Tweede Kamer, Bescherming persoonsgegevens en grote datalekken

VERSLAG VAN EEN COMMISSIEDEBAT
Concept

De vaste commissie voor Digitale Zaken heeft op 25 juni 2026 overleg gevoerd met mevrouw Aerdts, staatssecretaris Digitale Economie en Soevereiniteit, mevrouw Van Bruggen, staatssecretaris van Justitie en Veiligheid, en de heer Van der Burg, staatssecretaris Koninkrijksrelaties en Slagvaardige Overheid, over:

- **de brief van de staatssecretaris Koninkrijksrelaties en Slagvaardige Overheid d.d. 27 februari 2026 inzake ontwikkelingen over kwetsbaarheid in Ivanti Endpoint Manager Mobile (EPMM) (26643, nr. 1492);**
- **de brief van de staatssecretaris van Justitie en Veiligheid d.d. 6 februari 2026 inzake incident bij de Autoriteit Persoonsgegevens en de Raad voor de rechtspraak (26643, nr. 1462);**
- **de brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties d.d. 19 december 2025 inzake kabinetsreactie op rapport "De prijs van gratis internet" van het Rathenau Instituut (26643, nr. 1452);**
- **de brief van de minister van Justitie en Veiligheid d.d. 2 september 2025 inzake WODC-onderzoek over gegevensbescherming openbare registers (32761, nr. 331);**
- **de brief van de staatssecretaris Rechtsbescherming d.d. 14 juli 2025 inzake reactie op evaluatie Autoriteit Persoonsgegevens (25268, nr. 242);**
- **de brief van de staatssecretaris Koninkrijksrelaties en Slagvaardige Overheid d.d. 16 juni 2026 inzake kabinetsreactie op het NOS Nieuws-bericht Persoonsgegevens van vrijwel alle inwoners Epe gestolen bij cyberaanval (32761, nr. 341).**

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

De voorzitter van de vaste commissie voor Digitale Zaken,
Dekker

De griffier van de vaste commissie voor Digitale Zaken,
Boeve

Voorzitter: Dekker
Griffier: Muller

Aanwezig zijn zes leden der Kamer, te weten: Van den Berg, El Boujdaini, Dekker, Kathmann, Verkuijlen en Zwinkels,

en mevrouw Aerdts, staatssecretaris Digitale Economie en Soevereiniteit, mevrouw Van Bruggen, staatssecretaris van Justitie en Veiligheid, en de heer Van der Burg, staatssecretaris Koninkrijksrelaties en Slagvaardige Overheid.

Aanvang 10.03 uur.

De **voorzitter**:
Een hele goede morgen. Ik open de vergadering van de vaste commissie voor Digitale Zaken. Vandaag spreken we over bescherming persoonsgegevens en grote datalekken. Van de zijde van het kabinet zijn aanwezig mevrouw Van Bruggen, de staatssecretaris van Justitie en Veiligheid, staatssecretaris Van der Burg, van Binnenlandse Zaken en Koninkrijksrelaties, en staatssecretaris Aerdts. Ik moet altijd nadenken over de officiële titel van deze staatssecretaris: die is Digitale Economie en Soevereiniteit. Helemaal goed. Hartelijk welkom. Aan de zijde van de Kamer hebben we de heer Van den Berg, de heer Verkuijlen, mevrouw El Boujdaini, mevrouw Zwinkels en mevrouw Kathmann. We hebben vandaag tot 14.00 uur. De spreektijd voor de Kamerleden is vijf minuten. Ik wilde om te beginnen vier interrupties toestaan. Laten we eens kijken hoe dat zich verder in de tijd gaat ontwikkelen. Ik geef graag het woord aan de heer Van den Berg van JA21 voor zijn bijdrage.

De heer **Van den Berg** (JA21):
Voorzitter, dank u wel. Privacybescherming is een kerntaak van de overheid. Burgers moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden behandeld, bij de overheid, bij telecombedrijven, in de zorg en op digitale platforms. Dat vertrouwen staat onder druk. De afgelopen jaren zagen we incidenten bij onder meer Odido, de gemeente Epe, Clinical Diagnostics en kwetsbaarheden die ook overheidsinstanties als de Autoriteit Persoonsgegevens en de rechtspraak raakten. Voor JA21 is de les helder: privacybescherming vraagt niet alleen om nieuwe regels, maar ook om duidelijke wetgeving, effectieve handhaving en robuuste cyberbeveiliging. Datalekken ontstaan niet omdat technologie Amerikaans of Europees is, maar omdat beveiliging en databeheer tekortschieten.

Ten eerste de AVG. JA21 erkent dat de AVG burgers belangrijke bescherming biedt, maar de wet laat op cruciale punten te veel ruimte voor interpretatie. Dat veroorzaakt rechtsonzekerheid voor burgers, bedrijven en overheden. Neem het begrip "niet langer bewaren dan noodzakelijk". Wat is "noodzakelijk"? Een jaar? Vijf jaar? Tien jaar? Bij Odido bleek dat klantgegevens soms tot wel zestien jaar worden bewaard. Dan rijst de vraag of de norm nog voldoende houvast biedt. Het probleem is breder dan bewaartermijnen, niet enkel bij overheden, maar ook bij bedrijven die worstelen met begrippen als "gerechtvaardigd belang". Toezichthouders en rechters komen niet altijd tot dezelfde uitleg. Daardoor wordt de AVG te vaak afhankelijk van uitleg achteraf. Mijn vragen aan de staatssecretaris zijn daarom de volgende. Erkent hij dat de kernbegrippen binnen de AVG te veel ruimte laten voor interpretatie? Deelt hij dat meer rechtszekerheid nodig is voor burgers, bedrijven en overheden?

De **voorzitter**:
Welke staatssecretaris bedoelt u precies?

De heer **Van den Berg** (JA21):
Even tussendoor: ik heb er inderdaad even mee zitten worstelen welke staatssecretaris ik moet aanspreken. Uiteindelijk heb ik het maar bij "hij" gelaten en laat ik het aan het kabinet. Maar dat was niet aan de staatssecretarissen persoonlijk. Mijn excuus!

Voorzitter. Mijn vraag is dus: deelt zíj dat meer rechtszekerheid nodig is voor burgers,

bedrijven en overheden? Is zij bereid zich in Europees verband in te zetten voor duidelijke begrippen en concrete handvatten binnen de AVG?

Dan ten tweede de Autoriteit Persoonsgegevens. De AP heeft een belangrijke taak, maar het takenpakket is fors gegroeid: AVG-toezicht, klachten, datalekken en nu ook voorbereiding op toezicht onder de AI-verordening. Tegelijkertijd worden de problemen alleen maar groter. Ondanks extra budget voldoet nog altijd een groot deel van de websites en apps niet aan de privacyregels. De kernvraag is echter niet wat de AP doet, maar of burgers daardoor beter worden beschermd, zeker in het AI-tijdperk. Ik kom op mijn vragen. Heeft de AP volgens de staatssecretaris voldoende capaciteit én technische expertise voor privacy- en AI-toezicht? Welke concrete verbeteringen voor burgers verwacht zij van de extra middelen voor de AP? Hoe wordt gemeten of het toezicht daadwerkelijk leidt tot betere bescherming van persoonsgegevens? Hoe voorkomen we dat de AP vooral reactief optreedt nadat gegevens al zijn gelekt?

Voorzitter. Dat brengt mij bij mijn derde punt: de cyberveiligheid. In discussies over privacy wordt vaak gesproken over digitale soevereiniteit en de afhankelijkheid van buitenlandse technologie. Dat is een belangrijk debat. Maar soms ontstaat daarbij de indruk dat privacyproblemen vanzelf verdwijnen wanneer we overstappen op Europese technologie. JA21 deelt die conclusie niet. Buiten het feit dat bijvoorbeeld de Amerikaanse autoriteiten niet zomaar onze gegevens kunnen inzien, blijft één punt overeind staan: de grootste privacy-incidenten van de afgelopen jaren zijn niet vaak veroorzaakt door buitenlandse overheden, maar door beveiligingsproblemen, kwetsbaarheden in systemen en onvoldoende databeheer. Zo werd de gemeente Epe getroffen door een ernstige hack, waarbij persoonsgegevens van vrijwel alle inwoners werden buitgemaakt. De Autoriteit Persoonsgegevens, de rechtspraak en de DJI werden geconfronteerd met de gevolgen van kwetsbaarheden in de Ivantisoftware. Deze incidenten laten zien dat beveiligingsproblemen zich niet beperken tot één leverancier, één land of één continent. Uiteindelijk wordt een organisatie niet gehackt omdat software Amerikaans, Nederlands of Europees is. Organisaties worden gehackt omdat kwetsbaarheden niet tijdig worden ontdekt, omdat systemen onvoldoende worden gemonitord, omdat gegevens te lang worden bewaard of omdat de basisbeveiliging tekortschiet.

Voorzitter. De kwaliteit van beveiliging is belangrijker dan de nationaliteit van technologie. Dit betekent ook dat we kritisch moeten kijken naar onze eigen organisaties. De voorbeelden van de afgelopen jaren laten ook zien dat Nederlandse overheden, gemeenten en toezichthouders kwetsbaar zijn. Wie privacy serieus neemt, moet daarom niet alleen kijken naar de herkomst van technologie, maar vooral investeren in cyberweerbaarheid. Dat begint bij goed databeheer, het beperken van gegevensopslag, tijdige beveiligingsupdates, onafhankelijke audits en voldoende technische expertise binnen die organisaties. Daarnaast rijst de vraag waarom sommige sectoren veel strengere eisen kennen dan andere. In de financiële sector gelden uitgebreide eisen op het gebied van risicobeheer, auditing en gegevensbewaring, terwijl veel persoonsgegevens worden verwerkt. Ik ben de tijd even kwijt door de onderbreking van net, maar ik ga gewoon rustig door. Erkent de staatssecretaris dat Europese technologie op zichzelf geen garantie biedt tegen datalekken of cyberaanvallen en dat de kwaliteit van de beveiliging uiteindelijk belangrijker is dan de herkomst van de technologie? Welke investeringen zijn volgens de staatssecretaris nodig om de cyberweerbaarheid van vitale aanbieders te vergroten? Kan de staatssecretaris

toelichten waarom voor telecombedrijven niet dezelfde strenge beveiligings- en vernietigingsplichten gelden als voor de financiële sector? Is de staatssecretaris bereid om te onderzoeken of periodieke, onafhankelijke IT-audits voor vitale aanbieders kunnen bijdragen aan een betere bescherming van persoonsgegevens? En deelt zij de opvatting dat investeringen in cyberweerbaarheid en informatiebeveiliging uiteindelijk meer bijdragen aan de bescherming van persoonsgegevens dan uitsluitend het vervangen van buitenlandse technologie door Europese alternatieven?

Voorzitter, nog een half blaadje. Ten vierde AI. AI biedt kansen voor overheid, economie en dienstverlening, maar AI brengt ook risico's met zich mee voor transparantie, controle en persoonsgegevens. We zien dat AI-functionaliteiten steeds vaker standaard worden ingeschakeld door grote technologiebedrijven. Gebruikers worden daar niet altijd over geïnformeerd en hebben niet altijd een reële keuze. JA21 wil die innovatie niet afremmen, maar wel duidelijke spelregels. Burgers moeten weten welke gegevens worden verwerkt, met welk doel en hoe ze daar invloed op hebben. AI-functies die persoonsgegevens verwerken, horen niet standaard aan te staan. Dat moeten opt-ins zijn en niet opt-outs. Ook het trainen van AI-modellen met persoonsgegevens vraagt duidelijke, handhaafbare regels. Niet achteraf bijsturen als data al is verwerkt, maar vooraf controle en toestemming regelen. Ik heb alleen nog een vraag en dan rond ik af. Vindt de staatssecretaris dat AI-functionaliteiten die persoonsgegevens verwerken standaard opt-in moeten zijn? Hoe voorkomt de staatssecretaris dat burgers ongemerkt persoonsgegevens afstaan voor training van AI-systemen? Welke concrete eisen stellen zij aan de transparantie over datagebruik in AI-toepassingen? Heeft de AP voldoende capaciteit om effectief toezicht te houden op zulke complexe AI-systemen?

Ik rond af, voorzitter. Privacy vraagt om duidelijke keuzes, minder vaagheid in de wet, scherper toezicht, betere uitvoering en meer cyberweerbaarheid. Als we dat niet regelen, blijft de bescherming van persoonsgegevens achter bij de digitale werkelijkheid.

Dank u wel.

De **voorzitter**:
Dank u wel. U heeft een interruptie van mevrouw Zwinkels van het CDA.

Mevrouw **Zwinkels** (CDA):
Ik heb met interesse geluisterd naar het pleidooi van JA21. Ik heb een vraag aan de heer Van den Berg. Die opt-in spreekt mij ook wel aan, maar welke regels zijn wat de heer Van den Berg betreft nodig om dat ook goed te regelen? Of vindt hij dat de huidige regels daarvoor al toereikend zijn?

De heer **Van den Berg** (JA21):
Ik denk dat er op dit moment nog onvoldoende regels voor zijn. ChatGPT is hier een goed voorbeeld van. Ook al heb je een betaalde account, dan staat in principe de informatie beschikbaar voor het trainen van het model. Dat kan je zelf uitschakelen. Ik denk dat we het in ieder geval nationaal dan wel Europees moeten regelen dat we gewoon zeggen: het is op zich niet erg dat je daaraan kan meedoen, maar in beginsel staat het uit; als de burger beslist dat hij daar wel aan wil bijdragen uit mooie overtuigingen, dan kan dat.

De **voorzitter**:

Nog een vervolgvraag, mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Nee, een korte reflectie. Ik ben blij om dat antwoord te horen. Zo staan wij daar ook in. Ik ben benieuwd of we daarin samen kunnen optrekken.

De **voorzitter**:
Heel goed. Dan gaan we nu luisteren naar de heer Verkuijlen van de VVD.

De heer **Verkuijlen** (VVD):
Dank u, voorzitter. Een hack bij Odido, een hack bij Bevolkingsonderzoek Nederland en een hack bij het Openbaar Ministerie: het zijn slechts enkele voorbeelden van het afgelopen jaar waarbij persoonsgegevens zijn buitgemaakt. Persoonsgegevens worden steeds vaker digitaal verwerkt en opgeslagen door overheden, bedrijven en maatschappelijke organisaties. Dat biedt kansen voor betere en efficiëntere dienstverlening, maar brengt ook risico's met zich mee. Wanneer persoonsgegevens onvoldoende worden beschermd of in verkeerde handen terechtkomen, kan dit leiden tot financiële schade, identiteitsfraude, privacyschendingen en een afname van het vertrouwen in digitale dienstverlening. Mijn fractiegenote Queeny Rajkowski diende eerder een motie in waarin het kabinet werd gevraagd een handelingskader voor slachtoffers van grote datalekken op te stellen. Ik dank het kabinet voor de brief hierover.

Een organisatie die slachtoffer wordt van een datalek, moet betrokkenen direct informeren en een duidelijk handelingsperspectief bieden, zo valt te lezen. Ook de financiële gevolgen, wanneer risico's niet tijdig worden beperkt, komen daarbij aan bod. Ik heb hierover nog enkele vragen. Hoe worden slachtoffers actief gewezen op hun rechten en mogelijkheden? Hoe wordt de naleving van deze verplichtingen gecontroleerd en gehandhaafd? Wie ondersteunt getroffen overheidsorganisaties? We hebben een mooie brief gehad van de staatssecretaris over Epe, maar gemeenten geven aan dat zij die ondersteuning soms missen. Herkent het kabinet dat beeld? Daarnaast hoor ik graag of het kabinet inzicht heeft in de kwaliteit van de communicatie richting slachtoffers. Wordt geëvalueerd of mensen de verstrekte informatie daadwerkelijk begrijpen en ook kunnen gebruiken?

Voorzitter. Gestolen persoonsgegevens vertegenwoordigen in het criminele circuit een aanzienlijke waarde. De opsporing van daders blijft echter lastig. Wat kan het kabinet zeggen over de effectiviteit van de opsporing van cybercriminelen die verantwoordelijk zijn voor grootschalige datadiefstal? Berichtgeving over succesvolle datalekken hebben we veel, maar succesvolle vervolging blijft relatief schaars. Getroffen organisaties gaan bovendien niet zelden over tot het betalen van geldbedragen om gegevens terug te krijgen of publicatie te voorkomen. Hoe kijkt de staatssecretaris van JenV hiertegen aan? Heeft het kabinet zicht op de omvang van deze betalingen en ziet het kabinet mogelijkheden om organisaties beter te ondersteunen, zodat zij minder afhankelijk worden van dergelijke keuzes?

Voorzitter. In het handelingskader wordt tweefactorauthenticatie genoemd als belangrijke preventieve maatregel. Tegelijkertijd worden nieuwe technologieën ontwikkeld, zoals zero-knowledgetechnologieën. Daarmee kunnen eigenschappen of verificaties worden aangetoond zonder dat de onderliggende persoonsgegevens worden

prijsgegeven. Je spreidt als het ware de gegevens in meerdere databases. Dat kan bijdragen aan betere bescherming van persoonsgegevens en dataminimalisatie en daarmee de impact van datalekken beperken. Ziet de staatssecretaris mogelijkheden om dergelijke technieken binnen de overheid breder toe te passen? Worden er al pilots mee uitgevoerd? Welke belemmeringen staan een bredere invoering in de weg?

Voorzitter. De VVD heeft eerder schriftelijke vragen gesteld over de menstruatiecyclus- en zwangerschapsapps. Gebruikers delen daarin zeer gevoelige persoonsgegevens. Zijn gebruikers zich voldoende bewust van welke gegevens worden verzameld, hoe deze worden verwerkt en met wie deze worden gedeeld? Hoe beoordeelt de staatssecretaris van JenV de begrijpelijkheid van privacyverklaringen van dergelijke apps? Ziet zij mogelijkheden om de informatievoorziening te verbeteren, zodat gebruikers daadwerkelijk geïnformeerd keuzes kunnen maken? Welke verantwoordelijkheid kunnen aanbieders hierin nemen? Kan bovendien worden onderzocht of apps verplicht kunnen worden om op een eenvoudige en gestandaardiseerde manier inzichtelijk te maken wat er met die persoonsgegevens gebeurt? Hoe wordt toegezien op doorgifte van deze gevoelige gegevens naar partijen buiten Europa?

Voorzitter. De zorg is een bijzonder kwetsbare sector. Het beheer van persoons- en medische gegevens vereist maximale bescherming. Wanneer deze gegevens door een cyberaanval op straat komen te liggen of toegankelijk worden, kan dat grote gevolgen hebben voor zowel de privacy als de gezondheid van patiënten. Daarom vraag ik naar de uitvoering van de motie-Tielen/Bushoff, die verzoekt om lessen uit de financiële sector toe te passen en gesimuleerde cyberaanvallen in de zorg op te nemen in een ministeriële regeling. Wat is de huidige stand van zaken? Wanneer wordt de Kamer hierover geïnformeerd? Zijn zorginstellingen voldoende voorbereid op grootschalige cyberincidenten?

Voorzitter. Tot slot vraag ik naar de stand van zaken van de gesprekken die staatssecretaris Aerdts heeft gevoerd met de Amerikaanse ambassadeur over Meta en Microsoft. Hoe staat het daarnaast met Europese en Nederlandse alternatieven, zodat we minder afhankelijk worden van grote buitenlandse technologiebedrijven? In lijn met wat de heer Van den Berg zei: ook voor de VVD is die trans-Atlantische relatie belangrijk en kunnen we voorlopig nog niet zonder dat soort bedrijven. Welke concrete stappen zet het kabinet om de digitale autonomie te versterken?

Tot zover mijn bijdrage in eerste termijn, voorzitter. Ik dank u wel.

De **voorzitter**:
Dank u wel. Ik zie geen interrupties. Dan is het woord nu aan mevrouw El Boujdaini van D66.

Mevrouw **El Boujdaini** (D66):
Dank u wel, voorzitter. Vanaf dag één dat ik Kamerlid ben, houd ik mij bezig met de bescherming van persoonsgegevens en met grote datalekken. Dat is geen toeval, want als sociaalliberaal geloof ik in de vrijheid voor mensen om hun eigen leven vorm te geven. In een digitale samenleving betekent dat ook baas zijn over je eigen gegevens. Toch gaat het te vaak mis: Basic-Fit, Booking.com, Canvas, Odido, het bevolkingsonderzoek baarmoederhalskanker en het datalek in Epe. Dit zijn slechts

enkele voorbeelden uit een steeds langere lijst. Ik heb daar veel Kamervragen over gesteld, want we mogen niet wennen aan het feit dat er bijna wekelijks een grootschalig datalek in het nieuws verschijnt. Dat kan anders.

Voorzitter. Na ieder nieuw datalek voeren we steeds hetzelfde gesprek: hoe heeft dit kunnen gebeuren, welke gegevens zijn gelekt en hoe voorkomen we dat dit opnieuw gebeurt? Het zijn belangrijke vragen, maar ze komen pas nadat de schade al is aangericht. Als we echt vooruit willen, vraagt dat om meer dan het voorkomen van het volgende datalek. Het vraagt om een ander systeem, een steviger slot op persoonsgegevens waarvan iedereen de sleutel zelf in handen heeft. Vandaag de dag laten we onze gegevens immers nog overal achter, bijvoorbeeld voor een sportabonnement of bij de telecomprovider. Hiermee geven we die sleutel nog te vaak uit handen aan organisaties die grote hoeveelheden persoonsgegevens opslaan. De vraag is daarom hoe we ervoor zorgen dat mensen in het digitale tijdperk baas blijven over hun eigen gegevens. Vanuit die overtuiging heb ik de afgelopen tijd gewerkt aan een initiatiefnota, die ik later nog officieel zal indienen.

Voorzitter. Als we mensen meer regie willen geven over hun eigen gegevens, zijn digital wallets, ook wel digitale portemonnees genoemd, volgens mijn fractie veelbelovend. De veiligste persoonsgegevens zijn namelijk gegevens die niet onnodig worden gedeeld en opgeslagen. Met een digital wallet kan je bijvoorbeeld aantonen dat je meerderjarig bent, zonder direct je geboortedatum of identiteitsgegevens af te geven. Dat is precies de omslag die we nodig hebben: minder gegevens delen, meer dataminimalisatie en dus minder gegevens die opgeslagen worden. Vindt er toch een datalek plaats, dan is de schade beperkt omdat er minder gegevens te verliezen zijn. Kan de staatssecretaris daarom schetsen wat de actuele stand van zaken is rondom de ID-wallets en welke tijdlijn zij voor zich ziet voor de verdere invoering van de eIDAS-verordening?

Voorzitter. Rotterdam loopt voorop. Met de ID010-wallet krijgen Rotterdammers inzicht in welke gegevens ze delen, met wie en waarom; echte regie over hun digitale identiteit. De eerste toepassing die zij willen testen is een eerlijker inschrijfproces voor huurwoningen, waarbij op dit moment discriminatie nog altijd te vaak voorkomt. Technologie wordt hierbij ingezet voor gelijkwaardigheid. Hoe kijkt de staatssecretaris naar dit initiatief en ziet zij mogelijkheden om dit soort initiatieven ook landelijk verder uit te bouwen?

Voorzitter. Regels zijn uiteindelijk zo sterk als het toezicht daarop. De Autoriteit Persoonsgegevens ontving vorig jaar meer dan 44.000 meldingen van datalekken. Dat is in een jaar tijd meer dan verdubbeld. De AP geeft zelf aan meer te willen doen aan proactief toezicht, juist om grootschalige incidenten te kunnen voorkomen en omdat zij aan de lat staan voor toezicht en handhaving op de AI-verordening. Kan de staatssecretaris verkennen wat nodig is om de AP in staat te stellen het gewenste proactieve toezicht te kunnen gaan doen? In de reactie van de staatssecretaris op de evaluatie inzake de AP wordt aangegeven dat de AP in samenspraak met JenV een meetinstrument en indicatoren ontwikkelt om inzicht te krijgen of de middelen doelmatig en doeltreffend worden besteed. Hoe staat het daarmee?

Voorzitter. Verder kent de AVG geen uiterlijke verwijdertermijnen voor bijvoorbeeld persoonsgegevens. Organisaties mogen die zelf bepalen, wat voor veel onduidelijkheid en verwarring zorgt. Hoe ziet de staatssecretaris dit? Zouden we dit soort termijnen wel

moeten vaststellen?

Voorzitter. Persoonsgegevens worden niet alleen gelekt en gestolen, ze worden vervolgens verhandeld en misbruikt voor identiteitsfraude, phishing en oplichting. Achter die praktijken zitten mensen die hier geld mee verdienen. Ik noem ze datadieven. Zij stelen niet alleen persoonsgegevens, maar tasten ook het vertrouwen online en het veiligheidsgevoel van mensen aan. Daarom ben ik benieuwd hoe de staatssecretaris kijkt naar de opsporingskant van dit vraagstuk. Is de staatssecretaris bereid in kaart te brengen hoe de samenwerking tussen de politie en de AP momenteel is ingericht, waar knelpunten liggen en welke mogelijkheden er zijn om deze samenwerking verder te versterken?

Voorzitter, ik sluit af. Net zoals we regie willen over onze eigen pasjes in de portemonnee en die niet zomaar afgeven, geldt dit ook voor onze persoonsgegevens. In een digitale samenleving horen mensen de sleutel tot hun data in eigen handen te hebben. Mijn fractie gelooft dat we dat samen voor ze kunnen regelen.

Dank u wel.

De **voorzitter**:
Dank u wel. U heeft een interruptie van de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):
Ik heb wel een vraag bij het betoog van mevrouw El Boujdaini. Ik hoorde de zorgen over de AVG en, vooral in andere debatten, over soevereiniteit. Maar wat heeft D66 in de afgelopen jaren gedaan om deze problemen, die nu spelen, met al die datalekken van tevoren beet te pakken?

Mevrouw **El Boujdaini** (D66):
Ik denk dat we in de Kamer dat met z'n allen willen oplossen. Daar hebben we ons de afgelopen jaren ook voor ingezet. Dat hebben we onder andere gedaan door de debatten te voeren in de Kamer, maar ook juist door te kijken hoe we de AP kunnen inrichten en hoe we dat zo goed mogelijk kunnen doen. Voor mijn fractie en partij is privacy in ieder geval altijd een heel groot goed geweest, omdat we het gewoon belangrijk vinden dat de privacy van mensen gewaarborgd blijft, juist omdat er zo'n grote datahonger is gekomen vanuit organisaties. Daarnaast is privacy gewoon een grondrecht in Europa. Daar staan wij volledig voor.

De heer **Van den Berg** (JA21):
Het is natuurlijk mooi dat er debatten worden gevoerd hier in de Kamer, maar dat is volgens mij ook juist de kern van dit probleem. We rennen als Kamer van brandje naar brandje, maar de onderliggende problemen worden niet beetgepakt. Het volgende verbaast mij dan toch. Natuurlijk begrijp ik wat mevrouw El Boujdaini hier zegt, maar je kan toch op z'n minst stellen dat de inzet van in ieder geval D66 in de afgelopen jaren toch onvoldoende is geweest. Er wordt aan de staatssecretaris gevraagd: wat kunt u doen om dit op te lossen? Oké. Misschien biedt uw initiatiefnota nog kansen, maar ik zou toch wel echt meer een rol zien voor de Kamer om dit gewoon zelf beet te pakken, want dat is volgens mij de afgelopen jaren niet gebeurd. Ik ben benieuwd naar de mening van mevrouw El Boujdaini daarover.

Mevrouw **El Boujdaini** (D66):
Als we kijken naar wat er de afgelopen jaren is gebeurd, zien we dat het digitale leven veel groter is geworden. Met de komst van AI zijn we veel meer risico gaan lopen om gehackt te worden. Bedrijven en mensen zijn daar slachtoffer van. Dat probleem is dus alleen maar groter geworden. Ik denk daarom ook dat we juist nu in de Kamer hier zo veel aandacht voor hebben. Ik denk dat het juist een hele positieve ontwikkeling is dat dit nu zo hoog op de politieke agenda staat. Ik denk dat het nu ook aan ons is om hier, samen met dit kabinet, ook echt werk van te maken, om juist dit soort incidenten te kunnen voorkomen. Je ziet dat we het op deze manier willen voorkomen, maar ik denk ook dat we hele grote stappen kunnen maken met elkaar wanneer we kijken naar wat we niet meer willen. Daarom vind ik het ook zo belangrijk om te kijken naar de preventieve kant ervan. We hebben het steeds over incidenten. Ik denk dat we juist veel meer kunnen inzetten op wat we anders willen doen. Naar mijn mening en die van mijn fractie is dat om het systeem te veranderen door te werken aan dataminimalisatie: gegevens meer bij personen houden en die niet overal verspreiden.

De heer **Verkuijlen** (VVD):
Helder. Ik kan me goed vinden in het betoog van mevrouw El Boujdaini, maar ik zit even met het volgende. We hebben gisteren een debat gehad over digitale inclusie. Ik hoor u het hebben over het in eigen hand houden van je data, maar dan denk ik bij mijzelf, maar misschien heeft u dat ook: hoe zit dat dan met die club waar we het gister over hadden, van bijna 4 miljoen mensen? Hoe kunnen we dat nou op een goede manier doen? "In eigen hand" vraagt nogal het een en ander. Ik ben benieuwd hoe mevrouw El Boujdaini daarnaar kijkt.

Mevrouw **El Boujdaini** (D66):
Ik vind dat een heel terecht punt van de heer Verkuijlen. Ik heb hier de afgelopen tijd, en vooral ook na het debat van gisteren, over na zitten denken. Ik denk dat het daar ook heel erg gepaard gaat met juist bijvoorbeeld de IDO-punten, die mensen nu ook al helpen om een DigiD aan te vragen of DigiD op de telefoon te installeren. Bij het invoeren van zo'n nieuw systeem moeten we ook zeker die kant meenemen als het gaat om hoe we mensen hierin gaan helpen. Het is niet de bedoeling dat mensen het moeilijker gaan krijgen in de digitale samenleving, het is juist wel echt met het idee dat het makkelijker wordt, omdat je, als het goed is, ook overal minder wachtwoorden hebt. Daar is zo'n digital wallet immers ook voor bedoeld. Op die manier kunnen we samen het systeem aanpassen, zodat ook die 4 miljoen mensen uiteindelijk meekunnen. Maar ik kijk heel graag verder, ook met de heer Verkuijlen, naar hoe we dat zouden kunnen aanpakken.

De **voorzitter**:
Dank u wel. Dan gaan we nu luisteren naar mevrouw Zwinkels van het CDA.

Mevrouw **Zwinkels** (CDA):
Dank u wel, voorzitter. Stel je voor: iemand zoekt online naar informatie over schulden, bezoekt een gezondheidswebsite, klikt op een advertentie voor kinderopvang, logt in bij de gemeente, sluit een telefoonabonnement af en gebruikt een gratis app. Op zich lijken dat losse, normale handelingen. Maar digitaal laten mensen vooral overal kruimels achter. Die kruimels worden verzameld door websites, apps, advertentienetwerken, databedrijven, platforms en ook soms door organisaties die helemaal niet scherp genoeg nadenken over wat ze bewaren. Uit die losse gegevens ontstaat dan een profiel:

waar woont iemand, wat verdient iemand, waar is iemand bang voor, heeft iemand kinderen, is iemand ziek, heeft iemand schulden, is iemand beïnvloedbaar of zit iemand net in een kwetsbare periode? Als zulke gegevens uitlekken, blijven ze niet netjes in één mapje liggen. Nee, ze kunnen worden gecombineerd met andere lekken. En dan wordt een phishingbericht opeens heel erg persoonlijk, met de juiste naam, provider, woonplaats of zelfs een verwijzing naar een overheidsdienst. Met een kopie van een identiteitsbewijs kunnen criminelen proberen om een rekening te openen, een lening aan te vragen of een telefoonabonnement af te sluiten. Met gedragsgegevens kunnen bedrijven mensen volgen, sturen en soms manipuleren, zonder dat mensen echt weten wat er gebeurt.

Voorzitter. Dat is de kern van dit debat: persoonsgegevens zijn niet zomaar data; ze zijn de toegangspoort tot iemands leven. Te vaak zijn ze ook handelswaar geworden. We zijn ons als samenleving nog onvoldoende bewust daarvan. Dat komt ook tot uitdrukking in de cultuur van bedrijven en andere organisaties en in de beperkte naleving van regels in de praktijk, zowel in de directie als op de werkvloer. Wij maken ons zorgen en willen ingrijpen. Daarom heb ik vier punten.

Eén. Pak de datahonger aan, en ook het verdienmodel erachter. Het Rathenau Instituut laat zien dat gratis internet vaak helemaal niet gratis is. Mensen betalen met hun gedrag, aandacht en persoonsgegevens. Dat geldt voor volwassenen, maar zeker ook voor kinderen en jongeren, die vaak nauwelijks begrijpen hoever die tracking gaat. Is de staatssecretaris het met het CDA eens dat het huidige systeem van onlinetracking te veel uitgaat van doorklikken en toestemming en te weinig van echte bescherming? Gaat het kabinet in Europa actief pleiten voor privacyvriendelijke alternatieven, zoals contextueel adverteren, waarbij advertenties worden gebaseerd op de inhoud van een pagina in plaats van op het profiel van een persoon? Wil de staatssecretaris specifiek voor minderjarigen onderzoeken hoe onlinetracking verder kan worden teruggedrongen, juist omdat kinderen geen verdienmodel mogen zijn?

Twee. Verzamel minder, bewaar korter en geef niet iedereen toegang. Bij datalekken kijken we vaak naar de hacker van buitenaf, maar de kwetsbaarheid zit ook vaak binnen organisaties zelf. Te veel gegevens worden te lang bewaard en te veel mensen kunnen erbij. In veel organisaties kan een medewerker die voor zijn werk maar een klein deel van het dossier nodig heeft, toch bij grote hoeveelheden gevoelige informatie, niet uit kwade wil, maar omdat systemen zo zijn ingericht, omdat rechten ooit ruim zijn toegekend en daarna nooit meer zijn opgeschoond, omdat gemak het wint van veiligheid. Bij de Odidohack onderzoeken toezichthouders ook of gegevens niet te lang zijn bewaard. Dat is belangrijk, want wat je niet bewaart, kan ook niet gehackt worden. Is de staatssecretaris bereid om bewaartermijnen veel harder te laten handhaven, zeker bij organisaties die gegevens van miljoenen mensen beheren?

Drie. Zoek de samenwerking bij het adequaat reageren op datalekken. Gelet op de toename van AI-gedreven cyberaanvallen voorzien wij dat de uitdaging in de toekomst groter en groter wordt. Na een datalek krijgen burgers vaak tips: let op phishing, klik niet zomaar op links, wees alert. Dat is nuttig, maar ook wrang, want de burger heeft het lek niet veroorzaakt. De hacker is de boosdoener en bedrijven en organisaties dienen hun kwetsbaarheden goed in beeld te hebben en continu kennis op te doen, ook door hun ervaringen met datalekken beter uit te wisselen, zodat we het taboe eraf halen en de verbeteringen in de praktijk volgen. Komt er dan ook een landelijke standaard voor hulp

aan slachtoffers van grote datalekken, zodat mensen niet verdwalen tussen gemeente, bedrijf, politie, bank en toezichthouder? Ook hier kan vast worden voortgebouwd op de opgedane kennis.

Vier. De overheid moet zelf de hoogste norm hanteren en het toezicht moet kunnen leveren. De overheid vraagt van burgers om hun meest gevoelige gegevens, bijvoorbeeld over schulden, gezin, zorg, veiligheid en rechtspraak. Burgers moeten erop kunnen vertrouwen dat de overheid daar zuiniger en zorgvuldiger mee omgaat dan wie dan ook. Daarom is het extra pijnlijk als juist bij overheidsorganisaties datalekken ontstaan of kwetsbaarheden worden misbruikt. Mijn vraag aan de staatssecretaris is: welke concrete norm stelt zij aan overheidsorganisaties voor toegang tot persoonsgegevens? Mag een medewerker alleen zien wat nodig is voor zijn of haar werk of accepteren we nog steeds de systemen waarin veel te veel mensen bij veel te veel gegevens kunnen? Hoe gaat de staatssecretaris ervoor zorgen dat ministeries en uitvoeringsorganisaties hun toegangsrechten periodiek opschonen, zodat oude rechten en oude bestanden niet jarenlang blijven rondzwerven?

Voorzitter. Dan de Autoriteit Persoonsgegevens. De AP moet onafhankelijk haar werk kunnen doen; daar moeten we niet doorheen gaan lopen. Het kabinet is echter wel verantwoordelijk voor de randvoorwaarden: middelen, evaluatie, opdrachtgeverschap en het bredere stelsel. De Autoriteit Persoonsgegevens krijgt ook steeds meer op haar bord. Kan de staatssecretaris eerlijk aangeven of de AP voldoende capaciteit heeft om haar taken goed te kunnen uitvoeren? Als die capaciteit niet voldoende is, welke keuzes worden dan gemaakt? Welke risico's krijgen prioriteit en welke blijven daardoor liggen?

Dank u wel.

De **voorzitter**:
Dank u wel. U heeft een interruptie van de heer Verkuijlen van de VVD.

De heer **Verkuijlen** (VVD):
Helder betoog. Zo ken ik mevrouw Zwinkels ook. Het lijkt bijna een initiatiefnota als u die punten zo afloopt. U noemt daarbij echter ook aandacht voor de slachtoffers en de organisaties. Nou hebben we net een brief gekregen over een handelingskader voor de slachtoffers. Ik ben wel even benieuwd of u dat vindt aansluiten op waar u om vraagt in uw betoog.

Mevrouw **Zwinkels** (CDA):
Dank voor de vraag. Ik denk dat het heel erg belangrijk is dat we voor slachtoffers echt gaan doen wat nodig is: dat we ervoor gaan zorgen dat de communicatie eerlijk plaatsvindt, dat we goede ervaringen met hoe bedrijven dat hebben gedaan en hoe de overheid dat heeft gedaan, ook uitwisselen, en dat de overheid ook bijspringt als het bijvoorbeeld een lek betreft van miljoenen mensen. Ik zie dat het kabinet er terughoudend in is om zo'n verantwoordelijkheid op zich te nemen of om op die manier daarin gezamenlijk op te trekken. Dat zou ik dus graag meer willen zien. Volgens mij zijn we het met elkaar eens over het opsporen van die hackers en het aanpakken van de kwetsbaarheden van alle verschillende organisaties die het betreft. Daar wil ik nogmaals bij benadrukken dat het ook belangrijk is dat we het taboe eraf halen, want het mag niet zo zijn dat we daardoor juist minder delen. Daar hebben we ook in het rondetafelgesprek diverse suggesties voor gehoord.

De heer **Verkuijlen** (VVD):
De brief over een opvangkader voor slachtoffers, dus een handelingskader voor slachtoffers, grijpt ook heel erg terug op de AVG. Een aantal dingen zijn al gerealiseerd in de AVG. Ik heb alleen het idee, als ik de brief zo lees, dat dat nog vrij onbekend is. Ik ben even benieuwd hoe mevrouw Zwinkels daarnaar kijkt.

Mevrouw **Zwinkels** (CDA):
Ik weet niet helemaal of ik het antwoord ga geven waar de heer Verkuijlen naar op zoek is, maar ik denk dat er inderdaad nog best wel veel onbekend is. We hebben juist de afgelopen tijd een aantal heel grote datalekken gezien, waarmee ervaring is opgedaan en waarbij organisaties vooral hebben geprobeerd om snel te detecteren wat er aan de hand is, vervolgens ook snel te compartimenteren, te isoleren, om ervoor te zorgen dat het lek niet groter wordt of nog meer mensen gaat betreffen, om vervolgens te communiceren. In die communicatie proberen organisaties de informatie die ze hebben, snel te communiceren. De spanning zit volgens mij bij de snelheid en bij een volledige communicatie, en ik wil graag dat we meer informatie gaan uitwisselen over hoe je dat op een goede manier doet. Ik hoop dat de heer Verkuijlen dat met mij eens is en ik ben benieuwd welke blinde vlekken hij nog meer voor zich ziet, zodat we er met elkaar de schouders onder kunnen zetten om die te verhelpen. Uiteindelijk denk ik namelijk dat het goed is om er niet alleen vanuit een individualistisch perspectief naar te kijken, maar om ook juist om mensen heen te gaan staan zodat we het systeem ook echt anders inrichten. Dat hoorde ik mevrouw El Boujdaini net ook zeggen.

De **voorzitter**:
Dank u wel. Dan gaan we nu luisteren naar mevrouw Kathmann van PRO.

Mevrouw **Kathmann** (PRO):
Dank, voorzitter. Elke organisatie die een digitale kwetsbaarheid meldt, erkent en deelt, verdient echt een supergroot compliment, want we leren er allemaal van en we worden er ook allemaal veiliger van. Het is in dit tijdperk van digitale aanvallen namelijk niet de vraag óf, maar helaas wanneer je getroffen wordt. Hoe groter je bedrijf, hoe meer data je bijhoudt, hoe aantrekkelijker je bent als doelwit. Daarom moeten we iets doen aan de gestoorde datahonger in onze samenleving. Voor elk dingetje moet je nu een account aanmaken met adresgegevens, telefoonnummer, bankrekeningnummer en je naam en toenaam. Elk callcenter houdt notities bij van je persoonlijke situatie. Het is eigenlijk best bizar hoe diep dat gaat en hoe compleet onnodig het vaak is. We moeten ten strijde trekken tegen die datahonger. Daarover heb ik een aantal vragen. Hoe gaan we het principe van dataminimalisatie, wat eigenlijk al gewoon een basisprincipe is in wetgeving, versterken? Dat is namelijk nodig, want op een of andere manier staat het in de wet, maar doen we er niet aan. Wat gaat het kabinet doen om bedrijven te dwingen echt zo min mogelijk informatie op te slaan van klanten? Wat zijn bewaartermijnen waard als niemand ze eigenlijk naleeft? Hoe gaan we daar veel steviger op toezien?

Sinds de commercialisering van het internet worden we allemaal massaal bespied. Rathenau heeft op verzoek van de hele Tweede Kamer een goed onderzoek gedaan naar de gevolgen van trackingcookies, de reinste vorm van surveillancekapitalisme. Laat ik helder zijn: Progressief Nederland pleit voor een verbod op trackingcookies. Ze dienen het belang van het grootkapitaal ten koste van de privacy en keuzevrijheid van ons als digitale burgers. Het systeem is kapot. Een fundamentele wijziging is nodig. Ik vraag van

dit kabinet niet alleen om een nadere verkenning, maar eigenlijk ook om een politiek standpunt. Is het kabinet het met mij eens dat we naar een internet zonder trackingcookies moeten? Erkent het kabinet dat mensen veiliger worden als zo veel mogelijk Nederlanders cookies en tracking zouden blokkeren? Hoe gaan we ervoor zorgen dat zo veel mogelijk mensen dat doen?

Ik ben heel blij dat het kabinet al heeft gereageerd op het onderzoek van het Rathenau Instituut, maar willen we Nederlanders echt beschermen, dan moeten we nog een slag maken. Daarover de volgende vragen. Hoe gaat het kabinet de drie beleidsrichtingen concreet uitwerken? Welke heeft de voorkeur? Kan het kabinet na de zomer met een veel concretere uitwerking komen van hoe het cookies harder gaat aanpakken? Welke stappen kunnen we nationaal en internationaal zetten om hiernaartoe te werken? Hoe kijkt het kabinet naar maatregelen als het aanpassen van de Telecomwet en het verbieden van cookiemuren? Kunnen deze voorstellen ook na de zomer worden uitgewerkt? Ideeën voor een beter internet hebben we in Nederland genoeg. Nu moeten we nog het lef hebben om dat ook te bouwen.

Nog zo'n ranzig voorbeeld — ik noemde het woord net al — van surveillancekapitalisme is wat er met Pokémon is gebeurd. Iedereen die Pokémon GO heeft gespeeld op zijn telefoontje, heeft meegebouwd aan autonome moordwapens, omdat zijn locatiedata is verkocht aan de hoogste bieder. In dit geval waren dat bedrijven die oorlogswapens bouwen. The Privacy Collective is een massaclaim begonnen namens alle burgers wier data onrechtmatig is verzameld en is doorverkocht door gure bedrijven. Het is een rechtszaak tegen een bedrijf dat de data van 8,5 miljoen Nederlanders heeft buitgemaakt, waaronder van 1,5 miljoen kinderen. Dit is volstrekt onacceptabel. Dit soort tegenbewegingen moeten we politiek gewoon echt meer steunen. Hoe kijkt de staatssecretaris naar het nieuws over Pokémon GO, en wat kan de politiek doen om dit soort gedrag te voorkomen en te bestrijden? Is de staatssecretaris bereid om politieke steun te geven aan de massaclaim, om grenzen te stellen aan de datahonger van deze techbedrijven?

Tot slot de nazorgplicht, waarom de Kamer heeft gevraagd. Bij een grootschalig lek moeten we niet alleen boeven pakken en bedrijfsschade oplossen, we moeten ook de slachtoffers helpen. Dat vind ik een publieke zaak. Het gaat immers om de veiligheid van burgers, met name de mensen die al kwetsbaar zijn. De Raad van State heeft eind mei een advies gegeven over het Cyberbeveiligingsbesluit. Daarin zeggen ze: doe iets met nazorg. Hoe kijkt het kabinet naar die oproep? Gaat het die ter harte nemen na de zomer? Welke opties zijn er voor betere nazorg, en welke opties worden door het kabinet onderzocht? Hoe wordt eigenlijk mijn aangenomen motie hierover nu uitgevoerd? Is het kabinet bereid om de door de Kamer aangenomen amendementen op de Cyberbeveiligingswet, zoals de interventiebevoegdheid, ook aan de Raad van State voor te leggen?

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel. U heeft een interruptie van de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):
Ik kan het betoog van mevrouw Kathmann helemaal volgen als het gaat om

dataminimalisatie, spreiding en dat we daarmee zorgvuldig moeten zijn. Maar is mevrouw Kathmann het met ons eens dat databescherming hand in hand kan gaan met bijvoorbeeld Amerikaanse, Europese of nationale bedrijven, of in ieder geval dat het paspoort van degenen die die data zouden moeten beschermen, helemaal niet zou moeten uitmaken?

Mevrouw **Kathmann** (PRO):
Het paspoort van iedereen die waar ook ter wereld wil helpen om burgers te beschermen moet inderdaad niet uitmaken. Dat ben ik helemaal met de heer Van den Berg eens.

De heer **Van den Berg** (JA21):
Wat ik dan toch wel opzienbarend vind, is dat ik mevrouw Kathmann heel veel hoor spreken over het bigtechinfuus, over Amerikaanse bedrijven die door onze hele maatschappij zijn verweven en over dat dit een heel slechte zaak is. Maar als die bedrijven beter zijn in het beschermen van data dan onze eigen nationale of Europese bedrijven, dan zou mevrouw Kathmann het toch eigenlijk juist moeten toejuichen dat die bedrijven daar beter in zijn dan onze eigen bedrijven?

Mevrouw **Kathmann** (PRO):
Ik denk dat er hier twee dingen door elkaar worden gehaald. Op dit moment zitten we met het probleem dat digitale dienstverlening geopolitiek is geworden. Dat wij voor twee derde afhankelijk zijn van Amerikaanse techbedrijven maakt ons echt bizar kwetsbaar, omdat het geopolitiek is geworden en je daarmee onder druk kan worden gezet, of omdat de nationale veiligheid en de continuïteit van je digitale dienstverlening in gevaar kunnen komen. Dat is waarom wij toe moeten naar meer digitale autonomie. De bijsluiter daarbij is altijd: moet dat voor 100%? Nee, gelukkig niet. Moet dat morgen? Nee, gelukkig ook niet. Dat is wel de situatie waar we in zitten.

Voor deze geopolitieke situatie en voordat Trump aan zijn tweede termijn begon, was dit eigenlijk al een problematisch verhaal, omdat het nooit goed is om als land je eieren zo in één mandje te leggen. Het gaat er niet alleen om dat we aan een Amerikaans techinfuus liggen, maar we liggen voor 50% bij één merk. Dat is nooit een goed idee. We moeten veel meer gaan inzetten op het veiligstellen van ons eigen toekomstige verdienvermogen en op het groter maken van onze eigen ondernemers. Dat is nog het tweede wat daarbij hoort.

Daarbij is het niet voor niks dat heel veel Amerikaanse bedrijven zo groot zijn en dat mensen graag gebruikmaken van hun dienstverlening. Dat is ook omdat ze het qua basale beveiliging heel goed doen. We zeggen te vaak "in Europa kunnen we dat niet" of "in Nederland kunnen we dat niet". Dat is niet waar. Sterker nog, we hebben Nederlandse partijen die dat ook zouden kunnen, uitgenodigd in de Tweede Kamer. Daar moeten we gewoon veel meer gebruik van gaan maken.

We zien ook dat het juist heel vaak dezelfde Amerikaanse bigtechs en platformen zijn die de meest grote, gigantische datahonger hebben, wat ons kwetsbaar maakt. Dat zijn de drie redenen waarom ik vind dat we digitaal onafhankelijker moeten worden.

De heer **Verkuijlen** (VVD):
Dat was een helder betoog van mevrouw Kathmann. Ik ben even benieuwd naar het

volgende. We zijn natuurlijk twintig jaar lang afhankelijk geweest van Silicon Valley, waar alle ontwikkelingen zo'n beetje plaatsvonden. Dan komt de autonomiediscussie, de onafhankelijkheidsdiscussie. Dan staan er een aantal partijen in Nederland op — dat is hartstikke goed om te horen — die "dat kunnen wij ook wel" zeggen. U bent het toch met mij eens dat je zo'n evolutie van twintig jaar niet zomaar even inloopt? Ik ben daar dus even benieuwd naar. U zegt dat u naar meer onafhankelijkheid wil. Dat willen we allemaal, maar het transitiepad daarnaartoe zal lang zijn. Ik ben even benieuwd of mevrouw Kathmann dat met mij eens is.

Mevrouw **Kathmann** (PRO):
Ja, daarmee ben ik het zeker eens. Net vroeg de heer Van den Berg of we voor 100% onafhankelijk moeten zijn. In de beantwoording van die vraag zei ik al: nee, want dat kan ook helemaal niet. Kan dat morgen? Nee, dat kan al helemaal niet. En is dat moeilijk? Ja, dat is ook nog eens heel moeilijk. We hebben hier vaker debatten gehad over realistische tijdpaden. Die verschillen heel erg per dienstverlening waar het over gaat. Soms wordt er tegen de Kamer gezegd: voor deze dienstverlening gaat het twee jaar duren. Dan zeggen techexperts: ach, dat kan ook in zes maanden. Nou ja, dan kom je ergens op uit. Dat is in ieder geval niet morgen. Als je het hebt over het afbouwen van de twee derde afhankelijkheid, dan praat je gewoon over tien jaar en sommigen over vijftien jaar.

Het grote probleem is dat we elke keer niet beginnen omdat die paden lang zijn en omdat het moeilijk is. Het zou zo fijn zijn als we als Tweede Kamer gewoon eens dat plan krijgen, al is het een tienjarenplan: kom maar op! Daar kan ook gewoon "dit gaan we überhaupt niet doen" of "dit is niet realistisch" in staan, maar dan gaan we wel hier de eerste stappen zetten. Dat zou in ieder geval al heel fijn zijn.

De heer **Verkuijlen** (VVD):
Daar ben ik blij om. Op dat punt vinden we elkaar zeer. Volgens mij zitten we nu in de analysefase. We kijken waarvan we afhankelijk zijn en wat lopende contracten zijn. Wat betreft het pad waar u op doelt, met een plan voor de transitie, zult u ons op uw pad vinden.

De **voorzitter**:
Meneer Van den Berg, u heeft geen interruptie meer, of toch wel? Gaat uw gang.

De heer **Van den Berg** (JA21):
Ik ben verbaasd, maar ook positief verrast, dat er in ieder geval wordt erkend dat we zeker nog tien à vijftien jaar nodig zullen hebben om minder afhankelijk te worden van de big tech. Dat heb ik nog niet eerder zo duidelijk in een debat horen terugkomen. Zoals de heer Verkuijlen hier net zei, wordt er zo vaak geroepen dat Nederlandse of Europese bedrijven dit zomaar even kunnen overnemen. Als we terugkijken naar de geschiedenis, is het echter wel heel duidelijk. In 2024 werd het kabinet al gewaarschuwd: "Je hebt het niet op orde met exitprocedures. Wat nou als je wordt overgenomen? Hoe zit het met afhankelijkheden?" Wat dat betreft is er gewoon geslapen.

De **voorzitter**:
Wat is uw vraag?

De heer **Van den Berg** (JA21):
Mijn vraag is daarom: wat heeft mevrouw Kathmann, of PRO, in die tijd gedaan om dat in gang te zetten? Dit speelt namelijk al vele jaren.

Mevrouw **Kathmann** (PRO):
Dank voor de vraag. Dit speelt inderdaad al vele jaren. Ik ben eigenlijk ook al die vele jaren betrokken bij de strijd en bij alles om dit in ieder geval in gang te zetten. Het is dus ook helemaal geen verrassing dat het hier gaat over een lang tijdspad, want we hebben daar ook heel veel debatten over gehad. Daar worden deze ranges altijd in genoemd. Wat wij concreet hebben gedaan, is verschillende initiatiefnota's indienen. In het merendeel van de voorstellen staat dat de overheid echt een keertje moet gaan doen wat we hebben afgesproken. Dat is bijvoorbeeld een plan B hebben, die exitstrategieën invullen en risicoanalyses doen, zodat je veel beter je afhankelijkheden kent. Dan weet je ook veel beter: als we een plan gaan maken, waar moet je dan beginnen? Dat is natuurlijk het grootste risico. Ik denk niet dat er een initiatiefnota of motie is waar mijn naam niet als eerste onder staat, dan wel waar die mede onder staat op dit terrein. We hebben ook verschillende rondetafels en expertsessies georganiseerd om zo veel mogelijk kennis van buiten naar binnen te trekken. Daarnaast gebeurt het grote werk natuurlijk niet alleen maar hier in Den Haag, maar vooral ook in Brussel. Daar werken we ook elke dag heel hard om er vooral voor te zorgen dat wij vanuit Brussel als Nederland steun kunnen krijgen, ook juist op het gebied van wet- en regelgeving, om dit allemaal sneller mogelijk te maken. Want het gaat niet alleen om financiering; het gaat ook om wet- en regelgeving.

De **voorzitter**:
Dank u wel. Volgens mij zijn we hiermee aan het einde gekomen van de eerste termijn van de zijde van de Kamer. Ik kijk even naar rechts. Hoeveel tijd denkt u nodig te hebben voor de beantwoording van de vragen? 30 minuten, hoor ik. Dat lijkt mij redelijk. We gaan om 11.20 uur verder. Dank u wel. Ik schors de vergadering.

De vergadering wordt van 10.49 uur tot 11.20 uur geschorst.

De **voorzitter**:
Ik heropen de vergadering. Wij zijn toe aan de eerste termijn van de zijde van het kabinet. Wie kan ik het woord geven? Hoe gaat u het organiseren?

Staatssecretaris **Van Bruggen**:
Voorzitter. Dit hebben we voorbesproken, net als wie welke inhoud gaat doen. Het leek ons logisch dat ik begin, niet alleen naar aanleiding van het aantal vragen dat aan mij gesteld is, maar ook gewoon vanwege de volgorde waarin we zitten.

De **voorzitter**:
Dat is overzichtelijk. Gaat uw gang.

Staatssecretaris **Van Bruggen**:
Dank u wel, voorzitter. Voor mij is het …

De **voorzitter**:
Excuus. Vier interrupties wil ik toestaan. Gaat uw gang, sorry.

Staatssecretaris **Van Bruggen**:
Geen probleem, voorzitter. Dank. Het is de eerste keer voor mij dat ik met deze commissie in debat ga over deze belangrijke onderwerpen. De bescherming van persoonsgegevens en al die datalekken, waar we de afgelopen maanden naar gekeken hebben, raakt een hele brede portefeuille. Daarom treft u ons met z'n drieën vandaag. Een groot gedeelte van de vragen zag op de portefeuille Justitie en Veiligheid. Het is goed om zo dadelijk een aantal blokjes met u door te nemen. Ik hoop dat de beantwoording van de vragen daar voldoende in terugkomt.

Voorzitter. Ik heb eerst een inleidende spreektekst. Die ziet vooral op de zorg die ik deel met de commissieleden. Als ik zo eens eventjes terugkijk naar de afgelopen maanden, vanaf het begin van dit ambt, van 23 februari tot nu, zie ik tegen hoeveel ingewikkelde datalekken we hebben aangekeken en hoeveel brieven er met u gedeeld zijn vanuit het kabinet over deze onderwerpen. Dit is in ieder geval als dossier boven op mijn stapels beland, omdat het vaak ook heel technisch kan zijn, maar zeker ook vraagt dat er enige, laten we zeggen menselijke bevlogenheid, op dit dossier blijft. Die vindt u aan de kant van het kabinet in ieder geval vanuit ons drieën. Die zorg deel ik ook zeer. Dat is niet alleen onze zorg over de bescherming van persoonsgegevens, zoals we hier in deze samenstelling zitten, maar natuurlijk ook die van de mensen thuis. Ze zijn bang voor misbruik en voor toegang tot hun gegevens door onbevoegden of ze zijn bang dat die gegevens in verkeerde handen vallen, zoals te vaak gebeurt.

Incidenten, zoals de recente grote datalekken, leiden tot maatschappelijke onrust. Dat is heel terecht. Een datalek kan immense gevolgen hebben voor degenen wier gegevens dat betreft. Hoewel elk datalek anders is en eigen oorzaken kan hebben, hoop ik dat de recente gebeurtenissen ook een wake-upcall zijn, voor ons, voor de bedrijven en voor de inwoners zelf. Het illustreert hoe belangrijk de beveiliging van onze persoonsgegevens is. We spannen ons als kabinet in om de gevolgen van die datalekken dan ook te beperken door middel van het handelingskader voor slachtoffers van grote datalekken. Die brief is afgelopen week met u gedeeld. Sinds 2018 geldt de Algemene verordening gegevensbescherming, de AVG. Daarmee vertel ik u niks nieuws. Die heeft de correcte, veilige en transparante verwerking van persoonsgegevens tot doel. Daarbij houden individuele burgers de controle en wordt het gegevensverkeer tegelijkertijd niet onnodig gehinderd. Die balans moet er dus zijn.

Ook sinds 2018 geldt de UAVG, de uitvoeringswet. Deze wet treft voor Nederland meer specifieke regelingen en wijst de Autoriteit Persoonsgegevens aan als de onafhankelijke toezichthouder op de toepassing van de AVG. Maar de tijd staat niet stil sinds die tijd. Vanwege die voortschrijdende technologische ontwikkelingen is het van belang om de regels met betrekking tot de bescherming van persoonsgegevens regelmatig tegen het licht te houden. Zijn ze nog bij de tijd? Stellen ze onze inwoners nog in staat om regie te voeren over hun persoonsgegevens? Maar ook: zijn de regels werkbaar en begrijpelijk? Zorgen ze niet voor onnodige regeldruk?

De Verzamelwet gegevensbescherming is een belangrijke stap daartoe. Dit wetsvoorstel is op 20 mei 2025 door uw Kamer aangenomen en even later door de Eerste Kamer. In die verzamelwet worden diverse technische en inhoudelijke aanpassingen doorgevoerd, voornamelijk in de UAVG, met als doel het oplossen van knelpunten die in de praktijk sinds 2018 zijn ervaren.

Ook van groot belang zijn de verschillende voorstellen die in de Europese Commissie zijn gedaan en het voorstel voor de Digitale Omnibus. Daar hoorde ik uw zorgen ook over. Op Europees niveau gebeurt er ook ontzettend veel als het gaat over de bescherming van persoonsgegevens, in dit geval het voorstel voor de Digitale Omnibus. Een deel daarvan ziet op de wijziging van de AVG. Nederland levert daaraan een inhoudelijk stevige, constructieve bijdrage met ideeën om die wetgeving aan de ene kant eenvoudiger en duidelijker te maken, zonder dat aan de andere kant de bescherming van het Grondrecht, de gegevensbescherming, daarmee beschadigd zou worden.

We hebben als kabinet in dit coalitieakkoord opgenomen dat er gewerkt gaat worden aan een herziening en een vereenvoudiging van de AVG in Europees verband en van de toepassing van de huidige AVG in Nederland. Vanuit mijn verantwoordelijkheid voor het wettelijk kader en het stelsel met betrekking tot de bescherming van persoonsgegevens, ga ik dat dan ook graag aan. De ambitie uit het coalitieakkoord kent zowel die Europese als die nationale component. Juist op die niveaus voeren we dan ook de gesprekken. Het voornemen is om in het najaar een brede werkconferentie te organiseren die juist ook deze urgentie aangeeft, waarin we ook de input richting de Europese AVG en de nationale doorwerking met elkaar kunnen doorspreken. Graag informeer ik u daarna, in de loop van dit jaar — in het najaar komt er een brede werkconferentie; dat zal dan in Q3 zijn — over mijn aanpak, waaruit blijkt hoe ik van plan ben dat te gaan doen.

Vandaag heb ik een heel groot aantal vragen gekregen. Die zien op de onderwerpen: de algemene gegevensbescherming, datalekken en het toezicht. Ik heb ook het bekende blokje overig. Ik zou ze graag in die volgorde met u doornemen.

De eerste vraag die ik kreeg, is van JA21. Die ziet op de bereidheid om me in Europees verband in te zetten voor duidelijkere begrippen en concretere handvatten in de AVG. Ik zet mij daar zeker voor in. Ik heb het net in de inleiding al kort verteld. Ik herken dat die verwerkingsgegevens-verantwoordelijken in de AVG af en toe met de uitleg stoeien. Het is natuurlijk belangrijk om dat te verduidelijken. Onzekerheid over de juiste uitleg leidt niet alleen tot grotere lasten, maar zorgt er ook voor dat vereisten soms niet goed worden nageleefd. Daar zit dan vaak natuurlijk de crux. Het doet afbreuk aan de bescherming van het grondrecht. Op dit moment is de Digitale Omnibus in de EU in onderhandeling, waarmee de AVG wordt gewijzigd. De Nederlandse inzet is om met deze Digitale Omnibus de AVG te vereenvoudigen en te verduidelijken, en om daar geen afbreuk aan te doen. Er wordt gewerkt aan de verduidelijking van regels, bijvoorbeeld over de gegevensbeschermingseffectbeoordeling en het melden van een datalek wanneer dat noodzakelijk is. Daarnaast speelt in het stelsel van de AVG bij de uitleg van regels de onafhankelijke toezichthouder, in dit geval dus de Nederlandse Autoriteit Persoonsgegevens, een hele belangrijke rol. Zij hebben in Europees verband met elkaar overleggen hierover. De toezichthouder kan die richtsnoeren uitvaardigen over de uitleg van die complexe begrippen die toegesneden zijn op de praktijk.

De vraag die ik vervolgens kreeg van JA21 ziet op de rechtszekerheid die nodig is voor burgers, bedrijven en overheden. Deelt de staatssecretaris dat rechtszekerheid nodig is? Ja, zeker. In plaats van de starre regels, geeft de AVG ook juist die beoordelingsruimte. Dat heeft natuurlijk twee kanten. Aan de ene kant voelt het als minder duidelijkheid. Aan de andere kant kun je wel zeggen: die interpretatieruimte is bij tijd en wijle ook heel erg belangrijk. Het alternatief zou zijn dat er geen ruimte is om per geval afwegingen en

inschattingen te maken. Dat zou het vrije verkeer van persoonsgegevens, wat natuurlijk ook een van de doelen onder de AVG is, juist weer tekortdoen. Dus dit is steeds zoeken. Ik denk niet dat de rechtszekerheid dan per se tekortschiet. Ik denk wel dat, als de AVG wel de ruimte geeft voor die interpretatie, dat dan ook zorgvuldig moet gebeuren. Ik zie wel dat er af en toe wat handelingsverlegenheid is. Regels worden onnodig streng uitgelegd. Wat dat betreft hebben we waarschijnlijk nog veel te doen. Liever nietsdoen dan het verkeerd doen: dat merk je natuurlijk ook wel bij organisaties, bedrijven en misschien zelfs ook wel bij onze Rijksoverheid. De toezichthouder, de Autoriteit Persoonsgegevens, heeft hier oog voor. Die voorziet ook van veel informatie, bijvoorbeeld op haar website. Maar dit is een constante balans die je wilt hebben: die rechtszekerheid niet tekortdoen, maar wel die interpretatieruimte binnen de AVG houden.

Dan de vraag van JA21 of de AVG wel duidelijk is. Is er niet te veel ruimte voor interpretatie? Het ligt misschien in het verlengde daarvan. Mijn invulling daarvan is dat het ruimte geeft voor maatwerk. Dat hoeft geen afbreuk te doen aan de rechtszekerheid. Ik verwijs naar de uitleg die ik daarbij zojuist gaf.

De vraag in het verlengde daarvan zag op de doorgifte van gegevens aan derde landen. Dat ziet op privacy en rechtszekerheid. Indien de gegevens worden doorgegeven aan derde landen, is het slechts toegestaan onder de voorwaarden die gelden in de AVG. Zo is gegevensdoorgifte toegestaan indien de Europese Commissie een adequaatheidsbesluit heeft genomen voor het derde land. Dan beoordeelt de Europese Commissie dat het niveau van gegevensbescherming in essentie vergelijkbaar is met het beschermingsniveau in de EU en is die gegevensdoorgifte toegestaan indien de verwerkingsverantwoordelijke zorgdraagt voor die passende waarborgen. Het is in beginsel aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de doorgifte in overeenstemming is met de geldende voorwaarden. De rechter ziet daar ook op toe. In Europa is dat in laatste instantie het Europese Hof van Justitie.

Dan de vraag van de VVD. Die zag op de transparantie en begrijpelijkheid van privacyverklaringen bij apps, in dit geval zeer gevoelige persoonsgegevens, zoals, als het gaat over zorg, de cyclus- en zwangerschapsapps. Er was een vraag die daar in het verlengde van lag, namelijk of ik mogelijkheden zie om die informatievoorziening richting gebruikers te verbeteren, zodat ze beter geïnformeerd kunnen worden en die apps hun eigen verantwoordelijkheid kunnen nemen in de privacy-informatievoorziening. Ook werd gevraagd of het mogelijk is om dat laatste verplicht te stellen. De AVG stelt hele strenge voorwaarden aan de verwerking van gegevens, vooral als het gaat om gezondheidsgegevens. Ook verplicht de AVG al tot communicatie in begrijpelijke, duidelijke en eenvoudige taal. Voor het creëren van die additionele vereisten zie ik nu geen grondslag. Ik deel wel met uw Kamer dat ik het belang inzie van die goede regels en van de naleving daarvan, zeker als het gaat om gezondheid. In dit geval gaat het om de gezondheid van vrouwen, bijvoorbeeld omdat het ongewenste profiling oplevert en je wat agressiever gerichte advertenties krijgt, terwijl je je daar zelf minder bewust van bent. De verwerking van bijzondere persoonsgegevens, zoals deze gezondheidsgegevens, die daar namelijk onder vallen, is verboden, tenzij er een wettelijke uitzonderingsgrond van toepassing is. Dat is bijvoorbeeld het geval wanneer er uitdrukkelijke toestemming is gegeven.

Volgens rechtspraak van het Hof van Justitie van de Europese Unie vallen onder het

begrip "bijzondere persoonsgegevens" ook de persoonlijke gegevens die bij het online bestellen van geneesmiddelen worden ingevoerd, zoals namen en adressen. Het is belangrijk dat er scherp toezicht wordt gehouden op naleving van de AVG. Daarin heeft het kabinet weliswaar geen rol, maar dit zijn natuurlijk wel de gesprekken die ik voer met de Autoriteit Persoonsgegevens. Juist als het gaat over gezondheidsgegevens en gegevens die gedeeld worden in het kader van toch wel een hele persoonlijke beleving, die in dit geval zeker bij vrouwen aan de orde kan zijn, maar zeker niet in mindere mate bij mannen of bij whomever die iets deelt over zijn of haar gezondheid, moet men er extra alert op zijn dat dit bijzondere persoonsgegevens zijn die gedeeld worden. Er kan dus ook een zwaardere grond voor zijn om die gegevens zomaar te kunnen delen.

De heer **Verkuijlen** (VVD):
Dank aan de staatssecretaris voor haar uitvoerige antwoord. Zij ziet geen grondslag om dat extra te verplichten of op een andere manier te doen, maar volgens mij staat het er eigenlijk al. De staatssecretaris noemde het ook al zo, namelijk: je moet uitdrukkelijk toestemming geven. Daar zit volgens mij het grijze gebied. Mensen zijn zich te weinig bewust van het feit dat pas na uitdrukkelijke toestemming … Ik ben benieuwd hoe zij daarnaar kijkt en of zij daar nog mogelijkheden voor ziet.

Staatssecretaris **Van Bruggen**:
Ik denk dat het goed is dat ik dit gesprek, deze informatie en deze zorg ook deel met de Autoriteit Persoonsgegevens. Juist in de informatievoorziening hebben we namelijk iets extra's te doen. Het is een, laten we zeggen, bijzondere voorwaarde. Het is ook iets waar mensen zich misschien niet zo bewust van zijn. Ik kan in ieder geval in het gesprek met de Autoriteit Persoonsgegevens aangeven of de gebruiker het bewustzijn heeft en of het voor de gebruiker helder genoeg is dat voor het delen van hele specifieke persoonlijke gezondheidsgegevens daadwerkelijk toestemming moet worden gegeven. Daar zal ik later nog iets over zeggen.

De heer **Verkuijlen** (VVD):
Dank voor dat antwoord. Ik begrijp uw positie ook ten opzichte van de AP. U gaat hier nog in Europees verband voor pleiten. Zou u dit punt mee willen nemen?

Staatssecretaris **Van Bruggen**:
Die bijzondere persoonsgegevens en de uitleg daarvan zijn dagelijks onderwerp van gesprek, zou ik willen zeggen. In dit geval is dat zeker zo, omdat het natuurlijk ook raakt aan waar we mee bezig zijn in de onderhandelingen over de Omnibus. Ik zal hier voor mezelf ook alert op zijn dat dit meegenomen wordt.

Dan door naar een vraag van D66 ten aanzien van dataminimalisatie en het bewaren van persoonsgegevens. Welke stappen zijn er via de Europese route genomen? Welke maatregelen kunnen eventueel nationaal nog worden genomen? De AVG heeft als uitgangspunt dat er niet meer persoonsgegevens worden verwerkt dan nodig is en dat die niet langer worden bewaard dan nodig is. De AVG hanteert een risicogebaseerde aanpak, zoals dat heet. Dat betekent dat per geval bekeken moet worden hoe de normen uit de AVG moeten worden ingevuld. Dat geldt ook hiervoor. Elke verwerkingsverantwoordelijke moet objectief kunnen onderbouwen waarom gegevens worden verwerkt, welke gegevens dat betreft en hoelang deze bewaard worden. De Autoriteit Persoonsgegevens houdt niet alleen toezicht op de naleving, maar geeft ook juist de handvatten voor de toepassing van deze omstandigheden voor de

verwerkingsverantwoordelijken.

Ik denk dat de D66-fractie ook vroeg: wat vindt u daarvan? Ik wil niet vooruitlopen op de vraag die u daarover gesteld heeft, maar het belangrijkste is dat mijn rol ten opzichte van de Autoriteit Persoonsgegevens natuurlijk heel vaak gaat om het gesprek voeren met elkaar. Dat is het gesprek over hoe dat goede toezicht ingevuld wordt en over hoe je streeft naar dataminimalisatie. Dat gaat er in ieder geval om dat we op een goede manier, steeds weer in de geest van deze tijd, toezicht weten te houden op de honger naar data die er nu is. Daar zullen we zo dadelijk in het blokje Autoriteit Persoonsgegevens nog wel even over praten.

Bewaartermijnen ...

De **voorzitter**:
U heeft een interruptie van mevrouw Kathmann. O, ik hoor dat zij dit antwoord afwacht.

Staatssecretaris **Van Bruggen**:
PRO had vragen over bewaartermijnen. Wat doen we om bedrijven zo weinig mogelijk data te laten bewaren? Wat zijn bewaartermijnen waard als niemand ze naleeft, zelfs de politie niet? Hoe gaan we daar veel steviger op toezien? Zoals ik net zei, is de verwerkingsverantwoordelijke zelf verantwoordelijk volgens de AVG. Ik noem dus toch weer even de basis van waaruit we werken. Ik ben het wel met u eens dat de overheid zelf ook het goede voorbeeld moet geven bij het naleven van deze wettelijke regels. Wanneer overheidsorganisaties bewaartermijnen hanteren die in redelijkheid niet te verantwoorden zijn, kan dat een reden zijn om met hen in gesprek te gaan. Dat is investeren in goed intern toezicht, bijvoorbeeld door de positie van de functionaris voor de gegevensbescherming te versterken.

Het klopt dat er een discussie loopt over de bewaartermijnen bij de politie, juist ook in verband met de aanpak van cold cases. Je ziet daar dat er aan de andere kant een wens kan zijn om data langer te bewaren. Dit is een doorlopend, maar zeker ook heel actueel gesprek. De minister van Justitie en Veiligheid zal hier nader op ingaan in het halfjaarbericht dat de politie uitstuurt. Dat wordt volgende week nog verzonden. Hier wordt deze vraag nog in meegenomen.

Mevrouw **Kathmann** (PRO):
De vraag was niet per se bedoeld om naar de politie te wijzen; dat was slechts een voorbeeld. De overheid hoeft helemaal niet per se naar zichzelf te wijzen. We hebben gewoon een maatschappelijk probleem en daar gaat deze vraag over. We hadden een expertsessie. Daarin ging het ook over dataminimalisatie en over het feit dat we meer moeten doen dan alleen die wetgeving. Die datahonger leidt ertoe dat we in een maatschappij leven waarin het opslaan en verzamelen van data eigenlijk prioriteit één in de organisatie is, terwijl het beveiligen van de data prioriteit één moet worden. We moeten dat omdraaien. Het beveiligen moet op één gaan staan.

Eigenlijk gaat deze vraag over: hoe gaan we daar komen? Dat vraagt om veel meer dan wetgeving. Dat vraagt om bewustwording, cultuur en noem het allemaal maar op. Die cultuur hebben we gewoon niet. Omdat data het nieuwe goud was, is iedereen in de datahonger geschoten. Echt waar, dat geldt voor de hele samenleving. Daar moeten we vanaf. Het beveiligen van data moet de prioriteit worden. Dat is eigenlijk waar deze

vraag over gaat.

Staatssecretaris **Van Bruggen**:
Het is heel herkenbaar en wat mij betreft is het ook niet per se of-of. Het is ook echt en-en. In de dataminimalisatie die je nastreeft, kun je natuurlijk nog steeds de grondslag van stevige wet- en regelgeving vanuit de AVG beïnvloeden om te zorgen dat die actueel is en dat je niet blijft hangen in 2018. Dat is de ene kant.

De andere kant is voor mij het gesprek voeren met de toezichthouder. Als we dan weten dat hier zo'n honger naar is, hoe zorgen we dan dat de informatiepositie en informatievoorziening richting onze inwoners op orde zijn?

Dat zijn ongeveer de kaders waarbinnen ik mij beweeg. Als wij zorgen dat wij steeds dit gesprek blijven voeren ... Zoals ik al zei, is dit vanaf 23 februari boven op mijn stapel beland door zo'n beetje alle datalekken die we in de media zien. Ik zie ook dat wij qua gedachten af en toe nog even zijn blijven hangen in 2018. Zeg ik dan meteen dat het uitgangspunt beveiliging moet zijn? Ik geloof dat de balans die we nu in de AVG hebben gezocht een groot goed is. Dat betreft het punt dat het vrije verkeer van gegevens ook een van de doelstellingen is. Die balans is wellicht wat doorgeslagen. Hoe kunnen we die balans herstellen? Dat is voor mij een hele belangrijke.

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Van Bruggen**:
Dan de vraag van het CDA: is de staatssecretaris bereid om bewaartermijnen veel harder te laten handhaven, zeker bij organisaties die gegevens van miljoenen mensen bewaren? Harder handhaven is een ingewikkelde. Bewaartermijnen worden strikt toegepast en niet nodeloos opgerekt, om toch maar weer even die balans erin te brengen, zeker als het gaat om hele grote hoeveelheden of gevoelige data. Net als u vind ik het nodig dat er wordt gehandhaafd, dat die organisaties hier niet te veel ruimte in krijgen en dat ze ook ervaren dat een toezichthouder dit doet. Ik kan geen opdrachten geven aan de Autoriteit Persoonsgegevens om te handhaven bij bepaalde organisaties die heel veel data bewaren. Het enige wat ik kan doen — dat doe ik dan ook veelvuldig — is het gesprek voeren over hoe belangrijk het is dat, als het gaat over bewaartermijnen, het bewustzijn bij die organisaties vergroot wordt. Om het voorbeeld van Odido nog even te noemen: daar worden natuurlijk enorme lengtes van bewaartermijnen genoemd. Zoals ik net zei: als het gaat over cold cases, zou dat wellicht heel interessant zijn. Als het gaat over de data van de gemiddelde Odido-klant, die daarvoor nog bij Ben zat, geloof ik, denk ik vooral: daar hebben ze dus zelf wellicht ook in de informatievoorziening onvoldoende rekening mee gehouden. Dan moet je als Autoriteit Persoonsgegevens die informatie voldoende kunnen verstrekken. Daar zijn we natuurlijk steeds naar op zoek, ook bij die bedrijven die heel veel en gevoelige informatie van hun klanten te lang bewaren.

Dan was er een vervolgvraag …

De **voorzitter**:
Sorry. U heeft een interruptie van mevrouw Zwinkels, CDA.

Mevrouw **Zwinkels** (CDA):
Ik heb een vraag ten aanzien van de hardere handhaving, die wat ons betreft moet plaatsvinden. Ik snap dat dat ingewikkeld is. Ik heb in mijn inbreng ook al aangegeven dat ik begrijp dat er op die manier niet nog extra opdrachten richting de AP worden gegeven, omdat zij onafhankelijk hun werk doen. Ik ben wel benieuwd wat de staatssecretaris vanuit haar rol proactief kan doen richting die organisaties om die bewustwording op gang te brengen en om dat gesprek te voeren — dat is eigenlijk precies wat ze net aangeeft — om duidelijk te maken dat er wel degelijk een handhavingskader achter deze regels schuilgaat waar de overheid ook belang aan hecht. Anders voorzie ik toch dat we niet veel opschieten na dit debat.

Staatssecretaris **Van Bruggen**:
Het is niet voor niets dat we met dat handelingskader aan de slag zijn gegaan. Alleen maar verwijzen naar de toezichthouder en zeggen dat dat de Autoriteit Persoonsgegevens is en dat die toezicht zal moeten houden, vind ik te weinig. Als overheid heb je hier ook iets in te doen. Over dat handelingskader zijn verschillende vragen gesteld. Zo dadelijk zal ik daar nog op terugkomen in het blokje over datalekken. Ik denk juist dat we in dat handelingskader ook voldoende ruimte zoeken om het bewustzijn te vergroten bij inwoners die data delen en bij organisaties die een verantwoordelijkheid hebben, waar wij als overheid zorgen over hebben als dat niet goed gaat of daar onvoldoende bewustzijn is.

De **voorzitter**:
Een vervolgvraag?

Mevrouw **Zwinkels** (CDA):
Ja, één vervolgvraag. Is dat een soort toezegging dat we het handelingskader gaan uitbreiden op dit specifieke punt? Want ik zou dan wel graag willen dat we leren van bijvoorbeeld de casus van Odido. Wat kan ik op dat vlak verwachten?

Staatssecretaris **Van Bruggen**:
Ik begrijp even niet goed of de vraag is of het handelingskader op dat gebied uitgebreid zou moeten worden. Misschien kan die vraag nog één keer verduidelijkt worden. Dan kan ik daar in de tweede termijn een helder antwoord op geven.

Mevrouw **Zwinkels** (CDA):
Mijn indruk was dat het handelingskader op dit moment vooral toeziet op hoe om te gaan met de slachtoffers. Ik zou juist meer de preventieve kant daarin terug willen zien. Ik noem bijvoorbeeld dat je daarin meeneemt dat objectief moet worden onderbouwd waarom en hoelang je iets niet langer dan nodig bewaart.

De **voorzitter**:
Daarop komt u terug in de tweede termijn?

Staatssecretaris **Van Bruggen**:
Ja, in de tweede termijn kom ik daarop terug, want dat is een heldere vraag.

Voorzitter, met uw …

De **voorzitter**:

Sorry, nog één interruptie, van mevrouw El Boujdaini, D66.

Mevrouw **El Boujdaini** (D66):
Ja, ik heb nog één verhelderende vraag. Ik ben even benieuwd of de staatssecretaris nog gaat terugkomen op de termijnen die in principe ontbreken in de AVG, en op wat de staatssecretaris daarvan vindt. Want daar heb ik nog niet echt een heel concreet antwoord op. Ik vind het wel even belangrijk om dat scherp te hebben.

Staatssecretaris **Van Bruggen**:
Daar ga ik niet nog nader op terugkomen. Het ingewikkelde is dat je, als het gaat om de rek die we hebben, altijd moet bekijken wat zorgvuldig is. Een bewaartermijn kan soms juist … Dat is een beetje wat ik aangaf over de balans tussen een cold case versus een bedrijf dat ongeoorloofd veel te lang en veel te veel jaren gevoelige gegevens van z'n gebruikers bewaart. Als je het "one size fits all" zou maken, doe je beide misschien wel iets tekort. In die zin ga ik daar dus niet steviger op inzetten.

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Van Bruggen**:
Dan kom ik bij het volgende blokje: datalekken. Ik begin met het handelingskader voor de slachtoffers. De heer Verkuijlen vroeg aan mij of het kabinet inzicht heeft in de kwaliteit van de communicatie richting de slachtoffers en of ook wordt geëvalueerd of mensen de verstrekte informatie daadwerkelijk begrijpen en kunnen gebruiken. Het wil niet zeggen dat het kabinet het niet belangrijk vindt, maar ik ga er niet over, om het maar even zo te zeggen. Dat is een beetje zoeken. De verantwoordelijkheid ligt bij de organisatie zelf. Dat is het eerste belang. We werken wel vanuit dat handelingskader voor slachtoffers aan meer duidelijkheid. De overheid voelt wel dat ze niet te allen tijde een terugtrekkende beweging kan blijven maken en alleen maar de verantwoordelijkheid bij de organisaties kan blijven leggen. Die wil de slachtoffers een goede informatiepositie geven. Ik noem het gesprek met de organisaties waar de data bewaard worden, maar ook de informatie richting de slachtoffers zelf. De taak ligt wel bij de Autoriteit Persoonsgegevens. We werken vanuit het handelingskader voor slachtoffers. We hebben onderzoek laten uitvoeren onder inwoners naar hun ervaringen, behoeften, vragen en zorgen naar aanleiding van de datalekken. Over dat onderzoek bent u in de brief van 23 juni geïnformeerd. Dit is wat we doen, wat we kunnen doen en hoe we proberen om in ieder geval de positie van de inwoners te verstevigen, bijvoorbeeld met de vragenronde.

Dan een vraag van de heer Verkuijlen die zag op rechten en mogelijkheden. Dat ligt een beetje in het verlengde ervan. Die organisaties zijn zelf verplicht om te informeren over en bij een datalek. Ze kunnen en moeten verplicht in duidelijke en eenvoudige taal beschrijven wat er is gebeurd, wat de gevolgen zijn en wat de organisatie doet om het datalek aan te pakken en de nadelige gevolgen te beperken. Die informatie heeft het slachtoffer ook weer nodig om zelf stappen te kunnen zetten. De verplichtingen zijn opgenomen in de AVG. De Autoriteit Persoonsgegevens houdt hier formeel toezicht op.

De vraag die in het verlengde daarvan lag, ging over de ondersteuning richting andere overheidsorganisaties bij grote datalekken, dus bijvoorbeeld gemeenten die ondersteuning van de Rijksoverheid missen op het moment dat zij hiermee te maken

hebben. Het kabinet herkent dat beeld niet. Gelukkig maar, moet ik daarbij zeggen. Bij incidenten worden gemeenten ondersteund door de informatiebeveiligingsdienst van de VNG en waar nodig ook door het Nationaal Cyber Security Centrum. Daar is geen sprake van een terughoudende houding vanuit de Rijksoverheid. We gaan wel graag in gesprek met gemeenten en met de koepels indien dit beeld heerst om te kijken waar een dergelijk gevoel vandaan zou kunnen komen. Want het kan natuurlijk niet de bedoeling zijn, zeker als wij denken dat we er zijn voor onze collega-overheden, dat zij denken: waar blijft de Rijksoverheid? Dat is dus in ieder geval een alertheid voor onszelf. Ik hoop niet dat ik nu de enige vraag voor mijn collega voor zijn voeten heb weggemaaid.

De heer **Verkuijlen** (VVD):
De staatssecretaris deed dat uitstekend. Uw collega kennende, komt hij daar vast nog op terug. U zei net: wij voelen ons als overheid minder betrokken dan … Nou, niet betrokken, maar "wij zien onze rol wel anders als het gaat om de slachtoffers van die datalekken". Maar op het moment dat die slachtoffers aangifte gaan doen, vallen ze gewoon onder slachtofferzorg. Dan hebben ze in feite wel recht op zo goed mogelijke bijstand. Ik ben even benieuwd hoe u daarnaar kijkt, hoe u dat ziet en hoe u de rol van de AP ziet. Als je echt slachtoffer bent en je aangifte hebt gedaan, heb je juridisch volgens mij toch iets meer te doen als overheid en is het niet slechts een klant van een commerciële partij.

Staatssecretaris **Van Bruggen**:
Vermoedelijk kan die beter beantwoord worden in de tweede termijn, want ik zoek even naar: gaat dit over rechtsbijstand, gaat het over slachtofferhulp? Ik moet even kijken wat een goede interpretatie van uw vraag is om daar ook een goed antwoord op te kunnen geven.

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Van Bruggen**:
De vraag van mevrouw Zwinkels van het CDA was: komt er een landelijke standaard voor hulp aan slachtoffers van grote datalekken, zodat mensen niet verdwalen tussen gemeente, bedrijf, politie, bank en toezichthouder? Het antwoord is: ja. Het streven is erop gericht dat het handelingskader voor slachtoffers van grote datalekken op korte termijn wordt afgerond, in overleg met de relevante instanties, betrokken toezichthouders en vertegenwoordigers van het bedrijfsleven. Deze informatie kan vervolgens door de AP, als onderdeel of naar aanleiding van de meldingsprocedure voor datalekken, aan organisaties worden aangeboden en op de website van de betrokken organisaties ter beschikking worden gesteld. Uw Kamer zal nog dit jaar hierover nader worden geïnformeerd.

Dan de vraag van de heer Verkuijlen. Die zag op de cybercriminelen en de effectiviteit van de opsporing daarvan. Grote internationale acties van afgelopen week en vorige week bewijzen: ja, hiermee kunnen wij criminelen wel degelijk opsporen. Het blijven echter complexe internationale onderzoeken, waarbij heel veel partners een rol spelen. Naar de effectiviteit van opsporing bij ransomware en datadiefstal is wetenschappelijk onderzoek gedaan. Een mix van onvoorspelbaarheid in interventies bij de opsporing blijkt dan het meest succesvol. We kunnen dus eigenlijk niet eens voorspellen wat de

beste manier is, en dat is misschien dan ook de juiste. Politie en OM kijken voortdurend naar innovatieve interventies en worden ook wereldwijd als toonaangevende partners gezien. Het blijft lastig om verdachten van hightechcybercrime in Nederland te berechten. Verdachten bevinden zich vaak in landen waar geen goede rechtshulprelatie mee bestaat. Om die reden heeft het kabinet in het coalitieakkoord ook als ambitie uitgesproken om cybercriminelen vaker op de EU-sanctielijst te plaatsen. Wat we kunnen doen in de opsporing, doen we dus, op een manier die blijkbaar innovatief is, zodat dat ook internationaal gezien wordt. We proberen de ambitie om cybercriminelen op de EU-sanctielijst te plaatsen ook echt kracht bij te zetten.

Dan een vraag over betalingen na datadiefstal. Het advies blijft: altijd. Als een organisatie te maken krijgt met ransomware, kan dat heel veel impact hebben, maar de afweging is aan de getroffen organisatie. Advies: geen losgeld betalen, want het is bijna ... Ik heb hier een mooie quote van cyberexpert Rutger Leukfeldt: "Wie betaalt koopt geen oplossing, maar een uitnodiging voor de volgende aanval." Dat was, dat is en dat blijft ook in dit geval dus het advies. Ter aanvulling, want ik zie nog wat aarzelende bewegingen, ook bij de heer Verkuijlen: vanuit de overheid wordt op meerdere manieren voorlichting gegeven of worden hulpmiddelen ter beschikking gesteld, bijvoorbeeld via het Nationaal Cyber Security Centrum. Ook worden enkele specifieke activiteiten ondernomen, zoals de website "nomoreransom.org", waarop de politie en de internationale partners kosteloos sleutels aanbieden om de versleuteling door criminelen weer ongedaan te maken. Ransomware of datadiefstal: het is een gezamenlijk probleem. Elke partij die hierop actie kan ondernemen, zal dat ook moeten doen en door samen op te trekken kunnen we ervoor zorgen dat het minder loont. Maar dat het complex is, kan ik alleen maar bevestigen.

Voorzitter. Dat was blokje twee, datalekken. Dan ga ik met uw goedvinden naar het blok toezicht.

De **voorzitter**:
Er is eerst nog een interruptie van mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Ik vrees een beetje voor een gemiste vraag. Ik zit even te denken: wanneer gaan we die inventariseren? Ik kan de vraag nu stellen, maar misschien kan het ook later nog.

De **voorzitter**:
Kunt u de vraag nog even vasthouden? Meneer Van den Berg.

De heer **Van den Berg** (JA21):
Toch nog even over die datalekken, en dan specifiek over Odido. Nou zijn we zelf even in de exacte data gedoken: wat is er wel en wat is er niet gelekt? Dan zie je best wel een discrepantie. Odido zei zelf: er zijn 6,2 miljoen accounts gelekt. Als je echter zelf de data bekijkt, blijkt het te gaan om 21 miljoen accounts. Dat maakt niet zo veel uit, het gaat er meer om dat 5,5 miljoen van die accounts volgens de eigen voorwaarden van Odido allang verwijderd hadden moeten worden. Mijn vraag is hoe we nou optreden tegen dat soort excessen, als zelfs de eigen voorwaarden niet worden nagekomen. Wat kan het ministerie dan nog doen om dit te voorkomen?

Staatssecretaris **Van Bruggen**:

Dat is een logische vraag. De AP doet ook onderzoek naar deze casus bij Odido. Wat mij betreft is het gegeven dat de Autoriteit Persoonsgegevens ook daadwerkelijk optreedt en het onderzoek oppakt als een situatie zich voordoet, ook een bevestiging dat het stelsel van de toezichthouder werkt. Dat wacht ik natuurlijk af. Dat is niet iets waar ik op vooruit kan lopen.

De **voorzitter**:
Er is een vervolgvraag van de heer Van den Berg.

De heer **Van den Berg** (JA21):
Jazeker. Oké, maar hoe werkt het dan in de praktijk? Dan kan de AP een boete opleggen, maar er blijkt ook dat er data van zeker iets van 30 Kamerleden, ministers, oud-bewindspersonen en mensen van de AIVD, de MIVD en de politie tussen zaten. Het gaat om zeer kwetsbare data. De gevolgen daarvan kunnen enorm zijn. Kunnen de mensen die daar schade van gaan ondervinden — en dat kan ik me zomaar voorstellen — bijvoorbeeld Odido, of een ander in een vergelijkbare situatie, aansprakelijk stellen?

Staatssecretaris **Van Bruggen**:
Dat kan zeker. Die twee dingen staan eigenlijk los van elkaar. Het is belangrijk voor mij dat de AP hier onderzoek naar doet. Het staat mensen natuurlijk altijd vrij om daar zelf stappen op te ondernemen op het moment dat dit ze overkomen is.

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Van Bruggen**:
Dank, voorzitter. Dan ga ik verder met de vragen over de Autoriteit Persoonsgegevens en de manier van toezichthouden, dus het proactief toezicht. JA21 en D66 stelden daar vragen over. Hoe voorkomen we dat de AP vooral reactief optreedt, nadat gegevens gelekt zijn? Er is bijna geen mooier bruggetje denkbaar. Kan de staatssecretaris verkennen wat nodig is om de AP in staat te stellen tot het gewenste proactieve toezicht? De AP is een onafhankelijke toezichthouder. Die bepaalt zelf waar ze toezicht op houdt en of dat reactief of proactief is binnen de mogelijkheden die ze daarvoor heeft. Op eigen beweging kunnen ze nu ook onderzoek doen naar mogelijke overtredingen van de privacywetgeving. Daarnaast kunnen organisaties ook terecht bij hun interne toezichthouder, de functionaris gegevensbescherming. De FG's helpen juist op een laagdrempelige manier om toezicht te houden op de eigen organisaties. Die kennis en informatie worden met elkaar gedeeld. Dat is dus de manier waarop het nu is ingericht. Het proactieve is dus echt aan de Autoriteit Persoonsgegevens zelf en de keuze die ze daarin op een bepaald moment maakt.

Dan de indicatoren, want natuurlijk heb ik wel het gesprek met de Autoriteit Persoonsgegevens. Mijn ambtsvoorganger heeft met de autoriteit afgesproken dat die in samenspraak met JenV in de nabije toekomst een meetinstrument en indicatoren ontwikkelt om inzicht te krijgen in het doelmatig en doeltreffend functioneren van de AP. De AP kan dan op een transparante wijze gaan verantwoorden dat de middelen doelmatig en doeltreffend besteed worden. Daarmee wordt ook inzichtelijker hoe de activiteiten van de AP leiden tot concrete verbeteringen voor de inwoners. De EDPB, de Europese toezichthouder, is momenteel bezig met een landenvergelijkend onderzoek naar die doelmatigheid. Daarom is dat ook voor ons relevant. Naar verwachting wordt

dat onderzoek aan het einde van het jaar afgerond. Ook is de AP bezig met de uitwerking van doeltreffendheidsindicatoren door pilots en effectonderzoeken bij bepaalde projecten. De capaciteit die daarvoor nodig is, heeft de AP dan ook vrijgemaakt.

Dan de samenwerking tussen de AP en de politie.

De **voorzitter**:
Er is een interruptie van mevrouw El Boujdaini van D66.

Mevrouw **El Boujdaini** (D66):
Ik zat nog wel even te denken, want het meetinstrument en de indicatoren zouden in samenspraak tussen JenV en de AP worden opgesteld. Mijn vraag is dan nog wel eventjes wanneer wij dat kunnen verwachten, aangezien daaraan als het goed is ook vastzit dat we kunnen zien of de middelen doelmatig en doeltreffend worden besteed. Van daaruit zouden we weer kunnen bekijken wat gebruikt zou kunnen worden voor proactief toezicht, als daar middelen voor beschikbaar zouden moeten worden gesteld.

Staatssecretaris **Van Bruggen**:
De informatie die ik als laatste heb gekregen, is dat zij daar al capaciteit voor beschikbaar hebben gesteld omdat het gemeenschappelijk belang daarvan wel is uitgesproken. Ik kan in ieder geval toezeggen dat ik ze ga vragen wanneer ik mag verwachten dat er iets inzichtelijk wordt gemaakt.

Dan ga ik door naar de samenwerking tussen de AP en de politie. Is de staatssecretaris bereid om in kaart te brengen hoe de samenwerking tussen de politie en de AP momenteel is ingericht, waar knelpunten liggen en waar mogelijkheden liggen om die samenwerking te verbeteren? Dat was een vraag van D66. Het kabinet erkent het belang van de werkrelatie tussen de politie en de AP. Op een groot aantal dossiers staan ze dan ook in nauw contact met elkaar. In veel dossiers spelen natuurlijk die vraagstukken omtrent gegevensbescherming. Uit periodieke overleggen met de AP zijn mij vanuit hen geen klachten ter ore gekomen. Ook bij navraag over mogelijke knelpunten in de samenwerking bij de AP is dat niet gebleken. Het hoort juist bij de taak van de toezichthouder om in gesprek te gaan over de verschillen in de interpretatie van de wetgeving. Dit is dus wat zij binnen hun toezichthoudende rol doen. Die signalen dat dat niet goed zou lopen, zijn mij in die zin dus niet bekend.

De vraag vanuit het CDA zag op de capaciteit en prioritering van de Autoriteit Persoonsgegevens. JA21 heeft daar ook een vraag over gesteld. Ik bouw het even op. Heeft de AP volgens de staatssecretaris voldoende capaciteit en technische expertise voor privacy- en AI-toezicht? Heeft de AP voldoende budget? Kan de staatssecretaris aangeven of de AP voldoende capaciteit heeft? Als die capaciteit niet voldoende is, welke keuzes worden er dan gemaakt? Waar liggen de prioriteiten? Naar onze mening heeft de Autoriteit Persoonsgegevens voldoende capaciteit en financiële middelen om haar taken goed uit te voeren. Wel is het zo dat er extra middelen worden vrijgemaakt als er nieuwe taken bij komen, bijvoorbeeld toezichtstaken uit de AI-verordening. Als de taken blijven zoals ze zijn, zijn de middelen dus toereikend, en ook de capaciteit daarvoor — ze gaan zelf over de inzet daarvan — maar als er taken bij komen, zoals uit de AI-verordening, dan worden er middelen vrijgemaakt. Prioritering is dan ook niet een van de opdrachten die je daarbij meegeeft.

Mevrouw **Zwinkels** (CDA):
Ik denk dat er op dit moment verschillende beelden bestaan over de vraag of er voldoende middelen en capaciteit zijn bij de AP. Ik begrijp van de staatssecretaris dat zij aan ons toezegt dat wanneer die AI-verordening tot extra taken leidt, het kabinet zich ervoor gaat inspannen om extra middelen vrij te maken. Klopt dat?

Staatssecretaris **Van Bruggen**:
Dat klopt, dus dat kan ik bij dezen toezeggen.

Mevrouw **Zwinkels** (CDA):
Ik zou willen weten wanneer we daar dan wat meer informatie over krijgen, want de AI-verordening komt er natuurlijk aan.

Staatssecretaris **Van Bruggen**:
Daar kan mijn collega nog wat uitgebreider antwoord op geven, dus dat is helemaal fijn. Dat kan zo dadelijk, na mijn beantwoording.

De **voorzitter**:
Dat moeten we dan onthouden. Gaat u verder.

Staatssecretaris **Van Bruggen**:
Dank. Dan ben ik bij het blokje overig. Dat zijn nog best wat vragen. Dat geeft ook de breedte van het onderwerp aan.

Er was een vraag van de heer Van den Berg over het trainen van AI-systemen. Hij vroeg vooral het volgende. Vindt de staatssecretaris dat AI-functionaliteiten die persoonsgegevens verwerken standaard opt-in moeten zijn, hoe voorkomt ze dat burgers ongemerkt persoonsgegevens afstaan voor training aan AI-systemen en welke concrete eisen stelt hij — "zij" dus, daar hadden we het net al even over — aan transparantie over datagebruik in AI-toepassingen? Zodra gegevens van mensen in AI-systemen zitten, zijn ze er gewoon niet zomaar meer uit te halen. Ik vind het belangrijk dat gebruikers echter wel op de een of andere manier controle over die gegevens houden. Standaard opt-in kan daar zeker aan bijdragen. Ook de toezichthouder, de Autoriteit Persoonsgegevens, is hier alert op. Ze werkt in Europees verband nauw samen om hier goed mee om te gaan. Het is juist mijn gesprek met de autoriteit en mijn werk in Europa om ervoor te zorgen dat men hier alert op is. Zo werken de Europese toezichthouders samen aan het toezicht op de generatieve AI. De eisen aan transparantie over datagebruik in AI-toepassingen zijn hetzelfde als de eisen die de AVG stelt aan alle andere grote verwerkingen. Het concrete toezicht op veel van die grote AI-bedrijven ligt echter bij de Ierse privacytoezichthouder, omdat de Europese hoofdkantoren veelal daar gevestigd zijn. Daar kan de autoriteit dan dus weer niet zo veel aan doen. O ja, er is samenwerking. Dat is inderdaad volledig.

De cyberbeveiligingsvraag van de heer Van den Berg was of de staatssecretaris erkent dat Europese technologie op zichzelf geen garantie biedt tegen datalekken of cyberaanvallen en dat de kwaliteit van de beveiliging uiteindelijk belangrijker is dan de herkomst van de technologie. Ik erken dat Europese technologie op zichzelf staand geen garanties biedt tegen datalekken of voor cyberveiligheid. Wel zorgt de aankomende Cyberbeveiligingswet er wat betreft de kwaliteit van de beveiliging voor dat

de bedrijven en organisaties die onder die wet vallen, wettelijk verplicht zijn om passende maatregelen te nemen en risico's voor de beveiliging van hun netwerk en informatiesystemen te beheersen. Daarbij gaat het ook om de plicht om maatregelen te treffen om incidenten, bijvoorbeeld een cyberaanval, te voorkomen en de gevolgen van aanvallen zo veel mogelijk te beperken. Echter, ook met deze verplichtingen kan ik natuurlijk geen garantie bieden dat bij bedrijven of organisaties die onder de wet vallen, nooit meer een geslaagde cyberaanval zal plaatsvinden. U ziet dat het wel zo zorgvuldig en volledig mogelijk moet worden ingekaderd.

Dan de IT-auditsvraag, ook van den heer Van den Berg. Hij vroeg of de bereidheid tot periodieke onafhankelijke IT-audits voor vitale aanbieders zou kunnen bijdragen aan betere bescherming van persoonsgegevens. Jazeker, periodieke onafhankelijke IT-audits dragen hieraan bij. Een bekend voorbeeld is de ISO-certificering, ISO 27001 om heel specifiek te zijn. Daarbij wordt door een onafhankelijke auditor de beveiliging van de netwerk- en informatiesystemen vastgesteld. Doordat persoonsgegevens in deze netwerk- en informatiesystemen worden verwerkt, wordt er juist ook bijgedragen aan de betere bescherming van de persoonsgegevens.

Dan nog een vraag die niet op mijn terrein ligt. Die ging over de uitvoering van de motie-Tielen. Dat was een vraag van de heer Verkuijlen. Hij vroeg ook of de zorginstellingen wel voldoende voorbereid zijn op grootschalige cyberincidenten. De uitvoering van de motie wordt opgepakt door VWS. In de Kamer wordt er op een later moment informatie gedeeld over de uitvoering van de motie. Als zorginstellingen kwalificeren als essentiële entiteiten of belangrijke entiteiten, vallen ze straks onder de Cyberbeveiligingswet. Dan hebben ze bepaalde verplichtingen, zoals ons allemaal bekend is, zoals de zorgplicht, die bijdraagt aan de voorbereiding op grootschalige cyberincidenten. Maar zoals gezegd komt VWS hier nog op terug.

Dan de vraag van PRO over de massaclaim. Hoe kijkt de staatssecretaris naar het nieuws over Pokémon GO? Ik heb de meest tot de verbeelding sprekende vraag tot het eind bewaard. Wat kan de politiek doen om dit soort gedrag van bedrijven te voorkomen en te bestrijden? Ik heb het nieuws gevolgd en ik heb de procedure met belangstelling gevolgd. Ik heb daarin formeel geen rol. Het toezien op de rechtmatigheid van de gegevensbescherming in de private sector is geen rol van het kabinet of van de regering, maar ook weer van de onafhankelijke toezichthouder. Het is nu aan de rechtspraak. De rechter gaat tot een beoordeling komen, ook in dit geval. Die zal alle feiten en omstandigheden daarin wegen. Het is dus ook niet aan mij om daarop vooruit te lopen. Met die zorg begon ik natuurlijk wel mijn inleiding; als zoiets laagdrempeligs als een Pokémonapp, die eigenlijk alleen maar leuk zou moeten zijn, deze gevolgen kent, deel ik natuurlijk ook gewoon de maatschappelijke zorg, en zeker ook de politieke zorg die hier geuit wordt. Het is afwachten hoe de rechter daarin oordeelt.

Mevrouw **Kathmann** (PRO):
Het is helemaal logisch dat de staatssecretaris geen rol heeft in de rechtszaak, maar de vraag gaat natuurlijk over wat ik net ook al aangaf. Er is gewoon maatschappelijk iets aan de hand. We hebben gewoon een maatschappelijk probleem. Net ging het even over de datahonger. Hier gaat het eigenlijk over de skills die we allemaal missen. Je moet om jezelf veilig te wanen online ongeveer een techexpert zijn om te snappen wat er met je data gebeurt, hoe je dat doet en wat er allemaal van je geroofd wordt; zo kun je het gewoon noemen.

Het is wel een rol van de overheid om iets aan dat maatschappelijke probleem te doen. Dat kan bijvoorbeeld alleen al de inbreng in Brussel zijn over die rigoureuze datatracking, die gewoon gebeurt zodra wij ook maar een app installeren. Zijn we daar keihard aan het lobbyen om te zorgen dat er een heel hard geluid komt om dit tegen te gaan of om wet- en regelgeving aan te scherpen? Dit is namelijk ook een trend waarbij de techniek zo snel gaat dat het roven van data, wat ons allemaal de hele dag overkomt, steeds harder gaat. Kunnen we iets doen aan bewustwording daarvan? Kunnen we iets doen om Nederlanders te ondersteunen in wat ze daar zelf makkelijker aan kunnen doen? Dat is eigenlijk de rol waar ik naar op zoek ben. Ik snap helemaal dat de staatssecretaris zegt: er moet nu ook even een rechter over beslissen en dan hebben we misschien meer gereedschap in handen. Maar ik zou heel graag willen dat we daar meer aan gaan doen.

Staatssecretaris **Van Bruggen**:
Zoals ik net ook zei, is het de eerste keer dat ik het gesprek voer met deze commissie. Ik waardeer uw bevlogenheid en betrokkenheid op dit onderwerp zeer. Ik denk namelijk dat we het allemaal op dezelfde manier ervaren. Zo dadelijk gaat collega Aerdts ook nog wat dieper in op de inzet in Europa. Maar weet dat we op alle mogelijke manieren de zeilen moeten bijzetten. Het is ook aan dit kabinet om dat binnen onze mogelijkheden te doen. Af en toe moeten we natuurlijk ook een beetje de randen daarvan opzoeken, omdat de wereld sneller verandert dan we wellicht in 2018 verwacht hadden. We moeten daarbij dus steeds die stap naar voren blijven zetten. Ook dit betoog is dus zeer herkenbaar. Ik hoop van harte dat de uitspraak van de rechter die handvatten ook weer zal kunnen verrijken voor dit kabinet, zodat de juiste maatregelen getroffen kunnen worden om mensen te beschermen en om organisaties van voldoende kennis te voorzien om hier goed op voorbereid te zijn. Zoals ik al zei, zal collega Aerdts er zo dadelijk ook nog iets over vertellen.

Voorzitter, dank u wel.

De **voorzitter**:
Dank u wel. Dan gaan we nu over naar staatssecretaris Aerdts.

Staatssecretaris **Aerdts**:
Dank u wel, voorzitter. Het internet kenmerkt zich door een vrij en open karakter. Zolang je betaalt voor verbinding, is een groot deel van de wereld online vrij toegankelijk. Maar vrij toegankelijk betekent niet dat het gratis is. Redacties moeten worden betaald, servers moeten draaien en voor de financiering daarvan worden onder andere advertenties ingezet.

Het Rathenau Instituut heeft op verzoek van uw commissie het rapport De prijs van gratis internet geschreven. Het Rathenau Instituut concludeert dat consumenten profiteren van vrij toegankelijke diensten zoals sociale media, zoekmachines en AI, maar dat publieke waarden zoals privacy, autonomie, veiligheid, democratie en de vrije markt onder druk staan. De conclusies en de aanbevelingen uit het rapport zijn helder. Volgens het Rathenau Instituut schiet de naleving van de kaders voor onlinetracking tekort. Ze zien ruimte voor verbetering binnen de bestaande kaders, maar reiken ook alternatieve beleidsrichtingen aan.

Ik herken de risico's van onlinetracking die het Rathenau Instituut schetst. Het is wel belangrijk om daarbij op te merken dat de wettelijke kaders grotendeels in Europees verband zijn vastgelegd. Mijn collega ging er net ook al op in. Onze inzet ziet dus ook voor een aanzienlijk deel op Europese beïnvloeding op dit terrein. De Nederlandse inzet is daarbij het verbeteren van de privacypositie van burgers, bijvoorbeeld door effectievere handhaving en het stroomlijnen van cookie- en trackingregelgeving. Over de ontwikkelingen rondom het beleid ten aanzien van online tracking zal ik uw Kamer uiteraard informeren. Ik hoor ook graag — dat zijn we vandaag volgens mij met elkaar aan het uitwisselen — wat uw perspectief hierop is, zodat we ook gezamenlijk kunnen werken aan het tegengaan van de risico's.

Het CDA had ook nog een vraag over dit rapport. Daarop wil ik eerst even ingaan. Dan heb ik drie onderwerpen: bescherming minderjarigen online en privacy, de ID-wallets en een overig of algemeen setje.

Ik ga op de vraag van mevrouw Zwinkels in. Het Rathenau Instituut laat zien dat internet vaak helemaal niet gratis is. Ze vraagt of ik het met het CDA eens ben dat het huidige systeem van online tracking te veel uitgaat van doorklikken en toestemming en te weinig van echte bescherming. Ik herken de risico's van online tracking die het Rathenau Instituut schetst. Onlineadvertenties hebben ook voordelen, zoals het gratis toegankelijk zijn van veel websites, apps en diensten, maar ik vind het belangrijk dat mensen, en zeker ook kinderen en jongeren, hierbij effectief beschermd worden. Daarom zetten we ons ook in Europees verband in om de privacypositie van burgers te verbeteren. Dat doen we bijvoorbeeld met die effectievere handhaving en het stroomlijnen van de regels. Dit doen we op dit moment in de huidige onderhandelingen rond het Omnibuspakket. U heeft daarvan het BNC-fiche. Ik kan over onze exacte onderhandelingspositie op dit moment niet heel veel zeggen, maar onze inzet bestaat uit de uitgangspunten die in het BNC-fiche staan. Over de voortgang van de onderhandelingen wordt u ook volgens de informatieafspraken door ons geïnformeerd.

Aangaande de onlinebescherming van minderjarigen en hun privacy vroeg het CDA hoe die online tracking nou verder kan worden teruggedrongen, juist ook omdat kinderen geen verdienmodel mogen zijn. Binnen de huidige wetgeving bieden bijvoorbeeld op dit moment de AVG, waarover mijn collega sprak, maar ook de DSA, bescherming aan minderjarigen tegen online tracking. Op grond van artikel 28, lid 3 van de DSA mogen gegevens van minderjarigen niet worden gebruikt om hen te profileren en gericht advertenties te tonen. Momenteel lopen er vanuit de Europese Commissie, als de toezichthouder op dit terrein, verschillende onderzoeken, ook naar de onlinebescherming van minderjarigen. We volgen die onderzoeken natuurlijk op de voet.

Een andere vraag van het CDA ging over die privacyvriendelijke alternatieven, zoals contextueel adverteren, waarbij de advertenties worden gebaseerd op de inhoud van de pagina en niet op de persoon die op de pagina aan het kijken is. In Europa is mijn inzet voornamelijk het versterken van de privacypositie van burgers. Ik zet mij daar dan ook in voor de versterking van dit model, maar ook met specifieke aandacht voor de alternatieven zoals dit contextueel adverteren. Dat doen we onder andere in de onderhandelingen over de wijziging van de e-Privacyrichtlijn en de AVG in het kader van dat Omnibustraject, waarover ik net al eventjes sprak.

Ik ga naar de volgende vraag. PRO en het CDA hadden de vraag gesteld of het kabinet

het ermee eens is dat we naar een internet zonder trackingcookies moeten gaan. Ik herken de problemen rondom onlinetracking zoals die in het rapport naar voren komen, ook als het gaat om consentmoeheid, het maar doorklikken zonder echt te kijken waar je naartoe gaat, het gebruik van dark patterns en natuurlijk hele ingewikkelde gebruikersvoorwaarden met zo veel pagina's dat het eigenlijk niet realistisch is dat iedereen het snapt en helemaal leest. De beleidsrichtingen die door het Rathenau Instituut worden omschreven, hebben voor- en nadelen. Twee van die drie richtingen vragen in feite om een verbod of beperking van gepersonaliseerde advertenties. Een totaalverbod daarop is wel echt heel ingrijpend. Tegelijkertijd zijn die wettelijke kaders ook grotendeels in Europees verband vastgelegd. Daarom is alleen de beleidsoptie om het huidige systeem te verbeteren op dit moment realistisch, maar we nemen dit natuurlijk wel mee naar Brussel, ook als het gaat om die evaluatie en als het dus niet blijkt te werken. Ik wil daarin ook echt wel heel graag de Omnibuswetgeving afwachten, om daarna te kijken of het werkt. Als het inderdaad niet blijkt te werken, dan nemen we dat natuurlijk mee, zowel in de evaluatie, als in onze inzet die daarna zal komen. De inzet is natuurlijk altijd het versterken van de rechten van burgers binnen de verschillende systemen. Ik heb dit verhaal over de Omnibuswetgeving volgens mij net al uitgebreid aan u verteld.

Mevrouw **Zwinkels** (CDA):
Dank aan de staatssecretaris. Het is goed om te horen dat dit wordt herkend en dat ze het ook met ons eens is dat we hierop in moeten zetten, ook in Europa. Ik ben wel benieuwd naar de verbeteringen die wel zouden kunnen. Kan de staatssecretaris uitleggen wat we daarvan de komende tijd vanuit het kabinet kunnen verwachten?

Staatssecretaris **Aerdts**:
Daar moet ik even op terugkomen in de tweede termijn.

Mevrouw **Zwinkels** (CDA):
Dat is goed.

Mevrouw **Kathmann** (PRO):
In het vervolg daarop — ik hoop dat dat in de tweede termijn kan worden meegenomen — ben ik op zoek naar wat meer concreets. De staatssecretaris gaf aan dat ze de Kamer daar best over wil informeren. Dat is superfijn, maar het zou ook fijn zijn als we dan bijvoorbeeld na de zomer ook echt even een brief krijgen over wat we wel of niet kunnen of wat onze inzet wordt. We kunnen namelijk kijken of het niet werkt, maar we weten eigenlijk dat het nu niet werkt. Er is een massaclaim, omdat er data van 8,6 miljoen Nederlanders zijn gejat. Hier zitten 1,5 miljoen kinderen tussen, 1,5 miljoen Nederlandse kinderen! Dan is er nog het Pokémon GO-voorbeeld van net. We moeten gewoon keihard aan de bak. Nogmaals, dat zit 'm ook in het beter handhaven van de wet- en regelgeving, bewustwording en noem het maar op. Ik zou heel graag wat concreter van het kabinet willen horen, bijvoorbeeld na de zomer, wat we nou wel en niet kunnen, wat onze inzet in Brussel is en wat we nog moeten afwachten, zodat we iets beter weten wat we nou wel en niet gaan doen en wanneer er bepaalde momenten zijn dat we weer kunnen evalueren of harder kunnen ingrijpen.

Staatssecretaris **Aerdts**:
Op dit moment loopt dat Omnibustraject, waarin juist ook deels deze wet- en regelgeving wordt aangepast. Volgens mij is nu de verwachting dat er eind juni, dus komende week

ergens, een akkoord op komt en dan gaat dat geïmplementeerd worden. Sowieso zullen wij de Kamer volgens de informatieafspraken daarover informeren. Daarbij zal ik inderdaad ook wel even meenemen wat er nou concreet op het gebied van die trackingcookies is meegenomen. Vervolgens wil ik dat wel afwachten, voordat ik allerlei nieuwe maatregelen toe ga zeggen. Die Omnibuswetgeving moet ook wel even zijn werk kunnen doen, voordat ik weer extra dingen ga toepassen of extra inzet ga plegen. We zullen u informeren over de uitkomsten van de Omnibusonderhandelingen. Als u dat onvoldoende vindt, ga ik daarna natuurlijk heel graag met u in gesprek over het vervolg.

Voorzitter. Dan kom ik bij de vragen over de wallets. Mevrouw El Boujdaini stelde een vraag over de actuele stand van zaken rondom de ID-wallets. We werken aan de ontwikkeling van het stelsel Europese Digitale Identiteit, het EDI-stelsel, en de publieke wallet. We wachten daarbij ook nog op een aantal specifieke richtlijnen over hoe die eruit moet gaan zien en wat de specifieke technische vereisten van die wallets zijn vanuit de Europese Commissie. Dat is dus het eerste waarop we nog wachten. We streven ernaar om eind 2026 een uitvoeringswet in consultatie te brengen. Na parlementaire behandeling kunnen de wet, en dus ook het stelsel, in werking treden.

Voorzitter. Mevrouw El Boujdaini sprak ook over het initiatief ID010, dat we nu zien. Ik kijk heel positief aan tegen dat initiatief. Voor de maatschappelijke meerwaarde en de werking van het EDI-stelsel als geheel is het nodig dat partijen met verschillende use cases meedoen. Rotterdam is een van hen. Zo zorgen we er ook voor dat er gegevens in de wallets komen en dat die ook onderdeel uit gaan maken van het dagelijks proces, waarvan mensen dus gebruik kunnen maken. Al deze initiatieven moeten gecertificeerd worden om binnen dat stelsel te kunnen functioneren. Dat gebeurt op basis van de criteria waarop we nu nog wachten, maar we volgen dit initiatief op de voet en met heel veel interesse.

Dan kom ik bij mijn laatste setje met nog een aantal overige vragen. Ik pak even de laatste details erbij. Het gaat nog over de AP en het AI-toezicht. Daarop zou ik nog even terugkomen. Mijn collega heeft er al het een en ander over gezegd. De AP heeft sinds een aantal jaar de coördinerende rol in het toezicht op algoritmen en AI. Die heeft vanuit de opdracht een hele proactieve houding naar het veld. Ik vind het belangrijk dat dit wordt voortgezet als de AP de toezichthouder wordt op de AI-verordening. Daar zitten we nu namelijk zo'n beetje. Ze doen nu al algoritmes. Er komen straks met de implementatie van de AI-verordening nog taken bij. We hebben uw Kamer daarover ook een brief gestuurd. Hieruit blijkt dat de RDI, de Rijksinspectie Digitale Infrastructuur, en de AP de leidende toezichthouders zijn, maar dat een deel van het AI-toezicht ook bij de bestaande toezichthouders zal zitten. Denk aan speelgoed en gasinstallaties bij de NVWA, liften en drukapparaten bij de NLA et cetera. Daar wordt dus naar gekeken. De internetconsultatie is recentelijk afgerond. Deze week is ook de uitvoerings- en handhaafbaarheidstoets van de AP ontvangen. Daar moeten we als kabinet echt nog naar kijken voordat ik u daar meer over kan zeggen. We streven ernaar dat we de uitvoeringswet van de AI-verordening later dit jaar aan de Raad van State sturen. Daarover zullen we dan nog uitgebreid met uw Kamer in gesprek gaan.

Dan had ik nog de vraag van de VVD over de gesprekken die we met de Amerikaanse ambassadeur hebben gevoerd over Meta en Microsoft. Ik ga ervan uit dat u doelt op het bericht dat Microsoft de namen van Nederlandse ambtenaren aan de Amerikaanse overheid heeft verstrekt. Daar kan ik op zeggen dat we begrepen hebben dat Microsoft

die informatie heeft verstrekt. Het gaat om informatie die verstrekt is om opvolging te geven aan een overheidsbevel, zoals wij het hebben begrepen. Deze informatie is vervolgens deels terechtgekomen in een rapport van het Huis van Afgevaardigden. Daarbij zijn namen van individuele medewerkers van toezichthouders, zoals de ACM, ten onrechte niet altijd weggelakt. Er is via verschillende kanalen contact geweest met de Amerikaanse vertegenwoordigers over de publicatie van deze namen. In die contacten heeft het kabinet zijn zienswijze op de casus uitgedragen. Wanneer er een dispuut is over beleid of regelgeving, moet de discussie daarover via politici en beleidsmakers gevoerd worden. Toezichthouders en natuurlijke personen moeten als uitvoerders van dat beleid nooit onder druk gezet kunnen worden. De inzet van het kabinet is en blijft dat toezichthouders en ngo's hun wettelijke en maatschappelijke taak zonder belemmering kunnen uitvoeren. Conform de Kamerbrief die gisteren door mijn collega, de staatssecretaris van BZK, is verstuurd, gaat hij hierover ook verder in gesprek met de Amerikaanse ambassadeur.

Dan was er nog de vraag, ook van de VVD, hoe het staat met de EU en Nederlandse alternatieven. In de Agenda Digitale Open Strategische Autonomie zet het kabinet in op tien prioriteiten die vanuit het geopolitieke en geo-economische perspectief het meest cruciaal zijn, bijvoorbeeld cloud en AI. Hiertoe zet het kabinet in op het versterken van het concurrentievermogen van de digitale sector door onder andere de realisatie van de AI-fabriek in Groningen. Als beschermende maatregel is de investeringstoets om ongewenste technologieoverdracht te voorkomen uit de Wet vifo een van de middelen die kan worden ingezet. Ook kijkt het kabinet naar maatregelen voor het verdiepen van internationale samenwerking, bijvoorbeeld door het sluiten van vrijhandelsverdragen. Bovendien zet het kabinet onder meer via de Nederlandse Digitaliseringsstrategie in op het versterken van de digitale autonomie van de overheid, bijvoorbeeld via de inzet op opensourcealternatieven en het digitalcommonssysteem. We hebben net ook het European Tech Sovereignty Package gezien, dat nu geappreciëerd wordt en dat daarna met uw Kamer in een BNC-fiche wordt gedeeld. Ik heb de afgelopen maanden ook gezien dat bedrijven hier zelf heel erg actief in zijn. We hebben een initiatief rond cloud gezien waarbij ze samen optrekken. Ik ben ook heel blij dat die open source nadrukkelijk in het Tech Sovereignty Package terechtgekomen is, juist ook om het makkelijker te maken om het aanbod te vergroten, ook voor bedrijven. Hierdoor kunnen we weer onze eigen keuzes maken.

Dan heb ik een laatste vraag over de telecombedrijven, van de heer Van den Berg van JA21. Hij vroeg waarom er voor de telecombedrijven andere regels gelden dan in de financiële sector. Telecombedrijven hebben ook strenge wet- en regelgeving. De Telecommunicatiewet kent een algemene zorg- en meldplicht om veiligheid en integriteit van telecomnetwerken en -diensten te borgen. Onder de zorgplicht dienen de aanbieders passende technische en organisatorische maatregelen te nemen om risico's voor de beveiliging van hun netwerken en diensten te beheersen. Via het Besluit veiligheid en integriteit telecommunicatie en de Regeling veiligheid en integriteit telecommunicatie is die zorgplicht met enkele specifieke vereisten nog nader aangescherpt. Ook in dit domein is de RDI de toezichthouder.

Daarmee ben ik aan het einde gekomen van mijn beantwoording.

De heer **Verkuijlen** (VVD):
Dank voor de uitvoerige beantwoording. Never waste a good crisis, zou ik zeggen. Dat

bedrijven hier instappen, lijkt me heel logisch. Maar ik had nog één vraag, namelijk over die nieuwe technologieën waarbij je eigenlijk versnipperd met data omgaat. Ik weet niet of u die al geraakt heeft bij de ID-wallet? Het ging daarbij over zero-knowledgetechnologie. Welke staatssecretaris gaat daarover? Staatssecretaris Van der Burg? Oké, dan past mij zwijgen. Dan wacht ik op zijn termijn.

De **voorzitter**:
Dan wordt het hoog tijd … O, wacht even. Mevrouw El Boujdaini heeft nog een vraag.

Mevrouw **El Boujdaini** (D66):
Ik was nog wel even benieuwd naar het volgende. De staatssecretaris had het over de richtlijnen voor de ID-wallets die nog zouden komen, en dat er daarna eigenlijk pas echt aan de slag gegaan kan worden. Zou de use case die Rotterdam graag wil uitvoeren, daarop moeten wachten? Ik denk dat we dan best wel laat zijn, want het zou op zich best wel goed zijn als we kunnen leren van wat daar gebeurt. Daarom mijn vraag aan de staatssecretaris: wanneer zouden die richtlijnen dan komen? Is er een mogelijkheid om daarvoor al wel aan de slag te gaan in een beschermde omgeving?

Staatssecretaris **Aerdts**:
Ik moet hier even in tweede termijn op terugkomen om te bekijken wat precies de laatste stand van zaken is. Overall is natuurlijk het testen … Er zijn ook pilots geweest vanuit het Rijk, de overheid, om die omgeving te testen, maar voordat die wallets echt in werking kunnen treden, moeten ze aan een aantal specificaties voldoen, en die hebben we nog niet. Ik ga even kijken of ik daar qua data meer over te weten kan komen, en dan kom ik er graag op terug in de tweede termijn.

De heer **Van den Berg** (JA21):
Allereerst is het fijn dat de staatssecretaris de zorgen over de trackingcookies begrijpt. Maar nou is het juist wel heel vervelend dat bij diezelfde overheid — daar heb ik ook Kamervragen over ingediend — bleek dat gegevens vanuit het Belastingdienstportaal worden doorgestuurd naar Adobe in de Verenigde Staten. Die Kamervragen zijn trouwens nog niet beantwoord, ondanks dat de termijn is verstreken. Ik vraag daar dus aandacht voor. Nou speelt dat ook bij werkenbijdefensie.nl en bij VeVa, Veiligheid & Vakmanschap. Daar worden gegevens van mensen die die cookieverklaring weigeren, door onze eigen overheid doorgestuurd naar Adobe en Google, zonder dat ze daar toestemming voor hebben gegeven. Ik wil deze staatssecretaris vragen om dat zo snel mogelijk op te pakken met de staatssecretaris van Defensie; wat is precies de oorzaak ervan dat dit bij onze eigen overheid net zo goed voorkomt?

Staatssecretaris **Aerdts**:
Die vragen worden zo snel mogelijk beantwoord. Ik verwacht de antwoorden nog voor het zomerreces met u te kunnen delen. Ik kom graag in de tweede termijn eventjes terug op deze specifieke voorbeelden.

De **voorzitter**:
Da gaan we nu luisteren naar de heer Van der Burg, staatssecretaris BZK.

Staatssecretaris **Van der Burg**:
Voorzitter, ik vraag me af of we wel om 14.00 uur klaar zijn. Want nu ga ik even helemaal los. Nee hoor, ik heb nog twee vragen over. De ene was van de VVD over de

zero-knowledgetechnologieën. Ja, daar moeten we zeker naar kijken. Zeker in het kader van dataminimalisatie is het juist heel erg goed dat niet de data worden gedeeld maar er een signaal wordt afgegeven, dus dat je niet de broninformatie krijgt maar wel een signaal. Denk bijvoorbeeld aan leeftijd. Dan kunnen we inderdaad zeggen: de heer Verkuijlen is boven de 18, en daarmee kan hij bij Gall & Gall zijn fles wijn bestellen, zonder dat we alle andere gegevens van de heer Verkuijlen delen. Dat geldt natuurlijk ook voor de overheid. Een mooi voorbeeld dat ik in het verleden heb genoemd, en dat hieraan raakt, is niet zozeer de encryptievariant, maar het feit dat de Sociale Verzekeringsbank nu gewoon een signaaltje krijgt van het SIS, zonder dat ze als het om een dubbele uitkering gaat meteen alle medische gegevens krijgen. Dan heb je ook nog de encryptievariant. Dus ja, dit kan zeker helpen. We moeten ons overigens natuurlijk niet rijk rekenen. Het is een onderdeeltje van het gehele complex om ervoor te zorgen dat we aan dataminimalisatie doen en datalekken beperken. Maar hoe minder data je deelt, en hoe minder data er dus bij verschillende partijen is, hoe kleiner de kans dat die data gedeeld wordt. Dat is dus een terechte vraag van de heer Verkuijlen.

Tot slot alweer, voorzitter — zo snel kan het gaan — de vraag van het CDA. Mevrouw Zwinkels vroeg specifiek hoe het zat met overheidsorganisaties en de toegang tot gegevens en of die periodiek worden opgeschoond. Sorry, het CDA had meerdere vragen op dat punt. De overheid heeft natuurlijk een voorbeeldfunctie te vervullen. Uit de Algemene verordening gegevensbescherming blijken ook een aantal concrete normen. Eén. Persoonsgegevens dienen natuurlijk alleen verwerkt te worden op het moment dat het gaat om specifieke, welbepaalde doelen. Dat beperkt al de kring van medewerkers die er gebruik van mogen maken. De AVG, waar u het net over heeft gehad met mijn collega, heeft ook nog een aantal technische en organisatorische maatregelen getroffen om gegevens te beveiligen. Daarnaast moeten ze inderdaad periodiek worden opgeschoond. Dat betekent dat gegevens minimaal één keer per jaar moeten worden opgeschoond. Daar zeg ik nog bij: als het specifiek om de departementen gaat, dan is de Chief Information Security Officer verantwoordelijk voor het controleren of die toegangsrechten ook inderdaad worden en zijn opgeschoond.

Mevrouw **Zwinkels** (CDA):
U kunt de vraag misschien al wel voelen aankomen. Ik ben natuurlijk heel erg blij dat deze norm er ligt, dat we dat op die manier ook organisatorisch hebben ingericht en dat het aan specifieke doelen gekoppeld is. Dat is heel goed, maar dan ben ik natuurlijk benieuwd in hoeverre het ook de praktijk is. Wordt het ook nageleefd? En hoe gaat de staatssecretaris er vanuit zijn rol voor zorgen dat dit ook daadwerkelijk verbetert?

Staatssecretaris **Van der Burg**:
Het is de taak van de CISO's bij de verschillende departementen om dat in de gaten te houden. De CISO's hebben ook een gezamenlijk CISO-beraad. Daarnaast heb ik de verantwoordelijkheid rijksbreed, en op het moment dat mij signalen bereiken dat dingen niet gebeuren, kan ik zowel via de rijks-CIO als via de CISO van BZK daar actie op ondernemen.

De heer **Van den Berg** (JA21):
Mijn laatste interruptie heb ik natuurlijk voor staatssecretaris Van der Burg bewaard. Ook aan deze staatssecretaris de vraag hoe het nou zit met dat Odido-lek, want ik zei net al tegen staatssecretaris Van Bruggen dat er tussen die data — ik zal het beperkt houden om het niet ingewikkelder te maken — gevoelige data van onze inlichtingendiensten

zitten. Dan valt het onder uw verantwoordelijkheid. Worden daar wel maatregelen voor genomen en zijn de signalen ook bekend dat daar zaken zijn gelekt die ons niet zo heel goed zouden uitkomen?

Staatssecretaris **Van der Burg**:
De heer Van den Berg dicht mij iets toe wat in dit geval niet helemaal juist is. Als het gaat om de diensten mag de staatssecretaris van BZK daarin geen rol spelen. Dat ligt bij de minister. Dat is ook het enige onderdeel waarin ik hem niet vervang. Op het moment dat de minister niet aanwezig is — hetzelfde geldt overigens voor de staatssecretaris van Justitie als het gaat om de minister van Justitie — dan vervangen de ministers van Justitie, Defensie en Binnenlandse Zaken elkaar. Op alle andere punten vervang ik de minister van BZK en kan ook de staatssecretaris van Justitie de minister van Justitie vervangen, maar nou net niet als het om de diensten gaat. Dus helaas moet ik hierin erg terughoudend zijn. Ik weet het simpelweg niet.

De **voorzitter**:
Dat is in ieder geval een duidelijke beantwoording.

Staatssecretaris **Van der Burg**:
En verder uitermate dank, zowel aan mevrouw Zwinkels als aan de heer Van den Berg voor het stellen van een vraag aan mij, waardoor ik toch het gevoel heb dat ik van nut ben geweest vandaag.

De **voorzitter**:
Daarmee is de termijn van het kabinet beëindigd. Is er behoefte aan een tweede termijn? Ik stel vast dat dat zo is. Er wordt gevraagd om voorafgaand aan de tweede termijn kort te schorsen. Ik schors de vergadering voor tien minuten.

De vergadering wordt van 12.37 uur tot 12.46 uur geschorst.

De **voorzitter**:
Ik heropen de vergadering. Wij zijn toe aan de tweede termijn van de Kamer. Het woord is aan de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):
Dank, voorzitter. Ook dank aan het kabinet voor de beantwoording van alle gestelde vragen. Ik vind het in ieder geval fijn om te constateren dat er een brede consensus leeft dat het niet per se gaat om de nationaliteit van bedrijven, maar dat de cyberbeveiliging van die bedrijven echt vooropstaat. Dat doet JA21 deugd. Ik heb nog wel een laatste oproep aan de staatssecretaris. Ik wil haar vragen of zij bijvoorbeeld een handelingskader kan opstellen voor de Rijksoverheid, dus over alle departementen heen. Dat kan de handelingsverlegenheid binnen de overheid wellicht wat verminderen. Dat is dus eigenlijk een extra duiding voor de onduidelijkheid in de AVG.

De staatssecretaris heeft gezegd dat zij zich in Europa hard wil maken voor die opt-in in plaats van de opt-out voor data in AI. Kan zij dat verder concretiseren, bijvoorbeeld met een brief over de inzet, waarin dan staat hoe we dat dan gaan doen en waar we dat in gaan verwerken? Ik denk dat dat prima zo kan; ik denk dat ik daar helemaal geen motie voor hoef in te dienen.

Afrondend, voorzitter. Ik hou echt mijn zorgen over onze eigen overheid. Ik zou eigenlijk het hele kabinet willen oproepen om ook echt naar de eigen websites te kijken: hoe gaan wij nou met data om? Ik gaf zojuist het voorbeeld van de Belastingdienst, waar gegevens worden doorgestuurd, en nota bene van Werken bij Defensie. Het is ontzettend gevoelig als dat soort informatie, bijvoorbeeld wie daar solliciteert, bij buitenlandse statelijke actoren komt.

Laat ik daarmee afronden. Dank u wel.

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan de heer Verkuijlen van de VVD.

De heer **Verkuijlen** (VVD):
Dank u wel, voorzitter. Ik wil in ieder geval alle drie de staatssecretarissen danken voor een mooi inhoudelijk debat. Ik had graag nog meer gehoord van de heer Van der Burg, maar dat was hem niet gegeven.

We moeten meer inzetten op de voorkant; dat heeft mevrouw Kathmann ook met zoveel woorden gezegd. Die beveiliging is echt heel belangrijk. Dat gezegd hebbende is het ook geen moment te laat. Met technologieën die eraan komen, zoals kwantum en Mythos, moeten we hier echt heel snel mee aan de slag, juist in het belang van ieders persoonsgegevens.

Ik ben zeer content met het handelingskader. Nogmaals dank daarvoor, maar het moet nog wel meer bekendheid krijgen. Het mag niet blijven bij een brief; het moet ook nog meer uitgedragen worden. Ik hoor graag nog even op welke wijze we dit meer bekend gaan maken.

De staatssecretaris van Justitie en Veiligheid zag mij inderdaad wat terughoudend reageren op haar opmerking dat je niet moet betalen als je met ransomsoftware te maken krijgt. Ik laat mij op dit punt graag verbeteren, maar mij zijn geen lopende ransomzaken bekend waarin de partij die gijzelde, tussentijds werd aangepakt, opgespoord of gevonden. Het is heel goed dat we die daders op termijn gaan vinden, maar kan de staatssecretaris zich voorstellen dat zo'n bedrijf zegt: vanuit mijn bedrijfscontinuïteit kan ik het me niet permitteren om helemaal stilgelegd te worden en ga ik toch over tot betalen? Ik snap de onwenselijkheid daarvan, maar dit is wel de realiteit. Het internet is niet alleen maar vrijheid; het is in dit opzicht ook vogelvrijheid. Dat is wel een zorg die ik namens de VVD nogmaals op tafel wil leggen.

De **voorzitter**:
Dank u wel. Dan is het woord aan mevrouw El Boujdaini van D66. Sorry, een hele korte vraag tussendoor van de heer Van den Berg.

De heer **Van den Berg** (JA21):
Ja, heel kort, verduidelijkend. Is de VVD dan niet van mening dat we juist veel meer moeten inzetten op een soort cyberoffensief vanuit het principe "if you mess with us, we mess with you" en dus ook een afschrikwekkende werking moeten gaan toepassen?

De heer **Verkuijlen** (VVD):
Het valt niet onder de staatssecretaris Slagvaardige Overheid. Als u mij zou vragen of ik

bereid ben om heel veel geld te spenderen aan de opsporing, denk ik dat ik dat niet snel zou doen en dat ik meer zou investeren aan de voorkant om te zorgen dat die beveiliging sneller op orde komt. Ik vind met de heer Van den Berg en JA21 nog steeds dat we een slagvaardige opsporing altijd zo veel mogelijk inhoud moeten geven, maar het mag nooit zo zijn dat je daarop leegloopt.

De **voorzitter**:
Dank u wel. Nu is het woord echt aan mevrouw El Boujdaini van D66.

Mevrouw **El Boujdaini** (D66):
Dank u wel. Ik wil de staatssecretarissen ook graag bedanken voor hun beantwoording. Zoals ik al zei in mijn betoog, denkt mijn fractie echt dat er heel veel potentie zit in de ID-wallets om juist aan de preventieve kant te zitten en zo veel mogelijk persoonsgegevens veilig te houden omdat we die niet meer overal rondstrooien voor het afsluiten van allerlei abonnementen. We kunnen door de inzet daarvan dus echt werk maken van meer veiligheid en privacy.

Ik wil heel even terugkomen op de bewaartermijnen met betrekking tot de AVG, want in de AVG staat inderdaad niet duidelijk wat de precieze richtlijnen zijn voor de verwijdertermijnen, bijvoorbeeld voor persoonsgegevens. Dat zorgt echt voor heel veel onduidelijkheid bij organisaties en bedrijven. De AP zegt dit zelf ook en heeft dit ook aangegeven in het rondetafelgesprek dat we met de AP hebben gehad. Iets van richtlijnen, bandbreedtes of rode draden zouden daarbij echt heel erg helpen. Ik wil de staatssecretaris dus vragen om hier wellicht met enige creativiteit samen met de AP naar te kijken en hier het gesprek over te voeren, juist omdat de AVG ook alweer tien jaar in werking is. Dit zou dus echt heel mooi aansluiten bij kijken naar wat wél werkt en wat beter kan.

Dan wil ik ook nog even terugkomen op de samenwerking tussen de AP en de politie. Dat is dus juist de opsporingskant, hoe je goed toezicht houdt en handhaaft. Het is superbelangrijk om dit goed met elkaar te stroomlijnen. Ik heb signalen gekregen dat het heel waardevol zou zijn om wél te kijken hoe die samenwerking nu gaat en waar die versterkt kan worden. Juist van de grotere datalekken die we nu hebben, zouden we veel meer kunnen leren om dit aan de toezichts- en handhavingskant te kunnen voorkomen, maar ook om de datadieven op te sporen. Ik zou de staatssecretaris dus ook willen vragen hoe zij ertegenover staat om dit gesprek aan te gaan en in kaart te brengen hoe deze samenwerking nu gaat.

Dat was 'm.

De **voorzitter**:
Veel dank. Mevrouw Zwinkels van het CDA.

Mevrouw **Zwinkels** (CDA):
Dank u wel, voorzitter. Dank ook aan de drie staatssecretarissen. Erg fijn om te horen dat we extra middelen gaan uittrekken voor de Autoriteit Persoonsgegevens, gekoppeld aan de taken rondom de AI-verordening. Fijn dat er wordt gekeken naar het handelingskader en de bewaartermijnen en dat aan de voorkant aan bedrijven en organisaties wordt meegegeven dat er sprake is van een handhavend kader. Fijn dat er een landelijke standaard gaat komen voor het bieden van hulp van slachtoffers van

grote datalekken. Blij met de toezegging van staatssecretaris Aerdts dat er een duidelijke inzet is in Europa op de door mij aangeleverde punten bij tracking, ook voor kinderen, met hoe dat is geregeld in de DSA, met het volgen van de onderzoeken daarnaar van de Europese Commissie en ook met het contextueel adverteren, waar we later vast nog met elkaar over komen te spreken. Ook dank aan de heer Van der Burg voor de invulling van de toegang tot data binnen de overheid, want dat is inderdaad een belangrijke voorbeeldfunctie.

Ik heb voor nu nog één openstaande vraag, over het onderzoek van het Rathenau Instituut, namelijk hoe de uit de aanbevelingen van het Rathenau Instituut volgende verbeteringen kunnen worden doorgevoerd.

Dank allen voor het debat. Ik denk dat het belangrijk is dat we dit debat hebben gevoerd, ook voor het extra bewustzijn in de samenleving bij bedrijven en bij de overheid.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan geef ik nu het woord aan mevrouw Kathmann van PRO.

Mevrouw **Kathmann** (PRO):
Dank, voorzitter. Ik wil de staatssecretarissen bedanken voor de beantwoording. Ik merk echt dat we allemaal op een zoektocht zijn: wat kunnen we nou nog meer doen? Ik hoop wel dat die zoektocht straks in de tweede termijn iets concreter wordt gemaakt, ook in de reactie op al die goede dingen die het Rathenau Instituut heeft gezegd: wat kunnen we nou wel, wat kunnen we nou niet, hoe kunnen we ons Europees uiten zodat het daar misschien nog wat steviger wordt? Maar het begint gewoon bij het beschermen van mensen, want we hebben het vandaag over het beschermen van persoonsgegevens en over grote datalekken. Dat doen we met wet- en regelgeving, maar dat moeten we eigenlijk met veel meer doen, omdat het over miljoenen Nederlanders gaat. Daarom heb ik eerder gepleit voor dat basispakket digitale veiligheid. Daar heb ik ook een motie voor ingediend. Daar zitten niet alleen een soort VPN, wachtwoordmanager, adblockers en antivirus in — want daar begint het beschermen van persoonsgegevens ook mee — maar ook informatie over hoe je ervoor zorgt dat niet de hele tijd, zonder dat je het weet, je data worden geroofd zodra je ook maar iets op je telefoontje zet of daarmee bezig bent. Ik zou toch nog een keer aan het kabinet willen vragen: hoe kunnen we nou tot zo'n basispakket digitale veiligheid komen? Dat pakket moet dus niet alleen gaan over bewustwording, maar ook over concrete handvatten. En op welke manier kan het kabinet hierbij een rol spelen? Bij VPN en wachtwoordmanagers moet je dat uiteraard in gesprek en samen met de markt doen, maar het zou heel fijn zijn als er in ieder geval een rol gepakt kan worden.

De **voorzitter**:
Dank u wel. Dan zijn we hiermee aan het einde gekomen van de tweede termijn van de Kamer. Ik kijk even naar rechts om te zien of de staatssecretaris behoefte heeft aan een schorsing. De staatssecretaris geeft aan dat het zonder kan en daarom geef ik haar nu graag het woord.

Staatssecretaris **Van Bruggen**:
Voorzitter, dank u wel. JA21 heeft gevraagd naar een handelingskader over de

departementen heen. Deze vraag zal door collega Van der Burg worden beantwoord, zo begreep ik.

De vraag over de opt-in zal door mevrouw Aerdts beantwoord worden.

De vraag van de heer Verkuijlen over het handelingskader en de communicatie neem ik graag zelf mee. Deze vraag ligt eigenlijk in het verlengde van de vraag van mevrouw Zwinkels of we nog eens heel goed naar het handelingskader en de naleving van de bewaartermijnen kunnen kijken. Het is niet meteen onze eerste rol, maar welke verantwoordelijkheid kan de Rijksoverheid daar toch nemen? Ik wil zeker onderzoeken hoe we dat beter of in ieder geval zo goed mogelijk kunnen doen.

Ik kom op de vraag over de ransomware. Ik begrijp heel goed de zorgen die u daarover uit. Ik kan me het heel goed voorstellen, al was het maar omdat ik ook een leven als bestuurder van een grote zorgorganisatie had voordat ik staatssecretaris werd, want dan heb je doorlopend deze zorg. En wat doe je dan op het moment dat deze vraag aan je wordt voorgelegd? Mijn antwoord blijft: betaal geen losgeld. Daar ben ik heel eerlijk over, maar ik begrijp ongelofelijk goed dat het voor grote scholengemeenschappen en zorgorganisaties die in deze situatie terechtkomen, ontzettend ingewikkeld is om de juiste besluiten te nemen.

Wat kan de Rijksoverheid doen om hen te ondersteunen, zodat ze de goede besluiten nemen? Hopelijk heb ik daar in het debat voldoende handvatten voor gegeven. Ik denk namelijk dat we die kwetsbaarheid op alle mogelijke manieren herkennen.

De heer **Verkuijlen** (VVD):
Dank voor dat antwoord. Ik kan de lijn van de staatssecretaris volgen, maar ze zal zeker vanuit haar oude rollen het gevoel van onmacht herkennen. Ze herkent vast het gevoel dat de overheid je op dat moment niet kan bijstaan en dat je eigenlijk overgeleverd bent aan de willekeur van de mensen die je onder druk zetten. Dat aspect wil ik nog wel even raken, want dat is namelijk wel de consequentie als je zegt "we gaan niet betalen".

De **voorzitter**:
U vervolgt uw betoog.

Staatssecretaris **Van Bruggen**:
Waarvan akte, zou ik willen zeggen, maar alle begrip voor deze vraag.

Voorzitter. Ik kom op de vraag van D66 of er richtsnoeren denkbaar zijn voor de bewaartermijnen AVG. Wanneer kun je die persoonsgegevens verwijderen? De Autoriteit Persoonsgegevens kan die bandbreedte zelf aanleggen. Sterker nog, dat is haar verantwoordelijkheid. Als zij daar een zorg over uit, dan heeft ze zelf de tools in handen om daar duidelijk over te zijn. Ik denk ook dat dat een mooie kans voor haar is.

De tweede vraag van D66 ging over toezicht en handhaving. Kan ik in kaart brengen hoe die samenwerking precies gaat? Dat kan ik doen en dat wil ik ook best doen. Dat is bij dezen een toezegging.

Dank, voorzitter.

Mevrouw **El Boujdaini** (D66):
Dat vind ik heel fijn. Dank u wel.

Staatssecretaris **Aerdts**:
Voorzitter, zal ik dan doorgaan met de …

De **voorzitter**:
Gaat u verder.

Staatssecretaris **Aerdts**:
Mevrouw El Boujdaini vroeg of ik iets specifieker kan zijn over de exacte datum. We hebben van de Europese Commissie geen datum gekregen, maar in de gesprekken is wel naar voren gekomen dat het de verwachting is dat dat wel gaat gebeuren. We hopen eind dit jaar een uitvoeringswet in consulatie te brengen en daar hebben we die datum voor nodig. Het is misschien wel goed om nog even op te merken dat het gebruik van EDI-wallet vrijwillig is en blijft.

De heer Van den Berg vroeg naar de Kamervragen. De staatssecretaris beantwoordt nog deze week de vragen over de Belastingdienst. CISO Bijvoet gaat hier ook een aantal gesprekken over voeren en dan juist over de bredere casuïstiek van dit specifieke voorbeeld. Verder zal ik met mijn ambtsgenoot van Defensie in gesprek gaan over Werken bij Defensie. En ik zal dan ook uw vraag aan hem doorgeleiden.

Dan over het Rathenau Instituut en de Omnibuswetgeving. Het is een beetje moeilijk, hè. We hebben een kabinetsappreciatie gegeven …

De heer **Van den Berg** (JA21):
Dank voor het doorzenden van die informatie naar de staatssecretaris van Defensie. Wat betreft Adobe en de Belastingdienst: ik heb begrepen dat de hacker die dit heeft ontdekt en waar ik op mijn beurt Kamervragen over heb gesteld, is uitgenodigd bij de Belastingdienst. Hij heeft daar een leuk presentje gekregen. Complimenten daarvoor! Maar een briefje daarover aan de Kamer was misschien ook wel passend geweest. Maar ik denk dat dat meer staatssecretaris Eerenberg betreft. Ik wil de staatssecretaris Digitale Economie en Soevereiniteit nu vooral vragen of zij in haar horizontale rol goed in de gaten kan houden wat we doen met onze eigen websites. Het gaat me dus om meer dan alleen een signaal aan Defensie. Ik wil gewoon een continue blik naar binnen.

Staatssecretaris **Aerdts**:
Ik voel zeker mijn coördinerende rol, want ik heb een belangrijke taak bij het voeren van de gesprekken. Mijn collega-staatssecretaris van Binnenlandse Zaken kijkt natuurlijk in dit geval naar de Rijksoverheid. Dat is echt iets waarin we nadrukkelijk samen zullen optrekken. Maar ik hoor van hem dat hij daar zo ook nog iets over gaat zeggen.

Dan over het Rathenau Instituut, de Omnibuswetgeving en de cookies. Ik kan daar nog iets meer over zeggen, maar we zitten wel midden in de onderhandelingen. Wat daar precies uit gaat komen, weet ik dus niet. Maar we zullen de informatieafspraak gebruiken om de Kamer daarover te informeren. De kern blijft dat er toestemming nodig is voor het plaatsen van cookies. In het Omnibustraject is voorgesteld om dat geven of weigeren te versimpelen: niet langer 26 keer klikken, maar 1 keer. De Commissie stelt voor om het mogelijk te maken om met één klik en zonder dark patterns toestemming

voor het plaatsen van cookies te weigeren of om dit zelf centraal via de browserinstellingen mogelijk te maken. En daar staat Nederland positief tegenover. Maar op wat daaruit gaat komen, kom ik dus nog terug.

De VVD sprak nog even over kwantum. We sprake daar vorige week in deze commissie ook over. Er komt, zeg ik uit mijn hoofd, in Q3 een strategie naar de Kamer.

Mevrouw Kathmann van PRO vroeg naar het basispakket digitale veiligheid.

De **voorzitter**:
Voordat u daarop ingaat, is er nog een interruptie van mevrouw Zwinkels, CDA.

Mevrouw **Zwinkels** (CDA):
Dank voor het realistische antwoord. Het is goed om dat eerlijk met elkaar te delen, maar ik ben nog wel naar iets op zoek. In eerste termijn gaf de staatssecretaris namelijk aan dat ze een aantal aanbevelingen en adviezen in dat Rathenau-rapport zag staan. Dat zijn verbeteringen die we gewoon los van Europa door kunnen voeren. Ik ben daarom heel erg benieuwd wanneer we dat kunnen verwachten. Ze gaf zojuist aan om ons daarover te informeren, maar ik zou dan wel graag een tijdpad krijgen, want dan weet ik of ik moties moet indienen of even geduld moet hebben om daar later alsnog een oordeel over te vellen.

Staatssecretaris **Aerdts**:
Daar kom ik graag in een briefje vlak na het reces bij u op terug.

De laatste vraag voor mij is de vraag van mevrouw Kathmann, PRO, over het basispakket digitale veiligheid. Kunnen wij daar een rol in gaan spelen? Diverse marktpartijen bieden al veiligheidspakketten aan. Een deel van die producten wordt gratis aangeboden. Het kabinet wil met de aanbieders van die producten de inhoud en de toegankelijkheid van het aanbod bezien en bekijken of dit eventueel verbeterd kan worden. Maar ik wil nadrukkelijk gezegd hebben dat wij als overheid natuurlijk niet gaan concurreren met de markt. Het is dan ook belangrijk dat die pakketten door de markt zelf worden aangeboden.

Verder zijn we bezig met maatregelen voor de digitale weerbaarheid van burgers, bijvoorbeeld via veiliginternetten.nl. Gisteren spraken we daar al over in het verband met je digitale nalatenschap. Maar verder is er ook de campagne Phishkraam, waar ik laatst zelf was. U heeft terecht in dit debat gezegd dat het natuurlijk nooit de verantwoordelijkheid van burgers zelf is dat hun gegevens worden gelekt. Maar we willen ze wel graag weerbaarder maken en dat past, denk ik, ook heel goed in de strategie die we hier besproken hebben. Ook wordt in dit kader een nationale cursus Digitale Weerbaarheid georganiseerd voor alle Nederlanders van 12 jaar en ouder. Ten slotte is er de cursus Digisterker voor de doelgroep senioren. Deze cursus is specifiek bedoeld voor de bibliotheken.

Bedrijven worden op de website van het NCSC geïnformeerd over de cyber-basismaatregelen die zij kunnen nemen. Ook biedt het kabinet via Mijn Cyberweerbare Zaak jaarlijks subsidie aan voor de aanschaf van cybersecuritymaatregelen door kleine mkb'ers.

De **voorzitter**:
Heel goed. Dan gaan we naar de heer Van der Burg.

Staatssecretaris **Van der Burg**:
Voorzitter. Nog even twee dingetjes vanuit mij. De eerste heeft betrekking op Adobe. Daar werd ook wat over gevraagd. Ik zal in ieder geval eventjes via de rijks-CIO bij de departementen ophalen bij welke departementen het verder nog speelt. Ik kan daar dan via de CISO en de CIO mee aan de slag. Dat was het eerste punt. Het tweede punt is het handelingskader. Dat handelingskader is er. Dat staat op de website van het rijksarchief als het gaat om termijnen waarin bewaard moet worden, want we hebben daar de richtlijnen op staan. Die richtlijnen bepalen wanneer wat verwijderd moet worden. Dat kunt u op de website van het rijksarchief vinden, want die hoort dat in het kader van de Archiefwet ook allemaal bij te houden.

Waarom het langer laten duren als het korter kan, voorzitter?

De **voorzitter**:
Dat is uitstekend. Er is nog wel een vraag van mevrouw Kathmann.

Mevrouw **Kathmann** (PRO):
Een vraag, maar misschien eerder een opmerking. Ik wil niet gelijk een tweeminutendebat aanvragen, omdat ik nu vooral op zoek ben hoe we het concreet gaan maken. Hoe kan een Kamerlid weten wat we wel of niet gaan doen? We zitten hier echt met een gigantisch maatschappelijk probleem. Ik snap dat men dat aanvoelt en het is ook niet voor niets dat hier drie ambitieuze staatssecretarissen aanschuiven. Maar soms is dat voor een Kamerlid juist heel moeilijk, omdat het dan overal zit. Je hebt dan gewoon niet zo goed zicht op wat we wanneer gaan doen. Ik vraag daarom een tweeminutendebat aan, want dan kan ik daar een motie over indienen. Het is echt heel urgent.

Dan over de beantwoording van mijn vragen over het basispakket digitale veiligheid. Ik snap dat dat er allemaal is. Dat weten we, maar ik maakte daarom ook expliciet de opmerking: "Natuurlijk moet je dit met de markt doen. Je moet dit vooral niet zelf willen doen." Maar zolang mijn buren aan de ene kant en mijn overburen een de andere kant geen toegang tot die pakketjes hebben, gaat er iets niet goed. Gezien alle innovaties die nog op ons af gaan komen, hebben we eigenlijk geen tijd meer te verliezen. Concreet: als het antwoord is "dit doen we al", dan ga ik volgende week mijn motie in stemming brengen. Maar betekent dat dan ook dat die motie oordeel Kamer krijgt? Wat gaan we nou concreet wel of niet doen? Dat vind ik gewoon zo moeilijk.

De **voorzitter**:
Wie kan ik daarover het woord geven?

Staatssecretaris **Aerdts**:
Misschien een korte reactie. Er gebeurt misschien al veel, maar ik heb al toegezegd dat ik met de partijen in gesprek zal gaan, juist ook om te kijken waar het mogelijk nog aan schort en waar wij mogelijk bij zouden kunnen helpen. Meer kan ik daar op dit moment niet over toezeggen. Het is nu in beweging en daarom zou ik mevrouw Kathmann willen vragen om nog even te wachten met het indienen van die motie.

Mevrouw **Kathmann** (PRO):
Dan is het wel fijn dat we weten wanneer we de terugkoppeling over die gesprekken krijgen.

Staatssecretaris **Aerdts**:
In de tweede helft van dit jaar, voor het kerstreces.

De **voorzitter**:
Heel goed. Dan is er nog een vraag van mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Ik zit een beetje met dezelfde vraag als mevrouw Kathmann, daarom net ook mijn vraag aan staatssecretaris Aerdts. Ik zou het toch wel fijn vinden om straks met elkaar even de toezeggingen door te nemen en te kijken wanneer we wat kunnen verwachten. Mogelijk kunnen we al een aantal zaken na het reces verwachten, zodat we het tweeminutendebat daarna kunnen voeren. Dat zou wat mij betreft best wel een interessante optie zijn, dus dat we het tweeminutendebat niet nog voor het reces plannen.

De **voorzitter**:
Dat lijkt me ook planningstechnisch nogal lastig, eerlijk gezegd.

Staatssecretaris **Aerdts**:
Mag ik daar kort op reageren? De aanpassing van de cookiewetgeving en de Europese wetgeving: we verwachten nog deze maand een Omnibuscompromis. Daar zullen we u volgens de informatieafspraken over informeren, zodat we daar na het reces met elkaar over in gesprek kunnen gaan.

De heer **Verkuijlen** (VVD):
Eén vraag van mij aan staatssecretaris Van Bruggen is niet beantwoord. We hadden even discussie over het handelingskader voor de slachtoffers en toen gaf zij nadrukkelijk aan dat daar niet direct een rol is weggelegd voor de overheid. Maar zij zei wel mogelijkheden te zien om nog iets meer te doen. Dank daarvoor! Als iemand aangifte doet tegen zo'n bedrijf, verandert de status van slachtoffer. Heeft zij het idee dat de overheid op dat moment meer moet doen dan in het handelingskader staat?

Staatssecretaris **Van Bruggen**:
Ik denk dat het goed is om hier schriftelijk op terug te komen. Ik wil hier niet naar gissen. Ik zei net overigens al wel dat het uiteindelijk de vraag is of het een verlengde van slachtofferhulp is of dat we hier iets met rechtsbijstand moeten doen. Hoe kunnen mensen deze informatie achterhalen? Welke ruimte is er? Er is ongetwijfeld ruimte, want die hebben ze zelf. Maar wat is dan onze rol daarin? Gezien die vragen zou ik er graag schriftelijk op terug kunnen komen.

De **voorzitter**:
Heel goed. De laatste vraag is voor de heer Van den Berg.

De heer **Van den Berg** (JA21):
Ik moet wel lachen om wat staatssecretaris Aerdts zegt: na het zomerreces, voor de kerst. Dat is een mooie open deur intrappen om gewoon "ergens dit jaar" te zeggen! Er

zijn twee vragen van mij nog niet beantwoord over de opt-in bij de AI-verordening. Toch? Ik twijfel nu een beetje aan mezelf, maar volgens mij zijn die nog niet beantwoord. En dan is er nog de vraag over het verduidelijken van de handreiking voor de rijksoverheid voor de AVG. Volgens mij zei staatssecretaris Van Bruggen dat die vragen naar staatssecretaris Aerdts zouden gaan.

Staatssecretaris **Aerdts**:
Het tweede stuk heb ik even niet goed gehoord. Op de opt-in kom ik schriftelijk terug.

De heer **Van den Berg** (JA21):
Schriftelijk. Dank u wel. Maar op welke termijn? Het tweede punt was de handreiking voor de AVG. Kunnen we die niet door de Rijksoverheid heen pompen om de handelingsverlegenheid van de AVG te verduidelijken en om ervoor te zorgen dat de overheid beter weet waar ze aan toe is?

Staatssecretaris **Aerdts**:
De vraag over de AVG en de overheid ligt, denk ik, bij mijn collega Van der Burg. Op de opt-in kom ik dus nog even schriftelijk terug.

Staatssecretaris **Van der Burg**:
Laat ik dan ook even … Anders heb ik geen brief! U moet ook mij een brief gunnen.

De heer **Van den Berg** (JA21):
Heel goed. Van harte.

Staatssecretaris **Van der Burg**:
Dank u wel. Ik hoor u, mevrouw Zwinkels. Daar kom ik in de toekomst positief op terug.

De **voorzitter**:
Hiermee zijn we aan het einde gekomen van de tweede termijn van de Kamer. Ik zal mijn best doen om alle toezeggingen op te sommen. Dat zijn er volgens mij heel wat.

Maar eerst: het lid Kathmann van PRO vraagt een tweeminutendebat aan. Dat staat toch nog steeds, mevrouw Kathmann? Ja.

- De staatssecretaris JenV zegt toe om de Kamer na de brede werkconferentie, die in Q3 zal worden georganiseerd, te informeren over haar verdere aanpak van de bescherming van de persoonsgegevens, de AVG, en de nationale doorwerking van de Europese regelgeving. Hierbij zal de input uit de conferentie worden meegenomen.
- De staatssecretaris JenV zegt toe om het punt genoemd door het lid Verkuijlen inzake het geven van expliciete toestemming voor de verwerking van persoonsgegevens mee te nemen in de verdere Europese gesprekken hieromtrent.
- De staatssecretaris JenV zegt toe de Kamer dit jaar nader te informeren over het handelingskader voor slachtoffers van datalekken, waarbij ook de bewaartermijnen, de communicatie met slachtoffers en een landelijke standaard voor hulp aan slachtoffers zullen worden meegenomen.

Staatssecretaris **Van Bruggen**:
Dat gaat niet meteen over hoe we dat handelingskader inrichten, maar meer over hoe en op welke manier we het een plek kunnen geven. Een handelingskader voor slachtoffers betreft natuurlijk altijd iets wat plaatsvindt nadat de situatie is ontstaan. Die bewaartermijn is dus eigenlijk een ander onderwerp dat daar parallel aan zit. Het maakt misschien geen onderdeel uit van het handelingskader zelf, maar we willen er wel in dit verband op terugkomen, want volgens mij was dat de vraag van mevrouw Zwinkels.

De **voorzitter**:
Is dat juist, mevrouw Zwinkels? Is dat inderdaad de vraag?

Mevrouw **Zwinkels** (CDA):
Ja, dat is voor mij akkoord. Als we het er nu toch over hebben: ik dacht dat die landelijke standaard een aparte toezegging was. Maar het kan ook samengenomen worden. Dat laat ik aan de staatssecretaris, maar zij zei dus wel dat we daarover dit jaar nog zouden worden geïnformeerd.

De **voorzitter**:
Ja, dit jaar. Dat staat hier ook in.

Mevrouw **Kathmann** (PRO):
Ik heb hierover nog wel een vraag. Mevrouw Rajkowski van de VVD heeft dat handelingskader hier als initiatief neergelegd. Bij die handelingstermijn gaat het welzeker ook over het handelingsperspectief van de burger zelf. Bij de nazorg denken mensen namelijk heel vaak: maar dit gaat me niet nog een keer overkomen. Je hebt welzeker ook het recht om navraag te doen over bijvoorbeeld bewaartermijnen, maar heel veel mensen weten dat niet. Dat is in dat debat waarin mevrouw Rajkowski dit voorstel deed, ook aan bod gekomen. Het zou dus mooi zijn als het in die zin wel wordt meegenomen.

Ik hoor de staatssecretaris nu buiten de microfoon "dit neem ik mee, hoor" zeggen, maar het werd net even uit elkaar getrokken. Maar oké.

De **voorzitter**:
De staatssecretaris neemt het wel mee. Helemaal goed. Dan ga ik verder met de toezeggingen. Ik had er vijf, geloof ik.

- De staatssecretaris JenV zegt toe te vragen naar de termijn van afronding van een instrument, waarbij met indicatoren de doelmatigheid en de doeltreffendheid van de AP kan worden gemeten.
- De staatssecretaris JenV zegt toe dat de Kamer na de zomer wordt geïnformeerd over de implicaties van de uitvoeringswet van de AI-verordening en over de extra financiële middelen die hiervoor zullen worden vrijgemaakt voor de Autoriteit Persoonsgegevens.
- De staatssecretaris JenV zegt toe de Kamer te informeren over de samenwerking tussen toezicht en handhaving, de AP en de politie, bij grote datalekken.

Staatssecretaris **Van Bruggen**:
Een kleine nuance bij hoe dat precies gaat. De Autoriteit Persoonsgegevens houdt bijvoorbeeld ook weer toezicht op de politie. Dus ja, er wordt samengewerkt, maar er is ook een rolverdeling. Ik ga dus in kaart brengen hoe bij toezicht en handhaving die samenwerking precies gaat. Ik denk dat dat ook het overzicht is waar mevrouw El Boujdaini naar vroeg. Ik check het even en het klopt, want mevrouw El Boujdaini knikt.

De **voorzitter**:
De volgende.

- De staatssecretaris JenV zegt toe schriftelijk terug te komen op de vragen van het lid Verkuijlen over slachtofferhulp.
- De staatssecretaris EZK zegt toe de Kamer volgens de reeds gemaakte informatieafspraken te informeren over de uitkomst van de digitale Omnibusonderhandelingen. Zij zal hierbij tevens ingaan op trackingcookies.

Mevrouw **Zwinkels** (CDA):
Ik had expliciet gevraagd naar twee punten: kinderen en de contextuele advertenties. Ik begreep van de staatssecretaris dat ze dat wilde betrekken bij de toezeggingen.

De **voorzitter**:
Is dat juist? Ja? Dan is dat akkoord.

- De staatssecretaris EZK zegt toe de Kamer na het zomerreces te informeren over de uitwerking van de aanbevelingen van het Rathenau-rapport over onlinetracking.

Staatssecretaris **Aerdts**:
Dat wordt dus gecombineerd met wat er met die Omnibuswetgeving gedaan is. Als we de Kamer informeren, zal ik een link leggen met het Rathenau Instituut. Maar dat gaat op dit moment voor mij wel samen, omdat die aanbevelingen over cookies ook echt in Europees verband plaatsvinden. En daar loopt nu dus dat Omnibustraject voor.

De **voorzitter**:
Dat lijkt me logisch, hè.

Mevrouw **Zwinkels** (CDA):
Ik val een beetje in herhaling, voorzitter. Maar ik heb ook gevraagd welke verbeteringen we op basis van dit rapport op nationaal niveau kunnen doorvoeren. Daar wilde de staatssecretaris ook op terugkomen. Het mag wat mij betreft hierbij. Dat vind ik prima, want laten we het niet te ingewikkeld maken of om te veel brieven vragen. Maar dan hebben we dat wel scherp.

De **voorzitter**:
Dat is dit toch? Goed.

- De staatssecretaris van BZK komt in de tweede helft van het jaar, en in ieder geval voor het kerstreces, bij de Kamer terug op de genoemde gesprekken.
- De staatssecretaris van EZK zal schriftelijk terugkomen op de vragen van het lid Van den Berg over de opt-in.
- De staatssecretaris van BZK zegt toe de punten genoemd door het lid Van den Berg omtrent Adobe rijksbreed te onderzoeken.
- De staatssecretaris van BZK zegt toe schriftelijk terug te komen op de handreiking AVG.

Dan zijn we volgens mij compleet en dan rest mij om het kabinet te bedanken voor zijn openhartige inbreng en de Kamer voor haar gepassioneerde inbreng.

Sluiting 13.19 uur.