

Commissie voor Economie,
Consumentenbescherming en
Digitalisering

Commission de l'Économie, de la
Protection des consommateurs et de
la Digitalisation

van

du

WOENSDAG 19 NOVEMBER 2025

MERCREDI 19 NOVEMBRE 2025

Namiddag

Après-midi

La réunion publique de commission est ouverte à 14 h 17 et présidée par M. Roberto D'Amico.
De openbare commissievergadering wordt geopend om 14.17 uur en voorgezeten door de heer Roberto D'Amico.

Les textes figurant en italique dans le Compte rendu intégral n'ont pas été prononcés et sont la reproduction exacte des textes déposés par les auteurs.

De teksten die cursief zijn opgenomen in het Integraal Verslag werden niet uitgesproken en steunen uitsluitend op de tekst die de spreker heeft ingediend.

01 **Samengevoegde vragen van**

- Alexander Van Hoecke aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "Smishing" (56009848C)

- Serge Hiligsmann aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "Smishing" (56010638C)

01 **Questions jointes de**

- Alexander Van Hoecke à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le "smishing"" (56009848C)

- Serge Hiligsmann à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'hameçonnage par sms" (56010638C)

01.01 **Alexander Van Hoecke (VB):** Mijnheer de voorzitter, ik verwijs naar de schriftelijke versie van mijn vraag.

Pogingen tot fraude via sms of Whatsapp-berichten komt steeds vaker voor. Potentiële slachtoffers krijgen een bericht waarin criminelen zich voordoen als een bank, een leverancier, een overheidsorganisatie of zelfs familieleden. Het is een vorm van phishing die ook wel eens 'smishing' wordt genoemd.

Telecomproviders houden een deel van de fraudeberichten zelf tegen. Bij Telenet stelde men in 2024 dat het om 25 berichten per minuut gaat. Naar eigen zeggen is ook de filter die Proximus gebruikt succesvol. Voormalig minister van Telecommunicatie Petra De Sutter stelde dat ook Orange de software zou beginnen gebruiken in 2025.

De technologie werd deels gesubsidieerd vanuit de federale overheid. Daarvoor werd in 2022 een subsidie van twee miljoen euro toegekend aan Telenet en Proximus.

Welke telecomproviders maken vandaag gebruik van de filtersoftware?

Hoe wordt de effectiviteit van de filtersoftware opgevolgd? Rapporteren de telecomproviders hierover en op welke manier?

Wordt er ook op Europees niveau samengewerkt en informatie uitgewisseld om fraudeberichten via

sms tegen te gaan?

Bestaat er ook een samenwerking met aanbieders van berichtenapps zoals WhatsApp om phishing tegen te gaan? Zo ja, welke vorm neemt deze samenwerking aan?

01.02 **Serge Hiligsmann** (Les Engagés): Madame la ministre, les tentatives de fraude par SMS ou via des applications de messagerie instantanée, telles que WhatsApp, connaissent une croissance préoccupante.

Afin de lutter contre ces pratiques souvent qualifiées de *smishing*, plusieurs opérateurs télécoms belges ont mis en place un logiciel de filtrage visant à bloquer automatiquement une partie des messages frauduleux. Nos trois questions très concrètes sur le sujet sont les suivantes:

Quels sont aujourd'hui à l'aube de 2026 les opérateurs télécoms belges qui utilisent effectivement ce logiciel de filtrage des SMS frauduleux? Combien de messages frauduleux sont-ils captés par les opérateurs télécoms belges? Les opérateurs télécoms doivent-ils transmettre des rapports réguliers concernant le nombre de messages bloqués, le taux de détection ou les éventuels faux positifs?

01.03 **Minister Vanessa Matz**: Geachte Kamerleden, Telenet en Proximus hebben in 2024 samen 37 miljoen frauduleuze sms-berichten tegengehouden. Daardoor krijgen de gebruikers veel minder valse berichten binnen, en we zien dat de fraudeurs steeds minder sms kunnen gebruiken.

Orange utilise le même type de logiciel de filtrage. L'IBPT se réunit chaque trimestre avec les opérateurs télécom. Ces réunions permettent d'échanger des informations sur les systèmes de filtrage, sur les nouvelles formes de fraude observées et sur les mesures possibles.

Slechts een paar Europese landen gebruiken dezelfde soort filtersoftware als België. Bij sms lukt filteren goed omdat het om een open systeem gaat.

Pour WhatsApp, c'est différent: les messages sont chiffrés de bout en bout. Seul l'émetteur et les destinataires peuvent les lire. Les opérateurs ne peuvent donc pas analyser le contenu.

Om fraude te detecteren, zou op het toestel van de gebruiker zelf moeten kunnen worden gescand.

C'est très controversé. Cela affaiblirait le chiffrement, porterait atteinte à la vie privée et créerait des risques d'abus et de faux positifs.

Het debat loopt momenteel op Europees niveau in het kader van de nieuwe CSAM-wetgeving.

En Belgique, nous travaillons en étroite collaboration avec les services compétents. Le CCB avertit les citoyens des risques de fraude et renforce leur résilience numérique grâce à des campagnes de sensibilisation et de formation.

Het CCB werkt onder meer samen met het BIPT en de FOD Economie om frauduleuze websites te blokkeren en met banken om sneller in te grijpen wanneer criminelen via fraude geld proberen te stelen.

Nous avons réalisé des avancées importantes mais la fraude en ligne évolue sans cesse.

Daarom moet onze aanpak mee evolueren. Op politiek niveau is er een werkgroep actief tegen online fraude, waarin mijn kabinet erg betrokken is. Waar mogelijk nemen we extra maatregelen.

01.04 **Alexander Van Hoecke** (VB): Dank u wel, mevrouw de minister, voor uw antwoord. Het was zeer interessant.

U hebt aan het begin een aantal cijfers vermeld. Kunt u die schriftelijk bezorgen? Ik heb ze immers niet exact genoteerd. Wanneer ik kijk naar berichten die ik soms ontvang, stel ik vast dat het probleem zich blijft voordoen. Ik denk ook dat het bijzonder belangrijk is dat we die samenwerking op Europees niveau effectief blijven nastreven.

Als ik het goed begrijp, wordt de software die de telecomproviders vandaag gebruiken deels

gesubsidieerd door de overheid. Dat is althans wat uw voorgangster, minister Petra De Sutter, destijds heeft verklaard. Het lijkt me dan ook opportuun om na te gaan of andere Europese landen eventueel ook met die software aan de slag kunnen. Ze bestaat nu immers toch.

We kunnen ook kijken naar wat we eventueel nog kunnen leren van andere Europese landen in de strijd tegen smishing. Het betreft namelijk een zeer specifieke vorm van phishing, maar ik acht die ook zeer gevaarlijk. Veel mensen hebben namelijk de reflex om een e-mail te wantrouwen, maar om een of andere reden wantrouwen zij een sms veel minder. We moeten daarvoor zeker waakzaam blijven en dat probleem blijven aanpakken.

Dank u wel.

01.05 Minister **Vanessa Matz**: Het gaat om 37 miljoen frauduleuze sms-berichten.

01.06 **Alexander Van Hoecke** (VB): Voor alle providers?

01.07 Minister **Vanessa Matz**: Voor Telenet en Proximus.

01.08 **Alexander Van Hoecke** (VB): Oké, bedankt.

01.09 **Serge Hiligsmann** (Les Engagés): Madame la ministre, je vous remercie pour vos réponses et vous assure de notre confiance en vos services pour lutter contre ces pratiques tant frauduleuses que dangereuses, particulièrement pour notre jeunesse et les personnes les plus fragilisées.

*Het incident is gesloten.
L'incident est clos.*

02 **Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De gegevenssoevereiniteit" (56009923C)**

02 **Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La souveraineté des données" (56009923C)**

02.01 **Dieter Keuten** (VB): Mevrouw de minister, ik heb een vraag over gegevenssoevereiniteit.

In de Verenigde Staten bestaat de zogenoemde Cloud Act. Die wetgeving roept vragen op over het extraterritoriale bereik. Tijdens een hoorzitting in Frankrijk deze zomer verklaarde een jurist van Microsoft onder ede dat het bedrijf niet kon garanderen dat gegevens van de Franse of Europese overheid die in de cloud zijn opgeslagen niet onder bepaalde omstandigheden met de Amerikaanse autoriteiten worden gedeeld. In Schotland werd dit inmiddels bevestigd in een brief van Microsoft aan de Schotse autoriteiten.

Daarom heb ik enkele vragen aan u, mevrouw de minister.

In welke mate maken de overheidsdiensten onder uw bevoegdheid gebruik van cloudoplossingen van Amerikaanse dienstverleners? Die vraag is bijzonder relevant in het licht van wat er zich gisteren heeft voorgedaan bij Cloudflare.

Hoeveel van uw overheidsdiensten maken specifiek gebruik van cloudoplossingen van Microsoft, zoals Microsoft 365 en Azure?

Microsoft heeft aangegeven zijn klanten op de hoogte te zullen brengen als het aanvragen van de Amerikaanse autoriteiten zou ontvangen om in het kader van de Cloud Act gegevens te delen. Hebben de Belgische overheidsdiensten al dergelijke meldingen ontvangen?

Volgens het regeerakkoord zou een volwaardige *datagovernance* worden opgezet in het kader van de Belgische datastrategie en de *cloud-first strategy*. Wat is de stand van zaken van deze strategieën en van die *datagovernance*? Maakt de Belgische of Europese datasoevereiniteit – een *sovereign cloud*

policy – deel uit van de *datagovernance* die u nastreeft?

Ten slotte, in het plan Digitale Soevereiniteit wordt verwezen naar eigen infrastructuur, zoals datacenters, en naar een transversaal plan voor de invoering van cloudgebruik binnen de federale instellingen. Graag kreeg ik een stand van zaken van deze plannen en intenties, zoals opgenomen in het regeerakkoord en in uw beleidsverklaring.

02.02 Minister **Vanessa Matz**: Mijnheer Keuten, de federale overheidsdiensten gebruiken soms Amerikaanse clouddiensten voor basisdiensten zoals digitale werkplekken en samenwerkingstools. Dit gebeurt altijd binnen een strikt kader. De contracten moeten voldoen aan de GDPR. De gegevens moeten in Europese datacenters worden opgeslagen. Alle leveranciers moeten aan de federale veiligheidsvereisten voldoen. Microsoft 365 en enkele Azurediensten worden op die manier gebruikt. Er bestaat echter geen centrale lijst van de overheidsdiensten die deze oplossingen gebruiken.

Tot nu toe is er geen enkele melding gemaakt van een aanvraag of een melding in het kader van de Cloud Act.

Wat het Belgische databeleid en de *cloud-first strategy* betreft, wordt er momenteel gewerkt aan een federale *datagovernance*. Daarbij wordt ook met de (...) gegevenssoevereiniteit rekening gehouden. Binnen de federale administratie bestaan al meerdere initiatieven en overlegplatformen die werken aan een beter databeleid, *datagovernance* en het valoriseren van data. Het doel is om te komen tot een nationale en coherente datastrategie.

Daarnaast wordt een federale cloudstrategie verder uitgewerkt. Die moet ervoor zorgen dat de overheidsdiensten de cloudtechnologie op een veilige, consistente en gecontroleerde manier gebruiken. Een speciale taskforce werkt aan een beslissingsboom. Die moet helpen bepalen of data al dan niet naar de cloud mogen verhuizen.

Tot slot werkt men aan een analyse over het samenbrengen van de verschillende federale datacenters. Het doel is de eigen capaciteit van de overheid te versterken, de veerkracht te verbeteren en de huidige versnippering van de infrastructuur te verminderen.

02.03 **Dieter Keuten** (VB): Dank u wel voor uw antwoorden, mevrouw de minister.

U verwees naar de GDPR en naar het feit dat de data die in cloudtoepassingen door de overheid gebruikt en verwerkt worden opgeslagen moeten worden in datacenters die op Europees grondgebied staan. Ik meen echter dat dit geen garantie biedt dat ze niet onder de Cloud Act vallen, want ook al bevinden die datacenters zich op Europees grondgebied, als daar software op draait die uit de Verenigde Staten komt, valt die nog steeds onder de Cloud Act. We riskeren dus dat de Amerikaanse autoriteiten aan gevoelige Europese data kunnen komen zonder dat wij of Europa daar iets tegen kunnen doen.

U hebt me dus helaas niet kunnen geruststellen. Er is blijkbaar ook geen goed zicht op welke overheidsdiensten gebruikmaken van cloudoplossingen en van welke aanbieder. Door de Cloudflare storing van gisteren bijvoorbeeld zijn er ongetwijfeld overheidsdiensten geraakt, maar er is blijkbaar geen inventaris van welke overheidsdiensten gebruikmaken van welke clouddiensten. Het is misschien een goed idee om over zo'n inventaris te kunnen beschikken.

Tot slot, u hebt opnieuw uw doelstellingen herhaald, maar ik vroeg u specifiek naar een stand van zaken van uw plannen en daar heb ik geen antwoord op gekregen. Ik meen dus dat u nog steeds in de conceptuele fase zit en dat we nog moeten wachten op de uitvoering van uw plannen.

L'incident est clos.

Het incident is gesloten.

Le **président**: Les questions n^{os} 56009960C et 56010007C de Mme Meunier sont reportées.

03 Questions jointes de

- **Hervé Cornillie à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'appel mondial à la suspension des travaux sur la superintelligence" (56010022C)**

- **Leentje Grillaert à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Les risques potentiels de systèmes superintelligents d'IA autodidactes ou autorépliquants" (56010124C)**

03 Samengevoegde vragen van

- **Hervé Cornillie aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De wereldwijde oproep tot opschorting van de ontwikkeling van superintelligentie" (56010022C)**

- **Leentje Grillaert aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De potentiële risico's van zelflerende of zelfreplicerende superintelligente systemen" (56010124C)**

03.01 Leentje Grillaert (cd&v): Mevrouw de minister, in een recent opiniestuk waarschuwt filosoof Lode Lauwaert voor de risico's van artificiële intelligentie. Ik kan de boeken en opiniestukken van Lode Lauwaert trouwens zeer aanraden. Ze zijn zeer verhelderend en zitten vol nieuwe inzichten. Hij is een leeftijds- en streekgenoot van mij, en is ter zake zeer deskundig.

Wat het onderwerp zelf betreft, volgens hem kan een zelflerend en zelfreplicerend systeem zich onbeperkt verspreiden, waardoor menselijke controle volledig verloren gaat. Zoals u wellicht weet, pleiten inmiddels meer dan 30.000 ondertekenaars – onder wie een Nobelprijswinnaar en een futuroloog – voor een internationaal verbod op de ontwikkeling van superintelligente systemen. Hoewel die superintelligentie vandaag nog niet bestaat, tonen recente initiatieven van grote technologiebedrijven aan dat die richting effectief wordt ingeslaan en dat de mogelijkheid bestaat dat dit niveau ook wordt bereikt. Het risico bestaat dat zulke technologieën zich sneller ontwikkelen dan de regelgeving of veiligheidsnormen kunnen volgen.

Mevrouw de minister, in welke mate wordt in het Belgische en Europese beleid rond artificiële intelligentie rekening gehouden met de potentiële risico's? Werd bij de nationale uitrol van het Belgische AI-beleid of het federaal actieplan AI specifiek nagedacht over scenario's waarin menselijke controle over zulke systemen verloren zou kunnen gaan? Is een debat of initiatief op Europees of internationaal niveau wenselijk om onderzoek naar zelfreplicerend of onbeheersbaar AI-gedrag te beperken of te verbieden, zoals door Lode Lauwaert en andere experts wordt bepleit, en bent u bereid hiervoor stappen te ondernemen?

Ik dank u alvast voor uw antwoord.

03.02 Minister Vanessa Matz: Bedankt voor uw vraag.

Voordat men zich kan uitspreken over de opportuniteit om een internationaal moratorium op werkzaamheden rond superintelligentie te steunen, is het essentieel om de concrete impact te evalueren van de AI Act, waarvan de uitvoering momenteel op Europees niveau aan de gang is.

De AI Act verbiedt onder meer AI-systemen die gebruikmaken van subliminale manipulatie-technieken of die significante schade veroorzaken, wat in principe bepaalde risico's verbonden aan superintelligentie zou kunnen dekken. De AI Act voorziet echter in een mechanisme voor toezicht op risico's voor de grondrechten, waardoor de bevoegde autoriteiten aanvullende informatie kunnen vragen of technische tests kunnen uitvoeren wanneer een AI-systeem een potentieel gevaar oplevert. Als blijkt dat een AI-systeem inbreuk maakt op de grondrechten, kunnen corrigerende maatregelen worden genomen om het systeem in overeenstemming te brengen, van de markt te halen of terug te roepen.

België neemt actief deel aan de internationale discussie over AI-governance, met name binnen de Europese AI Board, waar de potentiële risico's van technologische ontwikkelingen worden besproken. Daarnaast overweegt de OESO om de resultaten van het AI International Safety Report om te zetten in praktische aanbevelingen, met het oog op de versterking van de internationale samenwerking op het vlak van AI-veiligheid.

België ondersteunt de inspanningen op VN-niveau om een mondiale governance voor AI tot stand te brengen. Twee nieuwe organen werden in augustus dit jaar opgericht: de Global Dialogue on AI Governance en een onafhankelijk internationaal wetenschappelijk panel over AI. Deze instanties hebben tot doel de internationale samenwerking te vergemakkelijken en de internationale gemeenschap te helpen beslissingen te nemen op basis van degelijk onderbouwde gegevens.

03.03 Leentje Grillaert (cd&v): Mevrouw de minister, ik dank u voor uw antwoord.

Het is goed te horen dat wij actief deelnemen aan dergelijke discussies waar de impact en de gevolgen daarvan worden besproken. Het is alleszins ook belangrijk om aandacht te hebben voor wat op ons afkomt, de superintelligente artificiële intelligentie.

Daarom wil ik een oproep doen om niet alleen te kijken naar wat vandaag al bestaat maar om een breder perspectief te hanteren en stil te staan bij de toekomstige mogelijkheden van artificiële intelligentie. Dat is iets waarvoor we bijzonder waakzaam moeten zijn.

Ik herhaal dus mijn oproep om ook filosofen en futurologen te lezen en na te gaan wat zij daarover aangeven. We kunnen daar immers heel veel uit leren. Zij spiegelen ons vele zaken voor waarmee wij heel voorzichtig zullen moeten omspringen.

Ik ben dus blij met uw antwoord, maar ik kijk verder dan wat we vandaag kennen. De wetgeving mag niet achterop lopen maar moet vooruitlopen op wat op ons afkomt.

*Het incident is gesloten.
L'incident est clos.*

04 Samengevoegde vragen van

- **Britt Huybrechts aan Vanessa Matz** (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De app MyGov.be" (56010037C)

- **Dieter Keuten aan Vanessa Matz** (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De digitale sleutel van de app MyGov" (56010086C)

04 Questions jointes de

- **Britt Huybrechts à Vanessa Matz** (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'application MyGov.be" (56010037C)

- **Dieter Keuten à Vanessa Matz** (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La clé numérique de l'application MyGov" (56010086C)

De **voorzitter**: De samengevoegde vraag nr. 56010037C van mevrouw Huybrechts wordt omgezet in een schriftelijke vraag.

04.01 Dieter Keuten (VB): Mevrouw de minister, in de pers werd onlangs de lancering van een nieuwe digitale sleutel die naast identificatiemiddelen zoals de eID en itsme kan worden gebruikt, mooi beschreven. Aangezien eerdere pogingen om een overheidsalternatief voor itsme te bieden, vooralsnog niet gelukt zijn, rijst de vraag waarom er nu wel hogere slaagkansen worden toegekend aan de digitale sleutel MyGov.

Welke lessen werden er getrokken uit de eerdere pogingen om een digitale sleutel te lanceren, digitale sleutel die al na enkele uren door veiligheidsproblemen lam werd gelegd?

Welke veiligheidsaudits of onafhankelijke controles werden er uitgevoerd voor de lancering?

Welke instanties of bedrijven waren betrokken bij de ontwikkeling van de nieuwe digitale sleutel?

Hoe werd de aanbesteding georganiseerd?

Wordt de bescherming van de persoonsgegevens gegarandeerd?

Welke partij draagt de uiteindelijke verantwoordelijkheid bij een datalek of misbruik? Wie is de DPO, met andere woorden?

Wat was de totale kostprijs van het project, inclusief verwachte onderhoudskosten en eventuele communicatiecampagnes, als die al gepland zijn; wat ik vermoed, gezien de vermeldingen in de pers?

In hoeverre sluit de nieuwe digitale sleutel aan bij de Europese eIDAS-verordening en de toekomstige Europese Digital Wallet?

Hoe beoordeelt u de samenwerking en mogelijke concurrentie tussen de overheid en private spelers zoals itsme?

04.02 Minister **Vanessa Matz**: Mijnheer Keuten, ik dank u voor uw vraag.

De eIDAS-verordening van 2014 heeft een kader gecreëerd voor een Europese digitale identiteit.

MyGov.be is de Belgische digitale portefeuille. Wij moeten voort werk maken van de ontwikkeling ervan, zodat alles tegen 2026 volledig in orde is. Die portefeuille moet ook de kwaliteit van de openbare dienstverlening verbeteren.

Sinds oktober kunnen burgers MyGov.be gebruiken om zich aan te melden op websites van overheidsdiensten. Ik wil geenszins dat dat de enige toegangssleutel wordt. MyGov.be is een aanvulling op het bestaande systeem.

Op het gebied van de kosten wordt MyGov.be voornamelijk gefinancierd door de FOD BOSA en door Europese middelen. Dat geld dient voor de verdere ontwikkeling van het ecosysteem. Voor meer details kunt u een schriftelijke vraag indienen.

Op veiligheidsvlak heeft MyGov.be een heel hoog beveiligingsniveau. Het bevat verschillende beschermingslagen en wordt regelmatig getest door externe experts. De ontwikkeling volgt ook de Europese normen.

Wij willen MyGov.be in de toekomst uitbreiden met extra functies zoals de gekwalificeerde elektronische handtekening en de digitale identiteitskaart. MyGov.be geeft nu al toegang tot Vlaamse overheidsdiensten via toegangsbeheer. Vanaf 1 december 2025 wordt de sleutel ook geïntegreerd in de app Mijn Burgerprofiel.

04.03 **Dieter Keuten** (VB): Dank u voor de uitleg, mevrouw de minister.

Ik zal u schriftelijk bevragen over de veiligheidsprocedures rond de nieuwe digitale sleutel MyGov.be. Ook zal ik u bevragen over het succes of het gebruik van de nieuwe sleutel en de betrouwbaarheid ervan en de gehaalde servicelevelagreements.

MyGov.be werd al een keer gehackt vorig jaar of begin dit jaar, gelukkig met beperkte schade. De hackers vonden blijkbaar nog niet veel gevoelige persoonsgegevens. Laten we hopen dat nu de app steeds breder wordt gebruikt en over meer data beschikt, hij ook veiliger wordt en niet opnieuw gehackt kan worden.

L'incident est clos.

Het incident is gesloten.

Le **président**: Les questions n° 56010038C de M. De Smet et n° 56010055C de Mme Huybrechts sont transformées en questions écrites.

05 Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De uitvoering van de NIS2-richtlijn" (56010352C)

05 Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La mise en oeuvre de la directive SRI2" (56010352C)

05.01 **Dieter Keuten** (VB): De Europese NIS2-richtlijn verplicht lidstaten kritieke infrastructuur en digitale diensten versterkt te beschermen. Er zou een coördinatie- en ondersteuningscel worden opgericht binnen de FOD BOSA om de implementatie van deze wet te ondersteunen. Om netwerken en informatiesystemen algemeen te beschermen en kmo's te ondersteunen, is het belangrijk hierover meer duidelijkheid te krijgen.

Mevrouw de minister, welke exacte taken, bevoegdheden en verantwoordelijkheden zijn aan deze cel binnen de FOD BOSA toegewezen en hoe verhouden die zich tot de bestaande federale, gewestelijke en sectorale cyberbeveiligingsinstellingen?

Hoe wordt de nieuwe coördinatie- en ondersteuningscel bemand? Kunt u het organogram met ons delen?

Hoe wordt de samenwerking tussen de federale overheid, de gewesten en de toezichthouders georganiseerd? Welke overlegstructuren bestaan er?

Welke federale taken en deadlines gelden in 2025-2026 voor de implementatie van NIS2 en welke resultaten verwacht u hiervan op korte termijn?

Welke sectoren vallen onder uw coördinatie? Kunt u dat verduidelijken?

Welke ondersteuning voorziet u voor kmo's die onder NIS2 vallen omdat ze in kritieke ketens opereren? Hebt u hierover overleg gehad met de minister bevoegd voor kmo's?

Hoe koppelt u de NIS2-doelstellingen aan andere federale digitaliseringsprojecten zoals de Single Digital Gateway?

Welke indicatoren worden gehanteerd om de cyberweerbaarheid en de incidentrapportering te monitoren?

Welke evaluatie- en rapporteringsmechanismen zijn voorzien waarin de cel periodiek verslag uitbrengt over haar werking, de voortgang en eventuele knelpunten? Wanneer mogen we een eerste verslag van die nog op te richten cel verwachten?

05.02 Minister **Vanessa Matz**: Mijnheer Keuten, op mijn initiatief wordt binnen de FOD BOSA een coördinatie- en ondersteuningscel opgericht, CISO-as-a-Service, die volgend jaar operationeel moet zijn.

Met dit initiatief willen we overheidsdiensten ondersteunen die niet over genoeg interne middelen beschikken om de NIS2-regels na te leven. De cel zal hen helpen met cyberveiligheidsexpertise, lagere kosten en een uniforme aanpak binnen de federale overheid. De aangeboden diensten zullen onder meer bestaan uit risicobeheer, de invoering van cyberveiligheidsoplossingen, het opvolgen van de NIS2-conformiteit en het efficiënt inzetten van middelen. Kleinere entiteiten zullen kunnen profiteren van voordelige tarieven dankzij de centralisatie van dienstverlening. De cel wordt opgebouwd rond een federale CISO, ondersteund door gespecialiseerde medewerkers in risicobeheer en beveiliging. De aanwervingen worden momenteel voorbereid. De diensten van CISO-as-a-Service zijn bedoeld voor alle federale entiteiten die onder de NIS2-wet vallen. Het team zal rapporteren aan het College van voorzitters en aan de bevoegde minister.

Voor de uitvoering van de NIS2-wet in de andere sectoren verwijs ik naar de eerste minister, die bevoegd is voor cyberveiligheid.

05.03 **Dieter Keuten** (VB): Dank u wel voor de verduidelijking.

U bent ermee bezig. Volgend jaar wordt de cel dus operationeel. Hopelijk gaan de aanwervingen vlot. Ik zal de vraag inderdaad ook stellen aan de eerste minister, bevoegd voor cyberveiligheid.

Ik heb u helaas niet horen antwoorden op het belangrijkste aspect van mijn vraag, namelijk wat dit betekent voor de kmo's. Hoe zult u, samen met uw collega die verantwoordelijk is voor kmo's, kleine bedrijven helpen om de onduidelijkheid weg te nemen die momenteel bestaat rond NIS2?

U hebt zelf blijkbaar tijd genoeg om die ondersteuningscel op te richten. Hopelijk lukt dat volgend jaar. We zullen dat mee opvolgen. Start-ups en kleine bedrijven maken zich echter nu, op dit moment, ongelooflijk veel zorgen over de NIS2-richtlijnen, die voor hen althans bijzonder streng zijn. Grote bedrijven kunnen consultants en specialisten inschakelen om zich aan de nieuwe richtlijn te conformeren. Kleine bedrijven en start-ups – ik hoop dat u eens met hen kunt spreken – kunnen dat echter niet en zij zien hun toekomstige werkzaamheden enorm beperkt door de richtlijn. Voor hen is vooral niet duidelijk of zij al dan niet onder die regelgeving vallen en, zo ja, wanneer. Dat moet echt worden opgehelderd en verduidelijkt.

Wij zullen pleiten voor een bepaalde vorm van uitsluiting van start-ups en scale-ups van de NIS2-regelgeving.

05.04 Minister **Vanessa Matz**: Wij zijn niet bevoegd voor de kmo's. Wij zijn enkel bevoegd voor de overheidsdiensten.

05.05 **Dieter Keuten** (VB): Ik dank u voor de verduidelijking.

De vraag was of u overleg hebt gehad met uw collega, de minister van kmo's, maar bij deze is die vraag beantwoord. Er is geen overleg of dat overleg is volgens u niet nodig.

*Het incident is gesloten.
L'incident est clos.*

06 **Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De datacentercampus" (56010353C)**

06 **Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le campus de centres de données" (56010353C)**

06.01 **Dieter Keuten** (VB): Mijn laatste vraag van vandaag gaat over de datacentercampus die in Neder-over-Heembeek zou worden gebouwd via een publiek-private samenwerking. Daarover wordt al verschillende jaren gesproken. Die datacentersite zou aanzienlijk meer rekenkracht ter beschikking kunnen stellen dan traditionele datacenters en zou bedoeld zijn om AI-toepassingen en onderzoek te kunnen uitvoeren zonder afhankelijk te zijn van infrastructuur in het buitenland.

Mevrouw de minister, welke waarborgen bestaan er voor bedrijven en overheidsdiensten inzake prijstoegang en technologische soevereiniteit bij de bouw van die digitale infrastructuur? Welke procedures zijn voorzien in het geval van storingen, zoals beveiligingsincidenten of datalekken? Hoe wordt de druk geëvalueerd die dergelijke datacenters uitoefenen op regionale infrastructuur, zoals wegen, elektriciteitsnetten en watervoorziening?

Welke garanties worden voorzien opdat de energievoorziening in de regio van Neder-over-Heembeek betrouwbaar blijft? Zal er bijvoorbeeld, zoals bij het Googledatacenter in Bergen, een beroep worden gedaan op grote hoeveelheden diesel als back-upenergiebron?

Hoe wordt vermeden dat dit zal leiden tot hogere kosten of verminderde dienstverlening voor de elektriciteitsafnemers in de buurt? Ik heb gelezen dat in een eerste fase 32 megawatt aan IT-capaciteit zou zijn voorzien.

Volgens eerdere berichten zou dit datacenter in 2025 operationeel zijn, maar blijkbaar is het project uitgesteld. Wat is nu het verwachte tijdspad?

In de aankondigingen wordt vermeld dat tegen 2030 100 % hernieuwbare energie zal worden gebruikt voor dit datacenter. Kunt u ook dat stappenplan toelichten?

06.02 Minister **Vanessa Matz**: Mijnheer Keuten, de datacentercampus in Neder-over-Heembeek is een strategisch project dat bedoeld is om de digitale capaciteit en de technologische soevereiniteit van de regio te versterken. Volgens mij blijven er nog verschillende onduidelijkheden bestaan.

Er is geen duidelijke publieke afspraak over de tarieven en over de toegang tot de diensten. Er is weinig informatie over de aanpak van incidenten en over de bescherming van gegevens. Er is geen energie- of infrastructuurimpactstudie gepubliceerd.

Op dit moment werk ik samen met mijn team aan een federale strategie voor datacenters, die de toekomstige capaciteitsbehoeften combineert met de principes van veiligheid, weerbaarheid, duurzaamheid en soevereiniteit. De datacentermarkt wordt daarbij van nabij opgevolgd, om mogelijkheden voor samenwerking te identificeren binnen een ruimer strategisch kader.

Er moeten dus nog veel essentiële punten worden verduidelijkt met betrekking tot de datacentercampus in Neder-over-Heembeek

06.03 **Dieter Keuten** (VB): Mevrouw de minister, ik dank u voor dit heel duidelijke antwoord.

Ik zal dit verder opvolgen en hopelijk komt er snel duidelijkheid, zodat er een nieuw datacenter kan worden gebouwd in onze buurt.

Het incident is gesloten.
L'incident est clos.

07 **Samengevoegde vragen van**

- Lieve Truyma aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "Het Digital Simplification Package" (56010363C)

- Patrick Prévot aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "Het deels op pauze zetten van de AI Act door de Europese Commissie onder Amerikaanse druk" (56010412C)

07 **Questions jointes de**

- Lieve Truyma à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le Digital Simplification Package" (56010363C)

- Patrick Prévot à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le recul de la Commission européenne sur l'AI Act face aux pressions américaines" (56010412C)

De **voorzitter**: De heer Prévot is afwezig. Zijn vraag zal als beantwoord worden beschouwd.

07.01 **Lieve Truyma** (N-VA): Mevrouw de minister, de Europese Commissie stelde op 18 oktober haar Digital Simplification Package voor. Het is een ambitieus plan om de complexe digitale wetgeving te vereenvoudigen. Het belangrijkste doel van dat pakket is de administratieve lasten voor bedrijven te verminderen, zodat ze zich kunnen richten op innovatie en groei. Op die manier zou er een betere harmonisatie moeten komen tussen de verschillende lidstaten en kan de concurrentiepositie van Europa versterkt worden ten opzichte van China en de Verenigde Staten.

Bent u op de hoogte van de inhoud van die maatregelen? Heeft men u, als bevoegd minister, daarover geraadpleegd?

De Europese Commissie heeft de afgelopen jaren zeer veel nieuwe regelgeving opgelegd. Zal dat pakket aan maatregelen onze bedrijven effectief helpen om hun administratieve lasten te verminderen?

Op welke termijn voorziet ons land de invoering? Zullen onze bedrijven voldoende tijd krijgen om dit te

implementeren?

Zal dit pakket een invloed hebben op de concurrentiepositie van Belgische bedrijven ten opzichte van hun buitenlandse collega's?

07.02 Minister **Vanessa Matz**: Mevrouw Truyma, de Europese Commissie kondigde inderdaad aan dat ze op woensdag 19 november een wetgevingspakket over digitale vereenvoudiging zou publiceren. De tekst werd tien minuten voor aanvang van deze commissievergadering gepubliceerd. Het aangekondigde doel is de vereenvoudiging van de Europese regels op digitaal vlak, het wegnemen van overlappingen tussen wetgevingen en het verminderen van lasten voor bedrijven.

De voorbereidende werkzaamheden zijn uitgevoerd zonder tekstvoorstel. België heeft in de afgelopen maanden echter de mogelijkheid gehad om voorlopige opmerkingen over te maken.

Ik heb recentelijk kunnen kennisnemen van de inhoud van het project. We analyseren momenteel dat omvangrijke project, dat uit twee afzonderlijke onderdelen zou bestaan. Het eerste is gericht op vereenvoudigingen op digitaal vlak, terwijl het tweede betrekking heeft op artificiële intelligentie.

Het is belangrijk te benadrukken dat de tekst nog niet formeel op Europees niveau besproken werd.

Zoals ik al aangaf, bevat het voorstel van de Commissie ook een onderdeel over AI. In dit kader is het niet uitgesloten dat de Commissie een overgangperiode zal voorstellen vanwege de vertraging bij de aanneming van de implementatiewetten die ze moest publiceren.

België heeft nog geen formeel standpunt ingenomen over deze tekst, die nog niet gepubliceerd was en die de komende weken op Europees niveau zal worden besproken.

Ik heb in de analyse van mijn dienst ook benadrukt hoe belangrijk het is om juridische zekerheid voor onze bedrijven te garanderen en een hoog niveau van bescherming voor de gebruikers te waarborgen.

07.03 **Lieve Truyma** (N-VA): Dank u wel.

Dat is letterlijk vers van de pers. We zullen het persbericht zeker raadplegen en verder opvolgen welk standpunt België zal innemen, alsook hoe we dat zullen implementeren voor onze bedrijven. Bedankt voor de info.

L'incident est clos.

Het incident is gesloten.

08 **Questions jointes de**

- **Sophie Thémont à Vanessa Matz** (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'accès à internet pour les ménages et la fracture numérique" (56010401C)

- **Sophie Thémont à Vanessa Matz** (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La fracture numérique et l'obligation de carte d'embarquement digitale chez Ryanair" (56010484C)

08 **Samengevoegde vragen van**

- **Sophie Thémont aan Vanessa Matz** (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De internettoegang voor gezinnen en de digitale kloof" (56010401C)

- **Sophie Thémont aan Vanessa Matz** (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De digitale kloof en de verplichte digitale boardingpass bij Ryanair" (56010484C)

08.01 **Sophie Thémont** (PS): *Madame la ministre, alors que la numérisation de notre société s'accélère, une partie importante de la population reste à l'écart. Selon les chiffres récemment publiés par Statbel, en 2024, plus de 11 % des personnes vivant seules n'avaient pas de connexion Internet à domicile, et près de 16 % des personnes âgées de 65 à 74 ans n'utilisaient que rarement le numérique. Parmi les plus de 75 ans, cette proportion dépasse encore les 40 %.*

Ces chiffres traduisent une fracture numérique persistante, qui menace directement l'inclusion sociale, l'accès aux droits et la participation citoyenne. Alors que la majorité des démarches administratives, bancaires ou même médicales passent désormais par le numérique, celles et ceux qui n'ont ni connexion stable, ni compétences suffisantes se retrouvent marginalisés.

L'actualité récente en fournit une illustration très concrète: depuis ce mercredi, la compagnie aérienne Ryanair n'accepte plus les cartes d'embarquement papier. Désormais, les passagers doivent impérativement utiliser l'application mobile de la compagnie pour pouvoir voyager. Cette obligation exclut de fait les personnes qui ne disposent pas de smartphone, qui ne maîtrisent pas les outils numériques, ou qui n'ont tout simplement pas de connexion mobile suffisante. Des organisations de défense des consommateurs, comme Test-Achats, dénoncent une mesure "discriminatoire" qui aggrave la fracture numérique et crée une nouvelle inégalité d'accès à un service de base : le transport.

Madame la ministre, ces situations se multiplient et rappellent à quel point la transition numérique, si elle n'est pas accompagnée, peut devenir un facteur d'exclusion.

Comment le gouvernement entend-il garantir un accès universel à Internet et un accompagnement effectif pour les publics vulnérables?

Des mesures sont-elles prévues pour renforcer la formation et la médiation numérique, notamment à destination des seniors et des ménages précarisés?

Enfin, face à la multiplication d'exemples comme celui de Ryanair, quelles garanties légales ou pratiques le gouvernement peut-il offrir pour que le numérique reste un droit d'accès aux services, et non un obstacle?

Je vous remercie pour vos réponses.

Madame la ministre, depuis ce 12 novembre, Ryanair impose à tous les voyageurs l'utilisation exclusive de son application mobile pour accéder à leur carte d'embarquement. Les documents imprimés ne sont plus acceptés, sauf exceptions limitées. Cette décision, présentée comme une simplification, interroge profondément en matière d'inclusion numérique.

En effet, elle suppose que chaque passager possède un smartphone récent, accepte d'y installer l'application, dispose d'une connexion stable et maîtrise les usages numériques. Or, nous savons que la fracture numérique reste une réalité concrète: personnes âgées, publics précarisés, voyageurs occasionnels... Tous ne disposent pas des compétences ou des outils nécessaires pour se conformer à cette obligation.

Pour beaucoup, cette digitalisation imposée peut devenir un frein à la mobilité, voire source de stress ou d'exclusion. L'enjeu dépasse donc Ryanair: il pose la question plus large de l'accès aux services essentiels lorsqu'ils deviennent exclusivement numériques.

Dans ce contexte, j'aimerais vous poser les questions suivantes :

Comment le gouvernement évalue-t-il l'impact de ces pratiques sur les publics en difficulté numérique, et quels principes défend-il pour garantir des alternatives accessibles dans les services essentiels?

Estimez-vous nécessaire de rappeler aux entreprises actives en Belgique qu'une transition numérique ne peut pas se faire au détriment de l'accessibilité universelle?

Le gouvernement envisage-t-il de renforcer les obligations d'alternative non numérique dans les secteurs où la digitalisation devient un passage obligé pour accéder à un service?

Plus largement, comment entendez-vous prévenir l'exclusion numérique dans les transports et services privés fortement digitalisés?

Je vous remercie.

08.02 **Vanessa Matz**, ministre: Madame Thémont, je vous remercie pour votre question qui aborde un

sujet qui me tient particulièrement à cœur, à savoir l'inclusion numérique.

Pour ce qui est de l'accès universel à internet, mon objectif est que chacun puisse disposer d'une connexion stable et abordable. À l'heure actuelle, seuls 4 % des 500 000 Belges qui pourraient bénéficier du tarif social pour internet en profitent réellement. Ce chiffre est évidemment bien trop faible. C'est pourquoi j'ai demandé une analyse au SPF Économie. Sur la base de ses résultats, je proposerai au gouvernement une amélioration concrète de l'offre internet sociale avec un volume de données plus élevé, une vitesse de connexion plus rapide et des conditions qui correspondent enfin à un usage de base réel digne de ce nom.

En ce qui concerne l'accompagnement, je travaille en ce moment avec mes équipes sur deux projets concrets. Le premier vise à aider les citoyens dans le développement de leurs compétences numériques via la mise en place de certificats numériques, comme ce qui existe à l'heure actuelle en Région wallonne avec la plateforme Pix. Le second a pour objectif d'évaluer les synergies entre partenariats publics-privés, notamment avec des entreprises comme bpost ainsi qu'avec les secteurs en contact direct avec des usagers, afin de déployer des aidants numériques capables d'apporter un soutien aux citoyens en difficulté.

Enfin, vous évoquez le droit à une alternative. Le cas que vous citez, celui de Ryanair, illustre une tendance préoccupante. C'est d'ailleurs en ce sens que j'ai déposé un avant-projet de loi garantissant à chacun la possibilité d'accomplir ses démarches administratives via un canal non numérique sans surcoût. Cet avant-projet de loi concerne les administrations fédérales et les entreprises publiques fédérales. Pour ce qui est du secteur privé, en principe, chaque entreprise est libre de déterminer sa propre politique commerciale à cet égard.

Je précise par ailleurs que nous avons cherché dans tous les sens la possibilité de contrer ce dispositif mis en place par Ryanair et que nous n'avons malheureusement pas trouvé de manière d'agir directement. Il se peut que les règles relatives aux discriminations s'appliquent dans le cadre de ce type de choix commercial.

Concernant la législation sectorielle, je vous invite à vous adresser à mon collègue Jean-Luc Crucke, en charge de la Mobilité.

08.03 **Sophie Thémont (PS):** Merci madame la ministre pour votre réponse exhaustive.

J'entends les démarches que vous entreprenez en la matière et je sais qu'il s'agit d'un sujet qui vous tient à cœur. Mais les chiffres dont il est question ici confirment une réalité. En effet, sans connexion, sans équipement et sans accompagnement, des milliers de personnes sont laissées au bord de la route. Et chaque nouvelle obligation numérique, telle que celle de Ryanair aujourd'hui, aggrave cette exclusion, parce que tout le monde n'a pas un smartphone ou accès à internet. La situation est compliquée pour les personnes qui sont en décrochage.

Je me permettrai de revenir vers vous pour ce qui concerne votre avant-projet de loi et j'interrogerai votre collègue M. Crucke.

L'incident est clos.

Het incident is gesloten.

Le **président**: La question n° 56010403C de Mme Meunier est reportée.

09 **Question de Dimitri Legasse à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le développement de DIGI" (56010461C)**

09 **Vraag van Dimitri Legasse aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De ontwikkeling van DIGI" (56010461C)**

09.01 **Dimitri Legasse (PS):** Madame la ministre, le développement de l'opérateur de télécommunications DIGI semble toujours aussi difficile. Sur son site internet, l'offre pour les abonnements à la télévision a disparu. Cette offre aurait pourtant, à mon sens, dû faire partie des

obligations de l'opérateur.

Auriez-vous de plus amples informations quant aux chiffres d'abonnés que DIGI a réussi à attirer jusqu'ici? Vont-ils vers l'offre mobile ou internet séparée ou l'offre internet et mobile combinée? Le chiffre qui m'a été rapporté à ce stade est de 62 000 abonnés, ou affiliés, consommateurs.

Par ailleurs, le développement de la fibre par DIGI ne semble pas particulièrement rapide non plus. Pour avoir testé des adresses dans différentes communes du Brabant wallon, je constate qu'il n'est pas possible de disposer de leur offre internet. Qu'en est-il de leurs perspectives en la matière?

Quelles sont finalement les obligations de DIGI?

09.02 Vanessa Matz, ministre: Monsieur Legasse, dans le cadre de l'attribution des licences du spectre, l'opérateur DIGI doit respecter un certain nombre d'obligations de couverture. Le gouvernement impose ces obligations parce que les fréquences radio constituent un bien public rare auquel sont associés des droits d'usage exclusifs. En matière de fibre optique, cette rareté n'existe pas. Chaque opérateur peut déployer librement son réseau sans droit exclusif. Le déploiement est dès lors déterminé par le marché, sans obligation légale de couverture.

DIGI est en cours de déploiement dans plusieurs grandes villes: Bruxelles, Charleroi et Gand. Par ailleurs, il a récemment repris le réseau de fibre optique de Be Cactus, un petit opérateur localisé dans la région de Liège, ce qui contribue à renforcer sa présence dans cette zone.

Le lancement d'une offre de télévision relève également d'un choix purement commercial. Si DIGI venait à proposer un service de télévision, mais que l'offre n'était pas rendue accessible ou visible sur le site internet de l'opérateur, cela constituerait un manquement à l'obligation de transparence.

L'Institut belge des services postaux et des télécommunications (IBPT) effectue régulièrement des contrôles afin de vérifier la conformité des informations publiées par les opérateurs, notamment pour garantir la transparence des offres commerciales vis-à-vis des consommateurs. Les chiffres précis relatifs au nombre de clients de DIGI ne sont pas publiés par le régulateur qu'est l'IBPT, mais l'évolution des parts de marché du secteur peut toutefois être suivie dans son rapport annuel sur le marché des communications électroniques et de la télévision.

Dans le rapport financier de DIGI du 30 septembre 2025, l'opérateur indiquait comptabiliser environ 78 000 unités génératrices de revenus mobiles en Belgique.

09.03 Dimitri Legasse (PS): Je vous remercie, madame la ministre.

J'ai pris bonne note des obligations qui existent et de celles qui n'existent pas, et aussi de l'action de l'IBPT dans le cadre de sa fonction de régulateur. Nous attendrons donc le rapport annuel; 78 000 consommateurs – ou plutôt unités –, ce n'est pas encore énorme, convenons-en. Il y a là des questions à se poser, me semble-t-il, mais nous y reviendrons certainement.

L'incident est clos.

Het incident is gesloten.

10 Question de Sophie Thémont à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'accompagnement numérique et l'accès des petites entreprises aux outils d'intelligence artificielle" (56010485C)

10 Vraag van Sophie Thémont aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De digitale ondersteuning van kleine ondernemingen en hun toegang tot AI-tools" (56010485C)

10.01 Sophie Thémont (PS): *Madame la ministre, l'intelligence artificielle représente aujourd'hui un levier important pour améliorer la productivité des entreprises, y compris les plus petites. Dans le secteur de la construction, Buildwise indique que 36 % des entreprises utilisent déjà l'IA, mais l'adoption reste très inégale et souvent limitée faute de compétences suffisantes. De nombreux indépendants et*

PME font état d'un manque d'accompagnement adapté pour comprendre, choisir et intégrer ces outils.

Pourtant, l'IA peut automatiser des tâches administratives, améliorer la gestion de projets ou faciliter l'analyse de documents techniques. Les solutions sont devenues financièrement accessibles, mais elles ne le sont pas toujours sur le plan numérique: manque de formation, d'encadrement, d'informations fiables et de garanties en matière de sécurité des données.

Dans un contexte où les cyberrisques augmentent et où les petites structures demeurent les plus vulnérables, il est essentiel que la transition numérique ne crée pas de nouvelles inégalités entre grandes et petites entreprises. L'enjeu n'est donc pas seulement de promouvoir l'usage de l'IA, mais de le rendre sûr, compréhensible et réellement accessible.

Madame la ministre, j'aimerais dès lors vous poser les questions suivantes:

Quelles actions le gouvernement prévoit-il pour renforcer l'accompagnement numérique et la formation à l'IA des indépendants et petites entreprises, afin qu'ils puissent utiliser ces outils en toute sécurité?

Envisagez-vous des mesures spécifiques pour améliorer la cybersécurité des PME qui adoptent progressivement des solutions d'IA, telles que des guides pratiques, des audits simplifiés ou un soutien à la mise en conformité?

Le gouvernement compte-t-il développer ou renforcer des plateformes publiques d'appui permettant aux petites entreprises de choisir, tester ou adopter des outils numériques et d'intelligence artificielle de manière encadrée?

Enfin, comment garantir que la transition numérique ne renforce pas les écarts entre grandes entreprises déjà très outillées et petites entreprises qui redoutent les risques, les coûts ou la complexité de ces technologies?

10.02 **Vanessa Matz**, ministre: Merci madame Thémont.

L'intelligence artificielle est une réelle occasion pour les entreprises, y compris les plus petites, mais son adoption reste très inégale. Avec le SPF Économie, nous lancerons prochainement une campagne d'information sur l'AI Act, spécifiquement conçue pour les entrepreneurs, en accordant une attention particulière aux PME et jeunes entreprises. Cette campagne vise à sensibiliser les entreprises à l'incidence de l'AI Act sur leurs activités et les aider à vérifier si elles relèvent du champ d'application du texte.

L'objectif est également de les guider pour répondre aux obligations et de les soutenir dans une utilisation responsable de l'intelligence artificielle. Un guide numérique pratique est en cours d'élaboration pour aider les entreprises à déterminer si elles sont concernées par l'AI Act et, le cas échéant, à s'y préparer. En collaboration avec la ministre Simonet, plusieurs actions ont déjà été entreprises en vue d'améliorer la cybersécurité des PME.

La première de ces actions consiste en une campagne de communication pluriannuelle sur les réseaux sociaux, afin de sensibiliser les PME et les indépendants à la cybersécurité. Ensuite, il existe désormais un site web qui propose un "cyberscan" permettant aux PME d'obtenir un aperçu de la maturité de leur cybersécurité et de trouver des informations sur les appels à projets. Enfin, neuf appels à projets ont été lancés, couvrant des thèmes comme la formation, l'accompagnement professionnel ou encore des projets ciblant les petits commerçants et les femmes entrepreneurs. Pas moins de 26 projets ont déjà été sélectionnés.

J'ajouterais encore que, pour permettre aux PME de tester et d'adopter des outils d'intelligence artificielle de manière cadrée, nous prévoyons également la mise en place d'un bac à sable réglementaire de l'intelligence artificielle.

Je vous remercie.

10.03 **Sophie Thémont** (PS): Merci pour vos réponses encourageantes, puisque vous confirmez le potentiel de l'intelligence artificielle.

Comme vous l'avez dit, sur le terrain, de nombreuses petites entreprises n'y ont tout simplement pas accès, faute d'accompagnement. Dès lors, il faut effectivement rendre cette utilisation accessible et sûre.

Les indépendants, les petites et moyennes entreprises et les petits indépendants attendent effectivement des formations qui puissent être adaptées ainsi que des outils simples. Nous avons parlé de cybersécurité, et c'est ce qu'ils attendent: un véritable soutien en matière de cybersécurité, car la fracture numérique dans une grande entreprise est différente par rapport à la fracture numérique chez un petit indépendant ou une petite et moyenne entreprise.

En tout état de cause, j'entends les initiatives qui sont prises en la matière concernant le guide numérique, votre collaboration avec votre collègue, la sensibilisation ainsi que ces appels à projets, qui, j'imagine, étaient destinés aussi aux petites et moyennes entreprises et aux femmes entrepreneurs.

Merci beaucoup pour vos réponses.

L'incident est clos.

Het incident is gesloten.

[11] Question de Ismaël Nuino à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La désignation de signaleurs de confiance en Belgique" (56010595C)

[11] Vraag van Ismaël Nuino aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De aanwijzing van betrouwbare flaggers in België" (56010595C)

[11.01] Ismaël Nuino (Les Engagés): Depuis l'adoption du Digital Services Act (DSA), que vous connaissez bien, il est devenu indispensable pour l'Union Européenne, mais aussi pour les États membres, de renforcer la responsabilité des grandes plateformes en ligne. Je sais, évidemment, que vous en avez fait un combat particulièrement important durant votre mandat. Ce règlement, pour rappel, permet de mieux prévenir la diffusion de contenus illicites. Cela peut paraître un peu abstrait lorsqu'on le dit, mais il s'agit de mieux prévenir la publication de fraudes, de faux investissements, de *deep fakes*, de discours de haine, d'images pouvant être problématiques pour certaines personnes.

Ce règlement impose des obligations croissantes aux hébergeurs en ce qui concerne la transparence, une modération plus active ou encore une coopération avec les autorités nationales. Une des innovations importantes du règlement, vraiment salubre, est la mise en place du statut de signaleur de confiance. Ces organisations sont spécialisées, reconnues pour leur expertise, et leurs signalements doivent être traités en priorité par ces grandes plateformes.

Ce dispositif est vraiment important. En effet, lors de la transposition de la directive au Parlement, nous étions inquiétés de la vitesse à laquelle nous pourrions réagir, parce que dans ces cas-là, quand on parle d'arnaque, de harcèlement, de menaces, la vitesse est excessivement importante. Il s'agit d'y mettre fin rapidement, d'où l'importance du signaleur de confiance faisant réagir l'opérateur plus rapidement par le biais d'une notification.

Malheureusement, je crois avoir lu récemment, dans un article de *L'Écho* me semble-t-il, que face à toutes ces arnaques en ligne, la Belgique n'avait toujours pas désigné de signaleur de confiance. Et pourtant, comme je viens de l'expliquer, il me semble qu'il serait fort utile que cela soit fait. Évidemment, ce retard de transposition n'est pas dû à ce gouvernement car nous étions déjà en retard pour le vote de la loi qui transposait le règlement.

La Belgique est souvent accusée de retard, et souvent à raison, dans les transpositions de directives, et c'est dommage en matière digitale. Disposez-vous d'éléments de réflexion sur la manière d'améliorer la vitesse de transposition de nos directives? Ensuite, est-il vrai qu'aucun signaleur de confiance n'a été désigné? Dans l'affirmative, allons-nous en désigner un? Dans la négative, qui a-t-il été désigné?

D'avance merci pour vos réponses.

11.02 Vanessa Matz, ministre: Merci, monsieur Nuino, pour votre question.

Le Digital Services Act (DSA) représente, vous l'avez rappelé, une avancée majeure pour renforcer la responsabilité des grandes plateformes en ligne et protéger les citoyens contre les contenus illicites. L'un des piliers de ce règlement est le statut de signaleur de confiance. Ce mécanisme est essentiel pour améliorer la détection des contenus dangereux, accélérer les retraits et ainsi préserver la sécurité et la dignité des citoyens dans leur vie numérique.

Je suis heureuse de vous annoncer que, depuis hier, Unia et l'Institut flamand des droits humains (Vlaams Mensenrechteninstituut) ont été officiellement reconnus en Belgique comme signaleurs de confiance. Les plateformes Facebook, Instagram, X ou TikTok sont désormais tenues d'examiner en priorité leurs signalements.

Grâce à ce statut, Unia et l'Institut flamand des droits humains disposent désormais d'un cadre clair pour signaler ces contenus et imposer leur traitement prioritaire, renforçant ainsi la protection des victimes. Il est vrai que, sous le gouvernement précédent, la Belgique a accusé un certain retard dans la mise en œuvre du DSA, notamment en ce qui concerne la loi fédérale et l'accord de coopération. Aujourd'hui, je me réjouis que les efforts déployés pour rattraper ce retard portent leurs fruits, permettant à la Belgique de tirer pleinement parti de ce texte européen essentiel.

Avec la désignation d'Unia et de l'Institut flamand des droits humains comme signaleurs de confiance, nous franchissons une étape décisive dans la lutte contre l'impunité des auteurs de discours de haine en ligne. Ce statut envoie un signal clair: les discours de haine sont interdits dans l'espace public, qu'il soit physique ou numérique.

11.03 Ismaël Nuino (Les Engagés): Merci beaucoup, madame la ministre, pour cette réponse évidemment satisfaisante. Il est vraiment réjouissant d'entendre qu'on a désigné ces deux organismes comme signaleurs de confiance.

Vous l'avez dit, ce règlement est primordial, et le fait de le mettre en œuvre de la manière la plus efficace possible est essentiel pour que ce qui est interdit dans la vraie vie le soit aussi en ligne. Je vous soutiens totalement dans cet engagement.

Par ailleurs, je lisais cet après-midi que la Commission européenne commencerait à rabaisser ses ambitions en ce qui concerne la protection des données et l'intelligence artificielle, et ce, en faveur de la compétitivité.

Il faut que, en tout cas en Belgique, on puisse affirmer que ce règlement est important pour protéger l'ensemble des utilisateurs. Nous devons donc l'appliquer de la manière la plus sérieuse possible pour que la crédibilité de notre État de droit continue d'exister.

Je vous remercie vraiment pour vos réponses, et je pense que cette nouvelle mériterait d'être mieux connue, parce qu'il faudrait que l'ensemble des citoyens et du public qui pourraient avoir à travailler avec Unia dans ce cadre-là soient au courant.

L'incident est clos.

Het incident is gesloten.

Le **président**: Monsieur Hiligsmann, merci pour votre patience. Vous avez attendu vos deux collègues mais ils ne sont pas venus.

12 Questions jointes de

- **Anthony Dufrane à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur**

"L'encadrement des algorithmes de TikTok et la lutte contre la viralité des contenus dangereux" (56009718C)

- Patrick Prévot à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Les algorithmes mortifères de TikTok" (56010419C)

- Serge Hiligsmann à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "L'effet "spirale" de l'algorithme de TikTok" (56010459C)

- Serge Hiligsmann à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le piège algorithmique de TikTok" (56010632C)

12 Samengevoegde vragen van

- Anthony Dufrane aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De regulering van de TikTok-algoritmes en het tegengaan van het viraal gaan van gevaarlijke content" (56009718C)

- Patrick Prévot aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De algoritmen van TikTok die tot zelfmoord aanzetten" (56010419C)

- Serge Hiligsmann aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De toxische spiraal die gecreëerd wordt door het algoritme van TikTok" (56010459C)

- Serge Hiligsmann aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De algoritmefuik van TikTok" (56010632C)

12.01 Serge Hiligsmann (Les Engagés): Un rapport de la commission d'enquête parlementaire française sur TikTok a été rendu public en septembre 2025. Ce rapport dénonce un piège algorithmique particulièrement dangereux pour les adolescents et un modèle économique privilégiant le profit à la santé mentale et recommande l'interdiction des réseaux sociaux pour les moins de 15 ans ainsi qu'un couvre-feu numérique pour les 15-18 ans. Amnesty International a également publié un rapport sur l'effet spirale de l'algorithme de TikTok qui oriente les jeunes vers les contenus suicidaires et d'automutilations, malgré les obligations du Digital Service Act.

À la lumière de ces éléments, comment la Belgique peut-elle renforcer le cadre réglementaire entourant les algorithmes, notamment en imposant aux plateformes une évaluation régulière des risques systémiques pour les mineurs et en les contraignant à adapter leurs mécanismes de recommandation lorsqu'elles créent des effets de spirale algorithmiques?

12.02 Vanessa Matz, ministre: Merci pour cette question essentielle.

Les questions sur les conclusions accablantes du rapport d'Amnesty International concernant l'algorithme de TikTok et son impact sur les jeunes belges me permettent de réaffirmer clairement ma volonté d'agir pour la protection des utilisateurs, singulièrement les jeunes.

Les risques liés à l'exposition des mineurs à des contenus normalisant la dépression, l'automutilation ou le suicide sont inacceptables et je partage pleinement votre vigilance sur le sujet. Dès ma prise de fonction, j'en ai fait une priorité. Mes actions concernent plusieurs volets. Sur le volet européen, nous participons activement à la recherche d'une solution commune permettant de renforcer le principe du Security by Design mais aussi de protéger les plus jeunes utilisateurs.

Je souhaite également vous faire part d'une avancée récente. Depuis le 29 octobre, les chercheurs peuvent obtenir un accès sans précédent aux données non publiques des grandes plateformes en ligne afin d'étudier l'incidence sociétale découlant des systèmes des plateformes. Cet accès répondra notamment aux préoccupations que nous partageons concernant la transparence des algorithmes. En outre, les résultats des études que pourront mener les chercheurs nous permettront de cibler et d'améliorer nos actions.

En ce qui concerne TikTok, les dialogues avec la plateforme s'inscrivent dans une démarche européenne renforcée. La Commission européenne a d'ailleurs ouvert une enquête pour manquements

présupposés en matière de protection des mineurs. Cette enquête est toujours en cours et – j'insiste – est beaucoup trop longue à notre goût, car les jeunes restent entre-temps confrontés à des contenus inappropriés, dangereux ou addictifs.

Je suivrai également avec beaucoup d'attention les travaux de la Chambre pour évaluer l'opportunité d'un âge minimal d'accès aux réseaux sociaux, proposer un cadre légal sur la vérification de l'âge et sur l'anonymat en ligne. Je compte évidemment sur votre soutien et sur celui de l'ensemble du Parlement pour faire de ce dossier une priorité.

12.03 **Serge Hiligsmann** (Les Engagés): Madame la ministre, vous connaissez mon goût pour la circularité, de sorte que j'utiliserai la réplique de tout à l'heure. Je vous remercie pour vos réponses et vous assure de notre confiance en vos services pour lutter contre ces pratiques tant frauduleuses que dangereuses, particulièrement pour notre jeunesse, nos adolescents, et plus particulièrement les personnes les plus fragiles.

Excusez ma paresse, qui fait suite à 17 heures passées à écouter M. Van Quickenborne hier et cette nuit. Je souhaiterais d'ailleurs qu'une solution soit trouvée afin d'éviter que ce genre de situation ne se reproduise. Ce serait bien, je pense, pour tout le monde.

L'incident est clos.

Het incident is gesloten.

Le **président**: Les questions n^{os} 56010405C et 56010410C de M. Patrick Prévot sont reportées.

La réunion publique de commission est levée à 15 h 24.

De openbare commissievergadering wordt gesloten om 15.24 uur.