

Vergaderjaar 2024–2025

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 1371

**BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN
EN KONINKRIJKSRELATIES**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 juli 2025

Met deze brief informeer ik u over openstaande moties en toezeggingen op het gebied van digitalisering. Verder neem ik u mee in de stand van zaken betreffende een aantal beleidsonderwerpen. In bijlage 1 heb ik opgenomen welke moties en toezeggingen ik met deze brief behandel.

Deze brief is als volgt ingedeeld. Allereerst zal ik stil staan bij toegankelijke en mensgerichte (digitale) dienstverlening. Ten tweede bij onderwerpen op het gebied van de digitale overheid, waaronder de Rijksdienst. Als laatste zal ik ingaan op nieuwe en opkomende technologieën en online platforms, welke zijn samengenomen onder de noemer Digitale Samenleving.

Alvorens hiertoe over te gaan vind ik het belangrijk om te markeren dat de Nederlandse Digitaliseringsstrategie (NDS) is gepubliceerd en met uw Kamer is gedeeld.¹ Hiermee heb ik tevens gehoor gegeven aan het verzoek van uw Kamer om de Nederlandse Digitaliseringsstrategie zo spoedig mogelijk te ontvangen.² Met deze strategie van het Rijk samen met de medeoverheden en publieke dienstverleners gaan we als één overheid te versnellen op zes digitale prioriteiten, te weten:

- Cloud;
- Data;
- Artificiële intelligentie;
- De overheid stelt burgers en ondernemers centraal in (digitale) dienstverlening;
- Versterken digitale weerbaarheid en autonomie van de overheid;
- Digitaal vakmanschap en een moderne werkomgeving.

¹ Nederlandse Digitaliseringsstrategie | Rapport | Rijksoverheid.nl

² Commissiebrief van de vaste commissie voor Digitale zaken van de Tweede Kamer inzake een verzoek om de Nederlandse Digitaliseringsstrategie zo spoedig mogelijk aan de Kamer te doen toekomen, d.d. 16 juni 2025, te raadplegen via: <https://www.tweedekamer.nl/downloads/document?id=2025D25573>

Vanwege deze keuze om op een beperkt aantal onderwerpen te versnellen komen in de NDS niet alle vraagstukken binnen het bredere digitaliseringsbeleid aan bod. Dat betekent echter niet dat er op andere onderwerpen geen voortgang meer wordt geboekt of belangrijke ontwikkelingen plaatsvinden. Ik zal de Kamer uiteraard ook blijven informeren over het bredere digitaliseringsbeleid. Zo doe ik dat ook in deze brief.

1. Toegankelijke en mensgerichte (digitale) dienstverlening

1.1 Digitale dienstverlening, Informatiepunten Digitale Overheid (IDO) en fysieke dienstverlening

1.1.1 Digitale dienstverlening

Voor mensen die hun weg weten te vinden in de online dienstverlening zet ik in op een digitaal landschap waarbij vanuit burger- en ondernemersperspectief een soepele klantreis voor dienstverlening van de overheid wordt neergezet. Van informatie en contact tot het daadwerkelijk regelen van zaken met de overheid. De concrete uitwerking daarvan vindt plaats in een overheidsbreed traject.

Eén van de mijlpalen is het moderniseren en doorontwikkelen van Overheid.nl als online wegwijzer waar alle informatie over publieke producten en diensten in samenhang kan worden gevonden. Door de integratie met MijnOverheid kunnen bezoekers die deze ingang kiezen straks in één keer worden doorgeleid van algemene informatie over producten en diensten van de overheid naar gepersonaliseerde informatie op basis van situatie of locatie of informatie die al bij de overheid bekend is. Daarnaast wordt ook gewerkt aan de ontwikkeling van overheidsbrede services, zoals «stand van zaken» en «notificatie». Dit is bedoeld om het contact en de online interactie met de overheid meer te standaardiseren, zodat de dienstverlening voor burgers en ondernemers overzichtelijker en makkelijker wordt.

Komende zomer start een bèta-versie van deze overheidsbrede wegwijzer onder Overheid.nl. Tegelijkertijd zal met behulp van technologieën als AI en in co-creatie met medeoverheden, publieke dienstverleners en departementen Overheid.nl stapsgewijs worden doorontwikkeld tot een overheidsbrede betrouwbare, herkenbare online wegwijzer naar informatie en dienstverlening. Daarnaast wordt in dit traject ook de verbinding met de informatie en dienstverlening specifiek voor ondernemers verder geoptimaliseerd.

1.1.2 Informatiepunten Digitale Overheid (IDO)

Ik vind het belangrijk dat publieke dienstverlening wordt aangeboden op plekken die voor mensen logisch en dichtbij voelen. Het is mijn visie dat gemeenten een regierol hebben in het vormgeven van het lokale netwerk voor publieke dienstverlening. Het is daarom ook aan hen om te bepalen waar lokaal welke vorm van laagdrempelige en empathische ondersteuning het meest geschikt is. Dat kan in de bibliotheek zijn, maar ook andere locaties zijn denkbaar. Ik heb uw Kamer toegezegd informatie te sturen naar aanleiding van de IDO's en de inspanningsverplichting om de dienstverlening aan burgers op peil te houden en hierbij het eerder gedeelde KPMG-rapport mee te nemen in de overwegingen ^{3, 4}

³ Exploitatieonderzoek Informatiepunt Digitale Overheid | Rapport | Rijksoverheid.nl

⁴ TZ202411-104

In het exploitatie-onderzoek, uitgevoerd door KPMG, wordt geconcludeerd dat de gemiddelde exploitatiekosten van de verschillende IDO's sterk verschillen en een reflectie zijn van de lokale inrichting en keuzes in de uitvoering. KPMG doet dan ook de aanbeveling om de opdracht voor uitvoering van IDO-dienstverlening meer te concretiseren, zodat beter gestuurd kan worden op hetgeen mogelijk is met het beschikbare budget. Dit beoog ik ook met de verdere versterking van de regierol voor gemeenten.

Het kabinet heeft besloten om per 2026 de Specifieke Uitkeringen (SPUKs) om te zetten in fondsuitkeringen met een budgetkorting van 10%. Uw Kamer heeft op 3 juli jongstleden een motie aangenomen om «*structureel extra middelen beschikbaar te stellen aan gemeenten voor de uitvoering van de IDO's door bibliotheken en dit voor de komende jaren te dekken uit de vrij te besteden middelen ten behoeve van betere overheidsdienstverlening.*» Ik zal uw Kamer hier na de zomer over informeren.

Door de afschaffing van de SPUK voor de IDO's en de overheveling van de middelen naar het gemeentefonds krijgen gemeenten meer beleidsvrijheid om de middelen in te zetten. Gemeenten hebben dus per 2026 niet langer de wettelijke plicht om een IDO in stand te houden. Wél wordt aan de decentralisatie-uitkering het doel waarvoor deze wordt verstrekt meegegeven, evenals afspraken over het beoogde resultaat en monitoring van de behaalde effecten. Dit kan worden vastgelegd in bestuurlijke afspraken, bijvoorbeeld een convenant. Over de afspraken die ik hierover met gemeenten maak zal ik uw Kamer in Q4 van dit jaar informeren.

Om gemeenten te ondersteunen bij hun regierol in het versterken van het lokale netwerk, zet ik, naast de structurele financiering, extra middelen in die structureel vanuit het regeerprogramma zijn toegekend om bestaande overheidsbrede ingangen, waaronder IDO-dienstverlening beter in te bedden in het lokale netwerk. Met deze informatie beschouw ik de toezegging als afgedaan.

Ik ben ervan overtuigd dat gemeenten overheidsbrede dienstverlening kunnen verzorgen op voor mensen logische plekken. En dat mensen zo ervaren dat ze goed worden geholpen en ondersteund. Belangrijk daarbij zijn wat mij betreft ook de blijvende aandacht voor deskundigheidsbevordering en het ophalen van signalen en feedback, waarmee we publieke dienstverlening kunnen verbeteren.

1.1.3 Beleidsvisie fysieke dienstverlening

Zoals aan uw Kamer toegezegd⁵, stuur ik bij deze brief mijn visie op lokale, fysieke dienstverlening. De beleidsvisie Persoonlijk en Dichtbij, die u in bijlage 2 vindt, geeft invulling aan het persoonlijke, fysieke contact binnen de loketfunctie van de overheid. De visie is tot stand gekomen na een uitgebreid beleidsontwikkelingstraject met medewerking van medeoverheden en publieke dienstverleners, burgers en ondernemers.

Mijn inzet is dat meer mensen gebruik maken van de diensten en producten van de overheid, met name mensen die we nu niet of nog onvoldoende bereiken. Gemeenten hebben hierin een belangrijke rol. Zij hebben zicht op de behoeften van hun inwoners en kennen de lokale netwerken die mensen kunnen helpen en die mensen vaak al weten te bereiken: formele en informele verbanden en voorzieningen die dicht bij burgers staan. En hebben zicht op sleutelpersonen die een betekenisvolle functie vervullen voor inwoners, goed verbonden zijn met de lokale

⁵ Kamerstukken II 2023–2024, 26 643, nr. 1099

gemeenschap en in staat zijn om groepen te bereiken die voor gemeenten en reguliere instellingen soms lastig toegankelijk zijn.

Het versterken van dit lokale ecosysteem staat centraal. Ik zet daarom ook in op de inbedding van overheidsbrede fysieke dienstverlening in dat lokale ecosysteem, zoals de laagdrempelige hulp geboden vanuit de Informatiepunten Digitale Overheid (IDO) en de verdergaande overheidsbrede dienstverlening in de overheidsbrede loketten. Vanaf dit kwartaal wordt op 28 locaties in de praktijk gewerkt met, getoetst en geleerd van het bieden van overheidsbrede dienstverlening. Ik beschouw de toezegging hiermee als afgedaan.

2. Digitale Overheid

2.1 Digitale Rijksdienst

2.1.1 Motie Buijsse – Maatregelen voor het borgen van de soevereiniteit, continuïteit en gegevensbescherming in cloudcontracten⁶

In het debat «Digitaliserende Overheid» op 23 april 2025 is toegezegd uw Kamer in deze brief te informeren over de motie van het lid Buijsse aangaande het borgen van soevereiniteit, continuïteit en gegevensbescherming in cloudcontracten en de handhaving van het Rijksbreed cloudbeleid.

In reactie op de motie van het lid Buijsse informeer ik u dat de departementen, via het Chief Information Officer (CIO)- en Chief Information Security Officer (CISO)-beraad, inmiddels zijn verzocht de bevindingen van de Algemene Rekenkamer uit het rapport *Het Rijk in de Cloud* voortvarend op te pakken. Onderdeel hiervan is om de ingezette verbetering door te zetten om de voorgenoemde achterstand in te halen. Waar nodig kunnen de departementen daarbij ondersteund worden.

Ook is de herziening van het Rijksbreed cloudbeleid, die medio 2025 wordt voorzien, hierbij leidend, evenals de nog op te stellen beleidskaders voor digitale autonomie en soevereiniteit van de overheid en de IT-sourcingstrategie Rijk. In de aanpak voor digitale autonomie worden onder meer risico's rond marktconcentratie en strategische afhankelijkheden opgenomen. In de herziening van het cloudbeleid wordt een uitbreiding van de scope voorzien, evenals een expliciete aanscherping van de verplichte exit-strategie. Een versteviging van de monitorende functie van CIO-Rijk moet leiden tot beter inzicht in het cloudegebruik van de rijksoverheid.

Tot slot informeer ik u dat, in lijn met de motie van het lid Six-Dijkstra⁷, het vaststellen van kaders ter bevordering van de digitale autonomie wordt opgenomen in het Coördinatiebesluit voor relevante informatiesystemen die door alle of een deel van de ministeries worden gebruikt. U ontvangt hierover verdere informatie na de zomer van 2025.

⁶ Kamerstukken II 2024/2025, 26 643, nr. 1321

⁷ Kamerstukken II 2024/2025, 26 643, nr. 1294

2.1.2 Motie Six Dijkstra en Buijsse – Onderzoek naar getrapte afbouw van digitale monoculturen en de van Small Business Innovation Research (SBIR) programma's voor meer digitaal autonome overheidsdiensten⁸

De leden Six Dijkstra en Buijsse hebben de regering verzocht te onderzoeken hoe op verantwoorde wijze interdepartementaal kan worden aangestuurd op een getrapte afbouw van digitale monoculturen, en tevens waar SBIR-programma's effectief kunnen worden ingezet om toe te werken naar meer digitaal autonome overheidsdiensten.

Ik deel de zorgen van uw Kamer over de risico's van digitale monoculturen, zoals ook benoemd in het Cybersecuritybeeld Nederland.⁹ Een te grote afhankelijkheid van één of enkele marktpartijen kan leiden tot ongewenste situaties. Daarom is het belangrijk om onze digitale (open strategische) autonomie¹⁰ te versterken en risico's van strategische afhankelijkheden te beheersen.

Met de aankomende, nieuwe IT-sourcingstrategie Rijk wordt ingezet op het actief terugdringen van afhankelijkheid van enkele leveranciers en het beheersen van marktconcentratie- en continuïteitsrisico's. Het moet leiden tot versterking van de departementale risicobeheersing en meer zicht op individuele risico's. Het maakt het mogelijk om departement-overstijgende risico's beter te beheersen en waar mogelijk digitale monoculturen terug te dringen of te voorkomen. De uitwerking van de moties van de leden Six Dijkstra en Buijsse om het Coördinatiebesluit uit te breiden zal hier naar verwachting een positieve impuls aan geven.¹¹ Daarnaast geven de nog op te stellen beleidskaders voor digitale autonomie en soevereiniteit van de overheid, naast de IT-sourcingstrategie Rijk, verdere invulling aan hoe we de continuïteit van de overheidsdienstverlening borgen en het IT-landschap toekomstbestendig en robuust inrichten. Ik werk bovendien aan een verkenning van het realiseren van een overheidsbrede soevereine clouddienst in samenwerking met bestaande overheidsdienstverleners en de markt. Dit als alternatief voor de afhankelijkheid van buitenlandse clouddaanbieders.

Deze inzet op versterking van de digitale autonomie raakt direct aan het bredere streven naar het verminderen van afhankelijkheden, waarin ook het gebruik en ontwikkelen van open source software een centrale rol speelt. De motie wijst dan ook terecht op het belang van open source als pijler van digitale autonomie. We hanteren het uitgangspunt «open, tenzij» bij het gebruik en ontwikkelen van overheidssoftware. Dit betekent dat broncode in beginsel wordt vrijgegeven als open source, tenzij er gegronde redenen zijn om dat niet te doen, zoals nationale veiligheid of vertrouwelijkheid. Voor wat betreft de «tenzij» is beleidsmatig aangesloten bij de uitzonderingsgronden van de Wet Open Overheid. Broncode van overheidssoftware is immers overheidsinformatie. Dit beleid is vastgelegd in eerdere Kamerbrieven en wordt o.a. actief ondersteund via onder meer de overheidsbrede community opensourcowerken.nl en het innovatiebudget Digitale Overheid.¹²

⁸ Kamerstukken II 2024/2025, 36 600 VII, nr. 77

⁹ Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV), *Cybersecuritybeeld Nederland 2024*, 28 oktober 2024, beschikbaar via: <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten>.

¹⁰ Ministerie van Economische Zaken en Klimaat, *Agenda Digitale Open Strategische Autonomie (DOSA)*, 17 oktober 2023, beschikbaar via: <https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa>.

¹¹ Kamerstuk 26 643, nr. 1294 en Kamerstuk 26 643, nr. 1322.

¹² Kamerbrief over digitale gemeenschapsgoederen | Kamerstuk | Rijksoverheid.nl

Ten aanzien van de suggestie om het SBIR-instrument (tegenwoordig Innovation Impact Challenge genoemd) in te zetten voor het versterken van digitale autonomie, zie ik duidelijke kansen. Het instrument is bij uitstek geschikt voor het stimuleren van markten die nog niet bestaan—zoals alternatieven voor huidige big tech-oplossingen—en biedt de rijksoverheid de mogelijkheid om als aanjager en launching customer het goede voorbeeld te geven. Daarmee sluit het goed aan bij de transitie van digitale monoculturen naar meer digitaal autonome overheidsdiensten.

Elk ministerie en elke uitvoeringsorganisatie is zelf verantwoordelijk voor het beheer van zijn IT. Dat maakt het des te belangrijker dat er instrumenten beschikbaar zijn die hen helpen om toekomstbestendige keuzes te maken. Het SBIR-instrument kan daarbij een waardevolle rol spelen door nieuwe inkoopopties te creëren die momenteel nog ontbreken. De combinatie van een SBIR-traject met een opvolgende aanbesteding kan bovendien de markt stimuleren en daarmee ook breder ten goede komen aan ondernemend Nederland. De oplossingen die binnen deze trajecten worden ontwikkeld, kunnen daarnaast ook beschikbaar komen voor andere publieke partijen en zelfs voor consumenten. Daarmee draagt de inzet van het instrument niet alleen bij aan de digitale autonomie van de overheid, maar ook aan bredere maatschappelijke meerwaarde.

De onderliggende motie(s) onderstrepen dan ook terecht het belang van minder afhankelijkheid en meer digitale autonomie binnen de overheid. Die ambitie sluit goed aan bij het ingezette beleid en de lopende beleidsontwikkeling. Ik dank uw Kamer voor de aandacht voor dit thema en blijf mij inzetten voor een weerbare, transparante en toekomstbestendige digitale overheid.

2.1.3 Stelselherziening na adviezen Auditdienst Rijk en Adviescollege ICT-toetsing

Uw Kamer is toegezegd op de hoogte te worden gehouden van de doorontwikkeling van het CIO-stelsel. De tijdelijke werkafspraken die in 2024 in het CIO-beraad zijn gemaakt worden opgenomen in het stelsel. Het stelsel wordt daarmee uitgebreid met functionarissen op het gebied van Privacy, Data en Technologie en de rol van de CIO van de Rijksdienst Caribisch Nederland. Ook zijn er aanvullende bepalingen opgenomen over interoperabiliteit tussen departementen. Om de werkwijze van het CIO-beraad en de verschillende voorportalen te verbeteren is het «Reglement CIO-beraad en voorportalen» opgesteld. Naast de aanpassingen in het besluit CIO-stelsel en het vaststellen van het reglement zijn er door de Auditdienst Rijk (ADR), het Adviescollege ICT-toetsing (AcICT) en door verschillende stakeholders kansen geïdentificeerd om de werking van het stelsel te verbeteren. Dit gaat om verschillende verbeteracties om de kwaliteit van kaders te verbeteren, monitoring beter in te richten en om de besluitvorming en informatie-uitwisseling tussen de departementen te verbeteren. Hier wordt actie op ondernomen. Ik zal uw Kamer in het najaar verder informeren over het aangepaste besluit.

2.1.4 Beschikbaar stellen IT-sourcingstrategie voor medeoverheden

In het commissiedebat Digitaliserende overheid van 22 april jl. heeft het lid Buijsse gevraagd of de IT-sourcingsstrategie ook beschikbaar kan worden gesteld aan medeoverheden. Ik werk hier stapsgewijs naartoe. Deze IT-sourcingsstrategie moet ons, als overheid, in staat stellen om risico-gebaseerd, verantwoord en uniform beslissingen te nemen over wat we inkopen en wie we contracteren. Hiermee verbeteren we de continuïteit van de IT-dienstverlening, verhogen we de weerbaarheid en bevorderen we een efficiënt gebruik van IT-diensten. De organisatorische

reikwijdte van deze strategie wordt stapsgewijs opgebouwd. De resultaten van de IT-sourcingstrategie worden eerst uitgewerkt voor de rijksoverheid (daarna met uitbreiding naar ZBO's en agentschappen) waarna er een overheidsbrede toepassing van de rijksbrede IT-sourcingstrategie wordt gevalideerd met als doel om aan te sluiten bij de overheidsbrede initiatieven.

2.1.5 Europees consortium digitale infrastructuur (EDIC)¹³

Uw Kamer is toegezegd dit voorjaar nader te worden geïnformeerd over het Europese consortium digitale infrastructuur (EDIC) voor digitale gemeenschapsgoederen, waarvan Nederland een oprichtende lidstaat zal zijn. Met onderstaande informatie doe ik die toezegging af.

Naar aanleiding van het rapport «Towards a Sovereign Digital Infrastructure of Commons», welke door 19 lidstaten waaronder Nederland, is opgesteld en ondertekend, bereiden Frankrijk, Duitsland en Nederland een aanvraag voor ten behoeve van de oprichting van een EDIC voor Europabrede digitale gemeenschapsgoederen. De doelstellingen van deze EDIC zijn onder andere het versterken van de Europese digitale soevereiniteit en het verminderen van technologische afhankelijkheden waarbij Europese waarden als privacy, transparantie en keuzevrijheid centraal staan. Een concreet gemeenschapsgoed waarop reeds wordt samengewerkt is de doorontwikkeling van werkplekomgeving «Mijn Bureau» (op basis van het Duitse OpenDesk en Franse LaSuite). De EDIC kan het vehikel gaan vormen om dergelijke samenwerkingen te bestendigen en op te schalen.

Sinds oktober 2023 heeft Nederland samen met Frankrijk de rol als co-voorzitter op zich genomen. De oprichting van de EDIC is in de laatste fase en de verwachting is dat de EDIC dit najaar statutair zal worden gevestigd in Parijs. De Europese Commissie heeft de toezegging gedaan 50% van de kosten te zullen financieren. De overige kosten zullen worden gedragen door de deelnemende lidstaten. Het is de uitdrukkelijke bedoeling om meer lidstaten te laten toetreden tot de EDIC. Naast Duitsland, Frankrijk en Nederland als oprichtende lidstaten, is er momenteel ook contact met een aantal andere lidstaten over mogelijke deelname.

2.1.6 Herinzet apparaten

In het commissiedebat Digitale Inclusie van 23 januari 2025 is uw Kamer toegezegd het kostenoverzicht van de keten van apparaten met een tweede leven te geven en daarbij in te gaan op de verschillende punten genoemd in het debat door het lid Kathmann.¹⁴ Hierna ga ik in op de kostprijs van de apparaten, de verwerkingstijd, of en hoeveel gratis apparaten er worden uitgegeven, hoeveel apparaten er worden verkocht, en de rol van dienst Domeinen Roerende Zaken (DRZ).

Het project herinzet apparaten is een aanpak waarbij er uitwerking wordt gegeven via publiek-, privaat- en maatschappelijke samenwerking aan het op een verantwoorde wijze hergebruiken van overheidsapparaten aan diegenen die de apparaten het hardst kunnen gebruiken.

Het lid Kathmann vroeg naar het kostenoverzicht van de keten van apparaten met een tweede leven. Kostprijs per apparaat:

- Totale kosten per laptop van € 80 bestaande uit:

¹³ TZ202501-151

¹⁴ TZ202502-015

- Licentiekosten¹⁵ € 24 per laptop
- All-in arbeidskosten¹⁶ € 65 per laptop
- Transportkosten (geschat) € 1 per laptop
- Bijdrage aanleverende instantie € 10 per laptop (kostprijsverlattend)

De verwerkingstijd die in de all-in arbeidskosten zijn opgenomen bestaat uit:

- Het ontvangen van de laptop,
- Het beoordelingstraject toetsen op werking, kwaliteit (A/B/C) vaststellen en type,
- Het verwijderen van de data op de laptop met genoemde licenties,
- Registratie werkzaamheden,
- Gereed maken voor afvoer.

Het lid Kathmann vroeg tijdens het debat ook hoeveel toestellen er gratis worden uitgegeven. Het doel is tussen de 8.000 en 10.000 apparaten per jaar te schenken aan mensen in financieel kwetsbare situaties, die momenteel geen toegang hebben tot digitale overheidsdiensten.

Daarnaast is gevraagd hoeveel toestellen worden doorverkocht. De dienst DRZ heeft tot en met de maand mei 4.768 toestellen met zeer diverse specificaties verkocht. Met verkoop geeft DRZ uitvoering aan de Regeling Materieel Beheer.¹⁷

Iedere Rijksoverheidsorganisatie dient overtollige roerende zaken bij DRZ in te leveren. Dit is wettelijk vereist zoals vastgelegd in de Regeling Materieel Beheer 2018. Daarnaast is het eventueel datavrij maken van deze overtollige roerende zaken/devices belegd bij DRZ. Devices worden door DRZ zoveel als mogelijk opnieuw ingezet doormiddel van verkoop, en indien verkoop niet mogelijk is, bijvoorbeeld bij oude of kapotte devices, worden de devices duurzaam verwerkt door deze te demonteren. Met de uiteenzetting op de genoemde punten van het lid Kathmann ten aanzien van de herinzet apparaten beschouw ik deze toezegging als afgedaan.

2.1.7 Uitstel verzending kamerbrief inzicht in rijksbrede digitalisering

Mijn voorganger heeft toegezegd u in het tweede kwartaal van 2025 te informeren over het verbeteren van het inzicht in rijksbrede digitalisering.¹⁸ Door vertragingen in het besluitvormingsproces lukt het helaas niet de Kamer deze brief voor het zomerreces toe te sturen. De verzending van de brief verschuift naar na het zomerreces.

2.1.8 Actueel overzicht gebruik verschillende onlineplatforms door de overheid¹⁹

In het debat over desinformatie en digitale inmenging op 16 januari 2025 heeft mijn voorganger toegezegd om een actueel overzicht op te stellen over het gebruik van verschillende onlineplatforms door de overheid. Er is

¹⁵ Per laptop wordt deze prijs vastgesteld door: 1,5 licentie * stuksprijs licentie € 16,21.

¹⁶ Er is een vastgesteld tarief voor all-in arbeidskosten van € 130 per uur. Per laptop is gerekend op 30 minuten wat neerkomt op € 65 aan all-in arbeidskosten per laptop. In dit all-in tarief zijn DRZ planning, administratieve en overige overheadkosten opgenomen.

¹⁷ De Regeling Materieel Beheer voorziet erin dat de financiële waarde van Rijksgoederen, die niet meer nodig zijn voor de beleids- cq bedrijfsuitvoering, terugvloeit naar de schatkist.

¹⁸ TZ202411–102. Zie ook: Kamerstukken II 2024/2025, 36600, VII 81 en Kamerstukken II 2024/2025, 26 643, nr. 1314

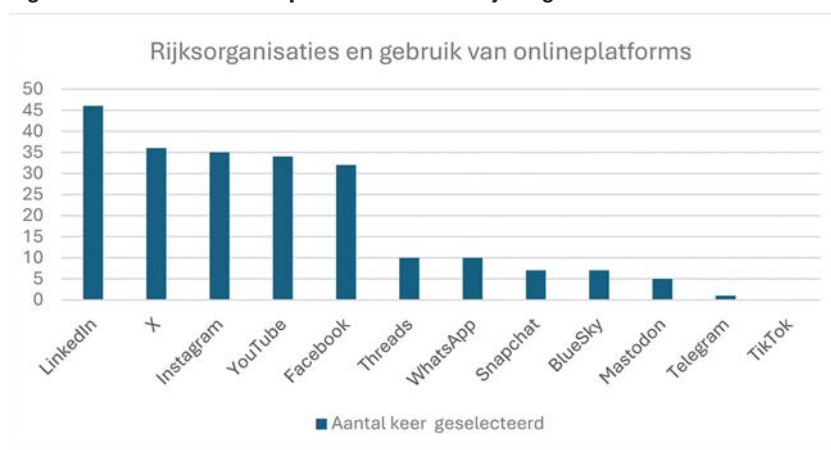
¹⁹ TZ202501-150

dit voorjaar een inventarisatie uitgevoerd onder de directies communicatie van 14 kerndepartementen en 34 publieke dienstverleners bij het Rijk naar de online sociale mediaplatforms waarop de rijksoverheid aanwezig is.

Verschillende organisaties gebruiken sociale media om met de juiste content op een efficiënte en laagdrempelige manier met hun doelgroepen te communiceren. Daarbij staan informatievoorziening aan- en contact met de burger en andere doelgroepen centraal. Sociale media worden ingezet voor publieksvoorlichting, informeren, gesprek en vraagbeantwoording (webcare), en luisteren naar de sentimenten, vragen en zorgen in de samenleving.

De 48 deelnemende organisaties geven aan op dit moment voornamelijk gebruik te maken van LinkedIn (46 organisaties), X (36 organisaties), Instagram (35 organisaties), YouTube (34 organisaties) en Facebook (32 organisaties). In mindere mate gebruiken zij Threads (10 organisaties), Whatsapp (10 organisaties), Snapchat (7 organisaties), BlueSky (7 organisaties), Mastodon (5 organisaties), Telegram (1 organisatie). Er wordt geen gebruik gemaakt van TikTok.

Figuur 1: Gebruik van onlineplatforms door 48 Rijksorganisaties



2.1.9 Geleerde lessen casus-NCTV en actualisatie VIRBI 2025

Op 31 januari heeft u de beantwoording van Kamervragen over het onderzoeksrapport Beveiligingsproces van staatsgeheime vertrouwelijke informatie bij NCTV en politie ontvangen vanuit het Ministerie van Justitie en Veiligheid.²⁰ Zoals uw Kamer daarin is toegezegd, ontvangt u de resultaten van de actualisatie van het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI). Hierin zijn de lessen uit de casus rondom de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) nadrukkelijk betrokken.²¹ In de beantwoording van de vragen is expliciet verwezen naar het belang om dergelijke lessen te verankeren in de toekomstige beveiligingsvoorschriften. Met het geactualiseerde VIRBI 2025 wordt hieraan invulling gegeven.

De aanscherpingen in het VIRBI 2025 richten zich op het versterken van de structurele en organisatorische waarborgen rondom de omgang met bijzondere informatie. Daarbij is specifieke aandacht besteed aan de

²⁰ Kamerstukken II 2024/2025, 2024Z21925

²¹ Toezegging in antwoord op vraag 25

volgende aandachtspunten, die direct voortkomen uit de bevindingen in de casus-NCTV:

- **Versterking van governance en verantwoordingsstructuren:** Door het verplicht hanteren van het three lines of defense-model wordt geborgd dat risico's rondom bijzondere informatie systematisch worden geïdentificeerd, gecontroleerd en beheerst. Dit voorkomt ongecontroleerde handelingsvrijheid en versterkt de interne toezichtslijn.
- **Striktere autorisatie en toegang:** Het VIRBI 2025 schrijft voor dat toegang tot bijzondere informatie enkel plaatsvindt op basis van need-to-know en strikt vastgestelde procedures. Personen dienen aantoonbaar geautoriseerd te zijn, inclusief een passende betrouwbaarheidstoets (VOG of VGB). Hiermee wordt ongeoorloofde toegang en verwerking voorkomen.
- **Verplicht risicogestuurd toezicht:** Door verplichte periodieke audits, reviews en accreditaties wordt structureel toezicht gehouden op de effectiviteit van beveiligingsmaatregelen. Bevindingen uit de NCTV-casus onderstrepen de noodzaak van dit cyclische toezicht.
- **Bewustzijn en cultuurverandering:** De casus maakte duidelijk dat naast technische en procedurele maatregelen ook gedragscomponenten cruciaal zijn. Daarom wordt vanuit het Ministerie van BZK een rijksbreed ondersteuningsprogramma opgezet dat zich naast implementatie van het VIRBI nadrukkelijk richt op bewustwording, normbesef en cultuurverandering in de omgang met bijzondere informatie.

Met deze maatregelen en uitgangspunten is beoogd om niet alleen de technische en organisatorische informatiebeveiliging te versterken, maar ook de cultuur en werkwijze binnen organisaties structureel te verbeteren. De geleerde lessen uit de NCTV-casus hebben op deze wijze concreet en integraal hun weg gevonden in het vernieuwde VIRBI 2025. Hiermee doe ik deze toezegging af.

2.2 (Digitale) Identiteit en Basisregistratie Personen

2.2.1 Onderzoeken MitID en vergelijkbare technologieën²²

In het debat over een digitaliserende overheid op 24 april jl. heeft het lid Kathmann gewezen op MitID, het Deense inlogmiddel. Zij wees erop dat dit middel gebruiksvriendelijker zou zijn dan DigiD en heeft gevraagd of DigiD in Nederland net zo zou kunnen werken als MitID. Tijdens het debat heeft mijn voorganger toegezegd om MitID en vergelijkbare technologieën te onderzoeken, en te bezien of en hoe hergebruik van uitgifte – en inlogmogelijkheden in Nederland mogelijk is. Met onderstaande informatie doe ik deze toezegging af.

De wijze waarop MitID is opgebouwd kenmerkt zich door de keuze die gebruikers hebben. Zowel bij de uitgifte van een MitID als het gebruik ervan. De uitgifte van een MitID is zowel digitaal (op afstand) mogelijk als bij (gemeente)loketten.²³ Gebruikers hebben een keuze in de wijze waarop zij MitID gebruiken: via de MitID app (verreweg de meest gebruikte optie), via een token, die per inlog een eenmalige code genereert of via een druppel met daarin een chip. De token kan tegen betaling worden aangeschaft door gebruikers die liever zonder smartphone inloggen, en biedt, voor mensen met een visuele beperking ook de variant om de inlogcode te laten voorlezen. De druppel met chip is tegen betaling aan te

²² TZ202504-147

²³ MitID is een privaat inlogmiddel ontwikkeld door de banksector in Denemarken. Deze is toegelaten binnen het publieke toegangsstelsel in Denemarken. Om deze reden is het ook mogelijk dat een loket zich in een bankkantoor kan bevinden.

schaffen en dient geactiveerd te worden met een identiteitsdocument of een identiteitsvaststelling aan de balie. De druppel biedt gebruikersgemak in de gevallen waarbij er zeer frequent moet worden ingelogd. Deze middelen kunnen gebruikers ophalen bij de gemeentebalie of digitaal aanvragen.

Doordat de combinatie van uitgifteprocessen (digitaal en balie) en gekozen inlogmethoden (app, token en druppel) in combinaties mogelijk zijn heeft de gebruiker verschillende mogelijkheden om MitID op betrouwbaarheidsniveau «substantieel» en «hoog» te activeren en te gebruiken.

Wanneer de MitID processen worden vergeleken met DigiD voor dezelfde betrouwbaarheidsniveaus, dan wordt DigiD op een andere manier geactiveerd en gebruikt. Op dit moment kunnen gebruikers van DigiD via een eenmalige handeling ophogen naar niveau «substantieel» middels het uitvoeren van een ID-check met een fysiek ID-document in de DigiD-app op een smartphone door middel van een NFC-lezer. DigiD op het niveau «hoog» is alleen beschikbaar via ID-check met een fysiek ID-document met een NFC-chip en bijbehorende PIN-code. Hierbij moet bij elke inlog een ID-check worden gedaan in de DigiD-app. Er zijn geen balieprocessen ingericht in Nederland waarbij een burger een inlogmiddel op een hoog betrouwbaarheidsniveau kan ophalen. Balieprocessen zijn complex en kostbaar en het inrichten van achterliggende dienstverlening heeft een lange doorlooptijd. Wel bieden de DigiD helpdesk en de Informatiepunten Digitale Overheid ondersteuning aan burgers die moeite hebben met de activatie of het gebruik van DigiD.

In Nederland zullen in de toekomst diensten op betrouwbaarheidsniveau «hoog» worden aangeboden. Dit gaat bijvoorbeeld gebeuren in de zorgsector, waar gevoelige gegevens van burgers worden verwerkt. Als we kijken naar middelen erkend op het hoogste betrouwbaarheidsniveau dan werken vrijwel de meeste landen in Europa met een fysiek ID-document met een chip en een bijbehorende PIN-code om deze te ontgrendelen.²⁴ De wijze van uitgifte verschilt per land. Dit kan bij een balie bij een gemeente, bank, politiebureau of postkantoor zijn. In veel landen is er ook een mogelijkheid om met gebruik van hardware in te loggen, waaronder de mogelijkheid om via een desktop in te loggen. De Wet digitale overheid (Wdo) en het te ontwikkelen Stelsel Toegang maakt het ook mogelijk dat private inlogmiddelen in de toekomst kunnen toetreden. De verwachting is dat een groter aanbod van inlogmiddelen zal leiden tot meer innovatie rondom activatie- en inlogmethoden.

Ik verken continu oplossingen om hogere betrouwbaarheidsniveaus bij DigiD toegankelijker te maken, met behoud van de bescherming die burgers geboden moet worden. Zo worden opties verkend om burgers zonder smartphone te helpen. De eerste is een desktopapplicatie van DigiD, waarbij de burger met behulp van een externe NFC-lezer kan inloggen. Dit vraagt een investering in uitgifte van NFC-lezers. Daarnaast wordt onderzocht of DigiD op het hoogste betrouwbaarheidsniveau bij de gemeentebalies uitgegeven kan worden. Bij de uitgifte is, zoals bij de uitgifte van een paspoort, een betrouwbare identiteitsvaststelling nodig, die door een gemeentebtenaar uitgevoerd zou kunnen worden. Dit vergt echter capaciteit van gemeentebaliemedewerkers en brengt financieringsvraagstukken met zich mee. Bij de doorontwikkeling van DigiD zal ik het Europese perspectief en lessen van onze buurlanden meenemen.

²⁴ Overview of pre-notified and notified eID schemes under eIDAS - eID User Community -

2.2.2 Meer regie voor burgers en ondernemers bij authenticatie en gegevensdeling

Op grond van de herziene *Electronic Identification and Trust Services* (eIDAS) verordening dienen lidstaten een Europese Digitale Identiteit (EDI)-wallet te verstrekken. Hiertoe ontwikkelt BZK de publieke EDI-wallet. EDI-wallets dragen bij aan een belangrijke transitie van de digitale overheid. Je rijvaardigheid of vakbekwaamheid aantonen kan in de toekomst, als burgers dat willen, met een EDI-wallet plaatsvinden. Om ervoor te zorgen dat dit betrouwbaar en veilig gebeurt, in verschillende toepassingen, publiek of privaat, online of offline, nationaal of binnen de Europese Unie, wordt gewerkt aan het opzetten van een Nederlands EDI-stelsel. Bekeken wordt hoe de verschillende rollen en voorzieningen in dat stelsel het beste hun beslag kunnen krijgen. Ik werk verder, naar analogie van het stelsel open toelating inlogmiddelen, aan een stelsel van open toelating voor EDI-wallets. Het Adviescollege ICT-toetsing heeft deze week een advies uitgebracht op dit dossier. Dit advies en de bestuurlijke reactie worden separaat naar uw Kamer gestuurd.

Sinds september 2024 worden in Europees verband verschillende technische vereisten en specificaties van de eIDAS-verordening nader uitgewerkt in uitvoeringshandelingen. De tweede set uitvoeringshandelingen heeft betrekking op o.a. de registratie van vertrouwende partijen, handelwijzen bij beveiligingsinbreuken en de wijze waarop lidstaten de identiteit van een burger koppelen zodra deze met een wallet inlogt bij een publieke dienstverlener. Nederland was het bij de behandeling van de uitvoeringshandeling over de registratie van vertrouwende partijen met de EDPS²⁵ en privacy belangengroepen eens dat de optionele, aanvullende privacybeschermende maatregelen EU-breed een verplicht karakter zouden moeten hebben. Het betreft het verplichte gebruik van zogenaamde registratiecertificaten, waarvan het gebruik nu door de lidstaat wordt bepaald. Door het optionele karakter van het gebruik van deze certificaten ontstaat een situatie waarin gebruikers van EDI-wallets in bepaalde lidstaten automatisch ondersteund kunnen worden met technische middelen om het risico op overvraging te verkleinen, terwijl die ondersteuning in andere lidstaten niet of minder goed kan worden verleend. Nederland heeft vanwege dit optionele karakter tegen de uitvoeringshandeling gestemd. Deze is met gekwalificeerde meerderheid aangenomen.

De tweede set is op 9 april 2025 met een gekwalificeerde meerderheid aangenomen door de lidstaten. In de komende maanden zullen nog meer sets aan uitvoeringshandelingen ter stemming worden gebracht in het kader van de comitologie van de Europese Commissie. De derde en vierde reeksen aan uitvoeringshandelingen gaan naar verwachting, op enkele na, over elektronische handtekeningen en zegels en vallen onder de verantwoordelijkheid van de Minister van Economische Zaken.

De eIDAS-verordening is rechtstreeks toepasselijk in Nederland. Wel is het nodig om de verordening nationaal op een aantal onderdelen verder te operationaliseren. Zo dient een toezichthouder te worden aangewezen en dient de inrichting en het beheer van een register voor vertrouwende partijen te worden geregeld.²⁶ Het kabinet bereidt hiertoe een uitvoeringswet voor. Deze uitvoeringswet borgt ook dat gebruikers van de Nederlandse publieke EDI-wallet op gelijke wijze toegang krijgen tot

²⁵ European Data Protection Supervisor

²⁶ Vertrouwende partijen zijn dienstverleners die bij hun dienstverlening vertrouwen op (gegevens uit) EDI-wallets.

publieke onlinedienstverlening als gebruikers van door andere lidstaten uitgegeven EDI-wallets.

2.2.3 Toekomstscenario's Identiteitskaart Bonaire, Sint-Eustatius en Saba

Eerder stuurde heeft uw Kamer een brief ontvangen over de wet invoering burgerservicenummer en voorzieningen digitale overheid in de openbare lichamen Bonaire, Sint Eustatius en Saba.²⁷ Hierin is uw Kamer toegezegd om het onderzoek wat is uitgevoerd naar de toekomstscenario's rondom de identiteitskaart op de openbare lichamen met deze brief mee te sturen. U vindt de gehele rapportage in bijlage 3. Een samenvatting van de rapportage in het Papiaments, Engels en Nederlands vindt u in bijlage 4. Op korte termijn ben ik niet voornemens om ingrijpende wijzigingen aan te brengen in de ID-kaart BES. Hiermee doe ik deze toezegging af.

2.2.4 Achterstand gegevenslevering reisdocumenten: technische oorzaak en oplossing

Tussen november 2024 en juli 2025 heeft zich een tijdelijk technisch probleem voorgedaan in de gegevensuitwisseling tussen het oude Basisregister Reisdocumenten en het onderliggende Verificatieregister, evenals in de gegevenslevering aan enkele ketenpartners. Dit probleem ontstond in de overgang naar het nieuwe Basisregister Reisdocumenten, waarbij een fout is opgetreden in de automatische doorlevering van gegevens vanuit het nieuwe register naar het oude.

Als gevolg hiervan zijn gedurende een periode ongeldig verklaarde documenten, zoals documenten van overleden personen of als vermist/gestolen opgegeven reisdocumenten, niet tijdig zichtbaar geweest voor enkele afnemers.

Het veiligheidsrisico is beperkt geweest. Voor zover bekend heeft zich geen misbruik voorgedaan en zijn er geen grootschalige continuïteitsproblemen ontstaan.

Het onderliggende technische probleem is inmiddels verholpen, de opgelopen achterstand is weggewerkt en de registers zijn weer volledig bijgewerkt.

2.3 Open data, openbaarheid van bestuur en informatiehuishouding

2.3.1 Motie Mohandis c.s. – Archiveerbaar maken van zakelijke en bestuurlijke

chatberichten van departementen²⁸

De motie van het lid Mohandis verzoekt de regering om voorafgaande aan de inwerkingtreding van de nieuwe Archiefwet te voorzien in een regeling voor het archiveerbaar maken van zakelijke en bestuurlijke chatberichten van departementen, en de Kamer hierover te informeren. Op 6 april 2023 heeft u een reactie op advies-rapporten over chatberichtenarchivering en informatiebeheer ontvangen.²⁹ Daarin zijn beleidspunten voor de Rijksdienst voor het archiveren van chatberichten van ambtenaren en bewindspersonen opgesteld. De hieruit voortvloeiende beleidslijn is op 1 april 2025 interdepartementaal vastgesteld. Hierin is ook de oplevering van een Rijksbrede voorziening voor de veiligstelling van chatberichten

²⁷ Kamerstukken II, 2024/2025, 36 639 nr. 16

²⁸ Kamerstukken II 2024/2025, 35 968, nr. 35

²⁹ Kamerstukken II 2022/2023, 32 802, nr. 67

opgenomen. Deze wordt medio 2026 verwacht en is in lijn met de motie van het lid Mohandis.

2.3.2 Voortgang afhandeling datalek in gepubliceerde documenten van de rijksoverheid

Onlangs heb is uw Kamer geïnformeerd over een datalek waardoor persoonsgegevens van ambtenaren achterhaald kunnen worden uit de metadata van gepubliceerde documenten.³⁰ Daarin is toegezegd uw Kamer voor de zomer over de voortgang op dit dossier te informeren. Met onderstaande informatie doe ik die toezegging af. Inmiddels zijn alle openbare publicaties in de (overheids)publicatiedomeinen die door het Kennis- en exploitatiecentrum Officiële Overheidspublicaties (KOOP) worden beheerd (waaronder open.overheid.nl en officielebekendmakingen.nl) zorgvuldig geanalyseerd. Hieruit blijkt dat 30% van de gepubliceerde documenten van ministeries op open.overheid.nl persoonsgegevens bevat. Op dit moment wordt de metadata van de betreffende documenten centraal opgeschoond van persoonsgegevens. In totaal gaat het om 230.000 documenten die opgeschoond moeten worden. Hiervan zijn op het moment van schrijven inmiddels 200.000 opgeschoond en teruggeplaatst.

Bij opschoning wordt alleen de strikt noodzakelijke metadata weggehaald; metadata die nodig is ten behoeve van digitale toegankelijkheid zullen zoveel mogelijk onaangepast blijven. In de metadata van elk opgeschoond document wordt opgenomen dat het een opgeschoond document betreft, zodat duidelijk blijft welke documenten zijn aangepast. Ook is er monitoring ingericht, waarmee nieuwe publicaties op rijksoverheid.nl worden gecontroleerd op de aanwezigheid van persoonsgegevens. Daarnaast zal een generieke tool beschikbaar worden gesteld aan alle aanleveraars van documenten van de rijksoverheid om persoonsgegevens uit documenteigenschappen te verwijderen vóór publicatie. Ten slotte wordt met KOOP gekeken of voor de actieve openbaarmaking van documenten een tool beschikbaar kan komen voor het centraal strippen van persoonsgegevens uit metadata.

3. Digitale Samenleving

3.1 Nieuwe en opkomende technologieën

3.1.1 Voortgang en financiering van Innovation Center for Artificial Intelligence (ICAI) labs³¹

In het commissiedebat over opkomende en toekomstige technologieën van 30 januari 2025 heeft mijn voorganger uw Kamer toegezegd u te informeren over de voortgang en financiering van de *Innovation Center for Artificial Intelligence* (ICAI) labs. Dit naar aanleiding van de vraag van het lid Kathmann. Het ICAI is een goed voorbeeld van publieke-private samenwerking voor het versterken van AI-kennis, innovatie en onderzoekstalent. Inmiddels zijn er meer dan 50 labs opgezet waarin universiteiten en veelal bedrijven vraag gestuurd samenwerken aan specifieke AI-uitdagingen. Er zijn ook publieke organisaties in labs actief, zoals de Nationale Politie. Er zijn circa 17 ICAI-labs mede mogelijk gemaakt door een financiële bijdrage van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) (€ 13,1 mln.) en het Ministerie van Economische Zaken (€ 7,5 mln.) in het kader van de eerste fase (2022–2027) van het programma *Trustworthy AI-based Systems for Sustainable Growth*

³⁰ Kamerstukken II 2024/2025, 32 761, nr. 319

³¹ TZ202502–135

(ROBUST). De NWO heeft € 11,9 mln. gereserveerd voor de tweede fase (2027–2032) van het programma ROBUST. Het plan van de tweede fase moet nog nader worden uitgewerkt en goedgekeurd. Met deze informatie beschouw ik de toezegging aan uw Kamer als afgedaan.

3.1.2 Publicatie UNESCO rapportage – Readiness Assessment Methodology (RAM) AI Ethiek

In de verzamelbrief van juni 2024 kondigde het kabinet aan het Nederlandse AI-beleid te laten toetsen aan de UNESCO Aanbeveling over de Ethiek van AI volgens UNESCO's *Readiness Assessment Methodology* (RAM), waarin zowel kwalitatieve als kwantitatieve indicatoren aan bod komen. Nederland heeft als eerste EU-lidstaat een dergelijk onderzoek afgerond.³² De resultaten van het onderzoek zijn positief: Nederland is vergevorderd met het ontwikkelen van beleidsinstrumenten voor de ethische ontwikkeling en inzet van AI-systemen. Goede voorbeelden zijn het Algoritmeregister en het Impact Assessment Mensenrechten en Algoritmes (IAMA), en het bestaande kader van Europese wet- en regelgeving. Het RAM-rapport bevat een tiental aanbevelingen voor Nederland, waarop is gereageerd langs de lijnen van bestaand en toekomstig AI-beleid van het kabinet. UNESCO heeft het RAM-rapport gepubliceerd.³³ Hierdoor kunnen andere landen inspiratie ontleen aan Nederlandse beleidsinstrumenten, en draagt het rapport bij aan de totstandkoming van een wereldwijd totaaloverzicht van AI-beleid in alle UNESCO-lidstaten. Tevens geldt de RAM als de Nederlandse inbreng in de eerste vierjaarlijkse monitoringronde van de uitvoering van de Aanbeveling, een belangrijke bouwsteen in de ontluikende mondiale AI-governance.

3.1.3 Opkomende technologieën

Nieuwe digitale technologieën ontwikkelen zich snel en hebben grote invloed op hoe we met elkaar leven en werken. De overheid heeft een rol als aanjager van nieuwe technologie en om kansen hiervan te benutten, maar ook om risico's voor burgers, bedrijven en overheden te beheersen.

Om te beoordelen wat de overheid kan doen om kansen te benutten en risico's te minimaliseren is het Rathenau Instituut gevraagd om technologiescans uit te voeren naar immersieve technologie en neurotechnologie. Hierin brengt het Rathenau Instituut in kaart in hoeverre het huidige Nederlandse beleid toereikend is en worden enkele handelingsopties gegeven. Deze onderzoeken kunt u vinden op de website van het Rathenau Instituut.^{34, 35}

Immersieve technologie, zoals virtual reality (VR) en augmented reality (AR), wordt vaak gebruikt om realistische of interactieve ervaringen te bieden, bijvoorbeeld in het onderwijs, in de zorg en in games. Het Rathenau Instituut geeft in het rapport een aantal handelingsopties voor overheden als suggesties voor het in goede banen leiden van de verdere introductie van immersieve technologie in de samenleving. Het is goed om te constateren dat er al veel wordt gedaan om kansen te verzilveren en risico's te verminderen. De uitkomsten van het onderzoek van het Rathenau Instituut worden inmiddels als leidraad gebruikt door de Creative Industries Immersive Impact Coalition (CIIC). CIIC wordt mede mogelijk gemaakt door het Nationaal Groeifonds. Hier wordt ingezet op

³² Verzamelbrief Digitalisering juni 2024 | Kamerstuk | Rijksoverheid.nl

³³ Netherlands | Global AI Ethics and Governance Observatory

³⁴ Rathenau scan: Immersieve technologieën

³⁵ Rathenau scan: Neurotechnologie

de verantwoorde ontwikkeling van immersieve technologie. Ik blijf de ontwikkeling van deze technologie volgen en zal beleidsaanpassingen voorstellen wanneer nodig.

Neurotechnologie is ook in veel domeinen toe te passen waaronder gezondheid, onderwijs, veiligheid, werk en defensie. UNESCO stelt momenteel een aanbeveling op over hoe lidstaten om kunnen gaan met de kansen en risico's van neurotechnologie. Deze aanbeveling zal dit najaar worden aangenomen tijdens de Algemene Vergadering van UNESCO. Ik zal uw Kamer in het voorjaar van 2026 verder informeren over de aanbeveling en hoe Nederland omgaat met de ontwikkelingen omtrent neurotechnologie. Hierbij zal ik ook de handelingsopties betrekken die het Rathenau Instituut in het rapport meegeeft.

Nieuwe technologieën komen in hoog tempo op ons af. Ze bieden vaak kansen voor bijvoorbeeld effectiviteit of veiligheid, maar ook risico's voor bijvoorbeeld privacy. Ik vind het belangrijk om deze ontwikkelingen goed in de gaten te houden. Daarom is TNO gevraagd om een technologieforecast te ontwikkelen. Dit is een brede voorspelling om te zien wat nieuwe technologische ontwikkelingen zijn en welke impact deze kunnen hebben op de Nederlandse overheid en samenleving. Mede op basis hiervan kunnen we bepalen of het kabinetsbeleid toereikend is om kansen te pakken en risico's te beperken. De eerste rapportage verwacht ik dit jaar aan uw Kamer te kunnen sturen. Ook werk ik aan een actie-agenda die mij in staat stelt om samen met het bedrijfsleven te werken aan de verantwoorde ontwikkeling en inzet van nieuwe technologie in Nederland. Ik verwacht u hierover in de eerste helft van 2026 te kunnen informeren.

3.2 Onlineplatforms

3.2.1 Motie Kathmann – Maximale naleving, handhaving en versteviging van regelgeving ten aanzien van grote onlineplatforms³⁶

Tijdens het tweeminutendebat desinformatie en digitale inmenging van 19 maart 2025 diende het lid Kathmann een motie in waarin de regering werd verzocht om bij de Europese Commissie blijvend en ondubbelzinnig aan te dringen op maximale naleving, handhaving en waar nodig versteviging van regelgeving ten aanzien van grote onlineplatforms, ongeacht druk van buitenaf. Kamerlid Kathmann verzocht de regering daarbij te verkennen wat EU-lidstaten kunnen doen om deze regelgeving zelf steviger te handhaven in het geval dat de Commissie niet of niet snel genoeg optreedt, en de uitkomsten vóór het zomerreces met de Kamer te delen.

Zoals aangegeven tijdens het tweeminutendebat zet de regering zich binnen de EU actief in om ervoor te zorgen dat de Commissie daadkrachtig optreedt tegen zeer grote onlineplatforms en zeer grote onlinezoekmachines die zich niet aan de EU-wetgeving houden. Tevens heeft Nederland met tien andere lidstaten een brief gestuurd aan de Commissie waarin wordt gevraagd volledig gebruik te maken van de handhavingscapaciteiten van de DSA. Er is gesproken met Eurocommissaris Virkkunen, die verantwoordelijk is voor de uitvoering van de Digital Services Act (DSA) en de Digital Markets Act (DMA). Tijdens dit gesprek is, in lijn met de motie Kathmann, aandacht gevraagd voor de maximale naleving van, en handhaving op de zeer grote onlineplatforms en de zeer grote onlinezoekmachines. Zoals de Europese Commissie in openbare uitingen heeft aangegeven, werken ze intensief aan lopende dossiers binnen de DMA en DSA. Inmiddels heeft de Commissie ook daadwerkelijk

³⁶ Kamerstukken II 2024/2025, 30 821, nr. 264

handhavingsbesluiten genomen, waaronder het opleggen van boetes aan Apple en Meta wegens overtredingen van de DMA.³⁷ Ik beschouw dit als een duidelijke bevestiging dat de Commissie haar toezichthoudende rol doeltreffend opneemt.

Verder mocht het tweede gedeelte van de motie zo geïnterpreteerd worden dat de nationale handhavingsautoriteiten ondersteund dient te worden in het geval dat de Commissie niet of niet snel genoeg optreedt. Daarbij blijft het essentieel dat de nationale toezichthouders, zoals de Autoriteit Consument en Markt (ACM) en de Autoriteit Persoonsgegevens (AP), hun taken onafhankelijk van de regering kunnen blijven uitvoeren. Ik blijf in gesprek met zowel de Europese Commissie als de nationale toezichthouders, volg de handhavingsontwikkelingen, en bied waar mogelijk ondersteuning. Hiermee geef ik uitvoering aan de motie van het lid Kathmann.

3.2.2 Motie Van der Werf en Six Dijkstra – Richtgetal voor de (relatieve) moderatiecapaciteit op Nederlands niveau van grote online platforms³⁸

Tijdens het wetgevingsoverleg van 11 november 2024 dienden de leden Van der Werf en Six Dijkstra een motie in waarin de regering wordt verzocht te verkennen of kan worden gekomen tot een richtgetal voor (relatieve) minimum moderatiecapaciteit op Nederlands niveau van grote online platforms en de Tweede Kamer hierover voor de zomer te informeren.³⁹ Door de Digitale dienstenverordening (DSA) geldt maximumharmonisatie. Daarnaast bevat de DSA geen verplichtingen om voldoende personeel aan te nemen voor contentmoderatie. Lidstaten kunnen op dit vlak dan ook geen aanvullende nationale wetgeving vaststellen. Eventuele wijzigingen in de DSA kunnen na de evaluatie in 2027 volgen. Om alvast te kijken naar de wettelijke mogelijkheden binnen de DSA na de evaluatieperiode, alsook om niet-juridische mogelijkheden te verkennen, is een onderzoek uitgezet naar het gebruik van normen voor contentmoderatie. De resultaten hiervan verwacht ik dit najaar en zal ik dan met uw Kamer kunnen delen.

3.2.3 Moties Kathmann en Van der Werf – Komen tot één nationale richtlijn over verantwoorde schermtijd en telefoongebruik en een bijsluiter^{40, 41}

De leden Kathmann en Van der Werf hebben de regering verzocht om samen met jongeren en experts op het gebied van gezondheid, jeugd en media te komen te één nationale richtlijn over verantwoorde schermtijd en telefoongebruik voor verschillende leeftijden. Het Ministerie van Volksgezondheid, Welzijn en Sport heeft op 17 juni jl. de Richtlijn gezond en verantwoord scherm- en sociale mediagebruik naar uw Kamer verzonden. Hiermee is de motie Kathmann c.s.⁴² afgedaan. Vanuit het Ministerie van BZK gaat in het najaar van dit jaar een meerjarige publiekscampagne over digitale opvoeding starten, die gericht is op bewustwording bij ouders over het gebruik van digitale middelen en diensten door hun kinderen. De richtlijn gezond en verantwoord scherm- en sociale mediagebruik van VWS zal mee worden genomen in het eerste jaar van deze publiekscampagne. In het kader van deze campagne wordt

³⁷ Commission finds Apple and Meta in breach of the Digital Markets Act

³⁸ Kamerstukken II 2024/2025, 36 600 VII, nr. 112

³⁹ Kamerstuk 36 600 VII, nr. 73

⁴⁰ Kamerstukken II 2024/2025, 36 600 VII, nr. 72

⁴¹ Kamerstuk II 2024/2025, 36 600 VII, nr. 74

⁴² Kamerstukken II 2024/2025, 36 600 VII, nr. 72

de mogelijk tot een bijsluiter bij de verkoop van apparaten als smart-phones en tablets verkend.

3.2.4 Financiering alternatieve sociale media⁴³

Tijdens het commissiedebat Online Kinderrechten op 19 december 2024 is uw Kamer toegezegd om geïnformeerd te worden over de financiering van alternatieve sociale media. Het afgelopen jaar zijn vanuit het programma Digitale Gemeenschapsgoederen verschillende alternatieve socialemediaplatforms ondersteund om de digitale autonomie en weerbaarheid van de overheid te versterken. Zo is een Mastodon instantie (social.overheid.nl) ingericht als extra communicatiekanaal en is in samenwerking met het SIDN-fonds geïnvesteerd in de doorontwikkeling PeerTube (een alternatief videodeelplatform) en Pubhubs (een alternatief communicatieplatform) voor veilige en verifieerbare digitale interactie. Tot slot zijn vanuit het Innovatiebudget Digitale Overheid verschillende landelijke en lokale opensource digitale participatieprojecten gesteund met cofinanciering, begeleiding en zichtbaarheid, zoals OpenStad en Pol.is. Dit gaat om investeringen van één tot tweehonderdduizend euro, vaak in samenwerking met andere overheden.

Met de huidige financiering zijn belangrijke stappen gezet in het verkennen en ontwikkelen van innovatieve en veilige digitale communicatiemogelijkheden. De vraag is of tijdelijke financiering voldoende is voor structurele levensvatbaarheid. Voor een succesvolle toepassing is het van belang dat overheden deze alternatieven actief benutten wanneer zij bijdragen aan betere dienstverlening en een veiliger digitaal landschap. In de komende periode zal daarom worden geëvalueerd of verdere investeringen nodig zijn om de meerwaarde op het gebied van dienstverlening, weerbaarheid en autonomie te borgen. Tot slot wordt ook in Europees verband samengewerkt aan alternatieve oplossingen om de digitale communicatiemogelijkheden van overheden te versterken. Daarmee is deze toezegging afgedaan.

3.2.5 Opzetten van een meldpunt ten behoeve van onlineplatforms

Tijdens het debat over desinformatie en digitale inmenging van 16 januari is de Kamer toegezegd om de Kamerleden te informeren over het opzetten van een meldpunt ten behoeve van onlineplatforms, oftewel een geschillenbeslechtsmechanisme.⁴⁴ Ik laat momenteel een scenario-analyse uitvoeren om de juridische voorwaarden voor een geschillenbeslechtsmechanisme, zoals voorgeschreven in de DSA, in kaart te brengen en om verificatie te verkrijgen van de nationale toezichthouder, de ACM.⁴⁵ Deze scenarioanalyse houdt rekening met verschillende relevante indicatoren, bestaande ervaringen van andere geschillenbeslechtsorganen en de certificatievoorwaarden die van toepassing zijn. Gezien de complexiteit van dit vraagstuk en de zorgvuldigheid die hierbij vereist is, is meer tijd nodig gebleken voor de afronding. De uitkomsten van deze analyse worden dit najaar verwacht en kan ik dan met uw Kamer delen.

⁴³ TZ202501-017

⁴⁴ TZ202501-149

⁴⁵ Kamerstukken II 2023/2024, 30 821, nr. 230

3.2.6 Middelen voor de handhaving van de Digitale dienstenverordening (DSA) en Digitale marktenverordening (DMA)⁴⁶

Tijdens het tweeminutendebat desinformatie en digitale inmenging van 19 maart jl. is met uw Kamer gesproken over een verhoging van de middelen voor de handhaving van de DSA en de DMA. Gelet op dat gesprek wil ik uw Kamer graag van meer informatie voorzien. In het debat is al aangegeven dat de Minister van Economische Zaken over dit onderwerp in contact is met de nationale toezichthouders Autoriteit Consument en Markt (ACM) en Autoriteit Persoonsgegevens (AP).

Met betrekking tot het nationale toezicht is de ACM belast met een aanzienlijk deel van het toezicht op de DSA. De ACM beschikt momenteel over voldoende middelen om deze DSA handhavingstaken uit te voeren. Voor de AP zijn ter uitvoering van amendement 36531–15 middelen van de ACM gerealloceerd naar de AP ten behoeve van 2 fte. Dit is nodig omdat de AP door dit amendement een taak van de ACM heeft gekregen. Over aanvullende middelen voor de AP wordt definitief besloten bij de Prinsjesdag besluitvorming. Hierbij heeft de Europese Commissie (hierna: de Commissie) de mogelijkheid om de kosten van dit toezicht te verhalen op de betreffende sector. Ook voor het nationale toezicht op de DMA geldt dat dit is belegd bij de ACM. De ACM beschikt momenteel ook over voldoende middelen om haar ondersteunende rol als nationaal bevoegde autoriteit onder de DMA goed te vervullen.

Ten aanzien van het Europese niveau beslist de Commissie zelf over haar middelenverdeling voor toezicht op de DSA. Zo breidt de Commissie haar capaciteit als toezichthouder momenteel met 60 fte aanzienlijk uit. De Commissie kan haar gemaakte kosten dekken met de jaarlijkse toezichtsvergoedingen die zij ontvangt van de zeer grote onlineplatforms en zeer grote online zoekmachines. Hiermee worden de kosten die de Commissie maakt in verband met haar DSA-toezichtstaken gedekt. In 2024 bedroeg dit € 50,11 miljoen. De Commissie gaat ook over haar eigen middelenverdeling voor toezicht op de DMA en heeft hiervoor aanzienlijke middelen beschikbaar gesteld. Er zijn vooralsnog geen signalen dat deze middelen ontoereikend zijn. Of de capaciteit van de Commissie voor het DMA-toezicht op lange termijn voldoende is, zal in de evaluatie van de DMA in 2026 worden meegenomen.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum

⁴⁶ Tweeminutendebat Desinformatie en digitale inmenging (CD 16/1) | Tweede Kamer der Staten-Generaal