Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2020–2021

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

J

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN EN DE HOGE COLLEGES VAN STAAT/ ALGEMENE ZAKEN EN HUIS VAN DE KONING [1]

Vastgesteld 29 september 2020

1. Inleiding

De leden van de **FVD**-fractie hebben het wetsvoorstel met belangstelling gelezen. Zij wensen nog een aantal vragen te stellen.

De leden van de fractie van **GroenLinks** hebben van het wetsvoorstel kennisgenomen. Zij hebben nog een aantal vragen.

De leden van de **D66**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en van de antwoorden van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties naar aanleiding van de commissiebrief van 10 juli 2020. Deze leden staan in beginsel niet afwijzend tegenover de inzet van de regering om een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op de verschillende niveaus te vormen. Toch hebben deze leden hierover nog een aantal zorgen, nadere vragen en opmerkingen naar aanleiding van de beantwoording van de Staatssecretaris op 31 augustus jl.[2] Op 30 juni 2020 heeft de vaste Kamercommissie voor Binnenlandse Zaken een deskundigenbijeenkomst in de Senaat georganiseerd. De regering is blijkens de brief van de Staatssecretaris van 31 augustus 2020 op de hoogte van wat de deskundigen aan kanttekeningen met betrekking tot het wetsvoorstel naar voren brachten. De leden van de D66-fractie zouden het op prijs stellen als de regering per deskundige op de geleverde kritiek zou willen reageren. Is zij daartoe bereid?

---

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

[2] Kamerstukken I 2019/20, 34 972, I.

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

De leden van de **PvdA**-fractie hebben kennisgenomen van het wetsvoorstel digitale overheid. Zij maken zich grote zorgen om de bescherming van de digitale identiteit van burgers en benadrukken het belang van de toegankelijkheid van nieuwe systemen ook voor mensen met minder doenvermogen. Zij hebben daarover verschillende vragen. Verder sluiten zij zich graag aan bij de vragen van de leden van de fracties van GroenLinks en ChristenUnie in paragraaf 2. De leden van de 50PLUS-fractie sluiten zich bij de vragen van de leden van de PvdA-fractie aan.

De leden van de **PVV**-fractie hebben van het wetsvoorstel kennisgenomen. Zij hebben een aantal vragen.

De leden van de **SP**-fractie danken de Staatssecretaris voor de reactie op de commissiebrief rondom de invoering van de Wet digitale overheid. Zij zijn echter verbaasd over de antwoorden. Zij menen een grote discrepantie te zien in de antwoorden van de Staatssecretaris ten opzichte van het huidige kabinetsbeleid.

De leden van de fractie van de **ChristenUnie** hebben met interesse kennisgenomen van het voorstel voor de Wet digitale overheid. Zij hebben hierover enkele vragen. De leden van de fracties van PvdD, 50PLUS en SGP sluiten zich bij deze vragen aan.

2. De Wet digitale overheid als Kaderwet

Op p. 24 van de memorie van toelichting staat als reden voor het regelen van de verwerking van persoonsgegevens bij algemene maatregel van bestuur het feit dat het voorstel het karakter heeft van een kaderwet. Dat is volgens de leden van de fractie van **GroenLinks** toch een toelichting die, samengevat, er een is van «het is een kaderwet omdat het een kaderwet is». Kan de regering hierop reageren? Volgens de aanwijzingen voor de regelgeving (artikel 2.23) moet delegatie van regelgevende bevoegdheid in de delegerende regeling zo concreet en nauwkeurig mogelijk worden begrensd. Wil de regering per onderdeel toelichten in welke mate de voorgestelde delegatie daaraan voldoet? De Raad van State stelt voor om een en ander in de wet zelf op te nemen omdat het anders te abstract wordt. Wil de regering dit advies alsnog opvolgen? De Raad van State wil zelfs een aantal centrale onderdelen van de generieke digitale infrastructuur (GDI) erin. Is de regering bereid om zich meer te schikken naar het advies van de Raad van State dan zij zich tot nu toe heeft gedaan? Waarom kiest de regering ervoor om als zaken als informatieveiligheid, het beheer van de infrastructuur, de toelating en erkenning van de aanbieders, de rechten en plichten die zij hebben, het beschermen van persoonsgegevens en het doorberekenen van kosten via algemene maatregel van bestuur te regelen? Graag ontvangen de aan het woord zijnde leden een argumentatie voor elk van deze onderdelen en een toelichting op de elementen waar ook subdelegatie («bij of krachtens algemene maatregel van bestuur») is toegestaan.

De memorie van toelichting stelt op p. 24 dat de Wet digitale overheid het karakter heeft van een kaderwet waarin hoofdzaken zijn geregeld, en dat het om reden van flexibiliteit opportuun is gedetailleerde (technische) uitwerking in de uitvoering vorm te geven. Ook wordt gezegd dat bij de nadere uitwerking de beginselen van proportionaliteit en subsidiariteit leidend zijn. De leden van de fractie van de **ChristenUnie** merken op dat het Jaarverslag 2018 van de Raad van State is kritisch met betrekking tot het gebruik van kaderwetgeving (hoofdstuk 1). Zij lezen:

«Kaderwetten bevatten vaak open normen die weinig rechtszekerheid bieden (...) Daardoor kan de rechter met vragen worden geconfronteerd over reikwijdte en toepassing. Handhaving en toezicht worden bemoeilijkt.» (p. 23).

Ook constateert de Raad dat op deze manier de wetgevende macht verschuift «van parlement naar regering, afzonderlijke ministers en private normstellers» (p. 23). «Zo geeft de wetgever zijn eigen macht uit handen en verliest hij aan betekenis. Deze rolopvatting van de wetgever zet het rechtsstatelijke kader – het fundament voor wetgeving – onder druk», aldus de Raad van State (p. 23). De leden van de fractie van de ChristenUnie vragen de regering om te reflecteren op deze kritische opmerkingen van de Raad van State in relatie tot de Wet digitale overheid als kaderwet.

In Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving wordt het primaat van de wetgever benadrukt. De leden van de fractie van de ChristenUnie lezen:

«Bij verdeling van de elementen van een regeling over de wet en algemeen verbindende voorschriften van lager niveau bevat de wet tenminste de hoofdelementen van de regeling. Bij de keuze welke elementen in de wet zelf regeling moeten vinden en ter zake van welke elementen delegatie is toegestaan, dient het primaat van de wetgever als richtsnoer.»

In de toelichting wordt benadrukt dat steeds moet worden onderzocht welke elementen van de regeling «zo gewichtig» zijn dat de volksvertegenwoordiging rechtstreeks bij de vaststelling moet worden betrokken. En, zo vervolgt de toelichting: «Aldus moeten ten minste de hoofdelementen van een regeling in de wet worden opgenomen.» De leden van de fractie van de ChristenUnie vragen de regering om aan te geven welke hoofdelementen van de Wet digitale overheid in de wet zijn opgenomen en welke elementen alleen in algemeen verbindende voorschriften van lager niveau zijn opgenomen.

In dit verband wijzen deze leden ook op het advies van de Raad van State om «de hoofdzaken van de Regeling voorzieningen GDI in de wet zelf op te nemen». Tevens stelt de Raad van State voor om de uitgifte van publieke identificatiemiddelen wettelijk te regelen en niet in lagere regelgeving. In haar reactie lijkt de regering deze adviezen niet in de strikte zin van de Raad van State op te volgen. Kan de regering uitleggen waarom niet gekozen is voor strikte opvolging van de adviezen van de Raad van State?

3. Standaarden, open source en (de)centrale opslag

Nederland kent een lange traditie aan technologische innovatie: van de eerste internetverbinding in 1988 tot het ontwikkelen van bluetoothtechnologie. De leden van de **FVD**-fractie hechten aan die Nederlandse voorloperspositie, ook op dit onderwerp. Kan de regering aangeven op welke wijze zij de Nederlandse concurrentiepositie en Nederlandse initiatieven en marktpartijen bij het ontwikkelen van vertrouwensdiensten ondersteunt? Welke rol speelt de Wet digitale overheid hierbij?

Waarom kiest de regering er bewust voor aanvullende zekerheden niet op te nemen in het kader, zoals open source, waar zij zelf een richtlijn op heeft voor overheidssoftware? Of decentraliteit, waarmee in ieder geval gegarandeerd is dat er geen centrale databases beheerd worden met

gevoelige persoonsgegevens die onderhevig zijn aan lekken, diefstal, verlies of oneigenlijke aanwending van persoonsgegevens?

Informatiebeveiliging wordt, zo stellen de leden van de **GroenLinks**-fractie vast, traditioneel bekeken vanuit de BIV-driehoek: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Is het vanuit deze benadering überhaupt wel wenselijk om private partijen nieuwe ruimte te geven in dit domein? Acht de regering bijvoorbeeld de grote Amerikaanse techbedrijven voldoende integer en vertrouwelijk? Waarom wel of waarom niet? Hoe denkt de regering hen te controleren zonder broncodes en open standaarden? Is de regering het eens met de leden van de fractie van GroenLinks dat concepten als open source van broncodes en privacy by design niet aantrekkelijk zijn voor private aanbieders? De regering verwacht dat door private aanbieders toe te laten de weerbaarheid en beschikbaarheid worden vergroot. Vreest zij niet dat er slechts enkele grote aanbieders zullen overblijven, zoals we bijvoorbeeld ook zien in de telecomsector en sociale media? Zo nee, waarom niet? En wordt het zogenoemde «aanvalsoppervlak» niet vele malen groter door het toelaten van private partijen? Heeft de regering overwogen om zelf meerdere systemen te ontwikkelen? Zo nee, waarom niet? Zorgt de keus voor private aanbieders er niet voor dat de overheid meer onderhoud en toezicht moet verzorgen? Hoe beoordeelt de regering het risico voor burgers die bij één partij een inlogmiddel voor alle diensten gaan gebruiken met alle persoonsgegevens van de desbetreffende persoon? Is de regering bereid in de wet op te nemen dat voor toelating van een inlogmiddel vereist is dat dit gebruik maakt van open source voor alle verwerking van persoonsgegevens en gebaseerd is op een decentrale structuur?

Klopt het dat bij de gecentraliseerde infrastructuur, zoals bij het eID, bedrijven die certificaten uitgeven precies kunnen zien waar mensen inloggen en welke documenten zij ondertekenen? Acht de regering dit wenselijk? Is de regering het met deze leden eens dat dit in inbreuk vormt op de privacy, zeker bij gevoelige transacties? Heeft de regering zicht op de toekomstige verdienmodellen? Mag er op enigerlei wijze geld verdiend worden met de data? Voor het publieke domein is verkoop van data niet toegestaan. Hoe kan de regering hier toezicht op houden of gaat zij simpelweg uit van vertrouwen? Ook profilering is niet toegestaan, maar zonder inzicht in de broncodes niet controleerbaar. Is de regering het hiermee eens? Hoe denkt de regering adequaat toezicht te kunnen houden of bijvoorbeeld op kredietwaardigheid wordt geprofileerd? Het Agentschap Telecom en de Autoriteit Persoonsgegevens zullen immers niet in de systemen van bijvoorbeeld Google mogen kijken. Of ziet de regering dit anders? Is open source van broncodes niet de eenvoudigste eis om adequaat toezicht te garanderen? Dit probleem doet zich niet voor bij decentrale systemen. Gaat de overheid actief uitdragen dat burgers hiervoor kunnen kiezen?

Is de regering bereid om het gebruik van pseudoniemen voor burgers toe te staan? Waarom heeft de regering hier niet louter voor gekozen?

De wet gaat uit van een centraal systeem en juist attributen voor inlogmiddelen voor individuen staan er niet in. Waarom is in 2017 het systeem van attributen losgelaten? Is de regering bereid, gelet op het lange voortraject van deze wet en de aanwezigheid, in tegenstelling tot 2017, van nieuwe attributenaanbieders, dit te heroverwegen? Is daardoor de wet niet feitelijk ingehaald door de tijd? Is de regering bijvoorbeeld bereid om in artikel 1 een zin toe te voegen waarin alsnog een definitie van een attributendienst wordt opgenomen, in artikel 5 de dienst als onderdeel van de generieke digitale infrastructuur toe te voegen aan het

eerste lid en als laatste in artikel 9 op te nemen dat attributendiensten worden toegelaten door verlening van een erkenning door de Minister? Wat is het gevolg dat privacy by design niet als voorwaarde is opgenomen in de wet?

Voorheen konden burgers met de overheid per brief communiceren. Met name ouderen, laagopgeleiden en laaggeletterden hechten hier veel waarde aan. In de digitale variant kan dat niet. Is de regering bereid na te denken om middels tweezijdig verkeer de mogelijkheid te openen om zowel via een fysiek loket als digitaal direct met een overheid te kunnen communiceren? Hoe kijkt de regering aan tegen een chatfunctie, zoals je bij veel bedrijven en zorgverzekeraars al ziet? Is de regering bereid toe te zeggen dat er een fatsoenlijke klachtbehandeling wordt verankerd in de wet, waarbij met name ouderen, laagopgeleiden en laaggeletterden meer worden ontzorgd? Is de regering bereid om financieel kwetsbare burgers tegemoet te komen in de kosten?

De regering heeft te kennen gegeven dat het van groot belang is dat de werking van processen transparant is, zodat deze controleerbaar zijn. Desalniettemin kiest zij niet voor het verplichten van open source software, zo constateren de leden van de **D66**-fractie. Waarom wil de regering niet in alle gevallen gebruikmaken van de kennis en kunde van een samenleving die meekijkt op de kwaliteit van de code en suggesties kan doen voor verbetering en de code kan aanpassen? Daarnaast vragen de leden van de D66-fractie of, en zo ja, welke onderdelen van closed source software door de aanbieders wel transparant aangeboden kunnen worden. Wanneer de broncode inzichtelijk is, hangt de waarborging van privacy, veiligheid en andere aspecten niet alleen af van de toezicht-houder. Hoe zorgt de regering voor transparantie in het geval van closed source software? En vindt de regering dat dit transparant moet zijn voor het publiek?

De leden van de D66-fractie vragen de regering of zij meer duidelijkheid over de uitgangspunten omtrent de vraagstelling centraal-decentraal wil geven. Verschillende sprekers hebben op de deskundigenbijeenkomst in verband met privacy en security gepleit voor een decentraal systeem en voor het werken met attributen. De regering sluit het gebruik van een decentraal systeem en het werken met attributen niet uit. De leden van de D66-fractie willen graag weten hoe de regering zorgt voor eenduidigheid. Deze leden krijgen sterk de indruk dat er aparte afspraken met de diverse aanbieders worden gemaakt over decentraal-centraal. Het gebrek aan eenduidigheid vraagt om meer toezicht. Hoe zorgt de regering ervoor dat de toezichthouder niet op verschillende obstakels stuit bij de controle op privacy, veiligheid en andere aspecten? En hoe gaat de regering om met een datalek als dit zich voordoet bij een centraal systeem?

De digitale bescherming van persoonlijke (inlog)gegevens is volgens experts het beste gediend met open source en decentrale opslag, zo stellen de leden van de **PvdA**-fractie vast. Wat is het oordeel van de regering over de volgende conclusie in het VNG-rapport Technische Analyse Digitale Identiteit van 11 september 2020, p. 31:

«Wat wel duidelijk is, is dat protocollen ... die voortkomen uit het meest recente paradigma van digitale identiteiten (het paradigma van de self sovereign identity), technisch gezien het meest kansrijk zijn om de beleidsdoelen te behalen, omdat deze protocollen de gebruiker centraal stellen en uitgaan van security by design.»

Deelt de regering deze conclusie? Zo nee, waarom niet? Zo ja, waarom hanteert zij deze niet als uitgangspunt bij de vormgeving van de Wet digitale overheid?

In de beantwoording van de vragen de commissie zegt de regering dat open source een mogelijkheid is, maar dat transparantie en veiligheid ook via closed source geborgd zijn door middel van afspraken met de leveranciers. De leden van de PvdA-fractie vragen de regering waarom niet gekozen is voor verplichte open source. De stelling in de brief van de regering dat open source mogelijk blijft, maar closed source ook kan, is geen antwoord op deze vraag. Volgens experts is open source veruit de beste garantie voor de bescherming van digitale identiteit van burgers. Zoals deskundige Marleen Stikker in een recente open brief aan de Eerste Kamer stelt: «Open source is een absolute voorwaarde. Bedrijven kunnen zo geen achterdeuren inbouwen en het is mogelijk voor een grote diversiteit van maatschappelijke actoren om daarop toe te zien.» Is de regering het met deze stelling eens? Zo nee, kan de regering uitleggen waarom volgens haar Marleen Stikker ongelijk heeft en open source geen absolute voorwaarde is? Zo ja, is de regering dan bereid in het toelatingskader voor private eID-middelen de verplichting op te nemen dat toetreding als aanbieder alleen mogelijk is indien de volledige broncode van alle applicatiesoftware die met persoonsgegevens omgaat gepubliceerd is en voor eenieder toegankelijk is om te beoordelen en te onderzoeken?

Een volgende vraag betreft de decentrale opslag van gegevens. In de beantwoording van de commissiebrief zegt de regering dat is gekozen voor een centraal noch decentraal systeem, maar dat eisen worden gesteld aan alle bij het eID-stelsel betrokken partijen. Om te weten of aan die eisen wordt voldaan, moet een toezichthoudend systeem in het leven worden geroepen. Waarom is, ten behoeve van een zo groot mogelijke bescherming, niet gekozen voor de verplichting te werken met decentrale opslag (op de eigen apparaten)? Kan de regering tevens uitleggen waarom bij de coronamelder wel is gekozen voor decentrale opslag en een gedistribueerd protocol, en in voorliggend wetsvoorstel niet?

Een laatste vraag betreft de toegankelijkheid. Kan de regering aangeven hoe dit wetsvoorstel voorziet in een goede toegankelijkheid van de voorzieningen voor mensen met minder doenvermogen?

De leden van de **PVV**-fractie stellen de volgende vragen. In het verslag van het schriftelijk overleg naar aanleiding van de deskundigenbijeenkomst stelt de Staatssecretaris:

«Het enkel beschikbaar zijn van een open source pakket «as is», dus zonder enige garantie op kwaliteit, zekerheid of zonder een transparant servicepakket, biedt geen meerwaarde. Daarom is ervoor gekozen om open source niet te verplichten en de eisen inzake veiligheid en continuïteit centraal te stellen.» ... «Ten aanzien van de veiligheid van closed source zullen met leveranciers afspraken gemaakt kunnen en moeten worden over het borgen van de veiligheid.»[3]

Kan de regering aangeven waarom dergelijke afspraken met leveranciers van closed source software over het borgen van de veiligheid niet zouden kunnen worden gemaakt met leveranciers van open source software?

[3] Kamerstukken I 2019/20, 34 972, I, p. 5.

In de deskundigenbijeenkomst hebben verschillende experts aangegeven dat voor de bescherming van de privacy van burgers het gebruik van open source de beste optie is en dit als harde eis zou moeten worden toegevoegd voor de toelating van eID-middelen.[4] Kan de regering uitleggen waarom niet gekozen wordt voor open source met toezicht vóóraf (door het Agentschap Telecom) in plaats van toezicht achteraf (door de Autoriteit Persoonsgegevens), waardoor het risico ontstaat van «dweilen met de kraan open»?

Kan de regering aangeven of zij bereid is om open source alsnog als enige standaard vast te leggen indien aanbieders van een open source pakket wél (aanvullende) garanties op kwaliteit, zekerheid en een transparant servicepakket kunnen leveren?

Verder stelt de Staatssecretaris in het verslag van het schriftelijk overleg:

«In dit verband wordt binnen het eID-stelsel ook de mogelijkheid geboden om met attributen (gegevenssets, zie artikel 1 van het wetsvoorstel) te werken.»[5]

Kan de regering aangeven waarom attributen slechts als «mogelijkheid» worden geboden in plaats als vaste standaard?

In de deskundigenbijeenkomst gaf mevrouw Bos van Stichting Lezen en Schrijven aan:

«Dit betekent dat er voor laaggeletterden veel keuzemogelijkheden zullen komen. Daardoor is de kans en het risico op oplichting binnen onze doelgroep groter.

(...)

Dit is een mooie ontwikkeling, maar die zorgt er wel voor dat er online extra handelingen zijn voor burgers die het toch al moeilijk vinden om online goed mee te kunnen komen. Door deze extra handelingen moeten zij meer stappen gebruiken en moeten zij hun inlog, die zij nu alleen voor semioverheidszaken gebruiken, ook opeens op commerciële pagina's gaan invoeren. Dit kan voor grote drempels zorgen.

(...)

Maar aan dit hoogste niveau van middelen zijn kosten verbonden. Het is net al een paar keer benoemd dat de vraag is of deze kosten er wel zouden moeten zijn. Maar zeker voor een doelgroep die vaker in de schulden zit en vaker onder de armoedegrens leeft, is het belangrijk dat deze kosten echt minimaal zijn. Als dit namelijk niet zo is, zullen laaggeletterden vaker kiezen voor een minder beveiligde optie. Daardoor zal er een ongelijkheid ontstaan tussen de groep burgers die hiervoor wel genoeg geld heeft en anderen die ervoor kiezen om hun geld uit te geven aan een pot pindakaas om thuis hun kinderen eten te kunnen geven.»[6]

Kan de regering aangeven in hoeverre bovenstaande risico's voor de betreffende doelgroepen worden ondervangen?

---

[4] Zie bijv. de opmerkingen van de heer Böhre (Privacy First) op p. 6, de heer Van Boheemen (Rathenau Instituut) op p. 14 en de opmerkingen van mevrouw Moerel (Tilburg University/ Cyber Security Raad) op p. 25 van het verslag van de deskundigenbijeenkomst (Kamerstukken I 2019/20, 34 972, G).

[5] Kamerstukken I 2019/20, 34 972, I, p. 7.

[6] Kamerstukken I 2019/20, 34 972, G, p. 19–20.

Met vallen en opstaan kwam onlangs de coronamelder app tot stand, zo stellen de leden van de **SP**-fractie vast. Wat het proces van deze app ons leerde, is dat veel bedrijven met goede bedoelingen leuke dingen bedenken, maar geen oog hebben voor de privacy en security van de gebruiker. Gelukkig leerde de Minister van VWS van dit traject en zette alsnog een andere route in, waarbij beide thema's wel de hoofdrol speelden. De voorliggende wet gaat de identiteit van onze burgers digitaliseren en geeft daar de kaders voor. Maar nu zullen niet alleen mensen met goede ideeën, maar ook partijen die in essentie andere belangen hebben dan die van het Nederlandse volk een product willen aanbieden en dus toegang willen tot de basisregistratie. De leden van de SP-fractie schromen niet om deze partijen bij naam te noemen. Onder andere Facebook en Google moeten keer op keer hun koers bijstellen omdat ze over de grenzen van de wetgeving zijn gegaan.

Een karige kaderwet is bij lange na niet voldoende om dit te borgen en de verwijzingen naar de Algemene verordening gegevensbescherming in de beantwoording van de vragen van de commissie laten zien dat er geen oog is geweest voor het grensoverschrijdende gedrag van deze partijen. Deze zeer machtige partijen, zo merken deze leden op, kunnen met veel middelen lange juridische procedures voeren, zijn buiten Europa gevestigd en kunnen daarmee de bescherming van de gegevens van de Nederlandse burgers in gevaar brengen. Om dit te borgen vragen de leden van de SP-fractie twee essentiële zaken op te nemen in deze kaderwet en niet over te laten aan de keuze van de aanbieder of een algemene maatregel van bestuur: open source en decentrale opslag.

In de beantwoording van de Staatssecretaris wordt gesteld dat closed source even zo veilig kan zijn als open source. Natuurlijk kan een gesloten oplossing net zo veilig zijn als een open, alleen moeten we dan de aanbieder op zijn blauwe ogen geloven. Bij open source kunnen we dit zelf controleren. Daar komt bij dat het ministerie zelf een beleidsnota heeft gepresenteerd waarin het stelt dat open source de norm moet zijn. Als er ergens ooit een wetsvoorstel is geweest waar dit voor geldt, dan is het wel dit wetsvoorstel. Hoe ziet de regering dit? Wil de regering vastleggen dat de aangeboden oplossingen open source moeten zijn?

De tweede vraag van de leden van de SP-fractie betrof decentrale opslag. Allereerst de vraag waar de attributen worden opgeslagen: centraal bij de aanbieder van de E-identificatie of decentraal bij de gebruiker? Maar dat zijn niet de enige data die verzameld zullen worden, want wanneer wij met onze Facebook ID mogen inloggen, kan Facebook niet alleen allemaal data van ons inkijken (waar log ik in?), maar die data ook opslaan, naast andere persoonsgegevens, zoals het burgerservicenummer (BSN). Wanneer dergelijke databases gehackt worden, is de ellende niet te overzien. Bij decentrale opslag kan er ook gehackt worden, maar dan is het leed wel te overzien. Wil de regering kiezen voor decentrale opslag?

Voorts vragen de leden van de SP-fractie de regering waarom er niet voor gekozen is om dit een publieke taak te laten zijn. Het verifiëren van iemands identiteit door middel van een check op de basisregistratie zou in de ogen van deze leden niet overgelaten moeten worden aan de markt. Maar wanneer de regering hier aan vast wil houden, dan zou een verstandige keuze zijn om geen aanbieders met een winstoogmerk toe te staan. Commerciële partijen hebben namelijk andere belangen dan puur een goed werkend product aan te willen bieden. De winsten hoeven zeker niet alleen uit inkomsten uit de applicatie te bestaan, vooral omdat meer geld verdiend kan worden met data. Wanneer ervoor gekozen wordt om commerciële partijen geen onderdeel te laten zijn, dan valt een belangrijk risico weg. Hoe ziet de regering dit?

Als laatste willen de leden van de SP-fractie meegeven dat dit iets is wat we niet aan het toeval moeten overlaten. Iedere bestuurder en passagier die in een auto stappen, gaan er vanuit dat er geen ongeluk zal gebeuren. Toch doen we de veiligheidsgordel om. Voor de leden van de SP-fractie is deze veiligheidsgordel hard nodig om goedkeuring te kunnen geven aan het wetsvoorstel. Zij kijken met verlangen uit naar de beantwoording van de regering.

De leden van de fractie van de **ChristenUnie** lezen in de memorie van toelichting dat de overheid mee moet gaan in de «digitale vaart der volkeren» om steeds meer diensten online te leveren. In haar visie vormt de Wet digitale overheid een eerste tranche van wetgeving ten behoeve van een verdere digitalisering van de overheid op verschillende niveaus. De memorie van toelichting stelt dat de onderhavige wet de meest urgente onderwerpen van regelgeving bevat (p. 1):

- de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid;
- het stellen van regels over informatieveiligheid;
- de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);
- de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen).

De memorie van toelichting spreekt over een «eerste tranche». Kan de regering aangeven welke tranches nog meer gaan volgen en hoe de verschillende tranches zich ten opzichte van elkaar verhouden? Anders gezegd, hoe ziet de structuur van het geheel van de wetgeving eruit? Dit roept ook de vraag op: kunnen de leden van de Eerste Kamer deze wet wel goed beoordelen als zij de andere tranches nog niet kennen?

De afgelopen jaren is de noodzaak van het gebruik van betrouwbare en veilige digitale identificatiemiddelen steeds urgenter geworden. Ondanks verschillende aanpassingen, zoals twee-factor-authenticatie en inloggen middels een applicatie, is het middel DigiD dringend aan vervanging toe. Ontwikkelingen in de markt nopen hier ook toe: consumenten willen steeds meer online zakendoen (in 2019 is de omzet van online winkelen met 7% gestegen). Tegelijkertijd is er geen zicht op een inlogmiddel vanuit de overheid en is het aanbod van digitale inlogmiddelen in de markt beperkt. Kan de regering aangeven welke rol de Wet digitale overheid speelt in het oplossen van dit urgente vraagstuk?

Is de Wet digitale overheid wel noodzakelijk, zo vragen de leden van de ChristenUnie de regering. Je kunt betogen dat de wet niet noodzakelijk is in het licht van de Algemene verordening gegevensbescherming en de Europese eIDAS-regeling voor elektronische identiteiten. Vanuit dit perspectief kun je ook betogen dat de Wet digitale overheid met name nodig is om private partijen de mogelijkheid te geven om via een centrale architectuur inlogmiddelen te ontwikkelen. Zou de regering kunnen reflecteren op dit betoog?

Daar komt het volgende bij. De Wet digitale overheid gaat uit van een centraal model waarbij inloggegevens (inclusief BSN) kunnen worden opgeslagen in de computersystemen van de leveranciers van de inlogmiddelen. Deze inloggegevens kunnen vervolgens door private partijen worden gebruikt voor het ontwikkelen van hun eigen business. Hoe kijkt de regering aan tegen dit dreigende gevaar, mede in het licht van kritische vragen over en onderzoeken naar de handel en wandel van grote techbedrijven?

Private partijen zullen voor dit soort inlogmiddelen twee typen verdienmodellen kunnen ontwikkelen. Het eerste verdienmodel is het laten betalen door de gebruiker, het tweede is gerelateerd aan alle persoonsgegevens die private partijen verzamelen om een nieuwe business te ontwikkelen. In dit model kan sprake zijn van het «verkopen van gegevens» maar ook het gebruiken van deze gegevens voor profilering en micro-targeting. De leden van de fractie van de ChristenUnie vragen de regering of zij overleg heeft gehad met private partijen over hun verdienmodel en wat daar uit gekomen is. Ook vragen zij of de huidige Wet digitale overheid het tweede verdienmodel volledig onmogelijk maakt. Indien het antwoord «ja» is, dan is de vraag hoe goed dit gehandhaafd kan worden met het oog op (machtige) private partijen. Een andere vraag is waarom private partijen eigenlijk dit soort inlogmiddelen zouden moeten aanbieden. Heeft het geen voorkeur alleen een of enkele publieke partijen toe te laten?

De leden van de fractie van de ChristenUnie merken op dat in de deskundigenbijeenkomst van 30 juni 2020 veel deskundigen hebben gewezen op de gevaren van de huidige Wet digitale overheid. Zo waarschuwde de heer Wolfsen van de Autoriteit Persoonsgegeven voor het feit dat deze wet onze «democratische rechtsstaat kwetsbaar [kan] maken». De heer Böhre van Privacy First waarschuwde voor de enorme risico's voor de privacy van burger gezien de «commerciële aard van de nieuwe eID-aanbieders, waaronder techbedrijven met dubieuze business modellen en schimmige profileringspraktijken». Zou de regering op deze mogelijke gevolgen kunnen reflecteren? Hoeveel garanties kan zij geven dat internationale ICT-giganten – die door hun omvang veel macht hebben – zich ook aan de regels gaan houden bij het aanbieden van inlogmiddelen in Nederland? Wat zou dat kunnen betekenen voor de Wet digitale overheid?

Tevens zien de aan het woord zijnde leden dat vrijwel alle deskundigen pleiten voor de opname van normen in de wet zelf. Onder andere worden de volgend normen genoemd: proportionaliteit en subsidiariteit (Wolfsen), decentrale structuur (Böhre, Van Bohemen, Moerel), open source (Böhre, Van Bohemen, Moerel), en doelbinding (Wolfsen, Böhre, Van Bohemen). In het memo «Onze digitale identiteit staat op het spel» van Waag. Technology & Society wordt expliciet gezegd dat twee normen in de wet zouden moeten staan. Als eerste open source en als tweede dataminimalisatie en lokale opslag. Zou de regering kunnen aangeven waarom zij het pleidooi van al deze deskundigen om belangrijke normen expliciet in de wet op te nemen niet heeft gevolgd?

De VNG heeft in het onderzoek Technische Analyse Digitale Identiteit een uitvoerig onderzoek gedaan naar protocollen en oplossingen die relevante functionaliteiten mogelijk maken en die alle veiligheidsrisico's mitigeren. De conclusie van de VNG is dat protocollen zoals IRMA, Sovrin en Trustchain het meest kansrijk zijn. De leden van de fractie van de ChristenUnie vragen of de regering bekend is met dit onderzoek, of zij de conclusie van dit onderzoek deelt en welke conclusies zij daar met betrekking tot de Wet digitale overheid uit zou willen trekken. Daar komt het volgende bij. Een initiatief als IRMA is van Nederlandse bodem en betreft een niet-commercieel initiatief. Hoe kijkt de regering naar dit initiatief? Zou dit een publiek alternatief kunnen zijn? En wat denkt zij van Sovrin en Trustchain?

Het rapport-Remkes (rapport van de Staatscommissie parlementair stelsel) benadrukt dat de overheid nabij de burger moet zijn. In tijden van digitalisering is dit met name belangrijk voor burgers die moeite hebben met lezen en schrijven. De leden van de fractie van de ChristenUnie

vragen de regering wat deze wet bijdraagt aan de nabijheid van de digitale overheid. Draagt deze wet bij aan een overheid die dichter bij haar burgers staat? Draagt deze wet bij aan het verminderen van de kloof tussen digitaal vaardige en niet digitaal vaardige burgers? In de deskundigenbijeenkomst kwamen twee aandachtspunten aan de orde: de klachtenregeling en machtigingsregeling. Hoe kijkt de regering naar deze onderwerpen? Is verbetering noodzakelijk? Zo ja, hoe gaat de regering dat vormgeven?

Kan de regering iets zeggen over de situatie in andere landen? Hebben die ook WDO-achtige wetten? Welke keuzen worden daar gemaakt met betrekking tot de software (centraal, decentraal, open source, closed source, et cetera)?

4. Elektronische identificatie (eID)

Wat is de noodzaak van een middel naast DigiD, zo vragen de leden van de **FVD**-fractie, als het op eenzelfde centrale manier beheerd wordt als het DigiD-stelsel, maar dan niet onder directe sturing/controle van de overheid geëxploiteerd wordt?

DigiD-aanbieder Logius trof verschillende maatregelen om het gebruik van profielen te voorkomen. In het huidige wetsvoorstel ontbreekt het echter aan regels om zulke maatregelen voor private eID's te verplichten, zo constateren de leden van de fractie van **GroenLinks**. Waarom heeft de regering dit niet minimaal zo stevig, of eigenlijk nog steviger door de groei van data verankerd?

5. Privacy en bescherming van persoonsgegevens

De leden van de **FVD**-fractie vragen of de regering kan garanderen dat deze Wet digitale overheid en het toelatingskader voor private middelen voorkomen dat data van personen via centrale verwerkers lekken, gestolen worden, dan wel oneigenlijk worden gebruikt.

De informatiebeveiliging bij de overheid laat nog vaak te wensen over, zo constateren de leden van de **GroenLinks**-fractie. Slechte beveiliging kan leiden tot datalekken, die bij de overheid meer impactvol kunnen zijn vanwege de veel aanwezige bijzondere of gevoelige persoonsgegevens. Welke mechanismen heeft de overheid ingebouwd om datalekken te voorkomen? Welke lessen zijn getrokken uit het verleden? Is hier documentatie van beschikbaar? Waarom heeft de regering niet gekozen om meer in te zetten op dataminimalisatie, privacy by design en privacy-attributed based identity? Garandeert de regering dat wordt gewerkt met de allerlaatste veiligheidsstandaarden en dat deze continu up-to-date worden gehouden? Hoe verklaart de regering dat de Wet digitale overheid leunt op een site die verouderde informatie en standaarden bevat en waarvan het lijkt dat deze niet (voldoende) actueel gehouden wordt terwijl dat essentieel is?

Het koppelen van bestanden en het voorkomen van schending van het beginsel van «doelbinding» is een belangrijke voorwaarde binnen de Algemene verordening gegevensbescherming, net als dataminimalisatie. Welke bestanden gaat de overheid koppelen en op welke wijze gaat dit gebeuren? Kan de regering hiervan een lijst geven? Het verzamelen van data moet tot een minimum beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Hoe heeft de regering daar binnen de verschillende facetten binnen de Wet digitale overheid rekening mee gehouden? Kan zij hiervan een exhaustieve lijst opsommen en

tevens uitleggen hoe zij kan garanderen dat de private aanbieders dit ook zullen doen?

Privacy by design en security by design liggen heel erg in elkaars verlengde, omdat data die je niet hebt ook niet kunnen lekken. Is de regering het met de leden van de fractie van GroenLinks eens dat een dergelijk model meer in de geest van de Algemene verordening gegevensbescherming is dan de huidige wetgeving, gelet op dataminimalisatie en privacy by design? En mocht de regering dit niet willen heroverwegen, hoe verhoudt zich dit dan tot het idee van informationele zelfbeschikking en de slogan «Regie op Gegevens» van het Ministerie van Binnenlandse Zaken zelf? Attributen lenen zich minder goed voor grootschalige hacks of heimelijke toegang, massale datalekken en function creep, oftewel sluipende doelverschuiving. Hoe ziet de regering dit en is de regering het met de leden van de fractie van GroenLinks eens dat juist de laatste jaren er in gevoelige domeinen een duidelijke verschuiving heeft plaatsgevonden van centrale naar decentrale infrastructuren, bijvoorbeeld op het terrein van biometrie en persoonsgegevens als het BSN? Hoe kan de regering garanderen dat er maximale standaardinzage, correctierecht en verwijderingsrecht worden verankerd, waarbij bij aanpassingen en verwijderingen deze in de gehele keten worden aangepast?

De leden van de **D66**-fractie vinden het zeer onwenselijk wanneer er een mogelijkheid is voor commerciële partijen om gevoelige data te vergaren door inloggegevens te koppelen. De Staatssecretaris geeft in zijn brief aan dat er doelbinding, onder meer in relatie tot private partijen, wordt opgenomen. Dit zou moeten voorkomen dat commerciële partijen inloggegevens kunnen misbruiken. De D66-fractie vraagt wie er verantwoordelijk is voor het vernietigen van onder meer inloggegevens als ze niet meer nodig zijn voor het doel, en hoe wordt gecontroleerd dat dit ook daadwerkelijk gebeurt. Een mogelijkheid om verkeerd gebruik van data aan de voorkant te voorkomen is door het verplichten van privacy by design, waardoor data niet verwerkt hoeven te worden. Waarom kiest de regering niet voor het verplichten van privacy by design? De leden van de D66-fractie missen in de brief de onderbouwing hiervoor. Dit is van wezenlijk belang omdat er mogelijk verdienmodellen aan verkeerd gebruik van data gekoppeld kunnen worden. Graag verzoeken de leden van de D66-fractie een reflectie van de regering op mogelijke verdienmodellen die gestoeld zijn op deze data.

In het verslag van het schriftelijk overleg met de Staatssecretaris lezen de leden van de **PVV**-fractie:

«Reden hiervoor is dat het van groot belang is dat gegevens die van burgers worden verkregen bij het inloggen bij de overheid alleen gebruikt worden voor het doel waarvoor ze verstrekt worden en niet anderszins, bijvoorbeeld als handelswaar.»[7]

Tijdens de deskundigenbijeenkomst stelde de heer Van Boheemen van het Rathenau Instituut in dit kader het volgende:

«In de nota van toelichting staat dat de verkoop van gegevens niet is toegestaan. Nu zijn er natuurlijk allerlei andere manieren om geld te verdienen met gegevens dan puur en alleen het verkopen van gegevens. Net werd al het profileren van mensen genoemd en het aanbieden van advertenties op basis van die profielen. Of denk aan kredietwaardigheidsscores en al dat soort zaken. In de nota van toelichting staat ook dat de

[7] Kamerstukken I 2019/20, 34 972, I, p. 6.

gegevens niet voor andere doelen mogen worden gebruikt, maar wij vragen ons af of het überhaupt mogelijk is om daarop toezicht te houden. Waarschijnlijk grote techbedrijven gaan een dienst aanbieden. Gaat een toezichthouder dan echt in hun systemen kijken hoe zij de profielen opstellen en of deze gegevens al dan niet gebruikt zijn? Is dat realistisch, vragen wij ons af, ook gezien de reputatie van deze partijen op dit gebied. Als de middelen niet open source zijn, dus als je niet in de bron kunt kijken, hoe kun je dit dan controleren als gebruiker van zo'n dienst?»[8]

Daarnaast sprak ook de heer Wolfsen van de Autoriteit Persoonsgegevens over de risico's van het koppelen met andere gegevens bij het inloggen en de uitwisseling van gegevens. Dit leidt bij de leden van de PVV-fractie tot de volgende vragen.

Kan de regering nader uiteenzetten in hoeverre in voorliggend wetsvoorstel voorkomen wordt dat er met gegevens geld wordt verdiend, anders dan het enkel verkopen van gegevens als «handelswaar»? Kan de regering tevens aangeven hoe daar toezicht op wordt gehouden en in hoeverre dit toezicht kan worden geëffectueerd bij grote techbedrijven, indien deze diensten gaan aanbieden? Kan de regering ook aangeven hoe voorkomen wordt dat er sprake kan zijn van koppeling van gegevens bij het inloggen (en daarmee het risico op profilering)? En kan de regering aangeven waarom niet expliciet wordt gekozen voor een decentraal systeem om daarmee profilering zoveel mogelijk te voorkomen? Graag ontvangen de aan het woord zijnde leden ook een toelichting hoe burgers effectief controle kunnen houden op de uitwisseling van gegevens.

Volgens de heer Böhre zou een decentrale opzet meer passen bij het idee van informationele zelfbeschikking conform de slogan «Regie op Gegevens» van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Kan de regering aangeven hoe de mogelijkheid voor een centrale opzet zich tot het «Regie op Gegevens»-concept van het ministerie verhoudt?

Kan de regering aangeven in hoeverre binnen het kader van deze wet voorkomen wordt dat (private) partijen gegevens opslaan op buitenlandse servers, wat gevolgen kan hebben voor de controleerbaarheid van (de omgang met) deze gegevens, waaronder zeer privacygevoelige gegevens zoals BSN en medische gegevens? In hoeverre acht de regering het risico aanwezig de regie te verliezen over de eigen digitale infrastructuur?

In het verslag van het schriftelijk overleg stelt de Staatssecretaris verder:

«In reactie hierop merk ik op dat het feit, dat privacy by design niet in het wetsvoorstel is opgenomen, niet betekent dat dit niet geldt voor eID en de aanbieders van inlogmiddelen. Dit beginsel, dat inhoudt dat er reeds bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd, is namelijk vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) en geldt per definitie voor verwerkingen van persoonsgegevens. EU-verordeningen zijn rechtstreeks toepasselijk in de lidstaten van de Europese Unie. Dat betekent dat zij niet hoeven en ook niet mogen worden omgezet in nationale regelgeving (overschrijfverbod). De – publieke en private – partijen die deel uitmaken van het eID-stelsel moeten derhalve zorgen dat zij aan de AVG voldoen. De wijze waarop dit gebeurt en de regelgeving die daarbij in acht moet worden genomen, zijn beschreven in de privacy-

[8] Kamerstukken I 2019/20, 34 972, G, p. 11.

visie eID, waaraan de commissie eerder refereerde. Privacy by design maakt daarvan onderdeel uit.»[9]

Bij de deskundigenbijeenkomst stelde mevrouw Moerel (Tilburg University/CSR) hierover:

«Privacy by design en security by design liggen heel erg in elkaars verlengde. Als je data niet hebt, kun je die ook niet kwijtraken, wat wel het beste beveiligingsmiddel is. Doordat privacy by design niet in die kaderwet staat en eigenlijk de opzet meer centraal is, komt natuurlijk de vraag op: houdt het AT dan bij de erkenning van een inlogmiddel daar toezicht op, terwijl dat in het inlogmiddel zelf moet zitten? Of gaat dan de AP – want de AVG is aanvullend van toepassing – er dan achteraf toezicht op houden of dat goed is gedaan? De vraag aan mij was: zeg iets over het toezicht. Ik hoop dat u ziet dat voorkomen beter is dan genezen en dat toezicht vooraf of een inlogmiddel voldoet aan de vereisten van privacy en security by design beter is, en dat het beter is daar ook toezicht op te houden zodat je de erkenning kan intrekken, dan dat je later, bij private partijen die global zijn en ondoorzichtig, als AP toezicht moet gaan houden om te kijken wat er gebeurt met de data.»[10]

Kan de regering aangeven in hoeverre naast privacy by design ook security by design bij dit wetsvoorstel wordt toegepast?

De regering stelt dat de gegevens goed worden beschermd omdat de Algemene verordening gegevensbescherming van toepassing is. Kan zij aangeven in hoeverre ook aan de «voorkant» wordt getoetst of aan de eisen van deze verordening wordt voldaan of dat dit toezicht alleen achteraf plaatsvindt? En kan de regering aangeven waarom er toch ingezet wordt op de mogelijkheid van een centrale opzet, terwijl juist volgens de moderne privacyvereisten op het gebied van privacy by design een decentrale architectuur meer voor de hand ligt, waarbij de kans op grootschalige hacks, heimelijke toegang, massale datalekken en sluipende doelverschuiving ook kleiner is?

In relatie tot dit wetsvoorstel wijzen de leden van de fractie van de **ChristenUnie** naar de ontwikkeling van de CoronaMelder. De ontwikkeling van deze app heeft geleid tot een maatschappelijke discussie met betrekking tot privacy. In de memorie van antwoord (18 september 2020[11]) benadrukt de regering dat privacy by design en dataminimalisatie zijn toegepast (p. 15). Ook benadrukt zij dat bij de ontwikkeling van de app de «grootst mogelijke transparantie [is] betracht om daarmee het vertrouwen in de werking, veiligheid en waarborgen van de privacy te vergroten» (p. 21). Met betrekking tot de eis van open source zegt de regering dat de transparantie in het gehele proces heeft bijgedragen aan het draagvlak voor de app. Daarbij noemt de regering niet alleen de transparantie met betrekking tot de broncode, maar ook met betrekking tot het ontwerpen, de architectuur en de inrichting van de informatiebeveiliging (p. 31). De regering bevestigt expliciet dat de CoronaMelder voldoet aan de eisen van privacy by design en open source (p. 32).

De leden van de fractie van de ChristenUnie vragen de regering welke lessen getrokken kunnen worden uit het maatschappelijke debat rond de CoronaMelder met betrekking tot normen als privacy by design, dataminimalisatie, lokale opslag, open source en transparantie. Wat zouden deze lessen kunnen betekenen voor de centrale architectuur binnen de Wet

---

[9] Kamerstukken I 2019/20, 34 972, I, p. 6.
[10] Kamerstukken I 2019/20, 34 972, G, p. 25.
[11] Kamerstukken I 2020/21, 35 538, C.

digitale overheid en voor de maatschappelijke acceptatie van de Wet digitale overheid? Is de regering het met de leden van deze fractie eens dat de maatschappelijke acceptatie van de Wet digitale overheid problematischer is omdat relevante hoofdelementen niet in de wet opgenomen zijn, maar al of niet als elementen in lagere regelgeving voorkomen?

De leden van de fractie van de ChristenUnie hebben ook vragen over de ethische aspecten van de COVID-app. De Minister van VWS heeft een aantal deskundigen gevraagd om een ethische analyse daarvan te geven en op basis van die analyse enkele aanbevelingen te doen. Hun rapport «Ethische analyse van de COVID-19 notificatie-app» identificeert tien kernwaarden. Deze leden vragen de regering welke kernwaarden ook van belang voor zijn de Wet digitale overheid, en in hoeverre die waarden in het onderliggende wetsvoorstel gerealiseerd zijn.

Ten slotte wijzen de leden van de fractie van de ChristenUnie op de dynamiek tussen innovatie enerzijds en ethische principes anderzijds. De vraag is: bepaalt innovatie de inhoud van ethische principes of geven ethische principes (mede) vorm aan innovatie? In de ethiek van de techniek wordt in het algemeen de opvatting gehuldigd dat ethische principes mede richting zouden moeten geven aan innovaties. Is de regering het met deze opvatting eens? Zo ja, wat zou dat betekenen voor de Wet digitale overheid in relatie tot kernwaarden in het voornoemde rapport?

6. Toezicht en handhaving

Het lijkt de leden van de **FVD**-fractie goed als het duidelijk is dat marktpartijen die gespecialiseerd zijn in veilig online handelen beschikbaar zijn voor burgers om zaken te doen met overheden en bedrijfsleven. Juist als deze partijen zich richten op het veilig houden van de informatie voor de burger los van de partijen waar zij zaken mee doen versterkt dit de positie van de burger. Want er kan natuurlijk ook een belangentegenstelling zijn tussen de burger en de overheid. Wat dan wel geborgd moet zijn, is dat deze partijen gedwongen zijn zich te houden aan strenge regelgeving (standaarden) en goed toezicht. De leden van de FVD-fractie vragen de regering in hoeverre de Wet digitale overheid toeziet op het handhaven van de hoogste veiligheids- en privacy-standaarden. Dit mag niet ondermijnd worden doordat sommige lidstaten een ander idee hebben over kwaliteit en handhaving. Kan de regering toelichten op welke basis, naast de Algemene verordening gegevensbescherming, kan worden gehandhaafd? Welke rol speelt hierbij de eIDAS-verordening? Worden er ook andere standaarden gewogen bij het toelaten van dit soort (vertrouwens)diensten in Nederland? Tot slot, hoe ziet de regering de rol van het Agentschap Telecom bij het implementeren van deze wet en of deze wet er inderdaad voor gaat zorgen dat de kracht van de normen in Nederland overeind blijft?

In welk licht, zo vragen de leden van de fractie van **GroenLinks**, ziet de regering de huidige tekorten bij de Autoriteit Persoonsgegevens gelet op de Wet digitale overheid? Acht zij de Autoriteit in staat om op voldoende adequate wijze haar taak uit te voeren op het gebied van toezicht van de digitale overheid? Is zij bereid de Autoriteit beter te faciliteren, mocht de wet in deze vorm worden aangenomen?

Hoe gaat de regering de governance vormgeven en hoe zal de informatie-uitwisseling met de toezichthouder tot stand worden gebracht? Waarom heeft de regering gekozen voor een verschillend normenstelsel voor bedrijven en burgers? Maakt dit het niet onnodig ingewikkeld voor de toezichthouder? Het Agentschap Telecom is aangewezen als toezicht-

houder. Overweegt de regering de toelating door een andere partij te laten doen of is het Agentschap Telecom hiervoor de meest logische partij? Hoe gaat de regering adequate handhaving vormgeven? Welke bevoegdheden gaat zij bij welke partijen beleggen, zoals bijvoorbeeld intrekking van toelating?

De leden van de **D66**-fractie constateren dat de Raad van State heeft gewezen op de noodzaak van voldoende ICT-expertise bij de overheid. Kan de regering aangeven op welke manier dit advies van de Raad van State is overgenomen? Hoe wordt het kennisniveau ook op de lange termijn gegarandeerd? En kan de regering aangeven in hoeverre de aanbevelingen van de tijdelijke commissie ICT uit de Tweede Kamer onder leiding van voormalig Kamerlid Ton Elias zijn uitgevoerd?

De heer Derksen van het Agentschap Telecom (AT) gaf, zo constateren de leden van de **PVV**-fractie, tijdens de deskundigenbijeenkomst aan:

«Dat betekent voor de uitvoering van ons toezicht dat wij goed zicht moeten hebben op het stelsel waarbinnen de inlogmiddelen hun werk moeten doen. Onder de wet DO is dit niet het geval en dat betekent dat de overheid, in dit geval het ministerie, een goede governance neer moet zetten en de informatie-uitwisseling met de toezichthouder goed op orde moet hebben. Daarover zijn we in gesprek, dus dat is een aandachtspunt.»[12]

Kan de regering aangeven hoe van deze wet verwacht kan worden uitvoerbaar en handhaafbaar te ze zijn als deze voor de toezichthouder cruciale aspecten ontbreken? Kan de regering tevens aangeven wat de meest actuele stand van zaken is van het overleg tussen het ministerie en het Agentschap hierover en welke consequenties dit eventueel heeft voor voorliggend wetsvoorstel? Kan de regering aangeven waarom een duidelijk toelatingskader binnen de wet ontbreekt en waarom dit niet middels wetgeving geregeld wordt?

In de huidige voorstellen houdt het Agentschap Telecom toezicht op een deel van de Wet digitale overheid. De leden van de fractie van de **ChristenUnie** hebben daar vragen over. Wie houdt toezicht op die delen waar het Agentschap niet verantwoordelijk voor is? En wie houdt toezicht op het geheel? Krijgen de toezichthouders ook de benodigde bevoegdheden? Wat is de relatie tussen toelating versus toezicht? Hoe kan voorkomen worden dat (private) partijen toegelaten worden waarvan later blijkt dat ze niet aan de eisen van bijvoorbeeld doelbinding of bescherming van persoonsgegevens voldoen?

Sommige deskundigen, vooral vanuit het bedrijfsleven, wijzen erop dat de openbaarheid van de software ook kan leiden tot een verzwakking van de veiligheid. Bijvoorbeeld wanneer ze geïnstalleerd worden op telefoons die (iets) verouderd zijn waardoor de open source software niet in een veilige omgeving kan opereren. Zij wijzen erop dat is dit soort situaties het verstandiger is als de software gesloten is. Kan de regering hierop te reflecteren? Om hoeveel telefoons gaat het? Pleit het bedrijfsleven voor gesloten software omdat er sprake is van een terechte zorg of om inzicht in het eigen handelen en functioneren te vermijden? Deze leden vragen de regering ook of in die situaties waarin open source niet wenselijk is, toch geborgd kan worden dat de software van deze partijen, die onder de Wet digitale overheid vergund zijn, op orde is. Bijvoorbeeld door audits van onafhankelijke partijen. Welke mogelijkheden ziet de regering daarvoor? Hoe vertrouwenwekkend is zulke toetsing zonder transparantie?

---

[12] Kamerstukken I 2019/20, 34 972, G, p. 24.

Daarnaast vragen zij of het niet mogelijk is om vooraf ten tijde van toelating de toezichthouder te laten toetsen op de naleving van de in de Algemene verordening gegevensbescherming gestelde eisen, waaronder privacy by design. Dit is nu al gebruikelijk in de systematiek van toelating en toezicht onder de eIDAS-verordening.

De commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning ziet met belangstelling uit naar de memorie van antwoord en ontvangt deze graag binnen **vier weken** na vaststelling van dit voorlopig verslag.

De voorzitter van de commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/ lgemene Zaken en Huis van de Koning,
Dittrich

De griffier van de commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis van de Koning,
Bergman