12
Wet digitale overheid

Aan de orde is de behandeling van:
- **het wetsvoorstel Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid) (34972);**
- **het wetsvoorstel Wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid) (35868).**

De **voorzitter**:
Aan de orde is de gezamenlijke behandeling van de wetsvoorstellen 34972, Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur, kortweg de Wet digitale overheid, en 35868, Wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur, de Wet digitale overheid.

Ik heet de staatssecretaris Koninkrijksrelaties en Digitalisering van harte welkom in de Eerste Kamer.

De beraadslaging wordt geopend.

De **voorzitter**:
Ik geef het woord aan de heer Ganzevoort namens GroenLinks.

De heer **Ganzevoort** (GroenLinks):
Voorzitter. Dat de Eerste Kamer heel lang op dinsdag na tweede paasdag niet vergaderde, had ermee te maken dat de reis per postkoets of anderszins soms zo lang duurde dat men al op maandag, en dus op een feestdag, moest reizen. Dat is, ondanks de klachten over overvolle en uitvallende treinen vandaag, natuurlijk een volstrekt verouderd principe. Daarom is dit een aantal jaren geleden aangepast en vergaderen we nu op de dinsdag na Pasen gewoon braaf door. Als de tijden veranderen, moeten wij mee veranderen om niet volstrekt achterhaald te raken. Daarom is de Eerste Kamer een jaar of tien geleden overgegaan op een totaal gedigitaliseerd systeem voor vergaderstukken. Dat was een vernieuwing waarmee wij onze tijd ver vooruit waren.

In dat licht bezien is de Wet digitale overheid een belangrijke poging om zaken bij de tijd te krijgen. In dit geval gaat dat om de communicatie met de overheid. In de afgelopen twee decennia is onze telefoon veranderd van een spraakverbinding naar een gecompliceerde computer, waarmee we realtime verbonden zijn met oneindig veel bronnen van informatie, communicatie en vermaak. Met die digitale revolutie zijn grote kansen, maar ook grote risico's ontstaan. Het zijn risico's die we vooraf vaak nauwelijks konden inschatten. Het is dus een goede zaak dat de regering probeert om het wettelijke kader te moderniseren, ook in het licht van de kabinetsbrede Werkagenda Digitalisering.

Dit wetsvoorstel is ingediend in 2018. Inmiddels zijn we vierenhalf jaar verder. Voor de liefhebbers: dat was ten tijde van de iPhone 8, terwijl we nu bij nummer 14 zijn. In digitale termen is dat een eeuwigheid geleden. Theologen rekenen anders, maar dat terzijde.

In die vierenhalf jaar zijn er niet alleen allerlei technische ontwikkelingen geweest en parlementaire discussies gevoerd. Er zijn inmiddels ook nieuwe Europese regels, er is een novelle enzovoorts. De vraag is dan ook op z'n plaats of de wet die we vandaag behandelen nog wel up to date is.

De regering had er al voor gekozen om er een kaderwet van te maken. Dat leidde tot de nodige bezwaren, zowel bij de Raad van State als bij de Eerste Kamer. Zo'n kaderwet is wel praktisch en wendbaar, maar ook weinig ingevuld. Dat betekent dat er allerlei waarborgen ontbreken die juist nodig zijn vanwege de enorm toegenomen risico's.

Op een aantal punten brengt de novelle, die op basis van een eerste schriftelijke uitwisseling in deze Kamer is aangeboden, een wezenlijke verbetering aan. Zo wordt nu veel beter geregeld dat open source het uitgangspunt moet zijn, waardoor veel beter kan worden nagegaan hoe inloggegevens worden verwerkt. Dat geldt ook voor privacy by design. Naar aanleiding van de vraag hoe grote techbedrijven omgaan met persoonlijke gegevens, is veel explicieter gemaakt dat die niet verhandeld mogen worden. Ten slotte is per amendement op enkele onderdelen vastgelegd dat de Kamers mogen eisen dat die niet per AMvB maar per wet worden geregeld. Mijn fractie is absoluut blij met deze verbeteringen. Het is de vraag of het genoeg is.

Een aantal aspecten van het oorspronkelijke wetsvoorstel steunt mijn fractie zeker. Dat geldt voor het verplichten van bepaalde standaarden in het elektronisch verkeer van de overheid. Het geldt voor het stellen van regels over informatieveiligheid. Het geldt voor de verantwoordelijkheid voor het beheer van de voorzieningen en de diensten binnen de GDI, de Generieke Digitale Infrastructuur.

Een struikelblok zit bij de digitale toegang tot publieke dienstverlening. Dat is wat ons betreft het belangrijkste punt. In onze ogen is ten eerste een verkeerde afslag genomen. Ten tweede is het op het punt van de decentrale opslag niet goed geregeld. Over die decentrale opslag is al heel wat uitgewisseld. Volgens de regering is een systeem met centrale opslag niet riskanter dan een systeem met decentrale opslag. Want, zo zegt de regering bij de beantwoording van de vragen, bij hacken is er altijd een risico; je moet het gewoon goed beveiligen. Dat laatste is natuurlijk waar, maar de regering miskent daarmee dat het veel aantrekkelijker is om een centrale opslag te hacken en dat een hack daarbij veel ernstigere en grootschaligere gevolgen heeft. Ik vraag de staatssecretaris waarom ze niet ook op dat punt de gevraagde verbetering heeft aangebracht. Deskundigen zeggen dat dit echt veiliger is, niet alleen als het gaat om hacken, maar ook als het gaat om dataminimalisatie en privacy by design. Had die privacy by design, die nu wel in de novelle is verankerd, niet ook vertaald moeten zijn in decentrale opslag? Dat is toch heel nauw aan elkaar verbonden? Graag een reactie van de minister.

Het echt ingewikkelde punt is voor ons de verkeerde afslag. Die is ingrijpender en ook niet zo heel makkelijk te repareren, hoewel er misschien nog wel manieren zijn om dit met

elkaar op te lossen. Het meest fundamentele bezwaar tegen de Wet digitale overheid is wat ons betreft dat de regering ervoor gekozen heeft om ook private inlogmiddelen toe te staan voor communicatie met de overheid. In de argumentatie waarom dat een goed idee zou zijn, kom ik eerlijk gezegd niet veel verder dan dat er gezegd wordt: het is riskant als er maar één inlogmiddel is, zoals nu met DigiD; als dat inlogmiddel eruit ligt, is immers alle communicatie geblokkeerd. Dat klinkt in alle eerlijkheid als een drogreden. Ik vergelijk het maar even met bijvoorbeeld banken. Zij verstrekken ook inlogmiddelen en moeten daarbij de hoogste veiligheid in acht nemen. Met de redenering die de regering ons voorhoudt, zouden banken dus nooit genoegen kunnen nemen met alleen een eigen inlogmiddel, terwijl ze dat allemaal wel doen. Daarnaast zou de redenering van de regering alleen opgaan als we ervan uitgaan dat alle Nederlanders er vervolgens voor zorgen dat zij minstens twee inlogmiddelen tot hun beschikking hebben, zodat ze nog steeds uit de voeten kunnen als een van die twee vastloopt. Het argument lijkt ons tot nu toe dus een drogreden.

Er is een nog principiëlere vraag. Dat is of de overheid er niet gewoon zelf voor moet zorgen dat burgers en bedrijven toegang hebben tot overheidsdiensten en andere publieke diensten. Dat DigiD verouderd is, verbaast ons niet. Dat werd gelanceerd in 2003 en dat is toch echt een soort digitale prehistorie. Alle reden dus voor de overheid om een nieuw of op z'n minst een grondig vernieuwd inlogmiddel te laten ontwikkelen dat voldoet aan de eisen van deze tijd. Daar wordt nu in voorzien. Er blijft een publiek, door de rijksoverheid uitgegeven identificatiemiddel over. Dat maakt de vraag eigenlijk des te prangender: waarom worden überhaupt private identificatiemiddelen toegestaan? Welk nut dient het om de toegang tot overheidsdiensten uit handen te geven en vervolgens allerlei regels te moeten toevoegen om misbruik en externe risico's in te dammen? Die regels kunnen dan best oké zijn, maar waarom doen we dit überhaupt?

Voorzitter. We hebben op dit punt een sluitende argumentatie van de regering nodig. Als wij deze afslag nemen, is namelijk tot in lengte van dagen de deur opengezet voor allerlei private partijen. We zien de afgelopen jaren de publieke en de politieke opinie wat opschuiven. We vragen vaker of het wel zo goed is om private partijen hierin een rol te geven. Dat geldt zeker als je kijkt hoe bedrijven als Google, Facebook en noem ze allemaal maar op omgaan met gegevens van burgers. Stel dat we over een paar jaar bedenken dat het toch niet zo'n goed idee was om de deur op te zetten. Dan is die bijna niet meer te sluiten. Als het dan al zou lukken om alsnog te besluiten om private aanbieders weer buiten de deur te houden, dan zal dat mogelijk leiden tot schadeclaims van bedrijven die geïnvesteerd hebben om dit te kunnen aanbieden. Kortom, als we nu de deur openzetten, gebeurt er iets groots. Alle reden om deze principiële vraag heel erg goed onder de loep te nemen.

Wij denken dat we daarbij niet naïef moeten zijn. Er zullen zeker private aanbieders komen die vanuit ideële motieven een inlogmiddel ontwikkelen met maximale privacy, dataminimalisatie, veiligheid en wat allemaal niet meer. Dat zullen modellen of inlogmiddelen zijn waar je als overheid misschien wel blij mee bent en waar kritische burgers blij mee zijn. Er zullen ook private aanbieders zijn met geen ander doel dan winst maken en/of het vergaren van persoonsgebonden informatie. Aanbieders met een van die laatste twee oogmerken zouden we toch echt buiten de deur moeten houden. Is de staatssecretaris er zeker van dat de private aanbieders niet slimmer zijn dan de wetgever? Zijn we er zeker van dat private aanbieders geen slimme manieren vinden om toch te bereiken wat zij graag willen, namelijk winst op data? Is de staatssecretaris ervan overtuigd, ook met alle waarborgen die nu zijn aangebracht, dat de private aanbieders op geen enkele wijze indirect informatie over gebruikers kunnen verzamelen waarmee zij hun voordeel kunnen en zullen doen?

Ik heb de neiging om de staatssecretaris een klein beetje te waarschuwen. Het kan politiek aantrekkelijk zijn om nu ja te zeggen. Om te zeggen: ja, ik ben daar zeker van; we hebben goede waarborgen; kijk maar naar alle voorwaarden die erin staan. Eerlijk gezegd zou dat ja wat mij betreft ongeloofwaardig zijn. Want hoe slim wij het ook regelen, het gevaar blijft altijd bestaan dat private aanbieders net iets slimmer zijn en net iets bedenken waardoor zij binnen de grenzen van de wet toch informatie over gebruikers vergaren en gebruiken. Of misschien doen zij dit net buiten de wet. Kijk naar de boetes die grote techbedrijven af en toe krijgen. De winsten die zij maken zijn zo veel groter dan die boetes, dat ze die boetes op de koop toe nemen. Hoe slim wij het ook doen, het gevaar blijft bestaan.

Is de staatssecretaris het met mijn fractie eens dat de digitale sluwheid van private aanbieders nooit en te nimmer onderschat mag worden? Deelt zij dan ook de conclusie dat het toelaten van private aanbieders per definitie risico's met zich meebrengt? Vindt zij het nog steeds een goed en noodzakelijk idee, zoals 4,5 jaar geleden misschien gevonden werd, om private aanbieders toe te laten op deze markt?

De heer **Koole** (PvdA):
Het betoog van de heer Ganzevoort kan ik helemaal volgen. Ik ben het er ook zeer mee eens. Ik heb wel een vraag over de private aanbieders. We moeten kijken of we vandaag toch nog een paar stappen kunnen zetten om eruit te komen. Mijn vraag aan de heer Ganzevoort is of er ook onderscheid te maken is tussen private aanbieders die commerciële belangen hebben en nastreven, en non-profit private aanbieders die ideëel — de heer Ganzevoort gebruikte zelf al de term "ideële organisaties" — inlogmiddelen ontwikkelen. Is dat een mogelijk behulpzaam onderscheid?

De heer **Ganzevoort** (GroenLinks):
Dank aan de heer Koole voor deze vraag. Ja, dat is een behulpzaam onderscheid, maar ik denk dat het juridisch niet goed te maken valt. Op welke basis zou je die twee kunnen onderscheiden? Ik denk wel dat je de vraag kunt stellen of er bij de inlogmiddelen die ontwikkeld worden geen modellen zitten die je als overheid heel graag zou willen gaan gebruiken. Dat zijn eigenlijk twee verschillende dingen. Het eerste is: welk type middelen gebruik je; welke technische oplossing kies je? Zijn er dan bijvoorbeeld aanbieders, zoals die er eerder waren, die met attribuutgebonden informatie een oplossing bieden voor heel veel van de vragen waar we voor staan? Het tweede is: vind je dan dat dit door een private aanbieder zou moeten worden geregeld? Of vind je dat dit eigenlijk zou moeten worden overgenomen door de overheid, waarmee het dan het publieke inlogmiddel wordt? Dat zijn volgens mij twee onderscheiden vragen.

Je kunt dus onderscheid maken tussen middelen die beter werken en middelen die minder goed werken. De ideële zullen waarschijnlijk beter werken op de criteria die ik noemde. Maar dan nog blijft de vraag of het meest heldere criterium, dat je ook juridisch hard kunt maken, niet bij de publieke aanbieder — dat wil zeggen bij de overheid — gehouden zou moeten worden en niet bij een private aanbieder.

De heer **Koole** (PvdA):
Ik begrijp dat de heer Ganzevoort het volgende zegt. Bij de ideële aanbieders zit waarschijnlijk een hele hoop knowhow en kennis waarvan de overheid zou kunnen profiteren. Dat kun je op twee manieren doen. De ene methode is om uitsluitend de private aanbieders met een non-profit businessmodel toe te laten, waarbij je ook een juridisch onderscheid moet kunnen maken, als dat gemaakt kan worden. Dat is de ene methode. De andere methode is: laat ze vooral hun werk doen, en als daar een goed project uit komt, dan moet de overheid dat gewoon aankopen, waardoor ze eigenaar wordt van dat project. Is dat het onderscheid dat de heer Ganzevoort voor ogen heeft?

De heer **Ganzevoort** (GroenLinks):
Dat laatste zou een heel goede route kunnen zijn. Bij het eerste zeggen wij: kun je dat onderscheid echt maken? Ik kan proberen om het slechte te bedenken — ik denk dat het kan helpen als we ook nadenken over waar het fout zou kunnen gaan. Stel dat ik zo'n privaat bedrijf ben dat graag data et cetera wil. Als dan de voorwaarde is dat ik een ideële afdeling moet oprichten om hieraan mee te mogen doen, dan zou ik alles op alles zetten om dat voor elkaar te krijgen. Dus ik weet niet of het onderscheid profit/non-profit ons nou helpt om de deur goed op slot te houden. Als er een ideële aanbieder is, die dit echt doet omdat hij ervan overtuigd is dat je deze communicatie veilig enzovoort moet doen, dan denk ik dat hij zeer vereerd zou zijn met een overheid die zegt: dat is nou eens een goed middel, daar zouden we graag mee willen samenwerken, dat zouden we graag willen overnemen en daarvoor betalen.

De **voorzitter**:
Vervolgt u uw betoog.

De heer **Ganzevoort** (GroenLinks):
De belangrijkste vraag aan de staatssecretaris is: kan zij ons overtuigen? Is zij er zeker van dat wij het op deze manier veilig houden? En als dat niet zo is, wat zijn dan de manieren — want er zit veel goeds in de wet — om deze angel eruit te halen en nog eens goed na te denken over de vraag of dit wel echt de goede afslag is? De fractie van GroenLinks geeft de staatssecretaris graag de kans om haar ervan te overtuigen dat deze route, met private aanbieders, het beste is voor de Nederlandse burgers. Wij hebben die overtuiging nog niet en dit punt weegt voor ons zwaar. Kortom, we zijn nog benieuwder dan anders naar de antwoorden van de staatssecretaris.

De **voorzitter**:
Dank u wel, meneer Ganzevoort. Dan is het woord aan mevrouw Prins namens het CDA.

Mevrouw **Prins** (CDA):
Meneer de voorzitter. Als eerste wil ik graag vermelden dat deze wet niet alleen burgers raakt — dus ook mij en ons allemaal — maar ook twee organisaties waar ik bij betrokken ben: als voorzitter van de raad van bestuur van de Kamer van Koophandel en als lid van de raad van commissarissen bij zorgverzekeraar CZ. Dit even voor de helderheid.

Dit gezegd zijnde, nu over naar de Wet digitale overheid zelf. Digitaal communiceren, digitaal informatie uitwisselen en zakendoen was en is voor veel Nederlanders al de gewoonste zaak van de wereld en dat heeft nog een extra groei doorgemaakt tijdens de coronacrisis. We staan al jaren in de top vijf van internetsnelheid in Europa en wij kopen meer dan gemiddeld op internet. Het is dan ook meer dan terecht dat de regering al in een vorig regeerakkoord heeft aangegeven dat ook het elektronisch zakendoen met de overheid veilig, toegankelijk en betrouwbaar moet zijn. Dit heeft in 2018 geleid tot de voorliggende wet. Een wet die enerzijds tot doel heeft te zorgen voor standaardisatie van de elektronische infrastructuur van de publieke sector en anderzijds voor een veilige toegang tot en controle van de elektronische dienstverlening van de publieke en semi-publieke sector, zoals de pensioenfondsen en de zorg, door ook inlogmiddelen van private aanbieders toe te staan. Dit laatste mede daar het huidige DigiD niet kan voldoen aan de hoogste betrouwbaarheidsniveaus.

Voorzitter. De CDA-fractie is positief over deze wet, nu deze dankzij een novelle in onze ogen ook daadwerkelijk invulling geeft aan beide doelstellingen. Sterker nog, gezien de vele ontwikkelingen in de digitale wereld en het aandeel burgers en bedrijven dat de voorkeur geeft aan elektronische dienstverlening, is deze wet in onze ogen eerder te laat dan te vroeg. In dat opzicht kijken wij ook met belangstelling uit naar de opvolger van deze wet, met name naar de verbetering van de persoonlijke informatiepositie van de burgers — oftewel: hoe heeft de burger regie op z'n eigen gegevens? — en naar een door de overheid gevalideerde online-identiteit die publiek en privaat bruikbaar is. Kan de staatssecretaris aangeven wanneer WDO-2 het licht ziet?

Voorzitter. Het standaardiseren van de elektronische dienstverlening van de overheid in de vorm van een generieke digitale infrastructuur vinden wij een groot goed. Enerzijds omdat dit technisch gesproken praktischer is en minder kans op fouten geeft, anderzijds omdat de burgers op deze wijze gekend worden door de overheid. De CDA-fractie is ook verheugd dat via deze wet de website van de overheid moet voldoen aan de eisen van goede toegankelijkheid voor mensen met een beperking. In dat kader zij wel opgemerkt dat wij het van belang vinden dat digitaal zakendoen met de overheid een recht is en geen plicht. Immers, zo'n 4 miljoen burgers zijn niet digitaal vaardig of geven de voorkeur aan menselijk contact. De Informatiepunten Digitale Overheid, vaak gevestigd in bibliotheken, voorzien dus in een grote behoefte. Afgelopen week hebben zij niet voor niks de Good Practice Award van de Rijksbrede Benchmark Groep gekregen, dat een leernetwerk is van publieke uitvoeringsorganisaties. Graag ontvangen wij een duidelijke toezegging van het kabinet dat deze informatiepunten ondersteund blijven.

Voorzitter. Dankzij de novelle is er nu een helder wettelijk kader waaraan inlogmiddelen voor de publieke sector

moeten voldoen. Onze fractie hecht eraan dat privacy by design, open source, het expliciete verbod op het verhandelen van de gegevens, inclusief het inzicht in de desbetreffende businesscase, en een actief toezicht door het Agentschap Telecom in de wet zijn opgenomen.

Wel zijn er nog enkele vragen. De staatssecretaris geeft aan dat er een geleidelijke overgang van closed source naar open source zal plaatsvinden. Welke acties onderneemt de regering om vaart te houden in dit proces? Hoe zorgt zij ervoor dat de ontwikkeling van het publieke middel DigiD minimaal gelijke tred houdt met de ontwikkelingen in de markt en niet voor vertraging zorgt in dit proces? Heeft de staatssecretaris een einddatum voor ogen waar naartoe gewerkt moet worden? Immers, ervaring leert dat dit de zaken goed op stoom houdt.

Deze wet beoogt dat straks diverse private aanbieders naast DigiD hun inlogmiddelen aanbieden aan de burger. Heeft de staatssecretaris zicht op de mate van belangstelling van de private aanbieders? In hoeverre kunnen zij concurreren met het, zo hebben wij begrepen, gratis inlogmiddel DigiD? Waarom zouden private aanbieders, gezien de terechte wettelijke kaders en beperkingen, deze markt willen betreden? Is er sprake van een level playing field tussen de publieke en private aanbieders? Gaat de praktijk daadwerkelijk invulling geven aan de doelstelling van deze wet?

Ten aanzien van de consequenties voor de burgers hebben we nog diverse vragen. De burgers vertrouwen nu op hun DigiD. Intussen blijkt dat de huidige DigiD niet kan voldoen aan de zwaardere betrouwbaarheidsniveaus. Voor het betrouwbaarheidsniveau "hoog" is straks een applet, een speciale functionaliteit, nodig op het rijbewijs of de Nederlandse identiteitskaart, waarvoor de burger ook extra leges moet betalen. In de uitvoering van deze wet moeten ten aanzien van de burgers nog diverse stappen gezet worden. Ik noem er enkele. De burger informeren dat in relatie met de digitale overheid en de semipublieke sector er sprake is van diverse betrouwbaarheidsniveaus bij het inloggen. Helder maken dat digitaal communiceren en zakendoen met de overheid en de semipublieke sector mogelijk is via diverse inlogmiddelen. Duidelijk maken welke inlogmiddelen door de overheid zijn toegelaten na een strenge screening. Komt er bijvoorbeeld een keurmerk? Wat te doen bij de introductie van nieuwe hoog betrouwbare inlogmiddelen terwijl je rijbewijs nog geldig is en je graag wel via een hoog betrouwbaar inlogmiddel wil communiceren met je zorgaanbieder? Hoelang blijven de uitvoeringsorganisaties, gemeenten en andere aanbieders nog de bestaande DigiD accepteren?

Voorzitter. In het kader van uitvoerbaarheid en handhaafbaarheid zijn er juist nog veel meer vragen te stellen. Voor ons is van belang dat juist waar het de veiligheid van soms zeer persoonlijke gegevens betreft, de overheid zich niet alleen door de inhoud van de wet, maar juist ook door een zorgvuldige en transparante aanpak van de uitvoering en heldere voorlichting betrouwbaar toont. Graag een uitgebreide reactie van de staatssecretaris in dezen.

Overigens, stevig toezicht hoort daar ook bij. De staatssecretaris heeft aangegeven dat het Agentschap Telecom dit toezicht gaat verzorgen. Graag ontvangen wij een bevestiging dat het Agentschap Telecom niet alleen de juiste digitale kennis heeft, maar ook in deze krappe arbeidsmarkt genoeg medewerkers heeft om niet alleen bij de ingang van de wet, maar juist ook de komende jaren alert en proactief toezicht te houden.

Voorzitter. Nog een enkele vraag aan de regering inzake de aanbieders van de inlogmiddelen. De aanbieders van inlogmiddelen dienen minimaal 60 uur per week telefonisch bereikbaar te zijn voor hun klanten. Wordt zowel bij de toelating als bij het toezicht niet alleen getoetst op deze meetbare 60 uren, maar juist ook op de contactuele kennis en vaardigheden van de medewerkers van de aanbieders? Zijn zij erop getraind om antwoorden te geven aan mensen die geen digitaal expert zijn?

Een andere vraag betreft het mogelijk stoppen met het aanbieden van een privaat inlogmiddel. Aangegeven is dat de minister van een zogenaamde "stopper" kan verlangen dat hij nog enige maanden het gebruik van zijn inlogmiddel mogelijk maakt. Hoe werkt dat bij een mogelijk faillissement van een aanbieder van een inlogmiddel?

Meneer de voorzitter. De CDA-fractie is benieuwd naar de antwoorden op onze vragen.

De heer **Ganzevoort** (GroenLinks):
Mevrouw Prins stelt een aantal heel terechte vragen over de uitvoering en dergelijke. Ik was heel erg benieuwd naar de visie van de CDA-fractie op de principiële wenselijkheid van private aanbieders.

Mevrouw **Prins** (CDA):
Dat is een hele terechte en logische vraag. Daar kun je vragen over stellen. Ik vind het wel begrijpelijk dat de overheid daarvoor gekozen heeft, ervan uitgaande dat men niet meer afhankelijk wil zijn van één inlogmiddel. Dat begrijp ik, want er kunnen overal storingen zijn. Naarmate de digitale contacten met de overheid en de semipublieke sector intenser worden, is het ook wel risicovol om slechts van één inlogmiddel afhankelijk te zijn.

De heer **Ganzevoort** (GroenLinks):
Maar dat zou dan betekenen dat alle burgers twee inlogmiddelen moeten hebben.

Mevrouw **Prins** (CDA):
Ik denk dat we die kant opgaan, in ieder geval dat dat aanbod er is of dat men op dat moment alsnog kan overstappen. Ik begrijp die filosofie en die visie, maar dan is het wel nodig — dat is de andere kant — dat er een helder plan van aanpak ten grondslag ligt aan de voorlichting en de communicatie.

De **voorzitter**:
Tot slot, meneer Ganzevoort.

De heer **Ganzevoort** (GroenLinks):
Ik had zelf nog niet gelezen in de stukken dat alle burgers twee of meer middelen moeten hebben om zeker te zijn. Dat maakt de vraag naar hoe je daarover communiceert alleen maar ingewikkelder: beste burger, zeker als u niet digitaal vaardig bent, word dat maar wel want u heeft twee inlogmiddelen nodig.

Mevrouw **Prins** (CDA):
Ik denk dat je daar volgende stappen voor moet zetten en dat je dat geleidelijk zult moeten doen. Alleen, als we daadwerkelijk willen dat dit gaat werken, zullen er zelfs mensen zijn met drie of vier inlogmiddelen. Dat is dan hun eigen keuze. Maar wij hebben er alle begrip voor dat je niet afhankelijk wil zijn van één middel.

Mevrouw **Gerkens** (SP):
Maar dat heeft nog verdere consequenties, want je logt in bij een ander systeem, en dat systeem kan ook storingen hebben. Betekent dat dat we al die databases waaruit de informatie wordt gehaald dan ook twee, drie, vier keer moeten hebben met verschillende systemen om ervoor te zorgen dat als het ene niet werkt, het andere dan kan werken? Hoever wil mevrouw Prins dit doortrekken?

Mevrouw **Prins** (CDA):
Ik wil dat helemaal niet verder doortrekken naar de databases, want ik vind dat de verantwoordelijkheid van de uitvoeringsinstanties, van de zorg of van de pensioenfondsen. Daar gaat het nu niet om in deze wet. Het gaat erom dat die organisaties ervoor zorgen dat men via verschillende inlogmiddelen daadwerkelijk bij de gewenste gegevens kan komen.

Mevrouw **Gerkens** (SP):
Ik begrijp dat mevrouw Prins niet over de pensioenfondsen of de zorginstellingen gaat, maar wij gaan bijvoorbeeld wel over de Belastingdienst, om er maar een te noemen, of over andere centrale databases waar wij als overheid informatie leveren aan de burger. Vindt mevrouw Prins dat ook die systemen verdrievoudigd, verviervoudigd zullen moeten worden in diverse uitvoeringen om ervoor te zorgen dat ze in ieder geval robuust zijn en dat we bij storingen kunnen overgaan op een ander systeem? Ik voorzie daar wel wat problemen in, zeg ik u alvast. Daarom stel ik die vraag, mevrouw Prins.

Mevrouw **Prins** (CDA):
Ik zie dat duidelijk anders. Het gaat alleen om het inlogmiddel, niet om de database zelf. We hebben dus niet meerdere systemen nodig. Het gaat erom dat er meerdere deurtjes zijn waardoor je in die database kan komen, om het maar even heel plastisch uit te drukken.

De **voorzitter**:
Mevrouw Gerkens, tot slot.

Mevrouw **Gerkens** (SP):
Maar dan constateer ik toch een inconsistentie. Mevrouw Prins zegt: we moeten wel toegang hebben en meerdere keuzes hebben, meerdere deuren om binnen te komen. Maar ja, als dan de deur aan de andere kant dicht is, dan maakt dat uit niet. Dan gaat ook het argument dat we meerdere deuren moeten hebben niet op. Ik zou mevrouw Prins toch nog eens willen vragen om te kijken naar die inconsistentie in haar argumentatie.

Mevrouw **Prins** (CDA):
Ik zie die inconsequentie niet. Ook nu kun je bij een aantal andere bedrijven via verschillende inlogmiddelen binnenkomen. Dat zegt niks over de database zelf. Ik zie dat dus niet. Je hebt soms de voordeur en soms de achterdeur.

De **voorzitter**:
Dank u wel. Dan is het woord aan de heer Van den Berg namens de VVD-fractie.

De heer **Van den Berg** (VVD):
Dank u wel, voorzitter. Onze samenleving ontwikkelt en digitaliseert in hoog tempo en dat is maar goed ook. Waar het twintig jaar geleden nog heel normaal was om je bankzaken te doen via een acceptgiro, doen velen van ons dit sinds enkele jaren via de mobiele telefoon of met hun slimme horloge. Digitalisering dwingt ons om nieuwe technologieën in de gaten te blijven houden en de wet te blijven toetsen op zijn kwaliteit en toepasbaarheid in de digitale samenleving. Hoe die digitale samenleving er in de toekomst precies uit zal gaan zien, mag nog ongewis zijn, maar het is duidelijk dat onze toekomstige vrijheid, veiligheid en welvaart voor een aanzienlijk deel zullen afhangen van de mate waarin we voorbereid zijn op, en ons kunnen aanpassen aan de digitale werkelijkheid.

De overheid die digitaal in contact staat met burgers, en daarmee ook digitale diensten verleent, moet de identiteit van die burgers goed kunnen vaststellen. Digitale identiteitscontrole is een stuk ingewikkelder dan wanneer dit face to face gebeurt, maar is daarom niet minder noodzakelijk. Om veilig, betrouwbaar en toegankelijk te kunnen communiceren met de overheid, wordt er bijvoorbeeld al jarenlang gebruikgemaakt van DigiD. Dit kan alleen nóg veiliger, nóg betrouwbaarder en nóg toegankelijker. Deze Wet digitale overheid regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de overheid en semioverheid. Burgers krijgen elektronische identificatiemiddelen die een stuk betrouwbaarder zijn dan het huidige DigiD.

Daarnaast beoogt deze wet een gelijker speelveld te creëren voor Nederlandse aanbieders van digitale inlogmiddelen ten opzichte van hun buitenlandse concurrenten. In veel andere Europese landen is vergelijkbare wetgeving al van kracht, waardoor ontwikkelaars uit die landen een voorsprong hebben. Deze bedrijven hebben al een trackrecord opgebouwd met hun producten, en breiden hun markt en hun marktaandeel gestaag uit, terwijl onze bedrijven nog op deze markttoegang zitten te wachten. Dat is onwenselijk.

Bij de behandeling van het oorspronkelijke wetsvoorstel — die was vóór mijn tijd — was de Eerste Kamer terecht zeer kritisch op een aantal privacywaarborgen. De staatssecretaris heeft de wet daar nu op aangepast en die aanpassingen zijn door mijn fractie met instemming ontvangen.

Voorzitter. Wat betreft de novelle is onder de AVG en de eIDAS-verordening het principe van privacy by design eigenlijk al leidend. Toch is het goed dat de staatssecretaris het principe nu heeft aangescherpt in deze wet. Zo weten we zeker dat er bij het ontwerpen van een informatiesysteem of nieuw product in beginsel al rekening wordt

gehouden met iemands privacy. Persoonsgegevens van burgers zijn de meest privacygevoelige gegevens. Deze worden nu extra beschermd in deze wet.

Ook is mijn fractie er tevreden over dat het verbod op het verhandelen van gebruikersgegevens nu in de wet is verankerd. De organisatie die het identificatiemiddel maakt, moet aannemelijk maken dat er geen inkomsten worden verkregen uit het verhandelen of verstrekken van gebruikersgegevens. Zo zorgen we er als wetgever voor dat de gegevens van gebruikers niet verhandeld worden.

Voorzitter. De leden van de VVD-fractie zien de WDO als onderdeel van een nieuwe tranche aan digitaliseringswetgeving die hard nodig is. En we zien de wet als een goede stap in de richting van een beter werkende digitale overheid. Iedere ingezetene van Nederland, maar met name zzp'ers en kleinere ondernemers — daar hebben we er gelukkig veel van in dit land — hebben veel te winnen bij een beter werkende digitale overheid.

Toch heeft de VVD ook zorgen bij dit wetsvoorstel, specifiek rondom de uitwerking van de opensourcemethode. Het open karakter van de broncode van de software maakt de digitale inlogmiddelen die met deze wet geregeld worden in zekere zin transparant, en draagt eraan bij dat meerdere slimme ontwikkelaars zorg kunnen dragen voor de kwaliteit en veiligheid van de producten, want ontwikkelaars van over de hele wereld kunnen meekijken in de broncode van de software en kunnen daarmee helpen deze te verbeteren. Door aan te geven waar de zwakke punten liggen, wordt de software waarschijnlijk veiliger. Dat is nuttig, want samen ben je slimmer. Daarnaast creëer je een situatie waarin de rijksoverheid niet afhankelijk wordt van één of een klein aantal softwareleveranciers, maar van een community van developers, zoals de staatssecretaris heeft aangegeven.

Toch is het werken met opensourcecodes lang niet zaligmakend in zichzelf. Ik doel hierbij op het risico dat de gemeenschap van ontwikkelaars niet groot genoeg is of van onvoldoende kwaliteit, of dat de community voor een deel zal bestaan uit developers die helemaal niet het beste voor hebben met Nederland of met de privacy en veiligheid van Nederlanders, van u en van mij. Deze kwaadwillende ontwikkelaars kunnen in de broncode zien waar mogelijk zwakke punten van de software liggen zonder dat deze verbeterd worden, waardoor de Nederlandse overheid en haar burgers risico's lopen.

Voorzitter. Doordat de mate van veiligheid van open source uiteindelijk afhankelijk is van de sterkte, activiteit en omvang van de vrijwilligersgemeenschap van ontwikkelaars, is het succes ervan niet automatisch gegarandeerd.

De heer **Ganzevoort** (GroenLinks):
Dat is een mooi woord, "gegarandeerd". Goed om dat nog te horen. Want daar gaat precies mijn vraag over. Er zijn kwaadwillende ontwikkelaars. Zijn die er bij closed source dan ook?

De heer **Van den Berg** (VVD):
Bij closed source is er minder risico. Althans, bij closed source verlaat je je minder op het feit dat er externen zijn die aan de bel zullen trekken en met elkaar tot verbeteringen komen. Daarin zit naar mijn beeld het grotere risico.

De heer **Ganzevoort** (GroenLinks):
Ik vraag dit omdat de heer Van den Berg een warm pleidooi houdt voor het bedrijfsleven dat zich zou moeten kunnen ontwikkelen en de markt op zou moeten kunnen en dergelijke. Op dat punt hoor ik geen enkele aarzeling bij mogelijk kwaadwillende aanbieders. Waarom is die er dan opeens wel bij open source?

De heer **Van den Berg** (VVD):
Waar het onze fractie om gaat, is dat wij aan de ene kant zo veel mogelijk gebruik willen maken van en zo veel mogelijk baat willen hebben bij de veelheid aan mogelijke aanbieders. We willen zo veel mogelijk gebruikmaken van de innovatiekracht, die in grotere mate bij private aanbieders ligt dan die er bij de overheid zou liggen. Tegelijkertijd proberen we er aan de achterkant voor te zorgen — dat zult u in het vervolg van mijn betoog ook horen — dat de overheid daar zo goed mogelijke garanties voor inbouwt. Dus ja, in beide gevallen zijn er risico's. Alleen, in het ene geval zijn de risico's naar ons idee groter en moeten we die proberen goed binnen de perken te houden en daar goede waarborgen voor in te bouwen.

De **voorzitter**:
Tot slot, meneer Ganzevoort.

De heer **Ganzevoort** (GroenLinks):
Nu klinkt het alsof de heer Van den Berg zegt: ik zie de risico's vooral aan de opensourcekant. Maar als we helemaal niet weten wat hun sourcecode is en we helemaal niet weten welke motieven ze hebben, dan willen we ze wel toelaten. Ik hoop dat de heer Van der Berg daar in zijn nadere betoog op ingaat, want dat lijkt me erg spannend.

De heer **Van den Berg** (VVD):
Ik wil daar wel direct op ingaan. Natuurlijk is het niet zo dat je bij closed source alle risico's of mogelijk problemen kunt uitsluiten. Wij zien dat je door private aanbieders wel toe te staan, voordelen binnen kunt halen, maar dat de risico's daar tegelijkertijd mee toenemen. Die moet je door middel van goede waarborgen zien te minimaliseren.

Mevrouw **Gerkens** (SP):
Sterker nog, met closed source kun je per definitie niet zien of er kwaadwillende programmeeractiviteiten hebben plaatsgevonden. Dat is mijn vraag. Het lijkt erop dat de heer Van den Berg zegt: je hebt ontwikkelaars die open source ontwikkelen en je hebt ontwikkelaars die closed source ontwikkelen. Heb ik dat goed begrepen?

De heer **Van den Berg** (VVD):
Ja, ik denk dat je inderdaad ontwikkelaars hebt die closed source ontwikkelen en ontwikkelaars die open source ontwikkelen. Althans, in een situatie waarin je open source hebt — dat is eigenlijk de kern van mijn betoog hier — en je daar gebruik van maakt, vertrouw je erop dat er een gemeenschap van ontwikkelaars op vrijwillige basis meekijkt, de zwakheden identificeert en met oplossingen daarvoor komt. We zeggen: daarmee maak je je eigenlijk afhankelijk van een community. Is die community altijd van

de kwaliteit, de omvang en de permanentie die je zou willen?

Mevrouw **Gerkens** (SP):
Ik denk dat de vragen rondom een stevige community terecht zijn. Daar heeft de staatssecretaris volgens mij ook aandacht aan besteed in de beantwoording. Maar mijn punt is niet of er specifiek opensource- of closedsourceontwikkelaars meekijken. Het gaat erom of je de broncode hebt gepubliceerd of niet. Zodra de broncode is gepubliceerd, kan de hele goegemeente, iedereen, meekijken, vrijwillig of niet. Ik kan de heer Van den Berg verzekeren dat het onder coders zo ongeveer een hobby is om te kijken naar codes. Er zijn genoeg mensen die dan onmiddellijk gaan kijken of daar kwetsbaarheden in zijn, dus men hoeft er niet bezorgd over te zijn of er voldoende opensource- of closedsourceontwikkelaars zijn. Zodra de broncode gepubliceerd is, kan iedereen meekijken en zijn er dus voldoende mensen die de kwetsbaarheden kunnen ontdekken. Bij closed source is dat niet zo.

De heer **Van den Berg** (VVD):
Mevrouw Gerkens geeft aan dat je die garantie hebt over de kwaliteit en de omvang van die community. Daar heb ik nog een aantal vragen over.

Ik vervolg mijn betoog dus eigenlijk precies op het punt waar we met de interrupties bij geëindigd zijn. Alleen als de gemeenschap groot genoeg is en bestaat uit goedwillende ontwikkelaars, wordt de software nog veiliger. Maar indien die gemeenschap niet groot genoeg blijkt of wanneer de community een ander belang dient dan het algemeen belang, wordt de opensourcemethode geen veiligheidsmaatregel meer, maar wordt die methode misschien een veiligheidsrisico. Het doel van dit wetsvoorstel is het creëren van een veiligere, betrouwbaardere en toegankelijkere digitale omgeving voor burgers. Daarom hechten de leden van de VVD-fractie eraan dat we in dit debat helder krijgen hoe de staatssecretaris van plan is om ervoor te zorgen dat de gemeenschap van ontwikkelaars die zich rondom de software ophoudt, inderdaad waarborgt dat de producten die zo veel gevoelige informatie bevatten, veilig en van hoge kwaliteit blijven. De staatssecretaris schrijft dat het er "in de kern om gaat dat de software veilig is, onderhouden wordt, en beschikbaar is en blijft", maar hoe zij van plan is om dat te waarborgen, is voor mijn fractie nog onvoldoende duidelijk.

Voorzitter. De staatssecretaris gaf schriftelijk aan te willen stimuleren dat de gemeenschap achter de open source groot genoeg is en blijft. Hoe en in welke mate deze stimulering nodig is, wil de staatssecretaris bezien in het licht van de ontwikkelingen. Dat vindt mijn fractie te vaag en te vrijblijvend, want als we de afgelopen tijd iets geleerd hebben, dan is het wel dat die veiligheid niet iets statisch is, maar een proces is. Wat vandaag veilig is, hoeft niet overmorgen nog steeds veilig te zijn. Het is daarom essentieel dat de veiligheidseisen ook procedures omvatten voor het geval dat er een gat in de code zit of een hack is, en ter voorkoming daarvan. Daarom is het noodzakelijk dat er altijd een organisatie verantwoordelijk is voor de goede werking van het middel en de veiligheid.

De heer **Van Hattem** (PVV):
De heer Van den Berg stelt op zich een aantal terechte vragen op het vlak van de opensourcecommunity, maar het punt is nu juist als volgt. Draai het even om. De kritiek die ook in de opmerking van de heer Van den Berg zit, is dat de opensourcecommunity ook kwetsbaarheden kent en dat er kwaadwillenden in actief kunnen zijn. Maar aanbieders van closedsourcesoftware kunnen evengoed kwaadwillend zijn. Daar kan ook de lange arm van China in zitten, waar de NCTV vandaag bijvoorbeeld nog voor gewaarschuwd heeft. Dus hoe ziet de heer Van den Berg van de VVD het voor zich dat dit bij zulk soort aanbieders wel uitgesloten kan worden?

De heer **Van den Berg** (VVD):
In reactie op de vraag van de heer Van Hattem, eigenlijk een andere formulering van de vraag die mevrouw Gerkens al eerder stelde: mijn betoog moet niet opgevat worden als een afwijzing van de opensourcemethode als zodanig of als een pleidooi voor closed source. Ik denk dat het werken met open source als zodanig een goede stap zou zijn, maar ik wil er ook voor pleiten of de staatssecretaris uitnodigen om duidelijker te maken hoe zij bij gebruikmaking van de opensourcemethode toch wil garanderen of in elk geval wil stimuleren, zoals zij schrijft, dat de community die daarop toeziet, van hoge kwaliteit is en dat je daar nog enige sturing op zou kunnen hebben. Daar richt mijn vraag zich op.

De heer **Van Hattem** (PVV):
Op dat punt is de vraag zeker terecht, zoals ik al aangaf. Maar de heer Van den Berg gaf eigenlijk ook aan dat er een situatie zou kunnen zijn waarin je werkt met closed source, eigenlijk met daarin de aanname dat dat toch veiliger zou kunnen zijn. Wil de heer Van den Berg hier nu toch pleiten voor het openhouden van de mogelijkheid van die closedsourcecommunity of zegt hij duidelijk dat we dat echt niet moeten willen en dat we echt voluit voor die opensourceoplossingen gaan?

De heer **Van den Berg** (VVD):
Mijn pleidooi moet niet opgevat worden als een afwijzing van open source als zodanig, maar ik wil er wel voor waken om te denken dat bij gebruikmaking van open source de veiligheid, de betrouwbaarheid en de kwaliteit automatisch verbeteren. Ook dan moet je waarborgen inbouwen om te kijken hoe al die veronderstellingen die bij open source horen, ook in de praktijk geborgd kunnen zijn.

Voorzitter. Daarom zouden de leden van de VVD-fractie de staatssecretaris graag het volgende willen vragen. Aan welke voorwaarden moet een groep ontwikkelaars in de ogen van de staatssecretaris voldoen om als een volwaardige gemeenschap te worden gezien? Hoe is de staatssecretaris concreet van plan te stimuleren dat een goed functionerende gemeenschap van ontwikkelaars ontstaat? De leden van de VVD-fractie zouden graag een verduidelijking krijgen van hoe de staatssecretaris dit van plan is en wat haar plannen zijn indien deze gemeenschap in de toekomst niet meer aan de vereisten zal voldoen. Op welke manieren is zij dan van plan te garanderen dat de inlogmiddelen waarover wij spreken veilig en van hoge kwaliteit blijven? Wie is uiteindelijk eindverantwoordelijk indien de opensourcemethode niet naar behoren blijkt te werken? Is dit de rijks-

overheid of is dit de betreffende softwareleverancier? Hoe gaat de staatssecretaris deze verantwoordelijkheid juridisch regelen?

En dan mijn laatste vraag. Kan de staatssecretaris de ministeriële regeling verder aanscherpen en hierbij aansluiten bij bijvoorbeeld breder gehanteerde vereisten vanuit de eIDAS-verordening en invulling in de Europese standaarden van ETSI, waarmee een hoog niveau van veiligheid kan worden behaald?

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Van den Berg. De heer Koole.

De heer **Koole** (PvdA):
Ik dank de heer Van den Berg voor zijn betoog. Ik dacht dat hij nog even op het punt van het toezicht zou komen, maar dat deed hij niet. Ik heb daar een vraag over. Hij zei in het begin dat hij zeer ingenomen was met het in de novelle opnemen van het handelsverbod op gegevens. Ik ben het met hem eens dat het heel goed is dat dit handelsverbod er is, maar hoe kun je dat nou op een adequate manier controleren? Want als private organisaties de beschikking krijgen over gegevens van burgers is het één ding om het juridisch te verbieden, maar een tweede om het te handhaven. Ziet de heer Van den Berg daarvoor voldoende adequate handhavings- en controlemiddelen opgenomen in deze wet?

De heer **Van den Berg** (VVD):
Ja, ik ben inderdaad ingegaan op het toezicht op de opensourcecommunity, om het zo maar te zeggen, en minder of niet op het toezicht op het verhandelverbod. Daar zijn natuurlijk ook vragen over gesteld en daar is in het verband van deze wet eigenlijk sinds 2018 over gediscussieerd. Wij zijn inderdaad blij met het toevoegen of verder expliciteren van het verhandelverbod door middel van deze novelle. Natuurlijk is de handhaafbaarheid daarvan een zorg voor ons in deze Kamer, maar wij hebben gemeend dat dit met de novelle en de toelichting van de staatssecretaris voldoende geregeld is.

De heer **Koole** (PvdA):
In de novelle en vooral in de wet is het toezicht natuurlijk geregeld. Het Agentschap Telecom speelt daarin een grote rol. Maar precies op welke manier kan zo'n agentschap dat ook controleren en nagaan? Is het niet noodzakelijk om nadere eisen te stellen aan commerciële partijen? Ik kom daar in mijn bijdrage ook nog op terug. Moet je niet eisen dat zij een soort Chinese muren bouwen tussen het gedeelte van de organisatie dat inlogmiddelen verzorgt voor de overheid en dus gegevens van burgers krijgt via die inlogmiddelen, en hun commerciële activiteiten, waarbij ze misschien over dezelfde burgers wel gegevens hebben verkregen op een andere manier? Die mogen niet worden verhandeld, maar ook niet worden gekoppeld, zo zegt de novelle. Hoe kun je dat in de praktijk nou controleren? Heeft de heer Van den Berg daar geen zorgen over?

De heer **Van den Berg** (VVD):
Natuurlijk zijn er altijd zorgen over de handhaafbaarheid. Wij hebben gemeend, zoals ik aangaf, dat dit met het expliciteren hiervan en de toelichting van de staatssecretaris nu beter en naar behoren geregeld is door middel van deze novelle. Ik kijk uit naar de bijdrage van de heer Koole. Ik denk dat dat verstandig is en ik zal met veel belangstelling volgen wat de staatssecretaris daarop antwoord. Uiteindelijk is zij namelijk degene die dit wetsvoorstel gaat verdedigen.

De **voorzitter**:
Tot slot, meneer Koole.

De heer **Koole** (PvdA):
De staatssecretaris moet in dit debat nog aan het woord komen, maar ze heeft natuurlijk op andere manieren van zich laten horen, in de Tweede Kamer en ook in antwoord op schriftelijke vragen van deze Kamer. Toch zou ik de heer Van den Berg willen vragen om een voorbeeld te geven waarvan hij denkt: ja, dat is nou een voorbeeld van hoe de staatssecretaris ziet dat het toezicht hierop goed is geregeld.

De heer **Van den Berg** (VVD):
Daarvan heb ik geen voorbeeld paraat. De explicitering dat het verhandelverbod nu zo is opgenomen in deze wet is voor ons een stap in de goede richting. Maar wat betreft de concrete uitwerking daarvan denk ik dat het goed is dat we dit debat gebruiken om daarover nadere informatie te krijgen.

De heer **Ganzevoort** (GroenLinks):
Nog een heel klein vraagje. Meta, het moederbedrijf van Facebook en dergelijke, heeft dit jaar tot nu toe voor ongeveer driekwart miljard aan boetes gekregen in Europa voor het niet goed omgaan met gegevens van klanten, om zo te zeggen. Driekwart miljard. Ik heb niet gemerkt dat het bedrijf daar last van heeft, maar het was driekwart miljard. Is het niet ontzettend naïef om nu te denken dat we met een verhandelverbod in een Nederlands wetje — ik zeg het niet oneerbiedig, maar toch — dat soort risico's hebben geweerd?

De heer **Van den Berg** (VVD):
Ik zou de kwalificatie "naïef" daar niet bij willen gebruiken. U geeft een heel sprekend voorbeeld, maar dat is gedetecteerd en daar is een sanctie op komen te staan. Over de hoogte en de serieusheid van die sanctie zegt u: dat voelt het bedrijf niet. Ik denk dat we er dan verder over moeten praten wat de sanctiemogelijkheden zijn, hoe we dat goed kunnen detecteren en hoe ons strafrecht of onze juridische waarborgen daarbij een goede rol kunnen spelen. Maar het feit dat die sanctie voor dat bedrijf is uitgevaardigd, geeft natuurlijk wel aan dat het handhaafbaar is.

De heer **Ganzevoort** (GroenLinks):
Dat stukje is handhaafbaar. Of het wel of niet opgespoord kan worden, daarover heeft de heer Koole net terecht vragen gesteld. Mijn punt is dat het de vraag is of je bedrijven die zo veel geld verdienen met data überhaupt op de markt

moet willen toelaten om onze persoonlijke gegevens te beheren. Dat is de belangrijkste vraag.

De heer **Van den Berg** (VVD):
Die vraag van de heer Ganzevoort begrijp ik. Ik zie dat mijn fractie en die van de heer Ganzevoort daar met een andere blik naar kijken, met een andere blik op de wereld en welke rol je private partijen hierin wil geven. Ik denk dat het antwoord op die discussie niet zou moeten zijn het totaal weren van private spelers bij dit soort onderwerpen, maar dat het antwoord meer gezocht moet worden in hoe je het juridisch goed kunt organiseren dat opsporing en effectieve sancties daar inderdaad mogelijk zijn.

Mevrouw **Gerkens** (SP):
Volgens mij betoogt van de heer Ganzevoort nu juist dat dat per definitie niet te doen is. Die boetes zijn gegeven nadat een strafbaar feit is geconstateerd. Dan zijn die data al gelekt. Dan is het kwaad dus al dusdanig geschied dat er enorme boetes tegenover staan. We hebben het hier over de meest vertrouwelijke informatie. Is de heer Van den Berg bereid daar toch zeg maar Russische roulette mee te spelen, wetende dat wij eigenlijk per definitie niet in staat zijn om binnen die systemen te ontdekken welke overtredingen Meta, Google, Microsoft et cetera hebben begaan?

De heer **Van den Berg** (VVD):
Ik denk dat het voor zich spreekt dat je dit pas kunt detecteren nadat het feit gepleegd is. Ik ben het ermee eens dat dit zeer onwenselijk is en dat je daar strenge regels voor moet hebben. Nogmaals, voor ons is dat een kwestie van een goede handhavingsstructuur eromheen bouwen in plaats van a priori te zeggen dat je private actoren sowieso van deze markt gaat weren.

Mevrouw **Gerkens** (SP):
Ik zou de heer Van den Berg ervan willen overtuigen dat het per definitie niet mogelijk is om te ontdekken of er misbruik is gemaakt van die gegevens omdat je het hebt over meta-, meta-, metagegevens. Het is alsof ik in uw brein zou moeten kijken, voorzitter, en zou zeggen: op dat plekje zit de naam van de heer Van den Berg. Dat is schier onmogelijk. Als ik de heer Van den Berg dit vertel, begint hij dan toch niet een beetje te twijfelen? Als ik hem ervan kan overtuigen dat het dus niet mogelijk is om dit goed in te richten, zou hij dan anders tegen het standpunt aankijken om dit soort private partijen toe te laten?

De heer **Van den Berg** (VVD):
Ik dank mevrouw Gerkens voor de vraag. Die ga ik even op mij laten inwerken, maar vooralsnog blijf ik bij het standpunt van mijn fractie.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan is het woord aan de heer Dittrich namens D66.

De heer **Dittrich** (D66):
Dank u wel, voorzitter. Nederland digitaliseert. Steeds meer diensten worden via onlinetransacties geleverd en ook de overheid moet moderniseren en in die ontwikkeling meegaan. Het voorstel voor de Wet digitale overheid past in die ontwikkeling. Of je het nu leuk vindt of niet, digitalisering gaat een steeds groter deel van ons leven uitmaken. Het biedt veel kansen en gemak maar ook uitdagingen en dilemma's. De transitie naar digitalisering vraagt ook van ons als parlement om scherp te blijven.

Het wetsvoorstel heeft een interessante voorgeschiedenis gehad. Een lang verhaal kort: de Eerste Kamer heeft een novelle afgedwongen en in die novelle zitten een aantal forse verbeteringen. Tijdens de deskundigenbijeenkomst die wij georganiseerd hadden, heeft de voorzitter van de Autoriteit Persoonsgegevens, de heer Aleid Wolfsen, de Kamer gevraagd alert te zijn bij het behandelen van deze kaderwet. Het staketsel wordt in dit wetsvoorstel geregeld maar de echte invulling ervan gaat via de AMvB's en ministeriële regelingen. Maar digitalisering raakt ook vaak de grondrechten van burgers, zoals het privéleven, het geheim van communicatie. Wolfsen zei in die bijeenkomst en ik citeer: "De grens tussen de twee uitersten van "fantastisch dat dit allemaal kan" en "levensgevaarlijk wat hier gebeurt" is nog nooit zo dun geweest." Met die blik kijkt de fractie van D66 naar dit wetsvoorstel. Wij hadden aangedrongen, met andere fracties overigens, op de novelle omdat we vonden dat bepaalde normen in de wettekst zelf moesten worden verankerd en niet in nadere regelgeving. Ik denk dan aan de open standaarden, privacy by design, het verhandelverbod van privégegevens, de dataminimalisatie en de doelbinding. Het is goed om te zien dat dat allemaal in de novelle terecht is gekomen. Ik vind het een voorbeeld van de meerwaarde van ons werk hier in de Eerste Kamer.

Dat gezegd hebbend zijn er toch wel een aantal vragen die de fractie van D66 naar voren wil brengen. Vandaag spreken we over het contact van burgers en bedrijven met de overheid. Dat wordt gedigitaliseerd. In andere debatten vraagt de fractie van D66 naar en wijst de fractie van D66 vaak op de vele mensen in Nederland — volgens de Nationale ombudsman tussen de 2 en 2,5 miljoen — die niet zo digitaal vaardig zijn. In de Algemene wet bestuursrecht is opgenomen dat er bij overheden een loket moet zijn waar menselijk contact mogelijk is, maar soms gaan wetten te zeer uit van burgers en bedrijven die goed opgeleid zijn, op de hoogte zijn van nieuwe ontwikkelingen, vaardig genoeg zijn om online hun zaakjes te regelen. Mijn vraag aan de staatssecretaris is: kan zij borgen dat naast alle regelingen die in het kader van de WDO tot stand zullen komen, ook in de tranches twee en drie, er rekening wordt gehouden met mensen die geen digitaal contact met de overheid kunnen of willen hebben? De tweede vraag daaraan gekoppeld is de volgende. In de stukken met betrekking tot de WDO worden veel jargon en afkortingen gebruikt. Soms zijn de teksten moeilijk te doorgronden. Uit onderzoek naar hoe scholieren het Nederlands beheersen, weten we dat bijna een op de vier moeite heeft met het begrip van de Nederlandse taal. Voor digitalisering is taal onontbeerlijk. Gaat de staatssecretaris erop letten dat er met burgers en bedrijven in begrijpelijke taal voorlichting wordt gegeven, ook op websites van lagere overheden?

Voorzitter. D66 is voorstander van het opensourcebeginsel, ook als groeimodel. We zijn blij dat dit in de novelle terecht is gekomen. De aanbieder van het inlogmodel moet voor een goed product zorgen. Wat daarbij hoort, is dat er een gemeenschap is van mensen die de openbroncode in de gaten houden, die testen of het inlogmiddel aan alle vereisten blijft voldoen, of er kwetsbaarheden in het systeem zitten, of hacken afdoende kan worden tegengegaan. Het is het meerogenprincipe.

Ik heb de volgende vragen. Hoe kunnen we er zeker van zijn dat dergelijke gemeenschappen ontstaan, hun werk goed doen en hun werk goed blijven doen? Welke rol ziet de staatssecretaris daarin voor de overheid? Is er een kwaliteitscontrole voor zo'n gemeenschap? Door wie? En wat als zo'n gemeenschap wegvalt? Vaak zijn het hele gedreven vrijwilligers. Ik heb twee weken geleden een gesprek met een aantal van hen gehad. De vraag dringt zich op of de overheid hier niet meer structuur moet bieden.

De heer **Van Hattem** (PVV):
Het zijn op zich terechte vragen van de heer Dittrich van D66, maar het punt is dat er nu heel sterk van uitgegaan wordt dat er noodzakelijkerwijs een gemeenschap moet zijn van mensen die met open source bezig zijn. Het is een soort conditio sine qua non, alsof het anders echt niet kan plaatsvinden. Het feit is dat als iets als open source wordt aangeboden, ook de individuele zolderkamernerd, om het zo maar even te noemen, hierop kan losgaan. Dat hoeft niet per se in een vaste gemeenschap te zijn. Is de heer Dittrich het met me eens dat juist het aanbieden van opensourcesoftware eenieder de mogelijkheid biedt om het systeem kritisch onder de loep te nemen en daar dus gewoon alle risico's en onzorgvuldigheden uit te kunnen vissen? Dat kan dus zowel een gemeenschap als een individu zijn.

De heer **Dittrich** (D66):
Ja, ik ben het ermee eens dat zo'n gemeenschap niet uit honderden personen hoeft te bestaan. Het kan misschien ook uit een enkeling of een klein groepje bestaan. Het gaat erom dat mensen bij de openbroncode terecht moeten kunnen en vandaaruit kunnen kijken of die open source aan de kwaliteitseisen voldoet die wij daaraan stellen.

De heer **Van Hattem** (PVV):
De heer Dittrich is het dus wel met mij eens dat open source het uitgangspunt moet zijn. Of die gemeenschap vervolgens uit één persoon of uit honderdduizend personen bestaat, is eigenlijk niet zo relevant, als er maar open source beschikbaar wordt gesteld.

De heer **Dittrich** (D66):
Wat onze fractie betreft moet het meerogenprincipe echt verankerd zijn. Dat betekent vaak dat één zolderkamernerd, zoals u dat noemt, misschien wel heel erg veel kan, maar het zou beter zijn als men met elkaar overleg pleegt, kijkt waar een kwetsbaarheid in het systeem zit en met elkaar gegevens uitwisselt. Over het algemeen zou ik zeggen "meer ogen is beter", maar daar zijn wel wat vragen over te stellen, en die heb ik gesteld.

Voorzitter. Wij zijn voorstander van het elektronisch identificatiemiddel. Open source moet dat zijn, omdat dat de meest effectieve manier is om onbetrouwbare partijen buiten de deur te houden en de veiligheid en privacy te waarborgen. Het wetsvoorstel kiest voor een duaal stelsel en laat ook private partijen, bedrijven, toe om inlogmiddelen aan te bieden, mits ze natuurlijk aan een aantal specifieke voorwaarden voldoen. Dat is dus een vorm van marktwerking naast het inlogmiddel dat de overheid aanbiedt. Dat betekent dat techbedrijven als Google, Twitter en Facebook mee kunnen dingen, terwijl hun businessmodel perverse prikkels kent, die zelfs schadelijk zouden kunnen zijn voor de democratische rechtsstaat. Denk aan de reclame-inkomsten die groter worden naarmate er meer reuring op het techplatform ontstaat, waardoor bijvoorbeeld complottheorieën en onlinehaatberichten welig tieren.

Onlangs lazen we: "De overheid stopt met Facebook als het bedrijf niet beter omgaat met persoonsgegevens. Doordat de kans klein is dat Facebook aan alle privacy-eisen zal voldoen, is het waarschijnlijk dat de overheid zich uiteindelijk terug zal trekken van het sociale netwerk." Dit kwam van RTL Nieuws. In het kader van de WDO vraag ik aan de staatssecretaris: moet de overheid eigenlijk wel willen meewerken aan het toelaten van dit soort techbedrijven met schimmige praktijken? Wil de overheid niet stimuleren — dat is eigenlijk waar ik de heer Koole over hoorde praten — dat organisaties zonder winstoogmerk, uiteraard op basis van open source en een transparant businessmodel, voorrang krijgen? Zo ja, hoe ziet de staatssecretaris dat voor zich?

Daaraan gekoppeld is de volgende vraag: hoe moet de burger eigenlijk een keuze maken uit die verschillende inlogmiddelen? Wie geeft daar eerlijke voorlichting over? Wat als het misgaat? Volgens de Venice Principles, principes van de Raad van Europa, moet er een fatsoenlijke klachtenbehandeling worden opgetuigd. Kan de staatssecretaris aangeven hoe zij de klachtbehandeling ziet? En bij wie moet de burger of het bedrijf zijn? Bij de private onderneming of bij de publieke, die het inlogmiddel —- bijvoorbeeld een verbeterde versie van DigiD — heeft aangeboden? Graag daarop een reactie van de staatssecretaris.

De heer **Van Hattem** (PVV):
Ik hoorde de heer Dittrich van D66 kritiek uiten op techbedrijven, die de nodige risico's met zich meebrengen voor de privacy en de veiligheid van burgers et cetera. Maar waarom zouden we dan wel blindelings vertrouwen op de goedertierenheid van de overheid? Evengoed kan de overheid ook de grondrechten van de burgers schenden en de digitale identiteit inzetten voor dergelijke beperkingen en middelen. Moeten we daar evengoed niet kritisch op zijn en niet alleen de bal leggen bij de commerciële aanbieders als de grote boosdoener?

De heer **Dittrich** (D66):
Daar heeft de heer Van Hattem een punt. Daar moeten we zeker kritisch over zijn, vandaar dat we dit wetsvoorstel en de novelle bespreken, met allerlei ankerpunten daarin. Maar dat ontslaat ons niet van de verplichting om ook in de toekomst goed de vinger aan de pols te houden, zeker als de kaderwet verder wordt ingevuld.

De heer **Van Hattem** (PVV):
Maar dan komen we al bij het punt dat die kaderwet verder moet worden ingevuld. Is het dan niet veel belangrijker dat we nu aan de voorkant al zeggen "wacht even, overheid, we gaan misschien twee stappen te ver door hier al de basis te leggen voor die verdere invulling, die misschien wel hele riskante ontwikkelingen met zich meebrengt voor de grondrechten, vrijheden en privacy van burgers," in plaats van nu drie stappen vooruit te doen? Is het niet veel belangrijker dat we nu gewoon eerst de basis op orde brengen met goede inlogmiddelen in plaats van nu al heel dat raamwerk op te tuigen waarvan we misschien wel moeten vrezen dat het ten koste gaat van de vrijheid en privacy van burgers?

De heer **Dittrich** (D66):
Vandaag bespreken we de eerste tranche van de Wet digitale overheid. Er volgen er hoogstwaarschijnlijk nog meer, een tweede, een derde en misschien nog wel meer. En er komen algemene maatregelen van bestuur en ministeriële regelingen. Daar moeten we echt goed naar kijken om te voorkomen dat er problemen ontstaan. Problemen zullen altijd ontstaan, maar het gaat erom dat je die adequaat kunt tegengaan.

De **voorzitter**:
Tot slot, meneer Van Hattem.

De heer **Van Hattem** (PVV):
Het punt is het volgende. Als wij deze fuik ingaan, lopen we wel het risico dat er straks geen weg meer terug is. We krijgen ook te maken met Europese richtlijnen en verordeningen die mogelijk ervoor zorgen dat het slikken of stikken wordt. Is de heer Dittrich het met mij eens dat als wij nu deze stappen gaan zetten, wij straks misschien toch in die fuik terechtkomen waarin er geen weg meer terug is en dat ze bij volgende tranches eigenlijk een soort van noodzakelijk kwaad worden om het maar in te moeten vullen, omdat we anders niet meer aan al die richtlijnen voldoen? Zou het niet veel beter zijn om nu een handrem in werking te kunnen zetten?

De heer **Dittrich** (D66):
Ik kan niet meegaan in het beeld dat de heer Van Hattem schetst dat we nu met z'n allen een fuik in zwemmen. Dit is een open kaderwet en die moet verder worden ingevuld. We zijn daar allemaal bij. Ik ben niet zo pessimistisch als de heer Van Hattem.

De heer **Ganzevoort** (GroenLinks):
De heer Dittrich vroeg net: hoe maken we de burgers erop attent waar ze uit kunnen kiezen en dergelijke? Ik kom weleens een keertje op internet en op steeds meer plekken zie ik "log in met Google" of "log in met Facebook". We krijgen allerlei opties aangeboden. Deze zijn op de een of andere manier betaald, denk ik. Moet de overheid daar dan naast gaan staan met "log in met de overheid" of zouden we moeten zeggen: misschien moeten we helemaal die kant niet op? Het zijn hele terechte vragen van de heer Dittrich, ook in de lijn van de heer Koole, naar het voorkomen dat de verkeerde aanbieders ertussen zitten. De goede aanbieders die er privaat zullen zijn, hebben nooit hetzelfde reclamebudget als die grote bedrijven.

De heer **Dittrich** (D66):
Dank voor de vraag, meneer Ganzevoort. Dat is ook de reden waarom ik aan de regering vraag wie er eerlijke voorlichting geeft over de bestaande of aangeboden inlogmiddelen zodat het publiek een goede keuze kan maken. Het kan heel wel zijn dat de overheid daar een belangrijke rol in gaat spelen. Daarom wil ik het antwoord van de staatssecretaris afwachten. Dat zou principieel helemaal niet verkeerd zijn.

De heer **Ganzevoort** (GroenLinks):
Dat snap ik, maar maken we het onszelf niet heel erg moeilijk door het überhaupt hybride te maken?

De heer **Dittrich** (D66):
Dat debatje hebben we eerder gevoerd met mevrouw Prins. Zij gaf daar wel een helder antwoord op, vond ik. Het is een probleem als je alleen als overheid een inlogmiddel aanbiedt. Dat hebben we in het verleden met DigiD gezien. Op een gegeven moment werkte het niet. Dan wordt alles afgesloten en kan niemand meer contact hebben met de overheid. Je moet kunnen kiezen tussen inlogmiddelen en je moet als individu misschien wel meer dan één inlogmiddel hebben. Dat is zeker een mogelijkheid. Dat heeft de regering ook eerder op schriftelijke vragen van ons en van anderen geantwoord. In het debat met de regering wil ik daar goed naar luisteren.

Voorzitter. De Stichting Lezen en Schrijven wijst erop dat laaggeletterden vaak iemand willen machtigen om iets bij de overheid te regelen, want ze zijn vaak slachtoffer van online-oplichting. Die stichting wil dat de manier van machtigen om iemand hulp te geven voor zowel de private als de publieke inlog hetzelfde is, ter verkleining van het oplichtingsrisico. Hoe ziet de staatssecretaris dat?

Over decentrale opslag is ook al het nodige gezegd. Verschillende experts pleiten voor een decentraal opslagsysteem voor de data, dus dat er geen centraal opslagsysteem is, maar dat de gegevens bijvoorbeeld op de smartphone van de gebruiker staan. Maakt dit wetsvoorstel en de volgende tranches die decentrale opslag gemakkelijk en gemakkelijker? Hoe zijn de ontwikkelingen?

Voorzitter. Tot slot de rechten van burgers en bedrijven. Er worden veel gegevens gekoppeld. Soms weten burgers en bedrijven niet eens dat die koppeling plaatsvindt. Doelbinding is hierin een belangrijk element. We weten dat burgers het soms fijn vinden dat ze niet steeds dezelfde dingen moeten invullen en dezelfde gegevens moeten overleggen. Een min of meer automatische koppeling stuit weer op privacybezwaren. Als medewetgever wilde D66 dat die doelbinding een wettelijke verankering kende en niet alleen in nadere regelgeving werd opgenomen. Dat roept toch nog een aantal vragen op. Hoe is het standaard inzagerecht geregeld voor de burger? Hoe ziet de staatssecretaris het correctierecht en het verwijderingsrecht als data niet blijken te kloppen? Hoe wordt het de burger of het bedrijf gemakkelijk gemaakt om veranderingen door te voeren?

Helemaal tot slot nog iets over toezicht en handhaving. Onder het toezicht in de WDO heeft de Autoriteit Persoonsgegevens een rol, maar het Agentschap Telecom uiteraard ook. Hoe vullen die twee elkaar aan? Hoe gaat het met de handhaving, bijvoorbeeld als de toelating van een private partij moet worden ingetrokken omdat hij niet meer aan de voorwaarden voldoet? Hoe zit dat dan precies? Hoe gaat het met de last onder dwangsom? Wie geeft die? En helemaal tot slot: heeft het Agentschap Telecom daadwerkelijk voldoende personeel, kennis en kunde in huis om deze belangrijke taken te vervullen?

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Dittrich. Dan is het woord aan meneer Talsma namens de ChristenUnie.

De heer **Talsma** (ChristenUnie):
Meneer de voorzitter. Het pakket van wetsvoorstellen en novelle dat we vandaag in deze Kamer behandelen, kent inmiddels een lange totstandkomingsgeschiedenis. Als de Kamer geen digitale Kamer zou zijn geweest, zouden we tegen een gemeen dik pak papier aangekeken hebben. Die lange voorgeschiedenis, in combinatie met de bijna ongrijpbare breedte van het etiket "digitale overheid" draagt zo maar het risico in zich dat het geheel een wat afstandelijk, abstract en theoretisch karakter krijgt. Met instemming haal ik dan ook de kernachtige samenvatting aan die de staatssecretaris gaf bij de behandeling van de novelle in de Tweede Kamer. Die luidde in de kern: deze wet gaat vooral over veilig en betrouwbaar inloggen, zakendoen met de overheid en over veilige en betrouwbare websites. Daarmee blijkt de kern ineens toch heel concreet en bovendien heel relevant voor bijna iedereen.

Het aanvankelijke wetsvoorstel leidde ook bij mijn fractie tot prangende vragen. Ik zeg hier graag hardop dat mijn fractie waardering heeft voor het feit dat de staatssecretaris op de vele vragen vanuit deze Kamer gereageerd heeft met een novelle die verbeteringen aanbrengt, verheldering biedt en de parlementaire betrokkenheid vergroot. Ook vindt mijn fractie het fijn dat we het wetsvoorstel en de novelle gelijktijdig behandelen. Dat alles neemt niet weg dat er nog punten zijn die voor onze afweging belangrijk zijn en waarop ik de staatssecretaris dan ook graag nader bevraag.

Evenals de Raad van State vindt mijn fractie dat de wet de hoofdelementen van de regeling moet bevatten en dat het primaat van de wetgever bij de beoordeling van de nadere concretisering goed geregeld moet zijn. Dat is wat mijn fractie betreft geen potje staatsrechtelijk touwtrekken. Het heeft direct te maken met wezenskenmerken als kenbaarheid en voorzienbaarheid voor burgers, uitvoerbaarheid en handhaafbaarheid in de praktijk, en tot slot met parlementaire controle op lagere regelgeving die vérstrekkende gevolgen kan hebben.

Waar het gaat om parlementaire controle geeft het voorgestelde artikel 15 hiervoor een voorziening. De leden 2 en 3 van die bepaling zijn het gevolg van amendementen. Ze waren door de staatssecretaris aanvankelijk niet zo voorzien. Ziet mijn fractie het goed dat de bij amendement opgenomen werkwijze een soort mengvorm is van de zogeheten gecontroleerde delegatie en van delegatie onder het vereiste van goedkeuring bij wet? Zo ja, komt die mengvorm dan eigenlijk vaker voor? Wat zijn daarmee de ervaringen? Hoe verhoudt het voorgestelde zich tot de door de staatssecretaris gewenste snelheid van handelen bij technische en andere ontwikkelingen?

Een ander punt van aandacht is in dit debat al eerder aan de orde geweest. Dat blijft de invulling en toepassing van open source. Dat is iets waar mijn fractie op zichzelf positief tegenover staat. Voor dit onderwerp is er in de parlementaire behandeling al veel aandacht gewest. De antwoorden van de staatssecretaris hebben in toenemende mate helderheid geboden. Het moet gaan om software die transparant is en waarvan de broncodes gepubliceerd zijn. Ook moet er een zogeheten "community" omheen zitten, die ervoor zorgt dat er steeds weer wordt gewerkt aan het verbeteren van de software. De staatssecretaris noemde die community zelfs "superbelangrijk". Dat is een citaat. Juist dat superbelangrijke krijgt mijn fractie maar niet goed helder. Het door de staatssecretaris zelf gehanteerde fraaie voorbeeld van de cv-ketel, die geïnstalleerd moet worden en daarna regulier onderhoud krijgt, is hier niet meer bruikbaar, of de staatssecretaris moet een wel heel buitenissig onderhoudsprogramma voor haar verwarming hebben. Hoe zit het dan wel? De staatssecretaris heeft aangegeven dat zij zelf gaat stimuleren "dat er een community komt die meekijkt op alle bij inlogmiddelen gebruikte softwarecomponenten". Kan de staatssecretaris zo concreet mogelijk uitleggen wat zij hiermee bedoelt en wat we op dit punt van haar te verwachten hebben? Kan de staatssecretaris uitleggen of, en zo ja hoe, die "superbelangrijke" community's formeel worden ingebed?

Een ander punt waarvoor mijn fractie bijzondere aandacht houdt, is privacy by design een verplichting op grond van de AVG. Het is een understatement dat de ontwikkelingen op het digitale vlak razendsnel kunnen gaan. Dat kan dus ook gelden voor aanmerkelijke stappen voorwaarts waar het gaat om de toepassing van AVG-beginselen. Is na een verleende erkenning voorzien in een periodieke toets of het bedoelde design nog altijd aan de eisen voldoet? Of speelt zo'n toets wellicht een rol bij het verlengen of wijzigen van de erkenning?

Voorzitter. Het in de wet opgenomen verbod op het verhandelen van persoonlijke gegevens maakt op mijn fractie op het eerste oog een robuuste en effectieve indruk, zeker met de toelichting die de staatssecretaris gaf in haar reactie op vragen vanuit deze Kamer. In die reactie gaf zij aan dat zij bij overtreding van de regels zelf zal ingrijpen of zal laten ingrijpen. In het kader van de handhaafbaarheidstoets vraag ik de staatssecretaris dat wat nader en concreter toe te lichten. Artikel 17, lid 5, bepaalt dat het Agentschap Telecom belast is met toezicht. Welke vormen van optreden bij overtreding van de regels en welke mogelijke uitkomsten van dat optreden zijn eigenlijk denkbaar? Bovendien is voor controle en handhaving capaciteit nodig. Verschillende collega's hebben daar al de vinger bij gelegd. Op eerdere vragen of die capaciteit er bij het Agentschap Telecom of elders daadwerkelijk is, reageerde de staatssecretaris met de mededeling dat haar geen signalen hebben bereikt van het tegendeel. De vraag van mijn fractie is of de staatssecretaris ons in dit debat op dit punt wat gefundeerder en concreter gerust kan stellen.

Meneer de voorzitter. Nog niet zo lang geleden debatteerden wij hier met de parlementaire onderzoekscommissie over de effectiviteit van antidiscriminatiewetgeving. In dat debat en in het onderliggende rapport trof mij opnieuw het grote verschil in het zogenoemde doenvermogen van inwoners van ons land. Een recent artikel in Trouw over kwetsbare mensen en de digitale overheid onderstreepte dat nog eens. Het voert te ver, kijkend naar de klok, om daar nu verder over uit te weiden, maar is de staatssecretaris het met mijn fractie eens dat dit verschil in doenvermogen een wezenlijk punt van aandacht is, juist bij het onderwerp van dit wetsvoorstel? Wil zij, omdat het zo wezenlijk is, ons nog eens meenemen in de maatregelen en voorzieningen die bij inwerkingtreding van deze wet getroffen worden voor hen die te kampen hebben met laaggeletterdheid, fysieke of geestelijke beperkingen, of anderszins moeite hebben met het contact met een digitale overheid?

Tot slot, meneer de voorzitter. Dit wetsvoorstel is de eerste tranche — collega's hebben er al op gewezen — in een groter wetgevingstraject. Mijn fractie is erg nieuwsgierig naar het vervolg, zowel inhoudelijk als qua planning. Kan de staatssecretaris ons daarover de laatste stand van zaken geven?

Als altijd ziet mijn fractie uit naar de beantwoording door de staatssecretaris. Dank u zeer.

De **voorzitter**:
Dank u wel, meneer Talsma. Dan is het woord aan de heer Koole namens de Partij van de Arbeid.

De heer **Koole** (PvdA):
Dank u wel, voorzitter. Wij spreken vandaag over een zeer belangrijk onderwerp: het elektronisch verkeer van burgers en bedrijven met de overheid, en dan met name de eerste tranche van een generieke digitale infrastructuur. Die eerste tranche is gericht op het ontwikkelen van nieuwe inlogmiddelen — een nieuwe DigiD, zeg maar. Daar waren we al even mee bezig. Eerder is al gezegd dat het wetsvoorstel hierover in 2018 werd ingediend en in 2020 deze Kamer bereikte.

De Eerste Kamer had grote bezwaren tegen dat wetsvoorstel, mede gevoed door informatie die we van deskundigen verkregen. De bezwaren golden vooral het gebrek aan privacybescherming in het oorspronkelijke wetsvoorstel. Dat is nogal wat, want het gaat hier om de toegang van burgers tot digitale overheidsdiensten. Belangrijke standaarden waren niet in dit wetsvoorstel over inlogmiddelen opgenomen, zoals privacy by design en open source, zoals dat in jargon heet.

Bij privacy by design gaat het erom dat bij het ontwerp van de inlogmiddelen rekening moet worden gehouden met de bescherming van persoonsgegevens. Dat moest al op grond van de Algemene verordening gegevensbescherming, de AVG. Maar deze Europese verordening regelde niet dat het ontbreken van privacy by design een grond is om een erkenningsaanvraag te weigeren. Dat laatste stond evenmin in het oorspronkelijke wetsvoorstel.

Open source houdt in dat de broncodes van de software openbaar zijn. Volgens deskundigen biedt dat de beste garanties dat de software veilig en betrouwbaar is, mits de gemeenschap die de software onder zijn hoede heeft voldoende groot is.

De Eerste Kamercommissie voor Binnenlandse Zaken — de heer Dittrich zei het al — stuurde daarom in juli 2020 een brief aan het kabinet over deze onderwerpen. De reactie van het kabinet destijds was nogal lauw. In september van hetzelfde jaar werden daarom scherpe schriftelijke vragen gesteld, ook door mijn PvdA-fractie. De privacy werd het beste gediend met verplichte open source en decentrale opslag, dus de vraag was waarom daar niet voor was gekozen. Inmiddels koos tijdens de coronacrisis een ander ministerie, VWS, daar wel voor bij de vormgeving van de CoronaMelder. De eenheid van digitaal overheidsbeleid was zoek.

De brede kritiek vanuit deze Kamer leidde gelukkig tot bezinning. In de memorie van antwoord van februari 2021 werd een drietal wijzigingen aangekondigd: privacy by design, open source en het verbieden van het commercieel uitnutten van gegevens door private partijen. Die hebben geleid tot de novelle die in juni van dit jaar werd ingediend bij de Tweede Kamer en die vandaag ook voorligt in deze Kamer. Wij zijn de regering dan ook erkentelijk dat ze naar bezwaren van deze Kamer heeft willen luisteren. In de novelle zijn belangrijke punten opgenomen die eerder ten onrechte ontbraken en zijn verschillende begrippen, mede op advies van de Raad van State, nader toegelicht.

Toch resten bij mijn factie nog verschillende prangende vragen. Ik begin met de al eerdergenoemde problematiek van de open source. Uitdrukkelijk is destijds door verschillende fracties in deze Kamer gevraagd om de opensourcebenadering verplicht te stellen. De broncode wordt gepubliceerd, zodat in een gemeenschap, een community van kenners en kunners, op transparante wijze verbeteringen kunnen worden gesuggereerd. Maar in de novelle is daarvoor niet gekozen. Weliswaar wordt de open source wenselijk geacht en spreekt de regering van een groeimodel waarin stapsgewijs componenten van inlogmiddelen worden aangewezen waarvan de broncode moet worden gepubliceerd, maar voorlopig kunnen private aanbieders van inlogmiddelen ook nog met closed source werken. Het is immers "open source tenzij" en niet "open source tout court". De regering overtuigt vooralsnog niet met haar redenering waarom dat het geval moet zijn. Waarom is niet gekozen voor het direct verplicht stellen van de open source in elk geval voor nieuwe aanbieders? Dat klemt temeer omdat het verplicht stellen van het open sourcevereiste bij toelating van elk inlogmiddel, zoals de Nijmeegse hoogleraar Jacobs het een jaar geleden in een artikel over open source als strategisch instrument schreef "ook een defensief wapen is tegen de agressie en het techkolonialisme van de dominante ICT-leveranciers. Open source is dus niet alleen goed voor de transparantie, hergebruik en onafhankelijkheid, maar ook als strategisch verdedigingswapen ten gunste van de eigen soevereiniteit." Verplicht open source dus, ook om de macht van de big tech — Huawei, Google, Microsoft en Apple — te kunnen pareren en om strategische veiligheid te kunnen bewerkstelligen.

Als antwoord op de vraag van onze fractie waarom de open source niet als harde eis is gesteld, schrijft de regering in de memorie van antwoord van vorige maand dat een van de redenen om voor een systeem van open toelating te kiezen, het creëren van vitaliteit in het stelsel is, doordat er

verschillende inlogmiddelen beschikbaar komen voor de toegang tot digitale overheidsdienstverlening. Kan de regering uitleggen wat het "creëren van vitaliteit" inhoudt? Welke evidente voordelen zou de betrokkenheid van commerciële bedrijven hier volgens de regering kunnen opleveren? Wegen deze op tegen mogelijke nadelen?

Tegelijkertijd benadrukt de regering in de memorie van antwoord op pagina 16 dat natuurlijke personen altijd op verschillende betrouwbaarheidsniveaus kunnen inloggen met een publiek middel. Dus ook zonder inlogmiddelen van private bedrijven is de overheid gehouden om burgers en bedrijven een kwalitatief goed inlogmiddel aan te bieden. Ook zonder de vitaliteit van een systeem van open toelating moeten burgers dus kunnen rekenen op een kwalitatief goed publiek inlogmiddel. Kan de regering dat bevestigen? Of is een tweede inlogmiddel op den duur nodig, zoals mevrouw Prins ook zei? En, zo ja, is dan dat tweede middel — als het er is, maar wat eerst werd ontkend omdat er één middel is waarop altijd door een burger moet kunnen worden gerekend — een publiek tweede middel of moet dat per se een privaat tweede middel zijn? Daar bestaat dus toenemende onduidelijkheid over.

Maar waarom wordt nog vastgehouden aan dat systeem van open toelating zonder de verplichting van open source? Waarom is het vooralsnog nodig om commerciële partijen toe te laten als nieuwe aanbieders van inlogmiddelen gebaseerd op closed source, wanneer de regering zelf zegt dat, ongeacht de aanwezigheid van private aanbieders, de burgers altijd moeten kunnen inloggen met behulp van een kwalitatief goed publiek middel? Vereist Europese regelgeving wellicht het toelaten van commerciële partijen? Kan de regering bevestigen dat een publiek inlogmiddel altijd gebaseerd is of zal moeten zijn op open source?

Voorzitter. Daar komt de problematiek van de controle nog eens bij. We hebben het daar net ook al even over gehad. Terecht is nu in de novelle vastgelegd dat het private partijen verboden is om data verkregen via het inlogmiddel voor overheidsdienstverlening, te koppelen aan data die het bedrijf via andere, commerciële, wegen heeft verkregen. Vereist het verbod op koppeling niet dat er in die commerciële bedrijven — ik noemde ze al eerder — Chinese muren bestaan tussen beide typen data? Kan de regering uitleggen waarom zij op dit punt geen eisen wil stellen aan de bedrijfsorganisatie van de commerciële aanbieders van inlogmiddelen? En hoe gaat zij het niet koppelen en niet verhandelen van data verkregen via inlogmiddelen voor de digitale overheidsdienstverlening, in de praktijk controleren? Heeft het Agentschap Telecom daarvoor voldoende capaciteit? Ook de heer Dittrich wees daar al op. Welke rol — als er één is — heeft de Autoriteit Persoonsgegevens bij de controle op en het handhaven van het niet koppelen en het niet verhandelen van data verkregen door inlogmiddelen voor overheidsdiensten? In elk geval dient de Autoriteit Persoonsgegevens toezicht te houden op de privacy by design. Die moet dan wel de nodige capaciteit hebben. Daarover gaat de staatssecretaris met de AP in overleg, zei zij in juni in de Tweede Kamer. We zijn inmiddels een halfjaar verder. Kan de staatssecretaris zeggen hoe het daarmee staat? Heeft de Autoriteit Persoonsgegevens wel voldoende capaciteit?

Voorzitter. Is de regering het eens met onze fractie dat de problematiek van controle op het niet koppelen en het niet verhandelen van data aanzienlijk zou worden gereduceerd bij het niet toelaten van commerciële partijen als aanbieders van inlogmiddelen voor overheidsdiensten? Kan de regering bovendien aannemelijk maken dat commerciële bedrijven zich als nieuwe aanbieders van inlogmiddelen zullen melden, wanneer open source verplicht is en/of wanneer zij door inlogmiddelen voor overheidsdiensten verkregen data niet mogen koppelen en ook niet mogen verhandelen of anderszins commercieel mogen uitnutten? Wat blijft er dan nog over van hun verdienmodel? Ik meen dat ook mevrouw Prins daar een vraag over stelde.

Voor het goed functioneren van open source, zo stelt de regering, is een actieve community nodig die over publiekelijk toegankelijke broncodes kan beschikken en suggesties voor verbetering kan doen. De staatssecretaris heeft in de Tweede Kamer aangegeven zelf actief het bestaan en functioneren van dergelijke community's te willen bevorderen. Kan zij aangeven hoe zij dat voor zich ziet? Op welke wijze wil zij dat gaan stimuleren? Is er één community voor alle broncodes gewenst of zijn er meerdere community's nodig voor verschillende broncodes?

In de praktijk zijn dergelijke community's nogal fluïde. Wat als een community ondanks alle inspanningen van de regering toch niet van de grond zou komen? Is de regering dan bereid om door middel van financiële vergoedingen een dergelijke community te creëren? En hoe onafhankelijk is een dergelijke community in dat geval?

Kan de staatssecretaris nog eens uitleggen wat zij bedoelde toen zij in de Tweede Kamer zei dat de broncode bij het opensourcemodel niet gratis hoeft te zijn? Wat bedoelde zij daarmee?

Kan de regering bovendien ingaan op de zorgen die sommigen uiten, ook vandaag nog, dat openbaar gemaakte broncodes in verkeerde handen vallen, bijvoorbeeld van geopolitieke tegenstanders of handelspolitieke concurrenten? Speelt het streven naar strategische autonomie van Europa nog een rol in de afweging? Kan een derde partij het goed functioneren en de privacy van inlogsystemen bij de Nederlandse overheidsdiensten ten nadele beïnvloeden, doordat ook zij over de publieke broncodes beschikken, zoals onder anderen de heer Van den Berg vandaag beweerde? Zijn deze zorgen wel reëel, is mijn vraag aan de staatssecretaris.

Voorzitter. Privacy by design is via de novelle geregeld in de artikelen 9, 11 en 14. Wat niet in de novelle is geregeld, is dat hierbij een zogeheten data protection impact assessment, DPIA, wordt geëist. Die eis komt, zo begrijpen wij, te staan in de ministeriële regeling. Waarom is die tamelijk principiële eis niet in de wet zelf opgenomen? Dit raakt aan de al eerdergenoemde problematiek van delegatie.

Eenzelfde vraag kan worden gesteld ten aanzien van de verplichte digitale inzage en correctie bij aanbieders van inlogmiddelen; de heer Dittrich had het er al over. Waarom is dit principiële uitgangspunt niet in de wet zelf opgenomen, maar komt het in de ministeriële regeling te staan? Een ministeriële regeling is toch bedoeld voor zaken die in de praktijk snel moeten kunnen worden gewijzigd? Maar dat geldt toch niet voor het principe van verplichte digitale inzage en correctie?

Voorzitter, tot slot. De in de oorspronkelijke wet en de novelle opgenomen vereisten brengen ook het nodige werk

met zich mee voor de decentrale overheden. Kan de regering aangeven in hoeverre de decentrale overheden beschikken over de nodige capaciteit om dit waar te maken? Kan de staatssecretaris aangeven hoe het staat met het voorstel aan IPO en VNG om het toezicht dat provincies houden op waterschappen en gemeentes in deze kwestie te centraliseren, dat wil zeggen op rijksniveau te leggen? Hoe staat het daarmee?

Vanzelfsprekend moet het verkeer van burgers met de overheid, ook het digitale verkeer, voor iedereen toegankelijk blijven, rekening houdend met het doenvermogen van burgers, zoals de heer Talsma ook al opmerkte.

De leden van de PvdA-fractie zien uit naar de beantwoording van hun vragen.

De **voorzitter**:
Dank u wel, meneer Koole. Dan is het woord aan mevrouw Gerkens namens de SP-fractie en mede namens de Partij voor de Dieren.

Mevrouw **Gerkens** (SP):
Dank u wel, voorzitter. Ik spreek vandaag inderdaad ook namens de fractie van de Partij voor de Dieren.

Ik werp even een blik op de kalender en zie dat het vandaag 29 november 2022 is. Dat is bijna dertien jaar nadat ik met het onderwerp "veilig inloggen bij de overheid" van start ging. Op 4 april 2010 stelde ik de eerste Kamervragen over de onveilige constructie van DigiD. De tweestapsverificatie, het gebruik van de app en andere tussenstappen hebben DigiD een stukje veiliger gemaakt, maar bij sommige overheidsdiensten wordt zelfs die tussenstap al niet eens gevraagd. De facto werken wij dus al meer dan dertien jaar met een systeem dat op z'n zachtst gezegd verbetering behoeft. Het is dus fijn dat er wetgeving komt voor een beter systeem.

Ik besef ook dat de senaat zelf debet is aan het feit dat de wet weer wat verder vertraagd werd. Het is immers ook door onze fracties aangegeven dat er absoluut een eis van opensourcesoftware in het wetsvoorstel opgenomen moet worden. Zonder deze novelle was het wetsvoorstel voor ons per definitie onaanvaard geweest. Maar de eis is niet absoluut en de novelle lost niet alle problemen op. Er blijven bij onze fracties vragen, die wij vandaag hopen beantwoord te krijgen.

Voorzitter. Digitaal communiceren is de norm geworden, maar naast die norm mag de uitzondering blijven bestaan, zo zegt de staatssecretaris. Het is belangrijk dat die uitzondering mag blijven bestaan, want niet iedereen is digitaal vaardig. Toch merken de fracties van de SP en de PvdD dat op papier communiceren steeds lastiger wordt. Zo word ik per mail gevraagd digitaal de waterstanden door te geven en mijn arts zet ongevraagd uitslagen in een digitaal beschikbare omgeving. Op papier ontvang ik van beide niets meer. Hoe gaat de staatssecretaris er zorg voor dragen dat de offlinekeuze ook actief aangeboden wordt, en niet iets is waar je om moet vragen?

Het digitaal identificeren is niet alleen nodig bij de Belastingdienst, een bezwaar bij de gemeente, het doorgeven van waterstanden, maar ook voor de totale zorgomgeving, van tandarts tot ziekenhuisuitslagen, het UWV, de reclassering, en ook de dienst Justis, om er maar een paar te noemen. Dat gaat dus om hele, hele gevoelige informatie. Dat hier een systeem moet komen met een veel hoger veiligheidsregime dan DigiD nu heeft, staat voor onze fracties buiten kijf.

Het is echter niet alleen de toegang die de informatie kan opleveren, ook het simpele feit dat er toegang gevraagd wordt, is al waardevolle informatie. Ik herhaal dit nog een keer, want ik denk dat het voor alle leden goed is om dat te beseffen. Niet alleen de informatie die opgevraagd wordt, is interessant, maar alleen al het feit dat men bijvoorbeeld informatie opvraagt bij de reclassering, kan al enorm interessant zijn voor commerciële partijen. Onze fracties zullen de wet dan ook beoordelen op deze punten, namelijk de verbeteringen ten opzichte van het huidige systeem en de kennis van de vraag om toegang.

De eerste van onze vragen gaat over de harde eis om open source te gebruiken. In antwoord op de vragen van de fractie van de PvdA zegt de minister dat er ruimte moet zijn om potentiële aanbieders de tijd te geven om opensourcemethoden te ontwikkelen. Afgezien van het feit dat ik nu al zie dat de markt zich aan het aanpassen is, vraag ik: stellen we nou juist niet die eis omdat we die transparantie willen garanderen? Die transparantie is ons inziens onlosmakelijk verbonden aan het gebruik van open source. Als een aanbieder dat niet kan leveren, zal hij dus niet toegelaten moeten worden. Hoe ziet de staatssecretaris dit?

Ik lees ook dat de staatssecretaris zegt dat de broncode niet openbaargemaakt hóéft te worden, bijvoorbeeld wanneer er een risico is voor de veiligheid. Maar de hele essentie van open source is dat je de broncode bekendmaakt, want daarvan wordt het systeem niet onveiliger, maar juist veiliger. Dit lijkt echt op een escape voor partijen die dan een beroep kunnen doen op deze clausule en hiermee open source kunnen ontwijken. Waarom heeft de staatssecretaris hiervoor gekozen?

Een andere vraag is waarom het wettelijke kader niet is uitgegaan van dataminimalisatie. De minister stelt in antwoord op vragen van D66 dat deze dataminimalisatie in het conceptbesluit zit. Is het nu zo dat private aanbieders alleen toegang kunnen krijgen tot de data die nodig zijn voor de toegang tot de dienst die gevraagd wordt? Of krijgt de aanbieder iedere keer opnieuw toegang tot alle informatie, ook al is slechts een deel ervan nodig? Onze fracties hebben dezelfde vragen als GroenLinks over decentrale en centrale opslag. Ik versterk de woorden door te benadrukken dat een decentrale opslag de facto veiliger is.

Dan de veiligheid en techniekonafhankelijkheid in de wetgeving. De MR biedt een uitwerkingen om de eisen te stellen dat de software veilig is, onderhouden wordt en beschikbaar is en blijft. De staatssecretaris koos ervoor om dit nu niet nader uit te werken. Maar die ruimte wordt in de MR wel geboden. Dan denken wij bijvoorbeeld aan de vereisten die aansluiten bij het hoogste veiligheidsregime rondom de gegevensuitwisselingen, namelijk die uit de eIDAS voor de QTSP's. Dan gaat het om normen uit die verordening voor audits, uitlegbaarheid, verantwoording van de securityprocedures, zoals procedures rondom een hack en het verlies van gegevens, en het vastleggen van de verantwoordelijkheid van dienstverleners om aan deze eis te voldoen. Is de

staatssecretaris bereid om deze mee te nemen? Ik neem aan dat de heer Van den Berg van de VVD hier ook goed naar luistert.

Ik zeg dit, terwijl ik weet dat dit helemaal geen garanties geeft. Bij sommige algoritmes weten de makers wel dat er een achterdeurtje is, maar weten wij dat niet. Dus zelfs als wij het hoogste niveau van beveiliging eisen en zeggen "dan moeten we deze tools gebruiken, want daarvan weten we dat het het hoogste niveau is", dan kunnen er nog steeds achterdeurtjes in zitten die de makers hebben gemaakt, maar waar wij totaal geen weet van hebben. Als we niet het hele proces zien, dan weten we niet alles. Open source kan hier zeker soelaas in bieden. Maar dat gaat over een deel van het systeem. Want open source gaat niet alleen over software, maar ook over open hardware en een open proces. Hoe garandeert de staatssecretaris deze driehoek?

De grootste zorg blijft toch wel het toelaten van commerciële private partijen tot het stelsel. Dat zijn partijen die naast het aanbieden van handige diensten nog een totaal ander doel hebben, namelijk zo veel mogelijk informatie verzamelen van de burger. De staatssecretaris stelt dat er voldoende waarborgen zijn om die informatie niet via het eID-stelsel te verzamelen. Zij verzekert ons meerdere malen dat de informatie die via het eID is verkregen, nergens anders voor gebruikt mag worden. De staatssecretaris geeft ook aan dat de informatie die op een andere wijze is verkregen, niet onder de reikwijdte van deze wet valt.

Ik vraag de staatssecretaris of zij beseft dat bedrijven die aan deze dataverzameling doen, die informatie helemaal niet nodig hebben. Die kunnen ze namelijk zelf al in combinatie met die andere dataverzameling genereren. Dat maakt het wat ingewikkeld. Maar zoals ik in het begin zei: het simpele feit dat iemand toegang vraagt tot bijvoorbeeld de reclassering kan, in combinatie met zijn surfgedrag online en onder andere inlog, al voldoende informatie over die persoon opleveren. Om in die gegevens te kunnen kijken hoeft de partij die toegang al helemaal niet meer. De enorme hoeveelheid data die daar verzameld is, kan het laatste puzzelstukje zijn om het hele plaatje te hebben. Die kunnen ze in combinatie met al die dataverzameling zelf genereren.

Ik wijs de staatssecretaris erop dat menig website van de gemeente een link naar Facebook of Instagram heeft, of zo'n mooi icoontje dat je aan kunt klikken, waardoor per definitie al data van je verzameld wordt. Ze kunnen ook met video's werken die op YouTube staan, of websites hebben die met Google Fonts werken. Dat zijn allemaal tools die trackers hebben en die vervolgens bijhouden wat je allemaal op het internet doet. De stelling dat private commerciële aanbieders geen overbodige informatie mogen verzamelen, gaat uit van de premisse dat zij dit ook niet willen. En dat is niet waar. Deze partijen is het niet zozeer te doen om die precieze informatie. Het is deze partijen er alleen om te doen dat zij weten dat iemand inlogt bij een dienst of een ziekenhuis. Met al die informatie kunnen zij in combinatie met de rest van het surfgedrag al heel erg veel.

Ik zei in een interruptie op meneer Van den Berg al dat deze informatie niet verzameld wordt per individu, maar dat dit gebeurt in statistische groepen. Dat is in eerste instantie helemaal niet naar één persoon te herleiden. Met deze statistische groepen en deze informatie in de huidige artificiële intelligentie, gaan neurale netwerken aan de slag om een profiel te maken van het individu. In die honderdduizenden megabits is dan niet meer terug te vinden of er daadwerkelijk misbruik is gemaakt van de informatie die is vergaard door de inlog. In feite hoeven deze private aanbieders ook helemaal geen toegang tot de data van de Basisregistratie. Als ze weten wanneer iemand inlogt, kunnen ze met die informatie hun neurale netwerken slimmer maken. Alle bescherming die wij nu hebben op onze overheidswebsites, bijvoorbeeld door geen trackers te gebruiken, is dan in één keer weggegooid. Wanneer de staatssecretaris zou verbieden dat er gebruikgemaakt mag worden van metadata, dan gebruikt men metametadata of metametametadata. Het zal hetzelfde resultaat hebben. Het duurt alleen ietsjes langer.

Voorzitter. Ik besef ook dat we nu al heel veel data weggeven. Ik besef dat vele overheden en zorginstellingen nog steeds niet de risico's zien van het gebruik van trackers op hun website. In juni van dit jaar bleek dat zeven ziekenhuizen in de Verenigde Staten door één pixel van Facebook gevoelige data weggaven aan het bedrijf. Meta zei deze informatie te filteren. Meta zei geen gebruik te maken van deze informatie, maar bewijzen deden ze dat niet. Hier geldt opnieuw dat het überhaupt niet te bewijzen is of Meta die data ook misbruikte, want wanneer er metadata of metametadata verzameld worden, is de herkomst onmogelijk te herleiden. Daar helpt geen wet tegen. Ik wil in dit kader ook mijn zorgen uiten over PRISM. PRISM is een surveillanceprogramma dat gericht is op personen buiten de Verenigde Staten en dat grote datastromen analyseert om onregelmatigheden te filteren en te linken aan personen en individuen. Daarbij richt het zich specifiek op persoonsgegevens verzameld via Google, Meta, Yahoo! en Microsoft. Met PRISM kan NSA dus direct in die systemen komen. Helaas doen ze dat niet op een manier waarop wij dat kunnen ontdekken, dus dat is niet transparant.

Voorzitter. Alles overziend, dit alles horend, vraag ik de staatssecretaris: waarom heeft zij geen uitsluiting opgenomen voor bedrijven die aan dit soort dataverzameling doen? Waarom kiest zij ervoor private commerciële partijen kennis te geven over welke toegang we vragen en hoe vaak? Waarom denkt zij dat deze partijen dat willen wanneer de toegang kosteloos wordt aangeboden? Waar zit dan het verdienmodel? Waarom heeft de staatssecretaris bijvoorbeeld niet gekozen voor het uitschrijven van een prijsvraag voor een aanbieder? De Rijndael-AES heeft laten zien dat dit soort prijsvragen uitstekende producten kunnen opleveren. Ik verwijs ook naar het bericht dat deze staatssecretaris overweegt te stoppen met overheidspagina's op Facebook. Wat heeft dit voor consequenties voor de toelating van Meta wat betreft het aanbieden van een eID?

Voorzitter. Het moge duidelijk zijn dat onze fracties nog niet overtuigd zijn van de juiste keuze voor het toelaten van private partijen voor de e-identificatie. Ik kijk daarom uit naar de antwoorden van de staatssecretaris op de vragen die wij gesteld hebben.

De **voorzitter**:
Dank u wel, mevrouw Gerkens. Dan is het woord aan de heer Van Hattem namens de PVV.

De heer **Van Hattem** (PVV):
Dank, voorzitter. Enigszins uitgedaagd door de heer Talsma, heb ik het papieren dossier van dit wetgevingstraject toch ook maar even bij de hand genomen. Er is ook helemaal niets mis mee om dat op papier te hebben, zeg ik er maar even bij. Alleen al de titel "wet digitale overheid" is potsierlijk en pretentieus. ICT en overheid staan in dit land immers als jarenlang garant voor mislukkingen, en met dit falen voor heel veel extra kosten voor de belastingbetaler. Terwijl het kabinet bijvoorbeeld voortblundert met het Digitaal Stelsel Omgevingswet, trekt het nu een grote broek aan en pretendeert het een digitale overheid te kunnen zijn. Een "wet dienstbare overheid" die de basis op orde brengt, ook qua ICT-dienstverlening, zou voor onze burgers veel nuttiger zijn.

De wetsvoorstellen die we vandaag behandelen, vormen een januskop. Enerzijds betreffen ze onvermijdelijke maatregelen, maar anderzijds zit er onder de WDO ook een zeer onwenselijke ontwikkeling. Het onvermijdelijke zit in de noodzaak van betere beveiligingsstandaarden voor inlogmiddelen voor de overheid. Het bestaande DigiD loopt qua veiligheid en betrouwbaarheid op zijn laatste benen en er zijn eerder al problemen ontstaan met aan DigiD gekoppelde systemen, zoals DigiNotar. In dat opzicht is het hoog tijd voor verbetering. Het lijkt op het eerste gezicht heel nuttig om in zo'n systeem ook andere praktische toepassingen mee te nemen, maar juist op dat vlak liggen de risico's en de onwenselijke ontwikkelingen op de loer. Nadat deze Eerste Kamer had gehamerd op met name risico's op het gebied van privacy en veiligheid, was ook het kabinet eindelijk wakker geschud uit zijn digitale droomwereld en besloot het met een novelle te komen waarmee zaken als open source, het verhandelingsverbod en hoogstnoodzakelijke aspecten van privacybescherming nu direct in de wet worden geregeld in plaats van in algemene maatregelen van bestuur. Daarmee is de novelle zeker een verbetering ten opzichte van het oorspronkelijke wetsvoorstel.

Desalniettemin blijven er nog veel bedenkingen bij de uitwerking van deze onderdelen. Ook de Tweede Kamer is nog niet overtuigd. Zelfs nog voor het debat van vandaag heeft de vaste commissie voor Digitale Zaken vragen gesteld over de uitvoerbaarheid van de Wet digitale overheid. Kan de staatssecretaris die antwoorden wel in dit debat geven? In ieder geval heb ik hier nog de nodige vragen over, deels in lijn met de Tweede Kamercommissie. Ten aanzien van open source spreekt de staatssecretaris over "een groeimodel dat stapsgewijs wordt ingevoerd en waarin uitzonderingen op open source mogelijk zijn vanwege veiligheid en beschikbaarheid van inlogmiddelen". Op zich is dat begrijpelijk, maar er zit geen horizonbepaling in. Dus wanneer is het wél veilig genoeg? Wat zijn daarvoor de concrete criteria? Kan er überhaupt wel gesproken van een systeem dat veilig genoeg is? Of kan er tot in lengte der dagen een tweesporenbeleid blijven bestaan ten aanzien van open source? Graag een reactie van de staatssecretaris.

Ook is nog steeds onduidelijk wat precies de rol gaat worden van de opensourcecommunity's. Uiteraard is het nuttig als ze meekijken. Ongeacht hoe groot zo'n community is, is die voor eenieder openbaar en daarmee ook bruikbaar. Maar het wetsvoorstel voorziet eigenlijk in een veel minder vrijblijvende rol. Kan de staatssecretaris aangeven hoe zij de uitvoering hiervan voor ogen ziet?

Dan over het verhandelingsverbod. De staatssecretaris stelt: "Bij het beoordelen van een aanvraag wordt getoetst of een aanvrager burgers de mogelijkheid geeft om het delen van gegevens aan derde partijen op elk mogelijk moment te beëindigen." Dat is een theoretische mogelijkheid, maar in de gebruikspraktijk kunnen ook situaties ontstaan waarbij het voor de burger in praktische zin nadelig kan uitpakken om het delen van gegevens te beëindigen. Kan de staatssecretaris aangeven in hoeverre er voorkomen zal worden dat er perverse prikkels ontstaan om het delen van gegevens in stand te laten omdat de praktische nadelen groter zullen zijn dan de voordelen? Of wordt hier geen rekening mee gehouden?

In de memorie van antwoord stelt de staatssecretaris over de uitwisseling van patiëntgegevens: "Inlogmiddelen voor zorgprofessionals om toegang te verkrijgen tot patiëntgegevens zijn nog niet breed beschikbaar op het hoogste betrouwbaarheidsniveau eIDAS hoog." Dit is omdat het niet verplicht, te duur en te gebruiksonvriendelijk zou zijn. Daarop stelt de staatssecretaris: "Uitgangspunt is dat voor uitgifte en gebruik van inlogmiddelen in ieder geval wordt aangesloten bij de digitale inlogmiddelen die vanuit de Wet digitale overheid ter beschikking komen." Kan de staatssecretaris aangegeven in hoeverre deze inlogmiddelen uit de WDO wél betaalbaar, gebruiksvriendelijk en voldoende betrouwbaar zijn voor de zorgsector?

Dan de kosten voor de gebruikers. De staatssecretaris stelt in de memorie van antwoord: "Voor het bereiken van het gewenste betrouwbaarheidsniveau van het gebruikte middel wordt een inlogfunctionaliteit op de identiteitskaart of het rijbewijs geplaatst. Met de uitgifte van deze documenten zijn leges gemoeid. Deze legesmogelijkheid is voor de identiteitskaarten geregeld inde Paspoortwet en wordt voor rijbewijzen geregeld in de WDO." Kan de staatssecretaris aangeven of de leges voor rijbewijzen en paspoorten hierdoor gaan stijgen en, zo ja, in welke mate? Worden onze burgers hiermee dus ook nog op extra kosten gejaagd terwijl hun portemonnee al leeggezogen is?

Verder stelt de staatssecretaris in de memorie van antwoord: "De juridische, organisatorische en technische basis van het stelsel zal naar verwachting circa een halfjaar na de inwerkingtreding van de wet gereed zijn, in juli 2023." Kan de staatssecretaris aangeven wat er juridisch nog geregeld moet worden? Zou dat niet nu al, bij de voorliggende wetsbehandeling, duidelijk moeten zijn?

In de brief aan de Eerste Kamer van 23 september jongstleden gaat de staatssecretaris in op de uitvoerbaarheid en de toezichthoudende taak van decentrale overheden, en stelt zij in gesprek te zijn met de koepelorganisaties. Kan de staatssecretaris aangeven wat hiervan de actuele stand van zaken is? Kan de staatssecretaris nader onderbouwen waarom ze in dit kader vertrouwt op de informatieveiligheid bij decentrale overheden? Is er voldoende grond om aan te nemen dat deze in afdoende mate op orde is? Veel decentrale overheden draaien immers zelf nog op krakkemikkige ICT-systemen. Graag een reactie.

Voorzitter. In de brief van de Tweede Kamer van 14 november jongstleden, waar ik eerder naar verwees, werden diverse relevante vragen gesteld, zoals over pseudoniemen in plaats van end-to-endencryptie, manipulatie van informatie door derde partijen, de rol van het Agentschap Telecom en de definitie van "open source" ten opzichte van "open-

bare broncode". Kan de staatssecretaris in dit debat alsnog op deze vragen antwoord geven?

Voorzitter. Ik kom nu op de januskop van dit wetsvoorstel en de onwenselijke kant ervan. De staatssecretaris stelt dat de WDO ook bedoeld is om reeds te voldoen aan toekomstige EU-regelgeving voor de Europese digitale identiteit. Ook stelt ze dat de WDO nodig is om de EU-wijzigingsverordening te kunnen uitvoeren, dus om mede uitvoering te geven aan de eIDAS-verordening. In het wetsvoorstel zit dus niet alleen Brusselse regelzucht verpakt; het loopt ook nog eens voor de fanfare uit voor de Europese digitale identiteit. Ik citeer de staatssecretaris: "De eerste tranche van de Wet digitale overheid creëert hiermee bovendien een stevig fundament voor toekomstige ontwikkelingen in lijn met de toekomstige Europese wetgeving." Het is dus een stevig fundament voor de Europese wallet-id, zoals de staatssecretaris ook in de memorie van antwoord aangeeft: "Andere functionaliteiten, zoals wallets en eisen daaraan, kunnen met enkele aanvullingen in de wet door middel van een wetswijziging in deze systematiek worden opgenomen. Dat zal naar verwachting zijn beslag krijgen in de tweede tranche van de WDO."

Over die Europese digitale identiteit is nog volop discussie gaande, ook in de Tweede Kamer, maar de staatssecretaris zet met de WDO de fuik al wagenwijd open voor dit megalomane project van de Europese Commissie. Afgelopen juli gaf Bart Custers, hoogleraar Law and Datascience bij eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden, in een kritisch opiniestuk aan dat het risico is dat voor de ontwikkeling van dit systeem de macht te veel in handen komt van bigtechbedrijven, dat toezichthouden hierdoor problematisch wordt, dat de grootschalige gegevensopslag kwetsbaar en kostbaar is, dat er risico's zijn van hacks, identiteitsfraude en profilering en dat de uitvoering te ingewikkeld is voor overheden.

In de recente antwoordbrief aan de Tweede Kamer geeft de staatssecretaris zelf aan dat er het risico is van overidentificatie bij de Europese digitale identiteit. Bovenal kan de Europese digitale identiteit, eID, ten koste gaan van privacy, persoonlijke vrijheden en grondrechten, zeker nu de Europese Commissie deze digitale wallet voor alle burgers verplicht wil stellen en tegelijkertijd kiest voor een breed toepassingsbereik. Welke garanties kan de staatssecretaris geven dat de vrijheden en de privacy van onze burgers via deze WDO niet worden meegezogen in deze Brusselse fuik?

Op haar website stelt de Europese Commissie immers dat de eID gebruikt zou kunnen worden voor, ik citeer: "officiële handelingen zoals de aanvraag van een geboorteakte of een medische verklaring, een adreswijziging enz., een bankrekening openen, uw belastingaangifte, een inschrijving aan een universiteit (ook in een ander land), een recept van uw dokter bewaren en in een ander EU-land afhalen, uw leeftijd bewijzen, een auto huren met uw digitaal rijbewijs, inchecken in een hotel."

Daarmee komen wel heel veel privacygevoelige data in één systeem samen, met alle risico's van dien. Deze wet legt hiervoor dus een stevig fundament, om het in de woorden van de staatssecretaris uit te drukken. Zo'n eID, oftewel een wallet, een digitale beurs, gaat dus al deze datakoppelingen bevatten. Wat gepresenteerd wordt als praktisch, is gevaarlijk als het in verkeerde handen valt, en bij de Europese Commissie is het bij uitstek in verkeerde handen.

Tevens kan de digitale identiteit gebruikt worden om vrijheidsbeperkende maatregelen te handhaven. Op de vraag in de memorie van antwoord of het identificatiemiddel ook benut kan worden voor coronamaatregelen zoals het vaccinatiepaspoort en testen voor toegang gaf de staatssecretaris aan dat, ik citeer: "toegelaten/erkende middelen gebruikt kunnen worden bij alle diensten die door de overheid worden aangeboden, dus ook voor de genoemde voorbeelden". En: "Dit betekent dat deze inlogmiddelen straks uiteindelijk gebruikt dienen te worden bij alle elektronische diensten die door de Nederlandse overheid worden aangeboden, dus ook overheidsdiensten in het kader van COVID-19 en daarmee het EU-covid-certificaat."

Dat is dus de onwenselijke kant van dit wetsvoorstel. Een basis voor een verplichte, Europese digitale identiteit, die alle persoonlijke data van burgers met elkaar verbindt, van belastingaangifte tot bankrekening tot coronatoegangspas en wellicht nog tal van andere mogelijkheden in de toekomst. Aan wie vertrouw je je eigen portemonnee, oftewel de digitale wallet toe? Niet aan de overheid en al helemaal niet aan de Europese Commissie. De PVV gaat voor baas in eigen beurs.

Kan de staatssecretaris dan ook aangeven waarom ze met deze wetgeving zo ver voor de Brusselse troepen uitloopt en de zaken niet beperkt zijn gebleven tot de kern van de zaak: de zaak op orde krijgen met een veilig en betrouwbaar inlogsysteem voor onze burgers? Dat is immers in de wereld van ICT en overheid al moeilijk genoeg.

Voorzitter, tot zover mijn eerste termijn.

De **voorzitter**:
Dank u wel, meneer Van Hattem. Wenst een van de leden in de eerste termijn nog het woord? Dat is niet het geval.

De beraadslaging wordt geschorst.

De **voorzitter**:
De behandeling van deze wetsvoorstellen wordt later vandaag voortgezet. Ik schors de vergadering voor enkele ogenblikken.

De vergadering wordt enkele ogenblikken geschorst.