. Dat probleem is levensgroot. Data komen om verschillende redenen incorrect in bestanden en gaan een eigen leven leiden. Onschuldige burgers raken daardoor in de problemen en hebben heel weinig mogelijkheden om op een snelle manier die gegevens te kunnen corrigeren. Dit houdt verband met allerlei oorzaken, waaronder de slechte kwaliteit van de opgeslagen gegevens, het mensenwerk van de opslag, maar ook met het feit dat mensen niet worden geïnformeerd over de opslag van hun gegevens, zodat zij niet kunnen corrigeren. Het houdt ook verband met de inherente onzekerheden van het op basis van algoritmes opsporen van onbekende feiten. Vooral echter als mensen niet weten dat gegevens over hen worden opgeslagen, kunnen zij natuurlijk niet vragen om correctie. De voorstellen van de commissie-Dessens om meer inzagerecht te krijgen in gegevens zijn goed. Dit kan echter niet los staan van het belang van meer notificatie van die gegevens. Wij begrijpen dat het werk van de veiligheidsdiensten zich er niet altijd voor leent om mensen erover te informeren dat hun gegevens worden gebruikt, maar misschien kan dit wel sneller achteraf gebeuren, of kunnen mensen, als er geen gevaar dreigt voor het werk van de inlichtingendiensten, vaker, beter en sneller worden geïnformeerd over het gebruik van hun gegevens.

□

De heer **Van Boxtel** (D66):
Voorzitter. Net als alle andere collega's herdenk ik bij dit debat met veel respect Willem Witteveen, mede vanwege het feit dat hij juist bij dit onderwerp enorm betrokken was en ook het voortouw genomen heeft om dit beleidsdebat hier te kunnen voeren. Door de bank genomen ben ik geen groot voorstander van het voeren van beleidsdebatten, maar dit beleidsdebat vind ik enorm belangrijk, omdat blijkt dat wij allemaal, dwars door alle partijen heen, worstelen met hetzelfde type vragen.

Wij leven in een wonderlijke tijd. Vanochtend nog lazen wij op teletekst dat Google een groot nieuw datacentrum zal vestigen in Groningen. Afgelopen vakantie las ik The Circle van Dave Eggers. Ik dacht toen: het zal toch niet waar zijn dat het allemaal die kant op gaat? De gang van zaken rond Snowden zit ons allemaal nog vers in het geheugen. Het zijn wonderlijke tijden; de digitale revolutie biedt heel veel kansen en mogelijkheden, maar tegelijkertijd ook veel bedreigingen. Tussen 1998 en 2002 mocht ik als minister verantwoordelijk zijn voor het overheidscommunicatiebeleid en de millenniumovergang. Iedereen voelde toen al aan dat wij aan de vooravond stonden van een digitale revolutie. Een echte digitale revolutie, dus geen industriële revolutie; die hadden wij 150 jaar daarvoor gehad.

Ik heb indertijd al eens gezegd dat de digitale ontwikkeling de individualisering van de mensen enorm versterkt en daarnaast de vertegenwoordigende representatieve democratie steeds meer onder druk zal zetten. Dat lijkt ook meer en meer het geval te zijn. Mensen verenigen zich in allerlei verbanden en vormen. In 2002 hadden wij nog nooit van Facebook of Twitter gehoord, maar nu zien wij steeds meer van dergelijke gremia opkomen. Ik ben benieuwd naar de zienswijze hierop van de minister van Binnenlandse Zaken, ook verantwoordelijk voor de Grondwet. Hoe ziet hij deze digitale ontwikkelingen in relatie tot de representatieve democratie? Is het voor hem aanleiding om zich eens met ons het hoofd te breken over de vraag hoe dit zich nu allemaal verder ontwikkelt? Voor een deel is dat misschien kijken in een glazen bol, maar toch is het echt van belang om niet alleen in termen van dienstverlening en digitalisering van de overheid te denken maar ook de vraag te stellen wat het doet met onze democratische rechtsorde.

Velen hebben er al aan gerefereerd. Collega Franken begon ermee en ging ook het verst terug. Ik trof vorig jaar een artikel in The New Yorker aan waarin nog eens de Mazzini-casus werd aangehaald, een casus die insiders bekend zal voorkomen: het ging om een Italiaan die in Engeland woonde en wiens brief werd geopend door de Britse overheid. Dat leidde tot een internationaal schandaal. De Amerikanen hadden het zelfs over een "barbarian breach of honor and decency". En dat ging dan nog maar over één geopende brief. Maar kijk waar we nu staan. We staan in het NSA-tijdperk, waarin "secrecy is what is known, but not to everyone" en waarin "privacy is what allows us to keep what we know to ourselves". Nou, met deze stellingen hebben we het allemaal verdomd moeilijk gekregen.

Vrijheid begint met het recht op de eigen levenssfeer. Door de almaar toenemende honger naar data en de daaruit resulterende dataverzameling door bedrijven, en vooral ook overheden, staan de privacy en de privacybescherming onder druk. Het nieuwe Utah Data Center van de NSA verwerkt per jaar 500 biljoen terabytes aan gegevens. Dat staat gelijk aan 23 miljoen jaar dvd's kijken. Het is echt theeblaadjes lezen en het levert niks op. Vorig jaar waren er de aanslagen bij de marathon in Boston. Dat was dramatisch en verschrikkelijk. Ze waren door niemand voorzien en door niemand ontdekt. De repressieve kant van de politie was fenomenaal: binnen een paar uur wisten we precies hoe het gedaan was, na 72 uur hadden we de foto's van de daders, acht uur later was één van hen gedood en een paar dagen later was de tweede vastgezet. Hieruit blijkt dat de repressieve kant heel effectief werkte, maar alle preventie daarvoor leidde tot niets, echt niets. Dat stelt toch vragen over wat we aan het doen zijn.

Regelmatig worden veiligheid en privacy gezien als tegenstellingen. Wij zien privacy echter als een vorm van persoonlijke veiligheid. Het beschermt burgers tegen censuur, identiteitsfraude en misbruik van macht. Een samenleving, of wereld eigenlijk, waarin niemand zich kan verbergen, is wat mijn fractie betreft niet veilig. Het is wel noodzakelijk dat burgers en bedrijven — het begint bij mensen en instellingen zelf — zich er permanent bewust van zijn dat zij zo veel mogelijk moeten doen om persoonlijke digitale gegevens zo goed mogelijk te beschermen. Dat vergeten we weleens in dit soort debatten. Ook anderen hebben daar de vinger bij gelegd. Welke inspanningen verricht de overheid in meer structurele vorm om burgers en bedrijven zich hiervan permanent bewust te laten zijn en zich hiervoor te equiperen? Ik weet dat de overheid samenwerkt met een instituut als ECP, maar er kan veel meer gebeuren. Het moet echt bij de mensen en instellingen zelf beginnen.

Vanzelfsprekend zijn internet en digitale technologie niet meer weg te denken uit de huidige wereld. Ik heb ook niemand horen roepen: zullen we ermee ophouden? Dat is ondenkbaar. Technologische ontwikkelingen hebben geleid tot een explosieve groei van data die elke seconde gegenereerd worden, en tot een groei van de diversiteit van gegevens die gegenereerd en verzameld worden. Digitale aanvallen op onder andere de bankensector door internetcriminelen, spionagepraktijken door buitenlandse overheden of ronselpraktijken voor jihadstrijders hebben ons in de afgelopen jaren doen inzien dat die gigantische berg aan data, om het zo maar even te noemen, aantrekkelijk is voor kwaadwillenden. Inmiddels weten we dat onze ICT-infrastructuur kwetsbaar is en zo goed mogelijk beschermd moet worden tegen cybercrime, spionage, digitale oorlogvoering en sabotage, om zo diefstal te voorkomen van onze staatsgeheimen, ons intellectuele eigendom en, niet in de laatste plaats, onze persoonsgegevens. Ook onze eigen inlichtingen- en veiligheidsdiensten maken gebruik van nieuwe en steeds verdergaande technologieën om in binnen- en buitenland gegevens te vergaren, te onderzoeken en te analyseren. De onthullingen van Snowden hebben ons duidelijk gemaakt dat het debat in Nederland over de werkwijze van de diensten, de juridische inbedding van de bevoegdheden en de organisatie van het toezicht op de diensten hoognodig is. Collega De Vries haalde ook nog even het bizarre feit aan dat de man die als klokkenluider de vrijheid van de burgerrechten naar buiten bracht, ons nu kaartjes stuurt met "from Russia with love". Dat is toch wel de wereld op zijn kop. Ik krijg hierop graag een reactie van het kabinet.

Ik kom op de diensten. Duidelijk is dat de AIVD en de MIVD volgens de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) alleen niet-kabelgebonden communicatieverkeer ongericht mogen vergaren. Mijn fractie ziet ook in dat het onderscheid tussen kabelgebonden en niet-kabelgebonden interceptie in de huidige samenleving, waarin bijna alle telecommunicatie over de kabel gaat, niet meer aansluit bij de praktijk. De vragen zijn ook door anderen gesteld, dus ik houd het kort. De commissie-Dessens heeft in haar rapport geadviseerd om die wet te verruimen. Wij zien echter ook dat de waarborgen en het toezicht ten aanzien van de bevoegdheden van de diensten nog niet optimaal zijn ingericht en nog niet optimaal functioneren. De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft in haar toezichtsrapport nummer 38 van dit voorjaar diverse onrechtmatigheden in het werk van de diensten geconstateerd. De D66 fractie ziet graag dat eerst wordt besproken hoe dergelijke onrechtmatigheden precies kunnen worden verholpen of voorkomen, zodat huidige en toekomstige waarborgen voor de bescherming van de persoonlijke levenssfeer betekenisvol kunnen worden ingevuld, voordat wordt overgegaan tot het uitbreiden van de bevoegdheden van onze diensten. Graag horen wij in dit beleidsdebat hoe het kabinet hierover denkt en wat het eraan gaat doen. Ook ontvangen wij graag een nadere toelichting van het kabinet over zijn zienswijze ten aanzien van het genoemde onderscheid in de Wiv tussen kabelgebonden en niet-kabelgebonden interceptie. Wil het kabinet het advies van de commissie-Dessens klakkeloos volgen om het weer ongebreideld te laten doen? Of zal het er veel selectiever mee omgaan, zoals ook collega Franken en anderen vroegen?

Ik kom op het hacken. Uit documenten van de Amerikaanse inlichtingendienst NSA, naar buiten gebracht door Snowden, is bijvoorbeeld gebleken dat ook de AIVD gehele webfora hackt en persoonsgegevens en inhoudelijke communicatie verzamelt. De CTIVD heeft in haar toezichtsrapport nummer 38 aangegeven dat het verwerven van webfora waarbij alle deelnemers op voorhand als onderzoekssubjecten van de AIVD kunnen worden aangemerkt, al snel voldoet aan de vereisten van proportionaliteit en subsidiariteit. De commissie waarschuwt echter dat dit anders ligt bij webfora die ook gegevens bevatten van personen die niet zijn aan te merken als potentiële onderzoekssubjecten van de dienst. Volgens de commissie dienen bij het verwerven en het leegtrekken van dergelijke webfora zwaarwegende operationele belangen aanwezig te zijn wil het proportioneel zijn om de communicatie te verwerven van personen die daartoe vanuit het perspectief van de nationale veiligheid geen aanleiding geven. In een nog recenter onderzoek heeft de CTIVD geconstateerd dat in een aantal gevallen het hacken van grote webfora niet voldeed aan het beginsel van proportionaliteit en dat deze verwerving onrechtmatig was, omdat de inbreuk op de persoonlijke levenssfeer van de overige gebruikers van de fora niet in verhouding stond tot de te verwachten opbrengst van de gegevens.

Het hacken van computers, het binnendringen in een geautomatiseerd netwerk, is een van de bijzondere bevoegdheden die de diensten mogen inzetten om informatie te vergaren. Webfora vormen natuurlijk een belangrijke bron van inlichtingen voor de diensten, maar het binnendringen in grote webfora met vele bezoekers om enorme hoeveelheden gegevens te verzamelen, is een grote inbreuk op de privacy van burgers. Dergelijke sleepnetmethodes, in de internationale visvangst allang verboden, zorgen ervoor dat de dienst de gegevens van alle gebruikers van een forum in handen krijgt. Volgens het ministerie van Binnenlandse Zaken past het inbreken in webfora binnen artikel 24 van de Wet op de inlichtingen- en veiligheidsdiensten. Deskundigen op het gebied van privacy en informatierecht vinden deze methodes echter veel te ver gaan. Hoogleraar informatierecht Nico van Eijk heeft in NRC Handelsblad gezegd dat de AIVD een grens overgaat: "Ze trekken een sleepnet door internetfora en nemen de data van willekeurige personen mee. Dit leidt tot een surveillancestaat." Hoogleraar recht in de informatiesamenleving Gerrit-Jan Zwenne vertelde in diezelfde krant dat de AIVD met deze "ongelooflijke privacyinbreuk" een pijler onder onze rechtstaat "weg zaagt". Mijn fractie is benieuwd naar de reactie van het kabinet in dit debat op deze observaties en ontvangt ook graag een standpunt van de bewindslieden over de inzet van deze sleepnetmethodes bij grote en drukbezochte webfora. Is het volgens de bewindslieden überhaupt mogelijk om bij sleepnettechnieken ervoor te zorgen dat de inzet proportioneel blijft?

Ik kom bij de metadata. Uit rapporten van de CTIVD en uit de gesprekken en bijeenkomsten met experts voorafgaand aan dit debat — waarvoor dank — is naar voren gekomen dat metadata, of gebruikergegevens, want dat zijn het eigenlijk, bijzonder privacygevoelig zijn. Los van het feit dat de inhoud van de communicatie en de metadata op internet sterk door elkaar lopen, geeft inzicht in en analyse van de kenmerken van communicatie een duidelijk inzicht in de persoonlijke levenssfeer: welk nummer belt met welk nummer, hoelang en wanneer? Ook bewegingspatronen en positie in het sociaal netwerk worden hierin meegenomen volgens het Rathenau Instituut. Het is ook belangrijk om te beseffen dat data inzicht kunnen geven, maar dat dit niet automatisch problemen oplost. Data-analisten kunnen fouten maken. Gegevens kunnen worden gemanipuleerd en de vraag kan worden opgeworpen of de verzamelde data wel echt de werkelijkheid weergeven.

Vorig jaar zei het hoofd van de MIVD dat de dienst het verzamelen van verkeersgegevens ziet als een "minimale privacyinbreuk". Het kabinet zegt in zijn reactie op het onderzoek van commissie-Dessens: bulkinterceptie en analyse van metadata zijn onder omstandigheden — cursief — ingrijpender dan een kortstondige — ook cursief — interceptie van de inhoud van telecommunicatie. Met andere woorden: het verzamelen van heel veel metadata kan in bepaalde gevallen ingrijpender zijn dan het afluisteren van de inhoud van communicatie gedurende een korte periode. Naar de mening van mijn fractie onderkent het kabinet hier niet in stevige bewoordingen dat deze gegevens over communicatieverkeer anno 2014 zeer privacygevoelig zijn. De D66-fractie hoort graag van het kabinet of zijn zienswijze ondertussen is veranderd en zo nee, waarom niet.

Ook de CTIVD geeft in haar toezichtsrapport 38 aan dat deze verkeersgegevens voor een deel aangemerkt moeten worden als persoonsgegevens, waardoor het verwerken ervan een inbreuk vormt op de persoonlijke levenssfeer. De commissie schrijft dat het van belang is dat het proces van metadata-analyse bij wet wordt voorzien van waarborgen die beschermen tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer. Wij horen graag of het kabinet al onderzocht heeft hoe de nodige waarborgen, zoals het motiveren van de noodzakelijkheid, de proportionaliteit en de subsidiariteit van de gegevensverwerking, ten behoeve van interne dan wel externe toestemming kunnen worden ingebouwd in de wet.

Dan heb ik nog een vraag over de samenwerking met buitenlandse diensten. De commissie-Dessens heeft geconcludeerd dat het op grote schaal delen van bulkdata wettelijk niet goed geregeld is. De juridische onderbouwing van de dataruil is zwak. Ook lijkt de wet alleen te voorzien in incidentele samenwerking, aangezien voor elke vorm van samenwerking toestemming is vereist van de minister. In de reactie op de conclusies van de commissie onderschrijft het kabinet dat onderzocht moet worden of de wet voldoende rechtsstatelijke en democratische garanties biedt bij de samenwerking met buitenlandse diensten. Ook hierop krijg ik graag een nadere toelichting van de bewindslieden. Is nu al duidelijk hoe het kabinet gaat zorgdragen voor voldoende rechtsstatelijke en democratische waarborgen in de wet, en kan het kabinet aangeven in welke situaties het delen van bulkdata met buitenlandse inlichtingendiensten gerechtvaardigd is? Kan het kabinet in deze toelichting de vraag betrekken hoe de toetsing op proportionaliteit en subsidiariteit, zoals gevraagd in het EVRM, is geregeld wanneer buitenlandse diensten gegevens over Nederlandse burgers in hun bezit krijgen door een uitwisseling van data? Wij zien graag, net als meerdere deskundigen op dit gebied, dat bestaande en nog in te voeren bevoegdheden op het gebied van grootschalig en ongericht verzamelen van communicatiegegevens door de diensten, onderworpen worden aan een volwaardige kritische analyse. Is het kabinet voornemens om een dergelijke "kosten-batenanalyse" te maken?

Dat brengt mij bij het toezicht. De veranderingen in de intelligence-praktijk vragen om aanscherping van het toe-

zicht en de toestemmingsvereisten, zo stelt het Rathenau Instituut. De commissie-Dessens heeft in haar rapport over de herziening van de wet voorstellen gedaan voor tijdig, onafhankelijk en bindend bestuurlijk toezicht. De CTIVD heeft deze voorstellen onderschreven. Ook wetenschappers hebben zich hierover uitgelaten. Zo stellen de hoogleraren informatierecht Egbert Dommering en Nico van Eijk dat de noodzaak van grootschalig en ongericht verzamelen en raadplegen van metadata vooraf door een onafhankelijke commissie getoetst dient te worden. Het niet-bindende rechtmatigheidsadvies achteraf van de CTIVD is wat hen betreft niet voldoende. De D66-fractie deelt die visie. Ook uit rechtspraak van het Hof van Justititie van de Europese Unie en het Europees Hof voor de Rechten van de Mens blijkt dat toezicht op de diensten in principe justitieel toezicht vooraf dient te zijn.

Mevrouw **Gerkens** (SP):
Ik hoor nu het woord "justitieel" erbij.

De heer **Van Boxtel** (D66):
Ja.

Mevrouw **Gerkens** (SP):
Ik heb zelf ook nagedacht over de vraag die de heer Van Boxtel nu stelt. Als je vooraf gaat toetsen, loop je het risico dat je al bijna gaat sturen. Dan zou de politiek kunnen beïnvloeden wat de veiligheidsdiensten zouden moeten doen. Het argument daartegen is dat de veiligheidsdiensten juist zelf moeten aandragen waar zij denken dat de risico's liggen. Hoe kijkt de heer Van Boxtel daartegen aan?

De heer **Van Boxtel** (D66):
Ik wil de redenering geheel omdraaien. Als veiligheidsdiensten gerede aanleiding zien om een dergelijke activiteit uit te voeren, vind ik het in een democratische rechtsorde volstrekt gepast om dan ook een toetsing los te laten op die veronderstelling. Als die goed in elkaar zit en deugt, kun je toestemming geven en ben je ook afgedekt, terwijl we nu gewoon überhaupt niet weten wat er gebeurt. Ik noem het dus niet voor niets allemaal in het licht van de rechtsorde.

Voorzitter. Ik zei zonet dat het Hof van Justitie en het Europees Hof voor de Rechten van de Mens dit delen. Zij vinden dat toezicht op de diensten in principe justitieel toezicht vooraf dient te zijn.

Ook kwam in de deskundigenbijeenkomst voorafgaand aan dit debat naar voren dat de huidige bezetting van de CIVD, de commissie-stiekem in de volksmond, ervoor zorgt dat er geen structurele controle uitgeoefend kan worden. Is weleens geopperd om de CIVD in te vullen met specialisten? Ook collega De Vries vroeg daarnaar. Hij ging zelfs verder en vroeg: moet daarbij misschien ook de Eerste Kamer worden betrokken? Mijn volgorde zou zijn: het mag primair bij de Tweede Kamer blijven, maar dan ook echt volwaardig en kwalitatief goed geborgd, en misschien met een andere of bredere samenstelling dan de huidige. Als dat allemaal niet kan, zou ook een rol voor de Eerste Kamer misschien kunnen, maar ik hoor eerst graag de reactie van het kabinet.

De heer **Franken** (CDA):
Haalt de heer Van Boxtel niet twee organen door elkaar?

De heer **Van Boxtel** (D66):
Nee, ...

De heer **Franken** (CDA):
De commissie-stiekem is een politiek orgaan, en de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten is een onafhankelijke commissie ...

De heer **Van Boxtel** (D66):
Jaja, maar ik had het ook eerst over die onafhankelijke commissie en later over de commissie-stiekem. Je hebt de CTIVD en je hebt de CIVD, en dat is de commissie-stiekem. Als u goed geluisterd had, had u gehoord dat het een ander moment was.

Nu ik toch over de CTIVD praat: ook daarin zouden misschien andere expertises nog een rol kunnen vervullen. Ik vond de suggestie van collega Gerkens om daarbij vooral ook de ethische kant te betrekken, een heel interessante. Je zou ook kunnen denken aan een lid van het CBP, het College bescherming persoonsgegevens. Dit zou kunnen waarborgen dat het belang van de privacy in de onderzoeken naar de diensten meer gewicht krijgt. Ik krijg graag een reactie van het kabinet op deze gedachte.

Ook rijst de vraag of de CTIVD, die structureel toetst op rechtmatigheid, niet ook structureel op doelmatigheid dient te toetsen. Ik hoorde ook andere collega's hiernaar vragen. Die doelmatigheid wordt eigenlijk steeds interessanter. Ik gaf het voorbeeld van de onwaarschijnlijke hoeveelheid preventief dataonderzoek die eigenlijk tot niets leidt, en wat dat kost. Daar gaan miljarden en miljarden in om, terwijl de effectiviteit gewoon niet aangetoond is. Als het anders is, hoor ik het graag, maar er is in ieder geval geen balans tussen de hoeveelheid geld die we erin stoppen en de revenuen die we er in termen van veiligheid uithalen. Ik hoor dus graag ook een reactie op de doelmatigheidstoets. En wat is de reactie van het kabinet op een idee van de heer Wiebes, voormalig senior analist van de Nationaal Coördinator Terrorismebestrijding en Veiligheid, om hier bijvoorbeeld een aparte staatssecretaris op te zetten?

Tot slot kom ik bij de Europese component. Dit debat is wat mijn fractie betreft niet compleet zonder het noemen van de herziening van de Europese privacywetgeving die momenteel gaande is. Het gaat zoals bekend om een algemene verordening bescherming persoonsgegevens en om een richtlijn die betrekking heeft op de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële activiteiten. Hier zien wij een rol voor de Nederlandse overheid weggelegd. Mijn fractie vindt het van groot belang dat de verstevigde privacyregels in de verordening niet alleen voor het bedrijfsleven gaan gelden, maar ook voor overheden, aangezien overheden vaak zeer gevoelige gegevens van hun burgers beheren. De voorbeelden zijn al genoemd, variërend van de IND, de COA, de Belastingdienst en de sociale diensten. Het zou goed zijn als de overheid ook wat dit betreft aan de normen dient te voldoen en zichzelf niet kan vrijstellen van regels die zij verplicht stelt voor het bedrijfsleven. Het is belangrijk dat

Nederland zich daarvoor blijft inzetten in de Raad van Ministers. Op welke wijze zien deze bewindslieden erop toe dat dit ook gebeurt?

Voor een effectieve politie- en justitiesamenwerking in Europa is een gedegen bescherming van persoonsgegevens noodzakelijk. Mijn fractie is van mening dat het aannemen van de richtlijn voor de bescherming persoonsgegevens een belangrijke plek moet krijgen bij de verdere samenwerking. Een hoog niveau van dataprotectie is essentieel. Wat betreft de richtlijn vinden wij het van belang dat de regels ook zullen gelden voor de politiële en justitiële diensten zelf, en niet alleen voor de uitwisseling van gegevens. Kunnen de bewindslieden toelichten wat de stand van zaken is bij de behandeling van de richtlijn?

Ik rond af. In het digitale tijdperk horen de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens tot de kern van onze burgerrechten. Daar moeten mensen ook zelf wat voor doen, zeg ik erbij. Bevoegdheden, verantwoording en toezicht dienen onderling in balans te zijn. Nederland heeft op veel onderwerpen een voorlopersrol ingenomen. Denk aan de strijd tegen het water, de Deltawerken, en alles wat we wat dat betreft doen. We exporteren kennis op dat gebied. Wat let ons — ik daag de bewindslieden daar haast toe uit — om een digitaal deltaplan te ontwerpen over de internetrevolutie, de dataverwerking en het databeheer? Dat kunnen we vervolgens in samenhang aan Europa maar ook mondiaal laten zien. We hebben namelijk onwaarschijnlijk veel IT-knowhow in dit land. Er vindt heel veel innovatie plaats en we hebben ook heel veel kennis van veiligheid daaromtrent. Kwade tongen beweren weleens dat dit kabinet door zijn hervormingsagenda heen zou zijn, maar ik vind dit typisch een onderwerp waarbij je geen dag op je handen kunt blijven zitten. Ik zou het kabinet willen uitdagen om ons meer, dieper en fanatieker mee te nemen in hoe wij de digitale revolutie voor onze inwoners tot een kansrijk geheel kunnen maken, en hoe wij die tot een goed einde willen brengen.

De **voorzitter**:
Dank, mijnheer Van Boxtel.

De beraadslaging wordt geschorst.

De vergadering wordt enkele ogenblikken geschorst.

Voorzitter: Linthorst