Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2019–2020

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en nzake de generieke digitale infrastructuur (Wet digitale overheid)

G

VERSLAG VAN EEN DESKUNDIGENBIJEENKOMST

Vastgesteld 3 september 2020

De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis van de Koning[1] heeft op 30 juni 2020 gesprekken gevoerd over **Wet digitale overheid**.

Van deze gesprekken brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,
Dittrich

De griffier van de commissie,
Bergman

[1] Samenstelling: Kox (SP), Koffeman (PvdD), Ganzevoort (GL), De Boer (GL), Van Hattem (PVV), Pijlman (D66), Rombouts (CDA), Schalk (SGP), Koole (PvdA). Klip-Martin (VVD), Baay-Timmerman (50PLUS), Wever (VVD), Bezaan (VVD), Van der Burg (VVD), Crone (PvdA), Dessing (FVD), Dittrich (D66), (voorzitter), Doornhof (CDA), Frentrop (FVD), Gerbrandy (OSF), Van der Linden (FvD), Meijer (VVD), Nanninga (FVD), Nicolaï (PvdD), (ondervoorzitter), Rietkerk (CDA), Rosenmöller (GL), Verkerk (CU) en De Vries (Fractie-Otten).

kst-34972-G
ISSN 0921 - 7371
's-Gravenhage 2020

Voorzitter: Dittrich
Griffier: Bergman

Aanwezig zijn tien leden der Kamer, te weten: Van der Burg, Dittrich, Ganzevoort, Gerkens, Van Hattem, Koole, Van Pareren, Rombouts, Schalk en Verkerk,

alsmede de volgende deskundigen:

Thema 1: Privacy en bescherming van persoonsgegevens (onder andere dataminimalisatie, commercieel gebruik gegevens, centrale versus decentrale opslag)
Aleid Wolfsen – Autoriteit Persoonsgegevens
Vincent Böhre – Privacy First

Thema 2: De WDO als kaderwet en betrokkenheid van het parlement
Pieter van Boheemen – Rathenau Instituut
Peter van Lochem – oud-rector van de Academie voor Wetgeving

Thema 3: Toegankelijkheid van de publieke dienstverlening (inclusief aspecten als betaling en algoritmen)
Lisanne Bos en Geke van Velzen – Stichting Lezen en Schrijven
Reinier van Zutphen – Nationale ombudsman

Thema 4: Handhaafbaarheid in de breedste zin
John Derksen – Agentschap Telecom
Lokke Moerel – hoogleraar Global ICT law, Universiteit van Tilburg; lid Cyber Security Raad

Aanvang: 9.31 uur.

De **voorzitter**: Goedemorgen. Ik heet iedereen van harte welkom. Dat zijn allereerst de deskundigen in blok 1, en daarnaast ook de collega-Kamerleden en degenen die via de livestream deze bijeenkomst volgen. We zijn hier vandaag bijeen in een deskundigenbijeenkomst. Daarin bespreken we het wetsvoorstel Wet digitale overheid, de WDO. Dat voorstel vormt, als het aan de regering ligt, het eerste deel van wetgeving ten behoeve van verdere digitalisering van de overheid op verschillende niveaus.
Ik zal even een korte toelichting geven, zodat iedereen weet waar we het precies over hebben. Het wetsvoorstel is op 18 februari van dit jaar door de Tweede Kamer aanvaard. De Eerste Kamercommissie voor Binnenlandse Zaken heeft in maart besloten dat zij eerst een technische briefing wilde, te verzorgen door ambtenaren van het Ministerie van Binnenlandse Zaken, en daarna een deskundigenbijeenkomst. En die laatste is dus vandaag aan de orde. De technische briefing heeft al plaatsgevonden op 26 mei jongstleden.
We hebben afgesproken dat de deskundigenbijeenkomst twee uur duurt. We hebben vier subthema's. Voor elk thema hebben we dus een klein 30 minuten. De bedoeling is dat de sprekers in maximaal vijf minuten hun visie op het wetsvoorstel toelichten. Daarna geef ik de leden de gelegenheid om vragen te stellen. Ik wil iedereen erop wijzen dat de deskundigen van tevoren hun positie hebben bepaald in een paper dat aan de commissie is toegestuurd. Die zijn ook toegevoegd aan de stukken voor de vergadering van vandaag. Ik zal tussendoor nog even wat huishoudelijke mededelingen doen over ontsmetting en dergelijke in het kader van de COVID-19-maatregelen.

Thema 1: Privacy en bescherming van persoonsgegevens (onder andere dataminimalisatie, commercieel gebruik gegevens, centrale versus decentrale opslag)

De **voorzitter**: We beginnen nu met thema 1. Dat gaat over privacy en bescherming van persoonsgegevens. Het gaat onder andere over dataminimalisatie, het commercieel gebruik van privégegevens, centrale versus decentrale opslag en alles wat de deskundigen ons verder willen melden over hun visie op de WDO.
Het woord is allereerst aan de heer Aleid Wolfsen, die sinds 2016 voorzitter is van de Autoriteit Persoonsgegevens.

De heer **Wolfsen**: Dank u wel, meneer de voorzitter. Geachte leden, dank voor de uitnodiging om even iets te mogen zeggen over deze kaderwet, zoals dat heet. Het is een wet op hoofdlijnen, dus het zou inderdaad kort moeten kunnen. Dank dat u de leden attendeerde op de position papers die wij hebben geschreven. Ik zal het niet allemaal herhalen, maar ik zal datgene wat we hebben geschreven, hier en daar wat inkleuren met steekwoorden.
Ik begin een beetje met twee open deuren. Dat is allereerst de constatering dat de digitalisering enorm snel gaat. Die neemt toe en maakt innovatie mogelijk. We lopen daar in Nederland ook mee voorop. Daarom is dit soort wetgeving voor Nederland ook extra belangrijk. Maar aan de andere kant zeg ik bij ons in huis ook weleens: als het om digitalisering gaat, bevinden we ons wellicht nog in de middeleeuwen van wat ons allemaal nog te wachten staan. Het gaat in een razend tempo. Nederland loopt ermee voorop. Daar hebben we in de coronatijd ook wel voordeel van gehad, bijvoorbeeld met het videobellen en het thuis via internet kunnen kopen van allerlei zaken. Dat is allemaal ontzettend fijn. Het biedt ook allerlei kansen. Je kunt je belastingaangifte vrij gemakkelijk doen met een paar drukken op de knoppen, je kunt even zien hoe het ervoor staat met de studieschuld. Dat is allemaal heel fijn.
Tegelijkertijd brengt dit ook grote risico's met zich mee. Echt serieuze risico's! Er wordt steeds meer over mensen vastgelegd. Je kunt zien waar iemand is. Nu zeg ik het even wat zwaar, maar dat kan ook onze democratische rechtsstaat kwetsbaar maken. Ik spreek vaak over de AVG. Mensen noemen dat vaak privacybescherming. Ik kan u een klein geheimpje verklappen, maar waarschijnlijk weet u dat al: het woord «privacy» komt in de AVG niet voor, niet één keer. Het gaat om gegevensbescherming. En als het om gegevensbescherming gaat, dan gaat het om de bescherming van de fundamenten van onze rechtsorde. Dat zijn natuurlijk alle grondrechten. Communicatie, privé, huisrecht, privacy; dat zit er allemaal achter. Dat wordt beschermd door je gegevens te beschermen. Ik noem de gelijkheid, de gelijkwaardigheid van mensen en het tegengaan van discriminatie. De democratie kan at stake zijn – zie wat er in Amerika en in Engeland is gebeurd – en de rechtsstaat zelf. Er zijn allerlei systemen om solidariteit te bewerkstelligen. Je verzekert je tegen onzekere gebeurtenissen. Maar ja, als alles voorspelbaar wordt, kun je je niet meer verzekeren. En zelfs de toegang tot de vreedzame conflictbeslechting – de rechtspraak – is in gevaar als heel veel digitaliseert, want soms weet je niet meer op basis waarvan wordt beslist. Dan kun je je niet meer verdedigen voor een rechter.
Dat is allemaal aan de orde als je praat over gegevensbescherming. Wij zijn de toezichthouder daarop. Dat zal ik u verder besparen, dat is vanzelfsprekend. En juist in deze tijden van corona, met allerlei nieuwe wetgeving, zijn we extra alert en soms ook extra streng.
Op twee manieren kan er inbreuk worden gepleegd op je grondrechten. Dat kan door je eigen wil of door de wet. Zo simpel is het eigenlijk. Dan is het uw wil of onze collectieve wil. De wetgeving maakt steeds meer mogelijk. De taken van de overheid worden ook steeds meer uitgebreid.

Als dat gebeurt, moet het toetsbaar en transparant zijn. Deze wet is daar een voorbeeld van. Als je er generiek naar kijkt, kun je zeggen dat de wet op zich goed lijkt, dat het goed is dat de overheid zich centraal bekommert om de technische infrastructuur. Een veilige en betrouwbare digitale infrastructuur is heel goed. U bent er ook over gebrieft, dat is op zich goed.
Ik ga met wat steekwoorden nog wat zorgen aan u voorleggen. Als wij kijken naar dat soort wetgeving, doen wij dat altijd aan de hand van zes vragen. Is het rechtmatig wat er gebeurt? Is het transparant en kun je zien wat er gebeurt? Is het behoorlijk; zitten er geen oneerlijke dingen in, bijvoorbeeld discriminatoire dingen? Ik noem dataminimalisatie, doelbinding en de belangrijkste vraag: is het ook veilig? Achter dat laatste heb ik een uitroepteken gezet. Wordt het goed beveiligd? Het gaat om inmenging in grondrechten. Dan moet het echt veilig zijn.
Ik zal voorts nog iets over de wet zelf zeggen. Ons wetgevingsadvies is al van 2017, dus de behandeling gaat niet helemaal in het tempo als dat waarin de digitalisering zich voltrekt. Dat gaat in een zeker rustig tempo. Dat gaat soms zo. Standaarden worden centraal voorgeschreven. Dat kunnen we steunen. Dan gaat het over het mailverkeer, over de beveiliging van sites en dat soort dingen. Prima! Maar dan kom ik bij de informatiebeveiliging. Zoals ik al zei: dat is key. Als we in willen loggen bij overheidsinstellingen, zijn we nu nog afhankelijk van DigiD. Dat is inmiddels 15 tot 17 jaar oud. Dat is qua beveiliging niet meer bij de tijd, dus dat moet vernieuwd worden. Er is zelfs een variant met alleen een wachtwoord en een gebruikersnaam. Dat is écht niet meer van deze tijd. Overheden kunnen zelf bepalen hoe je inlogt bij een overheid. Dat is ook niet goed. Dus dat de wetgever zich dat aantrekt, is heel mooi en heel belangrijk.
Maar het wordt ook mogelijk gemaakt dat private partijen die sleutels gaan afgeven. Dan gaat het dus om de manier waarop je inlogt bij een overheid. Op zich kan dat – dat leidt niet tot onrechtmatigheden – maar dan moet je wel weten hoe je dat regelt. En ook een privaat bedrijf kan best vaststellen of iemand degene is die hij zegt te zijn. Die kan best iemand identificeren, los van de vraag waar je toe geautoriseerd bent als je één keer bij de overheid ingelogd bent. Wij beoordelen het altijd beetje op beschikbaarheid, integriteit en vertrouwelijkheid. Als je meer partijen zo'n sleutel laat maken – ik zeg het even wat huiselijk – is het meer beschikbaar. Prima. Maar ja, als je het vergelijkt met een klassiek kasteel met ophaalbruggen, dan is één ophaalbrug die beveiligd wordt door de kasteelheer met zijn eigen sleutel, veiliger dan twee bruggen. Als je twee bruggen hebt en je hebt een private sleutel en een publieke sleutel, dan neemt de kwetsbaarheid toe. Het kan zijn dat degene die zo'n sleutel afgeeft – ik zeg het even wat huiselijk en wat beeldend – ook kan zien waar je inlogt. Privaat zeggen we vaak: als je elke dag bij het Antoni van Leeuwenhoekziekenhuis inlogt, dan weet je over het algemeen wel wat er aan de hand is. Maar als je bij de overheid inlogt, bij studiefinanciering of bij schuldhulpverlening, en een private partij kan zien dat je daar elke dag inlogt, dan weet die wel ongeveer wat er aan de hand is. Kun je dat koppelen met andere gegevens, ja of nee? Is het goed beveiligd, ja of nee? Dat moet je allemaal echt goed in de gaten houden. Ik leg het u nu wat vragend voor, maar u proeft wel lichte bedenkingen bij mij.
Ik heb afrondend nog twee andere onderwerpen. Dat is de uitwisseling van gegevens. Deze wet wil dat ook meer mogelijk maken. Er wordt dan gesproken over koppelingsvlakken. Dat is natuurlijk allemaal jargon. Het gaat erom dat je heel makkelijk tussen overheidsinstellingen data kunt uitwisselen. Burgers vinden dat vaak ook wel prettig. Het moet gefaciliteerd worden via wetgeving. Maar ja, de overheid weet steeds meer. Daardoor wordt het vaak ook steeds onduidelijker wat de overheid van je weet en waar die data zitten. Ik luister bij ons vaak mee bij telefoontjes. Vaak vragen mensen: hoe weten ze dat eigenlijk allemaal over mij? Dat

geeft een heel onbehaaglijk gevoel: dat de ene overheid wat weet, terwijl je die informatie aan een andere overheid hebt gegeven. Bij bedrijven is het idem dito. De mensen zeggen vaak: dat heb ik ook allemaal niet zo gewild. Dus alles wat makkelijker wordt, wordt op enig moment vaak ook gebruik.
Ik ga afronden, meneer de voorzitter. Proportionaliteit en subsidiariteit – ik doe het even in steekwoorden – gaat allemaal naar AMvB's. Wij zouden graag zien dat dat strakker in de wet geregeld wordt, dat ook de Kamer daarbij betrokken zijn. Die kaderwet maakt veel mogelijk, maar er wordt ook veel bij u weggehaald, weggehouden. Hoe zal ik dat netjes zeggen? En ik heb nog een afrondende opmerking over de FG's. Ik zou het ook fijn vinden als u bij de behandeling van de wet aandacht besteedt aan de positie van de functionaris gegevensbescherming bij overheden. Die hebben een interne toezichthoudende rol. Het is een buitengewoon belangrijke functie. En het is nog lang niet overal goed geregeld.
Voorzitter. Daar sluit ik mee af. Het is een kaderwet, er gaat veel naar AMvB's. Flexibiliteit zeker, maar het gaat wel om inbreuken op grondrechten. Weest u zich daar zeer bewust van – dat is in de Eerste Kamer zeker een open deur – want de grens tussen de twee uitersten van «fantastisch dat dit allemaal kan; geweldig» en «levensgevaarlijk wat hier gebeurt» wordt flinterdun. Die is eigenlijk nog nooit zo dun geweest. Dit zeg ik als een afsluitende waarschuwing aan u.
Dank u.

De **voorzitter**: Dank u wel, meneer Wolfsen van de Autoriteit Persoonsgegevens. We gaan meteen door met de volgende deskundige. Daarna kunnen we vragen stellen aan beide sprekers. De volgende deskundige is de heer Vincent Böhre. Hij is directeur van de stichting Privacy First. Aan u het woord.

De heer **Böhre**: Dank, voorzitter. Nogmaals dank voor uw uitnodiging om aan deze bijeenkomst deel te nemen. Onze voornaamste punten van kritiek op de huidige Wet digitale overheid hebben we reeds uiteengezet in onze position paper. Kortgezegd gaat het daarbij voornamelijk om de kwetsbaarheden en privacyrisico's van het nieuwe eID-stelsel, waaronder de volgende aspecten.
Ik noem allereerst de centrale in plaats van decentrale opzet van de infrastructuur. Over het algemeen is een centrale opzet riskanter en onveiliger dan een decentrale architectuur. Een decentrale opzet is ook meer in lijn met moderne privacyvereisten, zoals dataminimalisatie en privacy by design. Bovendien leent dit zich minder goed voor grootschalige hacks of heimelijke toegang, massale datalekken en function creep, oftewel sluipende doelverschuiving. Niet voor niets is er de laatste jaren in diverse gevoelige domeinen een ontwikkeling van centrale naar decentrale infrastructuren zichtbaar, bijvoorbeeld op het terrein van biometrie en in de medische wereld. Ook bij uitermate gevoelige persoonsgegevens als het bsn, het burgerservicenummer, en allerlei gevoelige transacties tussen burgers, bedrijven en overheden, zou dus bij uitstek voor een decentrale opzet gekozen moeten worden. Dat zou ook meer passen bij het idee van informationele zelfbeschikking en de slogan «Regie op Gegevens» van het Ministerie van Binnenlandse Zaken zelf. In dit verband is het een gemiste kans dat het wettelijk kader tot op heden onvoldoende gebaseerd is op een stelsel dat werkt aan de hand van minimale attributen. Dat wil zeggen relevante kenmerken van personen in plaats van volledige identificatie, waarbij veel meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is. Een actueel voorbeeld van een dergelijk privacyvriendelijk alternatief is IRMA – dat staat voor I Reveal My Attributes – dat op 28 januari 2018, de Europese Dag van de Privacy, de allereerste Nederlandse Privacy Award won. Vanuit gemeenten en wellicht

ook andere overheden lijkt daar ook steeds meer behoefte aan te zijn. Waarom wordt dit tot op heden niet wettelijk gefaciliteerd?
Een ander aspect, dat wij in onze position paper abusievelijk onvermeld gelaten hadden, is dat eID-middelen open source dienen te zijn. Dat is immers de meest effectieve manier om onbetrouwbare partijen buiten de deur te houden en de veiligheid en privacy te waarborgen. Open source zou daarom als harde eis toegevoegd moeten worden voor de toelating van eID-middelen.
Tevens zouden wij hier graag nogmaals willen benadrukken dat het eID-stelsel zoals dat nu in de Wet digitale overheid beoogd wordt, per definitie enorme risico's voor de privacy van burgers teweeg zal brengen, gezien de commerciële aard van nieuwe eID-aanbieders, waaronder techbedrijven met dubieuze businessmodellen en schimmige profileringspraktijken. Deze risico's lijken in dit wetstraject nog niet te zijn geadresseerd. Dit dient alsnog op democratische en toekomstbestendige wijze te gebeuren op het niveau van de parlementaire wet zelf, en niet in lagere bestuurlijke regelgeving.
Dank u wel voor uw aandacht.

De **voorzitter**: Dank u wel, meneer Böhre van de stichting Privacy First. We hebben nu een klein kwartier voor vragen. Ik kijk even naar de collega's. Wie wil er een vraag stellen? Ik begin bij de heer Van Hattem van de PVV. Een korte vraag, graag, en graag ook een kort antwoord.

De heer **Van Hattem** (PVV): Dank u, voorzitter. Dank ook aan de inleiders en alle anderen die een position paper hebben opgesteld. Ik heb twee heel korte vragen aan de heer Böhre. Allereerst noemt u centraal versus decentraal. Welke mogelijkheden ziet u binnen dit wetsvoorstel om met decentrale verwerking aan de slag te gaan? Verder noemde u op het laatst van uw betoog de enorme privacyrisico's. Kunt u dat misschien nog iets meer inkleuren met voorbeelden? Om welke privacyrisico's gaat het dan concreet?
Tot zover, voorzitter.

De **voorzitter**: Ik verzamel nog een paar vragen voordat we verdergaan met de antwoorden. Ik zie een vraag van mevrouw Gerkens van de SP.

Mevrouw **Gerkens** (SP): Dank u wel, voorzitter. Ik heb een vraag in vervolg op de laatste opmerking van de heer Böhre, over het adresseren van risico's in lagere regelgeving. U zegt dat dat in de wetgeving moet. Hoe vindt u dan dat terug moet komen? Hoe adresseer je die risico's?

De **voorzitter**: De heer Verkerk van de ChristenUnie.

De heer **Verkerk** (ChristenUnie): Ik had een vergelijkbare vraag. Betekent dit een novelle, dus eigenlijk nieuwe wetgeving?
Ook voor de heer Wolfsen had ik een vraag. U schrijft in uw position paper dat de WDO rust op een site die verouderde informatie bevat. Kunt u dat toelichten? U spreekt ook over koppelvlakken en doelbinding, met de gevaren daarvan. Kunt u iets zeggen over de vraag welke ethiek de overheid heeft of zou moeten hebben om daar goed mee om te gaan? Ik hoef alleen maar het Engelse woord «1984» te noemen. Mijn laatste vraag is: wat is de kwaliteit van het toezicht, met name met betrekking tot de koppelvlakken en de doelbinding? Heeft men voldoende middelen om goed toezicht uit te oefenen?

De **voorzitter**: De laatste in deze ronde is de heer Van Pareren van Forum voor Democratie.

De heer **Van Pareren** (FvD): Dank u, voorzitter. Ik heb eigenlijk maar één vraag, want veel vragen zijn al gesteld. Veel burgers hebben geen vermoeden waar hun gegevens zijn en welke gegevens bekend zijn. Is het ook mogelijk om toe te lichten hoe u denkt dat dat wel zou kunnen gebeuren? Want je kan wel angstig zijn dat je privacy er niet is, maar misschien heb je ook geen vermoeden waar het gevaar voor je privacy ligt. Ik denk dat het belangrijk is dat er een soort register komt, of dat daar inzicht in komt. Hoe kijkt u daarnaar?

De **voorzitter**: Ik laat het aan de heren achter de tafel over om te bepalen wie er gaat beginnen. We hebben tien minuten voor de beantwoording.

De heer **Böhre**: Er werd allereerst gevraagd naar mogelijkheden voor decentrale alternatieven. Daar heb ik reeds naar verwezen. Een bekend voorbeeld is IRMA, wat staat voor I Reveal My Attributes. Een ander voorbeeld is Soverin. Maar er zijn er wellicht nog meer. Je ziet bij dit wetsvoorstel dat het allemaal heel centraal georganiseerd lijkt en dat decentrale alternatieven überhaupt nauwelijks zijn overwogen. Die zaten vroeger wel meer in het wetsvoorstel. Dat was nog in 2017, toen er ook echt ruimte leek voor dat soort alternatieven. Ik heb dat ook in mijn position paper beschreven. Dat stond toen letterlijk in de memorie van toelichting, met een definitie vanuit de attributendiensten. Dat is er op een of andere manier uit gegaan. Ik weet niet hoe dat is gebeurd, maar het is eruit gehaald. Ik weet niet wat de krachten daaromheen waren destijds. Ik kan het heel concreet maken: als het aan ons zou zijn, zou artikel 1 van de wet bijvoorbeeld moeten worden herzien in die zin dat daarin alsnog een definitie van attributendienst zou moeten worden opgenomen. In artikel 5 dient die dienst als onderdeel van de generieke digitale infrastructuur te worden toegevoegd aan het eerste lid. En in artikel 9 dient een lid te worden opgenomen dat het mogelijk maakt om een private attributendienst toe te laten door verlening van een erkenning door Onze Minister. Dat zijn een paar mogelijkheden waarop ik had geanticipeerd in het kader van deze hoorzitting.
Verder werd er gevraagd hoe we de privacyrisico's beter kunnen ondervangen op het niveau van de wet zelf in plaats van de lagere regelgeving. Ik denk dat de heer Wolfsen daar meer over kan zeggen dan ik, maar ik denk dat het in ieder geval kan door de doelbinding strakker te reguleren op het niveau van de wet. Met name de risico's voor profilering lijken tot nu toe nauwelijks meegenomen in het wetstraject. Ik weet niet of dat in dit stadium nog zou kunnen, bijvoorbeeld middels een novelle. Dat zou misschien wel heel ver gaan, maar als dat de enige mogelijkheid is, moet dat maar. Anders valt er hier en daar wellicht nog wat te sleutelen door middel van moties. Dat laat ik graag aan u als Kamer.
Verder was er nog een vraag over inzicht in persoonsgegevens. Zeker bij dit wetsvoorstel dienen burgers zo veel mogelijk inzage te krijgen in de manier waarop hun persoonsgegevens worden verwerkt, niet alleen bij bepaalde overheden maar door de hele keten heen. Er zijn steeds meer vertakkingen. Ook bij dit wetsvoorstel is er sprake van koppeling van bestanden en daardoor meer risico's voor de privacy. Nogmaals, het standaardinzagerecht is hier heel belangrijk, evenals het correctierecht en het verwijderingsrecht als dingen niet kloppen. Als dingen niet blijken te kloppen, moeten ze in de hele keten worden gecorrigeerd.

De **voorzitter**: Ik ga nu even overschakelen naar de heer Wolfsen. Als er daarna nog vragen over zijn, kom ik weer bij u terug.

De heer **Wolfsen**: Dank u wel, meneer de voorzitter. De vragen van de heer Verkerk over verouderde informatie gingen met name over de standaarden. De overheid wil bewerkstelligen dat er vastere standaarden worden gebruikt. Dan gaat het bijvoorbeeld om https, de bekende

beveiligde sites. Daarvoor gelden bepaalde normen. Die zijn er ook voor het mailverkeer. Ons viel op dat er op die site nog verouderde normen staan. Zo'n site moet wel goed actueel worden gehouden.
Dan over de doelbinding. Wat is daar het gevaar van? Als u deze wet goedkeurt, maak je verwerking mogelijk voor een bepaald doel, heel expliciet. Het is goed om daar heel goed op te letten. De andere kant is vaak wel dat er in het algemeen wordt gezegd: het is zo fijn dat we één overheid zijn; waarom zou je dat niet allemaal koppelen? Dat gevaar is heel groot. Als er veel makkelijker informatie uitgewisseld kan worden, als er veel meer koppelingen kunnen worden gemaakt en als er veel meer koppelingsvlakken zijn, wordt er gezegd: maak dat dan maar mogelijk, want het is wel fijn dat je altijd overal alles van iedereen weet. Dat is toch fijn voor de burger, als de burger dat wil? Maar de burger heeft daarin geen keuze. U maakt die wetgeving. Het is vaak ook heel naar voor die burger, want dan weet iedereen alles over je. Let daarop, zou ik zeggen. Die doelbinding moet altijd goed en strak zijn geregeld. Daarom vinden wij het vaak niet goed als dingen in AMvB's worden geregeld. Dat maakt het wel heel flexibel, maar dan is de wetgever in volle omvang daar niet bij betrokken. Dat leidt vaak toch tot een zekere souplesse: maak dat maar mogelijk, want dat is toch zo handig. Daar waarschuwen we echt voor.
Dan het toezicht. Ik ga vandaag niet klagen over onze bezetting en formatie. Daar loopt nu een onderzoek naar. Maar ons werk wordt letterlijk per dag belangrijker en de groei loopt daar niet navenant in mee. Dat laat ik vandaag even rusten, maar er is wel een serieus gevaar dat het steeds maar verder gaat, als het toezicht niet is geregeld en als de wet te open is terwijl het met AMvB's allemaal te flexibel is. U kunt zich daar alles bij voorstellen.
De laatste vraag die u stelde ging over de onbekendheid. Iedereen wordt in Nederland geacht de wet te kennen; dat is een beetje de dooddoener. Dus in de wet is het dan goed geregeld. Maar dat is voor een normale burger niet meer mogelijk. De overheid weet veel meer van je en krijgt veel meer functies, maar het wordt feitelijk veel ondoorzichtiger. Er moeten verwerkingsregisters op sites staan, maar als het heel makkelijk kan worden doorgegeven, weet je als burger niet meer hoe het zit. Dan heb je het aan overheid A gegeven, maar weet overheid B het ook opeens. Dat is heel ondoorzichtig. Verwerkingsregisters moeten daarom goed op orde zijn en de wetgeving moet goed en strak en scherp zijn geregeld. In een wet zelf kun je dingen beter vinden dan in AMvB's.

De **voorzitter**: Dank u wel. Ik zie dat de heer Schalk van de SGP nog een vraag heeft.

De heer **Schalk** (SGP): Dank u wel, voorzitter. Eigenlijk is dit een vraag in vervolg op wat de heer Wolfsen zegt. We hebben hier net een wet voor de UBO-registratie aangenomen. De Raad van State heeft daarbij heel erg gewezen op het risico dat bestuurders van kerkgenootschappen risico's kunnen lopen op onwenselijk gedrag, intimidatie, pesterijen of zelfs chantage. Desondanks is de wet hier aangenomen. Wat doet de Autoriteit Persoonsgegevens met dat gegeven, wetende dat dit een risico is? Of moeten die bestuurders zich heel vroegtijdig gaan melden, of anderszins? Dat is mijn concrete vraag.

De **voorzitter**: De laatste vraag vanuit de Eerste Kamer is van de heer Ganzevoort van GroenLinks.

De heer **Ganzevoort** (GroenLinks): Dank. Mijn vraag sluit een beetje aan op de laatste opmerking van de heer Wolfsen over wat burgers weten et cetera. Op welke manier kunnen we hierin rekening houden met het verschil tussen bijvoorbeeld laaggeletterden en mensen die misschien

met meer gemak de complexiteit van de samenleving snappen? Is dat wettelijk te regelen of zijn daar anderszins ideeën over?

De heer **Wolfsen**: De eerste vraag is het gemakkelijkst, zou je kunnen zeggen, hoewel het een grote en ingewikkelde vraag is. Wij zijn toezichthouder. Als u wetgeving aanneemt die dit soort verwerkingen mogelijk maakt, houden wij er strak toezicht op dat er keurig in lijn met die wetgeving wordt gehandeld. Maar hoe meer daden er worden vastgelegd en hoe meer koppelingen er worden gemaakt, hoe groter het gevaar van lekken en beveiligingsincidenten. We hebben net het COA-incident gehad. Ik zal daar verder in het openbaar niks over zeggen, maar dan zie je wat een nare beveiligingsincidenten zich kunnen gaan voordoen. Dat is echt het gevaar van digitalisering. Ik kan u dus alleen maar waarschuwen dat u bij wetgeving altijd moet letten op doelbinding, beperktheid en goede beveiliging. Is zo'n register echt nodig, ja of nee? Dat is uw wegingstaak. Wij houden toezicht op de juiste naleving.
De vraag van de heer Ganzevoort sluit een beetje aan bij mijn eerdere opmerking. In Nederland zijn tussen de 1 en 2 miljoen mensen digibeet, dus hoe ingewikkelder de wetgeving wordt … Vaak wordt dan ook gezegd: laten we het maar makkelijk maken voor de mensen en alles met alles koppelen, zodat je niet tien keer je data aan al die overheden hoeft af te geven. Dat is ook waar, maar het gevaar is wel dat die mensen veel minder zicht hebben op de vraag wat er met hun data gebeurt. Dat heeft heel nare effecten. Mensen voelen zich heel onbehaaglijk, want ze worden op een gegeven moment wel met die data geconfronteerd door een heel andere instelling dan die waaraan ze hun data hebben afgegeven. Zeker als er een lek plaatsvindt, bijvoorbeeld van ggz-gegevens bij gemeenten of jeugdpsychiatrie, geeft dat mensen een heel onaangenaam, onrustig, onveilig bestaan: wie weet wat over mij? Er moet veel meer gebeuren aan voorlichting. Ik heb weleens gedacht aan een soort alternatieve bureaus voor rechtshulp, een alternatief Juridisch Loket. Je zou bijna digitale loketten moeten maken waar mensen kunnen binnenlopen, net als bij een Juridisch Loket, met de vraag om hun te helpen. Dat kun je als overheid faciliteren. Ik vind wel dat de overheid, als zij dit allemaal mogelijk maakt – daar sluit ik mee af, voorzitter – ook verplicht is om de burger te versterken. De overheid moet meer mogelijk maken om hier inzicht in te kunnen krijgen. Wij helpen daar als toezichthouder een beetje mee, maar dan kom ik weer op mensen en middelen: we kunnen dat natuurlijk niet allemaal bijlopen. Maar dit is echt een serieuze kwestie.

De **voorzitter**: We komen daar later in de ochtend nog over te spreken met de Stichting Lezen en Schrijven.
Meneer Böhre, wilt u nog reageren op vragen die aan u gesteld waren in de eerste ronde? Of wilt u nog iets vertellen?

De heer **Böhre**: Net werd kort het UBO-register genoemd. Dat valt een beetje buiten het onderwerp van deze sessie, maar het zou best kunnen dat daarover in de toekomst nog een rechtszaak komt, voornamelijk als prejudiciële vraag aan het Europees Hof of het UBO-register wel helemaal in lijn is met het Europees privacyrecht. Die rechtszaak gaat er komen, kan ik u alvast beloven, vanuit een brede coalitie.
Ik heb verder niks toe te voegen. Alles staat in onze position paper of heb ik net gezegd. Ik noem alleen nog even de term attributendienst; ik hoop dat u die al kende. Het gaat er vooral om dat je in je relatie met de overheid, in de communicatie of in het zakendoen met de overheid, alleen maar bepaalde kenmerken van jou als persoon of rechtspersoon of bedrijf hoeft te verstrekken, en niet al jouw identificerende gegevens. De hele wettekst is tot nu toe erg gebaseerd op authenticatie en identificatie. Dat is vaak helemaal niet nodig. Dat is soms helemaal niet nodig. Dan heb je dus een alternatief nodig, een zogeheten attributendienst, waarbij je als

persoon alleen maar bepaalde kenmerken van jezelf kenbaar maakt, op betrouwbare wijze, en meer niet. Dat past perfect in het simpele rijtje van noodzaak, proportionaliteit en subsidiariteit. De wet zoals die er nu ligt, schiet dus te ver door naar dingen die niet per se noodzakelijk zijn. Mensen gaan te veel data over zichzelf verspreiden via allerlei nieuwe eID-dienstverleners, waarvan we in de toekomst alleen maar kunnen hopen dat ze goed en betrouwbaar functioneren. Deze wet neemt op dit moment dus een flinke hypotheek op de toekomst.

De **voorzitter**: Dank u wel. Ik wil u beiden hartelijk danken voor uw bijdrage. Als u achter de tafel vandaan gaat, wordt die eerst schoongemaakt. Daarna beginnen we met het tweede onderdeel van deze hoorzitting. Ik heb nog niet gemeld dat er een verslag wordt gemaakt van alles wat er gezegd wordt vandaag. Dat betekent dat we alles wat u verteld hebt, nog eens rustig kunnen nalezen. U kunt dat zelf overigens ook doen. Mocht u nog dingen aan de Eerste Kamer willen meedelen, dan weet u ons wel te vinden. Hartelijk dank!
Ik vraag nu of de tafel even ontsmet kan worden. Uiteraard kunt u hier in de zaal blijven zitten als u dat interessant vindt en tijd genoeg hebt.

Thema 2: De WDO als kaderwet en betrokkenheid van het parlement

De **voorzitter**: In het tweede deel gaan we praten over de Wet digitale overheid als kaderwet en hoe het parlement in dat kader het beste betrokken kan worden bij de regelgeving. Dat was ook een onderwerp dat vanuit de commissie was aangedragen om daarop in te zoomen. We gaan spreken met de heer Pieter van Boheemen, die als onderzoeker is verbonden aan het Rathenau Instituut, en met de heer Peter van Lochem, die oud-rector en oud-directeur is van de Academie voor Wetgeving en van de Academie voor Overheidsjuristen. Ik verzoek hen om als de tafel ontsmet is, achter de tafel te gaan zitten. Ik zie dat ik mijzelf heb vergeten te introduceren. Mijn naam is Dittrich en ik ben voorzitter van de commissie Binnenlandse Zaken en ik ben van D66. Ik wil beginnen met de heer Van Boheemen van het Rathenau Instituut. Ook van u hebben we een position paper ontvangen, maar u hebt maximaal vijf minuten om uw visie op de wet nog eens toe te lichten.

De heer **Van Boheemen**: Geachte voorzitter en leden van de Eerste Kamer, nogmaals dank dat ik hier een bijdrage mag komen leveren. Ik heb een aantal slides voorbereid die afgedrukt op uw bureau liggen. Ik wil beginnen met het onderstrepen van het belang van een goede wet op de digitale overheid. Je zou kunnen zeggen dat hoe meer mensen digitaal zakendoen met de overheid, hoe belangrijker het wordt dat dat ook op een betrouwbare manier gebeurt. Er zijn net al een aantal voorbeelden genoemd van wat er mis kan gaan als gegevens uitlekken, als gegevens worden misbruikt of als gegevens onjuist zijn. Het is dus erg belangrijk dat dit op een goede manier wordt georganiseerd.
In januari van dit jaar heb ik samen met mijn collega Linda Kool een opiniestuk over dit wetsvoorstel geschreven, dat in Trouw is verschenen. In deze inleiding wil ik daar twee punten uitlichten en ook nog twee punten eraan toevoegen. Die staan op de tweede slide van mijn presentatie. Het eerste is democratische grip op de digitalisering. Dat past goed bij dit thema. Het tweede is het verdienmodel van private aanbieders, wat eigenlijk een voorbeeld is van de grip die je zou willen hebben. Het derde is het belang van de burger en het vierde zijn de politieke keuzes die nu naar de achtergrond lijken te verdwijnen in de verdere technische uitwerking van de wet.
Ik zal beginnen met de democratische grip op digitalisering. Ons viel in het wetsvoorstel op dat er een groot aantal algemene maatregelen van

bestuur in staat vermeld over bijvoorbeeld heel belangrijke onderwerpen als de informatieveiligheid, het beheer van de infrastructuur, de toelating en erkenning van de aanbieders, de rechten en plichten die zij hebben, het beschermen van persoonsgegevens – dat is al besproken – en het doorberekenen van kosten. Er is na de publicatie van onze opinie wel een artikel over de betrokkenheid van het parlement toegevoegd, artikel 25, maar daaruit blijkt dat er een grote alertheid wordt verwacht van het parlement, van de Kamers. Wij vragen ons af of het niet beter is om al in de wet zelf bescherming van persoonsgegevens en daarmee privacy goed vast te leggen. Dit artikel vereist grote oplettendheid en voortdurende betrokkenheid van het parlement.
De vierde slide gaat over het verdienmodel van private aanbieders. Dat is een ander punt dat we aanstipten in onze opinie. We vroegen ons al vrij snel af wat het verdienmodel wordt van de private partijen die in dit voorstel zijn voorzien. In de privacyvisie die door de Staatssecretaris is gepubliceerd, staat dat het enorm belangrijk is dat de belangen van commerciële partijen strikt gescheiden worden gehouden van de dienst die ze gaan aanbieden in het kader van deze wet. In het wetsvoorstel zelf zie je dat eigenlijk niet, maar wel in een conceptbesluit identificatiemiddelen voor burgers, dat is gepubliceerd als onderdeel van de internetconsultatie. Daar staat in artikel 2.19 dat er een bepaalde doelbinding is, dus dat de gegevens niet mogen worden gebruikt voor andere doelen dan de authenticatiedienstverlening. Op zich is dat een positieve ontwikkeling, zouden wij zeggen.
In de nota van toelichting staat dat de verkoop van gegevens niet is toegestaan. Nu zijn er natuurlijk allerlei andere manieren om geld te verdienen met gegevens dan puur en alleen het verkopen van gegevens. Net werd al het profileren van mensen genoemd en het aanbieden van advertenties op basis van die profielen. Of denk aan kredietwaardigheidsscores en al dat soort zaken. In de nota van toelichting staat ook dat de gegevens niet voor andere doelen mogen worden gebruikt, maar wij vragen ons af of het überhaupt mogelijk is om daarop toezicht te houden. Waarschijnlijk grote techbedrijven gaan een dienst aanbieden. Gaat een toezichthouder dan echt in hun systemen kijken hoe zij de profielen opstellen en of deze gegevens al dan niet gebruikt zijn? Is dat realistisch, vragen wij ons af, ook gezien de reputatie van deze partijen op dit gebied. Als de middelen niet open source zijn, dus als je niet in de bron kunt kijken, hoe kun je dit dan controleren als gebruiker van zo'n dienst?
Een ander punt is het belang van burgers. Is dat wel voldoende geadresseerd in de wet, vragen wij ons af. Hoe worden zij bediend? Wie gaat hen helpen bij het gebruiken van de identificatiemiddelen? Welke behoefte van hen staat echt centraal? Er staat wel dat er rekening wordt gehouden met toegankelijkheid, maar is dat vanzelfsprekend? Moet dat niet worden geregeld in de wet? We vragen ons ook af hoe burgers straks moeten kiezen tussen al die verschillende aanbieders. We weten dat de keuzes vaak beïnvloed worden door netwerkeffecten. Je kiest wat andere mensen om je heen ook hebben gekozen of het middel dat het meest gebruikt wordt of dat past bij het merk dat je toch al gebruikt. Wat voor criteria worden er straks gehanteerd? Dat wordt nu niet duidelijk uit de wet.
Een laatste punt: er zijn allerlei politieke keuzes die van invloed zijn op privacy, op autonomie, op controle en op zeggenschap. Nu worden die overgelaten aan de AMvB's of de verdere technische uitwerking. Neem de keuze tussen een decentrale of een centrale architectuur of een hybride vorm. Je zou kunnen zeggen dat een decentrale architectuur privacyvriendelijker is, maar een centrale structuur is misschien toezichtvriendelijker, alhoewel je bij een decentrale architectuur minder toezicht nodig hebt. Zo zijn er nog heel veel keuzes. Ik kan er nog een aantal noemen, bijvoorbeeld de keuze tussen volledige identificatie of het gebruik van attributen of zelfs van pseudoniemen. Wat ons betreft is de AVG de bodemlaag waar je als overheid aan zou moeten voldoen. Er zijn veel meer mogelijkheden

om de privacy te beschermen. Het zou mooi zijn als dat al in de wet was geregeld.

De **voorzitter**: Dank u wel. Dan is nu het woord aan de heer Van Lochem, oud-rector en oud-directeur van de Academie voor Wetgeving.

De heer **Van Lochem**: Dank, voorzitter, dank, leden, ook voor de uitnodiging. We hebben het hier niet over de kaderwet digitale overheid maar het is wel een kaderwet in de zin dat er veel gedelegeerd wordt. Door vorige sprekers is al in het bijzonder aangegeven wat er zoal in behoorlijke mate gedelegeerd wordt. In het algemeen wordt veel gewaarschuwd tegen veel delegatie en kaderwet, meestal in termen van het primaat van de wetgever. Dan gaat het vooral om het primaat van het parlement, dat in het geding zou kunnen zijn. Daar worden zowel in literatuur als elders nogal forse termen bij gebruikt om te waarschuwen: let op dat het parlement een niet te geringe rol krijgt. Ook de vicepresident van de Raad van State, de huidige en de vorige, heeft trouwens bij herhaling in zijn algemene beschouwing gewezen op deze tendens, die wat ruimer is dan alleen de kaderwetgeving maar die wel in de gaten zou moeten worden gehouden.
In die lijn, in die zekere bezorgdheid, zou je kunnen zeggen, over de positie van de wetgever, zie je dat de spelregels voor de kwaliteit van wetgeving, de Aanwijzingen voor de regelgeving waar u zelf als Kamer naar verwijst in uw aandachtspunten, erg gericht zijn op die ongerustheid en daarmee eigenlijk oproepen tot een behoorlijk grote terughoudendheid. Er worden eisen gesteld als «de hoofdzaken moeten toch wel in de wet» en «elke delegatie moet toch wel heel nauwkeurig begrensd zijn». Ook de Raad van State heeft er nog eisen en criteria aan toegevoegd. Wat gedelegeerd wordt moet kwantitatief niet te groot zijn in verhouding tot de wet. Het moet ook niet te abstract zijn, het moet zo helder zijn dat je precies weet wat er gedelegeerd wordt. Als je die criteria naast deze wet legt, dan is duidelijk dat er aanmerkelijk minder terughoudend gedelegeerd wordt dan de Aanwijzingen voor de regelgeving en andere voorschrijven. Vaak is er wel een toelichting, in de zin van «let op, het is maar een technische uitwerking». Daar zijn de voorgaande sprekers het minder mee eens, heeft u al gemerkt. Soms wordt er ook op gewezen: let op, het is hier nodig om te delegeren, want het is nu eenmaal een ontwikkeling die nu nog niet zo scherp is en die in de loop van de tijd scherper moet worden, en bovendien is het een vrij veranderlijke ontwikkeling, zodat er steeds aanvullende regelgeving nodig is. Daarmee zou je formele wetgeving te veel belasten, is dan vaak de overweging. Wordt aan de eisen voldaan? Niet ten volle. De Raad van State stelt voor om meer in de wet op te nemen omdat het anders te abstract wordt en ook te techniekonafhankelijke taal, zoals de raad zegt. De raad wil zelfs een aantal centrale onderdelen van de GDI erin. Van de Autoriteit Persoonsgegevens heeft u al gehoord hoe zij aankijkt tegen delegeren, ook op grond van de afweging van de proportionaliteit waar het hier om gaat. Weliswaar is daar in de wettekst enigszins rekening mee gehouden door in artikel 16 doelen te noemen aan de hand waarvan je later de proportionaliteitsafweging kunt maken. Er is ook wel enige argumentatie gegeven over de delegatie waar de Autoriteit Persoonsgegevens om vroeg. Die motivering in de memorie van toelichting is trouwens niet helemaal geslaagd. Ik geloof op bladzijde 24 van de memorie van toelichting staat als reden voor het regelen van de verwerking van persoonsgegevens bij AMvB het feit dat het voorstel het karakter heeft van een kaderwet. Dat is toch een toelichting die, samengevat, er een is van «het is een kaderwet omdat het een kaderwet is». En dat is zo.
Maar de kern is deze. Aan de ene kant staat de wet in het teken van innovatie en ontwikkeling en wordt er vaak de term «toekomstgerichte wetgeving» op geplakt. Overigens heeft het kabinet al een enkele keer

gezegd dat dat de lijn is die het meer zal volgen. Aan de andere kant gaan de regels nog uit van de klassieke terughoudendheid, zou je bijna zeggen. Daar zit natuurlijk enige spanning. Als je mij concreet zou vragen of de wet precies voldoet aan de regels, dan zou ik zeggen: nou, die regels zijn eigenlijk gericht op andere typen wetgeving. Vandaar dat ik mijn paper ook heb afgesloten met een overweging. Als Kamer zou je je moeten afvragen: wat doen wij met wetgeving die zo sterk delegeert? We kunnen natuurlijk zeggen «laten we er maar vertrouwen in hebben» en we kunnen het ook sterk zoeken in een goede voorbereiding, een ICT-scan en noem maar op. Dat kan. Je kunt ook zeggen: deze ontwikkeling gaat ons toch te ver, wij willen de ontwikkeling liever volgen, op de rem trappen of eigenlijk iedere stap meemaken. Ik heb de alternatieven genoemd. Dat hangt natuurlijk af van wat het oordeel van uw Kamer is over de mate van delegatie.

De **voorzitter**: Dank u wel, meneer Van Lochem. Ik kijk naar de leden. Wie wil een vraag stellen aan een van de sprekers of beiden?

De heer **Koole** (PvdA): Dank u wel voor de inleidingen. Ik heb een vraag aan de heer Van Boheemen. Ik begrijp uit zijn verhaal dat toezicht erg moeilijk wordt zodra de gegevens ook in handen komen van de grote techbedrijven. Zegt hij nu: we moeten eigenlijk die hele kant niet opgaan? Of zegt hij: de wet regelt dat lang niet precies genoeg? Of zegt hij: dat kun je oplossen door vooral te hameren op open source, en dat zou beter in de wet geregeld moeten worden? Ik was toch een beetje geschrokken van zijn constatering dat het toezicht bijna onmogelijk als je het uit handen geeft aan andere instellingen dan de overheid zelf.
De vraag aan de heer Van Lochem sluit aan bij zijn laatste opmerking. Hij is deskundige op het gebied van wetgeving. Valt deze wet nog te verbeteren in de richting van de regelgeving die over wetgeving gaat? U zegt als het gaat om wat te doen: enerzijds vertrouwen. Of u zegt: het gaat te ver. Maar wat bedoelt u met die laatste opmerking? Dat betekent toch gewoon dat u deze Kamer dan zou adviseren om de wet terug te sturen en ervoor te zorgen dat er veel meer bepalingen in de formele wet zelf komen te staan?

De **voorzitter**: Dank u wel. De heer Verkerk van de ChristenUnie.

De heer **Verkerk** (ChristenUnie): De heer Van Boheemen sprak over maatregelen tegen profiling voor aanbieders van eID-middelen. Mijn vraag is of hij dat kan toelichten. Ten aanzien van de heer Van Lochem heb ik een aanvullende vraag op die van de heer Koole.
Welke dingen zouden volgens de heer Van Lochem echt in de wet moeten worden opgenomen? Dank u wel.

De **voorzitter**: De heer Van Hattem van de PVV.

De heer **Van Hattem** (PVV): De heer Van Boheemen spreekt in zijn position paper en zojuist ook in zijn betoog over de democratische grip via de AMvB's. Hij spreekt daarbij onder andere over de doorberekening van kosten. Ik denk dat het ook te maken heeft met de kosten die worden doorberekend voor het inlogmiddel. Kan de heer Van Boheemen misschien toelichten in hoeverre het Rathenau Instituut van mening is dat zoiets inderdaad in een wet moet worden geregeld? Moet er niet meer een principiële afweging worden gemaakt of een overheid kosten moet vragen om over zulk soort middelen te kunnen beschikken? Is daar ook een visie op?

De **voorzitter**: En tot slot in deze eerste ronde mevrouw Gerkens van de SP.

Mevrouw **Gerkens** (SP): Ik wil aansluiten bij de laatste vraag van de heer Koole aan de heer Van Lochem. En voor de heer Van Boheemen heb ik de volgende vraag. Ik vraag me af of hij die wel kan of wil beantwoorden, omdat die ook nogal filosofisch is. Er is een reden waarom wij het mogelijk maken dat commerciële partijen dit soort middelen kunnen aanbieden. Dat heeft ook te maken met de gedachte dat de overheid niet altijd even gelukkig is in het uitvoeren van dit soort ICT-projecten. Tegelijkertijd ziet hij ook een risico om vele aanbieders dit te laten doen. Is het nou eigenlijk wel een voordeel dat we hier een vorm van marktwerking op introduceren? Of zegt hij: het zou veel veiliger en beter zijn om gewoon één aanbieder te hebben van een elektronische identificatiedienst?

De **voorzitter**: De allerlaatste vraag gaat naar de heer Van Pareren van Forum voor Democratie.

De heer **Van Pareren** (FvD): Dank u, voorzitter. Ik heb hopelijk goed begrepen dat de heer Van Lochem zegt dat delegeren wel erg veel op vertrouwen gaat. Verwacht hij dat als deze wet zo wordt aangenomen, er dan veel rechtszaken kunnen komen die zaken ter discussie stellen die dus niet voldoende zijn afgedekt door deze wet?

De **voorzitter**: Wie van de heren wil als eerste beginnen met de beantwoording? Dat is de heer Van Boheemen.

De heer **Van Boheemen**: Dank u wel. Ik zal beginnen met de eerste vraag van de heer Koole van de PvdA. Hij vraagt of toezicht op algoritmes die techbedrijven gaan gebruiken, überhaupt wel mogelijk is, of het überhaupt wel wenselijk is dat zij dit soort diensten gaan aanbieden en of open source een oplossing kan zijn. Ik zou zeggen: inderdaad, als de broncode inzichtelijk is, is dat een enorme stap voorwaarts, want dan kun je als onafhankelijke partij maar ook als toezichthouder zien hoe het systeem is gebouwd. Dan gaat het dus niet alleen om de privacy maar ook om de veiligheid en om andere aspecten. Die kunnen worden getoetst. En of het überhaupt mogelijk is, dat is een beetje een kwestie van vertrouwen. De partijen waar je snel aan zult denken – de Googles en de Facebooks van deze wereld – hebben qua reputatie wel iets goed te maken, want de manier waarop ze omgaan met persoonsgegevens is niet altijd volgens de normen die we hebben. Als je zegt «we staan het wel toe en we nodigen ze uit om een dienst te ontwikkelen», dan ga je dus bewust dat risico aan.
Dan de vraag van de heer Verkerk. Hij vroeg om een toelichting op profilering. Ik neem aan dat hij wil weten wat voor soort profilering er mogelijk is en wat ik me daarbij moet voorstellen.

De heer **Verkerk** (ChristenUnie): Meer eigenlijk: welke maatregelen zijn nodig om dat te voorkomen?

De heer **Van Boheemen**: Dat gaat wederom over de doelbinding. In de doelbinding staat wel dat het niet is toegestaan, maar ik zou wederom willen zeggen dat ook die opensourceaanpak daar een mogelijke oplossing voor is. Dan kun je echt controleren of het daadwerkelijk gebeurt. Nu is het eigenlijk een kwestie van vertrouwen dat die partijen dat niet doen. Dat zou dus een maatregel kunnen zijn. Verder is het natuurlijk goed als echt in de wet staat dat het niet is toegestaan om dat te doen, en niet alleen in een AMvB.
De heer Van Hattem vraagt om de democratische grip, om de doorberekening van de kosten. Ik ken die discussie inderdaad. Er is ook een discussie over de vraag of je zou moeten betalen voor een paspoort of niet. Dat is in feite wel zo, terwijl het voor veel mensen toch best een

bedrag kan zijn. Zij moeten eens in de vier jaar € 80 of iets dergelijks betalen om een middel dat zij nodig hebben, te kunnen gebruiken. Het is volgens mij inderdaad een principiële afweging of je dat als overheid van burgers verwacht of niet. Je kunnen zeggen: dit is zo essentieel, dit moet gewoon kosteloos worden aangeboden. Maar aangezien we ten aanzien van paspoorten en andere identificatiemiddelen ook besloten hebben dat daar kosten voor kunnen worden gerekend, zou je kunnen zeggen: dat is hier dan ook wel redelijk. Maar in andere landen staat het wel in de wet. Volgens mij staat in Finland in de wet een vast bedrag gedefinieerd. In dit wetsvoorstel is dat niet aan de orde.
Dan mevrouw Gerkens met haar vraag over de commerciële partijen. Is dat nou een voordeel of zou één dienstverlener beter zijn? Daarbij wordt echt uitgegaan van de weerbaarheid. Je denkt dat als je meerdere partijen hebt, het weerbaarder is. Want als een partij uitvalt, dan kunnen mensen van een andere partij gebruikmaken. Ik weet het niet. Het is een filosofische vraag, en ik denk dat het deels wensdenken is. Bij heel veel digitale dienstverleners zijn er vaak uiteindelijk een of twee die het grootste deel van de markt bedienen. Dat zou je, denk ik, hier ook kunnen verwachten. Waarschijnlijk worden het dan een, twee of drie partijen, net zoals je er bij telefoonmaatschappijen twee of drie hebt. Dat is dan natuurlijk ook weer een voordeel wat betreft het toezicht. Maar het volledig uitsluiten van commerciële partijen lijkt mij niet redelijk. Je kunt van ze verwachten dat als je alle normen goed stelt en het toezicht goed hebt geregeld, ze gewoon voldoen aan de wensen.

De **voorzitter**: Ik ga nu even over naar de heer Van Lochem voor de beantwoording van enkele vragen.

De heer **Van Lochem**: Dank, voorzitter. De vragen waren overwegend: gelet op het feit dat nu veel gedelegeerd wordt, wat zou er dan alsnog in de wet kunnen? En vind je dat ook aangewezen? Wanneer je op grond van met name de regels, de aanwijzingen en de kanttekeningen die mensen erbij maken, vindt dat er te veel gedelegeerd wordt, zijn er natuurlijk zaken aan te wijzen die je dan in de wetgeving kunt brengen. In feite is het zo dat in het advies van de Raad van State wordt gezegd: breng meer van die GDI-onderdelen in de wet. De Autoriteit Persoonsgegevens beveelt aan: breng toch in ieder geval op hoofdlijnen de afweging in de wet in termen van proportionaliteit.
Als u het mij vraagt, zou ik denken: er komt, als ik de aankondiging goed zie, meer van dit type wetgeving aan. Dat heeft de regering eigenlijk wel geconcludeerd. Die vindt dat een goede manier bij wetgeving die vooral op het terrein ligt van technologie, innovatie en dergelijke. Mijn indruk is dat de argumenten om daarin behoorlijk wat te delegeren, voor minstens een flink deel wel valide zijn. Het gaat vaak om iets wat ontwikkeld moet worden in de toekomst, waar we nu niet concreet over zijn. Het gaat vaak om zaken die nogal veranderlijk zijn. Dus als u mijn opvatting zou vragen, dan zit ik zelf meer op de lijn van «dit is voor een deel op die terreinen nieuwe wetgeving».
Als ik de Kamer was, zou ik er dan misschien minder op aandringen om toch nog zo veel mogelijk in die wet onder te brengen. Ik zou kijken of er geen mogelijkheden zijn om met de uitvoerende wetgeving toch wat meer dan normaal mee te kijken, om het zo maar te zeggen. Heel extreem zou zijn dat je zegt: wij vinden dat wij als Kamer bij elke gedelegeerde wetgeving de voorwaardelijke voorhang moeten toepassen. Dan willen we het hier namelijk hebben en dan willen wij ons er per gedelegeerde wetgeving over uitspreken of we het in de wet willen opnemen. Dat lijkt me nogal uitvoerig. Dat lijkt me de meest uitvoerige kant. Dan zou je de uitvoering wel erg belasten en niet in de laatste plaats uw Kamer ook. Maar ik kan me wel voorstellen dat u zegt: we willen wel een vinger aan de pols houden; we willen ten minste een jaarlijkse rapportage van de

Minister over de stand van zaken bij de ontwikkeling van gedelegeerde wetgeving, zodat we ook kunnen oordelen of het niet tijd is om een tweede tranche van de wetgeving te maken. Dat zou kunnen.
Op zichzelf is het denkbaar dat voor sommige onderdelen je er wel voor kiest dat mogelijk andere instanties de gedelegeerde wetgeving volgen. De Autoriteit Persoonsgegevens heeft bijvoorbeeld al gevraagd om aan haar alle gedelegeerde wetgeving voor te leggen, om te kijken vanuit deze belangrijke invalshoek. Dus in die zin kunt u het volgen en de vinger aan de pols houden en voor een deel ook wel delegeren. Maar ik zou zelf zeggen: op het terrein van technologie, innovatie en ontwikkeling past, om het zo te zeggen, naar mijn gevoel de aanwijzing regelgeving en dergelijke in termen van terughoudendheid toch echt minder.

De **voorzitter**: Dank u wel. Ik kijk even naar de leden of zij nog een vraag hebben. Ik zie de heer Van Pareren.

De heer **Van Pareren** (FvD): Mijn vraag is nog niet beantwoord.

De heer **Van Lochem**: Excuus. Uw vraag was: voorziet u veel rechtszaken? Dat is op zichzelf altijd wel een heel moeilijke voorspelling. Je kunt wel constateren dat er in de delegatie nog veel principiële punten aan de orde komen. Daarvan is denkbaar, zeker omdat het gedelegeerde wetgeving is en de rechter in relatie tot de Grondwet wel kan toetsen en die wetgeving de maat kan nemen, dat zeker instanties die op dit punt op het vinkentouw zitten, voor wel wat procedures zouden kunnen zorgen. Ik ben niet in staat om te voorspellen of het er veel zullen zijn.

De **voorzitter**: Ik kijk nog even naar de heer Van Boheemen. Misschien wil hij nog een vraag beantwoorden? Of hebt u alles kunnen vertellen wat u wilde vertellen aan ons?

De heer **Van Boheemen**: Er schoot mij nog één ding te binnen naar aanleiding van de vraag over maatregelen tegen profilering. Ik noemde open source, maar ik dacht daarna: een decentraal systeem, dus een systeem waarbij gegevens überhaupt niet in een centrale database worden opgeslagen maar bij de gebruikers op de telefoon staan, zou het hele probleem in één keer oplossen. Dus een andere architectuur zou het kunnen oplossen. Het is dus in die zin jammer dat in het wetsvoorstel geen keuze wordt gemaakt. Het lijkt nu te gaan om een centraal systeem. Alles wijst daarop. Maar omdat dat soort keuzes niet zijn gemaakt, is het ook lastig om het daar nu over te hebben.

De **voorzitter**: Goed. Dan wil ik u beiden hartelijk bedanken voor alle informatie die u ons gegeven hebt. We zullen daar ons voordeel mee kunnen doen. Hartelijk dank.
We gaan na het ontsmetten van de tafel door met het derde blok van deze deskundigenbijeenkomst van de vaste Kamercommissie voor Binnenlandse Zaken. Als u wilt en als u daar tijd voor hebt, kunt achter in de zaal blijven zitten om te luisteren naar de volgende sprekers.

Thema 3: Toegankelijkheid van de publieke dienstverlening (inclusief aspecten als betaling en algoritmen)

De **voorzitter**: We zijn aangekomen bij het derde thema dat we als Kamercommissie van Binnenlandse Zaken van tevoren hadden bedacht: de toegankelijkheid van de publieke dienstverlening. Daarin zitten aspecten als betaling, algoritmen en al het andere wat de deskundigen voor ons naar voren willen brengen. We hebben hiervoor twee instanties uitgenodigd, allereerst de Nationale ombudsman, de heer Reinier van Zutphen, en daarnaast de Stichting Lezen en Schrijven. Zijn zij ook al

aanwezig? Ja, dat is het geval. Dan verzoek ik hun om achter de inmiddels schoongemaakte tafel plaats te nemen. Van de Stichting Lezen en Schrijven hebben we Geke van Velzen en … Ik zie twee mensen. Misschien kunt u zichzelf straks nog even voorstellen.
Ik wil graag eerst het woord geven aan de Nationale ombudsman sinds 2015, de heer Van Zutphen. Gaat uw gang. U heeft maximaal vijf minuten. Daarna volgt de Stichting Lezen en Schrijven en daarna komen de vragen van de commissieleden.

De heer **Van Zutphen**: Dank u wel, voorzitter. Dank u wel voor de kans om hier in uw Kamer iets te zeggen over het burgerperspectief op deze digitalisering. Het woord «burger» ben ik in de wet eigenlijk niet heel erg tegengekomen en het woord «burgerperspectief» in de toelichting ook niet echt, dus ik ben blij dat u dit onderwerp hier al op dit moment hebt geagendeerd. Als je naar de wet zelf kijkt, denk je: dat komt allemaal later wel een keer. Maar ik denk dat het heel belangrijk is om nu al vooruit te kijken naar wat er straks allemaal gaat gebeuren als die kaderwet leidt tot allerlei besluiten en aanwijzingen die de burger en de manier waarop hij met de overheid communiceert, wel echt gaan raken.
Ik probeer me te beperken tot een aantal zaken. In onze position paper hebben we al wat gezegd. Het gaat om een paar essentiële dingen. Als de overheid digitaliseert, doet de overheid dat niet voor zichzelf, maar voor het goede verkeer tussen overheid en burger. De burger mag nooit vergeten worden. Ons jaarverslag over 2018 heette niet voor niks Iedereen moet mee kunnen doen. Dat geldt ook voor de digitale wereld. Wij weten dat er in Nederland heel veel mensen zijn die moeite hebben om met de overheid te communiceren – ik weet zeker dat de collega's aan tafel daar straks nog iets over gaan zeggen – zowel op papier als aan de telefoon en zelfs aan het loket, maar zeker ook digitaal. Als je weet hoeveel mensen moeite hebben met lezen en schrijven en rekenen, zijn we toch in de buurt van 2 à 2,5 miljoen. Uit onderzoek naar hoe scholieren het Nederlands beheersen, weten we dat bijna een op de vier moeite heeft met begrip van de Nederlandse taal. Voor digitalisering is taal toch echt onontbeerlijk.
We hebben in het verleden een aantal dingen geschreven over wat er gebeurt als er wordt gedigitaliseerd. U weet vast nog wel dat de blauwe envelop ging verdwijnen. U hebt vast de reclame nog in uw hoofd die daarvoor gemaakt werd, met dat vogeltje dat met die blauwe envelop wegzweefde. U weet ook dat dit een soort fade-out was bij de Belastingdienst. Dat gingen ze niet meer laten zien. Uiteindelijk is het ook in de overheid zover dat we zeggen: iedereen moet kunnen meedoen, ook niet-digitaal. Eind vorig jaar hebben we een grote inventarisatie gedaan onder 1.500 mensen die in Nederland wonen en gevraagd: hoe kijk je tegen die overheid aan? Iedereen weet dat de digitale overheid een hele belangrijke zal zijn, maar iedereen zegt tegelijkertijd: we willen wel op een of andere manier echt in contact kunnen blijven, anders dan digitaal, met de overheid. Het moet een begrijpelijke en deskundige overheid zijn. Als burgers een vraag hebben over wat de overheid hun digitaal aanlevert, willen ze ook een echt antwoord krijgen.
Dat geldt voor wat hier op basis van deze wet gaat gebeuren ook. De aanbevelingen die wij hebben opgeschreven voor hoe de overheid met de burger zou moeten digitaliseren, vindt u al in een eerder rapport, De burger gaat digitaal. Het verdwijnen van de blauwe envelop noemde ik net al, maar ik wijs ook op het rapport «Hoezo MIJNoverheid?», over de Berichtenbox. Het gekke wat je ziet, is dat we vroeger gewoon een briefwisseling met de overheid konden hebben, terwijl we in de Berichtenbox geen verkeer meer kunnen hebben, alleen maar eenzijdig verkeer, van de overheid naar de burger. De burger moet wel weer op een andere manier, namelijk op schrift of via de telefoon, reageren richting die overheid over wat hij in de Berichtenbox ziet. Met andere woorden, als hij daar een besluit vindt waartegen hij bezwaar wil maken, kan dat niet

digitaal. Dat bezwaar moet uiteindelijk toch weer op papier. Dat is een rare constatering, omdat je denkt dat we met digitalisering een stap voorwaarts maken, terwijl we eigenlijk een stap achterwaarts doen.
Er is nog een ander onderwerp dat ik graag nog onder uw aandacht zou brengen. Er zijn heel veel mensen in het buitenland die op de Nederlandse overheid zijn aangewezen. Buitenlandse Zaken zegt: we hebben een stad van 1 miljoen, alle mensen in het buitenland. Daarnaast hebben we nog heel veel mensen op de BES-eilanden wonen. Bedenkt u zich dat bijvoorbeeld de mensen op Bonaire vaak geen bsn-nummer hebben, maar wel met de Rijksdienst Caribisch Nederland moeten verkeren en zich moeten laten verstaan. Ze komen soms naar Nederland en kunnen dan niet in de systemen. Ik ben nu bezig met een onderzoek naar studenten en DUO. Heel veel studenten in het buitenland moeten ook met de overheid communiceren. Daar doen zich ook allerlei problemen met het gebruik van gegevens, zoals het bsn.
Een ander punt dat ik onder uw aandacht wil brengen, is dat de overheid niet erg voortvarend is. Meneer Wolfsen zei al: we hebben in 2017 al ons advies gegeven. Wij vragen de overheid al sinds 2015 om de machtigingsfunctie goed te organiseren. Dat is nog steeds niet gebeurd. Er zit dus ook echt een enorme vertraging in de uitvoering en de mogelijkheden die er zijn. Ik zou u dus willen vragen om vooral te kijken wat er straks met deze wet gaat gebeuren in de concrete uitvoering, want daar is het burgerperspectief wel heel erg op de achtergrond geraakt. Ik ben het van harte eens met een aantal sprekers hiervoor die zeiden dat er democratische controle zou moeten zijn op wat er vervolgens met de besluiten en de aanwijzingen gebeurt.
Ten slotte nog één opmerking over het feit dat het hier voor een heel groot deel gaat om een publiek-private onderneming. Daarbij doet zich de vraag voor hoe het zit met de rechtsbescherming. Dat kwam net al even aan de orde. Komen er veel rechtszaken? Daar is moeilijk iets over te zeggen. Ik heb ook zorgen over het volgende, wat ik moeilijk kan kwantificeren: wat betekent het nou als private dienstverleners straks iets gaan doen voor burgers om een koppeling te maken naar de overheid, voor zaken die de overheid voor de burger moet regelen? Bij wie gaat u dan klagen, als u de burger bent die ermee geconfronteerd wordt? Op het terrein van het klachtrecht, het geven van signalen en het uiten van onvrede moet nog wat verder doordacht worden bij wie de burger terechtkan als het misgaat tussen hem en die privaat-publieke onderneming, of de publieke onderneming.
De Raad van Europa heeft een belangrijk document geproduceerd, de Venice Principles. Die gaan over Ombudsmanorganisaties, dus ik zou haast zeggen dat dat een beetje praten voor mijn eigen bestaan is. Maar die Venice Principes zeggen eigenlijk dat er op «all general interest and public services provided to the public» een fatsoenlijke klachtbehandeling mogelijk zou moeten zijn. Die moet echt wel geregeld gaan worden. Daarvoor vind ik in deze wet weinig aanknopingspunten.
Dank u wel.

De **voorzitter**: Dank u wel. Wij hebben twee vertegenwoordigers van de Stichting Lezen en Schrijven, Lisanne Bos en Geke van Velzen. Ik laat het aan u over wie het woord wil voeren. Gaat uw gang.

Mevrouw **Bos**: Allereerst dank dat wij namens Stichting Lezen en Schrijven naar deze deskundigenbijeenkomst mogen komen om voor een kwetsbare doelgroep, namelijk de laaggeletterden, een reactie te geven op de toegankelijkheid van de publieke dienstverlening.
Zoals meerdere sprekers net al verteld hebben, is het voor de doelgroep laaggeletterden ingewikkeld als dit soort veranderingen plaatsvinden. In Nederland zijn 2,5 miljoen mensen laaggeletterd. Dat betekent dat zij moeite hebben met taal en/of rekenen. Zij hebben drie keer zo vaak

minder digitale vaardigheden. Met de veranderingen die in dit wetsvoorstel worden voorgesteld, kunnen zij aanlopen tegen drempels om de digitale overheid te bereiken. In onze position paper noemen wij daarom verschillende drempels en verschillende middelen om de wet toch toegankelijker te maken. In onze presentatie willen wij dan ook vooral ingaan op de uitvoering van dit wetsvoorstel.
Allereerst: er komen publieke en private inlogmiddelen. Dit zorgt ervoor dat je als burger kan kiezen voor alleen een publiek inlogmiddel, alleen een privaat inlogmiddel of een combinatie van beide. Binnen de private inlogmiddelen is daarnaast nog marktwerking van invloed. Dit betekent dat er voor laaggeletterden veel keuzemogelijkheden zullen komen. Daardoor is de kans en het risico op oplichting binnen onze doelgroep groter. Onze doelgroep vindt het namelijk vaak moeilijk om te zien wat een veilig en betrouwbaar inlogmiddel is en om deze vergelijking te maken. Je kan je voorstellen dat hoe meer opties en keuzes er zijn, hoe sneller je het overzicht kwijtraakt. Daarnaast is het bij de toepassing van deze wet zo dat er, als je iets gekozen hebt en moet gaan inloggen op een pagina, ook nog heel veel keuzeopties zijn bij het inloggen. Klik ik als laaggeletterde wel op de juiste knop? Wat moet ik daarvoor kiezen en wat moet ik daarbij invullen? Verder zal ik waarschijnlijk meerdere inlogs hebben omdat ik bij het oude vertrouwde wil blijven en een publieke inlog zal hebben, maar daarnaast zal ik een private inlog moeten nemen om ook op andere sites goed te kunnen inloggen. Moet ik dan voor de ene of voor de andere kiezen? Wij raden vanuit de stichting dan ook heel erg aan dat duidelijk moet zijn wanneer en hoeveel inlogmogelijkheden je als burger moet hebben om goed mee te kunnen doen in de samenleving.
Daarnaast zien wij een drempel rondom die private inlogmiddelen. Het is heel mooi dat commerciële bedrijven door de mogelijkheid van private inlogmiddelen nu ook een extra beveiliging kunnen inbouwen. Bij het online verkopen van drank kunnen ze bijvoorbeeld controleren of de leeftijd van de burger wel hoog genoeg is om dat veilig te kunnen doen. Dit is een mooie ontwikkeling, maar die zorgt er wel voor dat er online extra handelingen zijn voor burgers die het toch al moeilijk vinden om online goed mee te kunnen komen. Door deze extra handelingen moeten zij meer stappen gebruiken en moeten zij hun inlog, die zij nu alleen voor semioverheidszaken gebruiken, ook opeens op commerciële pagina's gaan invoeren. Dit kan voor grote drempels zorgen. Het kan ervoor zorgen dat ze extra hulp nodig hebben, ook bij zaken buiten de semioverheid. Wij pleiten er dan ook voor dat het machtigen van deze inlogmiddelen op alle vlakken hetzelfde blijft. Zowel voor de private als de publieke inlog moet de manier van machtigen om iemand hulp te geven, hetzelfde zijn. Wij horen namelijk uit verhalen vaak dat laaggeletterden het nu al moeilijk vinden om deze machtiging goed rond te krijgen. Daarom geven ze hun gegevens vaak maar gewoon aan anderen. Deze gegevens worden dan verspreid, wat natuurlijk heel andere privacygevoeligheden met zich meebrengt.
Ten derde zagen wij in het wetsvoorstel dat er verschillende niveaus van beveiliging komen. Dat is natuurlijk heel goed voor de veiligheid van de burger, maar zorgt ook weer voor extra stappen voor onze doelgroep om te begrijpen welk niveau nodig is. Je zou kunnen zeggen dat het hoogste niveau het veiligste niveau van beveiligen is, dat elke burger daarom maar gewoon het hoogste niveau van beveiliging moet gaan gebruiken, en dat we deze stappen willen aanleren aan de kwetsbare doelgroepen. Maar aan dit hoogste niveau van middelen zijn kosten verbonden. Het is net al een paar keer benoemd dat de vraag is of deze kosten er wel zouden moeten zijn. Maar zeker voor een doelgroep die vaker in de schulden zit en vaker onder de armoedegrens leeft, is het belangrijk dat deze kosten echt minimaal zijn. Als dit namelijk niet zo is, zullen laaggeletterden vaker kiezen voor een minder beveiligde optie. Daardoor zal er een ongelijkheid ontstaan tussen de groep burgers die hiervoor wel genoeg geld heeft en

anderen die ervoor kiezen om hun geld uit te geven aan een pot pindakaas om thuis hun kinderen eten te kunnen geven.
Wij hopen dus ook dat met de benoemde adviezen in onze position paper en de middelen die we aanreiken, de doelgroep goed wordt meegenomen in de uitvoering als deze wet wordt aangenomen. Want het moet een vertrouwd en inclusief ontwerp zijn, zodat iedereen in de samenleving goed op deze digitale route kan meekomen.
Dank jullie wel.

De **voorzitter**: Dank u wel, mevrouw Bos. Mevrouw Van Velzen, wilt u ook het woord voeren?

Mevrouw **Van Velzen**: Ik zou graag bij de beantwoording van de vragen betrokken worden. Dank u wel.

De **voorzitter**: Dan gaan we nu over naar de vragen van de zijde van de Kamer. Wie mag ik het woord geven voor een vraag? De heer Koole namens de PvdA-fractie.

De heer **Koole** (PvdA): Dank u wel, voorzitter. Ik heb vragen aan beide inleiders. Bij de Stichting Lezen en Schrijven proef ik: hoe eenvoudiger, hoe beter het is voor de doelgroep. Tegelijkertijd vereist de veiligheid vaak juist een wat ingewikkelder vormgeving. Hoe kun je nou in de wet de juiste balans proberen te bevorderen tussen de toegankelijkheid voor de doelgroep en de vereiste veiligheid? Heeft u een aantal wat concretere suggesties om dat in de wet te bevorderen?
Dan een vraag aan de Nationale ombudsman, de heer Van Zutphen. In uw position paper staat dat de overheid verantwoordelijkheid moet nemen. Ik zou van u willen weten op welke punten dat dan zou moeten en hoe dat in deze wet zichtbaar moet zijn, volgens u.

De heer **Verkerk** (ChristenUnie): Voorzitter. Ik heb af en toe ook het gevoel dat ik laaggeletterd ben als ik op bepaalde websites zit. Dat punt lijkt me dus heel belangrijk. Ik wou vragen hoe goed het huidige wetsontwerp is op het gebied van inclusiviteit. En vindt u dat die inclusiviteit op AMvB-niveau geregeld kan worden, of vindt u dat het in de wet moet? Mijn laatste vraag is of de Stichting Lezen en Schrijven ook vanzelfsprekend aan tafel zit bij de overheid en andere mensen die deze wet maken.

De heer **Van Hattem** (PVV): Voorzitter. Ik heb een vraag aan de heer Van Zutphen. Ziet hij, ten opzichte van de huidige situatie met DigiD, in het voorliggende voorstel een verbetering of een verslechtering ten opzichte van de positie van de burger?

De heer **Van Pareren** (FvD): Voorzitter. Aan de heer Van Zutphen heb ik de vraag of hij als Ombudsman nu al veel klachten van de burgers krijgt over privacy en deze wetgeving, die er al is en dadelijk nog verder uitbreidt.
Aan een van de dames van de Stichting Lezen en Schrijven heb ik de volgende vraag. De wet is op een gegeven moment natuurlijk een wet. Dan komt er een uitvoering. Het punt dat u noemt, gaat over de uitvoering van de wet en de toegankelijkheid van de wet voor deze specifieke, heel grote groep burgers. Dat is dus erg belangrijk. Is er dan niet een beweging – ik noem het maar even zo; ik gebruik die term veel – om tot een soort jip-en-jannekeachtige methodiek te komen, waardoor die mensen zich veel sneller vertrouwd voelen met de steeds verder voortgaande technieken? Hoe denkt u daarover? Want het blijft een gegeven dat die mensen hier mensen moeite mee houden, dus je zult het ook buiten de wetgeving moeten faciliteren.

De **voorzitter**: Dank u wel. Ik nodig de heer Van Zutphen uit om als eerste te antwoorden.

De heer **Van Zutphen**: Dank u wel voor de vragen. Ja, «neem verantwoordelijkheid». Ik ben niet voldoende deskundig om te zeggen dat dat in deze wet zou moeten worden vormgegeven. Ik denk dat het ook heel goed kan in andere regelingen en uitvoeringen. Er is heel veel gezegd over op welk niveau regelgeving moet plaatsvinden. Ik herinner me het symposium «De waarde van de wet» bij de Raad van State in 2018. Van Ommeren heeft daar toen het een en ander gezegd over wat op welke manier zou moeten worden geregeld. Het kwam net ook aan de orde bij meneer Van Lochem. Ik sluit me daar dus bij aan. Ik vind wel dat het duidelijker kan dan het nu in de wet staat, omdat ik het graag zelf wil begrijpen. De verantwoordelijkheid zit «m erin dat de overheid zich moet realiseren dat door moeilijke, ingewikkelde regels en systemen mensen buiten de boot vallen. Dat betekent dat de overheid de verantwoordelijkheid moet nemen door de regie te nemen voor diegenen die moeilijk of niet meekunnen in de nieuwe systemen. De titel van ons jaarverslag luidde het afgelopen jaar dan ook «Regel regie!».
U vroeg iets over een machtigingsvoorziening. Over de DigiD zoals die er nu is, krijgen we van verschillende kanten klachten. Aan de ene kant zijn er klachten van mensen die zeggen: ik weet niet hoe dat moet en ik kan het niet. En aan de andere kant krijgen we klachten van professionals, bijvoorbeeld bewindvoerders die mensen bijstaan die onder curatele zijn of in schuldenbewind verkeren. Zij zeggen: ik wil zo graag die echte machtigingsmogelijkheid hebben, want dan kan ik heel gericht doen waar ik voor ben, namelijk het belastingadvies geven of het bijstaan bij zorgcontracten; dan kan ik helpen. Nu zijn er heel veel mensen die bij ons klagen en zeggen: ik kan maar één ding doen, namelijk al mijn DigiD-gegevens aan een ander geven, die vervolgens overal naar kan kijken, tot de waterschapsbelasting aan toe. Dat is heel erg onwenselijk. In die zin zou deze wet dus een verbetering kunnen zijn, ja, als in de uitvoering wordt geregeld dat met de juiste beveiligingsniveaus en gebruiksvriendelijkheid zowel de mensen die graag een machtiging willen afgeven als degenen die met een machtiging aan het werk gaan, daarbij gebaat zijn. Dat is meteen een antwoord aan meneer Van Hattem. En eigenlijk maakt het niet uit welke wet of welk systeem je hebt; dat is de verantwoordelijkheid die je moet hebben. Je moet ervoor zorgen dat als je iets maakt, de burger ermee uit de voeten kan. Dat heb ik zelf gezegd op dat symposium in 2018: kun je er een beetje mee uit de voeten of niet? Als het antwoord nee is, is de overheid nodig voor de regie. Dat is ook wel een beetje de zorg die ik heb bij dat publiek-private. Wat betreft het publieke is de vraag hoe de overheid dan zorgt dat die regie genomen wordt. Daar heb ik dus wat zorgen over.
Krijgen we veel klachten? Nou, u had bij ons moeten zijn toen de blauwe envelop verdween. Toen konden we het niet bijbenen. Iedereen moest de telefoons opnemen, tot de receptionisten aan toe. Er waren duizenden klachten. Dat is overigens daarna vrij constant gebleven, maar we hebben het vooral ook proberen om te zetten in: waar moeten we aan denken? Mijn Berichtenbox bijvoorbeeld was er een. Wij vragen aan de burgers wat zij van de overheid verwachten in 2030. Hoe moet die eruitzien en ben je bereid om digitaal te gaan? Dan is het antwoord: ja, wij willen best digitaal, maar daar hoort nog wel iets bij; dan moet de overheid wel deskundig zijn. Algoritmen werden ook eerder genoemd. Dat was ook een kopje in dit onderwerp. Wij hebben daarover gezegd, overigens samen met heel veel anderen, dat je een algoritme niet van tevoren hoeft uit te leggen, maar dat er als het systeem op basis van een algoritme een besluit produceert, een ambtenaar moet zijn die kan zeggen waarom dat besluit op jou van toepassing is. Daarover zien wij heel veel vragen rijzen: klopt het eigenlijk wel wat hier gebeurt?

Ik zal u een voorbeeld geven van wat er gebeurt als mensen niet meekunnen in de digitale wereld. Daarna sluit ik mijn antwoord af. We kregen een klacht van een meneer die bij het UMCG in Groningen zijn patiëntendossier wilde inzien, elektronisch. Dat kan alleen maar met een sms-identificatie, maar die meneer zat in de schulden en zijn bewindvoerder had gezegd: jij gaat geen iPhoneabonnement afsluiten. Hij had dus niks. Hij kon het aanvragen op papier en dan duurde het zes weken. Met een sms-code had hij het binnen twintig seconden gehad. Daaraan zie je wat er kan gebeuren. Het is een beetje een parabelachtig verhaal, maar als die overheid dus niet alert is op hetzelfde niveau van dienstverlening voor diegenen die niet meekunnen of niet mee mogen, gaat het fout. En daar is die verantwoordelijkheid van de overheid van het allergrootste belang, om te zorgen dat iedereen op dezelfde manier mee kan doen. Dank u wel.

De **voorzitter**: Dank u wel. Dan de Stichting Lezen en Schrijven.

Mevrouw **Van Velzen**: Dank u wel, voorzitter. De heer Koole vroeg of de Stichting Lezen en Schrijven eigenlijk stelt: hoe eenvoudiger hoe beter. Hij vroeg ook hoe ik de balans in de wet beoordeel tussen toegankelijkheid en veiligheid. Wij zeggen niet dat in algemene zin geldt: hoe eenvoudiger hoe beter. Het geldt wel voor de grote groep mensen die moeite heeft met lezen, schrijven en rekenen en bij wie de digitale vaardigheden dikwijls tekortschieten. Maar wat we eigenlijk concluderen is dat in deze wet ook private inlogmiddelen en mogelijkheden worden toegevoegd aan datgene wat publiek al behoorlijk moeilijk wordt gevonden. Daarmee neemt de toegankelijkheid voor die grote groep zeker niet toe. Sterker nog, het wordt complexer, en het wordt ook complexer voor de overheid om te kunnen garanderen dat de informatie voor die grote groep mensen met al die verschillende inlogsystemen ook toegankelijker wordt. De vraag is dus of, in ieder geval vanuit het perspectief van de grote groep laaggeletterden, de toevoeging van extra mogelijkheden om ook via private middelen te kunnen inloggen daaraan bijdraagt. Daar hebben wij wel grote zorgen over.
De heer Verkerk vroeg bijvoorbeeld hoe inclusief de huidige websites eigenlijk zijn, en hoe de huidige toegankelijkheid van de dienstverlening van de overheid voor die grote groep is. Die is beperkt. Er wordt altijd voor gepleit om op B1-niveau te schrijven, maar voor deze groep zou A2 eigenlijk nog beter zijn. Maar het is natuurlijk een beperkte groep en ik begrijp dat de afweging wat goed is voor de gehele Nederlandse bevolking door u te maken is. Maar vanuit het perspectief van een grote groep, die dus niet afneemt, zoals je zou willen, maar op dit moment alleen nog maar toeneemt, is dat lastig. Dat is één uitgangspunt.
Dus ja, voor deze groep zou het belangrijk zijn dat in ieder geval datgene wat publiek blijft op een lager taalniveau geschreven wordt. Waar wij zorgen over hebben in de uitvoering, is of alle initiatieven vanuit de overheid om een inclusieve digitale samenleving te bevorderen, met voorstellen zoals DIGIbeter, waarin digitale vaardigheden voor iedereen worden aangeboden in cursussen, parallel blijven lopen met deze WDO. Zou alles dan in jip-en-janneketaal geschreven moeten worden? Dat hoeft niet, maar het is wel belangrijk dat ook private aanbieders op een toegankelijke manier hun dienstverlening blijven aanbieden. Nog één laatste punt daarbij. Het is natuurlijk één ding of de overheid zicht houdt op de private aanbieders die zij zelf toestaat om een inlogsysteem aan te bieden, maar het is niet uit te sluiten dat voor die groep met een lage mediawijsheid de kans bestaat op oplichting, omdat er ook andere, malafide aanbieders kunnen komen die niet door de overheid erkend worden maar toch veinzen dat ze eHerkenning mogen aanbieden.
Dank u wel.

De **voorzitter**: Dank u wel. Mevrouw Bos, wilt u nog een aanvulling geven?

Mevrouw **Bos**: Ja, een hele korte aanvulling. Er werd gevraagd hoe we kunnen faciliteren dat laaggeletterden wél kunnen meekomen met dit soort wetsveranderingen. Daarbij is het wel erg van belang dat er naast het online aanbieden ook een papieren route beschikbaar blijft, die snel beschikbaar is. Er moeten loketten zijn waarnaartoe gebeld kan worden met vragen, of assistant-digitalprincipes, waarmee digitaal ondersteund kan worden zodat het wel toegankelijk blijft.
Daarnaast wil ik nog het volgende toevoegen. DIGIbeter werd al door Geke genoemd, maar er zijn veel onlineomgevingen waar je dit kan inbouwen zodat laaggeletterden kunnen oefenen met deze nieuwe veranderingen, waardoor ze beter kunnen meekomen in de samenleving.

De **voorzitter**: Dank u wel. Ik kijk nog even naar de leden. We hebben ruimte voor nog één laatste vraag als daar behoefte aan is. Nee, zie ik. Dan wil ik u hartelijk danken voor uw bijdragen. Zoals al eerder gezegd wordt dit allemaal keurig opgeschreven, zodat wij het allemaal nog eens kunnen nalezen. We gaan het dan verder betrekken bij de behandeling van het wetsvoorstel. Dat zal uiteraard na de zomer zijn. Dank u wel.

Blok 4: Handhaafbaarheid in de breedste zin

De **voorzitter**: We gaan naar het laatste onderdeel van deze deskundigenbijeenkomst, over de handhaafbaarheid in de breedste zin van de wet en alle maatregelen van bestuur en dergelijke die daaronder hangen. Daarvoor hebben we als commissie twee sprekers uitgenodigd. De eerste is de heer John Derksen, die hoofd toezicht is en tevens plaatsvervangend hoofdinspecteur bij het Agentschap Telecom, de tweede mevrouw Lokke Moerel, hoogleraar Global ICT law aan de Universiteit van Tilburg en lid van de Cyber Security Raad. Ik zie dat de heer Derksen al in de zaal zit en achterin staat mevrouw Moerel. Ik zou u willen vragen achter de tafel plaats te nemen. Dan kunnen we beginnen. Zoals u in de vorige onderdelen van de hoorzitting hebt gezien, vragen we u om maximaal vijf minuten uw visie op de Wet digitale overheid nog eens toe te lichten. Daarna gaan de leden u wat vragen stellen. Ik laat het aan u over; misschien hebt u dat onderling afgesproken. Ik zie dat meneer Derksen als eerste het woord krijgt. Alstublieft, gaat uw gang.

De heer **Derksen**: Dank u wel, voorzitter. Dank voor de gelegenheid om hier te mogen spreken. Agentschap Telecom is een toezichthouder op de generieke digitale infrastructuur. Het houdt onder andere toezicht – gerelateerd aan dit onderwerp – op de eIDAS-regelgeving, de Wet beveiliging netwerk- en informatiesystemen, voorheen de cybersecuritywet en aanverwante wetten. Zo zijn wij nu in de Wet DO – digitale overheid – aangewezen als toezichthouder op de inlogmiddelen. Een kenmerk bij ons toezicht op dit soort systemen is dat het opennormtoezicht is, dus dat de eisen in lagere regelgeving verwoord worden maar ook veelal een open karakter kennen, waardoor wij intensief toezicht houden op deze partijen, aan de hand van normen die de stand der techniek weerspiegelen. Op die manier kunnen we in ons toezicht de meest moderne inzichten meenemen in het beoordelen van veiligheid, betrouwbaarheid en integriteit van dit soort inlogmiddelen.
Daar hebben we veel ervaring mee. We houden opennormtoezicht ook in het kader van telecomsecurity en de continuïteit van telecom.
Als we naar de wet kijken, vallen ons een aantal dingen op. Allereerst de reikwijdte, tenminste vanuit ons perspectief. Wij houden onder de Wet digitale overheid geen toezicht op het hele stelsel maar op een onderdeel van het stelsel, namelijk de eerder genoemde inlogmiddelen. We houden

op dit moment toezicht op eHerkenning, dat is een bedrijfsinlogmiddel. Onder een bepaald construct houden we daar wel op het hele stelsel toezicht. Dat betekent voor de uitvoering van ons toezicht dat wij goed zicht moeten hebben op het stelsel waarbinnen de inlogmiddelen hun werk moeten doen. Onder de wet DO is dit niet het geval en dat betekent dat de overheid, in dit geval het ministerie, een goede governance neer moet zetten en de informatie-uitwisseling met de toezichthouder goed op orde moet hebben. Daarover zijn we in gesprek, dus dat is een aandachtspunt.
Het tweede wat ons opvalt is de dualiteit in het stelsel. We kennen inlogmiddelen voor bedrijven en inlogmiddelen voor burgers. De eisen die in lagere regelgeving terechtkomen, lijken anders te zijn in aanvang. Dat is allemaal nog onder construct, dus daarover zijn we ook in gesprek met het ministerie. De gedachte daarachter is om innovatie mogelijk te maken, maar wij zullen als toezichthouder innovatie niet inruilen voor veiligheid en betrouwbaarheid. Omwille van eenduidigheid pleiten wij, in ieder geval op termijn, voor één normenstelsel op het geheel.
Het derde punt is de kwestie toelating versus toezicht. We zijn aangewezen als toezichthouder. De toelating staat nog open. Wij gaan ervan uit dat wij de toelating ook gaan doen, dus een partij die een inlogmiddel aanbiedt, moet toegelaten worden tot het stelsel en daarna volgt het toezicht. In ons perspectief is dat één beweging, want je kunt niet iemand toelaten en vervolgens vanuit het toezicht zeggen: u hoort hier eigenlijk niet. Dan wordt het heel ingewikkeld, ook voor de burger, om te kijken wat hij wel en niet mag gebruiken. Ook daarover zijn we nog in gesprek met het ministerie.
Het vierde punt – dat raakt ook het thema van dit blok – is de handhaafbaarheid. Daarvoor zijn we wel aangewezen als toezichthouder, alleen hebben we nog geen handhavende bevoegdheden. We gaan ervan uit dat dat mandaat aan ons verstrekt wordt, voor zowel de private als de publieke inlogmiddelen.
Tot slot. In het eerste blok heeft u ook een andere toezichthouder ontmoet, AP. Wij sluiten onderling convenanten af om het grijze gebied dat hier altijd speelt goed met elkaar te verkennen en te zorgen dat we geen dubbele toezichtactiviteiten uitvoeren. Dat convenant zal straks gemaakt worden, op het moment dat de lagere regelgeving helder is.
Tot zover mijn inleiding.

De **voorzitter**: Dank u wel. Dan zijn we gekomen bij de laatste deskundige van deze ochtend, professor Lokke Moerel, hoogleraar Global ICT law in Tilburg. Aan u het woord.

Mevrouw **Moerel**: Dank u, voorzitter. Goede, veilige inlogmiddelen zijn belangrijk voor onze digitale infrastructuur. Ik wil even de context schetsen dat dat ook goed is voor de privacy. Als je dat niet op deze manier organiseert, dan moet iedereen overal weer zijn bsn-nummer invoeren en dergelijke, waardoor de kans op identiteitsdiefstal en fraude groter wordt. Dus vanuit privacyoptiek kan dit iets goeds zijn in de brede zin.
Dan heb je de inlogmiddelen zelf. Die kun je ook privacy by design inrichten. Voor de corona-app wilden we eerst een centrale database waar alles in ging. Nu zeggen we: het kan ook decentraal, waarbij de check alleen op je eigen device gebeurt. Dat is wat Privacy First heeft laten zien. Het tweede is dat privacy by design betekent dat je met attributen werkt. Ik ga hier niet verder op in, maar het gekke is, als je naar deze wet kijkt, dat die is ingestoken op een centraal systeem en dat juist attributen voor inlogmiddelen voor individuen er niet in staan. In zoverre is die wet eigenlijk al ingehaald door de technologie, door de manier waarop die is opgezet. Het gekke is dat we privacy by design dus niet als vereiste in de kaderwet hebben staan. Wat is daarvan het gevolg?

Dan wil ik nog een ding zeggen. Privacy by design en security by design liggen heel erg in elkaars verlengde. Als je data niet hebt, kun je die ook niet kwijtraken, wat wel het beste beveiligingsmiddel is. Doordat privacy by design niet in die kaderwet staat en eigenlijk de opzet meer centraal is, komt natuurlijk de vraag op: houdt het AT dan bij de erkenning van een inlogmiddel daar toezicht op, terwijl dat in het inlogmiddel zelf moet zitten? Of gaat dan de AP – want de AVG is aanvullend van toepassing – er dan achteraf toezicht op houden of dat goed is gedaan?
De vraag aan mij was: zeg iets over het toezicht. Ik hoop dat u ziet dat voorkomen beter is dan genezen en dat toezicht vooraf of een inlogmiddel voldoet aan de vereisten van privacy en security by design beter is, en dat het beter is daar ook toezicht op te houden zodat je de erkenning kan intrekken, dan dat je later, bij private partijen die global zijn en ondoorzichtig, als AP toezicht moet gaan houden om te kijken wat er gebeurt met de data.
Er is een keuze gemaakt voor private aanbieders. Daar zit altijd een verdienmodel achter. Ik werk voor die grote techbedrijven, dus ik heb vrij goed inzicht in wat die verdienmodellen zijn. Het eerste is: als je een hele infrastructuur gaat bieden, dan moet daar een verdienmodel aan zitten. Het ene is dat je iets met de data kan. Dan kom je op dingen zoals dat je verder niks doet met het bsn-nummer maar wel bekijkt bij welke websites wordt ingelogd, wat voor profilering je daarmee kan doen, of je daar een verdienmodel aan kan hangen. Het tweede is dat je gewoon een prijs vraagt voor de dienst. Als private partijen dat doen, is de kans groot dat dat een hogere prijs wordt, wat een nadeel is voor de burger.
Als je naar dat eerste model kijkt – laten we ervan uitgaan dat dit het model is dat gekozen wordt – en als je kijkt naar het profileren en de risico's daar, dan hoop ik dat u kunt zien dat daar een decentraal stelsel, waar die data niet centraal bij die partij is maar decentraal op de devices zelf aanwezig is, een hele goede oplossing is vooraf, om te voorkomen dat die data misbruikt wordt, zodat je dat niet achteraf met toezicht houden moet oplossen. Dat is een. Het AT zou er dan vooraf toezicht op kunnen houden dat dat ook goed is ingericht.
De tweede manier om daar wat aan te doen, is inderdaad door gewoon te zeggen: open source is een vereiste, waardoor ook daar het AT toezicht vooraf bij de erkenning kan houden, in plaats van dat de AP achteraf, als dingen al gebeurd zijn, met de kraan open moet dweilen. De AP is een vangnet voor als er daarna nog iets misgaat, maar het zou in het toezicht vooraf moeten worden opgevangen.
Datzelfde idee zag ik bij open banking. Daar is niet goed over nagedacht. Er is later ook ontzettend veel kritiek gekomen op PSD2 en open banking. Door niet die vereisten in de vergunningverlening te zetten, moet de AP op de hele branche het toezicht houden. Aleid Wolfsen heeft duidelijk gemaakt dat hij daar het geld en de middelen niet voor heeft.
De kans is groot dat als je zegt dat dat privacy by design moet en dat het open source wordt, het minder aantrekkelijk wordt voor partijen die eigenlijk stiekem denken: ik kan van alles met die data. Ik denk dat dat ook precies de bedoeling is.
Ik kijk naar wat de vraag is aan uw Kamer. Ik kom hier niet zo vaak, dus ik dacht: wat zou ik zelf doen? Het eerste is dat privacy by design, dus niet alleen security maar echt specifiek privacy by design, waardoor data überhaupt niet verwerkt hoeft te worden, in de kaderwet komt. Mijn voorstel zou zijn – misschien is Aleid Wolfsen het daar niet mee eens – dat het toezicht op het design van die inlogmiddelen bij het AT komt, ook al is dat een privacyvereiste. Ik denk dat dat zo verweven is met security dat het scheiden daarvan niet zinvol is.
Ik ben er, gezien de beperkte middelen voor toezicht, sowieso voor dat niet per wet toezicht wordt georganiseerd maar meer per functie. In dit geval is dat echt op de technische infrastructuur. Dat zou bij de AT moeten

liggen. Blijkt er later alsnog misbruik te zijn van data, dan is dat het level waarop de AP dan met de dweil achteraf toezicht kan houden.
Het tweede voorstel zou zijn dat open source echt toegevoegde waarde kan hebben, net als met de corona-app. De enige reden dat dat ding nu hopelijk een succes gaat worden, is omdat het open source is geweest. Dat is ook de voorkeur van de overheid. Alles wat gebeurt met overheidsdingen zou open source first moeten zijn. Ik zit in de Cyber Security Raad. Het is een beetje «Wc-eend beveelt Wc-eend aan», maar we hebben daar een advies over de e-Identification gegeven, met als voorkeur open source. Ik zit daar niet alleen in, maar met twintig experts. Daar is lang over gepraat. Dit is het advies van de Cyber Security Raad. Dus dat is het derde.
En dan het laatste, een beetje buiten de vraag. De wet lijkt een centrale oplossing primair te stellen. Ik vraag aan de secretaris of hij kan bevestigen dat ook decentrale oplossingen voor erkenning in aanmerking komen. Je kan erover twisten of dat überhaupt kan. Ik zou die bevestiging vragen. En verder zou ik ook attributen mogelijk maken voor de identificatie van burgers.

De **voorzitter**: Dank u wel, mevrouw Moerel. We hebben de heer Van der Burg van de VVD nog niet gehoord, dus die krijgt als eerste het woord. Ga uw gang.

De heer **Van der Burg** (VVD): Mevrouw Moerel, u zei dat deze wet eigenlijk alweer is achterhaald door de werkelijkheid. De heer Wolfsen zei dat met betrekking tot DigiD. Deze wet volgt daarop. Kunt u eens reflecteren op wat erger is: een DigiD-houder die achterhaald is of deze wet? Daaraan gekoppeld: wat zou u doen in onze plaats? Wij kunnen een wet niet wijzigen. Uiteindelijk stemmen wij voor of tegen de wet. Wij zijn helaas … Nou, dat «helaas» heb ik niet gezegd, voorzitter. Wij zijn geen Tweede Kamerleden, dus wij kunnen geen wetten wijzigen. Zou u voor- of tegenstemmen?
Dan richting de heer Derksen. U bent op dit moment ook toezichthouder van heel veel commerciële partijen die data van ons hebben. Vodafone, KPN en al die andere partijen kunnen zien wie ik bel en waar ik ben. Google weet op basis van algoritmes en zoekactiviteiten eerder wanneer iemand zwanger is dan die persoon zelf. Kortom, kunt u daar eens op reflecteren?

De **voorzitter**: In deze ronde zou ik ook nog de heer Van Pareren het woord willen geven voor een vraag.

De heer **Van Pareren** (FvD): Dank u, voorzitter. Ik heb een vraag aan mevrouw Lokke Moerel, een beetje inhakend op wat hiervoor werd gezegd. U komt met een aantal suggesties en zegt dat de Cyber Security Raad druk bezig is. Ik krijg een beetje het idee dat ook wij als Eerste Kamer achter de feiten aan lopen, net als de Tweede Kamer. Bent u ook geconsulteerd bij het opstellen van de wet? Er werd gesteld – daar begon u mee – dat vaak alles al wordt ingehaald door de ontwikkelingen bij de technologie. Hoe kan je dat voorkomen in de flexibiliteit?
Aan de heer Derksen heb ik een vraag over het blokje handhaving. Heb ik goed begrepen dat u aangeeft niet te kunnen handhaven?

De **voorzitter**: Dan de heer Koole van de Partij van de Arbeid.

De heer **Koole** (PvdA): Dank u wel, voorzitter. Ik sluit me aan bij de vraag wat wij als Eerste Kamer kunnen doen, aangezien we geen amendementsrecht hebben. Wat zou u doen? Zou u, mevrouw Moerel, voor of tegen de wet stemmen? Anders geformuleerd: zijn de voordelen van deze wet groter dan de nadelen?

Aan de heer Derksen wil ik het volgende vragen. In uw paper zegt u dat door middel van een amendement van de Tweede Kamer het toezicht is geattribueerd aan het agentschap, maar dat de handhavende bevoegdheden daar niet in zijn meegenomen. Nu moeten wij de wet beoordelen. Dit is er kennelijk op het laatste moment in gekomen en zat dus niet in het ontwerp van de wet. Maar de handhavende bevoegdheden zijn er niet. Als de telecom iets moet doen is het toch wel toezicht houden, ook op de handhaafbaarheid. Kunt u op basis van de wet überhaupt uw werk verrichten als die handhavende bevoegdheden daar niet of nog niet in staan?

De **voorzitter**: De heer Verkerk van de ChristenUnie en daarna mevrouw Gerkens van de SP. De laatste minuten zijn vervolgens voor de twee deskundigen.

De heer **Verkerk** (ChristenUnie): Voorzitter. In de position paper van de heer Derksen heb ik een paar keer het woord «oeps» gezet, juist vanwege het feit dat hij zegt: hé, ik ga wel over dit soort middelen, maar niet over het totale systeem. Eigenlijk vind ik dat heel erg zorgelijk. Misschien kan hij dat nog iets toelichten.
Mevrouw Moerel zou ik het volgende willen vragen. Ik ben redelijk op de hoogte van privacy by design. Het verbaast me inderdaad, als u dat zo zegt, dat dit niet in de wet zit. Wat zouden wij moeten doen om dat in de wet te krijgen? Kan dat op AMvB-niveau geregeld worden? Of is een novelle nodig, waarbij we de wet moeten terugsturen naar de Tweede Kamer? Wat betekent dat?

Mevrouw **Gerkens** (SP): Voorzitter. Aanvullend op privacy by design. Een aantal sprekers hebben al betoogd dat een decentrale opslag veiliger is, bijvoorbeeld op de eigen device. Zou u daar ook voor pleiten? Hoe ziet u dan nu de wet, die neigt naar centrale opslag?

De **voorzitter**: Dan kijk ik naar de deskundigen achter de tafel. Wie van u wil beginnen?

Mevrouw **Moerel**: Ik wil graag even een seconde overleggen.

De **voorzitter**: Dat is prima. We zien hier, zeg ik tegen de mensen die met ons meekijken, dat twee deskundigen achter de regeringstafel met elkaar overleg plegen over de inhoud van de beantwoording en wie als eerste antwoord gaat geven. Dat is mevrouw Morel, blijkt nu. Gaat uw gang.

Mevrouw **Moerel**: Ik ben geen wetgevingsexpert. We hebben daarom ook even overlegd. We denken dat je op eisenniveau privacy by design en open source zou kunnen inbrengen. Wat dat betekent voor uw stemming vind ik lastig in te schatten. Ik ben daar geen expert in.
Als ik even hoog over kijk – ik weet niet of u daarop zit te wachten, maar zo kijk ik ertegen aan – hebben we de eIDAS-verordening, waarin in feite een heel stelsel staat voor de erkenning van e-identitydingen. Als ik hoog over kijk naar de wet, herken ik daar als toegevoegde waarde voor Nederland in dat de overheid die dingen moet accepteren als inlogmiddelen. Er ontstaat namelijk een wildgroei aan wat iedere overheidsinstantie doet. Ik zeg het maar even simpel: dat zou met een simpeler wetje kunnen gebeuren dan er nu ligt.
Wat de toegevoegde waarde van deze wet zou kunnen zijn, is een opensourcegedeelte. Dat staat er overigens niet in, want dat zit niet in de Europese verordening. Maar als je echt nadenkt over de risico's van de private middelen, is dát de weg om te gaan. Als dat ingericht kan worden en als u als wetgevingsexperts ook denkt dat dit op eisenniveau ingevoerd kan worden, net als het privacy-by-designgedeelte, dan denk ik dat ik voor

zou stemmen, op voorwaarde dat dit er dan ook komt. Als dat niet kan, zou ik zelf tegenstemmen. Ik zeg het u gewoon zoals het is.

De **voorzitter**: Zoals u het ziet. Dan de heer Derksen voor zijn beantwoording.

De heer **Derksen**: Als eerste het stelstel. U geeft aan een aantal oepsmomenten gehad te hebben. De oepsmomenten zijn in onze beleving op te lossen in lagere regelgeving, maar die moeten dan wel geadresseerd worden. We hebben die ook in onze position paper geformuleerd, omdat die in lagere regelgeving geregeld moeten worden. De Minister kan de toelating aan ons mandateren. Dat heeft onze sterke voorkeur, precies om de reden die mevrouw Moerel aangeeft. Je borgt daarmee de toegang tot het stelsel. Bij die toegang zijn de eisen die de toezichthouder stelt van kracht. Daardoor garandeer je de integriteit van de inlogmiddelen. Dit is nog niet bij wet aan ons geattribueerd. Het kan wel in lagere regelgeving of in mandaat gegeven worden. Er zijn oplossingen voor. Wij vinden dat dit integraal aan ons zou moeten worden toegewezen als je de betrouwbaarheid van inlogmiddelen adequaat wil garanderen.
Dat we niet toezicht houden op een heel stelsel, is een keuze van de wetgever. Wat daarvoor pleit is dat je integraal alle koppelvlakken in zo'n stelsel ook onder toezicht hebt. Aan de andere kant is het in overheidsbeheer. De Minister heeft daar een governancestelsel voor, waar wij kennis van dragen. Wij kunnen dat hele stelsel dus wel overzien en kunnen vanuit onze signalerende en agenderende functie als toezichthouder de Minister hierover gerichte adviezen geven. We kunnen dat alleen niet zelf bewerkstelligen; dat moet de Minister doen.
De handhavende bevoegdheid is onlosmakelijk verweven met onze toezichthoudende bevoegdheid. Als ik alleen maar toezicht kan houden en niet kan handhaven, wordt het heel ingewikkeld. De Minister moet dan zelf handhaven. Daar kun je wel goede afspraken over maken, maar over het algemeen is het te doen gebruikelijk dat de toezichthouder én toezicht houdt én handhaaft waar nodig. We werken onder de aanwijzing van de Minister-President, dus met een zekere onafhankelijkheid. Op die manier heeft u ook de garanties dat dit op die manier uitgevoerd wordt. We gaan ervan uit dat dit aan ons gemandateerd wordt, ook de handhavende bevoegdheden. Dat staat nu niet voor alle middelen zo in de wet en moet nog wel geregeld worden.
Dan de vraag van de heer Van der Burg over data in telecomsystemen. Wij voeren een deel van het gegevenstoezicht uit vanuit de Telecommunicatiewet. Wij letten erop of de verkeersgegevens in telecomsystemen slechts en uitsluitend voor het doel – er zit een hele sterke doelbinding op – gebruikt worden. Dat ligt bij ons en niet bij de AP, omdat daar een heel sterke technische component in zit. Ons vak is om in dergelijke systemen die beoordeling te doen, dus om ook vanuit de techniek die garantie te bieden.
Volgens mij heb ik dan alle vragen beantwoord, voorzitter.

De **voorzitter**: Ik kijk nog even naar de collega's of alle vragen beantwoord zijn. De heer Koole.

De heer **Koole** (PvdA): Ik heb nog één vervolgvraag. U zegt dat de handhavende bevoegdheden absoluut nodig zijn omdat u anders uw werk niet kan doen. Maar deze staan niet in de wet. Zou de heer Derksen een paar voorbeelden kunnen noemen van dergelijke bevoegdheden? We moeten duidelijk hebben of de handhaving niet in een formele wet moet, wat mij voor de hand lijkt te liggen, of eventueel in lagere regelgeving terecht kan komen. Ik zou graag een paar voorbeelden krijgen van situaties waarin het absoluut nodig is om te kunnen handhaven en waarin u die bevoegdheden als telecom hoort te hebben.

De **voorzitter**: Een van de andere leden nog een laatste vraag? Dat is niet het geval. Dan de heer Derksen voor de beantwoording.

De heer **Derksen**: Bij handhavende bevoegdheden moet u als eerste denken aan intrekking van de toelating. Dat is meteen het zwaarste middel. Als een partij – dit kan een private partij maar ook een overheidspartij zijn – willens en wetens niet voldoet en ook niet van plan is om dat te doen, moeten we de toelating kunnen intrekken. Dan is het voor de burger ook helder dat dat middel niet meer gebruikt mag worden. Andere middelen zijn een last onder dwangsom en een bestuurlijke boete. Een last onder dwangsom gebruiken we veel om partijen te stimuleren om te voldoen waar ze nog niet voldoen, maar waar we wel een sterke intentie voelen dat de partij wil voldoen. We kunnen daar dan enige druk achter zetten. Een bestuurlijke boete kan gegeven worden als er een aperte overtreding is geweest die nog niet zo ernstig is dat een intrekking aan de orde is. Dat palet aan bevoegdheden hebben we ook onder de Telecommunicatiewet. Onze ervaring is dat we partijen daarmee goed ervan kunnen overtuigen dat ze hun werk goed moeten doen.

De **voorzitter**: Mevrouw Moerel, wilt u nog een laatste opmerking maken voordat ik de bijeenkomst afsluit?

Mevrouw **Moerel**: Nee.

De **voorzitter**: Dat is ook een heerlijk, helder en kort antwoord. Daardoor heeft meneer Van Pareren nog even de gelegenheid om een vraag te stellen.

De heer **Van Pareren** (FvD): Het is meer een aanvullende vraag, of beter gezegd: ik heb de vraag al gesteld. Zou de Cyber Security Raad ons – te beginnen bij de Tweede Kamer – al van tevoren adviezen kunnen geven van: jongens, het gaat zo snel; let op, kijk uit? De gang voordat het bij de EK komt en voordat wij besluiten nemen of bijeenkomsten houden, is vrij traag. Hoe kijkt u naar het naar voren schuiven van het geheel?

De **voorzitter**: Mevrouw Moerel, een kort antwoord graag.

Mevrouw **Moerel**: Ik vind dit traject sowieso lastig te doorgronden. De adviezen liggen er en zijn gericht aan de ministers. Daar gebeurt niet veel mee. Dat rommelt maar door en dan komt het hier, en dan mag ik hier toevallig wat zeggen. Dit is toch hoe het gaat. De CSR heeft verder geen officiële bevoegdheden, maar geeft adviezen af. Heel vaak gebeurt daar echt wat mee, maar soms ook niet.

De **voorzitter**: In dat kader kan ik u vertellen namens de commissie Binnenlandse Zaken dat we alle bijdragen die we vandaag van de deskundigen gehoord hebben, uiteraard zullen meenemen in de behandeling van het wetsvoorstel. Hartelijk dank daarvoor. Na de zomer zullen we daar eerst schriftelijk op reageren en te zijner tijd zal er, neem ik aan, een mondelinge behandeling van het wetsvoorstel komen in de plenaire zaal. Dat kunt u allemaal volgen, want het is openbaar. Als u tussentijds nog ergens een advies over wil geven, zijn wij graag bereid dat verder bij de beoordeling te betrekken. Dus nogmaals hartelijk dank. Ik wil ook degenen die via de livestream mee hebben gekeken hartelijk bedanken voor het feit dat zij dat gedaan hebben. Uiteraard dank ik ook de collega-senatoren voor hun betrokkenheid bij de voorbereiding van deze deskundigenbijeenkomst en het wetsvoorstel zelf. Tot slot wil ik met name de mensen die de techniek verzorgd hebben, de Bodedienst en uiteindelijk ook Laurens Dragstra hartelijk bedanken voor de voorbereiding van deze

toch wel heel goed geslaagde deskundigenbijeenkomst. Iedereen hartelijk bedankt.
Dan sluit ik hierbij deze deskundigenbijeenkomst van de commissie voor Binnenlandse Zaken. Dan hebben we hier nog een prachtig presentje voor de deskundigen, zodat zij niet met lege handen naar huis gaan. Dank u wel.

Sluiting 11.28 uur.