Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1016

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 8 mei 2023

De vaste commissie voor Digitale Zaken heeft op 5 april 2023 overleg gevoerd met mevrouw Van Huffelen, Staatssecretaris Koninkrijksrelaties en Digitalisering, over:

- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 29 september 2022 inzake generiek kader voor vitale digitale processen van de overheid (Kamerstuk 26 643, nr. 917);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 10 november 2022 inzake update hack bij ID-ware (Kamerstuk 26 643, nr. 936);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 22 november 2022 inzake informeren burgers over verhoging authenticatieniveau (Kamerstuk 26 643, nr. 942);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 18 november 2022 inzake Facebook Pages DPIA en HRIA (Kamerstuk 32 761, nr. 252);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 16 januari 2023 inzake broncode DigiD-app openbaar gemaakt (Kamerstuk 26 643, nr. 960);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 24 januari 2023 inzake beleidsreactie advies Autoriteit Persoonsgegevens inzake het Rijksbreed cloudbeleid 2022 (Kamerstuk 26 643, nr. 965);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 24 januari 2023 inzake implementatiekader risicoafweging cloudgebruik 2022 (Kamerstuk 26 643, nr. 964);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 7 maart 2023 inzake publicatie Woo-besluit inzake documenten over de hack bij ID-ware (Kamerstuk 26 643, nr. 981);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 20 februari 2023 inzake vertaling data protection impact assessment (DPIA) en human rights impact assessment (HRIA) (Kamerstuk 32 761, nr. 262);**

kst-26643-1016
ISSN 0921 - 7371
's-Gravenhage 2023

– **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 21 maart 2023 inzake maatregelen over het weren van apps op mobiele devices van rijksambtenaren (Kamerstukken 26 643 en 30 821, nr. 984).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,
Kamminga

De griffier van de commissie,
Boeve

Voorzitter: Dekker-Abdulaziz
Griffier: Boeve

Aanwezig zijn zes leden der Kamer, te weten: Bouchallikh, Dekker-Abdulaziz, Leijten, Rahimi, Slootweg en Van Weerdenburg,

en mevrouw Van Huffelen, Staatssecretaris Koninkrijksrelaties en Digitalisering.

Aanvang 10.00 uur.

De **voorzitter**:
Goedemorgen. Ik open de vergadering van de vaste commissie voor Digitale Zaken. Vandaag spreken we over informatiebeveiliging bij de overheid. Ik heet de Staatssecretaris Digitalisering, Alexandra van Huffelen, welkom. Ik heet de Kamerleden die aanwezig zijn ook welkom. Dat zijn mevrouw Van Weerdenburg van de PVV, de heer Rahimi van de VVD, mevrouw Bouchallikh van GroenLinks en de heer Slootweg van het CDA. Ik voer zelf aan het eind ook nog het woord. We spreken vier minuten spreektijd en twee setjes interrupties van twee af. Ik geef het woord aan mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Vandaag spreek ik weer mede namens BVNL.
Ik ga proberen om er geen rommeltje van te maken, maar eerlijk gezegd heb ik wel moeite gehad met de voorbereiding van dit debat. Er staan namelijk veel stukken op de agenda, die ook allemaal belangrijk zijn. We zitten al een tijdje met een DPIA en HRIA over Facebook. We hebben die lang voor ons uitgeschoven. Vandaag staan die eindelijk op de agenda. Eerlijk gezegd vond ik het sowieso moeilijk om me in vier minuten toe te spitsen op de punten waarover ik vragen heb bij een best belangrijk Engels stuk van zo'n 160 pagina's met hele taaie kost. Dat stuk is juridisch-technisch namelijk best ingewikkeld.
Toen bedacht ik dat de reden dat het indertijd in het Engels naar de Kamer is gestuurd, was omdat de Staatssecretaris heeft gezegd dat ze dat dan direct kon delen met haar Europese collega's. Daar nam ik al een beetje aanstoot aan. Er werd ons echter een vertaling toegezegd, dus ik dacht: oké. Vervolgens hebben we drie maanden gewacht. In februari kwam eindelijk de vertaling.
Tot mijn verbazing zag ik van de week pas dat het geen vertaling van die 160 pagina's is, maar een Nederlandse samenvatting in jip-en-janneketaal van 9 pagina's. De redenering om dat in begrijpelijke taal, in jip-en-janneketaal, te doen, is omdat de Staatssecretaris het belangrijk vindt dat de inhoud van het document begrijpelijk is voor een breed publiek. Dat vind ik natuurlijk heel goed. Dat zouden ze vaker moeten doen met Kamerbrieven. Alleen, het probleem is nu dat wij als Kamer over een best wel inhoudelijk stuk ... Dat stuk is belangrijk, omdat de beslissing die hieraan hangt, best wel grote gevolgen kan hebben. We hebben het er namelijk over of de Facebookpagina's van de overheid wel of niet blijven bestaan. De overheid bereikt daar namelijk 5,5 miljoen Nederlandse burgers mee. Ik vind dat dus nogal wat.
We hebben natuurlijk al eerder tegen de Staatssecretaris gezegd dat we hier eerst over willen spreken voordat er besluiten over worden genomen. Nu spreken we erover, maar eigenlijk vind ik niet dat wij een stuk hebben gekregen op basis waarvan wij als Kamer een gesprek kunnen voeren met deze bewindspersoon. De Engelse versie van het stuk is namelijk voor de Europese collega's. Vervolgens is de Nederlandse samenvatting – ik weiger dit een vertaling te noemen – voor het publiek. Dat is op zich goed. Maar de Kamer dan? Wat moeten wij dan?

Natuurlijk, ik heb het Engelse stuk wel gelezen. Nogmaals, ik vond het heel moeilijk om daardoorheen te komen. Maar goed, dat is nou eenmaal het karakter van dat soort stukken. Maar om dit goed te kunnen bespreken ... Ik heb er echt moeite mee om dat stuk te vertalen in een spreektekst waar ik maar vier minuten voor heb. Ik heb daar gewoon heel veel vragen over. Die kan ik niet allemaal stellen.
Eén. Is de Staatssecretaris bereid om een volledige vertaling van het Facebook-DPIA naar de Kamer te sturen? Kan zij dat toezeggen? Ik hecht daar namelijk echt aan. Ik kijk de collega's even aan. Daar moeten we gewoon echt op staan als Kamer. Wil de Staatssecretaris dat dus alsnog doen? Dan kunnen we daar op een later moment ook nog inhoudelijk over spreken.
Verder wil ik graag van haar weten hoe de onderhandelingen met Meta gaan. Ze zijn namelijk in gesprek. Hoe staat het ermee? Naar mijn weten zou er in het eerste kwartaal van dit jaar een besluit genomen worden of zouden daar uitkomsten van zijn. Ik heb echter nog niets gezien. Ik hoorde via via dat de Staatssecretaris in januari op de radio heeft gezegd dat het pas eind dit jaar wordt. Graag had ik daar ook eventjes wat over gehoord. Ik wil daar dus graag even duidelijkheid over.
Voorzitter, ik rond af. Wie heeft de Nederlandse samenvatting gemaakt? Uit de beslisnota blijkt namelijk dat de opstellers van het rapport ook de samenvatting hebben gemaakt. Dat hebben zij gedaan aan de hand van openbare informatie. Dat begrijp ik ook niet helemaal.
Tot zover, voorzitter.

De **voorzitter**:
Dank. Ik geef nu het woord aan de heer Rahimi.

De heer **Rahimi** (VVD):
Dank u wel, voorzitter. Allereerst felicitaties aan mevrouw Leijten. Zij is namelijk politicus van het jaar. Ik vind het toch mooi om dat even te benoemen. Ik hoop dat dit niet van mijn tijd af gaat.
Voorzitter. Geen vrijheid zonder veiligheid, zowel fysiek als thuis. Daar staat de VVD wat mij betreft ook voor. Als er ingebroken wordt, dan weet je wat er gestolen wordt. Dat gebeurt echter ook digitaal. Je weet niet wat er digitaal gestolen wordt. Wat je thuis hebt, dat is van jou. Wat wij hier hebben van burgers en ondernemers is van hen. Beveiliging van IT-systemen is dus superbelangrijk.
Voorzitter. In de brief van 29 september 2022 is toegezegd dat informatiebeveiliging bij de overheid een wettelijke status krijgt. Wat is de stand van zaken? Komt daar aparte wetgeving voor of gaan we wetgeving aanpassen? Zo ja, welke? Op pagina 2 staat ook iets anders. Daar heb ik een vrij technische vraag over, dus ik hoop dat ik daar antwoord op kan krijgen. Er staat: «Daardoor komt de focus meer te liggen op feitelijk beveiligen in plaats van administratief beveiligen.» Kan de Staatssecretaris dit specificeren? Kan zij toelichten wat daarmee bedoeld wordt met betrekking tot de BIO? Is de Staatssecretaris voornemens om ook te kijken naar concrete richtlijnen vanuit de VS? Is zij voornemens om die in ogenschouw te nemen? Daarmee bedoel ik bijvoorbeeld de zerotrust-policy op apps, netwerk en al die onderdelen.
Voorzitter. Daarnaast hebben we de hack bij ID-ware, waarbij de gegevens van de rijkspassen van Kamerleden en ambtenaren van de Eerste en de Tweede Kamer op straat lagen. De getroffenen zijn bericht via een brief. Er zijn verschillende maatregelen genomen. Wij vroegen ons wel af aan de hand waarvan is bepaald dat alles goed geregeld is en dat de veiligheid van de getroffenen geborgd wordt. ID-ware geeft ook aan dat zij maatregelen hebben genomen en dat zij gaan monitoren om herhaling te voorkomen. Wij zijn benieuwd welke maatregelen zijn genomen. Daar zien wij namelijk niet veel over staan. Ik vind dat belangrijk. Fouten maken kan. Dat hebben we natuurlijk liever niet, maar je leert er wel van. Andere

ministeries en andere overheidsinstanties kunnen daar ook van leren, zodat ze fouten kunnen voorkomen. Dat zijn momenten om dingen te leren. Dan worden daar in ieder geval geen fouten meer gemaakt.
Voorzitter. Dan DigiD. Dat is zeker belangrijk bij het vorige agendapunt. De kwetsbaarheid van overheidssystemen is zeer cruciaal. De technische en organisatorische fouten op authenticatie en autorisatie in DigiNotar – ik weet niet of jullie dat nog allemaal kennen – waren best heftig. Hoe stellen we met een hoge mate van zekerheid vast dat de DigiD-app voor 99,9% veilig is?
Voorzitter. De broncode van de DigiD-app is na een Woo-verzoek openbaargemaakt. DigiD moet voor iedereen veilig zijn, vinden wij. Hoe is dat gewaarborgd? Enkele fragmenten van die broncode kunnen echt een beveiligingsrisico hebben. Er moet een continuïteit zijn op het gebied van de veiligheid daarvan. Het moet blijven werken. Denk daarbij ook aan informatie over infrastructuur en waar de app op draait. Dat is best een risico voor hackers. Hoe gaat de overheid om met dit soort Woo-verzoeken? Dat geldt ook voor andere applicaties. Wat mij betreft is het: Woo tot hier en niet verder. Niet alles hoeft altijd openbaar.
Ik ga wat dingen overslaan, voorzitter. Dat is het nadeel van een IT'er.

De **voorzitter**:
Sorry, ik wil heel graag een interruptie plaatsen, mag dat? Ja? Oké.
Hoor ik de VVD nou zeggen dat de opensourcecode niet openbaar hoeft? We hebben namelijk met z'n allen afgesproken dat de code wel onder de Woo valt. Kan de VVD daar toch heel eventjes op reflecteren?

De heer **Rahimi** (VVD):
Ik maak me als IT'er zorgen om het volgende. We willen alles openbaar hebben. Dat lijkt soms goed, maar soms kan het ook best dingen prijsgeven over de infrastructuur die wij hebben, de codes die wij gebruiken en de parameters die worden doorgestuurd. Daar kan een hacker best wel wat mee. Daar kan een regering ook best wel wat mee. Daar maak ik me gewoon zorgen om. Ik vind dat openbaarheid goed is. We moeten wel echt naar het volgende kijken. De broncode van de DigiD-app is gepubliceerd op GitHub. Daar kan iedereen bij. Daar zitten letterlijk fragmenten bij waarop «security» staat. Dat kan ervoor zorgen dat sommige dingen eruit worden gehaald. Iemand kan dan iets bouwen. Denk even aan de websites met phishing. Dan staat er: log in op Mijn ING. Als jij die code hebt, dan kan jij als programmeur dingen ontwikkelen. Als je net iets te veel info hebt, kan je dingen neerleggen. Over een paar jaar hebben we dan heel veel narigheid. Daarom zei ik ook, voor de grap: Woo tot hier en niet verder. Dit soort dingen moeten we niet doen.

De **voorzitter**:
Ik zie een interruptie van mevrouw Van Weerdenburg. O, de openingsbel van de vergadering gaat. Die wachten we even af.
Dat was de vergaderbel. De heer Rahimi gaat verder met zijn betoog.
O, nee, sorry. Mevrouw Van Weerdenburg heeft nog een interruptie.

Mevrouw **Van Weerdenburg** (PVV):
Ik wil de heer Rahimi vragen: als de broncode openbaar is en iedereen meekijkt, komt het dan ook niet vaak voor dat daardoor eventuele fouten of zwakheden worden verbeterd? Die worden dan namelijk gesignaleerd.

De heer **Rahimi** (VVD):
Als oud-IT'er zou ik zeggen dat het echt heel slechte software is. Ik zou die niet laten testen door mensen. Dan is je hele watervalstraat – ik verval even in oude IT-termen – niet goed geweest. Dat wil je gewoon niet. Als je fragmenten publiceert van die broncode, kun je zaken herleiden. Daarmee kan je ook dingen doen waardoor je bij privacygevoelige gegevens komt.

Dat is mijn angst. Ik vind dat de software die wij maken goed moet zijn. Die moet goed getest zijn. Anders moet je die niet publiceren. Als die gepubliceerd is, dan wil ik niet uitgaan van mensen die die dan testen, waardoor we fouten ontdekken. Ik zei al dat als er thuis ingebroken wordt, je eigen spullen dan gejat worden. Het gaat hier echter om gegevens van burgers. Er moet dus gewoon geen fout in de software zitten. Deze broncode geeft heel veel informatie aan heel veel mensen en aan heel veel overheden, waarmee zij dus veel dingen kunnen doen. Dat is mijn angst.

De **voorzitter**:
De antwoorden mogen puntiger. De heer Rahimi gaat verder met zijn betoog.

De heer **Rahimi** (VVD):
Voorzitter. Omdat software continu evalueert en aan kwetsbaarheid onderhevig is, vinden we de volgende vraag ook relevant. Is de broncode onderhevig aan ons eigen responsible disclosure programme? Daar wordt in de notities niets over gezegd.
Voorzitter, als laatste. Ik heb die 160 pagina's in het Engels wél gelezen. Ik heb daar toch wel een aantal vragen over. Ik denk dat de conclusie goed is. Ik denk dat het goed is dat we in gesprek blijven. Ik vind het goed dat de Nederlandse overheid dat doet. Ik moet wel zeggen dat de Facebook-pagina's niet groter zijn dan die van elke andere overheid. Mijn laatste vraag is hoe het met andere socialmediaplatforms zit. Hoe bewaken wij de oplossingen van de in 17.1 genoemde maatregel op de zeven hoge risico's?
Ik moet afronden.

De **voorzitter**:
Ik zie nog een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Ik heb een vraag aan de heer Rahimi. Hij had ongetwijfeld heel veel meer vragen over het Facebook-DPIA. Ik zie hem knikken. Ik kan u er helaas ook geen vijf minuten bij geven. Is hij bereid zich te voegen bij het verzoek van de PVV en BVNL om een volledige, volwaardige Nederlandse vertaling? Dan kunnen we namelijk op een later moment, in een apart commissiedebat zodat we wat meer tijd hebben, op de materie ingaan. Is hij bereid om zich te scharen bij dat verzoek aan de Staatssecretaris?

De heer **Rahimi** (VVD):
Zeker, aangezien ik nog negen vragen had over dat punt. Ik had zelf ook nog vragen over Google en andere dingen. Ja, dat verzoek zal ik dus zeker steunen.

De **voorzitter**:
Ik zie verder geen interrupties meer. Dan geef ik het woord aan mevrouw Bouchallikh, GroenLinks.

Mevrouw **Bouchallikh** (GroenLinks):
Dank, voorzitter. Deze bijdrage is mede namens de PvdA. «Het Ministerie van Privacy» bestaat niet, maar ik vond het wel mooi gevonden. Met die naam werd in opdracht van het ministerie een testaccount op Facebook gemaakt om te onderzoeken wat de risico's zijn. Goed dat dit gedaan is, want de risico's zijn groot. Daar kom ik later op terug.
Eerst een ander punt over waarom privacy zo belangrijk is. De afgelopen twee weken zagen we namelijk – weliswaar niet bij de overheid maar bij bedrijven – hoe verkeerd het kan gaan als informatie en in dit geval persoonsgegevens niet goed genoeg beveiligd zijn en via een datalek op

straat komen te liggen. Het is dus erg belangrijk dat bedrijven, maar zeker ook overheden, zorgen dat hun informatiebeveiliging goed op orde is. Kan de Staatssecretaris aangeven of ook overheden samenwerken met het bedrijf waarvan nu zo veel gegevens zijn gelekt? Hoe zorgen overheden dat de informatiebeveiliging op orde is bij de externe bedrijven waarmee zij samenwerken?
In het verlengde hiervan de vraag bij wie de verantwoordelijkheid precies ligt voor het waarborgen dat IT-producten voldoen aan de wet- en regelgeving en de standaarden voor informatiebeveiliging. Wat GroenLinks betreft moet die verantwoordelijkheid liggen bij de leveranciers van IT-diensten. Zij moeten actief kunnen aantonen dat hun diensten voldoen aan onze voorwaarden. Deelt de Staatssecretaris dit uitgangspunt?
Voorzitter. Ik kom op social media. Er wordt al langere tijd terechte kritiek geuit op het gebruik van socialmediaplatforms zoals Facebook en TikTok. De Staatssecretaris heeft ons een zogeheten data protection impact assessment en een human rights impact assessment toegestuurd die zijn uitgevoerd op het gebruik van Facebookpagina's door de overheid. Hieruit komen grote risico's naar voren en voorstellen voor maatregelen. Wat gaat de Staatssecretaris precies met alle aanbevelingen doen? GroenLinks is van mening dat er stevige regulering nodig is van de digitale wereld. We moeten af van de gedachte dat de techbedrijven zichzelf kunnen reguleren. De regie moet worden teruggepakt. De EU Digital Services Act is wat ons betreft daarom ook erg belangrijk. Hiermee moeten overheden de veel te grote rol van de techplatforms inperken en onze persoonsgegevens beter beveiligen. Kan de Staatssecretaris aangeven hoe het met de Digital Services Act staat? Denkt zij dat met de komst hiervan de informatiebeveiliging ook substantieel verbetert?
Tot slot op dit vlak nog één punt. Zowel social media als bijvoorbeeld clouddiensten zijn erg vaak afhankelijk van bedrijven van buiten de EU. Dit levert extra risico's op voor onze informatiebeveiliging. Ziet de Staatssecretaris mogelijkheden om als Europa digitaal autonomer te worden door technische ontwikkelingen hier te stimuleren, zodat we in Europa in de toekomst ook meer voor Europese aanbieders kunnen kiezen?
Voorzitter. Ook de decentrale overheden en de uitvoeringsorganisaties bezitten veel persoonsgegevens van inwoners. Het is daarom erg belangrijk dat ook zij goede informatiebeveiliging hebben. Wij krijgen echter vanuit decentrale overheden soms bezorgde signalen dat zij onvoldoende capaciteit en middelen hebben om alles goed op orde te krijgen. Kan de Staatssecretaris garanderen dat gemeenten, provincies en waterschappen voldoende middelen hebben? Of ziet zij ook knelpunten? Wat gaat zij eraan doen om hen te ondersteunen?
Verder geven de decentrale overheden zelf ook aan dat zij zich zorgen maken over de hoeveelheid nieuwe wetgeving op het gebied van digitalisering die op hen afkomt. Kan de Staatssecretaris hen en ons als Kamer geruststellen dat de andere overheden de noodzakelijke acties die voortvloeien uit de wetgeving goed kunnen implementeren?
Voorzitter. Tot slot nog een vraag over het cloudbeleid. De Autoriteit Persoonsgegevens heeft afgelopen najaar een advies uitgebracht over het rijksbrede cloudbeleid. In de kabinetsreactie op dit advies schrijft de Staatssecretaris dat overheden die niet tot de rijksdienst behoren, geadviseerd wordt zich aan dat beleid te houden. Maar zij zijn daartoe niet verplicht. Zou het niet logisch zijn dat de richtlijnen die we hebben opgesteld voor het gebruik van clouddiensten waaraan risico's verbonden zijn voor alle overheden gelden, en dat zij dus niet enkel als advies gelden?
Ik zie uit naar de beantwoording. Dank u wel.

De **voorzitter**:

Dank, mevrouw Bouchallikh. Keurig binnen de tijd, eigenlijk als enige. Ik zie geen interrupties. Dan geef ik nu het woord aan de heer Slootweg, CDA.

De heer **Slootweg** (CDA):
Dank u wel, voorzitter. Ook ik wil mevrouw Leijten feliciteren met de status van politicus van het jaar. Toch blij dat je dat in zo'n commissie kunt doen waar je samen in zit; dan kun je toch proberen om die meetlat zelf ook te gaan bereiken.
Voorzitter. De overheid bezit veel informatie over ons als inwoners en die informatie heeft ze nodig, zodat we een beroep kunnen doen op onze rechten en zodat zij ons kan aanspreken op onze plichten. Ze bezit ook informatie waarmee ik kan aantonen dat ik ík ben en niet een ander. Die informatie is niet opgeslagen in ordners in een brandveilige bunker, maar op computers of in clouds. Informatie die allerlei medewerkers van de overheid, wanneer ze daartoe geautoriseerd zijn, kunnen inkijken en zo nodig verwerken. Als inwoner van dit land wil je dan zeker weten dat deze informatie veilig is. Hacks en datalekken zorgen ervoor dat er onrust ontstaat bij de bevolking.
Ik begin met datalekken. Zeker 2 miljoen Nederlandse klantgegevens blijken betrokken bij een groot Nederlandse datalek. Niet alleen private bedrijven als VodafoneZiggo zijn getroffen, maar ook publieke organisaties als de NS en de Rijksdienst voor Ondernemend Nederland. De oorzaak lijkt te liggen bij een softwareleverancier die diensten aan marktonderzoekers levert. Dat is zorgwekkend. Heeft de Staatssecretaris al een eerste beeld van welke organisaties zijn getroffen? Wanneer worden de eerste bevindingen van de Autoriteit Persoonsgegevens verwacht?
Er zit een principieel vraagstuk achter, namelijk waar precies de verantwoordelijkheid van wie ligt voor de gegevens van onze inwoners. Nu wordt snel gewezen naar de marktonderzoekers, maar de getroffen Nederlanders zijn toch eerst en vooral klant van dat grote bedrijf of die grote organisatie. Is het wel verantwoord om zulke enorme hoeveelheden data te delen met of uit te besteden aan marktonderzoekbureaus? Zijn er extra waarborgen voor deze organisaties voordat zij data met onderzoekers delen en, zo nee, moeten die er niet komen?
Voorzitter. In Het Financieele Dagblad stond een prachtig artikel – het leek wel een advertorial – over hoe het kleine Nederland big tech weet te beteugelen. In een aantal sectoren onderhandelen we collectief over de inkoop van digitale diensten, wat onze positie sterker maakt. De overheid bijt haar tanden vast in de techniek met de zogeheten DPIA's. Kunnen we het collectief inkopen en onderhandelen uitbreiden naar andere sectoren, zoals de zorg?
Er klinkt ook kritiek. Daar zou enkele vragen over willen stellen. Het CDA heeft met name zorgen over de marktmacht van enkele partijen. Ondanks scherpe onderhandelingen van onderwijsorganisatie SURF zit nu bijna 95% van de Nederlandse universiteiten in de cloud van Microsoft. Is de Staatssecretaris het ermee eens dat we ook hier goed moeten kijken als we big tech willen temmen? Wat kan zij leren van andere landen, zoals Duitsland en België, die op sommige punten verder zijn met het ontwikkelen van eigen digitale diensten?
Markttoezichthouder ACM waarschuwde onlangs voor het lock-ineffect: wie nu data eenmaal in de Amerikaanse cloud heeft, krijgt die er moeilijk uit. Het is dus belangrijk dat we werk maken van de eigen Europese clouddiensten. Wil de Staatssecretaris voortmaken met de IPCEI-cloud? Wat is de status hiervan? Ik had het ongetwijfeld in het Engels moeten uitdrukken, maar ik dacht: anders gaat mevrouw Van Weerdenburg misschien vragen wat de Nederlandse vertaling is. Nee, het is een zeer terecht punt dat zij heeft.

De **voorzitter**:

De heer Slootweg, u krijgt toch even een interruptie.

Mevrouw **Van Weerdenburg** (PVV):
Ja. Zelf uitgelokt, meneer Slootweg. Dat laat ik echt niet over mijn kant gaan. Nee, alle gekheid op een stokje. PVV'ers zijn niet snel beledigd. Even om het principe. Ik weet dat de heer Omtzigt al een tijdje weg is bij het CDA, maar er moet ergens nog een soort restje zijn van rechtsstatelijkheid en hoe we hier in de Kamer dingen doen. Is de heer Slootweg het niet ook met ons – de VVD, de PVV en BVNL – eens dat we hier de regering goed moeten controleren en daarom ook echt de informatie moeten hebben, zodat we daar vragen over kunnen stellen? En in het verlengde daarvan ... Dat ben ik even kwijt. Excuus, voorzitter.

De **voorzitter**:
De vraag is dus of het CDA het eens is met uw vraag.

De heer **Slootweg** (CDA):
Ik heb helemaal niet mevrouw Van Weerdenburg op deze manier ... Als het badinerend klonk, dan bied ik daarvoor mijn excuses aan, want dat is helemaal niet de bedoeling geweest. Ik vind dat u een zeer terecht punt heeft. Ik weet niet helemaal of ik het met u eens ben dat de samenvatting die is gestuurd nu alleen in jip-en-janneketaal was. Ik denk dat het op zichzelf een degelijke samenvatting was, maar ik vind wel dat wij in Nederland op het moment dat we de overheid moeten controleren ... Iedere Nederlander moet met ons kunnen meekijken en meedenken. Dus op het moment dat u verzoekt om dat te vertalen, kan ik u daar alleen maar in bijstaan.

De **voorzitter**:
De heer Slootweg gaat verder met zijn betoog.

De heer **Slootweg** (CDA):
Voorzitter. De eisen om in te loggen bij bijvoorbeeld Mijn Belastingdienst worden best complex. Dat heeft alles met veiligheid te maken. De Staatssecretaris geeft aan dat ze zich realiseert dat de veranderingen voor veel mensen lastig zijn. Belangrijk om de mensen die dit lastig vinden te helpen, zijn de Informatiepunten Digitale Overheid, de IDO's, bij de bibliotheken. De Staatssecretaris zegt: we werken aan alternatieven voor mensen die niet mee kunnen komen. Is dat eigenlijk niet de verkeerde volgorde? Door eerst de alternatieven op orde te hebben en dan het authenticatieniveau te verhogen zorg je ervoor dat je de mensen niet in de steek laat. Hoeveel mensen hebben er in 2022 eigenlijk gebruik gemaakt van IDO's? Hoeveel uur is een IDO bemenst? Zijn er rond de belastingaangifte extra mensen beschikbaar om mensen te kunnen helpen?
Dank u wel, voorzitter.

De **voorzitter**:
Dank. Nu geef ik het woord aan de IT-politicus van het jaar, mevrouw Leijten.

Mevrouw **Leijten** (SP):
Voorzitter, dank u wel. Dank ook aan deze commissie. Deze commissie heeft wel degelijk door haar bestaan en door ons samenwerken betere debatten opgeleverd over digitale zaken. Het helpt natuurlijk dat we een Staatssecretaris hebben. Het helpt ook zeer zeker voor de controlefunctie van het parlement dat wij bestaan. Ik wil deze prijs dus ook deels doorgeven aan jullie. Het is natuurlijk een grote eer, maar, eerlijk is eerlijk, ik had die niet gekregen zonder deze commissie.
Waar staan we nou precies op het gebied van cyberveiligheid en de overheid? Dat zou ik eigenlijk aan de Staatssecretaris willen vragen. Hoe

vliegen we dit aan? Wat verstaat zij onder veiligheid? We kijken bijvoorbeeld naar de vitale sector. We kijken naar de fysieke gevolgen. Er moeten 1.000 mensen dood, gewond of chronisch ziek zijn. Ik denk dan: wauw! Als ik de impact zie van gisteren bij Voorschoten, dan denk ik: wat is dat voor een raar criterium? Er moet een criterium voor zijn, maar denkt de Staatssecretaris dat dat nog van deze tijd is? Ik denk dat een hack bij een ziekenhuis en andere hacks die we de afgelopen tijd hebben gehad – mevrouw Bouchallikh had het daar al over – ook grote impact hebben gehad. Die laten zien hoezeer data met elkaar verweven zijn. Data worden doorverkocht, gedeeld of geveild. Denk aan het artikel waar de voorzitter gisteren zelf een debat over heeft aangevraagd.
We worden ons meer bewust van wat data zijn. We weten beter wat de waarde is van het delen van data. We weten ook beter wat de risico's zijn van het delen van data. Die kunnen namelijk ergens komen te liggen waar we ze niet willen hebben liggen. Waar vindt de Staatssecretaris dat we staan op het gebied van veiligheid? Dat zou ik graag van haar willen horen.
Wat de SP betreft ontbreekt de fundamentele discussie over de wenselijkheid van allerlei nieuwe technologieën. Volgen wij de technologie of hebben wij bepaalde waarborgen waarbij we zeggen dat we technologie wel of niet toepassen? We hebben nu bijvoorbeeld een discussie over TikTok op telefoons. Je kunt via TikTok namelijk mogelijk bij andere documenten komen. Waarom voeren we geen debat over alle foto's en filmpjes die wij van onszelf delen, waardoor de gezichtsherkenning in de kunstmatige intelligentie beter wordt? Daardoor kunnen staten of commerciële partijen ons volgen tot waar we ook zijn. Zij weten onze behoeftes soms beter in te schatten dan wijzelf. Die discussie ontbreekt. Natuurlijk, we hebben het nu over TikTok en China. Maar ik heb het advies van de Autoriteit Persoonsgegevens over het Rijksbreed cloudbeleid 2022 gelezen. Zij zeggen dat er risico's zijn als onze persoonsgegevens – de heer Slootweg had het er al over – gedeeld worden door de overheid en in allerlei systemen uit het cloudbeleid staan. Als ze eenmaal bij een Amerikaanse aanbieder hangen, dan krijgen we ze misschien nooit meer terug. Onze eigen Autoriteit Persoonsgegevens wijst daarop. Wat is precies de reactie van de Staatssecretaris? Op 22 augustus 2022 stelt zij in de ministerraad het Rijksbreed cloudbeleid 2022 vast. Ik stel vast dat er dus geen overleg is geweest met de Autoriteit Persoonsgegevens. Er is ook geen overleg geweest met de Tweede Kamer. De Tweede Kamer kan nu de evaluatie van later dit jaar afwachten. Ik vind dat nogal wat. Dit gaat namelijk over wat de overheid doet met onze gegevens.
Je kunt opschrijven dat je een algoritme of dataminimalisatie wil, maar wat nou als die gehackt worden? Is dat vitale infrastructuur? Er zullen namelijk geen 1.000 doden vallen, om het maar even heel hard te zeggen, maar de impact daarvan kan wel gigantisch zijn. Ik zou dus graag aan de Staatssecretaris willen vragen waar wij nu precies staan. Waar staat de overheid precies?
Ik wil nog een principiële vraag neerleggen. Misschien is het een beetje een rare vraag, op de dag dat ik IT-politicus van het jaar ben geworden. Moeten wij wel door met de strategie van de overheid en de politieke opvatting dat je altijd alles digitaal moet doen wat digitaal kan? Moeten we niet gewoon zeggen: nee, dat is niet de automatische weg? Dan kom je ook bij de discussie die de heer Slootweg had over zwaardere authenticatiesystemen bij de Belastingdienst. Hartstikke fijn en hartstikke prettig voor iedereen. Voor sommige mensen is het gewoon niet bij te houden. Kunnen we dit wel bijpassen met flankerend beleid? Of moeten we gewoon zeggen: het kan wel digitaal, maar dat hoeft niet? Kan dat niet het standpunt worden als men contact heeft met de overheid? Dat is misschien handig vanuit het veiligheidsperspectief.
Dank u wel, voorzitter.

De **voorzitter**:
Dank. Dan zou ik nu het voorzitterschap over willen dragen aan mevrouw Van Weerdenburg.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dan geef ik nu het woord aan mevrouw Dekker voor haar inbreng namens D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Vorige week was er elke dag van de week een nieuw datalek, zowel bij private partijen als bij publieke organisaties zoals de GGD en het Kadaster. Het digitale leven vraagt van ons als overheid dat wij onze systemen goed beveiligd hebben, want als overheid zijn wij verzot op data. Dan moet men er ook op kunnen vertrouwen dat die in goede handen zijn. Ik heb vandaag een overzichtelijke bijdrage met drie onderwerpen: ten eerste DPIA, dan de end-to-endencryptie en ten derde de datalekken.
Voorzitter. Naar aanleiding van een goed voorbeeld bij onze oosterburen gaat de overheid een zogeheten DPIA uitvoeren naar het gebruik van Facebookpagina's door de overheid. Een data protection impact assessment is bedoeld om te beoordelen of er privacyrisico's zijn voor burgers bij de gegevensverwerking op overheidspagina's, in dit geval dus op Facebookpagina's. Het DPIA laat geen spaan heel van het privacybeleid: zeven hoge risico's en één laag risico. Facebook informeert burgers niet over wat men met de gegevens op die pagina's doet en gebruikt bijvoorbeeld cookies op een misleidende manier, aldus het rapport. Het mag geen verrassing zijn, want in Duitsland roept de data protection commissioner al sinds 2019 dat de overheid haar Facebookpagina's moet sluiten. Mijn vraag is heel simpel: hoeveel tijd wil de Staatssecretaris aan Meta bieden om veranderingen door te voeren? Is zij het met D66 eens dat hier onvoldoende voortgang wordt geboekt en, zo ja, dat de overheid moet overwegen om wellicht van Facebook af te gaan?
Ten tweede, voorzitter. End-to-endencryptie is voor D66 een groot goed. Het garandeert privacy in onze communicatie. Zo kunnen we er bijvoorbeeld zeker van zijn dat Meta – ja, daar zijn ze weer – niet mee kan lezen als wij whatsappjes sturen. Het zorgt ervoor dat cybercriminelen niet zomaar namens ons iets kunnen verzenden. De keerzijde is ook waar: berichten zijn privé, ook als de inhoud niet deugt. Nog steeds worden berichten van criminelen ontcijferd, zoals we recentelijk hebben kunnen zien met de arrestaties van criminele kopstukken. Echter, het lijkt alsof het Ministerie van JenV gefixeerd blijft op het verbreken van de encryptie. Eerder was het ministerie bezig met het inbouwen van een achterdeur in de encryptie. Nu heeft het ministerie wat nieuws: client-side scanning. Dat is een beetje alsof je een pakketje voordat je het verstuurt eerst door de scanner op de luchthaven haalt. Die scanner zoekt dan naar tekenen van dingen die niet mogen, in dit geval illegale praktijken. Dat klinkt misschien mooi, maar het compromitteert onze privacy in enorme mate. Er wordt dan immers op grote schaal meegelezen in berichten. Je leest ze dus van tevoren en vervolgens zeg je dat encryptie nog steeds werkt. Maar dan heb je het al gelezen, waarmee encryptie waardeloos is geworden. Wat ons betreft is dit een slecht idee. Deelt de Staatssecretaris dit? Kan zij toezeggen dat end-to-endencryptie wat haar betreft intact blijft en er niet zoiets als client-side scanning wordt toegevoegd?
Voorzitter, ten slotte. Zoals ik zei, was het vorige week elke dag raak. De NS, Vodafone, het Kadaster, de GGD en noem maar op: overal gingen persoonsgegevens van klanten en burgers verloren. De gevolgen daarvan zijn nu nog niet te overzien. Daarom wil D66 dat hiervan werk wordt gemaakt. Wij zullen op korte termijn een plan lanceren om persoonsge-

gevens beter te beschermen. Dat willen wij met drie maatregelen doen. Eén: het recht om vergeten te worden. Iedereen zou bij niet noodzakelijke bedrijven of diensten moeten kunnen aangeven om vergeten te willen worden. Twee: het datadieet. Overheid en bedrijven vragen meer data dan nodig en bewaren ze langer dan nodig. Wat ons betreft komt hierover strenge wetgeving. Drie: een verbetering in cookiewetgeving. Nu klikken Jan en alleman ongezien op het opslaan van cookies. Dat is onnodig; dat kan veel beter. Kan de Staatssecretaris op deze punten reflecteren?
Dank u wel.

De **voorzitter**:
Dank u wel. Keurig binnen de tijd. U krijgt het voorzitterschap weer terug.

Voorzitter: Dekker-Abdulaziz

De **voorzitter**:
Inderdaad. Ik ben ook verrast. Ik zie geen interrupties. Staatssecretaris, hoeveel tijd heeft u nodig?

Staatssecretaris **Van Huffelen**:
Ik krijg net door van mijn collega's die boven aan het werk zijn dat de mail eruit heeft gelegen, dus ik denk dat we iets meer tijd nodig hebben. Kunnen we tot 11.00 uur schorsen? Dan heb ik even de tijd om naar boven te gaan en kunnen zij ervoor zorgen dat er dingen worden geprint enzovoort.

De **voorzitter**:
Geen probleem. Dan schorsen we de vergadering tot 11.00 uur.

De vergadering wordt van 10.34 uur tot 11.00 uur geschorst.

De **voorzitter**:
Ik geef het woord aan de Staatssecretaris Digitalisering, voor de beantwoording van de vragen in eerste termijn.

Staatssecretaris **Van Huffelen**:
De ironie: we hadden en hebben last van een storing in ons e-mailsysteem. Ik heb geprobeerd om de vragen zo veel mogelijk te verzamelen. Er komt zo meteen nog wat aan, maar ik hoop dat ik uw vragen zo veel mogelijk kan beantwoorden.
Natuurlijk ook van mijn kant felicitaties aan mevrouw Leijten, die IT-politicus van het jaar is geworden. Van harte! Ik ben het met haar eens dat het heel fijn is dat we ook een aparte commissie hebben die hierover praat, want in de meeste gevallen levert dat interessante en goede debatten op over een onderwerp dat gelukkig steeds meer in de publieke belangstelling staat.
Vandaag gaat het over het onderwerp informatiebeveiliging bij de overheid. Dat is een zeer belangrijk thema. De kern is dat burgers en bedrijven erop moeten kunnen vertrouwen dat de overheid niet alleen zorgvuldig met gegevens omgaat, maar ook systemen en processen heeft die werken, zodat er systemen en processen beschikbaar zijn wanneer je zaken wilt doen met de overheid, dat die veilig en betrouwbaar zijn en dat je de regie kunt behouden over wat je met de overheid deelt.
Wat veiligheid betreft zijn er natuurlijk veel beren op de weg. Er zijn veel problemen. We zien digitale dreigingen van statelijke actoren en van criminelen. We zien die steeds vaker plaatsvinden, op allerlei manieren: aanvallen op onze infrastructuur, op onze programma's, pogingen om gegevens van mensen te ontfutselen. Dat is een heel zorgelijke ontwikkeling, waar ik zo meteen nog op terugkom, die ook laat zien dat het niet ophoudt. Steeds weer, iedere dag weer, is er werk aan de winkel om

ervoor te zorgen dat de veiligheid verbetert. Of het nu gaat om hacking, om phishing, om aanvallen op systemen: alles moet worden aangepakt. We hebben ook gezien dat cybercrime toeneemt. Dat geldt niet alleen voor de overheid, maar ook in het algemeen. Zo'n 2,5 miljoen mensen in ons land geven aan dat zij weleens slachtoffer zijn geworden van cybercriminaliteit en ook dat is iets wat ons zorgen baart.
Vorige week hebben we met de commissie van Justitie en Veiligheid ook over dit onderwerp gesproken. Ook bij de overheid is op dit vlak veel te doen. Dat zal ook zo blijven, want als wij onszelf beter weten te beschermen, wordt er altijd weer naar nieuwe manieren gezocht – soms worden ze ook gevonden – om ons aan te vallen. De oorlog die Rusland voert tegen Oekraïne, de cyberoorlog, laat ons zien hoe hard wij die bescherming nodig hebben.
Het is goed om dat in het openbaar bestuur goed te regelen. Informatiebeveiliging is daarbij belangrijk, zoals gezegd. We moeten onze systemen en processen op orde houden. We hebben in de werkagenda Waardengedreven Digitaliseren gezegd dat versterken van cybersecurity een belangrijk onderwerp is. Dan gaat het om de combinatie van systemen, processen en gegevens. In al die vormen moeten we kijken hoe we dat doen. We werken op dit moment aan een wettelijke basis voor informatiebeveiliging van de overheid. Ik kom daar nog op terug naar aanleiding van vragen die door de heer Rahimi werden gesteld. We hebben natuurlijk ook al van alles gedaan de afgelopen tijd, bijvoorbeeld het kader opgesteld, dat Baseline Informatiebeveiliging Overheid heet. Verder oefenen we op allerlei manieren en werken we aan het veilig houden van de overheid. Mijn ambitie is om niet alleen toe te werken naar meer inzicht in financiën rondom digitalisering, maar ook om een IT-verslag en een IT-auditverklaring te maken. Daarmee willen we bekijken hoe we ervoor kunnen zorgen dat er aandacht en tijd wordt besteed aan allerlei aspecten, waaronder zeker ook veiligheid. Jaarlijks oefenen we. Inmiddels doen al vele, vele overheidsorganisaties mee aan die oefeningen: vijf jaar geleden begonnen we met zo'n 700 deelnemers en nu zijn het er zo'n 3.000. Vorig jaar oktober hebben we geoefend en we gaan ook dit jaar weer oefenen op het gebied van cyberveiligheid en het bestrijden van cybercriminaliteit. Daarmee wil ik de inleiding afronden. Vanuit de rijksoverheid hebben wij een stelselverantwoordelijkheid voor het openbaar bestuur en daarmee ook voor veiligheid. Ik vind het van belang dat we op basis daarvan niet alleen zorgen voor een wet, maar ook inhoudelijk blijven samenwerken. Gelukkig hebben we ook afgesproken met alle lagere overheden om samen te gaan werken aan die informatiebeveiliging en cyberveiligheid.
Ik heb op dit moment drie blokjes die ik wil aflopen. Nogmaals, er komen nog een paar vragen aan, maar ik ga proberen op basis van de vragen die u gesteld heeft, zo goed mogelijk antwoord te geven. Ik wil beginnen met het blokje informatie en beveiliging. Dan heb ik een blokje privacy en dan een blokje open source.
Het blokje over informatie en beveiliging begint met de vraag van de heer Rahimi van de VVD. Hij vroeg: wat is nou de stand van zaken rondom de voorbereiding van wetgeving op dit gebied? Komt er ook aparte wetgeving? Het antwoord daarop is dus ja. We zijn voornemens dat te doen, ook omdat alle overheden binnen de scope van de zogenaamde NIB2 moeten vallen. Dat is de wetgeving die we in Europa hebben afgesproken op dat gebied. Ik wil daarmee een versnelling maken om te verankeren dat informatieveiligheid voor de publieke sector ook wordt gerealiseerd.
Een tweede vraag op dit gebied van de heer Rahimi was of er op één plaats een algemene zorgplicht voor informatieveiligheid bij de overheid kan worden geregeld en wat ik bedoel met «daardoor». Het is de bedoeling dat die NIB2-richtlijn ervoor zorgt dat we allerlei interbestuurlijke regelgeving goed harmoniseren. We zien het dus vooral als een kans. Uiteindelijk werkt het op het punt van cyberveiligheid natuurlijk pas

wanneer we het als overheden met elkaar doen en zo veel mogelijk combineren. Daar hebben we dus ook al afspraken over gemaakt met onder andere de VNG en een aantal gemeentes. We willen juist die harmonisatie gebruiken om het daarmee haalbaarder, betaalbaarder en uitvoerbaarder te maken, omdat het voor heel vele lagere overheden ingewikkeld is om het allemaal zelf te bedenken, zelf de aanbestedingen te doen en zelf te zorgen voor verbetering van de informatieveiligheid.
De heer Rahimi vroeg ook of wij van plan waren de richtlijnen rondom dit thema vanuit de Verenigde Staten in ogenschouw te nemen, zoals zero trust. Wat wij aan het doen zijn, is een nieuwe versie maken van die Baseline Informatiebeveiliging Overheid. Daarin nemen we ook die concretere richtlijnen uit de Verenigde Staten mee, zoals die veiligheidsstrategie zero trust. De bedoeling is om in 2024, dus volgend jaar, een geactualiseerde BIO beschikbaar te hebben. Dat doen we met experts vanuit binnen- en buitenland. Met die expertaanpak kunnen we garanderen dat het zo veel mogelijk aansluit op de hedendaagse praktijk, hoewel we natuurlijk ook steeds opnieuw moeten bekijken of we voldoen aan de meest recente eisen en ontwikkelingen. Daarom doen we ook deze vernieuwingsslag.
Een andere vraag van de heer Rahimi ging over ID-ware en de hack die heeft plaatsgevonden waar ook de Tweede Kamer en u als leden last van hebben gehad. De Beveiligingsautoriteit Rijk en de CISO, onze cybersecurity officer, hebben nog recent contact gehad met ID-ware. Ze hebben zich in detail laten informeren over alle maatregelen die ze hebben genomen, onder meer de continue monitoring die moet plaatsvinden om te zorgen dat het systeem niet opnieuw gehackt kan worden of dat nieuwe aanvallen in ieder geval kunnen worden afgewend. Om dit verder in de gaten te houden doet de CISO Rijk dat continu, niet alleen maar voor ID-ware, maar ook voor andere, rijksbrede voorzieningen.
Er was ook de vraag wat er nou precies gebeurd is met de gegevens rondom die hack van ID-ware. Ik geloof dat dat een vraag was van een van de andere leden, maar ik kom daar dan maar gelijk op. Het ging vooral over gegevens als foto's, namen, geboortedata, dus eigenlijk gegevens die ook wel anderszins in het publieke domein beschikbaar zijn. Het is daarmee niet minder vervelend, maar het geeft wel aan dat het bijvoorbeeld niet echt mogelijk is om de passen die er zijn na te maken of op een of andere manier onder valse voorwendselen hier in de Kamer of bij gebouwen van het Rijk binnen te komen. Maar goed, we blijven dit soort ontwikkelingen natuurlijk in de gaten te houden en proberen daar ook steeds van te leren. Dat was ook de vraag van de heer Rahimi: wat doen jullie nou om inzicht te krijgen in wat hier gebeurd is en hoe kun je ervan leren, zodat volgende aanvallen niet meer plaatsvinden of in ieder geval zo veel mogelijk worden voorkomen?
Een vraag van GroenLinks ging over ...

De **voorzitter**:
Staatssecretaris, ik ga u heel even onderbreken, want ik zie dat de heer Rahimi wil interrumperen.

De heer **Rahimi** (VVD):
Ik ben blij om dit te horen. Ik doelde eigenlijk meer op de verschillende normenkaders en de BIO. Het lijkt soms meer op administratieve rompslomp, terwijl je soms gewoon een hek of weet ik veel wat wilt. Waar komt ID-ware zelf mee in plaats van dat wij daarnaar moeten kijken? Dat las ik nergens. Dat was mijn concrete vraag. Heeft ID-ware zelf punten die andere instanties eventueel kunnen gebruiken?

Staatssecretaris **Van Huffelen**:

Ik kan op dit moment geen antwoord geven op de vraag wat zij zelf doen. Wij monitoren wel bij hen. Ik zal in de tweede termijn even terugkomen op de vraag wat zij precies aan het doen zijn.
Wat betreft de Baseline: natuurlijk zijn dat richtlijnen die we op papier zetten. Maar dat doen we natuurlijk niet om het alleen maar papier te laten zijn. We willen ze daadwerkelijk gebruiken, niet alleen bij de rijksoverheid maar ook bij de gemeentes en de provincies, om ervoor te zorgen dat we zo goed mogelijk zijn gewapend tegen aanvallen van buitenaf. Het is natuurlijk helder dat we dat steeds moeten updaten.

De **voorzitter**:
Een vervolgvraag van de heer Rahimi.

De heer **Rahimi** (VVD):
Ik wil het volgende meegeven. Toen de cookiewet speelde, zat ik niet in de Kamer, maar ik ben daar zo allergisch voor. Ik bedoel eigenlijk: wilt u er echt voor waken dat dat gebeurt, zodat het niet een vinkjeslijstje wordt, waarna het goed is? Wilt u dat meenemen, zodat we niet weer in dat soort dingen vervallen?

Staatssecretaris **Van Huffelen**:
Ik denk dat we het daar ook over kunnen hebben bij de wet die we aan het maken zijn. Hoe kunnen we ervoor zorgen dat we de juiste maatregelen treffen en niet iedereen denkt: hoe kom ik hier zo snel mogelijk vanaf? Want dat is natuurlijk precies datgene wat we niet willen.

De **voorzitter**:
De Staatssecretaris vervolgt.

Staatssecretaris **Van Huffelen**:
Ik kom zo meteen nog even terug op het onderwerp cookies.
Vanuit GroenLinks werd de vraag gesteld: hoe kun je ervoor zorgen dat IT-producten voldoen aan de wet- en regelgeving en aan de standaarden voor informatiebeveiliging? U zei: die verantwoordelijkheid moet vooral liggen bij de leverancier. Dat ben ik zeer met u eens. Overheden worden op allerlei manieren geholpen om de juiste eisen te stellen, maar het gaat er natuurlijk om dat de leveranciers voldoen aan de vereisten en dat er van alles wordt gedaan om ervoor te zorgen dat ze daaraan voldoen. Daar is allerlei regelgeving voor, met name op Europees niveau. De Cyber Resilience Act gaat ervoor zorgen dat leveranciers van hard- en software worden gedwongen om veilige producten te leveren. Het is heel belangrijk dat dat gebeurt.
Mevrouw Bouchallikh vroeg of wij mogelijkheden zien om als Europa digitaal autonomer te worden. Dat is zeker een heel belangrijke ontwikkeling, die meer aandacht heeft gekregen binnen de Europese Commissie naar aanleiding van de situatie die ontstaan is door de oorlog in Oekraïne. We zagen toen als Europa hoe afhankelijk we zijn, bijvoorbeeld van energieleveranties. Dat heeft ertoe geleid dat er opnieuw wordt gekeken naar dit thema. Het gaat niet alleen over autonomie wat betreft de hardware en de infrastructuur, zoals datacenters, maar ook wat betreft de software. Het is relevant om te kijken hoe we op onszelf kunnen vertrouwen als dat nodig is. Op dit moment werkt het Ministerie van EZK samen met ons aan het verder uitwerken van beleid op het gebied van digitale autonomie en infrastructuur. Dat wordt naar verwachting in de tweede helft van dit jaar opgeleverd.
Mevrouw Bouchallikh vroeg of gemeenten, provincies en waterschappen voldoende middelen hebben om er daadwerkelijk voor te zorgen dat ze veilig digitaal kunnen werken. Ik kan natuurlijk niet garanderen dat dat altijd zo is, want ze hebben natuurlijk hun autonome taken en keuzes wat betreft hun bedrijfsvoering. Maar we zorgen er natuurlijk wel voor dat we

medeoverheden ondersteunen met kennis en met allerlei vormen van informatie, en natuurlijk ook met het uitvoeren van grote cyberoefeningen. Het is niet onbelangrijk om te vermelden dat de Minister van Justitie en Veiligheid en ik in december een convenant hebben gesloten met de gemeentes om ervoor te zorgen dat we niet alleen kijken naar wat er inhoudelijk moet gebeuren om veilig te zijn, maar ook naar hoe we ervoor kunnen zorgen dat daarvoor voldoende kennis, kunde en middelen ter beschikking komen. Het is dus een punt waar we aandacht voor moeten hebben en houden. We kunnen niet zeggen dat er gegarandeerd altijd voldoende middelen zijn. We moeten er vooral voor zorgen dat we de goede keuzes maken, zodat de gemeenten en de provincies die veiligheid kunnen invoeren.

Mevrouw **Bouchallikh** (GroenLinks):
Een vervolgvraag. Dat «garanderen» heb ik inderdaad heel specifiek zo opgeschreven, omdat we hier allemaal hele goede beleidsontwikkelingen op gang kunnen proberen te brengen met regels en dat soort zaken, maar als een lagere overheid niet de middelen of de capaciteit heeft om dat ten uitvoering te brengen, gaat het uiteindelijk ten koste van de burger. Daarin komt dat dan weer terug. Wat kan de Staatssecretaris dan wél doen? Ik vind het namelijk toch best wel een heikel punt als ik hoor dat het niet mogelijk is om dit te garanderen.

Staatssecretaris **Van Huffelen**:
Ik vind «niet mogelijk» niet een goed woord hiervoor. Ten eerste hebben we met gemeenten en provincies natuurlijk een convenant afgesloten. We doen er ook alles aan om gemeenten en provincies te laten meedoen aan datgene wat wij voor onszelf als beleid maken. Dat geldt bijvoorbeeld ook voor de recente afspraken die we gemaakt hebben voor de rijksoverheid zelf rondom het gebruik van apps uit landen met een offensief cyberprogramma. Daarbij hebben we ook aan gemeenten gevraagd om dat beleid te volgen. Wij willen hen waar dat nodig is ondersteunen met kennis, kunde, handreikingen, enzovoorts, enzovoorts. We gaan ook die wet maken. Die gaat natuurlijk ook gelden voor lagere overheden. Maar ik vind het in de komende tijd natuurlijk vooral van belang ... U vraagt: is er altijd een garantie dat alle middelen er zijn? Dat is natuurlijk te moeilijk en te breed om te beantwoorden. Maar ik ben het zeer met u eens dat we natuurlijk willen dat dit op alle niveaus in de overheid goed geregeld is, want anders kunnen problemen die in een gemeente of in een provincie ontstaan ook doorwerking hebben voor het Rijk. Wij blijven daar dus heel goed over in overleg met hen, om te zorgen dat dat wat we wensen, namelijk voldoen aan een hoog niveau van veiligheid, ook geldt voor onze medeoverheden.
Dan ...

De **voorzitter**:
Er is nog een interruptie van de heer Rahimi.

De heer **Rahimi** (VVD):
Ik weet niet of het mag, maar ik wil mevrouw Bouchallikh graag een vraag stellen.

De **voorzitter**:
Nee, officieel mag dat niet, dus u moet die dan bewaren voor de tweede termijn. De Staatssecretaris gaat door met haar beantwoording.

Staatssecretaris **Van Huffelen**:
Ik zou ook willen zeggen dat die NIB2-richtlijn, die dus ook gaat gelden voor provincies en gemeenten, ons ook de kans biedt om de regelgeving op dit gebied veel meer te harmoniseren. Ik ben daar blij mee, want dat

zou ook weer kunnen bijdragen aan ervoor zorgen dat we de haalbaarheid en de uitvoerbaarheid maar zeker ook de betaalbaarheid van die informatiebeveiliging beter op orde kunnen krijgen.
Dan de vraag van mevrouw Bouchallikh over het gebruik van clouddiensten, waaraan risico's verbonden zijn: zouden we die richtlijnen alleen voor de rijksoverheid moeten laten gelden of ook voor provincies, gemeenten en andere delen van de overheid? Wij hebben hen geadviseerd om dat te doen. We hebben daar overleg over gehad. Ik heb daarbij met hen afgesproken dat we elkaar daarvan op de hoogte houden. Uiteraard hebben de verschillende onderdelen van het Rijk zelfstandige posities, dus een gemeente kan er bijvoorbeeld voor kiezen om ervan af te wijken. Maar gegeven het feit dat wij er zelf niet alleen maar heel goed over hebben nagedacht maar ook zeer goed hebben gekeken naar wanneer wat wel of niet zou kunnen, raden wij hen vooral ook aan om te zorgen dat ze dat beleid volgen. Ik hoop natuurlijk dat de lokale gemeenteraden of Provinciale Staten daar ook goed op letten.

Mevrouw **Bouchallikh** (GroenLinks):
Mijn vraag hierover lijkt op mijn vorige vraag, want een keten is zo sterk als de zwakste schakel, om het zo maar even te zeggen. Stel dat lagere overheden besluiten om het niet te doen, wat kan de Staatssecretaris dan doen om hen wel zover te krijgen, los van adviseren en aanmoedigen?

Staatssecretaris **Van Huffelen**:
Uiteindelijk zou dat dan natuurlijk moeten via bijvoorbeeld een wet. Die zou dan namelijk ook voor hen gelden. Maar op dit moment hebben we daar nog niet voor gekozen, ten eerste omdat het ook veel tijd kost om zo'n wet te maken en wij vooral alvast aan de slag wilden om duidelijk te maken onder welke zeer strikte condities het mogelijk zou moeten zijn om gebruik te maken van clouddiensten en ook van clouddiensten van leveranciers die niet in Europa gevestigd zijn. Maar ik hoop vooral – ik zie dat ook steeds meer gemeenten en provincies dat graag willen – dat we met elkaar gaan optrekken en samenwerken, juist omdat deze zorgen net zo goed bij provincies en gemeenten leven als hier. Dan doel ik op zorgen over de veiligheid, over hoe er met de gegevens wordt omgegaan en over hoe zeker men ervan is dat de beschikbaarheid groot blijft. Ik zie dus juist dat er steeds meer behoefte is om samen te werken, en om niet allemaal eigen beleid en eigen keuzes te maken maar om zo veel mogelijk te teamen. In het kader van die NIB2 werken we de komende tijd samen ook verder aan het maken van die wetgeving. We zouden daarbij ook kunnen kijken naar de veiligheid van clouddiensten.
Dan een vraag van de heer Slootweg, ook over de cloud en dan met name over het onderwijs. Hij zei: ondanks scherpe onderhandelingen van de onderwijsorganisatie SURF zit 95% van de Nederlandse universiteiten in de cloud van Microsoft. Hij vroeg of ik het ermee eens ben dat we daarnaar moeten kijken en of ik daarbij zou kunnen leren van bijvoorbeeld Duitsland en België, als landen die daarmee aan het werk zijn.
Misschien mag ik eerst even specifiek inzoomen op die onderwijsinstellingen, want universiteiten zijn natuurlijk verantwoordelijk voor hun eigen keuzes op dit gebied. Die keuzevrijheid betreft natuurlijk zowel grotere als kleinere diensten. Er is ook een risico dat de afhankelijkheid van marktpartijen te groot wordt. Dat is ook de reden waarom wijzelf zo inzetten op risicoanalyses en op het bevorderen van concurrentie. Overigens is SURF, de leverancier van vele clouddiensten voor universiteiten, daarmee aan het werk. Zij hebben ook al een mix van clouddiensten in de aanbieding. Dat zijn dus niet alleen maar Amerikaanse maar ook Nederlandse en Europese aanbieders en leveranciers. Ze hebben bovendien nog hun eigen clouddiensten. Maar goed, het is dus wel van belang om het onderwijs er steeds op te blijven wijzen dat ze goede afwegingen moeten maken bij het gebruik van clouddiensten.

Misschien is het ook goed om te weten dat wij in het kader van andere landen inderdaad in Europa hard aan het werk zijn om te kijken of wij Europese clouddiensten verder kunnen ontwikkelen. Daar lopen verschillende projecten voor. U had het zelf ook over zo'n project: de IPCEI CIS. Dat is de Important Project of Common European Interest Cloud Infrastructure and Services, om dat nog maar eens in goed Nederlands toe te lichten. De bedoeling is dat we in het tweede kwartaal van dit jaar horen welke projecten op basis hiervan kunnen worden gehonoreerd en van start zullen gaan. Binnen dat programma is het idee namelijk dat er verschillende Europese clouddiensten worden ontwikkeld. De Minister van Economische Zaken en Klimaat gaat u daar ook verder over informeren. Er zijn natuurlijk ook andere ontwikkelingen, met name wetgeving gericht op de cloud, om ervoor te zorgen dat er een goed en volwaardig Europees aanbod komt in die cloudmarkt, want dit is zeker een onderwerp waar we in Europa in brede zin maar ook in Nederland graag aan willen werken om daarmee te voorkomen dat je op basis van relatief weinig concurrentie bijna automatisch terechtkomt bij clouddiensten van Amerikaanse leveranciers.
Dan een vraag van mevrouw Leijten op dat gebied, namelijk of er risico's zijn voor het delen of het niet goed omgaan met persoonsgegevens. Ze zei: als je ze aan een Amerikaanse aanbieder aanbiedt, krijg je ze misschien niet meer terug. Dit gaat ook over het cloudbeleid dat we hebben afgesproken. Wij hebben samen met de andere departementen dat cloudbeleid ontwikkeld. Ik heb er ook een gesprek over gevoerd met de Autoriteit Persoonsgegevens. U heeft hier op 20 oktober ook een technische briefing over gehad. Er is ook nog schriftelijk overleg over geweest. Ik denk dat het van belang is dat wij risico's zien bij cloudgebruik. Dat maakt ook dat we in het beleid dat we hebben geformuleerd, hebben gezegd dat het ongelofelijk belangrijk is dat wanneer je ervoor kiest om iets in de cloud te zetten en gebruik te maken van een zogenaamde private cloud, dus clouddiensten van bedrijven die dat leveren, je dan ook hele goede keuzes maakt. Sommige van die persoonsgegevens of bijzonder gevoelige gegevens kunnen dus niet zomaar worden geplaatst in een cloud en al helemaal niet in een cloud buiten de zogenaamde economische ruimte. Dat is ook precies in lijn met wat de European Data Protection Board wil.
Dan is er de vraag van mevrouw ...

De **voorzitter**:
Mevrouw de Staatssecretaris, er is nog een interruptie van mevrouw Leijten.

Mevrouw **Leijten** (SP):
De reactie van de Autoriteit Persoonsgegevens was niet: hier wordt een weg ingeslagen die wij willen. Het waren vooral een aantal pagina's met heel veel waarschuwingen. De reactie die de Staatssecretaris daar weer op geschreven heeft, is summier. Als het bijvoorbeeld gaat over het uniformeren van het cloudbeleid, gaat de Staatssecretaris het advies van de Autoriteit Persoonsgegevens dan volgen? We zijn geconfronteerd met uw besluit, zonder overleg met de AP of de Kamer. De Staatssecretaris gaat dit evalueren in het najaar. Hoe gaat die evaluatie lopen? Gaat dat langs de lijnen van de adviezen en de waarschuwingen van de AP? Of gaat dat verder op de aanvliegroute van het management die tot nu toe is gekozen bij het cloudbeleid? Als het dat laatste is, maakt de SP zich daar wel zorgen over.

Staatssecretaris **Van Huffelen**:
Het is natuurlijk ontzettend belangrijk dat we hebben gezegd dat we cloudbeleid maken. We vinden het belangrijk om goed te omschrijven hoe wij als overheid op een veilige manier gebruik kunnen maken van

clouddiensten, zowel clouddiensten binnen de Europese ruimte als clouddiensten van bedrijven die met name in de Verenigde Staten zijn gevestigd. Wij vinden het juist heel erg belangrijk dat we dat beleid niet alleen maar gemáákt hebben. We hebben dat uiteraard ook met de Kamer gedeeld en we praten er vandaag ook over. Dat is, denk ik, niet onbelangrijk. We hebben er ook voor gezorgd dat u goed op de hoogte bent gebracht via die technische briefing. Maar als we gaan evalueren, nemen we daarin natuurlijk alles mee. Dan gaat het zeker ook over de adviezen van de Autoriteit Persoonsgegevens en over de evaluatie en de ontwikkelingen die we daarin zelf zien. Dan gaat het bijvoorbeeld over de vragen: werkt dat cloudbeleid nu ook goed voor de departementen en hoe kunnen we andere overheden, provincies en gemeenten, meenemen in het verder vormgeven van dat cloudbeleid?
Ik denk dat het oogmerk dat we hebben heel helder is. Dat is namelijk dat we wanneer we gebruikmaken van clouddiensten, die ons soms heel erg kunnen helpen in termen van efficiency of bijvoorbeeld het eenvoudiger maken van het inzetten van nieuwe programmatuur of nieuwe beveiligingstools, er ook voor zorgen dat het veilig blijft omdat er met de gegevens van onze burgers wordt gewerkt, of met data en programma's die gebruikt worden door de overheid. We willen ervoor zorgen dat dat op een goede manier gebruikt kan worden.
Kort en goed samengevat in antwoord op de vraag van mevrouw Leijten: we betrekken al die ontwikkelingen en ervaringen daar natuurlijk ook bij, evenals de aanbevelingen van de AP.

De **voorzitter**:
De Staatssecretaris. O, mevrouw Leijten.

Mevrouw **Leijten** (SP):
De Staatssecretaris is in haar brief van 24 januari ingegaan op de drie adviezen van de Autoriteit Persoonsgegevens. Daarbij verwijst zij ook de hele tijd naar de evaluatie, maar dan wel met zinnen als «we kijken of het beoordeeld moet worden», «we kijken of het een plek gaat krijgen», «we kijken of ...» Ik probeer iets meer gevoel daarbij te krijgen. De Autoriteit Persoonsgegevens zegt: enerzijds is het goed dat erover nagedacht wordt, anderzijds missen we een uniforme aanpak. Dat is toch wat de Autoriteit Persoonsgegevens de hele tijd doet: je krijgt een complimentje en je krijgt een waarschuwing. Wat gaat de Staatssecretaris nu doen bij haar evaluatie? Gaat ze naar de complimentjes leunen of gaat ze de waarschuwingen ter harte nemen? Ik zou graag willen dat ze op dat laatste zou ingaan.

Staatssecretaris **Van Huffelen**:
Uiteraard kijk ik juist ook naar die waarschuwingen, want ik ben heel blij dat de Autoriteit Persoonsgegevens ook vindt dat dit beleid nodig is. Als het gaat over die uniformering en harmonisering, is het natuurlijk ontzettend belangrijk dat we in de uitvoering en verdere evaluatie van dat cloudbeleid zo veel mogelijk samen optrekken. Gelukkig hebben we in het cloudbeleid heel veel afspraken gemaakt over hoe we dat, als het bijvoorbeeld gaat over die harmonisering over de departementen heen, gaan doen met de rol die er is voor de CIO Rijk, de CISO enzovoorts, enzovoorts. Maar uiteraard vind ik het ontzettend belangrijk dat we juist ook kijken naar: waar maakt de AP zich zorgen over en hoe zorgen we ervoor dat we die zorgen zo goed mogelijk meenemen in het beleid en de evaluatie daarvan in dit najaar?

De **voorzitter**:
Oké. De Staatssecretaris vervolgt haar beantwoording.

Staatssecretaris **Van Huffelen**:

Dan kom ik bij de vraag van mevrouw Dekker-Abdulaziz over end-to-endencryptie: blijft die intact? Laat ik daar het volgende over zeggen. Het kabinet is een enorme voorstander van die sterke encryptie, want die heeft een grote beschermende waarde en moet niet ter discussie staan. Op 31 januari heeft de Minister van JenV uw Kamer een brief daarover gestuurd die uitvoering geeft aan de motie-Van Raan. Tegelijkertijd, zegt de Minister van JenV, moeten we de mogelijkheid houden om effectief te kunnen blijven opsporen. Daarom wordt er gekeken naar manieren om binnen wat is afgesproken op basis van de motie-Van Raan, dus met behoud van encryptie, rechtmatig toegang te kunnen krijgen tot versleutelde informatie. Daarbij speelt natuurlijk een rol dat fundamentele rechten, dataprotectie, behoud van cybersecurity, enzovoorts, enzovoorts, niet worden geschonden.
Dan is er nog de vraag van GroenLinks over de Digital Services Act: verbetert de komst hiervan de informatiebeveiliging substantieel? De Digital Services Act wordt in fases ingevoerd; de regulering is al afgesproken. De grote onlineplatforms zijn vanaf eind van dit jaar aan die regelgeving gebonden. Voor deze onlineplatforms, bijvoorbeeld socialmediaplatforms en onlinezoekmachines, geldt dat ze jaarlijks een risicoanalyse moeten uitvoeren om te onderzoeken welke risico's voortkomen uit de algoritmes die zij gebruiken, waaronder de risico's op het gebied van desinformatie, kinderen, het publieke debat en fundamentele rechten. Zij moeten zorgen dat die risico's worden beperkt op last van boetes wanneer ze dat niet doen. Wij gaan ervan uit dat dat ook effecten zal hebben op de informatiebeveiliging, omdat de risico's daarvoor ook in kaart moeten worden gebracht. De wetgeving gaat nu van start. We zullen goed in de gaten moeten houden of dat daadwerkelijk op deze wijze nog effecten zal hebben.
Dan de vragen van mevrouw Leijten en van mevrouw Bouchallikh over de strategieën die we hebben op het gebied van cybersecurity of beter gezegd de vragen over: wat zien we nou wanneer het veilig is? Daar hebben we in Nederland een aantal dingen over afgesproken. We hebben in Nederland de cybersecuritystrategie, die in oktober van vorig jaar naar uw Kamer is gestuurd met een actieprogramma erbij. We hebben onlangs ook een Nederlandse veiligheidsstrategie vastgesteld. Die heeft uw Kamer vorige week ontvangen. Die strategieën gaan erop in dat we willen zorgen dat we digitaal veilig zijn, of het nu gaat om beveiligingen tegen hacks of om zorgen dat er geen data gedeeld kunnen worden met partijen die daar geen recht op hebben, dat we veilige IT-middelen gebruiken, dat we voldoende deskundigheid ontwikkelen en allerlei andere maatregelen, bijvoorbeeld om ransomwareaanvallen tegen te gaan, enzovoorts, enzovoorts, enzovoorts. Natuurlijk zijn die strategieën erop gericht om ons veilig te houden, maar we zien dat de dreigingen toenemen. Dat vraagt dat we er steeds meer aan moeten blijven werken om die dreigingen tegen te gaan, of het nou dreigingen zijn vanuit criminele organisaties of dreigingen vanuit statelijke actoren. Het uitwerken van die strategieën zal betekenen dat we steeds weer verder moeten gaan om te zorgen dat we ons verder blijven bewapenen en onszelf veilig houden. Dat zal een ontwikkeling zijn die ook in de komende jaren nog heel veel aandacht zal vergen.
Dan wilde ik doorgaan naar het blokje over privacy. Ik begin met de vraag van mevrouw Van Weerdenburg over Facebook Pages. U vraagt of u de volledige vertaling in het Nederlands kan krijgen. Dat kan natuurlijk. We hoopten u enigszins te bedienen door alvast een samenvatting te sturen, maar uiteraard kunnen we dat doen. Ik denk, ook naar aanleiding van de punten die u noemde, dat het goed is om iets meer en vooral iets meer in diepte met uw Kamer te delen wat deze onderzoekers precies hebben gevonden, welke risico's ze zien en wat onze strategie is om daarmee aan het werk te gaan. Ik zou willen aanbieden om daarover een zogenaamde technische briefing te organiseren. Wellicht vragen we de onderzoekers

om u dan te informeren over wat ze hebben gezien en hoe ze daartegen aankijken, zodat er meer helderheid komt over dit onderwerp.

De **voorzitter**:
Mevrouw Van Weerdenburg voor een reactie.

Mevrouw **Van Weerdenburg** (PVV):
Dank voor het aanbod, maar dat is eigenlijk niet waar ik naar zoek. Het punt is namelijk dat ik als Kamerlid die discussie ... Wat mij betreft is het een politieke discussie. Moeten we willen dat mensen een account moeten aanmaken om bij informatie van de overheid te komen? Moeten we willen dat de overheid niet meer vertegenwoordigd is op een platform waar ze een publiek had van vijf miljoen mensen? Die waardendiscussie moeten we hier voeren. Ik vind het een beetje lastig dat daar nu een juridisch document van 150 pagina's voor wordt geplaatst waaraan die beslissing hangt: blijft de overheid wel of niet op Facebook? Maar goed, als dat de procedure is, prima. Dan moeten we het hebben over dat document. Ik wil dat niet met de opstellers van het document. Het is voor mij duidelijk. Ik vind wel dat we alsnog de volledige Nederlandse vertaling moeten hebben, al is het alleen maar om ons te helpen om de juiste vragen te stellen. Ik heb het Engelse document ook gelezen. Als dit erbij hoort, de discussie over wel of niet ... De Staatssecretaris is er juist om met haar over dat besluit te discussiëren. We hebben heel bewust gezegd dat we hierover willen spreken voordat er stappen worden genomen. Dat proberen we hier vandaag; dat lukt dus niet. Ondertussen hoor ik wel op de radio allerlei dingen zeggen en moeten we in het FD lezen dat pas vorige week de onderhandelingen zijn begonnen met Meta. Ik heb alsnog het gevoel dat er een heleboel langs ons heen gaat, en dat wil ik voorkomen. Ik heb niet zozeer behoefte aan een technische briefing met de opstellers van het rapport. Ik wil met de bewindspersoon hierover nader spreken.

De **voorzitter**:
Eerst de beantwoording en dan een vervolgvraag van de heer Rahimi. De Staatssecretaris.

Staatssecretaris **Van Huffelen**:
Dat kan ook, want dit onderzoek is natuurlijk niet onbelangrijk, om het maar even zo te zeggen. Wij willen heel graag dat als Nederlanders gebruikmaken van een dienst als Facebook, dat veilig kan en dat de dienstverlening voldoet aan de Nederlandse of in Nederland geldende regelgeving. In dit geval gaat het over de privacyregelgeving ofwel de AVG. Wij hebben gezien dat ... Dat kunnen wij onderzoeken, omdat wij zelf gebruikmaken van dit kanaal om Nederlanders van informatie te voorzien. Dat doen we omdat heel veel Nederlanders gebruikmaken van Facebook. We hebben vele kanalen om informatie te delen met inwoners van het land en dit is er een van. Wij hebben op basis van dat onderzoek gezien dat er niet wordt voldaan aan de privacyregelgeving. Dat maakt dat wij het belangrijk vinden om niet zomaar te zeggen dat we het dan niet meer gebruiken, maar om te kijken of we samen met dit bedrijf kunnen komen tot een veilige dienstverlening, in de hoop dat daarmee niet alleen maar het gebruik van de overheid van deze dienst verbetert, maar ook dat de dienstverlening van dit bedrijf gaat voldoen aan de wet- en regelgeving en dat dit ook voor de Nederlanders gaat gelden. Dat is ons oogmerk met dit traject.
Als u zegt dat u niet meer informatie hoeft te hebben over het onderzoek, prima. Ik dacht dat u daarnaar op zoek was. Maar als dat niet zo is, dan is dat op zich begrijpelijk. Ik zal in ieder geval zorgen dat u wordt voorzien van een vertaling.

De **voorzitter**:
Dank. Een vervolgvraag van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Voor zover ik wist hebben we hier volgens mij maanden geleden al over gesproken. Ik ging ervan uit dat de gesprekken met Meta al gaande waren, maar blijkbaar dus niet. Waar ik aanstoot aan neem, is dat dit document nu eigenlijk wordt gebruikt in een soort strategie: Meta staat al tegen de muur. Ik heb niet het gevoel dat de Staatssecretaris daadwerkelijk probeert om eruit te komen. Ik heb meer het gevoel dat ze nu munitie verzamelt om alvast Meta voor een voldongen feit te stellen. Dan vraag ik me af wat die gesprekken überhaupt nog voor zin hebben. Maar nogmaals, ik hoef niet meer informatie over het rapport. Ik wil gewoon hét rapport! Voor mijn gevoel heb ik het rapport niet als ik het niet in het Nederlands heb. Daarmee zeg ik niet dat ik geen Engels kan lezen, maar ik wilde bijvoorbeeld vragen stellen over de invulling van de term «joint controllership» en over wat de opstellers van het rapport daaronder verstaan. Wat voor gevolgen heeft het bijvoorbeeld voor een platform als Mastodon, waarop de Staatssecretaris nu ook actief is? Maar omdat ik een Nederlandse term zocht, pakte ik de Nederlandse vertaling erbij en dan blijkt gewoon dat het een jip-en-jannekesamenvatting van de DPIA te zijn van niet negen maar zes pagina's. Sorry, maar dan heb ik de informatie dus nog niet ontvangen. Ik wil dus wel spreken over dit rapport met de Staatssecretaris, maar ik wil het rapport ook gewoon in het Nederlands kunnen lezen.

De **voorzitter**:
Duidelijk. Ik wil mevrouw Van Weerdenburg erop wijzen dat we tijdens de pv nog altijd een commissievergadering kunnen agenderen.

Staatssecretaris **Van Huffelen**:
Ik heb mevrouw Van Weerdenburg al toegezegd dat die vertaling er komt. Misschien even iets over wat mijn intentie is, want kennelijk is dat niet goed helder. Het is niet onze intentie om Nederlanders of Nederland van Facebook af te halen. Onze intentie is te zorgen dat de producten en diensten die dit bedrijf levert – in dit geval is dat dienstverlening – voldoen aan de Nederlandse wetgeving. Dat is ook de reden waarom we met hen in gesprek zijn. Zijn dat eenvoudige gesprekken? Nee, dat zijn het niet. Het zijn indringende gesprekken, die ook tijd kosten. Dat hebben we ook gezien bij eerdere trajecten die we hebben doorlopen, bijvoorbeeld met Google en Microsoft. Het vereist namelijk dat we het niet alleen maar met elkaar eens worden over welke problemen we zien, maar ook over de mogelijke aanpassingen die het bedrijf kan doen. Dat vergt dus tijd. Nogmaals, wij zijn daar dus over in gesprek. Dat betekent dat we aan beide kanten vertegenwoordigers moeten hebben. Het heeft even tijd gekost voordat Facebook ook iemand had met wie we kunnen praten. Die hebben we nu en wij hopen vooral dat we er met hem uit komen in lijn met de eerdere keren dat we dit hebben gedaan. Want nogmaals, onze strategie is niet gericht op dingen verbieden. Dat kan uiteindelijk altijd de consequentie zijn, maar onze strategie is juist bedoeld om ervoor te zorgen dat dienstverlening die beschikbaar is voor Nederlanders en de Nederlandse overheid ook voldoet aan de Nederlandse regelgeving.

De **voorzitter**:
Helder. Tot slot, mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Ja, tot slot op dit punt, voorzitter. Vorige week stond er in Het Financieele Dagblad een stuk over die onderhandelingen en in dat stuk staat: «de Staatssecretaris trekt een streep in het zand» en «de Nederlandse

overheid is van plan geen duimbreed toe te geven in de onderhandelingen met Facebook over privacyregels». Zijn het dan nog onderhandelingen of ... Ja, ik weet dus niet wat ik moet geloven, want de Staatssecretaris sust ons nu een beetje met: nee nee, er is echt nog wel ruimte. Maar dat gevoel krijg ik dus niet.

De **voorzitter**:
We vallen een beetje in herhaling, maar tot slot de Staatssecretaris hierover.

Staatssecretaris **Van Huffelen**:
Ik ben daarin ook wel vrij eenvoudig, want natuurlijk is dit een gesprek, namelijk over hoe wordt er door deze dienst voldaan aan de Nederlandse wet- en regelgeving. Volgens mij is de AVG helder over wat je bijvoorbeeld mag doen met de gegevens van de mensen die gebruikmaken van jouw diensten. Ik denk dat we daarin heel scherp moeten zijn, want we, u en ik, hebben die wetten niet voor niks opgesteld. We hebben dat gedaan om te zorgen dat je gegevens beschermd zijn als je ergens gebruikmaakt van een bepaalde dienst. We hebben het net over hacks gehad en over data delen. Dus het is ontzettend belangrijk dat we zeker weten dat wanneer de overheid gebruikmaakt van Facebook Pages, Facebook op zo'n manier omgaat met de data van Nederlandse burgers dat het in lijn is met de Nederlandse wetgeving op dat gebied. En nogmaals, we hebben dit soort trajecten eerder gedaan. Daar zijn we goed uit gekomen en ik hoop dat dat ook zo zal zijn bij dit traject.

De **voorzitter**:
De heer Rahimi voor een interruptie.

De heer **Rahimi** (VVD):
Ik vind een technische briefing juist heel goed, al is het maar om mijn negen resterende vragen te stellen.
Volgens mij is deze vraag al beantwoord, maar ik wil toch zeker weten dat we eerst de vertaling krijgen. Ik vind dat namelijk ook belangrijk. Daarna is er eventueel een technische briefing, iets waar ik echt een voorstander van ben. Klopt dat? «Wij maken afspraken en wij zijn in gesprek» is wat ik hoor en ik vind ook dat we dat moeten doen. Kamer en kabinet moeten ook continu alert zijn en we moeten weten of de afspraken nagekomen worden. Met Google Workspace hebben we dat ook gedaan. Is dat dan na een aantal jaar werkelijk gebeurd of zitten er hier dan andere Kamerleden die het helemaal vergeten zijn? Dat vind ik heel belangrijk. Maar de technische briefing, daar ben ik wel groot voorstander van, inclusief de vertaling. Soms zijn de vertalingen ook helemaal niet te volgen, hoor. Nederlandse teksten zijn ook best wel lastig, zeg ik maar even.

De **voorzitter**:
Zeggen wij allebei als niet-native speakers.

Staatssecretaris **Van Huffelen**:
Om even op uw vraag in te gaan: u moet als commissie zelf bepalen wat u gaat doen met die wel of niet technische briefing. Het is natuurlijk zo dat wij die checks niet maar één keer willen doen. We willen dat blijven herhalen, want de dienstverlening wordt ook aangepast. Dat betekent dat je blijvend moet kijken of er wordt voldaan aan de wetten en regels die gelden voor de privacy.

De **voorzitter**:
De Staatssecretaris vervolgt haar beantwoording.

Staatssecretaris **Van Huffelen**:

De vraag die net werd gesteld, was of daar inderdaad continuïteit in zit. Die heb ik dus beantwoord.
Dan de vraag van mevrouw Bouchallikh van GroenLinks of ik kan aangeven of door overheden wordt samengewerkt met de bedrijven waar vorige week dataleks hebben plaatsgevonden. Op basis van een interdepartementale inventarisatie hebben we geconstateerd dat vijf partijen van de rijksoverheid getroffen zijn door dit datalek. Op dit moment wordt er onderzoek verricht naar de effecten daarvan. Ik heb nog geen signalen gekregen van andere overheden, dus van gemeenten of provincies, maar ik zal voor u navraag doen om te zien of zij daardoor geraakt zijn. Maar u wordt in ieder geval op de hoogte gehouden van wat dit betekent voor de rijksoverheid.
De heer Slootweg vroeg wat de Autoriteit Persoonsgegevens doet met dat datalek van vorige week. Zij is natuurlijk een onafhankelijke toezichthouder en bepaalt dus ook zelf of en wat ze ermee gaat doen. Het feit dat het gemeld is, is natuurlijk conform de regels over wat te doen wanneer er een datalek heeft plaatsgevonden.
Is er sprake van een overtreding van de AVG? De Autoriteit moet natuurlijk haar werk doen om te bepalen of dat aan de orde is. Maar daar kan ik geen opdracht of instructies toe geven.
De heer Slootweg en deels ook mevrouw Leijten vroegen of het verantwoord is om zo veel data te delen met marktpartijen. Moeten er niet extra waarborgen zijn voor het delen van data, aangezien er zoals vorige week dataleks plaatsvinden? Ik ben het zeer met u eens dat het nodig is dat er extra waarborgen komen. Dat is ook waarom er heel veel nieuwe wetgeving is opgesteld, zoals de Data Governance Act, de Digital Markets Act en de Data Act. Daarmee willen we extra waarborgen op datadelen organiseren. De verplichtingen die er zijn, zijn met name bedoeld om ervoor te zorgen dat er meer vertrouwen kan zijn in de data die worden gedeeld, niet alleen direct maar ook via tussenpersonen. De Data Act zal meer regie geven aan burgers en in de Digital Markets Act wordt het makkelijker gemaakt voor burgers om te zorgen dat ze hun data zelf meenemen naar andere diensten als ze dat zouden willen. Er worden ook extra verplichtingen gesteld aan het zorgen dat er data moeten worden gedeeld.
Dus ja, kort en goed: er moet meer worden gedaan om te beschermen. Ook het onderwerp «dataminimalisatie» is een belangrijk onderwerp. Dat geldt overigens ook voor ons als overheid. Daar waar we data met elkaar moeten delen om diensten of producten te kunnen uitwisselen, moeten we er ook voor zorgen dat dat gebeurt op basis van zo weinig mogelijk data en dus niet op basis van hele grote hoeveelheden en datasets.

De **voorzitter**:
Ja. Een interruptie van de heer Slootweg.

De heer **Slootweg** (CDA):
Ik wil de Staatssecretaris bedanken voor de antwoorden, maar aan de andere kant: als ik het goed beluister, moet ik dus voor die extra waarborgen wachten tot de nieuwe wetgeving van kracht is geworden. Op dit moment blijken ook overheidsorganisaties enorme hoeveelheden data uit te wisselen met zo'n marktonderzoeksbureau. Daardoor kunnen grote hoeveelheden informatie van onze inwoners zomaar op straat komen te liggen. Dan vind ik het toch een beetje een raar idee dat ik moet wachten tot er een keer wetgeving komt voordat er iets kan worden gedaan. Ik denk toch dat je ook iets in je interne proces zou kunnen doen en dat je nu al om waarborgen kunt vragen, vooruitlopend op wetgeving, opdat dit niet nog een keer kan gebeuren. Of is dat te optimistisch gedacht?

Staatssecretaris **Van Huffelen**:

Nee, want als we het over de overheid specifiek hebben, geldt dat vandaag de dag al. Heel zorgvuldig omgaan met data is iets wat we verwachten van niet alleen de rijksoverheid, maar ook van gemeentes en provincies. U vroeg of er nog extra waarborgen moeten komen. Ja, die moeten er nog komen. Overigens geldt de Digital Markets Act al. Maar als het gaat om het voortdurend blijven nadenken over de vraag hoe we zo gering mogelijke hoeveelheden data kunnen delen en hoe we kunnen zorgen dat er extra waarborgen zijn: dat werk moeten wij natuurlijk nu al doen. Dat blijft iets wat van kracht is, ook voor de rijksoverheid.

De heer **Slootweg** (CDA):
Dan zou ik het toch wel fijn vinden – volgens mij vroeg de heer Rahimi daar ook al om – om te horen wat wij leren van dit soort fouten. Dit is echt een gigantische hoeveelheid informatie, die ook via overheidsdiensten hiernaartoe gaat komen. Ik begrijp dat u de Autoriteit Persoonsgegevens geen opdracht kunt geven, maar ik denk toch dat deze casus ons wel iets leert van: hoe zit het nou met die waarborgen en met een soortement van stresstesten, opdat dit niet nog een keer kan gebeuren? Met name als het gaat om de situatie waarin mensen informatie toevertrouwen aan een overheidsdienst, waarna die informatie blijkbaar op een andere manier bij marktpartijen terechtkomt, geloof ik echt wel dat de overheid die informatie wel goed op orde heeft. Maar daar waar die informatie gedeeld wordt met een aantal marktpartijen, zit er toch een lek. Ik zou toch heel graag willen zien dat we binnen een aantal maanden weten wat we extra moeten beveiligen, zodat zo'n lek niet nog een keer kan ontstaan.

Staatssecretaris **Van Huffelen**:
Ik begrijp uw punt. We hebben het in dit geval niet zozeer over de overheid zelf, maar over partijen die wij inhuren om diensten of taken voor ons te verrichten. Deze partijen blijken dan onvoldoende te voldoen aan de bescherming die nodig is om te zorgen dat je geen datalekken hebt. Nu is 100% bescherming natuurlijk altijd ingewikkeld. Als het gaat over aanbestedingen en het vragen aan anderen om voor ons activiteiten te doen, hebben we daar allerlei regels over. Ik wil er graag nog even op kauwen of de aanbestedingsregels voldoende zijn en of wanneer je dat doet, je niet alleen goede afspraken maakt over bescherming, maar ook nog een soort extra waarborgen inregelt en in hoeverre we dat kunnen invullen op basis van al dan niet reeds bestaande regelgeving. Kijk, het is helder dat bedrijven dit niet mogen doen. Je mag geen data lekken. Dat is helder. Daar is de AVG voor, die allang geldt. Data lekken mag niet. Het gaat erom hoe wij, als we iemand vragen werk voor ons te doen, wat we altijd zullen blijven doen omdat we als overheid nu eenmaal vaak opdrachten geven aan partijen om iets te doen, beter kunnen zien of het vooraf zo kunnen beschermen dat er niks fout gaat. Ik wil daar graag nog even op kauwen. Daarna kom ik daar graag bij u op terug. Dat zal ik niet à la minute kunnen doen, dus niet in de tweede termijn, maar ik zal daar een brief over sturen.
Dan was er nog de vraag van de heer Slootweg over het beteugelen van big tech. Die ging erom of we die collectieve inkoop niet ook in andere sectoren zouden kunnen doen, bijvoorbeeld in de zorg. We delen daar actief kennis over. In het DPIA dat we gemaakt hebben over Google Workspace, een programma dat gebruikt wordt in het onderwijs, hebben we samengewerkt met een aantal andere internationale partijen. We hebben onze kennis en kunde daar gedeeld. We doen dat niet alleen in het kader van bijvoorbeeld dit soort onderhandelingen, maar we weten ook dat daar bijvoorbeeld in de zorg gebruik van wordt gemaakt.

De **voorzitter**:
Staatssecretaris, u krijgt nog een interruptie van de heer Rahimi over het vorige blok, geloof ik.

De heer **Rahimi** (VVD):
De Staatssecretaris heeft haar microfoon nog aan en ik zag dat dit een technisch probleem kan veroorzaken. Die is nu uit. Dank u wel.
Ik was heel blij met de opmerking over de aanbestedingen, want ik had zó'n blok dat ik moest overslaan. Ik probeer het even te begrijpen. U gaat kijken hoe we de aanbestedingen beter kunnen inrichten. Bij sommige aanbestedingen vind ik dat we in Nederland soms best wel kijken naar «ons ben zuunig» en «doe maar een Chinees laptopje» of wat dan ook. Is het op dat soort aspecten dat er soms niet gelet wordt op waar de hardware en de software vandaan komen, maar dat er te veel gelet wordt op de prijs? Of is dat op andere vlakken? U gaf daar heel kort iets over aan, maar ik voelde niet welke kan het opging.

De **voorzitter**:
De Staatssecretaris over aanbestedingen.

Staatssecretaris **Van Huffelen**:
Dan wil ik er wel even scherp op zijn. Er is nu een datalek voorgekomen, bij een marktpartij, die werd ingehuurd door andere marktpartijen en voor een deel ook door de overheid. Dat is niet oké; dat is niet goed. We willen dat ook zo veel mogelijk voorkomen. Maar het is niet zo dat alle data van de overheid nu voortdurend op straat liggen of dat alle aanbestedingen voor dit soort dingen fout gaan. Aan de heer Slootweg heb ik toegezegd om nog eens te bekijken waarom het toch nog fout kan gaan, want allerlei wet- en regelgeving geeft aan dat dit op orde moet zijn wanneer je iets aanbesteedt, en of er dan een extra waarborg nodig zou zijn. Ik wil dus ook een beetje het beeld wegnemen alsof de overheid voortdurend partijen inhuurt om daarmee de data van burgers te grabbel te gooien. Dat beeld zou niet goed zijn. Ik wil wel bekijken of het verstandig is om extra waarborgen of checks in te bouwen, om wat nu toch is fout gegaan een volgende keer te voorkomen.

De **voorzitter**:
Helder. Heel kort, meneer Rahimi.

De heer **Rahimi** (VVD):
Dat is toch iets anders dan wat ik bedoelde. Ik bedoelde als voorbeeld de hardware en infrastructuur van Huawei. Maar het is mij helder. Mijn punt was niet wat u net aangaf; het was niet mijn bedoeling om dat te zeggen. Dat wil ik nog even rechtzetten.

De **voorzitter**:
De Staatssecretaris gaat verder met haar beantwoording. Hoelang heeft u nog nodig?

Staatssecretaris **Van Huffelen**:
Dat kan ik niet helemaal overzien. Dat ligt natuurlijk ook altijd aan de interrupties. Ik denk tien, vijftien minuten.
De heer Slootweg had nog een vraag over de beveiliging van persoonsgegevens en de mens die vaak de zwakste schakel is. Dat ging met name over de medewerker bij de IDO's, dus de Informatiepunten Digitale Overheid bij bibliotheken. Hoe voorkomen we dat mensen die daar werken aan de haal gaan met data van de burgers die bij hen informatie vragen? Laten we er helder over zijn: de mensen die daar werken, krijgen een training om burgers te helpen met problemen, bijvoorbeeld wanneer ze moeite hebben met inloggen of niet goed weten hoe de digitale overheid werkt. Ze nemen nooit activiteiten of datgene wat de burger moet doen, over. Eerlijk gezegd is mijn eigen ervaring – ik heb inmiddels vele IDO's bezocht en blijf dat ook met grote regelmaat doen – dat mensen daar ook echt heel precies mee omgaan. Soms vinden ze dat zelfs

ook wel een beetje ingewikkeld. Ze zeggen: ik zou de burger nog een stapje verder kunnen helpen als ik wat meer zou mogen doen, bijvoorbeeld bij het aanvragen van een DigiD, omdat ik nu iemand weliswaar kan vertellen hoe je het moet doen, maar niet zelf even kan meekijken of dit kan doen. Ik vind het dus belangrijk dat we samen met de gemeenten gaan bekijken hoe we die hobbel oplossen. Dat wil ik niet doen om daarmee bevoegdheden te geven die ervoor zorgen dat dingen fout gaan, maar juist om mensen ook op een goede manier te helpen. Het is dus eerder zo dat de mensen die bij die IDO's werken, vinden dat ze te weinig kunnen doen dan te veel.
Dan was er ook de vraag hoeveel IDO's er op dit moment zijn. Er zijn er op dit moment 673. Er zijn in 2022 ongeveer 45.000 vragen gesteld, en meer dan 80.000 sinds 2019. Daartussen was er de coronaperiode, waarin er minder mogelijkheden waren voor mensen om naar de bibliotheek te gaan en vragen te stellen. Ze zijn gemiddeld zestien uur per week open. We hebben de gemeenten nu structurele financiering gegeven voor deze informatiepunten. Het is juist onze ambitie om samen met de gemeenten te bekijken hoe we het netwerk verder kunnen uitbreiden. Dat hoeft niet altijd alleen een bibliotheek te zijn. Het kan ook gebeuren op andere plekken dicht bij burgers, dus in een buurthuis of op een andere plek waar mensen gemakkelijk naartoe komen. Ik was deze week in Rotterdam en zag ook dat het nodig zal zijn om zelf naar burgers thuis toe te gaan. We ontwikkelen en rollen een programma uit om te zorgen dat iedereen kan meedoen in de digitale wereld. We zien ook dat het nodig kan zijn om bij mensen thuis te komen, omdat lang niet iedereen naar een bibliotheek, buurthuis of andere plek gaat. Dat willen we in de komende tijd ook verder gaan ontwikkelen.
U vroeg ook: waren er extra mensen rondom de belastingaangifte? Ja, dat hebben we ook samen met de Belastingdienst gedaan om te bekijken of er op die plekken extra mensen beschikbaar waren om vragen te beantwoorden.
Dan was er nog een vraag. Het gaat een beetje door elkaar heen, want ik kom weer terug op het thema van Facebook en Meta. De vraag van D66 was: hoeveel tijd willen we aan hen geven? We hebben het traject gestart met het idee dat we aan het eind van dit jaar een stap verder hopen te zijn. We zien wel dat dit soort trajecten tijd kosten. We zijn hier natuurlijk niet alleen zelf aan de bal. Het is een gesprek tussen twee partijen. Maar we hopen vooral aan het eind van dit jaar u meer te kunnen vertellen over waar we dan staan.
Dan was er de vraag van mevrouw Dekker-Abdulaziz over hoe je bij niet-noodzakelijke bedrijven zou kunnen aangeven dat je vergeten wil worden. Ze vroeg of ik op dat punt kan reflecteren. De AVG bevat al eisen daarover en zegt dat de hoeveelheid data die wordt gevraagd, de termijn daarvan en dataminimalisatie een rol spelen, en dat bij organisaties waar je zegt «ik wil vergeten worden» dat ook mogelijk is. Voor een deel is dat dus afgedekt in de AVG. Ook in de DSA, de Digital Services Act die voor online platforms gaat gelden, wordt niet alleen geregeld dat je vergeten kunt worden, maar ook dat je de aanbevelingsalgoritmes kunt uitzetten. Datzelfde geldt voor het gebruiken van data van minderjarigen voor advertentieprofilering. Met andere woorden, even heel kort reflecterend: ik vind het een belangrijk punt. Dat vergeten worden is dus onderwerp van de AVG en proberen we verder uit te werken in andere regelgeving. Ik bedoel niet alleen dat je helemaal vergeten kunt worden, maar ook dat je voorkeuren vergeten kunnen worden doordat je algoritmes kunt uitzetten.
Dan ga ik naar het laatste blokje over open source. De heer Rahimi had een vraag over DigiD en de broncode. De vraag is of dat niet leidt tot grotere kwetsbaarheid. Onze strategie bij open source is om broncodes te delen om daarmee de kwetsbaarheid van overheidssystemen te verminderen, door ervoor te zorgen dat partijen, al dan niet door onszelf daartoe uitgenodigd – we hebben dat in een eerder debat al besproken – mee

kunnen kijken naar hoe onze programmatuur eruitziet. Daarmee kunnen ze fouten eruit halen en aangeven of er zwaktes in die programma's zitten. Dat wil niet zeggen dat je daarmee de beveiligingssleutels ook openbaar maakt. Dat hebben we bij DigiD ook niet gedaan. Dat zou namelijk kunnen leiden tot veiligheidsrisico's. Dat willen we natuurlijk vooral voorkomen. Dus ons idee is vooral om open source te gebruiken om daarmee programma's veiliger te maken. Opensourcesoftware of combinaties van verschillende opensourceprogrammatuur is overigens ook iets wat heel veel partijen gebruiken. Maar we doen dat vanuit veiligheid en natuurlijk op een manier die verantwoord is, door ervoor te zorgen dat informatie die afbreuk doet aan de veiligheid van systemen, zoals versleutelingsmechanismes, wachtwoorden, verwijzingen naar technische infrastructuur enzovoorts, natuurlijk niet wordt gedeeld.

De **voorzitter**:
Een kort vraagje, meneer Rahimi, want u bent door uw interrupties heen.

De heer **Rahimi** (VVD):
Heel kort. Er is een verschil tussen een code die openbaar is, en een structuur en blauwdrukken die duidelijk zijn en een hacker die weet hoe daarmee om te gaan. Maakt u dat onderscheid dan wel, zodat kwetsbare burgers niet worden geraakt? Daar gaat het mij om, niet om dat er alleen in de software fouten zitten.

Staatssecretaris **Van Huffelen**:
Dat is precies wat het is. We willen niet ervoor zorgen dat daarmee de mogelijkheid ontstaat om juist het omgekeerde te doen van wat je wil, waarmee je het onveiliger in plaats van veiliger maakt. Die broncodes maken we openbaar om daarmee de programma's die wij gebruiken veiliger te maken. En we maken zelf ook gebruik van open source en van door anderen ontwikkelde software, bijvoorbeeld voor het aanbieden van diensten. Ik weet dat we bijvoorbeeld open source hebben gebruikt voor de corona-app.
Dan over DigiD en de toegankelijkheid daarvan. DigiD moet natuurlijk toegankelijk, betrouwbaar en veilig zijn. In 2022 was er een beschikbaarheid van 99,9%. Wij willen dat natuurlijk behouden. We zorgen ervoor dat DigiD steeds weer verder wordt ontwikkeld, niet alleen om ervoor te zorgen dat de beschikbaarheid groot blijft, maar ook om te zorgen dat het veilig blijft. Dat is wat ik daarover zou willen zeggen, ook naar aanleiding van een vraag van de heer Rahimi.
Volgens mij ben ik er dan doorheen. Ik dacht dat ik hiermee alle vragen had beantwoord. Maar als dat niet zo is, dan hoor ik het graag.

De **voorzitter**:
Ik zie in ieder geval opgestoken vingers. Of zullen we gewoon de tweede termijn beginnen? O nee, het is toch specifiek. Het woord is aan mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Excuus, voorzitter. De tweede termijn is al zo kort en ik heb nog zo veel. Ik wil graag nogmaals de Staatssecretaris even horen over DPIA. Klopt het dat er meerdere van dit soort onderzoeken lopen, ook naar andere socialemediaplatforms zoals LinkedIn en Twitter? De overheid is natuurlijk op meerdere platforms vertegenwoordigd. En zo ja, in welke fase zijn die en worden die net zo lang? Als dezelfde invulling, dezelfde redenering gevolgd wordt als bij het Facebook DPIA, dan vrees ik ervoor dat ze straks concludeert dat de overheid maar van alle socialemediaplatforms af moet.

De **voorzitter**:

Ik laat deze even toe, maar we gaan zo meteen toch over naar de tweede termijn. Eerst even de Staatssecretaris en dan gaan we toch over naar de tweede termijn, want het klonk heel erg als een tweede termijn.

Staatssecretaris **Van Huffelen**:
Misschien toch nog weer even, zeg ik dan tegen mevrouw Van Weerdenburg. Het is niet onze bedoeling om het onmogelijk te maken voor wie dan ook, inclusief de overheid zelf, om gebruik te maken van socialmediaplatforms, want we weten dat veel mensen daarvan gebruikmaken. Ons oogmerk is dat dat veilig kan op een manier waarbij die diensten voldoen aan de wetgeving die we in Nederland en in Europa hebben op dit gebied. Op dit moment loopt in een startfase een onderzoek naar de brillen die door Google worden gebruikt, sorry, door Meta worden gebruikt. Ik moet het goede bedrijf noemen. Dat zijn van die brillen die je gebruikt voor augmented reality of anderszins. Die worden in het onderwijs ingezet. Wij willen kijken of dat op een veilige manier gebeurt. Dat is het onderzoek dat op dit moment loopt.

De **voorzitter**:
Dank voor de beantwoording. Dan gaan we nu in verband met de tijd – excuses – toch alsnog over naar de tweede termijn. Ik geef het woord aan mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel voorzitter. Alvast de aankondiging dat hier nog niet het laatste woord over gezegd is, ook niet na mijn tweede termijn, want ik vind dit echt heel erg onbevredigend. Op mijn laatste vraag welke andere DPIA-onderzoeken er lopen, ook LinkedIn en Twitter, krijg ik alleen maar terug: nee, nog eentje naar Meta en dat is dan de Quest. Ik weet niet of de Staatssecretaris cijfers heeft over hoeveel jongeren rondlopen met zo'n Quest-headset. Het lijkt mij redelijk vroeg, dus ik hoor dat graag. Nu komt het een beetje over alsof het een soort onderhandelingstactiek is in de al lopende onderhandelingen.
Voorzitter. De PVV heeft zich ook in deze commissie al vaker verzet tegen de kruistocht die er gaande is tegen bigtechbedrijven. Het zijn nagenoeg allemaal Amerikaanse bedrijven. Ik vraag me af: wanneer hebben we besloten dat we ineens concurreren met de VS, dat het een soort vijandige ... We hebben gedeelde waarden. Het is altijd een bevriend land geweest. We hebben altijd samengewerkt. Ook Nederlandse bedrijven zijn daar groot mee geworden en door geworden. Ik denk dat die weerzin voortvloeit uit antiamerikanisme en afgunst, en vooral dat een groepje machtswellustelingen in Brussel die wereldregerinkje willen spelen dit allemaal instigeren. Nou moet er ineens overal een Europees alternatief voor komen. Wij zien graag de lijn die de Staatssecretaris wél volgt bij het cloudbeleid. Op dit moment zijn de beste en de veiligste aanbieders nou eenmaal big tech, de grote Amerikaanse bedrijven. Natuurlijk blijven we de Europese initiatieven financieren en wie weet komt er ooit een volwaardig Europees alternatief. Dat zou mooi zijn; daar hopen wij ook op. Maar tot die tijd gaan we gewoon in zee met degenen die het beste product kunnen leveren, een volwaardig alternatief. En die lijn ...

De **voorzitter**:
Ik ga u heel even onderbreken, want u krijgt een interruptie, eerst van de heer Slootweg en daarna van de heer Rahimi.

De heer **Slootweg** (CDA):
Ik vind het in ieder geval prachtig om te horen hoe belangrijk mevrouw Van Weerdenburg de samenwerking tussen de Verenigde Staten en Nederland vindt. Ik hoop dat we dan in het vervolg ook mogen rekenen op de steun van de PVV als daar een beroep op wordt gedaan, ook op het

terrein van Defensie. Maar dat terzijde. Vindt mevrouw Van Weerdenburg het ook niet van belang dat als wij hier in dit parlement met regelgeving, wetgeving, komen waarin staat waar bigtechbedrijven aan moeten voldoen, ze zich dan ook moeten houden aan die Nederlandse wetgeving, of ze nou uit China komen, uit de Verenigde Staten of uit welk land dan ook? Of vindt ze dan dat de Amerikaanse wetgeving boven de Nederlandse wetgeving gaat, vanwege ons bevriend partnerschap?

Mevrouw **Van Weerdenburg** (PVV):
Dank aan de heer Slootweg voor de vraag. Natuurlijk moet aan de Nederlandse wet worden voldaan. Ik heb ook helemaal niets anders beweerd. Maar we moeten niet doen alsof hier een rechterlijke uitspraak voorligt die constateert dat Facebook daar niet aan voldoet. Dat is wel de waarde die hier nu gehangen wordt aan een rapport van twee mensen. Nogmaals, daar is genoeg op aan te merken. Dat ga ik niet nu doen. Begrippen worden daarin op een andere manier geïnterpreteerd. Nogmaals, dit is geen rechterlijke instantie die the be-all and end-all is, waardoor we moeten zeggen: ach, nou kunnen we niet anders dan weggaan van Facebook. Zo wordt dat hier wel neergezet, en daar verzet ik me tegen. Daar heb ik me vaker tegen verzet. Ik wil alleen maar aangeven dat dit ingegeven is door motieven die niet de mijne zijn en waar de PVV gewoon vraagtekens bij zet. Natuurlijk zou het mooi zijn als overal een werkend, volwaardig Europees alternatief voor was, en natuurlijk moet ook Amerikaanse big tech voldoen aan regelgeving. Ik zie dus niet in waar we op dit punt anders over denken dan het CDA.

De **voorzitter**:
Helder. De heer Slootweg heeft een vervolgvraag.

De heer **Slootweg** (CDA):
Ik dank mevrouw Van Weerdenburg voor dit antwoord. Daarmee begrijp ik het wel zo dat zij vindt dat als de Staatssecretaris constateert dat een Amerikaans bigtechbedrijf zich niet houdt aan de Nederlandse wetgeving, dat het vertrekpunt moet zijn voor de Staatssecretaris om een gesprek aan te gaan met Amerikaanse big tech, Chinese big tech of big tech overall over the world.

De **voorzitter**:
In goed Nederlands.

Mevrouw **Van Weerdenburg** (PVV):
Dat is iets te kort door de bocht. Nogmaals, er is een privacyonderzoek uitgevoerd, en dat is uiteindelijk de basis van het politieke besluit dat de Staatssecretaris hopelijk wel in gesprek met de Kamer gaat nemen. In ieder geval wil ik daar als Kamerlid ook iets over te zeggen hebben. Ze mag het natuurlijk als basis nemen, maar ze moet niet doen alsof ze niet anders kan dan van Facebook af gaan nu uit dit rapport blijkt dat het allemaal niet in de haak is. Zo is het niet. Dat is ook niet eerlijk. En als het zo'n waarde heeft – ik vind van niet, maar goed – dan is het helemaal belangrijk dat we als Kamer allemaal alle 150 pagina's in het Nederlands lezen en uitpluizen en alle vragen stellen die we daarover willen stellen. Dan krijgt het namelijk een soort waarde die het niet zou moeten hebben, en dan vind ik het raar dat dit alleen bij Facebook, bij Meta, wordt ingezet en niet bij al die andere socialmediaplatforms.

De **voorzitter**:
Helder. U had nog een interruptie van de heer Rahimi.

De heer **Rahimi** (VVD):

Er was wel een Nederlands alternatief. Dat was Hyves. Volgens mij is dat toen overgenomen door Facebook.
Ik snap het punt van mevrouw Van Weerdenburg dat Amerika een bevriende staat is. Maar ik kom uit een gebied in de wereld waar regimes weleens wisselen. Is mevrouw Van Weerdenburg het met mij eens dat we ook vooruit moeten zien en daarvoor moeten uitkijken? Niet dat dat gebeurt, hoor. Ik zie echt nooit voor me dat iemand het Capitool bestormt of dat soort dingen. Maar áls er iets gebeurt, ook in een bevriend land, is alles omgedraaid. Moeten we niet ook daarvoor waken en ervoor zorgen dat er juist aan de Nederlandse wetgeving moet worden voldaan? Dat is één. Twee: nog bedankt, want die vraag die niet beantwoord was, de vraag om juist alles te onderzoeken, heb ik ook gesteld. Dus nog een bedankje daarvoor.

Mevrouw **Van Weerdenburg** (PVV):
Ik had van een heleboel mensen hier aan tafel de Trump-angst verwacht, maar niet van mijn collega van de VVD. Dat is een beetje teleurstellend, maar goed. Ik ben het er natuurlijk mee eens dat er altijd een regime change kan komen, ook in de Verenigde Staten. Ik zeg ook niet dat we niet moeten proberen om een volwaardig Europees alternatief te bereiken. Je moet dan overigens ook nog maar hopen dat het in Europa allemaal koek en ei blijft. Op dit moment is er geen Europees alternatief voor een heleboel dingen. Het is een gegeven, een fact of life, dat het allemaal Amerikaanse grote bedrijven zijn die deze ontwikkelingen, bijvoorbeeld in de cloud, leveren. Daar kun je van balen – dat doe ik ook wel een beetje – maar het is nou eenmaal zo. Gaan we nou daadwerkelijk zeggen: eigenlijk is dit het beste alternatief, eigenlijk is dit de enige oplossing, maar ja, het is zo'n groot Amerikaans bedrijf en je weet maar nooit, dus we doen het maar niet? Dit is een politieke discussie die we hier uitgebreid gehad moeten hebben voordat we dat soort beslissingen nemen.

De **voorzitter**:
Helder. U bent duidelijk. De heer Rahimi nog heel kort.

De heer **Rahimi** (VVD):
Ik zei niet dat ik anti-Trump of whatever ben en ik pleitte ook niet voor verbieden. Ik zeg dat we moeten blijven praten om dichterbij te komen. Tech moet je gebruiken om er de juiste dingen mee te doen, maar men moet wel zijn best doen om zich aan de regels te houden. Dat is het enige dat ik zeg.

De **voorzitter**:
Dat behoeft geen antwoord, dus ik ga gelijk naar mevrouw Leijten, dan kan mevrouw Van Weerdenburg in één keer antwoorden.

Mevrouw **Leijten** (SP):
Ik heb niemand horen zeggen wat mevrouw Van Weerdenburg hier nu zo groot maakt. Dat punt wil ik graag even gemaakt hebben.

De **voorzitter**:
Mevrouw Van Weerdenburg, een korte reactie. U heeft al twee minuten gesproken, dus u komt tot een afronding.

Mevrouw **Van Weerdenburg** (PVV):
Oké, voorzitter. In reactie op mevrouw Leijten: zo wordt het wel in de media ingezet. Met mevrouw Leijten hoop ik dat de soep niet zo heet gegeten wordt. In Het Financieele Dagblad en op AG Connect zie je termen als big tech enzovoort. Ik neem daar aanstoot aan, want dan kom je niet tot een fatsoenlijke onderhandeling. Dit is een heel groot bedrijf dat echt wel wil meedenken in de zin van «wat kunnen we doen om jullie te

accommoderen». Het bedrijf heeft er geen baat bij dat de overheid zegt: aju paraplu. Dan moet je het niet via de media spelen en zeggen: wij eisen dit en dat. Dat is toch geen onderhandeling? Daar neem ik aanstoot aan. Ik hoop het niet, maar ik vrees dat we die kant opgaan. Nogmaals, ik hoop dat ik aan het overreageren ben, maar better safe than sorry.

De **voorzitter**:
Mevrouw Van Weerdenburg, u hoeft nog niet af te ronden, want er is nog een interruptie van mevrouw Bouchallikh.

Mevrouw **Bouchallikh** (GroenLinks):
Een hele korte vraag: komt de PVV op voor de belangen van de Nederlandse burger of voor een Amerikaanse multinational?

Mevrouw **Van Weerdenburg** (PVV):
Dank voor die vraag, want dat willen we heel graag ophelderen. Vanaf dag één heeft de PVV dit naar voren gebracht. Er zijn ruim 5 miljoen mensen die hun informatie van de overheid krijgen via Facebook. Ik heb geen Facebookaccount – nooit gehad – en ik ben het er ook niet mee eens, maar het is wel zo. Die burgers hebben recht op informatie. Ik heb het gevoel dat dat niet genoeg wordt meegewogen in deze beslissing. Ik snap de reactie van «boe, rotbedrijf, veel te veel macht», maar helemaal achteraan staan die burgers daar. Daar is de PVV altijd voor opgekomen. Die burgers hebben straks dat informatiekanaal niet meer en die krijg je ook niet allemaal naar Mastodon. Het is prima als de overheid als primair kanaal de eigen website gebruikt of Mastodon, maar zet dan een kopietje op alle andere socialmediakanalen. Ik vind het belangrijk om dat in het oog te houden: dat informatiekanaal is een recht en dat moet blijven bestaan. Natuurlijk kunnen we erover praten hoe dat beter kan. Daar hebben we ons nooit tegen verzet. Omdat de PVV de enige partij is die dit redelijke argument hier inbrengt, is het misschien net alsof ik gestuurd wordt door Facebook, Meta of wat dan ook, maar ik kan mevrouw Bouchallikh geruststellen: dat is zeer niet het geval.

De **voorzitter**:
Dank. U kunt uw betoog kort vervolgen.

Mevrouw **Van Weerdenburg** (PVV):
Ik had denk ik het meeste wel genoemd. Nogmaals, ik wil deze discussie op een later moment in rust kunnen voeren. Dan kunnen we het ook hebben over alle overige vragen die nu nog blijven liggen. Maar dit moet dus een politieke discussie zijn en niet, zoals het nu wordt ingestoken, in de trant van «kijk, hier ligt een oordeel; we kunnen niet anders». Dat is echt niet het geval. Ik hoop dat ook de andere collega's hier aan tafel, ook al zijn ze het niet allemaal met ons eens, zichzelf serieus willen nemen en vinden dat we over dit soort beslissingen hier moeten discussiëren. Ik wil geen stukken in de media lezen terwijl we zelf niet eens een briefje hebben gehad over hoe de onderhandelingen verlopen.
Tot slot hoor ik graag van de Staatssecretaris wanneer we de Nederlandse vertaling kunnen ontvangen.

De **voorzitter**:
Dat wilde ik bij de toezeggingen ook vragen. Ik geef het woord aan de heer Rahimi.

De heer **Rahimi** (VVD):
Dank u wel, voorzitter. Ik kreeg niet de gelegenheid voor een interruptie – dat snap ik – maar ik was degene die vroeg of u naast Facebook ook wilt kijken naar andere platforms en of u dat wilt onderzoeken. Dat antwoord kreeg ik niet, maar gelukkig werd die vraag alsnog gesteld. Ik heb ook

gevraagd hoe wij de oplossingen bewaken in het kader van de zeven hoge en het ene lage privacyrisico. Ik hoef daar nu niet per se een antwoord op; ik vind het fantastisch als wij een technische briefing krijgen.
In de IT wordt vaak een tegenstelling gecreëerd: je wilt het veilig, maar dan wordt het minder gebruiksvriendelijk. Ik roep u op om daar niet in te trappen. Er hoeft geen tegenstelling te zijn tussen toegankelijkheid en een makkelijk systeem. Dan heb je minder vaak extra hulp nodig of mensen die bij je thuis moeten komen, wat op zichzelf mooi is. Maak het systeem meteen toegankelijk en goed. Dat is geen contradictie.
Voorzitter. Het is goed om het structureel in de gaten te houden. Wij hebben niks tegen big tech. Big tech kan goed gebruikt worden. Er zijn hier ook hele mooie grote bigtechbedrijven. Ik noem geen namen, maar ze zijn er gewoon. Het zijn grote bedrijven die veel banen hebben gecreëerd. Daar staan wij als VVD ook echt voor. We moeten die bedrijven niet weren, maar we moeten wel opletten en in gesprek blijven: in dit land vinden we dit belangrijk en daar moet u aan voldoen. Dat is wat wij vanuit de VVD zeggen.
Wij zijn ook benieuwd wanneer wij de vertaling krijgen en de extra input.

De **voorzitter**:
Meneer Rahimi, u krijgt een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Heel kort. Mag ik het betoog van de heer Rahimi als volgt samenvatten? De VVD wil net als de PVV het beste voor de Nederlandse burger, ongeacht of het een Amerikaans bigtechbedrijf is of een Europese oplossing of wat dan ook.

De heer **Rahimi** (VVD):
Dat vind ik echt ontzettend moeilijk. Alsof ik zou weten wat het beste is voor de Nederlandse burger. U gaf aan dat 5 of 5,2 miljoen mensen willen communiceren. Dat moeten we niet zomaar aan de kant schuiven. Het is niet zo dat wij moeten weten wat het beste op elk gebied is voor de Nederlandse burger.

De **voorzitter**:
Dank. Keurig binnen de tijd. Mevrouw Bouchallikh voor de tweede termijn.

Mevrouw **Bouchallikh** (GroenLinks):
Dank u wel, voorzitter. Dank aan de Staatssecretaris en haar team voor de beantwoording van de vragen. In mijn bijdrage heb ik het gehad over de verschillende niveaus waarop we beleid en politiek aan het maken zijn, zowel op Europees als op nationaal niveau, ook als het gaat om overheden. Ik vind het ontzettend belangrijk om op dat laatste punt terug te komen. Ik ben niet helemaal gerustgesteld als de Staatssecretaris zegt dat zij niet kan garanderen dat lagere overheden de capaciteiten en de middelen hebben om te voldoen aan datgene wat we hier met z'n allen besluiten. Ik betwijfel niet dat er in alle lagen van de samenleving en de overheid sprake is van goede wil, maar we zien toch te vaak dat het misgaat. Die zorg wordt ook vanuit de lagere overheden zelf geuit. Ik wil mijn tweede termijn gebruiken om aan te geven dat juist die lagere overheden vaak het gezicht van de onlineoverheid voor de burger zijn. Ik doe nog een keer de oproep om toch een stok achter de deur te bedenken, om manieren te vinden om toch te faciliteren en de capaciteit te vergroten, juist ook om te voorkomen dat de burger uiteindelijk het vertrouwen in de onlineoverheid verliest.

De **voorzitter**:
Dank. U krijgt een interruptie van de heer Rahimi.

De heer **Rahimi** (VVD):
Ik bedank mevrouw Bouchallikh, want ik was inderdaad een vraag vergeten. Ik snap wat u aangeeft. Bij gemeenten, waterschappen en provincies zitten namelijk ook persoonsgegevens die beveiligd moeten worden. Wat vindt mevrouw Bouchallikh ervan dat gemeenten en provincies de vrijheid moeten hebben om op hun eigen manier eigen systemen met eigen software te ontwikkelen? Hoe staat zij daarin?

Mevrouw **Bouchallikh** (GroenLinks):
Toen ik als Kamerlid begon met dit dossier heb ik me heel vaak verbaasd over hoe vaak er een gebrek aan capaciteit, kennis en kunde is als het gaat om ICT en online organisatie van overheden. Op nationaal niveau gaat het helemaal niet goed, laat staan als het gaat om lagere overheden die, zoals ik net al aangaf, beperkte capaciteit, kennis en kunde hebben. Dus op dit moment lijkt het mij niet verstandig om dat te doen. Wat ik wél heel belangrijk vind, is dat we kijken naar hoe we al die overheden kunnen helpen om in ieder te voldoen aan de eisen die we nu met z'n allen stellen en dat we misschien later kunnen kijken naar de ontwikkeling. Laten we eerst orde op zaken stellen.

De **voorzitter**:
Meneer Rahimi heeft een vervolgvraag.

De heer **Rahimi** (VVD):
Misschien heb ik de vraag niet duidelijk gesteld. Wat ik daarmee bedoel, is dat elke gemeente die vrijheid heeft en dus van alles ontwikkelt. Het is dan soms best lastig dat er allemaal verschillende systemen zijn als je bij 345 gemeentes iets wil regelen. Dat is waar ik op doel. Zouden we dan iets strikter moeten zijn, zodat die vrijheid er niet is? Dat was eigenlijk mijn vraag, maar misschien heb ik hem niet goed gesteld.

De **voorzitter**:
Dat was uw laatste interruptie. Mevrouw Bouchallikh voor een antwoord.

Mevrouw **Bouchallikh** (GroenLinks):
Dank voor deze vraag. Ik vind het ook een belangrijke vraag, juist omdat ik de Staatssecretaris heb gevraagd of zij kan garanderen dat dingen opgelost worden. Als dit een oplossing zou kunnen zijn, dan wil ik daar best naar kijken. Ik moet eerst weten wat de alternatieven zijn, vandaar mijn constante vraag aan de Staatssecretaris. Zij geeft aan dat we in gesprek moeten gaan, maar dat vind ik nog niet voldoende.

De **voorzitter**:
Helder. Mevrouw Van Weerdenburg voor een interruptie.

Mevrouw **Van Weerdenburg** (PVV):
Ik heb even getwijfeld, want mevrouw Bouchallikh spreekt ook namens PvdA en ik weet dat mevrouw Kathmann in het verleden ook echt altijd een lans brak voor overheidsinformatie die de burgers goed kan bereiken. Ik vind het moeilijk te rijmen met de kritische houding die mevrouw Bouchallikh tegenover Facebook en de hele DPIA heeft. Maar ik vind het ook niet netjes om haar nu aan te vallen op een PvdA-standpunt. Dus ik wil alleen even markeren – misschien kan ze er nog op reageren – dat het een beetje wringt.

De **voorzitter**:
Een vraag was wel beter geweest. Mevrouw Bouchallikh voor een reactie.

Mevrouw **Bouchallikh** (GroenLinks):

Ik vroeg net aan de PVV of zij opstaat voor de belangen van de big tech of van de burger. Wij proberen beide te doen. Althans, we staan niet op voor de belangen van de big tech, maar we willen dat zij zich aan de regels en de wetten gaan houden. Zo kan de burger nog steeds met Facebook omgaan. Maar we zien gewoon dat het constant en structureel niet gebeurt. Dus ja, de toegang van de burger tot informatie is belangrijk, maar we hechten ook ontzettend veel aan diens privacy. We willen die zaak in balans brengen. Dat is een zoektocht die we hier, volgens mij met z'n allen, aan het doen zijn.

De **voorzitter**:
U was ook klaar met uw betoog. Dan gaan we door naar de heer Slootweg.

De heer **Slootweg** (CDA):
Dank u wel, voorzitter. Ik wil de Staatssecretaris bedanken voor de toezeggingen. Wat ik met name belangrijk vind om te horen, is dat vanuit het IDO outreachend gewerkt gaat worden, ook voor mensen die daar eigenlijk niet naartoe kunnen gaan. Ik denk dat dat echt een hele belangrijke voorwaarde is. Het is misschien wel een beetje de verkeerde volgorde, want in eerste instantie wil je dat iedereen gewoon kan deelnemen en dat digitaliseren een hulpmiddel is. Nu is het vaak de enige polsstok waarmee je eigenlijk een riviertje over kunt komen. Dat blijft gewoon raar.
Ik wil de Staatssecretaris nog wel even vragen of ik haar nu goed begrijp als het gaat om de marktmacht die bij een aantal partijen ligt. Vanuit het CDA vinden wij dat je zelf eigenaar bent over je persoonsgegevens. Ik vind het zorgelijk dat je nu ziet dat heel veel van die data toch opgeslagen zijn bij Amerikaanse bedrijven en dat het moeilijk is om die data terug te kunnen krijgen. Ik begrijp de inzet om te zorgen voor andere partijen waar je terechtkunt, want dat is misschien ook wel de eerste voorwaarde. Daarna moeten we nog wel dat eigenaarschap, dat jij zelf eigenaar ben van jouw data, terug zien te krijgen. Hoe ziet de Staatssecretaris het traject voor zich waarin we uit dat lock-ineffect komen? Ik hoop dat ze daar nog enkele woorden aan zou kunnen wijden.

De **voorzitter**:
Komt er een interruptie van mevrouw Leijten?

Mevrouw **Leijten** (SP):
Nee hoor.

De **voorzitter**:
Dank voor uw betoog. Dan gaan we door naar mevrouw Leijten.

Mevrouw **Leijten** (SP):
Ik vond het een goed en helder betoog van het CDA. Ik kan me daar grotendeels bij aansluiten. Het heeft niets te maken met antiamerikanisme. Het heeft vooral te maken met datgene doen wat de technologie je aanbiedt of zelf beslissen over wat je wenselijk vindt voor snelheid in de samenleving. Die vraag is niet beantwoord door de Staatssecretaris. We hebben altijd gezegd «digitaal waar het kan» maar moeten we het niet omdraaien? Moeten we niet zeggen: moet het altijd digitaal als het kan? Ik snap wel dat het een heel ander denkparadigma is, maar de bypasses die we nu hebben, via de bibliotheken en digitale ondersteuning, zijn uiteindelijk een hulpmiddel voor contact met een overheid die gewoon beschikbaar moet zijn. Het is altijd wel de Kamer die zegt: hou sowieso ook de analoge optie open. We weten dat dat eigenlijk bij belastingaangifte helemaal niet meer kan. Mevrouw Dekker-Abdulaziz zegt als voorzitter: het kan wel. Ja, maar ga eens proberen wat je moet opvragen.

Feitelijk kan het niet meer. Als het gaat over die authenticatie met DigiD dan willen we natuurlijk ook dat het veilig is. Maar als je ziet dat er zoveel waarborgen nodig zijn dat dit ook weer groepen gaat uitsluiten, dan heb je juist dat politieke debat nodig. Waartoe hebben we de digitale ondersteuning? Of is het een digitale voorkeur? Daar heb ik de Staatssecretaris nog geen duidelijk antwoord op horen geven. De Staatssecretaris kent mij als volhardend en vasthoudend om dit onder haar aandacht te blijven brengen.
Dan de veiligheidsstrategie. Ik heb haar gevraagd over de vitale functies in onze samenleving. We hebben dan die zoveel duizend doden en 5 miljard impact op het bruto binnenlands product. Ik vroeg haar in alle serieusheid: is dat nog de juiste graadmeter? Het kan best zijn dat ze daar nu geen antwoord op heeft en dat ze daar nog op terugkomt. Maar ik vraag me dat echt serieus af.
Voorzitter, ik ben al over de tijd. Dank u wel.

De **voorzitter**:
Dat klopt. Ik zie dat de heer Rahimi nog wil interrumperen, maar hij is door zijn interrupties heen. Volgende keer appen!
Dan geef ik het voorzitterschap aan mevrouw Van Weerdenburg.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dank u wel. Dan heeft u nu tijd voor uw tweede termijn namens D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Ik heb nog een aantal vragen. Laat ik de Staatssecretaris eerst bedanken voor de antwoorden. Ik wil het eerst over de encryptie hebben. Het is ons bekend wat JenV vindt, want dat is wat de Staatssecretaris vertelde over client-side scanning. Maar we zijn zo benieuwd of deze Staatssecretaris het met D66 eens is dat client-side scanning, hoewel legaal, de encryptie en daarmee de veiligheid van de gegevens ondermijnt?
Dan over de cookiewetgeving. De cookies worden nu klakkeloos door iedereen uitgegeven. Wat zijn precies de concrete plannen van de Staatssecretaris?
Tot slot wilde ik zeggen wat wij vinden van die discussie over Facebook. D66 vindt dat een bedrijf niet groter is dan een land. Dat heeft een andere collega ook al gezegd. Bedrijven moeten zich houden aan de wet, maar we zijn wel benieuwd hoe de Staatssecretaris kijkt naar de afhankelijkheid van deze platformen voor de informatie voor de burgers. Wat gaan we doen om de juiste informatie bij die 5,5 miljoen burgers te krijgen? Hoe kijkt ze bijvoorbeeld aan tegen ontwikkelingen als PublicSpaces?
Dank, voorzitter.

De **voorzitter**:
Dank u wel. Dan krijgt u het voorzitterschap terug.

Voorzitter: Dekker-Abdulaziz

De **voorzitter**:
Dank. We zijn door de tweede termijn heen. Ik schors de vergadering voor vijf minuten.

De vergadering wordt van 12.37 uur tot 12.42 uur geschorst.

De **voorzitter**:
Ik zie dat de Staatssecretaris er al is. Ik geef haar het woord.

Staatssecretaris **Van Huffelen**:
Dank u wel, voorzitter. Ik zou graag nog de vragen beantwoorden die in tweede termijn zijn gesteld.
De vraag van mevrouw Van Weerdenburg was waarom we nu al aan het werk gaan met het kijken naar de mate waarin bijvoorbeeld die Metabrillen voldoen aan de vereisten die wij daaraan stellen. De belangrijkste reden daarvoor is dat het in dit geval gaat om de inzet voor kinderen en dus ook over kinderrechten. Wij achten het in dat verband van belang. We vinden het natuurlijk ontzettend belangrijk om juist dat te bereiken wat mevrouw Van Weerdenburg volgens mij ook wil. We willen dit soort ontwikkelingen niet tegenhouden, maar juist mogelijk maken. Maar we willen er wel voor zorgen dat de bedrijven die dit soort diensten of producten aanbieden voldoen aan de Nederlandse wet- en regelgeving, juist om mensen te beschermen.
Zij stelde, net als de heer Rahimi, ook de vraag voor welke andere platforms ik aan het werk ben. Ons idee is inderdaad om dit verder te gaan ontwikkelen. Ik zou u eigenlijk willen toezeggen dat ik een voorstel daarvoor zal opsturen naar uw Kamer, zodat u weet wat de volgende stappen zijn die wij willen zetten en wat de volgende bedrijven, of beter gezegd services, zijn die wij onder de loep willen nemen.
Mevrouw Van Weerdenburg maakte ook nog het volgende punt. Ze vroeg: wat gebeurt er nu, en is het zo dat de Staatssecretaris hier een strategie kiest waarbij de rechterlijke macht geen rol speelt? In het geval van Facebook is dat wel degelijk ook aan de orde, want de rechtbank in Amsterdam heeft de constateringen van onze DPIA recentelijk nog onderschreven.
Dan ga ik naar de vragen van de heer Rahimi.

De **voorzitter**:
Staatssecretaris, mevrouw Van Weerdenburg heeft nog een vraag hierover.

Mevrouw **Van Weerdenburg** (PVV):
Ja, even over het eerste punt, dat van die VR-brillen. Ik heb helemaal niet willen zeggen dat we daar niet heel scherp op moeten zijn. Ik denk dat deze Kamercommissie daar ook heel goed aandacht voor heeft. Ik vind het alleen maar goed dat de Staatssecretaris daar heel scherp op is. Maar moet dat per se weer in de vorm van een DPIA? Ten eerste duurt het lang. Ik weet niet of dat het goede instrument is, want ook voor de metaverse geldt: het is allemaal in ontwikkeling, en wat er vandaag mogelijk is, is misschien weer helemaal anders als dat rapport is opgeleverd. Dan zijn er misschien weer andere toepassingen. We hebben bij AI gezien hoe snel het gaat. Dit komt dus een beetje vroeg over. Daarom dacht ik: heeft dat niet te maken met de onderhandelingen met Meta? Maar goed, misschien zie ik dingen die er niet zijn.

De **voorzitter**:
Dat is een duidelijke vraag.

Staatssecretaris **Van Huffelen**:
U hoeft er niks anders achter te zien dan wat wij u vertellen. Ik denk dat het heel belangrijk is dat wij ons werk in alle opzichten in alle transparantie doen. Daar informeren we u ook over. Nogmaals, ik vind het zo belangrijk dat we dit doen en ook zo vroegtijdig doen omdat dit zich de komende tijd wellicht verder gaat ontwikkelen. We gebruiken de instrumenten die we daarvoor hebben, maar we gaan daar ook niet meer tijd voor nemen dan nodig is. We hopen dat dus zo snel mogelijk in te zetten. We doen dit overigens ook samen met scholen, want scholen zijn degenen die deze brillen gaan gebruiken. We doen dat op hun verzoek.

Daarom vind ik het belangrijk om dat door te zetten. Ik ben blij dat mevrouw Van Weerdenburg dat ondersteunt.

De **voorzitter**:
De Staatssecretaris gaat verder.

Staatssecretaris **Van Huffelen**:
Dan ga ik door met de vraag van de heer Rahimi over dat voorstel rondom andere platforms. Ik heb net al gezegd dat ik met een aanpak daarvoor zou willen komen. Wij gaan de vertaling zo snel mogelijk naar u toe sturen. Ik weet niet precies hoelang dat duurt. Die juridische vertalingen zijn altijd een beetje complex, maar ik hoop dat het niet meer dan enkele weken duurt. Wat betreft uw oproep over de balans tussen veilig en gebruikersvriendelijk: wij willen dat natuurlijk zo veel mogelijk in balans brengen, maar we zien wel dat er soms toch uitdagingen zijn. Het is niet zo dat veilig niet gebruikersvriendelijk kán zijn, maar we zien tegelijkertijd ook, bijvoorbeeld bij de beveiligingseisen voor DigiD, dat veiligheid wel degelijk kan leiden tot minder gebruikersvriendelijkheid voor een deel van de inwoners van dit land. Daarom moeten we daar goed naar kijken. Als er problemen ontstaan, dan weet u mij te vinden. Dan dat hebben we ook in dit debat gezien. Tegelijkertijd willen we er ook voor zorgen dat mensen gewoon gebruik kunnen blijven maken van onze dienstverlening.
Dan de oproep van mevrouw Bouchallikh. In het kader van het convenant dat is gesloten met de gemeenten ben ik, samen met het Ministerie van JenV, hard aan het werk om gemeenten zo veel mogelijk te ondersteunen. Daarin speelt een rol dat gemeenten zeker ook hun eigen afweging kunnen maken. Ik vind het belangrijk dat gemeenteraden kritisch blijven kijken naar de dienstverlening en de beveiliging van de digitale diensten die worden geleverd door een gemeente. Daar roep ik ze ook steeds toe op. Ik wil dus vooral dat we niet alleen maar in gesprek blijven – dat is het niet, zoals u zegt – maar dat het ook leidt tot goede afspraken. Ik hou u daar graag van op de hoogte. Niet alleen dat; ik wil er ook vooral samen voor zorgen dat de wetgeving die we aan het ontwikkelen zijn ertoe leidt dat we zeker weten dat er voldoende waarborgen blijven bestaan op het gebied van veiligheid. Ik denk dat we hier nog niet mee klaar zijn, maar dat we hier de komende tijd met elkaar over in gesprek moeten blijven.
Dan de opmerkingen en vragen van de heer Slootweg. U zei: kiezen we niet de verkeerde volgorde? Dat is toch een balans die je elke keer blijft zoeken, denk ik. We weten namelijk dat ongelofelijk veel Nederlanders het heel fijn vinden dat ze digitaal zaken kunnen doen met de overheid, niet alleen in de rest van hun leven, maar ook met de overheid. Het maakt dat je het kunt doen op een moment dat je zelf prettig vindt, dat je er de deur niet voor uit hoeft en dat het in heel veel gevallen ook veel makkelijker is. Dat niet iedereen mee kan komen, is ook helder. We moeten er dus alles aan doen om mensen daarmee te helpen. Dat hebben we afgesproken. Dat doen we niet alleen door ervoor te zorgen dat dienstverlening ook altijd offline kan, dus gewoon met face-to-facecontact aan een loket of door te bellen, maar ook door mensen te helpen die graag digitaal vaardiger willen worden. Dat willen we ook blijven doen. Dat is eigenlijk mijn antwoord daarop. Die combinatie willen we altijd blijven behouden.
Dan was er nog de vraag over het eigendom van persoonsgegevens. Daarover is er in het verleden al een grote juridische discussie geweest: wie is nou eigenlijk de eigenaar van persoonsgegevens? Daarbij is vooral het volgende van belang. Het is niet zo dat je persoonsgegevens als eigendom van jezelf kunt beschouwen. We willen er wel voor zorgen dat mensen in staat zijn en het recht hebben om hun persoonsgegevens te beschermen en te bepalen wie die persoonsgegevens wel en niet heeft. De overheid heeft die natuurlijk altijd. Maar het is vooral ook van belang dat je tegen private instellingen moet kunnen zeggen dat ze je moeten vergeten, dus dat je persoonsgegevens daar niet meer mogen worden

opgeslagen, en dat gegevens die je hebt, kunnen worden verhuisd van de ene dienst naar de andere. Daar gaat de Europese regelgeving over. Als je gebruikmaakt van een dienst als WhatsApp, is de bedoeling van de regelgeving dat als je daar niet meer gebruik van wilt maken, je je gegevens kunt verplaatsen naar een andere berichtenservice. Ik denk dat het ongelofelijk belangrijk is dat we dat blijven invullen, omdat we er ook voor willen zorgen dat mensen, als het bijvoorbeeld specifiek over de overheid gaat, niet alleen maar weten welke gegevens de overheid over hen heeft, maar ook wat daarmee gebeurt, welke inzichten er zijn en hoe ze er regie over kunnen houden welke data er bij wie zijn.
Dan de vraag van mevrouw Leijten. Die ging over het onderwerp waar ik het net ook over had. Het blijft ontzettend belangrijk dat mensen ook niet digitaal, dus analoog, gewoon in het normale leven, bij een loket of via de telefoon, terechtkunnen bij de overheid. Het is ook van belang dat dat op een hele goede manier mogelijk blijft. Wil ik daarmee zeggen dat we niet ook digitale dienstverlening moeten inzetten? Jawel, want heel veel mensen vinden dat juist heel erg prettig.
Dan specifiek over de veiligheidsstrategie. Er zijn inderdaad definities gemaakt om aan te geven wat behoort tot de vitale functies. Die hebben we ook in Europa afgesproken. Het is van belang dat we daar wel kritisch naar blijven kijken, want bij processen die misschien niet vitaal zijn, maar waarbij wel heel veel persoonsgegevens worden gedeeld, de zogenaamde hoogrisicocategorieën, is zorgvuldigheid natuurlijk ontzettend belangrijk. Ik vind het dus ook van belang dat we daarnaar blijven kijken en dat we de vereisten die we daaraan stellen, of het nou gaat over die biorichtlijn of andere dingen, juist willen inzetten. Juist daar waar de impact van bijvoorbeeld langdurige onbeschikbaarheid heel groot kan zijn, is het wat mij betreft goed om na te denken over extra eisen en extra toezicht. Ik ben daarnaar onderzoek aan het doen, dat ik graag in juni met uw Kamer wil delen.
Dan de vragen van mevrouw Dekker-Abdulaziz over een speciale vorm van encryptie. Encryptie gaat over de dienstverlening ...

De **voorzitter**:
Sorry, ik ga u onderbreken, want de heer Rahimi heeft een vraag.

De heer **Rahimi** (VVD):
Ik hoorde dat we in juni informatie krijgen. Ik heb expres niet zo veel vragen gesteld over data en verouderde data, omdat daar op 11 mei een debat over komt.

De **voorzitter**:
Nee, dit ging over de veiligheid.

De heer **Rahimi** (VVD):
O, sorry. Oké.

Staatssecretaris **Van Huffelen**:
Dit ging over veiligheid en processen. Ik heb daarbij aangegeven: ook al definiëren we iets niet als een heel hoog risico of zit het niet in de vitale sector, de impact van bijvoorbeeld langdurige onbeschikbaarheid zou wel degelijk heel groot kunnen zijn. Dat ben ik eens met mevrouw Leijten. Het is dus ook belangrijk om daar aanvullende afspraken over te maken. Daar wordt onderzoek naar gedaan. Ik hoop dat in juni met uw Kamer te kunnen delen.
Dan de vragen van mevrouw Dekker-Abdulaziz over encryptie. Ik vind het heel belangrijk dat we hier als overheid een duidelijk antwoord over geven. We zijn daarover aan het nadenken en we zijn er ook over in discussie wat we nou precies vinden van die specifieke vorm van encryptie en de vraag of je wel mag meelezen als iemand iets aan het

typen is. Het gaat namelijk niet zozeer om de encryptie die ontstaat wanneer je een bericht van A naar B stuurt, maar juist om de encryptie als je aan het typen bent. Dat vraagstuk is bij ons in onderzoek. Daar komen we dan ook graag bij u op terug. Een definitief antwoord daarop kan ik op dit moment nog niet geven.
Dan iets over cookies. Met u vind ik de manier waarop de cookiewetgeving in de praktijk uitwerkt heel ingewikkeld. Anderen gaven dat ook al aan. Het is niet alleen maar ingewikkeld; het is gewoon irritant. Wanneer je een website bezoekt en iets wil bestellen of regelen, dan komen die cookies voorbij. Het is vaak heel erg lastig of een stuk lastiger om nee te zeggen, omdat je dan heel veel vragen moet beantwoorden en dat steeds opnieuw moet doen als je zo'n website bekijkt. Er zijn ook websites die je, wanneer je «nee, nee, nee» zegt, vervolgens een tijdje in de wacht houden voordat je van de dienstverlening gebruik kan maken. Er is in Europa onderhandeld over een zogenaamde e-Privacyverordening, waarin verbetering werd beoogd op dit gebied. Die richtlijn ligt eigenlijk nog vast. Ik ben van mening dat dat niet goed is. Ik heb daarover gesproken met de Europese Commissie. Die is daar overigens zelf mee aan het werk, maar ik ben, samen met de Minister van Economische Zaken, ook aan het werk om te kijken of wij vooruitlopend op wat er nu in Europa wordt besproken een soort voorstel kunnen doen voor hoe we hier verder mee kunnen. Want nogmaals, de ergernis die velen van ons ondervinden – dat speelt ook in uw Kamer – rondom de huidige uitwerking van de cookiewetgeving moet wat mij betreft worden aangepakt. Dat wil ik niet doen door te zeggen dat cookies weg moeten en al onze gegevens vervolgens zomaar door iedereen kunnen worden gebruikt, doorverkocht enzovoort enzovoort, maar door ervoor te zorgen dat het veel makkelijker wordt om nee te zeggen, zonder dat dat iets afdoet aan de dienstverlening.
Mevrouw Dekker-Abdulaziz vroeg ook nog hoe we nou omgaan met het delen van informatie als veel Nederlanders ook gebruikmaken van Facebook om overheidsinformatie binnen te krijgen. Mensen gebruiken natuurlijk nooit één kanaal; heel vaak worden er veel meer kanalen gebruikt. We weten dus dat Facebook een kanaal is. Zoals ik al eerder in dit debat heb aangegeven, denk ik, is het ook helemaal niet mijn bedoeling dat we zomaar gaan stoppen met Facebook. Ik wil alleen dat Facebook, Meta, zich houdt aan de Nederlandse wetten en regels. Daarom zijn we ook met hen in gesprek. Maar ik denk dat het altijd belangrijk blijft dat wij als overheid nadenken over een strategie waarin we meerdere kanalen blijven gebruiken en we uiteindelijk alleen maar de keuze maken om een kanaal niet meer in te zetten wanneer we het niet voor elkaar krijgen dat zo'n kanaal, dat in dit geval door veel Nederlanders wordt gebruikt, zich niet houdt aan de regels. Onze eerste strategie en ons eerste oogmerk is vooral om ervoor te zorgen dat de kanalen die veel gebruikt worden en door mensen ook worden gezien als belangrijke kanalen, voldoen aan onze wetten en regels.
Dan ben ik volgens mij aan het einde gekomen van de beantwoording van de vragen.

De **voorzitter**:
Ja, dat denk ik ook. Dank voor de beantwoording. Ik ga de toezeggingen even oplezen, dus even opletten met z'n allen.
– In de tweede helft van dit jaar ontvangt de Kamer het beleid inzake digitale autonomie en infrastructuur dat we samen met EZK maken. «De tweede helft van dit jaar» is wel heel ruim gedefinieerd. Kan de Staatssecretaris daar iets over aangeven?

Staatssecretaris **Van Huffelen**:
De coördinatie van die strategie ligt bij de Minister van EZK. Ik kan daar dus niet iets meer over zeggen. Ik denk dat het niet langer nodig zal hebben dan het nodig heeft, maar ik kan het niet precies zeggen.

De **voorzitter**:
Goed. Als het maar niet 31 december is.

– In het tweede kwartaal wordt de Kamer geïnformeerd over projecten die gehonoreerd worden binnen het programma IPCEI door de Minister van EZK.
– De Staatssecretaris stuurt de volledige vertaling van het DPIA en HRIA binnen een aantal weken.
  We hebben op 19 april een procedurevergadering. Zou het lukken voor 19 april?

Staatssecretaris **Van Huffelen**:
Die vertaling moeten wij laten maken en die moet ook juridisch kloppen, dus ik doe het gewoon zo snel mogelijk.

De **voorzitter**:
Ik hoop dat het lukt. Laten we daarop hopen.

– De Staatssecretaris biedt aan om een technische briefing te organiseren. Dit komt aan de orde tijdens de volgende procedurevergadering, op 19 april.
– De Kamer wordt op de hoogte gehouden van onderzoek naar getroffenen bij de rijksoverheid van het datalek van vorige week.
  Ik heb hier niet staan wanneer.

Staatssecretaris **Van Huffelen**:
Er moet eerst nog wat uitzoekwerk worden gedaan. Ik kan dus niet helemaal zeggen wanneer dat is, maar het komt zodra dat er is.

De **voorzitter**:
Zodra dat er is. Oké.

– De Staatssecretaris stuurt een brief naar aanleiding van de vraag van de heer Slootweg over extra waarborgen in de aanbestedingsregels ten behoeve van mensen die de overheid informatie toevertrouwen.
  Ook hierbij weet ik niet wanneer.

Staatssecretaris **Van Huffelen**:
Ik zou zeggen: in de zomer of voor de zomer. We doen het zo snel mogelijk. We moeten er even goed naar kijken en er ook met de verschillende partijen over overleggen.

De **voorzitter**:
Check. Rond de zomer.

– De Staatssecretaris stuurt een voorstel naar de Kamer ten behoeve van onderzoek naar andere socialmediaplatforms, naar aanleiding van een vraag van mevrouw Van Weerdenburg en de heer Rahimi.
  Dat voorstel komt dan zo snel mogelijk, neem ik aan? Ook voor de zomer? Dan hoef ik het niet nog een keer te vragen.

Mevrouw **Van Weerdenburg** (PVV):
Excuus. Ik kreeg van de Staatssecretaris eigenlijk het idee dat dat op korte termijn kon. Als het «voor de zomer» komt, dan zijn we alweer maanden verder. We hebben het over een opzet, hè? Het hoeft geen brief van achttien kantjes te zijn.

De **voorzitter**:
Een opzet.

Staatssecretaris **Van Huffelen**:
Die komt voor de zomer, ja.

De **voorzitter**:

Hopelijk aan de korte kant voor de zomer dan, en niet in juli. Laten we dat hopen.
Tot slot.
– In juni ontvangt de Kamer onderzoek naar extra eisen en toezicht voor vitale functies, naar aanleiding van een vraag van mevrouw Leijten.

Dan zijn we aan het eind gekomen van deze commissievergadering. Dank aan de Staatssecretaris voor haar aanwezigheid en antwoorden. Dank aan de ambtenaren die het allemaal opgeschreven hebben, en ook aan de Kamerleden, de bode en de mensen die meekijken.

Sluiting 13.00 uur.