Tweede Kamer, Uitvoeringswet cyberweerbaarheid (36875)

VERSLAG VAN EEN WETGEVINGSOVERLEG
Concept

De vaste commissie voor Digitale Zaken heeft op 7 september 2026 overleg gevoerd met mevrouw Aerdts, staatssecretaris Digitale Economie en Soevereiniteit, over:

- **het wetsvoorstel Uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid) (36875).**

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

De voorzitter van de vaste commissie voor Digitale Zaken,
Dekker

De griffier van de vaste commissie voor Digitale Zaken,
Boeve

Voorzitter: Bikkers
Griffier: Boeve

Aanwezig zijn vijf leden der Kamer, te weten: Van den Berg, Bikkers, El Boujdaini, Kathmann en Zwinkels,

en mevrouw Aerdts, staatssecretaris Digitale Economie en Soevereiniteit.

Aanvang 18.34 uur.

De **voorzitter**:
Dames en heren, van harte welkom. Hierbij open ik de vergadering van de vaste Kamercommissie Digitale Zaken. Aan de orde is het wetgevingsoverleg over de Uitvoeringswet cyberweerbaarheid, Kamerstuk 36875. Ik heet van harte welkom: de staatssecretaris en, aan de zijde van de Kamer, mevrouw Zwinkels, mevrouw El Boujdaini en nog een aantal anderen die wat later zullen komen.

Ik ga aan de voorkant aangeven dat we in totaal vier uur de tijd hebben. We hebben van tevoren uw spreektijden geïnventariseerd. Laten we kijken of we onszelf daaraan kunnen houden. Ik stel voor in de eerste termijn vier interrupties toe te staan, als u dat ook een goed idee vindt. Mooi, dan gaan we dat doen. Dan geef ik het woord aan mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Dank u wel, voorzitter.

Een slimme deurbel, een smartwatch, allerlei gratis apps die je kunt downloaden op je telefoon, en tegenwoordig zelfs een camerabril met vergaande AI-functies: steeds meer producten die we dagelijks gebruiken bevatten digitale elementen. Daarmee geldt steeds vaker: als de digitale veiligheid niet op orde is, is het product als geheel niet veilig. Kwetsbaarheden kunnen door criminelen en andere kwaadwillende actoren worden misbruikt om via een achterdeur toegang te krijgen tot systemen en zo waardevolle persoonlijke of belastende gegevens te verzamelen. Digitale toegang verschaffen is ook een geopolitiek pressiemiddel. Denk daarom ook aan statelijke actoren, naast het online verdienmodel van kwaadwillige individuen, bedrijven en criminele organisaties.

Om dat tegen te gaan moeten we beginnen bij het ontwerp van het product zelf. Het CDA steunt daarom het principe van de Cyber Resilience Act. We leggen de verantwoordelijkheid voor cyberveiligheid veel nadrukkelijker daar waar die hoort: bij degene die een digitaal product ontwikkelt en op de markt brengt. Van een fabrikant mag worden verwacht dat een product vanaf het ontwerp veilig is, dat kwetsbaarheden worden opgelost en dat veiligheidsupdates beschikbaar blijven gedurende de levensduur van het product.

We delen dus de opvatting van de CRA, die meer verantwoordelijkheid bij de producenten legt. Een nuancering is wel dat digitale weerbaarheid vraagt om bewustwording bij iedereen: weten wat je in huis haalt en alert zijn op eventuele risico's. De consument moet ervoor zorgen dat zijn wachtwoorden op orde zijn en dat updates worden geïnstalleerd. Als we consumenten meer kennis en vaardigheden bieden, in samenwerking met het onderwijs en bijvoorbeeld bibliotheken, staan we samen sterk. Zou bijvoorbeeld een digitale apk kunnen helpen, waarbij mensen periodiek kunnen nagaan of hun apparaten nog veilig zijn, welke risico's er zijn en welke acties zij zelf kunnen ondernemen? Dat kan beginnen met een duidelijke website met zoekfunctie, en op termijn worden uitgebreid naar meer interactieve dienstverlening. Zo'n digitale apk zien wij nadrukkelijk als een aanvulling op de CRA. De verantwoordelijkheid voor een veilig product blijft altijd bij de fabrikant. Kan de staatssecretaris toezeggen de mogelijkheden voor zo'n digitale apk verder te verkennen en de Kamer te informeren over hoe dit praktisch kan worden vormgegeven, ook in samenhang met de Europese uitvoering van de CRA?

Voorzitter. De digitale apk is een concreet voorbeeld van hoe we consumenten kunnen helpen om ook tijdens het gebruik zicht te houden op de digitale veiligheid van hun apparaten. Bij de uitvoering van deze wet hebben we daarnaast ook nog vier bredere aandachtspunten. Allereerst werkbare normen en uitvoerbaarheid. Ten tweede: het gelijke speelveld, het mkb en start-ups. Drie. De toekomstbestendigheid van deze wetgeving. Vier. De vraag: wat als het toch misgaat?

Allereerst de werkbare normen en de uitvoerbaarheid. Voor een ondernemer is natuurlijk vooral de vraag: wat moet ik concreet doen om aan al die eisen te voldoen? Geharmoniseerde Europese normen zijn daarbij belangrijk. Ze vertalen deze algemene eisen naar concrete technische maatregelen. Voor belangrijke producten uit de zogenaamde klasse I is dat extra relevant. Zelfbeoordeling is daar alleen mogelijk als zo'n geharmoniseerde norm wordt toegepast. Is die niet beschikbaar, dan is er een

zwaardere conformiteitsbeoordeling nodig.

Kunnen Nederlandse bedrijven straks in de praktijk ook aan die regels voldoen? Hoe worden ze hierin ondersteund? Want tussen een goede regel op papier en een goed werkende regel in de praktijk kan nogal wat ruimte zitten. Zo zien we bij de NIS2 dat ondanks de registratieplicht, nog niet alle organisaties die onder de wet vallen zich hebben geregistreerd. De RDI wijst in haar uitvoeringstoets dan ook nadrukkelijk op het belang van de tijdige totstandkoming van deze normen voor een goede werking van de CRA. Kan het kabinet aangeven hoe het staat met de ontwikkeling van deze normen? Zijn deze tijdig beschikbaar voordat de CRA volledig van toepassing wordt? En zo niet, wat betekent dit dan concreet voor de Nederlandse bedrijven? We moeten voorkomen dat bedrijven straks wel weten waaraan ze moeten voldoen, maar onvoldoende duidelijk hebben hoe ze dat kunnen aantonen. Onduidelijkheid en stapeling van complexe regels moeten we zo veel mogelijk voorkomen.

Dat brengt me bij het tweede punt, het gelijke speelveld, het mkb en de start-ups. Regels voor veilige producten werken alleen als ze voor iedereen gelden. Een Nederlandse fabrikant die investeert in cybersecuritytesten en -documentatie moet niet vervolgens concurreren met goedkope producten van buiten Europa waarvoor die kosten niet worden gemaakt. Op papier is de CRA daar duidelijk over: ook producten van fabrikanten van buiten de Europese Unie moeten aan dezelfde eisen voldoen wanneer zij op onze markt worden aangeboden.

Maar uiteindelijk staat of valt het gelijke speelveld natuurlijk met de handhaving. Dagelijks komen miljoenen pakketten van buiten de Europese Unie onze markt binnen. Natuurlijk kunnen we die onmogelijk allemaal controleren. De vraag is dus: hoe zorgen we ervoor dat de pakkans groot genoeg is en de onveilige producten daadwerkelijk van de markt verdwijnen? Hoe gaat de RDI risicogericht toezicht houden op producten die rechtstreeks en vanuit derde landen aan Nederlandse consumenten worden verkocht? Welke verantwoordelijkheid hebben importeurs en onlineplatforms daarbij? Heeft de RDI voldoende capaciteit en instrumenten om hier daadwerkelijk effectief op te handhaven? Anders bereiken we namelijk precies het tegenovergestelde van wat we willen: Europese bedrijven maken hun producten veiliger, maar worden daarvoor economisch bestraft met oneerlijke concurrentie.

Dat brengt me bij het mkb. Een multinational heeft een cybersecurityafdeling, compliance officers en een batterij aan juristen. Een innovatieve ondernemer met vijftien werknemers heeft dat meestal niet. Toch kan die ondernemer precies hetzelfde digitale product op de markt brengen en krijgt hij dus ook met deze verordening te maken. Het CDA wil voorkomen dat cybersecurityregels onbedoeld een nieuwe toetredingsbarrière worden: goed te dragen voor de grootste bedrijven, maar een flinke hindernis voor een start-up die juist een innovatief product probeert te ontwikkelen. Cybersecurity moet een hogere bodem onder de gehele markt leggen en geen toegangsbarrières creëren voor start-ups.

De CRA probeert daar terecht rekening mee te houden. Er komt een vereenvoudigde technische documentatie voor het mkb, er moet bij de kosten van de conformiteitsbeoordeling rekening worden gehouden met kleinere bedrijven en er komen trainingen, ondersteuning en subsidies. Dat is goed, maar de vraag is of dit in de praktijk genoeg is. Heeft het kabinet zicht op de daadwerkelijke nalevingskosten voor

verschillende typen en groottes bedrijven? Gaat de staatssecretaris monitoren of de CRA in de praktijk leidt tot hogere toetredingsdrempels voor start-ups en het mkb? Wat is voor de staatssecretaris hét moment om in te grijpen als blijkt dat die lasten inderdaad disproportioneel bij kleine bedrijven terechtkomen?

Daaraan gekoppeld het volgende. In het wetsvoorstel staat het voornemen om een regulatory sandbox op te richten bij de Rijksinspectie Digitale Infrastructuur. Ondernemers kunnen daarmee vooraf duidelijkheid krijgen over hoe zij innovatieve producten conform de CRA op de markt kunnen brengen. Het CDA is hier groot voorstander van. Kan de staatssecretaris aangeven wanneer deze sandbox operationeel is en hoe ervoor wordt gezorgd dat juist start-ups en mkb-bedrijven hier laagdrempelig gebruik van kunnen maken?

Dan mijn derde punt, de toekomstbestendigheid van deze wetgeving. Wij zien namelijk dat de technologische ontwikkelingen hard gaan. Iets dat gisteren nog veilig en verantwoord leek, is dat over een jaar niet meer door nieuwe dreigingen of andere zaken. Op welke manier kan de overheid hier samen met het bedrijfsleven op anticiperen? Blijven de standaarden en normen actueel of lopen we achter de feiten aan? En biedt dit ook een kans voor samenwerking op de marktintroductie van digitale innovaties?

Dan kom ik op het punt van de consumentenbescherming. Een fabrikant moet zijn product gedurende de verwachte gebruiksduur blijven ondersteunen en moet bij de verkoop duidelijk maken tot wanneer veiligheidsupdates worden geleverd. Dat lijkt technisch, maar heeft behoorlijk concrete gevolgen. Een laadpaal kan vijftien jaar meegaan, maar wat heeft een consument aan een slimme laadpaal die technisch nog uitstekend functioneert maar waarvan de digitale component na vijf jaar niet meer veilig gebruikt kan worden? Voor industriële producten is dit misschien nog wel relevanter. Machines kunnen 20 of 30 jaar meegaan, terwijl digitale componenten of software veel sneller verouderen, waardoor soms de gehele machine vervangen moet worden. Dat is zonde vanwege de verspilling van materiaal dat nog veel langer mee had gekund. Hoe kijkt de staatssecretaris naar die spanning? Hoe voorkomen we dat goed functionerende apparaten of machines feitelijk worden afgeschreven omdat één digitale component niet langer wordt ondersteund?

De CRA verplicht de fabrikant de ondersteuningsperiode te laten aansluiten bij de verwachte gebruiksduur. Die is in beginsel minimaal vijf jaar. Maar "verwachte gebruiksduur" is wel een vage en open norm, die de fabrikant uiteindelijk zelf vaststelt. Graag maken wij hierbij ook de koppeling met de voorgestelde digitale apk. Kan zo'n voorziening gebruikers ook duidelijkheid geven over hoelang een product nog wordt ondersteund en wat zij kunnen doen wanneer die ondersteuning afloopt? Ziet de staatssecretaris mogelijkheden om fabrikanten te stimuleren de ondersteuning overdraagbaar te maken wanneer zij die zelf niet langer willen of kunnen bieden? In preambule 61 van de verordening staat een optie dat fabrikanten na afloop van de ondersteuningsperiode zouden moeten overwegen de broncode vrij te geven aan het publiek of aan andere ondernemingen die de afhandeling van kwetsbaarheden willen overnemen. Daarbij mogen intellectuele eigendomsrechten worden beschermd, bijvoorbeeld contractueel. Dit is wat ons betreft een mooie optie. Hoe kijkt de staatssecretaris hiernaar en hoe zou ze die willen vormgeven?

Dan kom ik bij mijn vierde en laatste punt: wat als het misgaat? De CRA is er in de eerste plaats op gericht om cyberrisico's te voorkomen door al bij het ontwerp rekening te houden met de digitale veiligheid. Maar ook dan kan achteraf een kwetsbaarheid aan het licht komen. Denk aan een slimme deurbel, die onverwacht eenvoudig te hacken blijkt. De fabrikant moet actief en uitgebreid kwetsbaarheden melden en maatregelen nemen om deze te verhelpen. Maar wat gebeurt er als dat onvoldoende of niet snel genoeg gebeurt? Is er dan een centraal meldloket ingericht, ook in relatie tot de Cyberbeveiligingswet en de NIS2? Welke mogelijkheden heeft de RDI om bij een ernstig cyberrisico snel in te grijpen? Kan zij een fabrikant verplichten onmiddellijk een beveiligingsupdate uit te brengen? Kan een onveilig product worden teruggeroepen, uit de handel worden gehaald, online verwijderd worden of op zwart worden gezet? Hoe werkt dat bij software of apps? Kan ook worden afgedwongen dat deze niet langer worden aangeboden? Hoe snel zullen er ook boetes worden uitgedeeld, en van welke hoogte? Misschien nog wel belangrijker voor mensen die zo'n product al in huis hebben: hoe worden gebruikers snel gewaarschuwd als blijkt dat ze daadwerkelijk risico lopen? We moeten met elkaar ook leren van fouten. Gaan we geleerde lessen over uitgebuite kwetsbaarheden ook goed vastleggen in een register? Het heet de Resilience Act, dus dan komt ook de vraag op of we op deze manier veerkrachtig zijn. Hoe herstellen we? Hoe makkelijk kunnen we overschakelen op een alternatief of een back-upsysteem?

Voorzitter, tot slot. Het CDA steunt de richting van deze verordening. Digitale veiligheid hoort geen extraatje te zijn dat een consument achteraf moeten installeren. Het hoort onderdeel te zijn van een goed product. Maar dan moeten we er ook voor zorgen dat bedrijven weten wat er van hen wordt verwacht, dat kleine bedrijven niet vastlopen in procedures en dat dezelfde eisen daadwerkelijk ook gelden voor producten van binnen en buiten Europa. De uitvoeringswet legt daar de juridische basis voor neer. Nu komt het aan op de uitvoering en de handhaving daarvan.

Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Zwinkels. Dan geef ik het woord aan mevrouw El Boujdaini.

Mevrouw **El Boujdaini** (D66):
Dank u wel, voorzitter. In een gemiddeld Nederlands huis hangen tientallen apparaten aan het internet, zoals de router in de meterkast, de digitale deurbel, de babyfoon, de thermostaat, de omvormer van de zonnepanelen op het dak, de laadpaal voor de deur en de telefoon in je hand. Al die apparaten zijn toegangspoorten tot ons dagelijks leven. Wij moeten ervoor zorgen dat die poorten niet wagenwijd openstaan. Nu is het vaak zo dat mensen de consequenties ondervinden van fouten. Mensen worden slachtoffer van een datalek of de camera in huis waar een vreemde op meekijkt. Gaat het mis met de software van een ziekenhuis, een sluis of een ministerie, dan merkt heel Nederland dat. Dat is geen theorie. Vorige zomer moest het Openbaar Ministerie wekenlang van het internet af omdat aanvallers binnenkwamen via een lek in een product van een leverancier. Chinese staatshackers drongen bij Defensie binnen via een lek in een firewall. Al na de Citrixcrisis in 2020 was de conclusie van de Onderzoeksraad voor Veiligheid glashelder: leg de verantwoordelijkheid voor veilige software bij de maker, niet bij de gebruiker. Het goede nieuws is: dit is te regelen. Een veilig apparaat is geen kwestie van geluk, maar van afspraken. Die afspraken maken we vandaag met de rest van Europa.

Voorzitter. Voor het eerst gelden voor alle digitale producten in Europa dezelfde regels met deze wet: veilig vanaf de tekentafel, gratis beveiligingsupdates zolang je een product redelijkerwijs gebruikt. Ontdekt de fabrikant een lek, dan moet dat binnen 24 uur worden gemeld. Wie zich er niets van aantrekt, riskeert een boete tot 2,5% van de wereldwijde omzet. Hoe zien deze waarborgen er in de praktijk uit? Een voorbeeld: je koopt een slimme deurbel en op de doos staat "updates tot juni 2033" en er wordt ergens in Europa een lek ontdekt. Dan weet de fabrikant het binnen een dag en jij komt daarna. Veiligheid wordt zoiets waar je in de winkel al op kunt letten en waar bedrijven mee kunnen concurreren. Juist Nederlandse ondernemers, die het nu al goed doen, kunnen daarmee winnen.

Europa zet hiermee ook de standaard. Dat is digitale soevereiniteit in de praktijk. Wij bepalen de spelregels voor wat hier in de winkel ligt en niet de fabrikant aan de overkant van de wereld. En neemt de rest van de wereld die standaard over, dan wordt de hele keten ook veiliger. D66 steunt deze wet dan ook van harte. Het laat zien wat er kan als Europa samen optrekt. Maar een wet op papier maakt nog niemand veiliger. Het komt aan op de uitvoering. Daarom heb ik vandaag over drie dingen vragen: de ondernemers die het moeten gaan uitvoeren, de toezichthouder die het moet controleren en de toekomst waar deze wet klaar voor moet zijn.

Voorzitter. Nederland telt zo'n 52.000 fabrikanten en 12.000 importeurs en distributeurs die met deze regels te maken gaan krijgen. Veel van hen doen het al goed en voor hen is deze wet een kans. Veiligheid wordt eindelijk iets waarmee je je kunt onderscheiden, maar hieraan voldoen kost ook extra geld per nieuw product. En dan bestelt de buurman bijvoorbeeld voor een tientje een beveiligingscamera op Temu of Aliexpres, rechtstreeks van een verkoper die zich waarschijnlijk niets van onze veiligheidseisen aantrekt. Dat is onveilig voor de buurman en oneerlijk voor de Nederlandse ondernemer die hier wel in investeert.

Die ondernemer verdient een eerlijke kans en de buurman ook een veilig product. Daarom vraag ik de staatssecretaris of hierover nagedacht is en hoe er rekening is gehouden met de concurrentiepositie van bedrijven in Nederland en Europa die zich vaak al goed inzetten voor cyberweerbaarheid. Kan de staatssecretaris toezeggen dat zij zich in Europa blijft inzetten voor een gelijker speelveld, zodat de goedkope onveilige camera van buiten Europa het niet wint van de veilige producten van hier?

Voorzitter. Hoe werkt deze wet straks in de praktijk? Neem een bedrijf van vijf mensen dat slimme thermostaten maakt. Sinds half augustus valt het onder de Cyberbeveiligingswet, op 11 september komt de meldplicht van deze wet erbij en dan hebben we ook nog de AI-verordening. Als we zo veel van zo'n bedrijf vragen, moeten we ook helpen. Het eerste wat zo'n bedrijf nodig heeft, is iemand om het aan te vragen. Het ministerie is begonnen met webinars en een gids CRA, en straks komt er een nationaal communicatiekanaal. Hoe dat eruit gaat zien, is nog open. En vanuit Europa is er subsidie speciaal voor het mkb en microbedrijven. Komt er een helpdesk waar deze bedrijven terechtkunnen met vragen over de meldplicht en de samenloop met andere cyberwetten en wanneer kunnen we dat verwachten?

Hoe ziet de ondersteuning vanuit de Europese subsidie er voor Nederlandse bedrijven in de praktijk uit? Stel nu dat dit bedrijf ontdekt dat een lek in zijn thermostaat actief wordt

misbruikt, dan moet dat binnen 24 uur worden gemeld bij het NCSC. Zo kan er snel actie worden ondernomen en kan verdere schade worden voorkomen. Maar dit bedrijf wel met de vraag zitten of het onder de cyberweerbaarheidswet valt, onder de Cyberbeveiligingswet of onder allebei. De NCC legt uit hoe je moet melden, maar niet of dat voor beide wetten moet. Precies daar kunnen we nog het verschil maken. Kan het melden laagdrempeliger met ondersteuning voor kleine mkb- en microbedrijven? En hoe zorgen we dat bedrijven überhaupt weten dat ze moeten melden? Wat wordt er dus gedaan aan bewustwording?

Die melding komt vervolgens ook bij de RDI terecht, de toezichthouder. Diezelfde RDI kreeg in korte tijd de Cyberbeveiligingswet, de AI-verordening en nu deze wet erbij en moet straks tienduizenden fabrikanten volgen. De RDI levert goed werk en dan moeten we haar dus ook in staat stellen dat te kunnen blijven doen. Dus vraag ik de staatssecretaris hoe zij ervoor gaat zorgen dat de RDI al deze taken kwalitatief goed kan blijven uitvoeren.

Diezelfde thermostaat ligt ook in de winkels in Duitsland en Spanje. Dan moet de regel in Spanje hetzelfde betekenen als in Nederland. Ook hier in Nederland moet het duidelijk zijn. De Raad voor de rechtspraak waarschuwt dat de overlap met de NIS2 en de AI-verordening het toezicht kan versnipperen. Hij adviseert dan ook om meer duidelijkheid te creëren over hoe deze wetten zich tot elkaar verhouden, want een bedrijf wil gewoon weten welke regels voor hem gelden en bij wie hij moet zijn. Neemt de staatssecretaris het advies van de Raad voor de rechtspraak over en zorgt zij dat toezichthouders hier en in andere lidstaten de regels op dezelfde manier uitleggen en handhaven?

Voorzitter. De wet biedt ook een mooie kans. De gereguleerde testomgeving, ook wel de "regulatory sandbox", is een testomgeving waarin een fabrikant met de toezichthouder aan tafel zit voordat het product op de markt komt.

De **voorzitter**:
Ik hoorde een punt. De heer Van den Berg heeft een interruptie.

De heer **Van den Berg** (JA21):
Excuus dat ik wat later was, maar zo kon ik nog even eten na het vorige WGO. Dan even op de inhoud. Ik hoor mevrouw El Boujdaini vragen of er dan wel ondersteuning is voor die ondernemers, en specifiek ook voor de micro-ondernemers, maar het was eigenlijk een positieve verrassing voor mij toen ik zag dat de RVO sinds 7 september, volgens mij vandaag zelfs, Mijn cyberweerbare zaak heeft opengesteld, die precies in dit soort vragen voorziet. Was mevrouw El Boujdaini daar ook bekend mee?

Mevrouw **El Boujdaini** (D66):
Ik ben blij om te horen dat de heer Van den Berg dat aanhaalt. Alleen wil ik toch nog wel graag weten hoe dat er dan precies uitziet en ook of wat de RVO doet dan voldoende zou zijn. Ik denk zelf dat er nog heel vragen zijn op het gebied van toezicht en handhaving. De RVO gaat in principe niet over specifiek de toezicht en handhaving. Omdat die melding gedaan moet worden bij het NCSC en de RDI de toezichthouder is, denk ik toch dat er juist vanuit die hoek meer kan worden gedaan aan ondersteuning en hulp op dat gebied.

De **voorzitter**:
Een vervolgvraag.

De heer **Van den Berg** (JA21):
Dan nog even op een ander vlak, iets verder terug in de spreektekst. Ik hoorde mevrouw El Boujdaini vragen of het gelijke speelveld wel van toepassing is op een slimme deurbel of beveiligingscamera's, bijvoorbeeld van Temu, ten opzichte van de Europese markt. Maar is het niet zo dat we juist ook met de douane-unie en de Conformité Européenne dezelfde standaard afdwingen bij producten die worden geïmporteerd?

De **voorzitter**:
Dat zag ik als een tweede interruptie.

Mevrouw **El Boujdaini** (D66):
Ja. Hoe het volgens mij zit, is dat de fabrikanten, leveranciers en importeurs die we hier in Europa hebben, ervoor moeten zorgen dat de producten die ze naar Europa halen en hier vervolgens verkopen, voldoen aan die CRA. Maar op het moment dat de klant rechtstreeks bestelt bij Temu of AliExpress, hoeft daar niet per se een Europese leverancier tussen te zitten. Daar gaat het mij eigenlijk specifiek om, om dat stukje waar wij eigenlijk geen zicht op hebben omdat daar geen Europese tussenleverancier zit.

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

Mevrouw **El Boujdaini** (D66):
Ik vervolg met de regulatory sandbox. Dat is een testomgeving waarin een fabrikant met de toezichthouder aan tafel zit voordat het product op de markt komt. Vooraf weten waar je aan toe bent, in plaats van achteraf tegen problemen aanlopen: voor een innovatieve start-up is dat goud waard. Het is precies hoe wij toezicht graag zien: een partner die vooraf meedenkt. De RDI gaat de sandbox opzetten, maar over de invulling moet nog nagedacht worden. Wanneer komt er dus duidelijkheid over wat de sandbox precies inhoudt, wie er toegang toe krijgt en onder welke voorwaarden?

Voorzitter. Tot slot de toekomst. Een apparaat dat in 2028 wordt verkocht, draait in 2035 nog. Daarom moeten we voorbereid zijn. Als er vandaag gegevens worden gestolen, kunnen die straks met de kwantumcomputer worden ontsleuteld. Het goede nieuws is: de oplossing bestaat al. Kwantumveilige versleuteling is er, de standaarden zijn er en met Q-Tech in Delft en Quantum Delta NL heeft Nederland de kennis in huis om voorop te lopen. In het vorige debat heeft de staatssecretaris mij ook toegezegd om met een kwantumvisie te komen. Die is ook voor onze cyberweerbaarheid hard nodig. Ik kijk daar ook naar uit. Kan de staatssecretaris in die visie meenemen hoe we onze cyberwetten toespitsen op post-kwantumcryptografie? Kan zij toezeggen dat post-kwantumcryptografie een vast onderdeel wordt van de evaluatie van deze wet?

Voorzitter. Ik begon met de meterkast en de deurbel.

De **voorzitter**:
Voordat u daar ook mee afsluit, gaan we naar mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Ik had wel een vraag over dat vorige punt. Is mevrouw El Boujdaini het met mij eens dat het echt wel een probleem is dat die verwachte gebruiksduur nog zo'n open en vage norm is, nu er alleen staat "minimaal vijf jaar"? Ik dacht dat ze dat zojuist aanhaalde in haar stukje rondom kwantum. Als zij dat met mij eens is — ik stel gelijk de tweede vraag — is zij het dan ook met mij eens dat we daar een oplossing voor moeten vinden en dat we dat ook eventueel nog moeten aanpassen met elkaar in deze uitvoeringswet?

Mevrouw **El Boujdaini** (D66):
Wat voor ons vooral belangrijk is, is dat de producten zo veilig mogelijk zijn voor een zo lang mogelijke periode. Daarom gaf ik eerder in mijn betoog aan dat wanneer iemand een product op een redelijke wijze gebruikt, we er dan ook voor zorgen dat de juiste beveiligingsupdates altijd mogelijk zijn en gratis zijn, omdat de toegangspoort anders gewoon wagenwijd open gaat staan voor andere mogelijke statelijke actoren. Ik ben dus ook benieuwd naar de beantwoording van de vraag van mevrouw Zwinkels.

De **voorzitter**:
En u vervolgt.

Mevrouw **El Boujdaini** (D66):
Voorzitter, ik sluit af. Ik begon bij de meterkast en de deurbel, maar daar eindig ik ook. Mensen thuis hoeven geen cyberexpert te zijn. Ze moeten erop kunnen vertrouwen dat dat wat ze kopen, veilig is en veilig blijft en dat de rekening niet bij hen ligt als een fabrikant een steek laat vallen. Dat kunnen we regelen, niet met achterdocht maar met heldere afspraken en een overheid die ondernemers helpt om die afspraken na te komen. Het komt ook aan op de uitvoering. Daar blijft mijn fractie op letten. Als we dat goed doen, wordt Nederland niet alleen veiliger, maar ook een plek waar de veilige digitale producten van morgen vandaan komen. Daar werkt mijn fractie graag aan mee.

Dank u wel.

De **voorzitter**:
Dank voor uw inbreng. Dan gaan we naar mevrouw Kathmann.

Mevrouw **Kathmann** (PRO):
Dank, voorzitter. Laat ik beginnen met het toeteren op de loftrompet. De Europese Unie is goed op weg om stukje bij beetje onze digitale wereld terug te winnen. Het besef dat onze levens knetterdigitaal zijn geworden, daalt eindelijk in. Net zoals onze auto's een gordel hebben en ons eten wordt gecontroleerd op voedselveiligheid, moeten de digitale onderdelen van onze samenleving ook veilig zijn. Je zou zeggen dat dat de normaalste zaak van de wereld is, maar dit was lang niet verplicht. Belangrijke apps en software mochten verouderen, ook als dat betekende dat processen onveiliger werden. Met de komst van de Cyberweerbaarheidsverordening is dit verleden tijd. Fabrikanten worden verantwoordelijk gesteld: bouw jij software, dan moet die veilig zijn.

Ik begin met deze wet. Lang verhaal kort: die is eigenlijk prima en Progressief Nederland zal die steunen. Het gaat immers om een vrij simpele uitvoeringswet. De verordening die daarachter ligt, staat wat mij betreft voor een grotere omslag in ons denken. De digitale wereld hou je allang niet meer veilig door achteraf te handhaven en boos te worden. Dat lukt pas als je veiligheid als de basis ziet van onze digitale wereld. Je mag maximale beveiliging verwachten. De leveranciers van software en hardware staan daarvoor aan

de lat, niet de individuele consumenten, die erop moeten kunnen vertrouwen dat hun spullen goed en veilig zijn. Dat is niet anders dan de verwachting dat je moderne auto bijvoorbeeld met gordels komt. De verordening geldt straks echt voor alles, van je smartphone tot je deurbel tot je VPN en je dagelijkse apps.

Het kabinet schat in dat er zo'n 26.000 tot 52.000 fabrikanten zijn die straks aan de nieuwe regels moeten voldoen en onder Nederlands toezicht vallen. Aangezien we als Nederland wederom te laat zijn met de implementatie van de wet, heb ik daar een paar vragen over. Welke gevolgen heeft de late Nederlandse implementatie voor het voldoen aan de verordening? Hoe is die schatting van 26.000 tot 52.000 fabrikanten gemaakt? Kan het kabinet concreter aangeven welke fabrikanten straks wel of niet onder de verordening vallen? Zijn er al gesprekken met fabrikanten over deze verordening? Voorzien zij dat ze op tijd en volledig aan de eisen kunnen voldoen?

Simpel gezegd moeten de makers straks bewijzen hoelang hun diensten redelijkerwijs gebruikt gaan worden en moeten zij voor die gehele tijd ondersteuning bieden. Er is echter een groot verschil tussen een stukje software of hardware dat de komende 30 jaar onze sluizen veilig houdt en de tijdelijke festivalapp die je maar voor één zomer gebruikt. Daar heb ik wat vragen over. Hoe wordt de redelijke termijn van de ondersteuning in de praktijk vastgesteld? Bij wie ligt daarvoor de bewijslast? Hoe maak je een verschil tussen soorten apps en diensten? Aan welke tafels gebeurt dat en op basis van welke eisen? En hoe zorgt Nederland ervoor dat het belang van de consument in die gesprekken vooropstaat?

Dit soort details doen ertoe. Niks is namelijk zo veranderlijk als een onderneming en het is nogal wat om jarenlang ondersteuning te verwachten van kleine ontwikkelaars. Welke regels zijn er om ervoor te zorgen dat belangrijke updates blijven komen, ook als de fabrikant vóór de redelijke termijn failliet gaat, opgeheven wordt of is opgeslokt? Kan ondersteuning bijvoorbeeld ook geboden worden door derde partijen en, zo ja, hoe gaat dat in z'n werk? Hoe verschillen de verplichtingen voor de daadwerkelijke makers en de partijen die hun opdracht hebben gegeven om iets te bouwen? Oftewel: als de overheid iemand vraagt om software te bouwen, is de overheid er dan verantwoordelijk voor dat die software ondersteund blijft of is de maker daar dan verantwoordelijk voor?

In het uiterste geval stelt de verordening voor dat onveilige digitale producten van de markt geknikkerd kunnen worden; een zwaar middel met grote gevolgen, wat ik iets verder wil uitdiepen. Onder welke voorwaarden is hiervan sprake? Wanneer is de grens bereikt en wordt deze bevoegdheid ingezet? Hoe wordt omgegaan met de gevolgen van zo'n marktverbod als het gaat om hardware of software die noodzakelijk is voor een gevoelig proces? Dit soort vragen moeten voor 11 december 2027 beantwoord zijn, want dan treedt de verordening in werking. Dan moet dus iedereen weten welke technische eisen gelden. Ik hoop dat het kabinet daar dan meer duidelijkheid in kan verschaffen. Heeft het kabinet een tijdlijn voor de implementatie tot en met december 2027? Wat is het plan B als implementatie vóór die tijd niet lukt?

Dan het toezicht. De Rijksinspectie Digitale Infrastructuur zal in Nederland toezien op de verordening. Logisch volgens mij, maar ik vraag de staatssecretaris om deze keuze toch nog wat nader toe te lichten. Zijn er andere toezichthouders overwogen? Waaruit blijkt dat de RDI het best hiertoe in staat is? Hoe worden de middelen hiervoor bepaald? Het kabinet zegt dat alles gedekt wordt vanuit de EZ-begroting. Is dit nu goed geregeld, ook

als de kosten toch hoger uitvallen?

Dan de amendementen. Tot mijn grote blijdschap — ik word altijd blij van amendementen bij wetgeving — zag ik dat collega Van den Berg van JA21 vanmorgen nog wat amendementen heeft voorgesteld. Daar moet dit debat dan natuurlijk ook over gaan. Ik zal ze een voor een even langslopen. Ten eerste het amendement op stuk nr. 7 over het lokverbod. Daar zet PRO een vraagteken bij. Ja, het is een zwaar middel om als toezichthouder als een ander het woord te mogen doen, om zo te testen of een fabrikant zich aan de regels houdt, maar wellicht wel eentje dat met de juiste waarborgen uitlegbaar en effectief kan zijn. Helaas kan men op zo'n korte termijn slecht beoordelen wat precies de gevolgen zijn. Daarom kijk ik even naar het kabinet. Onder welke voorwaarden mag er worden uitgelokt? Kan worden verzekerd dat het uitlokken door de toezichthouder alleen aan de orde is als minder zware middelen niet logisch zijn? Welke gevolgen heeft dit amendement voor de minimumuitvoering van de verordening?

Dan het tweede: het amendement op stuk nr. 8 over de evaluatie na drie jaar. Daar ben ik positief over. Ingewikkelde wetgeving na een tijdje kritisch bekijken, dat is natuurlijk hartstikke goed, maar het is geen doel op zich. Daarom een paar vragen aan het kabinet. Sluit deze termijn aan op de verordening en is dit ook aan te sluiten op de evaluaties van samenhangende wetgeving, zoals ook de Cyberbeveiligingswet? Wat kunnen we eigenlijk met de uitkomsten van de evaluatie? Is er nationaal en in Europa ruimte om aanpassingen van de verordening voor te stellen?

Ook over het derde en laatste amendement ben ik positief. Wettelijke bewaartermijnen houden onze data veilig. En dat mag je verwachten van een toezichthouder. PRO ziet een voordeel in het wettelijk vaststellen hiervan. Daarom nog een paar vragen. Ik denk dat de indiener die zelf ook zo beantwoordt. Waarom is de termijn één jaar? Is korter of langer bijvoorbeeld ook overwogen, en zitten er nog problemen aan die termijn van één jaar, bijvoorbeeld gevolgen voor de toezichthouder als een zaak nog niet is afgerond na één jaar? Ik hoor het allemaal graag en betrek de antwoorden bij het uiteindelijke oordeel over de amendementen.

Natuurlijk staat deze verordening niet op zichzelf. Die hangt samen met de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten, de Europese ecodesignwetgeving en een hoop meer. Ik kan het een fabrikant niet kwalijk nemen als die de weg kwijtraakt in al dat papier, terwijl er best veel gevraagd wordt in het kader van meldplichten nakomen en compliance. Daarom heb ik bij de Cyberbeveiligingswet dit voorgesteld: laten we nou één meldloket maken, om het overzichtelijk te maken voor de fabrikanten. Wat mij betreft noem je dat bijvoorbeeld "MeldpuntNL" en breng je zo veel van die meldplichten samen, ook wat raakt aan de wetten van andere departementen. Hoe staat het met de uitvoering van de motie-Kathmann c.s. over één meldloket? Welke departementen zijn hierbij betrokken? Ziet de minister de mogelijkheid om hier ook andere meldplichten, zoals die voor datalekken onder de AVG of Seveso-meldingen, onder te brengen? Kan deze mogelijkheid onderzocht worden, expliciet met de samenwerking van andere departementen, en kan er later in het najaar worden teruggekoppeld? In de Digitale Omnibus wordt bijvoorbeeld ook één single entry point voorgesteld: één meldloket voor digitale ongelukken. Nederland kan van zoiets leren. Hoe kijkt het kabinet naar dit voorstel? Gaat Nederland ook zo'n mechanisme optuigen? En wordt de motie over het meldloket daarin meegenomen?

De **voorzitter**:
Ik hoorde een punt. De heer Van den Berg.

De heer **Van den Berg** (JA21):
Eerder een komma, voorzitter. Ik dacht, laat ik toch even reflecteren op het betoog van mevrouw Kathmann. Dank daarvoor, ook voor het doornemen. Kijk, het amendement op stuk nr. 9 gaat er eigenlijk specifiek over dat wanneer zo'n fictieve entiteit bijvoorbeeld in een woning binnentreedt en er daaruit geen overtreding blijkt, de gegevens die zijn opgenomen wel binnen een redelijke termijn verdwijnen. Ik bedoel: ik heb in het verleden bij de Koninklijke Marechaussee gewerkt en als je dan zag wat voor waarborgen er waren voordat je kon binnentreden in een woning ... Dan moest er iemand in levensgevaar zijn of anders moest het gaan om zeer zware misdrijven waarbij je echt niet kon wachten, omdat het zo'n beschermde omgeving is. Dan vinden wij het heel ver gaan als je, zeker wanneer het uiteindelijk niet terecht blijkt te zijn, wel al die gegevens van die persoonlijke levenssfeer hebt gedocumenteerd en die dan niet hebt verwijderd, want dat is op dit moment niet geregeld. Vindt u dat ook?

De **voorzitter**:
Ik begrijp dat u uw interruptie gebruikt om uw amendement toe te lichten, maar ik wil u graag vragen uw interrupties kort en bondig te houden. Mevrouw Kathmann, ga uw gang.

Mevrouw **Kathmann** (PRO):
Nou, dat is een hele goede vraag. Ik ben dus ook heel erg benieuwd naar de beantwoording van het kabinet, maar ik heb het amendement van JA21 ook gelezen, waarbij ik dacht: gaat dit nou bijvoorbeeld ook over het mystery shoppen? Dan denk ik: dat is minder relevant om te gaan beknotten. Ik snap namelijk dat het soms lastig is of als uitlokken voelt als je een tiener die eruitziet als een 24-jarige een winkel in stuurt en dat die dan niet wordt gepakt terwijl die alcohol koopt. Maar hierbij zou je dan gewoon een product kopen, zoals heel veel anderen ook doen, waarna je test of het aan de regels voldoet. Dat zou ik dus niet allemaal willen beknotten. En als iemand wel gepakt wordt en je hebt een kortere bewaartermijn ... Er zijn gewoon nog heel veel vragen, niet alleen over de voorwaarden van uw amendementen, maar ook over de vraag of we hiermee volgens het kabinet niet te rigoureus ingrijpen in de wet. Ik ben daar dus gewoon heel erg benieuwd naar.

De **voorzitter**:
De laatste interruptie van de heer Van den Berg.

De heer **Van den Berg** (JA21):
Dit is een echte interruptie. Maar het is een WGO, toch? Dan is er dus geen ...

De **voorzitter**:
We hebben afgesproken dat we vier interrupties doen; daarmee kijken we hoever we komen.

De heer **Van den Berg** (JA21):
Oké. Nou, dat heb ik even gemist door het korte diner.

Maar in ieder geval ken ik mevrouw Kathmann als een Kamerlid dat zich juist heel erg druk maakt om de Algemene verordening gegevensbescherming, de AVG. Daarin staan juist allerlei waarborgen opgenomen, bijvoorbeeld hoe je het moet borgen bij bijzondere persoonsgegevens. Je moet daar zorgvuldig mee omgaan. Eigenlijk had ik dus verwacht dat zeker PRO daarin mee zou gaan. Maar als ik het in dat perspectief plaats, is PRO dan nog te bewegen om toch voor dit amendement te stemmen?

Mevrouw **Kathmann** (PRO):
Nou, het is goed dat u die vraag stelt. Misschien heb ik me namelijk niet helder genoeg uitgedrukt, maar ik zei: in principe sta ik positief tegenover alle drie de amendementen. Maar ik ben heel benieuwd: zitten we dan niet te veel de wet te beknotten, en welke waarborgen horen dan bij de amendementen en welke waarborgen horen bij de wet? Ik ben hierin dus heel erg benieuwd naar de beantwoording van het kabinet. Maar mijn houding is open en positief.

De **voorzitter**:
Mevrouw Kathmann, u vervolgt uw betoog.

Mevrouw **Kathmann** (PRO):
Ja, het was een komma en eigenlijk wilde ik nu over de regulatory sandboxes beginnen, maar zowel mijn collega van het CDA als mijn collega van D66 hebben daar hele goede vragen over gesteld, dus dat kan ik dan even achterwege laten.

Twee andere punten. Ik lees in de toelichting waardering voor de Nederlandse inzet voor vrije en opensourcesoftware in deze verordening. PRO steunt dat van harte. Er zijn essentiële diensten die niet zouden bestaan zonder opensourcecomponenten. De rol van dit soort diensten moet dan ook op waarde worden geschat. Ik heb de volgende vragen voor het kabinet. Wat is de Nederlandse inzet geweest voor opensourcesoftware? Zijn deze punten voldoende ingewilligd in de uiteindelijke verordening? Is Nederland bereid zich op te blijven werpen als pleitbezorger voor opensourcesoftware? Hoe gaat het kabinet dit in Europa en ook nationaal uitdragen.?

Als laatste punt, de Caribische gebieden van het Koninkrijk. Tot mijn grote spijt zijn Bonaire, Sint-Eustatius en Saba niet meegenomen in deze verordening. Ik snap hoe dat technisch gezien kan, maar ik ben het er toch niet mee eens. We moeten echt toe naar een integrale samenwerking op digitale veiligheid. Ons hele Koninkrijk moet namelijk digitaal veilig zijn. Ik roep dit kabinet dan ook met klem op om beter met de BES-eilanden samen te werken en ook de belangen van de inwoners van de eilanden te vertegenwoordigen bij de kabinetsinzet op dit terrein. Hoe wordt de Nederlandse inzet voor Europese cyberwetgeving afgestemd met de BES-eilanden? Is hier bij deze verordening ook sprake van geweest? Is het kabinet bereid om alle mogelijkheden aan te grijpen om Europese cyberwetgeving ook zo veel als mogelijk te laten gelden in Caribisch Nederland?

Tot slot. Er ligt hier eigenlijk wel weer een hele mooie schakel in dat hele totaalpakket van onze digitale veiligheid. Dat is gewoon echt van groot belang. Brussel kan dat en Nederland moet dat ten volste ondersteunen. Beter nog, eigenlijk zouden we als Nederland daarin voorop moeten willen lopen. We blijven het kabinet daarom aansporen om dat vooral te blijven doen. Ik ben heel erg benieuwd naar de beantwoording van alle vragen.

De **voorzitter**:
Voordat u helemaal afsluit, heeft u nog een interruptie van mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Dank aan mevrouw Kathmann voor haar inbreng. Ik hoorde een tweetal zaken die mooi in het verlengde liggen van wat ik had ingebracht. Die gaan over open source. Wat als een bedrijf failliet gaat of als er een situatie ontstaat waardoor het bedrijf niet meer in staat is om die ondersteuning en beveiligingsupdates te bieden? Ik had zelf de suggestie gedaan om vanuit preambule 61 te kijken of we de optie kunnen gebruiken waarin dat overdraagbaar is en we de broncode publiek vrij kunnen geven of dat het via het intellectueel eigendomsrecht contractueel overgedragen kan worden. Ik heb aan de staatssecretaris gevraagd hoe ze kijkt naar die opties. Ik ben uiteraard ook benieuwd hoe mevrouw Kathmann kijkt naar de voorstellen die ik zojuist heb gedaan.

Mevrouw **Kathmann** (PRO):
Dan moet ik eigenlijk in de eerste plaats mevrouw Zwinkels complimenteren, want ik had een hele open vraag gesteld hierover: zouden ook derden dat over kunnen nemen, wat gebeurt er dan? Ik dacht: dan ga ik eens even achterover hangen en kijken waar het kabinet mee komt. Mevrouw Zwinkels heeft dat beter aangepakt en is zelf met hele goede voorstellen gekomen. Het lijkt me hartstikke goed om daarnaar te kijken.

De **voorzitter**:
Dank u wel. Dan kijk ik naar de heer Van den Berg. Ga uw gang.

De heer **Van den Berg** (JA21):
Dank u wel, voorzitter. Vrijdag gaat de Europese meldplicht in. Fabrikanten moeten dan klaarstaan. Dan wil JA21 vandaag weten: staat de overheid zelf al klaar? Digitale veiligheid raakt mensen namelijk thuis en bedrijven op de werkvloer. Een slecht beveiligde router kan een bedrijfsnetwerk blootstellen aan een aanval. Een kwetsbaar apparaat kan een productieproces stilleggen. Wie zulke producten verkoopt, moet verantwoordelijkheid nemen voor de beveiliging, ook na de verkoop. Maar het woord "cyberveiligheid" is geen vrijbrief voor iedere nieuwe overheidsbevoegdheid en ieder extra formulier. Wij willen veilige producten en een overheid die haar eigen grenzen kent. Daar gaat deze Nederlandse uitvoeringswet over.

Neem het toezicht onder een fictieve identiteit, het zogeheten "mystery shopping". Een inspecteur doet zich voor als klant en koopt een product. Dat kan nodig zijn. Wie weet dat de inspectie langskomt, kan de zaken mooier voorstellen dan ze zijn. Maar hier geldt een eenvoudige grens: de overheid mag een overtreding ontdekken, maar de overheid mag die overtreding niet zelf creëren. Een inspecteur mag vaststellen wat een ondernemer doet. Hij mag een ondernemer niet aanzetten tot een overtreding die deze zelf niet van plan was en hem daar dan vervolgens voor beboeten. De toelichting bij deze wet erkent die grens. Dan moet hij ook in de wet zelf staan. Ondernemers moeten hun rechten kunnen nalezen in de bepaling die de inspecteur zijn bevoegdheid geeft, zeker als het onderzoek kan leiden tot een boete. Dat is de inzet van mijn amendement over het uitlokkingsverbod. Steunt de staatssecretaris die wettelijke grens en bevestigt zij dat de inspectie voor zo'n onderzoek vastlegt waarom gewone controlemiddelen niet volstaan? Dat kan gewoon in de bestaande verslaglegging. Ook de overheid moet kunnen uitleggen waarom zij zo'n zwaar middel nodig heeft.

Voorzitter. Stel dat de inspecteur een product koopt en na onderzoek geen overtreding vaststelt. De ondernemer heeft zijn zaken bij deze controle op orde, maar zijn persoonsgegevens staan inmiddels wel in een verslag van heimelijk toezicht. Hoe lang blijven die daar dan staan? De AVG stelt daar al grenzen aan. De vraag is wat die grenzen voor deze ondernemer concreet betekenen. "Niet langer dan noodzakelijk" staat er dan. Dat vertelt hem nog niet op welke datum zijn gegevens worden verwijderd. Mijn amendement maakt dat concreet. Persoonsgegevens in het verslag worden in beginsel uiterlijk na één jaar na het opstellen verwijderd. Hebben de bevindingen geleid tot een boete of een andere handhavingsbeslissing, dan kan bewaring langer noodzakelijk zijn. Maar ook dan geldt de grens: verwijderen zodra het niet meer nodig is, met een maximum van vijf jaar nadat die beslissing onherroepelijk is geworden. "Misschien komt het later nog van pas" is voor JA21 geen reden om persoonsgegevens te blijven bewaren. Natuurlijk moet bewijs beschikbaar blijven als iemand dat nodig heeft om zijn recht te halen. Ook de wettelijke archiefplichten moeten worden gerespecteerd. Wil de staatssecretaris uitleggen hoe zij dat combineert met een duidelijke grens aan het bewaren van persoonsgegevens?

Voorzitter. Dan de evaluatie. Als deze Kamer de overheid nieuwe bevoegdheden geeft, dan moet zij ook controleren wat ermee gebeurt. Hoe vaak wordt heimelijk gecontroleerd en wat levert dat dan op? Houden de besluiten stand bij de rechter? Hoeveel tijd en geld zijn kleine bedrijven kwijt aan de uitvoering van deze regels? Dat zijn vragen over Nederland. Een Europese evaluatie ontslaat ons niet van onze eigen verantwoordelijkheid. Mijn amendement regelt daarom een evaluatie binnen drie jaar na inwerkingtreding van deze wet. Wil de staatssecretaris bevestigen dat die dan onafhankelijk wordt uitgevoerd? Daarmee bedoel ik dat die niet door de Rijksdienst Digitale Infrastructuur wordt uitgevoerd. En wil zij de Kamer in 2028 al informeren over eerste ervaringen en knelpunten, als die er zijn? Ik wil weten of onveilige producten worden aangepakt en of de lasten voor ondernemers binnen de perken blijven. Alleen het aantal controles op verstuurde brieven zegt mij te weinig. Gebruik bestaande gegevens zo veel mogelijk. Een onderzoek naar regeldruk moet geen nieuwe bureaucratische molen worden.

Voorzitter. Neem een klein softwarebedrijf, waarvan de ontwikkelaar soms ook de verkoper is, de helpdesk en degene die 's avonds de administratie doet. Dat heeft geen juridische afdeling om iedere Europese verordening helemaal uit te pluizen. Zo'n bedrijf kan onder meerdere Europese regels vallen en die regels komen uiteindelijk op hetzelfde bureau van die ondernemer terecht. Den Haag hoeft daar niet nog eens een keer een extra stapel bovenop te leggen. JA21 wil daarom geen onnodige Nederlandse extra eisen, geen nationale koppen. Laat bedrijven dezelfde documentatie hergebruiken waar dit kan. Zorg voor één duidelijke route bij samenlopende verplichtingen en voor iemand die technische vragen echt kan beantwoorden. In april kondigde het kabinet een communicatiekanaal en een testomgeving bij de RDI aan. Wat werkt daarvan vandaag bij die aankondiging? Waar kan een kleine ontwikkelaar terecht? Wat kost dat en hoe snel krijgt hij antwoord? Meten we vervolgens of hij hulp, tijd en geld bespaart? Een website online zetten is nog geen geslaagde ondersteuning. En hoe controleert de staatssecretaris producten van buiten Europa die hier worden verkocht? Ik hoorde het een collega net al zeggen, een Nederlandse ondernemer mag niet alle kosten van alle regels dragen terwijl een concurrent met een onveilig product onder de radar blijft. Wie hier verkoopt, moet aan dezelfde eisen voldoen. Laat ik daaraan toevoegen dat voor mij

nog niet helemaal scherp is of bedrijven zoals Temu alsnog aan diezelfde regelgeving moeten voldoen of dat we daar nog aanpassingen op moeten maken.

Dan terug naar vrijdag 11 september. Dan begint de meldplicht voor actief uitgebuite kwetsbaarheden en ernstige incidenten. ENISA heeft het Europese meldplatform getest en plant de start op die datum. Is de Nederlandse ontvangst en opvolging al klaar, met voldoende mensen en bereikbaarheid bij urgente meldingen? En wat doet de fabrikant als het platform uitvalt? ENISA noemt rechtstreeks contact met het bevoegde incidententeam wanneer onmiddellijk contact nodig is en alsnog melden via het platform zodra het weer werkt. Zorg dat Nederlandse bedrijven die route kennen. Wil de staatssecretaris ook voor vrijdag duidelijk maken hoe zij moeten handelen en aantoonbare storingen kunnen vastleggen? Die meldingen bevatten bovendien gevoelige informatie over beveiligingslekken. Wie krijgt dan de toegang om te voorkomen dat technische details onnodig worden verspreid voordat een lek is verholpen? Wie ondernemers verplicht te melden moet ook zorgvuldig met die informatie omgaan.

Op 11 december 2027 — het werd al gezegd — gaan die volledige producteisen gelden. Daarvoor zijn Europese normen en voldoende keuringscapaciteit nodig. Niet elk product hoeft extern te worden gekeurd. Maar waar dit wel moet, mag een ondernemer niet vastlopen omdat er niemand beschikbaar is om zijn product te beoordelen. Hoeveel geschikte instanties zijn er? Welke wachttijden verwacht de staatssecretaris? Wat is de uitweg als Europese normen te laat komen? Een start-up kan de salarissen niet betalen met de mededeling dat de uitvoering nog in ontwikkeling is.

Dan tot slot. JA21 wil dat onveilige digitale producten worden aangepakt. Daarvoor moeten fabrikanten hun verantwoordelijkheid nemen en moet de overheid haar werk doen. Onze amendementen stellen grenzen aan het heimelijke toezicht en het bewaren van persoonsgegevens en verplichten tot verantwoording over de uitvoering. Ik vraag de staatssecretaris die voorstellen te steunen en concreet te maken hoe zij ondernemers door deze invoering helpt. Kortom, wie ondernemers aan strenge eisen houdt, moet zijn eigen uitvoering wel op orde hebben. En vrijdag is daarvoor de eerste test van onszelf.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan geef ik graag het voorzitterschap even door aan mevrouw Zwinkels, aangezien ik namens de VVD het woord zal voeren.

Voorzitter: Zwinkels

De **voorzitter**:
Dat voorzitterschap aanvaard ik. Als tijdelijk voorzitter geef ik graag het woord aan de heer Bikkers van de VVD voor zijn inbreng.

De heer **Bikkers** (VVD):
Dank u wel. Ik vervang vandaag mevrouw Rajkowski en dat doe ik heel graag. Ik zal dat waarschijnlijk niet zo goed doen als zij, maar zij luistert mee. Ik heb beloofd dat te zeggen, dus dat heb ik in ieder geval gedaan.

Voorzitter. Steeds meer mensen worden slachtoffer van cybercriminelen en ondervinden hiervan vaak financiële en mentale schade. Als consument mag je verwachten dat als je een product koopt met een digitale component, de fabrikant er alles aan doet dat het product veilig is en blijft. Daarom vinden wij het goed dat deze verordening dit tracht te regelen. Voor de consument moet het echter duidelijk zijn waar hij terecht kan, wanneer een fabrikant van een product met een digitaal component failliet gaat tijdens de verwachte levensduur van dat product; mevrouw Zwinkels en mevrouw Kathmann spraken daar ook al over. Ook moet de consument laagdrempelig aan de bel kunnen trekken wanneer er geen veiligheidsupdates meer worden aangeboden, terwijl dit nog wel verplicht is volgens de verordening. Hoe voorkomen we rechtszaken en procedures en zorgen we ervoor dat de consument laagdrempelig gebruik kan maken van de bescherming die de verordening tracht te bieden? Graag een reactie van de staatssecretaris.

Daarnaast maken we ons zorgen over de toenemende regeldruk voor de mkb'ers. Ook daar werd al een aantal keren aan gerefereerd. We moeten voorkomen dat Nederland de uitvoering van deze verordening strenger interpreteert dan andere landen en daarmee onze innovatiekracht onnodig remt. Er is ook al gesproken over de regulatory sandbox. We zien graag dat die zo snel mogelijk toegankelijk is. We zijn benieuwd wanneer die beschikbaar is.

Als laatste is mijn fractie nieuwsgierig naar de 16,5 miljoen subsidie die beschikbaar is gesteld door de Europese Commissie voor ondersteuning bij de naleving van deze wet. Hoe worden startende en kleine Nederlandse ondernemers zo goed mogelijk naar deze subsidie gedirigeerd? Graag een reactie van de staatssecretaris.

Tot zover.

De **voorzitter**:
Dank voor uw inbreng. Ik zie geen interrupties, dus ik draag het voorzitterschap weer graag aan u over en dan kunnen we verder met de vergadering.

Voorzitter: Bikkers

De **voorzitter**:
Dank u wel. Dan zijn we aan het einde gekomen van de eerste termijn van de zijde van de Kamer. Ik kijk even naar de staatssecretaris om te zien hoelang zij wil schorsen.

Staatssecretaris **Aerdts**:
Mijn voorstel zou zijn tot 20.10 uur.

De **voorzitter**:
Er zijn aardig wat vragen gesteld, dus ik vind het een goed voorstel. Laten we tot 20.10 uur schorsen en dan zien we elkaar terug.

De vergadering wordt van 19.25 uur tot 20.13 uur geschorst.

De **voorzitter**:
Dames en heren, ik heropen de vergadering en geef graag het woord aan de staatssecretaris voor de beantwoording namens het kabinet.

Staatssecretaris **Aerdts**:
Dank, voorzitter. We hebben al allerlei slimme items voorbij zien komen: van babyfoons tot slimme horloges, van apps op je telefoon tot bedrijfssoftware en de computers waarmee fabrieken en sluizen worden aangestuurd. Digitale producten maken onderdeel uit van ons dagelijks leven. Dat geldt voor alle onderdelen van de maatschappij. Het is dan ook belangrijk dat we erop kunnen vertrouwen dat deze producten digitaal veilig zijn en dat zij niet door een kwaadwillende partij kunnen worden uitgeschakeld of gehackt om persoonlijke data of bedrijfsgevoelige gegevens te stelen. En het is belangrijk dat de verantwoordelijkheid voor de digitale veiligheid van producten op de Europese markt wordt neergelegd bij de fabrikanten, importeurs en distributeurs, net zoals dat al tientallen jaren geldt voor de fysieke veiligheid van producten op de Europese markt. De Cyber Resilience Act regelt dit. Daarom ben ik blij dat we hier vandaag zitten om te spreken over de Uitvoeringswet verordening cyberweerbaarheid, ook wel de Cyber Resilience Act, de CRA, genoemd. Deze Europese verordening gaat ontzettend veel betekenen voor de weerbaarheid van zowel consumenten als bedrijven en organisaties in Nederland en in de Europese Unie: iedereen die gebruikmaakt van producten met digitale componenten, alle hardware, software en componenten.

Op grond van de CRA moeten al deze digitale producten aan essentiële cybersecurity-eisen voldoen, voordat ze op de Europese markt mogen worden aangeboden. Producten moeten secure-by-design worden ontworpen en secure-by-default worden aangeboden. De CRA introduceert een meldplicht voor fabrikanten bij ernstige beveiligingsincidenten of misbruik van zwakke plekken in hun producten. De CRA bevat ook een zorgplicht, waardoor fabrikanten verantwoordelijk worden om producten voor de hele verwachte gebruiksduur veilig te houden met gratis veiligheidsupdates, die in beginsel automatisch kunnen worden geïnstalleerd. Hierdoor kunnen consumenten en bedrijven rekenen op veilige digitale producten op de Europese interne markt. Dit is iets waar ik me graag voor inzet. Met de uitvoeringswet die voorligt, worden uitvoering, toezicht en handhaving van de Europese verordening in Nederland geregeld. De Rijksinspectie Digitale Infrastructuur, de RDI, wordt hierin aangewezen als toezichthouder. Ook wordt de RDI aangewezen als de autoriteit voor het beoordelen, aanmelden en monitoren van de testhuizen, die nodig zijn om de belangrijke en kritieke producten te testen. Het Nationaal Cyber Security Centrum zal het meldloket voeren voor de verplichte melding op grond van de CRA.

De eerste deadline uit de CRA is gepasseerd en de volgende naderen. Vanaf juni zou het mogelijk moeten zijn om de testhuizen aan te wijzen. De meldplicht bij ernstige beveiligingsincidenten of actief misbruikte kwetsbaarheden start al vanaf 11 september. We hebben dat vandaag al een aantal keer gehoord. Vanaf december 2027 moeten alle digitale producten veilig ontworpen en geproduceerd zijn voordat ze op de Europese markt mogen worden gebracht. Het is daarom van belang dat we zorgen voor een spoedige implementatie van het toezicht en de handhaving waarmee we de digitale weerbaarheid van Nederland verhogen.

Voorzitter. Ik heb verschillende onderwerpen bij elkaar gepakt, te beginnen met bedrijfsleven, mkb en start-ups. Vervolgens de implementatie en de werking van de wet, toezicht en toezichthouders, en overig. Daarna wou ik de amendementen en vragen die rond de amendementen zijn gesteld zowel appreciëren als beantwoorden.

Om te beginnen een vraag die door zowel mevrouw El Boujdaini als mevrouw Zwinkels is gesteld: is erover nagedacht wat het betekent als mensen producten bestellen van buiten Europa? Temu is hierbij een aantal keren als voorbeeld genoemd. Elk digitaal product dat binnen het toepassingsbereik van de CRA valt en dat op de Europese markt wordt gebracht moet aan de essentiële cybersecurityeis van de CRA voldoen. Dat geldt ook voor fabrikanten van buiten de EU die hun producten aanbieden op de Europese markt. Er is dus geen sprake van een concurrentievoordeel voor fabrikanten van buiten de Unie. Omdat fabrikanten onder de CRA verplicht zijn om alleen producten op de markt te brengen die cybersecured by design zijn, kan dit ook in de export juist een kwaliteitsvoordeel voor Nederlandse producenten opleveren. Europese producten zijn namelijk gegarandeerd digitaal veilig.

Het is ook mogelijk dat consumenten individueel producten kopen via buiten de EU gevestigde handelsplatforms. Volgens mij zijn dat de voorbeelden waarover we vanavond spraken. Ook deze moeten aan de eisen van de CRA voldoen. Dat is in de eerste plaats de verantwoordelijkheid van degene die het product aanbiedt, maar ook — indien daarvan sprake is — de platforms die tussenpersoon zijn, hebben daarin een verantwoordelijkheid.

De Europese Digitaledienstenverordening, DSA, is ook van toepassing op buiten de EU gevestigde platforms die hun diensten aanbieden in de Unie. Zij kunnen aansprakelijk worden gesteld als er via hun platform illegale producten worden verhandeld en als ze niet tijdig reageren op meldingen daarover. Ook gelden er zorgvuldigheidsverplichtingen voor hen, waaronder voor de traceerbaarheid van handelen en het kunnen tonen van de vereiste CE-markering op hun platforms. Voor consumenten … Nee, laat ik het daarbij laten.

Een vraag was ook hoe Nederlandse bedrijven hierbij ondersteund worden. Onder anderen mevrouw Zwinkels stipte dat aan. Er zijn verschillende documenten beschikbaar die de CRA op een begrijpelijke manier uitleggen aan bedrijven. Het ministerie van Economische Zaken heeft de Gids CRA uitgebracht. De Europese Commissie heeft al richtsnoeren opgesteld die de wet uitleggen. Er komen een nationaal communicatiekanaal en een veilige testomgeving voor innovatieve producten. Voor mkb-bedrijven is er extra ondersteuning. Zo worden er vanuit subsidie digitale hulpmiddelen beschikbaar gesteld vanuit het Digital Europe Programme.

Mevrouw El Boujdaini vroeg of er een helpdesk voor bedrijven komt voor vragen over de meldplicht die ingaat, juist ook over de samenloop van verplichtingen uit andere wetten op het gebied van cybersecurity. Mevrouw Kathmann ging daar ook op in. Ja, die ondersteuning is er al. Het NCSC biedt echt helpdeskondersteuning aan fabrikanten met betrekking tot de meldplicht. Daarnaast is voor bedrijven toegankelijke informatie over de verplichtingen uit de CRA beschikbaar. Ik noemde net al de CRA-gids die het ministerie van EZK heeft uitgebracht. Ook de Europese Commissie heeft uitgebreide richtsnoeren opgesteld, ook wel "guidance", waarin de werking van de verschillende onderdelen van de verordening wordt uitgelegd. Ook zijn allemaal frequently asked questions opgenomen. Verder werken wij bij EZK aan de inrichting van een nationaal communicatiekanaal waar bedrijven terechtkunnen met alle vragen die ze mogelijk nog hebben over de CRA.

Mevrouw El Boujdaini vroeg hoe de subsidie die beschikbaar wordt gesteld voor Digital

Europe eruit komt te zien. Die subsidie wordt beschikbaar gesteld via een opgezet project, namelijk het SECURE-project. Hiermee kunnen mkb-bedrijven cofinanciering krijgen voor interne acties die ze ondernemen om hun producten aan de CRA te laten voldoen. Hierbij kan gedacht worden aan het uitvoeren van kwetsbaarheidstesten, het volgen van cybersecuritytrainingen of het ontwikkelen van software om cybersecurity by design te kunnen produceren. Per project kan maximaal €300.000 aan subsidie worden aangevraagd. In totaal is er 16,5 miljoen euro beschikbaar, verdeeld over twee rondes. De eerste ronde is al begin van dit jaar opengesteld. Verschillende Nederlandse bedrijven hebben dan ook al een aanvraag ingediend.

Mevrouw Kathmann vroeg hoe het kabinet aankijkt tegen het Omnibusvoorstel voor een single entry point. Gaat Nederland ook zo'n mechanisme optuigen en wordt de motie over het meldloket daarin meegenomen? Het kabinet steunt het stroomlijnen van meldplichten op Europees niveau. Daarbij is het wel van belang dat ook de vertrouwde relatie die bedrijven bijvoorbeeld met het Nationaal Cyber Security Centrum al hebben, behouden blijft. Melden op nationaal niveau moet daarom mogelijk blijven. Het NCSC zorgt voor een goede koppeling met ENISA, het Europees agentschap voor cyberbeveiliging. Ik houd rekening met de motie. Vandaar ook dat het meldloket voor de CRA aansluit bij dat van de Cbw, zodat bedrijven zich allemaal bij het Nationaal Cyber Security Centrum kunnen melden.

Mevrouw El Boujdaini vroeg of de meldplicht op een laagdrempelige manier kan worden ingericht, waarbij ook ondersteuning wordt geboden aan micro- en mkb-bedrijven. Wij vinden het ontzettend belangrijk om de meldplicht op een zo eenvoudig mogelijke wijze mogelijk te maken. Daarom is er voor de meldplicht onder de CRA ook zo veel mogelijk aangesloten bij het meldloket voor de Cyberbeveiligingswet, zodat de bedrijven bij één loket bij het NCC terechtkunnen, daar al hun vragen kunnen stellen en daar meteen goed geholpen kunnen worden. Het NCC biedt via zijn klantcontactcentrum helpdeskondersteuning aan bedrijven bij het doen van meldingen onder de CRA. Dat is op dit moment al zo. Dat is vanaf vrijdag zo, maar dat is nu ook al zo op grond van de Cyberbeveiligingswet, dus dat is echt wel volledig ingericht.

Mevrouw El Boujdaini stelde ook de vraag of er gewerkt wordt aan bewustwording, zodat bedrijven ook inderdaad gaan melden. Om bedrijven bewust te maken, worden diverse communicatiekanalen ingezet, onder andere de website van het NCSC, maar ook die van de RDI. Ook via brancheverenigingen wordt dit onder de aandacht gebracht. Er worden regelmatig presentaties gegeven over de CRA, bijvoorbeeld via webinars en congressen. We proberen echt zo veel mogelijk alle verschillende partijen te benaderen op de plekken waar ze zelf al actief zijn. Bijvoorbeeld is er twee weken geleden op het ministerie van EZK samen met het NCSC een webinar gegeven aan het bedrijfsleven. Daaraan deden 150 deelnemers mee. Daarin werd ook een demonstratie van de meldplicht gegeven. Dit webinar zullen we in het najaar nog een keer herhalen. Mogelijk, als dat nodig is, zullen we dat volgend jaar nogmaals doen.

Mevrouw Zwinkels stelde de vraag wanneer het moment is om in te grijpen als een disproportioneel grote last bij het mkb terechtkomt. Ook vroeg zij wanneer de sandbox, de veilige testomgeving, beschikbaar zal zijn. De producten van mkb-bedrijven moeten aan dezelfde kwaliteitseisen voldoen, maar in de CRA is nadrukkelijk wel voorzien in manieren om de regeldruk voor het mkb te verlichten; u schetste dat zelf ook al. Dit is natuurlijk iets om nadrukkelijk in de gaten te houden. In het amendement wordt ook

gesproken over een evaluatie. Er komt een Europese evaluatie aan. Ik kan me goed voorstellen dat wij als Nederland daarbij zullen aansluiten. Als daaruit inderdaad naar voren zou komen dat de lastendruk onevenredig is, is dat natuurlijk iets wat we op moeten gaan brengen.

Mevrouw Kathmann vroeg mij nog of er gesprekken met fabrikanten zijn geweest over de verordening en of zij voorzien dat zij op tijd volledig aan de eisen kunnen voldoen. Er vinden gesprekken met fabrikanten plaats, onder andere tijdens de voorlichtingsbijeenkomsten die georganiseerd worden. Hiermee worden fabrikanten aangespoord om tijdig aan de eisen te voldoen. Er is dus zeker al contact met de fabrikanten geweest. Ik kan me ook voorstellen dat zij zullen aangeven waar zij tegenaan lopen, zodat wij dat kunnen meenemen.

Dan was er nog de vraag van mevrouw Kathmann over de stand van zaken rond de eerder ingediende motie over het centraal meldpunt in Nederland. Wij vinden het belangrijk dat er één plek is waar je naartoe kan gaan, het liefst een bekende plek waar je al bekend bent en de mensen of hun telefoonnummer kent. Daarom hebben wij ervoor gekozen om het meldloket te laten aansluiten bij het meldloket voor de cyberbeveiligingsrichtlijn. Over het vervolg van de motie wordt u door mijn collega van JenV in Q4 van dit jaar geïnformeerd, zoals ook in de motie specifiek genoemd staat.

Alle meldplichten rond cybersecurity hebben we dus op dit moment op één plek bij het NCSC belegd. Dat is ook het antwoord op de vraag van mevrouw Zwinkels of er een centraal meldpunt ingericht is in relatie tot de cybersecurity. Dat meldpunt is bij het NCSC, waar deze dingen gemeld kunnen worden.

Mevrouw Kathmann vroeg nog hoe de schatting is gemaakt van 26.000 tot 52.000 fabrikanten die onder de wet zouden vallen. Er is geen exacte informatie beschikbaar over het aantal fabrikanten, importeurs en distributeurs dat aan de verplichtingen van de CRA moet voldoen, omdat het niet op deze manier wordt geregistreerd. Bedrijven kunnen bovendien natuurlijk meerdere rollen vervullen. In de memorie van toelichting heeft het kabinet deze getallen genoemd op basis van de cijfers van het Centraal Bureau voor de Statistiek. Die houden dit ook niet precies op die manier bij; vandaar dat wij die vrij grote range aangeven. Uit de algemene gegevens uit StatLine, de databank van het CBS, werd afgeleid dat er naar schatting tussen de 26.000 en 52.000 fabrikanten en 12.000 importeurs en distributeurs in Nederland aan de regels van de CRA moeten voldoen. Hierbij is gekeken naar de aantallen bedrijven die betrokken zijn bij het produceren en verkopen van de verschillende producten die onder de brede scope van de CRA vallen.

De heer Bikkers vroeg mede namens mevrouw Rajkowski hoe Nederlandse ondernemers naar de door de Europese Commissie beschikbaar gestelde subsidie worden gedirigeerd. Het ministerie van Economische Zaken en NCC-NL, van RVO, hebben eind 2025 al een webinar voor het bedrijfsleven georganiseerd. Dat was speciaal om al aandacht te vragen voor de mogelijkheid voor bedrijven om zich begin 2026 in te schrijven voor de eerste subsidieronde. Ook de Europese Commissie heeft een informatief webinar georganiseerd. Verder heeft het ministerie van Economische Zaken verschillende sectorale informatiebijeenkomsten georganiseerd, waarbij ondernemers onder andere gewezen zijn op de subsidiemogelijkheden en de rol van het nationale competentiecentrum hierbij. Ook werd er aandacht gevraagd door middel van

informatieve mails en nieuwsbrieven die door hen verstuurd worden.

Dan nog de vraag van mevrouw Zwinkels hoe ik ga monitoren of de CRA leidt tot hogere markttoetredingsdrempels voor het mkb en voor start-ups. De CRA leidt natuurlijk tot hogere toetredingsdrempels in de zin dat het mkb en start-ups ook moeten zorgen dat hun producten cybersecure zijn als ze op de markt worden gebracht. Inherent is het natuurlijk een drempel, maar wij vinden secure by design en secure by default zo belangrijk, dat wij daar wel voor gaan. Er is een drempel, maar we zullen natuurlijk kijken wat de reacties daarop zijn in de komende tijd, als dit ingevoerd gaat worden.

De **voorzitter**:
Bent u daarmee klaar met het eerste blokje?

Staatssecretaris **Aerdts**:
Ja, ik ben klaar met het blokje bedrijfsleven, mkb en start-ups.

Mevrouw **Zwinkels** (CDA):
Dank aan de staatssecretaris voor de eerste beantwoording. Ik heb eigenlijk nog twee vragen bij dit blokje. De eerste vraag is nog niet helemaal beantwoord. Die ging over de pakkans ten aanzien van oneerlijke concurrentie door niet-Europese landen en fabrikanten. Ik heb aangegeven dat dat om zo veel pakketten gaat en dat dat niet altijd via een platform gaat. Hoe gaan we die pakkans zo groot mogelijk maken, zodat dit daadwerkelijk in de handhaving wordt aangepakt?

Mijn tweede vraag gaat over het laatste punt, over de toetredingsdrempels. Ik begrijp wat de staatssecretaris daarover zegt. Ze geeft daarbij aan dat er gekeken wordt naar de reacties. Ik ben benieuwd of de staatssecretaris kan aangeven wanneer de balans wordt opgemaakt. Er werd ook iets gezegd over een Europese evaluatie en misschien een Nederlandse evaluatie. Wat kan ik op dat punt verwachten? Dan hebben we het moment in de tijd om de bevindingen te delen ook scherp met elkaar.

Staatssecretaris **Aerdts**:
Op de eerste vraag, over de pakkans bij oneerlijke concurrentie, kom ik graag in de tweede termijn terug.

Wat betreft de drempel zeg ik het volgende. De richtlijn gaat in Europees verband sowieso in 2030 worden geëvalueerd. Dat staat dus. Op de Nederlandse evaluatie komen we straks terug bij het amendement. Ik kan alvast zeggen dat ik dat amendement graag oordeel Kamer wil geven, als we wel een beetje kunnen aansluiten bij de Europese evaluatie. Dan ga je bedrijven en iedereen niet twee keer opzadelen met het verzamelen van gegevens. Laten we dus goed kijken naar de timing, maar ik sta zeker open voor een Nederlandse evaluatie.

Ik noem nog even een aantal voorbeelden van hoe het mkb ondersteund wordt. De CRA schrijft voor dat er bij het vaststellen van de vergoeding voor de conformiteitsbeoordelingsprocedures rekening moet worden gehouden met de belangen en behoeften van het mkb. De vergoeding dient ook te worden verlaagd in verhouding tot die belangen en behoeften. Verder is er voor het mkb helpdeskondersteuning bij het NCSC voor het doen van meldingen. Micro- of kleine ondernemers ontvangen geen administratieve boete bij het niet behalen van de gestelde termijnen voor de meldingen.

Verder heeft de Europese Commissie de richtsnoeren gepubliceerd voor mkb-fabrikanten waarmee de naleving kan worden vergemakkelijkt. Aan de hand van praktijkvoorbeelden geeft dit mkb-fabrikanten helderheid, onder andere over de reikwijdte en de ondersteuningsprocedure. Ik sprak al even over de Gids CRA en de testomgeving, de regulatory sandbox bij de RDI. Daar kunnen ook mkb-ondernemers gebruik van maken. Ook de subsidies staan hen, deels, ter beschikking. Dat in antwoord op uw tweede vraag.

Mevrouw **El Boujdaini** (D66):
Ik ben in ieder geval blij met het antwoord dat er ook al hulp wordt geboden vanuit het NCC richting het mkb en ook de microbedrijven. Waar ik nog wel mee zit is het volgende. Op het moment dat blijkt dat de hulpvraag zo groot is dat de capaciteit van het NCC niet meer toereikend is, wordt dit dan ook meegenomen in het evaluatiemoment van deze uitvoeringswet? Wordt dan ook bekeken of de ondersteuning op orde blijft?

Staatssecretaris **Aerdts**:
Het lijkt me heel goed om dit mee te nemen en om naar het NCC maar ook naar de RDI te kijken. Ze hebben nu de uitvoeringstoets gedaan, maar het lijkt me heel goed om ook te kijken naar de invoering en waar ze tegenaan lopen. Als dat eerder nodig is dan 2030 omdat er grote problemen zijn, dan gaan wij daar vanzelfsprekend eerder over in gesprek.

De **voorzitter**:
Dan denk ik dat u door kunt naar het volgende blokje, over implementatie.

Staatssecretaris **Aerdts**:
Ja, implementatie en werking. Mevrouw Kathmann vroeg heel terecht: wat betekent het dat we te laat zijn met de eerste implementatiedatum? De CRA schrijft inderdaad voor dat het vanaf 11 juni van dit jaar mogelijk zou moeten zijn voor de conformiteitsbeoordelingsinstanties — bij ons ook wel kortweg "testhuizen" genoemd — om beoordeeld en aangemeld te worden onder de CRA. Die beoordeling en aanmelding wordt gedaan door de RDI. Om de gevolgen voor het bedrijfsleven te beperken is de Raad voor Accreditatie, die ten behoeve van de beoordeling door de RDI de accreditatie uitvoert, ook al begonnen met de beoordeling van de conformiteitsbeoordelingsinstanties. Dus ondanks dat de wet nog niet is ingevoerd, is hierop vooruitlopend de RDI daar al wel mee begonnen, zodat die stap kan worden gemaakt. Het is van belang dat de RDI zo snel mogelijk bevoegd wordt om de geaccrediteerde conformiteitsbeoordelingsinstanties aan te kunnen melden, want het wordt ook geregeld in deze uitvoeringswet. En inderdaad, hoe langer het duurt, hoe groter de kans op vertraging voor het Nederlandse bedrijfsleven en de impact daarvan. We willen voorkomen dat Nederlandse producten bij het ingaan van de producteisen in december volgend jaar nog niet gekeurd zijn en dus niet de Europese markt op kunnen. Vandaar dat ik hoop dat we vanaf nu tot snelle inwerkingtreding van de uitvoeringswet over kunnen gaan. Daarnaast ontstaat uiteraard het risico op ingebrekestelling door de Europese Commissie bij niet tijdige invoering.

Mevrouw Kathmann vroeg: zijn we zelf nu al klaar? De heer Van den Berg van JA21 vroeg dat ook: heeft Nederland zijn ontvangst en opvolging van de meldingen vanaf vrijdag klaar? Ja, het meldloket van het NCC is op 11 september, of eigenlijk nu al, klaar om te voldoen aan deze meldplicht.

Mevrouw Kathmann vroeg wat de tijdlijn voor implementatie is tot december 2027. Wat moet er dan geregeld zijn? De meldplicht voor de geëxploiteerde kwetsbaarheden en incidenten gaat aanstaande vrijdag in. Het NCC is er klaar voor om deze meldingen via het eigen portaal te verwerken. Zodra de uitvoeringswet is aangenomen zal de RDI formeel conformiteitsbeoordelaars kunnen gaan aanwijzen. Op 11 december gaan de essentiële cybersecurityeisen voor producten in. De RDI is ter voorbereiding daarvan al bezig met het werven en opleiden van inspecteurs.

Ook wordt onder meer door de RDI gewerkt aan de inrichting van een nationaal communicatiekanaal voor vragen van fabrikanten over de CRA en aan het inrichten van een veilige testomgeving: de sandbox waarover we al eerder spraken.

Experts vanuit de RDI en NEN dragen bij aan het Europese werk op het gebied van standaardisering. Er zijn nog een aantal dingen die we begin volgend jaar verwachten voor de technische standaarden die behulpzaam zijn voor fabrikanten bij het aantonen van conformiteit. Ook daar is Nederland al op het hele praktische niveau bij betrokken.

Mevrouw Kathmann vroeg naar plan B voor het geval implementatie niet op tijd lukt. Er is eigenlijk geen reden om aan te nemen dat plan A niet zou slagen. Een effect zou kunnen zijn dat fabrikanten van producten die als belangrijk of kritiek zijn aangemerkt vertraging ondervinden bij het op de markt kunnen brengen van hun product, omdat de conformiteitsbeoordeling nog niet mogelijk zou zijn. Een ander effect zou kunnen zijn dat er nog maar weinig inspecteurs beschikbaar zijn voor toezichtwerk wanneer alle eisen van de CRA zijn ingegaan. Daarom vraag ik u — ook al realiseer ik me dat we straks ook nog naar de Eerste Kamer gaan — om te kijken of we op basis van het gesprek vandaag haast kunnen maken met het verdere wetgevingsproces.

Meneer Van den Berg had vragen over de keuringsinstanties. Hoeveel geschikte instanties zijn er? Welke wachttijden verwachten we? Wat is de uitweg als de Europese normen laat komen? De hoofdregel van de CRA is dat fabrikanten zelf de conformiteit van hun producten mogen beoordelen. Dit is alleen anders voor producten die als belangrijk of kritiek zijn aangemerkt in de bijlage van de CRA. De verwachting is dat het om ongeveer 10% van de producten onder de CRA zal gaan. Belangrijke producten zijn ingedeeld in twee klassen. Klasse 1 kan met een zelfbeoordeling volstaan, maar alleen als daarbij gebruik wordt gemaakt van een geharmoniseerde norm. Als die nog niet beschikbaar is, zal het product langs een aangemelde conformiteitsbeoordelingsinstantie moeten. Dit is altijd het geval voor klasse 2 en de kritieke producten. Als de geharmoniseerde norm niet op tijd af is, zal er dus meer druk bij de testhuizen gaan ontstaan. Op dit moment zijn er zes geïnteresseerde conformiteitsbeoordelingsinstanties in Nederland. Zij doorlopen nu het accreditatieproces bij de Raad voor Accreditatie. Na accreditatie zullen zij worden aangemeld door de RDI. De RDI kan de aanmelding formeel pas doorvoeren wanneer de uitvoeringswet in werking is getreden, omdat hierin de RDI de bevoegdheid krijgt om op te treden als aanmeldende autoriteit. Zolang een conformiteitsbeoordelingsinstantie nog niet is aangemeld, kunnen zij ook nog geen beoordelingen uitvoeren. Wat dat betreft is het echt wachten op deze uitvoeringswet.

Dan een aantal vragen over de ondersteuningsperiode. Gevraagd werd wat er zou gebeuren bij een faillissement. Mevrouw Zwinkels vroeg hoe de ondersteuningsperiode

van een product wordt vastgesteld. Zij was benieuwd of wij zouden kunnen aangeven hoe het staat met de ontwikkeling van deze normen en of deze normen beschikbaar zullen zijn als de CRA van toepassing wordt. Dat is inderdaad de planning. In Europees verband wordt op dit moment onder anderen door mensen van de RDI hard gewerkt aan het opstellen van die normen. Het is de planning dat aan het eind van dit jaar en in Q1 van 2027 de eerste normen zullen worden opgeleverd.

Mevrouw Kathmann en mevrouw Zwinkels vroegen of ondersteuning kan worden geboden door derde partijen en hoe dat werkt. Dat is mogelijk. Het is mogelijk om te zeggen: dit is ons product en deze persoon of dit bedrijf verzorgt voor ons de updates. Hier bestaan echter geen vaste regels voor in de CRA. Technisch gezien kan het, maar dan moet je ook IP overdragen et cetera. Dit moet natuurlijk wel duidelijk zijn voor de mensen die de spullen kopen. Dat is heel belangrijk daarbij, denk ik.

Er werd gevraagd of belangrijke updates ook na een faillissement nog beschikbaar zijn. Als een fabrikant zijn activiteiten stopzet en daardoor niet meer aan de CRA zal voldoen, moeten de betrokken markttoezichtautoriteiten daarover vooraf geïnformeerd worden. Ook gebruikers van de betrokken producten moeten met alle beschikbare middelen en voor zover mogelijk over de aanstaande stopzetting van de activiteiten worden geïnformeerd. Bij een faillissement wordt dikwijls de boedel geheel of gedeeltelijk overgenomen. De verplichtingen om die updates te blijven verzorgen horen bij de boedel. Markttoezichthouders en gebruikers worden dan via alle kanalen die ik net al noemde geïnformeerd over wie voortaan al die updates zal moeten verzorgen. Er is echter niet altijd een onderneming die die verplichtingen over wil nemen. In dat geval is het onvermijdelijk dat de updates toch zullen stoppen. Als het gebrek aan beveiligingsupdates een significant cyberbeveiligingsrisico oplevert, dan kan de RDI de andere marktdeelnemers die het product op de markt aanbieden verplichten om zo mogelijk de producten in lijn te brengen met de verordening. Als dat niet kan, dan kunnen ze verplicht worden om de producten uit de handel te nemen of zelfs terug te roepen.

Mevrouw Kathmann vroeg hoe met het meest vergaande scenario, het marktverbod, wordt omgegaan als het bijvoorbeeld om hard- of software gaat die noodzakelijk is voor een gevoelig proces. Kijk, dat marktverbod is wel echt een uiterst redmiddel. In eerste instantie zal de RDI natuurlijk in gesprek gaan. Zij kan vervolgens aangeven: dit is het minimale en anders gaan we dat doen. De RDI zal bij het inzetten van het marktverbod rekening houden met de gevolgen van zo'n besluit en die gevolgen ook afwegen tegen de risico's in het concrete geval. Ik kan daar nu niet een soort checklist voor geven, maar het is wel een van de mogelijkheden. Het is gereedschap dat de toezichthouder in zijn gereedschapskist heeft. Als je dan naar die voorwaarden zou kijken, dan moet de RDI als markttoezichthouder over de hele set bevoegdheden beschikken. In het uiterste geval gaat het inderdaad om het verbieden van het aanbieden, maar dat is alleen aan de orde als de fabrikant heeft nagelaten om zelf de nodige maatregelen te treffen. In dat geval is er ook verplicht contact met de toezichthouders in andere lidstaten en met de Europese Commissie.

Dan nog de vraag van mevrouw Kathmann hoe je bij de ondersteuningstermijnen verschil maakt tussen soorten apps en diensten. Volgens mij noemde u het voorbeeld van een festival dat alleen in de zomer plaats zou vinden. Of noem maar een willekeurig ander voorbeeld. De CRA verwijst naar een ondersteuningsperiode van minstens vijf

jaar of de verwachte levensduur van het product indien langer. Die periode mag alleen korter als expliciet wordt verwacht dat het product zelf minder dan vijf jaar meegaat, bijvoorbeeld in het geval van de app van het evenement. De ondersteuningstermijn dient de verwachte gebruiksduur te weerspiegelen. Daarbij wordt rekening gehouden met de verwachting van de gebruikers, de aard van het product en de EU-wetgeving, die minimale levensduur van producten met digitale elementen bepaalt. Als je aangeeft dat deze app voor het festival beschikbaar is, mag je er natuurlijk niet van uitgaan dat die app het tien jaar later nog doet, maar het belangrijkste hierbij is dat de consument hierover van tevoren wordt geïnformeerd, zodat die daar een keuze in kan maken.

Mevrouw Kathmann stelde ook nog de vraag hoe in de praktijk de redelijke termijn wordt vastgesteld en bij wie de bewijslast ligt. Het is aan de fabrikant om de redelijke termijn van de ondersteuning vast te stellen en dit ook in technische documentatie te onderbouwen. Hierbij dient onder andere rekening te worden gehouden met de verwachte levensduur van het product. De RDI zal daar ook toezicht op houden. Om de uniforme toepassing te bevorderen, zal de samenwerkingsgroep van markttoezichthouders onder andere statistieken publiceren van de gemiddelde ondersteuningsduur voor categorieën producten met digitale elementen. Als blijkt dat de gehanteerde ondersteuningsperioden ontoereikend zijn, kan de ADCO de markttoezichtautoriteiten aanbevelen om het toezicht specifiek op die categorie producten te richten. Ook kan de Europese Commissie met gedelegeerde handelingen de minimale ondersteuningsperiode vaststellen.

De heer Bikkers stelde ook nog een vraag over de ondersteuningstermijn: hoe voorkomen we rechtszaken en procedures en zorgen we dat consumenten gebruik kunnen maken van de bescherming die deze verordening tracht te bieden? Consumenten hoeven niet zelf rechtszaken of andere procedures te volgen. De nationale markttoezichthouders — in Nederland zou dit de RDI worden — houden toezicht op de naleving van de CRA. De RDI kan fabrikanten op hun verantwoordelijkheden aanspreken en zo nodig sancties opleggen, zoals een last onder dwangsom of een bestuurlijke boete en in het uiterste geval het van de markt halen ván, wanneer de fabrikant die verplichtingen niet nakomt.

Mevrouw Zwinkels stelde nog een vraag over de machines, die soms langer meegaan dan de software of de componenten: wat betekent dit voor de ondersteuningstermijn? Het is aan fabrikanten om te zorgen dat er een passende ondersteuning wordt gehanteerd voor het gehele product. Gedurende deze periode moet de fabrikant blijven voorzien in veiligheidsupdates. Als de software of componenten in een machine niet meer ondersteund worden, levert dat een veiligheidsrisico op. Daarom zijn we blij dat je dat aan de voorkant vooral heel duidelijk moet maken, zodat je als consument ook een keus kan maken. Als wordt verteld dat de ene ijskast zolang wordt ondersteund en de andere zolang, kan je daar echt een keus in maken. Ik gaf al eerder aan: mocht dit de spuigaten uitlopen of mocht de ADCO aangeven dat er steeds overtredingen plaatsvinden in een categorie, kan dat natuurlijk voor de toezichthouders een reden zijn om daar veel specifieker naar te gaan kijken. Ik ben heel blij dat het heel actief moet worden aangeboden aan de consument, zodat je op de website waar je software koopt of op de verpakking bij wijze van spreken kan zien wat die termijn zal zijn.

Dan de laatste twee vragen als het gaat om die termijn. Nee, sorry, deze horen bij het volgende blokje. Dit was het eerste stuk, over implementatie en de werking.

De **voorzitter**:
Ik kijk even naar de leden. Mevrouw Kathmann.

Mevrouw **Kathmann** (PRO):
Ik vraag mij af — door die laatste beantwoording weet ik niet zeker of het wel nodig is — of er onderscheid gemaakt wordt in de soorten apps. Wordt er bijvoorbeeld vaker toezicht op gepleegd? Neem dan niet alleen het voorbeeld van een app voor een festival: dat festival is maar één keer en daarna nooit meer. Maar wordt er bijvoorbeeld ook gekeken naar — ik noem maar iets — een apparaatje waarmee je hartfilmpjes kan maken versus zo'n festivalapp? Wordt daar ook nog een soort van onderscheid in gemaakt, dus eigenlijk in de noodzaak van het gebruik?

Staatssecretaris **Aerdts**:
In principe wordt dat toezicht risicogebaseerd ingericht. Ik kan me voorstellen dat de toezichthouder een festivalapp als een minder groot risico ziet dan een apparaat dat hartfilmpjes maakt. Dus in principe wordt het risico daarop beoordeeld, maar uiteindelijk is het nu wel aan de toezichthouders om daar een weging in aan te brengen. Maar ik denk dat het goed is dat er in de samenwerkingsgroep van markttoezichthouders heel specifiek naar categorieën gekeken gaat worden.

Mevrouw **Zwinkels** (CDA):
Mijn vraag sluit hierop aan. Ik merk dat ik het allemaal goed in elkaar vind zitten, maar ik hoor in de antwoorden ook wel dingen die ik al gelezen heb en die ik al wist. Ik ben echter juist een beetje op zoek naar hoe we die verwachte gebruiksduur concreet gaan maken en goed gaan afbakenen, zodat mensen weten wat ze daarvan mogen verwachten. In de beantwoording hoor ik wel heel sterk: "Ja, dat komt nog. Een geharmoniseerde norm. Het komt nog via de markttoezichthouders en via de statistieken die ze gaan analyseren."

Kan de staatssecretaris misschien iets toezeggen over de informatie die wij kunnen verwachten op dit vlak? Kan zij ervoor zorgen dat wij weten wat voor normen dat bijvoorbeeld voor die verschillende productcategorieën gaan worden? Ik heb een punt gemaakt van de digitale apk, want ik wil weten hoe de consument daarover geïnformeerd gaat worden. Die koopt iets — ik ga ervan uit dat hij goed geïnformeerd is — maar de verpakking gooit hij daarna natuurlijk wel weg. En dan? Ik ben toch een beetje benieuwd naar wat we hiervoor kunnen verwachten bij die geharmoniseerde normen.

Staatssecretaris **Aerdts**:
Om eerlijk te zijn ligt dit in eerste instantie bij de fabrikant. Het is dus niet vooraf helemaal door de toezichthouders geregeld. Dit ligt bij de fabrikant.

De apk. Op dit moment geeft de website veiliginternetten.nl eigenlijk al antwoord op dit soort vragen, bijvoorbeeld: hoe update ik mijn slimme ijskast? Waar kan ik iets vinden? Waar kan ik dat opzoeken? Over die digitale apk zou ik dan ook in eerste instantie willen voorstellen dat we op deze website, een plek die al veel mensen weten te vinden, een subpagina hiervoor inrichten. Daar kan je dan een heel specifieke checklist vinden — als ik dat zo mag zeggen — voor zaken waaraan het moet voldoen. Daar kunnen dan ook een aantal van dit soort vragen worden beantwoord. Vaak staat de naam van de

fabrikant natuurlijk ook nog wel op het product dat je hebt gekocht en je zou dus ook die manier daar uit moeten kunnen komen. Maar in eerste instantie kan ik dat nu niet zeggen, want dit ligt ook bij de fabrikant. Het is als eerste aan de fabrikant om daarnaar te gaan kijken. Het is dus ook niet zo dat wij, ik of de toezichthouder, van tevoren echt al een lijst zullen uitgeven met daarop: ijskasten zeven jaar, slimme deurbellen drie jaar. Dat is niet hoe de situatie volgend jaar zal zijn.

De **voorzitter**:
Een vervolgvraag.

Mevrouw **Zwinkels** (CDA):
Dat begrijp ik. Tegelijkertijd denk ik toch ook dat we niet alles bij de fabrikant kunnen leggen als je het hebt over het bepalen van de spelregels. Daar heeft de overheid ook echt een rol in te spelen. Ik ben daarom heel erg benieuwd waar dat spel wordt gespeeld. Gaat het gewoon in Brussel plaatsvinden? Zo ja, dan wil ik daar gewoon van op de hoogte gehouden worden en horen wat daaruit is gekomen. Het gaat me dus wat meer om de informatie over de eventuele stappen die hierin gezet worden. Ik dacht dat er in verband met die statistieken werd gehint op een soort benchmarking in de toekomst. Dus ja, daarom heb ik daar veel vragen over gesteld. Maar ik heb nu nog steeds niet helemaal een beeld bij de oplossingsrichtingen die gekozen gaan worden.

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

Mevrouw **Zwinkels** (CDA):
Mijn vraag is of de staatssecretaris toe kan zeggen dat wij daar de komende periode over geïnformeerd gaan worden. Zo ja, op wat voor manier en wanneer?

Staatssecretaris **Aerdts**:
Misschien nog even dit. De fabrikant stelt het vast, maar hij doet dat onder andere op basis van die technische documentatie, die hij zelf ook moet vastleggen. Daarin moeten fabrikanten aangeven waarom dit de levensduur zal zijn. De consument kan dat ook vooraf inzien. Ik snap ook dat niet iedereen bij een hele kleine aankoop dat hele dikke boekje door gaat lezen, maar dat zijn natuurlijk wel de dingen waar de toezichthouder naar gaat kijken en op gaat toetsen. De RDI houdt er namelijk toezicht op dat die levensduur volledig ondersteund gaat worden. Maar die lijst zal er niet vooraf liggen.

Ik ben ook een beetje aan het zoeken naar hoe een toezegging eruit moet gaan zien over hoe u daarover geïnformeerd gaat worden en hoe dat er in de praktijk uit moet zien. Het betekent namelijk iets heel anders voor apps voor festivals dan voor apps voor ijskasten en slimme deurbellen. Ik vraag me ook wel af hoe wij daar een volledig overzicht van kunnen krijgen. Ik denk dat het echt aan de toezichthouder is om daarmee aan de slag te gaan en om op basis van meldingen te gaan kijken wat daaruit naar voren komt. In eerste instantie zullen we de fabrikant aan zet moeten laten zijn.

De **voorzitter**:
U kunt door naar het volgende blokje, staatssecretaris.

Staatssecretaris **Aerdts**:
Voorzitter. Dan ga ik door met het blokje over het toezicht en de toezichthouders. De

vraag van mevrouw Zwinkels was: heeft de RDI voldoende capaciteit en instrumenten om te handhaven? Op basis van de uitvoerings- en handhaafbaarheidstoets acht RDI haar taken uitvoerbaar. RDI heeft aanvullende middelen ontvangen voor het toezicht en de capaciteit daarvoor. Ik gaf daar net ook al een paar voorbeelden van.

Mevrouw El Boujdaini vroeg ook hoe ervoor gezorgd wordt dat RDI kwalitatief goed kan blijven uitvoeren, ook in het licht van de toezichthoudende taken die erbij komen, bij RDI in brede zin. Bij het toekennen van de nieuwe wettelijke taken wordt altijd de uitvoerbaarheids- en handhaafbaarheidstoets uitgevoerd. Daarbij hebben ze ook in kaart gebracht welke taken uitvoerbaar zijn en welke middelen nodig zouden zijn. U noemde net ook al een aantal sollicitatieprocedures die lopen om nieuwe mensen te werven. Bij de uitvoeringstoets heeft RDI aangegeven de taken uitvoerbaar te achten. Het wetsvoorstel verleent RDI de nodige bevoegdheden om op een effectieve manier toezicht op de handhaving van de CRA mogelijk te maken. De benodigde middelen voor het aannemen van de nodige mensen bij RDI zijn vrijgemaakt op de begroting van EZK. Verder is RDI goed aangesloten bij de Europese gremia waarin over die handhaving en uitvoering wordt gesproken. Ook als het gaat om het kwalitatief goed blijven uitvoeren is dat, denk ik, een hele belangrijke stap, net als het feit dat ze bij die normalisatie en die standaardisering op dit moment ook al betrokken zijn.

Mevrouw Zwinkels vroeg nog naar de mogelijkheden die RDI heeft om snel in te grijpen bij veiligheidsrisico's. Dat sluit ook een beetje aan bij de vraag van mevrouw Kathmann die ik al had beantwoord. Niet-naleven van de CRA kan resulteren in boetes en dwangsommen, een percentage van de wereldwijde omzet. Bovendien kan niet-naleven natuurlijk ook resulteren in reputatieschade. In het geval van voortdurende non-conformiteit kan de toezichthouder maatregelen nemen om het op de markt aanbieden van het product te beperken, om het te verbieden, het product terug te roepen of echt helemaal uit de handel te nemen. Dat is eigenlijk de gereedschapskist van RDI hierin.

Mevrouw Kathmann snapte de keuze voor RDI, maar vroeg zich af of er ook nog andere toezichthouders overwogen zijn. Het simpele antwoord is eigenlijk "nee", omdat RDI de meest voor de hand liggende toezichthouder is, omdat ze al een wettelijke taak, de expertise en de infrastructuur hebben voor markttoezicht op digitale en elektronische producten. Zo houdt RDI bijvoorbeeld al toezicht op de cyberbeveiligingseisen onder de Radio Equipment Directive. De RED, of de Radio Equipment Directive, gaat ook op in de CRA, waardoor het voor de hand ligt om hier ook dezelfde toezichthouder voor aan te wijzen.

De benodigde middelen voor het toezicht zijn gebaseerd op de raming van RDI zelf. U vroeg nog: wat zijn de implicaties als de kosten hoger uitvallen? De benodigde middelen die nu zijn toegekend, zijn gebaseerd op de raming van RDI zelf. Indien de middelen toch anders uitvallen, ga ik daar natuurlijk met RDI over in gesprek. Maar op dit moment zijn de middelen toegekend die zij zelf hebben aangegeven nodig te hebben om dit toezicht te kunnen houden.

Mevrouw El Boujdaini vroeg nog of ik kan aangeven of afstemming met andere toezichthouders in andere lidstaten plaatsvindt. We hebben volgens mij al een aantal keer aangestipt dat het ontzettend belangrijk is om dat te doen. CRA voorziet dan ook in de oprichting van het afstemmingsorgaan, ADCO, waar ik eerder al over sprak. Dat bestaat uit vertegenwoordigers van nationale markttoezichthouders, die in elk van de

lidstaten van de EU worden aangewezen door de uitvoeringswetten. RDI is actief deelnemer van dat afstemmingsorgaan. ADCO staat voor: Administration Corporation for the Cyber Resilience Act.

Verder vroeg een aantal van u duidelijkheid over die regulatory sandbox. Wanneer zou die er nu gaan komen? RDI gaat die sandbox opzetten. Daarbij is het doel dat bedrijven met de toezichthouder in gesprek kunnen gaan over die innovatieve producten en hoe die CRA-conform op de markt worden gezet. Er wordt al zo veel mogelijk aangesloten bij de sandbox die al wordt ontwikkeld door RDI voor de AI-verordening. Ik verwacht hier aan het einde van dit jaar meer duidelijkheid over.

Ik kom als laatste terug op de mysteryshopper en op de evaluatie. Ik pak die even allebei mee bij het amendement zo direct.

Dat is dus het einde van het stuk over het toezicht en de toezichthouders.

De **voorzitter**:
Ik zie geen beweging bij de leden. Ik zou dus zeggen: ga vooral door.

Staatssecretaris **Aerdts**:
Dan ga ik door naar het blokje overig, voordat ik inga op alle punten van de voorgestelde amendementen. Mevrouw Kathmann stipte heel terecht ook Caribisch Nederland aan: hoe wordt de Nederlandse inzet voor Europese cyberwetgeving afgestemd met de BES-eilanden en is daar bij deze verordening sprake van geweest? In dit geval is er geen sprake geweest van afstemming van de cyberwetgeving met de BES-eilanden over deze specifieke verordening, omdat ze geen onderdeel van de Europese Unie zijn en dus eigen wet- en regelgeving kennen. Dit wordt in dit geval gezien als een nationale kop, die niet past bij dit kabinetsbeleid, maar dat is een beetje een technisch verhaal. Op dit moment zijn wij kennismakingsgesprekken aan het plannen met de gevolmachtigde ministers en kijken wij ook hoe we kunnen omgaan met het college van de BES-eilanden en de eilandsraad, omdat we natuurlijk nadrukkelijk wél zien dat een aantal issues die wij hier bij de CRA proberen te regelen, ook ontzettend van belang zijn voor het Caribisch deel van het Koninkrijk. De CRA zal daar niet van toepassing zijn, maar we zijn nog aan het zoeken wat daar wel de beste manier voor is. "Bent u bereid om alle mogelijkheden aan te grijpen om de CRA zo veel mogelijk te laten gelden?" Het gaat vooral om kijken waar in het Caribisch deel van Nederland behoefte aan is om dat gesprek echt goed op te zetten en om inderdaad te kijken hoe je ervoor kan zorgen dat zij toegang hebben en dat zij ook van veilige producten gebruik kunnen maken. De CRA is daar niet zozeer het haakje voor, maar ik kom hier heel graag nog uitgebreider bij u op terug, want we zien nadrukkelijk het nut om juist ook met de Caribische delen van het Koninkrijk hierover in gesprek te gaan.

De **voorzitter**:
Mevrouw Kathmann wil een vraag stellen, maar zullen we dat aan het eind van het blokje doen? Vindt u dat goed?

Mevrouw **Kathmann** (PRO):
Ja.

Staatssecretaris **Aerdts**:

Ik ga naar mevrouw Zwinkels. Ik had het zojuist al even over de digitale apk waarmee burgers periodiek zouden kunnen checken of hun apparaten nog veilig zijn. Ik begrijp die behoefte heel erg goed. Het ministerie van Economische Zaken heeft jarenlang de campagne Doe je updates gedaan. Ik roep u ook allemaal op om dat echt heel trouw te doen, maar met de CRA leggen we die verantwoordelijkheid heel bewust bij de fabrikanten. Dat betekent niet dat je niet zelf alert moet zijn, maar de CRA is er echt op gericht om die fabrikanten hier ook verantwoordelijk voor te stellen. Maar veiliginternetten.nl zien wij wel echt als de pagina waar mensen naartoe kunnen gaan. Ik ben graag bereid om ook te kijken hoe we daar nog een soort subpagina aan kunnen toevoegen voor een apk, een checklist of hoe u het noemen wilt om te kijken hoe we het daar voor consumenten nog makkelijker kunnen maken om zich ervan bewust te zijn welke updates ze misschien uit moeten voeren en waar ze aan moeten denken waar ze misschien zelf niet automatisch aan denken als het gaat om een slim apparaat. Het lijkt mij heel goed om te kijken hoe we die website daar ook voor in kunnen zetten.

Mevrouw El Boujdaini vroeg ons nog naar de kwantumvisie en hoe we de cyberwetten toespitsen op de postkwantumcryptografie. De CRA schrijft voor dat producten met digitale elementen zodanig worden ontworpen, ontwikkeld en geproduceerd dat ze een passend cyberveiligheidsniveau waarborgen. Dit niveau moet passend zijn gelet op de beoordeling van de cybersecurityrisico's van het product. Bij die risicobeoordeling wordt uitgegaan van de stand van de techniek op dat moment. Dat houdt in dat met de tijd postkwantumcryptografie nodig zal zijn voor passende bescherming onder de CRA. Door deze open norm zal de CRA ook meebewegen met de technologische ontwikkelingen. We verwachten die kwantumvisie in Q4 van dit jaar.

Kan de postkwantumcryptografie meegenomen worden in de evaluatie van de Cyberweerbaarheidswet? De CRA zal uiterlijk op 11 december 2030 worden geëvalueerd en daarna elke vier jaar. Hierbij zal op dat moment ook worden gekeken naar het vermogen van de verordening om de producteisen mee te laten bewegen met de ontwikkeling van de stand van de techniek: wordt die open norm inderdaad zo beleefd of kan die zo ingezet worden? Vanwege de open geformuleerde cybersecurityeisen die worden uitgewerkt in geharmoniseerde technische normen die elke vijf jaar worden herzien, is de verwachting dan ook dat de CRA goed kan reageren op de technologische ontwikkelingen. Maar ik zal voor onszelf wel een notitie maken dat wij dit specifiek mee zullen nemen bij die evaluatie.

Mevrouw Kathmann en mevrouw Zwinkels kwamen samen tot een hele mooie formulering over de inzet van opensourcesoftware en hoe we daarmee bezig zouden zijn. Wat was nou de Nederlandse inzet voor opensourcesoftware en in hoeverre zijn die punten ingewilligd in de uiteindelijke verordening? Het Nederlandse kabinet had als een van de speerpunten in de onderhandelingen over de CRA dat er een heldere en eerlijke regeling voor opensourcesoftware zou worden vastgelegd. Ontwikkelaars van opensourcesoftware die daar vrijwillig aan bijdragen, moeten niet geconfronteerd worden met dezelfde verantwoordelijkheden als commerciële fabrikanten. Tegelijkertijd is het belangrijk dat er wel de juiste prikkels zijn om die open software ook veilig te laten zijn, want opensourcecomponenten zitten bijna in alle digitale producten. We hebben ons hier hard voor gemaakt en er input op gevraagd, ook vanuit de opensourcecommunity. Die inbreng heeft tot het gewenste resultaat geleid.

Dan nog de vraag of het kabinet bereid is om zich te blijven opwerpen als pleitbezorger

van opensourcesoftware, en hoe we dat gaan doen. Het kabinet ziet dat voor de innovatiekracht de beschikbaarheid van open source ontzettend belangrijk is. We zetten ons daar dan ook continu voor in op Europees niveau. Dat hebben we gedaan tijdens de onderhandelingen voor de CRA. Ook als het gaat om alle wetgeving die nu voorligt, vinden we open source ontzettend belangrijk. We zullen daar dus ook pleitbezorger voor zijn. Het kabinet zet zich in Europabrede ontwikkelingen en opschaling ook in voor die oplossingen, bijvoorbeeld voor het European Digital Infrastructure Consortium, het EDIC, opgezet voor de digitale gemeenschapsgoederen. Hier wordt onder andere aan opensource-netwerksoftware gewerkt. Dat blijven we doen en daar mag u ons zeker op aanspreken.

Dan was er nog een vraag van mevrouw Zwinkels over technologische ontwikkelingen: hoe kan de overheid met de markt samenwerken om te anticiperen op die technologische ontwikkelingen, ook om de standaarden actueel te houden? De essentiële eisen van de CRA zijn techniekneutraal geformuleerd en worden nader uitgewerkt in technische normen, ook voor de standaarden waar ik eerder over sprak, door de markt en de overheid gezamenlijk. Daarbij wordt inderdaad juist ook samengewerkt met bedrijven. Die standaarden worden elke vijf jaar geactualiseerd, zodat ze altijd zullen meegaan met die technologische ontwikkelingen en veilig blijven, gelet op de stand van de techniek. Ook als het gaat over innovatie, zowel bij ontwikkelingen als bij marktintroductie, werken overheid, wetenschap en markt samen. Dat is vastgelegd in de Nationale Technologiestrategie, waarin cybersecurity is aangemerkt als een sleuteltechnologie. Digital Holland beheert de actieagenda voor die cybersecuritytechnologieën.

Een vraag die daar nog aan raakte, van u beiden, was over het intellectuele-eigendomsrecht: mag dat contractueel beschermd worden? Als de fabrikant niet langer de update wil of kan doen, kan hij die taak overdragen aan een ander bedrijf. Maar die overnemer zal dan moeten kunnen beschikken over de daarvoor benodigde broncodes. De wet biedt de fabrikant mogelijkheden om enerzijds de intellectuele-eigendomsrechten contractueel te beschermen, maar anderzijds overheden wel in staat te stellen om die updates dan te verzorgen.

Mevrouw **Kathmann** (PRO):
Ik was al blij met de beantwoording van de staatssecretaris van mijn vraag over cyberveiligheid op de BES. Mocht dat lukken, dan zou ik alleen een iets strakkere toezegging willen over wanneer we een soort terugkoppeling kunnen verwachten over cyberveiligheid op de BES, over hoe die gesprekken verlopen of hoe het kabinet daarnaar kijkt.

Staatssecretaris **Aerdts**:
Ik ga even overleggen over de termijn. Ik kom daar in tweede termijn graag even op terug.

De **voorzitter**:
In tweede termijn. Dan gaan we volgens mij richting de amendementen. Wil u daarop reageren? Ja, mevrouw Zwinkels?

Mevrouw **Zwinkels** (CDA):
Dit was het blokje overig, toch? En daarmee het laatste blokje, denk ik ook?

De **voorzitter**:
Het laatste blokje.

Staatssecretaris **Aerdts**:
Behalve dat ik nu op de amendementen inga, de mysteryshoppers et cetera.

Mevrouw **Zwinkels** (CDA):
Ik had nog een vraag gesteld. Die ging over hoe we geleerde lessen over uitgebuite kwetsbaarheden kunnen vastleggen in een register. Het mag ook in tweede termijn.

Staatssecretaris **Aerdts**:
Ik kom daar heel graag in tweede termijn op terug.

Mevrouw **Zwinkels** (CDA):
Die vraag had ik eerder gesteld. Dank u wel.

De **voorzitter**:
Dan kan u naar de appreciaties.

Staatssecretaris **Aerdts**:
Yes. Dan begin ik met het amendement op stuk nr. 7 over het verbod op uitlokking bij toezicht met een fictieve hoedanigheid. Allereerst de strekking van het amendement: die vult de bepaling over het gebruik van die fictieve hoedanigheid van het toezicht in. De bepaling dat een markttoezichthouder onder een valse identiteit als mysteryshopper producten moet kunnen verkrijgen om die producten te kunnen testen, komt voort uit de Europese markttoezichtverordening. Die is van toepassing op alle productwetgeving van de Unie, waaronder de CRA. In alle nationale uitvoeringswetgeving is voor productwetgeving die bevoegdheid uniform geïmplementeerd. Ambtelijke uitlokking is daarentegen in alle gevallen verboden; dat volgt ook uit de rechtspraak. Het expliciet regelen van een verbod op ambtelijk uitlokken is daarom eigenlijk niet nodig. Aan de andere kant kan het ook geen kwaad om het zo op te nemen. Dat is ook al zo gebeurd bij het regelen van de bevoegdheid van wetgeving op andere terreinen. Ik kan het amendement dus oordeel Kamer geven.

De **voorzitter**:
Het amendement op stuk nr. 7: oordeel Kamer.

Staatssecretaris **Aerdts**:
Precies. Mevrouw Kathmann vroeg nog wat eigenlijk de voorwaarden zijn waaronder mag worden "uitgelokt". Uitlokking mag dus niet, maar op grond van de markttoezichtverordening moet een toezichthouder beschikken over de bevoegdheid om een fictieve hoedanigheid te gebruiken, zodat als jij als toezichthouder iets bestelt, je niet het beste product krijgt terwijl anderen dat niet krijgen. Zonder die bevoegdheid bestaat dus ook het risico dat de toezichthouder andere en betere producten verkrijgt dan de gewone consument. Uitlokking van een strafbaar feit door een toezichthouder is nooit toegestaan, ook niet bij mystery shopping. Het gebruik van die bevoegdheid is ook aan bepaalde voorwaarden verbonden. Zo moet de inzet noodzakelijk zijn voor het toezicht en moet de toezichthouder een uitgebreid verslag opstellen van elke toepassing van die bevoegdheid.

Mevrouw Kathmann vroeg naar aanleiding daarvan ook nog: hoe kan je verzekeren dat dat mystery shopping alleen aan de orde is als zwaardere middelen niet logisch zijn? U noemde het uitlokking. Nou, uitlokking is dus nooit mogelijk. In het algemeen kan de toezichthouder alleen die bevoegdheid tot mystery shopping inzetten als het noodzakelijk is voor het toezicht. Dat is niet het geval als de toezichthouder met het gebruik van minder zware middelen hetzelfde resultaat kan behalen.

Mevrouw Kathmann vroeg ook nog welke gevolgen dit amendement zal hebben voor de minimumuitvoering van de verordening. Ook zonder het amendement zou het verboden zijn om bij die strafbare feiten uitlokking toe te passen. Dit wordt hiermee enkel formeel bekrachtigd. Er zijn dus ook geen gevolgen voor de minimumuitvoering van de verordening. Je kan het expliciet maken, zoals ook gebeurt in andere wetgeving, maar het is niet strikt noodzakelijk om dat te doen.

Nog de laatste vraag: hoe vaak controleert RDI heimelijk op producten en houden die sancties stand bij de rechter? Voor dit hele specifieke geval moet RDI dat gewoon nog gaan zien; dat moet nog worden ingericht. RDI heeft in enkele gevallen producten anoniem, dus met een fictieve identiteit, aangekocht voor andere wet- en regelgeving. Voor de CRA wil RDI dit gaan doen om de golden sample te voorkomen, dus om te voorkomen dat je het goede, mooie product krijgt terwijl gewone mensen dat niet krijgen. RDI heeft wat de inzet van mystery shoppers betreft in vergelijkbare zaken geen zaken voor de rechter gehad.

Dan het amendement op stuk nr. 8 over de evaluatie: krijgt de Kamer drie jaar na de inwerkingtreding van de uitvoeringswet verslag van de effectiviteit en doeltreffendheid? Eigenlijk kunnen we dit amendement ook oordeel Kamer geven, want de Europese evaluatie staat gepland voor 2030. Dat zou dus mooi op elkaar kunnen aansluiten. Als de termijn voor de uitvoeringswet inderdaad kan aansluiten bij die van de implementatie van de verordening, ben ik zeker bereid om dan ook naar de Nederlandse situatie te kijken en die te evalueren. Het is daarbij wel belangrijk om het af te stemmen op de evaluatieclausule uit artikel 30 van de CRA, waarin staat "uiterlijk 11 december 2030", zodat we het ook in samenhang kunnen bezien. Op die manier zouden we de uitkomsten van de evaluatie van de nationale uitvoeringstoets ook kunnen gebruiken als input voor die evaluatie op Europees niveau. Wat mij betreft krijgt dit amendement dus ook oordeel Kamer.

De **voorzitter**:
Het amendement op stuk nr. 8: oordeel Kamer.

Staatssecretaris **Aerdts**:
Dan het amendement op stuk nr. 9, over de bewaartermijn. Dit amendement vult de bepaling in over het gebruik van een fictieve hoedanigheid bij het toezicht, met twee termijnen, waarna die gegevens moeten worden verwijderd. In het geval dat de wet niks regelt over die bewaartermijnen bij de inzet van een mystery shopper, kan RDI zelf bepalen hoelang zij persoonsgegevens bewaart, maar uit de Algemene verordening gegevensbescherming volgt dat die bewaartermijn zo veel mogelijk beperkt moet worden. Ik ben het met de indiener van het amendement eens om het nader te regelen in het wetsvoorstel, want dat biedt transparantie en zekerheid. Daarom ook voor dit amendement: oordeel Kamer.

De **voorzitter**:
Het amendement op stuk nr. 9: oordeel Kamer.

Staatssecretaris **Aerdts**:
Mevrouw Kathmann vroeg volgens mij aan de heer Van den Berg: waarom is het dan één termijn en is er ook korter of langer overwogen in het amendement? Volgens de tekst van het amendement moeten persoonsgegevens worden verwijderd uit het verslag als er niet binnen één jaar een handhavingsbesluit is genomen. Bij het stellen van een opzegtermijn moet er een evenwicht worden gevonden tussen de werkbaarheid en het beginsel van de opslagbeperking van persoonsgegevens. De RDI heeft bij mij aangegeven dat die termijn van één jaar in het amendement werkbaar is.

De **voorzitter**:
Tot zover de beantwoording vanuit de zijde van het kabinet. Ik kijk even naar de leden om te zien of er behoefte is aan een schorsing voor de tweede termijn of dat we gelijk door kunnen. We gaan gelijk door naar de tweede termijn. Het woord is aan mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Dank u wel, voorzitter. Nogmaals dank aan de staatssecretaris voor de beantwoording. Om positief te beginnen: ik ben erg blij met de antwoorden die zijn gegeven rondom het gelijk speelveld, het mkb en start-ups. Het is ook mooi dat het amendement van de heer Van den Berg positief is geadviseerd. Dat ziet op de regeldruk en eventuele toetredingsdrempels voor het mkb. Ik ben op zich ook wel blij met de positieve reactie op ons voorstel voor zo'n digitale apk en het voorstel dat daar een subpagina voor ingericht kan worden. Ik zou van de staatssecretaris met een toezegging te horen willen krijgen op wat voor termijn dat gerealiseerd kan worden. Dan hebben we dat goed met elkaar in de gaten.

Ik heb net al uitgesproken dat ik nog wat aarzelingen heb bij de implementatie. Een aantal zaken zijn nu nog niet helemaal helder, maar gaan nog gevormd worden in de komende tijd. Ik ga er nog even over nadenken. Ik kom niet met een voorstel, maar vind het wel heel erg belangrijk dat we dit goed met elkaar monitoren en dat we daarover geïnformeerd worden de komende tijd. Daarmee valt of staat de uitvoering en de handhaving.

Tot slot. Over de handhaving gesproken: ik zou in de tweede termijn nog een antwoord krijgen op de vraag ten aanzien van de pakkans voor de niet-Europese producten, als ik dat zo mag samenvatten. Ook de vraag over de geleerde lessen zie ik graag nog beantwoord.

Dank u wel.

De **voorzitter**:
Mevrouw El Boujdaini.

Mevrouw **El Boujdaini** (D66):
Dank u wel, voorzitter. Ik wil de staatssecretaris ook graag bedanken voor haar beantwoording. Ik ben blij om te horen dat post-quantum cryptografie ook meegenomen

wordt en de CRA in principe meegroeit met de nieuwe technologieën die er komen. Dat is heel fijn, want de digitale ontwikkelingen gaan razendsnel. Het is ook goed om te horen dat mkb'ers en microbedrijven ook nu al hulp kunnen krijgen vanuit het NCSC. Zoals ik al eerder aangaf, vinden wij het vooral belangrijk dat de capaciteit van het NCSC altijd toereikend blijft om deze hulp bij de meldplicht te kunnen blijven bieden aan de bedrijven.

Al mijn andere vragen waren al beantwoord.

De **voorzitter**:
Mevrouw Kathmann.

Mevrouw **Kathmann** (PRO):
Voorzitter. Ook vanuit mij dank voor de beantwoording van de vragen. Ik vind dat een boel is opgetuigd om klaar te staan voor 11 december 2027, maar ik vind het ook wel spannend. Volgens mij vindt iedereen dat. Misschien zijn signalen vanuit de samenleving en fabrikanten nodig om er nog een keer over te spreken, maar nu is in ieder geval alles op alles gezet om dat zo goed mogelijk te doen. Dat vind ik nog wel even spannend. Ook de beantwoording op de vragen over de pakkans vind ik spannend. Daar ben ik benieuwd naar.

Ik wil deze mogelijkheid gebruiken om nog naar iets heel anders te vragen. Ik vond het heel opmerkelijk en heel mooi om te lezen dat dit cyberveiligheidsbeleid de Europese Unie 180 tot 290 miljard gaat besparen. Toen dacht ik: wauw. Daar ben ik wel door getriggerd. Heeft het kabinet gedacht: moeten we dat niet naar Nederland doorvertalen? Wat betekent dit voor Nederland? Het is namelijk nogal wat: voor de hele Europese Unie 180 tot 290 miljard. Dan kan ik me ook voorstellen dat je dan nog meer alles op alles zet om klaar te zijn en om die loketten in te richten om al die vragen te beantwoorden. Betekent dit bijvoorbeeld ook dat we andere soorten van cyberveiligheidsbeleid kunnen doorrekenen en dat dat misschien ook een soort businesscase is? Vaak is er, als we over cyberveiligheid spreken, geen ruimte om te investeren of is er geen geld. Nu vliegen de miljarden ons om de oren, dus misschien is dit ook wel een pot of een manier waarmee de staatssecretaris naar de rest van het kabinet kan om investeringen af te dwingen. Ik vond het echt heel opmerkelijk en eigenlijk ook supergoed nieuws. We weten dat de maatschappelijke kosten van cybercriminaliteit en cyberonveiligheid heel hoog oplopen. Ik vond dit wel mooi.

De **voorzitter**:
Meneer Van den Berg, in tweede termijn.

De heer **Van den Berg** (JA21):
Voorzitter. Eigenlijk heb ik hier weinig aan toe te voegen. De beantwoording was helder. Dank voor de positieve appreciaties van de amendementen. Het werk is niet voor niets geweest. Ik kijk uit naar een succesvolle uitvoering van deze wet.

Ik vond het een terecht punt van mevrouw Kathmann. Ik zag dat de VVD in het schriftelijk overleg heeft gevraagd naar de onderbouwing van de besparing van kosten. Ik ga er niet verder op doorvragen. Ik weet dat bij eerdere voorstellen van de EU niet goed te onderbouwen viel waar de besparingen terecht zouden komen. Dat zegt wel wat. Ik vind dat Nederland dat beter moet doen. Dit is alles wat ik er op dit moment over

te zeggen heb.

Dank u wel, voorzitter.

De **voorzitter**:
Dat was de tweede termijn van de zijde van de Kamer. Ik sla de tweede termijn over, omwille van de tijd. Ik kijk even naar de staatssecretaris. Tien minuten? Dan gaan wij om 21.25 uur weer verder.

De vergadering wordt van 21.15 uur tot 21.26 uur geschorst.

De **voorzitter**:
Ik heropen de vergadering en geef het woord aan de staatssecretaris voor de tweede termijn.

Staatssecretaris **Aerdts**:
Voorzitter. Mevrouw Kathmann vroeg of we iets specifieker konden zijn over wanneer de Kamer geïnformeerd zou worden over de gesprekken met de BES. In november en december vinden er gesprekken plaats met de BES-eilanden over de routekaart voor het cybersecuritystelsel voor het Caribisch deel van het Koninkrijk. Mijn collega, de staatssecretaris van Binnenlandse Zaken, is primair verantwoordelijk voor de routekaart en hij zal de Kamer hierover informeren. In algemene zin zal ik in Q1 2027 de Kamer een brief sturen over de connectiviteit van het Caribisch deel van het Koninkrijk.

Mevrouw Zwinkels vroeg nog om een toezegging over de subpagina over veilig internetten. Die komt binnen een halfjaar, uiterlijk Q1 2027. Mocht u suggesties hebben voor wat erop moet komen te staan, laat die dan het liefst zo snel mogelijk onze kant op komen, dan kunnen we daarnaar kijken.

Mevrouw Zwinkels vroeg ook nog wat er precies te verwachten valt bij de Nederlandse en Europese evaluatie van de wet. Bij de Nederlandse evaluatie wordt specifiek gekeken naar de werking van de nationale uitvoeringswet: hoe doeltreffend en effectief is die wet? Zo'n evaluatie valt onder de verantwoordelijkheid van het ministerie van Economische Zaken, maar zal door een externe partij, niet door RDI, worden uitgevoerd. De evaluatie van de Europese Unie wordt uitgevoerd door de Europese Commissie en die geldt voor de hele CRA. Die moet plaatsvinden voor 11 december 2030.

Mevrouw Zwinkels vroeg ook nog hoe om te gaan met de kwetsbaarheden, de CRA en de geleerde lessen. Het NCSC verzamelt allerlei informatie over de kwetsbaarheden, zeker wanneer het grote incidenten betreft. Het informeert op zijn website over kwetsbaarheden en neemt daarin de geleerde lessen nadrukkelijk mee.

Er was nog een vraag van mevrouw Kathmann over de doorrekening. Keep it coming! Ik heb wel leuke ideeën daarvoor, maar die doorrekening is bij het impactassessment gedaan. De Europese Commissie heeft toen gekeken naar de kosten. Het bespaart kosten als het gaat om datalekken, ransomware, schade door uitval van producten en hacks. Daar zit die besparing in. Ik kan nu niet die rekensom opnieuw voor u maken, maar ik kan me voorstellen dat het ook in Nederlandse gevallen niet alleen bij de overheid voor een besparing kan zorgen als dit soort dingen voorkomen worden, maar ook bij consumenten, fabrikanten en ondernemers.

De laatste vraag, waar anderen ook zeer benieuwd naar waren, was van mevrouw Zwinkels en ging over de pakkans van niet-Europese landen en fabrikanten: hoe kan je die zo groot mogelijk maken? In veel gevallen worden producten van een niet-Europese fabrikant op de Europese markt gebracht door een in Europa gevestigde importeur. In dat geval heeft de importeur de verplichting om te controleren of aan alle eisen is voldaan. Daar is hij op aanspreekbaar. Feitelijk betekent dit dat de RDI gewoon bij de importeur kan controleren of in de haven kan gaan staan om de controle uit te voeren. Als er sprake is van de verkoop van producten via onlineplatforms buiten de Unie aan afnemers in de Unie, dan is het in eerste instantie aan de aanbieder van het product om ervoor te zorgen dat aan de CRA wordt voldaan. Als hij dat niet doet, kan het platform gevraagd worden om het aanbod te verwijderen. De Digitaledienstenverordening geeft nadere invulling aan de verplichtingen van de onlineplatforms hierbij. Dat geldt ook voor platforms die buiten de Unie zijn gevestigd. Zo voorziet de verordening ook in de nodige mogelijkheden voor handhaving en sanctionering. Praktisch gezien kan daarbij worden gedacht dat ook de toezichthouder zelf gaat kijken, maar hij kan ook geautomatiseerde data van dit soort platforms bekijken. Als de toezichthouder producten ziet die niet aan de vereisten voldoen, kan hij met het platform in gesprek treden.

Het laatste punt was natuurlijk dat u nog wat ongemak voelde over dat er ook nog standaarden moeten worden uitgewerkt, et cetera. Mijn voorstel zou zijn dat ik u voor het zomerreces een update geef in een briefje met de stand van zaken op dat moment. Dat is dus voor de ingangsdatum van onderdelen van de verordening op 11 september 2027. Dan ontvangt u dus voor de zomer de laatste stand van zaken van mij per brief.

De **voorzitter**:
Dat leidt tot vragen. Mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):
Heel kort. Ik wil even die datum met elkaar scherp hebben. Ik ben heel erg blij met die toezegging, want die behoefte is inderdaad goed begrepen. Maar volgens mij ging het om 11 december, uit mijn hoofd. Dat was de tweede datum. Maar goed, voor het zomerreces is voor mij heel goed werkbaar.

Staatssecretaris **Aerdts**:
Mijn voorstel zou zijn voor het zomerreces. Inderdaad, excuus, ik zei het verkeerd; het is 11 december 2027. Mijn verwachting is dat een aantal standaarden voor de zomer zijn vastgesteld. Ik had het gevoel dat u behoefte had aan wat houvast over wat er de komende tijd gaat gebeuren. Voor de zomer kunnen we ook een update geven over de meldplicht en wat we daar in het eerste bijna-jaar van zien. Vandaar mijn voorstel. Als u zegt dat u het liever in november 2027 wilt, mag dat natuurlijk altijd.

Mevrouw **Zwinkels** (CDA):
Dan hier nog over. In de eerdere beantwoording gaf de staatssecretaris aan dat de EU en de RDI nog in Q1 2027 normen gaan opleveren. Welke normen zijn dat dan? Hoe verhoudt zich dat tot de zojuist toegezegde brief?

Staatssecretaris **Aerdts**:
Er zijn verschillende standaarden, uit mijn hoofd 42, die nog moeten worden ingevuld. Mijn voorstel is niet om u elke keer daarover te informeren. Daarom wil ik dat voor de

zomer doen. Dan geef ik een update van de normen die op dat moment zijn ingevuld in Europa en met behulp van RDI.

De **voorzitter**:
Als dat verder niet leidt tot vragen aan de staatssecretaris, kom ik tot een afronding van uw tweede termijn. Ik ga de toezeggingen nog even herhalen.

- De staatssecretaris zegt toe aan het einde van het jaar de Kamer meer duidelijkheid te geven over de opzet van de regulatory sandboxes.
- Een terugkoppeling van gesprekken over cyberveiligheid BES-eilanden ontvangt de Kamer uiterlijk Q1 2027.
- De staatssecretaris zegt toe de digitale APK op te nemen als onderdeel van de website www.veiliginternet.nl en de Kamer hierover te informeren in Q1 2027.
- Voor het zomerreces komt de laatste stand van zaken ten aanzien van de implementatie veiligheidsnormen en -standaarden.

Dan zijn wij volgens mij compleet. Ik kijk nog even de leden aan. Nog een laatste, mevrouw El Boujdaini.

Mevrouw **El Boujdaini** (D66):
Volgens mij was er nog een toezegging. We hebben ook genoteerd dat bij de evaluatie van de CRA ook de postkwantumcryptografie wordt meegenomen, of in ieder geval het kunnen meebewegen met nieuwe technologieën. Dat we dat ook even duidelijk hebben.

De **voorzitter**:
Ik kijk naar de staatssecretaris. Dat is een toezegging. Die gaan we vanuit de staatssecretaris teruggekoppeld zien middels een brief.

Staatssecretaris **Aerdts**:
Niet middels een aparte brief. Op het moment dat wij de Nederlandse evaluatie gaan doen, zullen we ook kijken of het meegroeien met nieuwe technieken, waaronder mogelijk postkwantumcryptografie, inderdaad werkt zoals de verwachting is. Dus geen aparte brief. Ik wil dit meenemen in de evaluatie.

De **voorzitter**:
Dan gaan we dat als zodanig doen. Daarmee zijn we rond.

Ik wijs u er nogmaals op dat we gaan stemmen op dinsdag 22 september. Dat is iets later, maar Prinsjesdag zit ertussen. Vandaar dat we dan zullen stemmen over deze wet. Ik zie een kleine teleurstelling bij de staatssecretaris, maar het is wat het is.

Daarmee sluit ik deze vergadering.

Sluiting 21.34 uur.