36 905 **Regels ter uitvoering van Verordening (EU) 2023/1543 van het Europees parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure en Richtlijn (EU) 2023/1544 van het Europees parlement en de Raad van 12 juli 2023 tot vaststelling van geharmoniseerde regels inzake de aanwijzing van aangewezen vestigingen en de aanstelling van wettelijke vertegenwoordigers ten behoeve van de vergaring van elektronisch bewijsmateriaal in strafprocedures (Uitvoeringswet elektronisch bewijsmateriaal)**

Nr. 6 **NOTA NAAR AANLEIDING VAN HET VERSLAG**
Ontvangen 26 mei 2026

Met veel belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Justitie en Veiligheid inzake dit voorstel van wet. Ik dank de leden van de verschillende fracties voor hun vragen en opmerkingen over het voorstel. Bij de beantwoording van de gestelde vragen is de volgorde van het verslag aangehouden. In het navolgende is de inhoud van het verslag cursief weergegeven. De antwoorden zijn in gewone opmaak weergegeven.

I. ALGEMEEN

1. Inleiding

De leden van de D66-fractie hebben met belangstelling kennisgenomen van de Uitvoeringswet elektronisch bewijsmateriaal (hierna: het wetsvoorstel). Het is van belang om daadkrachtig op te kunnen treden tegen de toenemende grensoverschrijdende en digitale criminaliteit in Nederland en andere lidstaten van de Europese Unie (EU). Deze leden vinden het daarom goed dat er een Europees e-Evidence pakket is gekomen om dit mogelijk te maken. Zo kunnen we samen met onze Europese buren en bondgenoten samenwerken om sneller, directer en grensoverschrijdend digitaal bewijsmateriaal te verkrijgen. Zeker omdat erg veel

strafonderzoek tegenwoordig een digitale component kent. Toch is het hierbij van belang om in de gaten te houden dat we het kind niet met het badwater weggooien. Meer daadkracht mag niet ten koste gaan van grondrechten van Europese burgers en principes van proportionaliteit, subsidiariteit en noodzakelijkheid. Ook de uitvoerbaarheid van de wet is een punt van aandacht, want pas in de toepassing vindt een wet zijn daadwerkelijke effect. In dit kader hebben deze leden nog enkele vragen.

De leden van de VVD-fractie hebben met interesse en enige zorgen kennisgenomen van het wetsvoorstel. Deze leden stellen dat elektronisch bewijsmateriaal tegenwoordig in circa 85% van de strafzaken een rol speelt. Vaak zijn gegevens echter buiten het grondgebied van Nederland opgeslagen en de toegang tot deze gegevens blijkt in de praktijk soms weerbarstig en langdurig. Het wetgevingspakket van de EU inzake elektronisch bewijsmateriaal is dan ook voor deze leden een waardevolle aanvulling op de bestaande EU-instrumenten voor de justitiële samenwerking in strafzaken. In die zin steunen deze leden ook de doelen van het wetsvoorstel. Toch hebben zij een aantal vragen en opmerkingen over het voorliggende wetsvoorstel.

De leden van de GroenLinks-PvdA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden begrijpen dat dit wetsvoorstel voortvloeit uit bindende Europese regelgeving waardoor de speelruimte van de Nederlandse wetgever om eigen regels te stellen beperkt is. Wel zouden de aan het woord zijnde leden er, wellicht ten overvloede, op willen wijzen dat met de invoering van het Europees verstrekkingsbevel en het Europees bewaringsbevel, waardoor buitenlandse opsporingsdiensten rechtstreeks bij Nederlandse dienstaanbieders elektronische gegevens kunnen opvragen of doen bewaren, twee ingrijpende instrumenten voor Europese rechtshulp worden ingevoerd. Hoewel deze leden ook begrijpen dat in deze tijden waarbij ook de criminaliteit als het ware "gedigitaliseerd" is effectievere en snellere wederzijdse rechtshulp nodig kan zijn, menen zij dat er reden tot zorg is ten aanzien van onder andere de rechtsbescherming nu het gebruik van deze instrumenten zonder tussenkomst van een

rechter vooraf gaat gebeuren. Deze leden hebben daarmee een aantal vragen en opmerkingen.

De leden van de CDA-fractie hebben met interesse kennisgenomen van het wetsvoorstel. Deze leden hebben nog enkele vragen aan de regering over dit wetsvoorstel.

De leden van de CDA-fractie lezen dat een van de voorwaarden voor een Europees verstrekkingsbevel en bewaringsbevel is dat een bevel slechts kan worden uitgevaardigd indien een soortgelijk bevel zou kunnen zijn uitgevaardigd in een soortgelijk nationaal geval. De uitvaardigende autoriteit moet dus ook voorwaarden uit het Wetboek van Strafvordering in acht nemen. Begrijpen deze leden het goed dat dit dus niet hoeft te gelden voor de autoriteit die het bevel ontvangt?

In Nederland kunnen de officier van justitie en de rechter-commissaris uitvaardigende autoriteit zijn. De e-Evidence verordening en het Wetboek van Strafvordering, zoals gewijzigd door het onderhavige wetsvoorstel, vormen daarbij voor de officier van justitie en de rechter-commissaris de wettelijke kaders. In de uitvoerende lidstaat vormen de e-Evidence verordening en het nationale recht van die lidstaat de wettelijke kaders voor de uitvoering van een verstrekkings- of bewaringsbevel.
In de spiegelbeeldige situatie vormen de e-Evidence verordening en het nationale recht van de uitvaardigende lidstaat de wettelijke kaders voor de uitvaardiging van een verstrekkings- of bewaringsbevel. De e-Evidence verordening, het Wetboek van Strafvordering en de onderhavige uitvoeringswet vormen de wettelijke kaders voor de uitvoering van deze bevelen in Nederland.

De leden van de CDA-fractie lezen dat in sommige gevallen een verplichting bestaat tot kennisgeving aan de tenuitvoerleggingsautoriteit op grond van artikel 8 van Verordening 2023/1543, bijvoorbeeld als het gaat om verkeersgegevens en inhoudelijke gegevens. Is het denkbaar dat een bewarings- of verstrekkingsbevel dat buiten die verplichting valt, soms ook ter kennisgeving wordt gegeven aan de tenuitvoerleggingsautoriteit? En zo ja, in welke gevallen?

De e-Evidence verordening biedt het wettelijke kader voor het al dan niet in kennis stellen van de tenuitvoerleggingsautoriteit in een andere lidstaat van de EU. Hoewel het wenselijk is dat bevoegde autoriteiten met het oog op de juiste toepassing van de verordening ook informeel contact kunnen onderhouden en de verordening daarvoor ook ruimte laat, laat de verordening geen ruimte voor (formele) kennisgevingen buiten de in artikel 8 van de verordening genoemde gevallen. Daarmee zou immers een kennisgevingsprocedure ontstaan die uitdrukkelijk niet is beoogd door de Europese wetgever. Dat zou onduidelijkheden tot gevolg hebben over de toepassing van het wettelijke kader.

De leden van de CDA-fractie lezen dat er sprake kan zijn van verschillende weigeringsgronden in het kader van de tenuitvoerleggingsprocedure, zoals het geval waarin naleving niet mogelijk is vanwege feitelijke omstandigheden. Kan de regering daar verder op ingaan en aangeven welke gevallen hieronder kunnen vallen?

Van feitelijke onmogelijkheid om uitvoering te geven aan een verstrekkingsbevel is bijvoorbeeld sprake indien de persoon om wiens gegevens wordt gevraagd geen klant is van de dienstaanbieder of de dienstaanbieder niet over de gevorderde gegevens beschikt, omdat de gegevens niet meer worden bewaard (op grond van de door de dienstaanbieder gehanteerde termijn voor het bewaren van gegevens).

2. Hoofdlijnen van het elektronisch bewijsmateriaalpakket

De leden van de D66-fractie hebben vragen over de omschrijving van de hoofdlijnen van het elektronisch bewijsmateriaalpakket. In de memorie van toelichting is opgenomen dat elektronisch bewijsmateriaal in dezen gaat over "abonneegegevens, verkeersgegevens of inhoudelijke gegevens die door of namens een dienstaanbieder zijn opgeslagen op het tijdstip van de ontvangst van het bevel". Toekomstige gegevens zijn uitgesloten, net als versleutelde berichten (decryptie/ontsleuteling valt buiten de reikwijdte). Nationaal kan er niet zomaar getornd worden aan het type

gegevens wat onder deze wetgeving valt. Dat kan alleen via wijziging van de Europese verordening. Dat roept bij deze leden de vraag op hoe gemakkelijk dit op Europees niveau gewijzigd kan worden en welke waarborgen er op dat niveau zijn voor oprekken of wijziging van het type gegevens in de toekomst. Kan de regering daar toelichting op geven?

Voor een wijziging van de e-Evidence verordening geldt de gewone wetgevingsprocedure. Dit houdt in dat alleen de Europese Commissie een voorstel voor wijziging van de verordening kan doen betreffende het type gegevens waarop de verordening ziet. De Commissie stuurt dit voorstel aan de Raad van Ministers van de EU en het Europees Parlement ter behandeling. Tegelijkertijd legt de Commissie het voorstel ter beoordeling voor aan de nationale parlementen. Indien nodig wordt het voorstel ook voor advies toegezonden aan andere EU-instellingen en -organen, zoals het Europees Economisch en Sociaal Comité.
De Raad en het Europees Parlement bespreken beide het voorstel en kunnen het wijzigen. Deze bespreking wordt een lezing genoemd. De hele procedure kan tot drie lezingen omvatten. Het voorstel wordt aangenomen als de Raad en het Europees Parlement in een van de lezingen overeenstemming bereiken over de tekst ervan. Als er geen overeenstemming wordt bereikt, wordt het voorstel niet aangenomen.
Voor een eventueel voorstel tot wijziging van de verordening geldt – net als dat voor nationale wetgeving geldt – dat het voorstel in overeenstemming moet zijn met hoger recht, zoals het Handvest van de Grondrechten van de EU en het Europees verdrag voor de rechten van de mens. Als dat niet het geval is, kan het Hof van Justitie van de EU de (wijzigings)verordening ongeldig verklaren, zoals dat bijvoorbeeld in 2014 is gebeurd met de dataretentierichtlijn (HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12*, Digital Rights Ireland en Seitlinger e.a.*).

De leden van de D66-fractie vragen daarnaast hoe wordt gecontroleerd dat gegevens niet breder gebruikt worden dan voor het doel van het strafrechtelijk onderzoek in kwestie, en wie daar op controleert als er niet altijd sprake is van tussenkomst van een rechter-commissaris. En onder welke voorwaarden kunnen deze gegevens worden ingezien op

aanvraag? Hoe worden maatregelen tegen misbruik van deze gegevens genomen?

Voor de rechtmatige verwerking van gegevens die met een verstrekkingsbevel zijn verkregen is het nationale recht van de desbetreffende lidstaat van belang. Dit betekent in het algemeen dat de rechtmatigheid van het gebruik van gegevens door de rechter kan worden getoetst in het kader van een specifieke strafzaak, maar betekent ook dat de regels en waarborgen van het gegevensbeschermingsrecht van toepassing zijn. Waar het gaat om de verwerking van persoonsgegevens door politie en justitie in het kader van het strafrecht geldt dat daarop de regels van EU-richtlijn 2016/680 van toepassing zijn. Deze richtlijn geldt voor alle lidstaten. In Nederland is deze richtlijn met name geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Op de naleving van deze wetten wordt toezicht gehouden door de Autoriteit Persoonsgegevens, die zo nodig een last onder bestuursdwang of een bestuurlijke boete kan opleggen.
In het kader van een strafzaak heeft de verdachte recht op de kennisneming van de processtukken op grond van de regeling in het Wetboek van Strafvordering. Daarnaast heeft de persoon op wie persoonsgegevens betrekking hebben op grond van de Wpg en Wjsg het recht op inzage in zijn of haar persoonsgegevens. Een dergelijk verzoek wordt gericht aan de verwerkingsverantwoordelijke, dat wil zeggen de korpschef bij de politie en het College van Procureurs-Generaal bij het Openbaar Ministerie. Een verzoek kan wegens een limitatief aantal in de wet vastgelegde gronden worden geweigerd.

De leden van de VVD-fractie constateren dat criminele netwerken zich niet laten tegenhouden door landsgrenzen. In dat licht is het cruciaal dat elektronische gegevens over criminele activiteiten die zijn opgeslagen op servers buiten Nederland en in beheer zijn van hostingdiensten snel kunnen worden opgevraagd en vervolgens snel kunnen worden betrokken bij de opsporing, vervolging en berechting van criminelen. Kan de regering aangeven welke impact het wetsvoorstel zal hebben op de werkdruk en de doorlooptijden bij de nationale politie, het Openbaar Ministerie (OM) en de rechtspraak? Is het de bedoeling dat er na inwerkingtreding

van het wetsvoorstel meer capaciteit vrijkomt voor het verwerken van rechtshulpverzoeken? Kunnen er dus ook meer rechtshulpverzoeken worden gedaan door Nederland?

Mede op basis van de impactanalyse die de EU Commissie heeft gepubliceerd in 2018 bij de presentatie van het e-Evidencepakket en de concepttekst van de verordening en de richtlijn, is in het voorjaar van 2024 een nadere impactanalyse uitgevoerd. De politie, het OM en de rechtspraak zijn daarbij inhoudelijk betrokken en hebben voor nadere analyse van gegevens over rechtshulp van en naar Nederland en via deskundigenpanels input geleverd. Die input was gebaseerd op een gezamenlijke beschrijving van de toenmalige werkprocessen rond rechtshulp en van de toekomstige werkprocessen. Daarbij is uitdrukkelijk benoemd dat e-Evidence een nieuwe vorm van rechtshulp is, maar dat bestaande vormen van rechtshulp, zoals rechtshulpverzoeken op grond van de EU rechtshulpovereenkomst, de richtlijn Europees onderzoekbevel en de rechtshulp op basis van artikel 35 van het Cybercrimeverdrag, ook in stand blijven. Het e-Evidencepakket kenmerkt zich ten opzichte van die bestaande instrumenten door aanmerkelijk kortere doorlooptijden van een bevel tot bewaren of verstrekken van gegevens, een grotere afdwingbaarheid van de bevelen op grond van de verordening e-Evidence in de richting van bedrijven, mede door de extraterritoriale werking ten aanzien van bedrijven die in de EU diensten aanbieden maar daar niet zijn gevestigd en efficiëntere, gedigitaliseerde, communicatie over de bevelen. In de impactanalyse is daarom aangenomen dat zich een verplaatsingseffect zal voordoen. Minder rechtshulpverzoeken, Europese onderzoeksbevelen en verzoeken op basis van artikel 35 van het Cybercrimeverdrag en meer e-Evidencebevelen. Bij de e-Evidencebevelen die zullen worden gericht aan in Nederland gevestigde of vertegenwoordigde bedrijven (de inkomende bevelen) valt een deel van het werk van politie en OM weg omdat de bevelen rechtstreeks naar de bedrijven gaan. Bij de uitgaande bevelen zal het werk bij politie en OM niet zozeer vervallen, maar zal de capaciteit kunnen worden ingezet die vrij komt door het initieel minder belastende proces van e-Evidencebevelen, en zal er sprake zijn van het hiervoor genoemde verplaatsingseffect. Wel zal sprake zijn van extra impact als gevolg van de notificaties in het geval een justitiële

autoriteit van een andere lidstaat een bevel uitvaardigt aan een in Nederland gevestigd of vertegenwoordigd bedrijf en dat bevel betrekking heeft op verkeers- en/of inhoudelijke gegevens. Deskundigen merken daarbij op dat zij verwachten dat gelet op de uitzonderingsgronden waarbij geen notificatie is vereist, met name de gevallen waarin het in het onderzoek naar een concreet strafbaar feit gaat om een in het uitvaardigende land gepleegd feit en/of de verdachte onderdaan is of verblijft in die uitvaardigende lidstaat, het aantal notificaties een relatief kleiner deel van het totaal zal omvatten. Ten slotte is vanwege de steeds grotere toename van het aantal strafbare feiten waarin digitaal bewijs een rol speelt, een mogelijk aanzuigende werking van het e-Evidencepakket aangenomen, in uitgaande bevelen, als ook in inkomende bevelen.
In de impactanalyse zijn op basis van de beschikbare gegevens over de huidige rechtshulpprocessen scenario's (laag, midden, hoog) ontwikkeld waarmee een schatting is gedaan over de impact op de werklast bij politie en OM. Het middenscenario werd uiteindelijk als meest waarschijnlijk geduid. Daarin sprake van vermindering van werklast bij de politie en beperkte toename bij het OM. Vanwege de beschikbare basisgegevens over de werklast bij de ZM in de huidige rechtshulp was het niet mogelijk daar een schatting te doen over verandering van de last. De ZM gaf in de begeleiding van het impactonderzoek aan geen grote impact te verwachten.
Overigens bezien OM en de politie nu al op basis van de verder gevorderde implementatieactiviteiten of de inzichten over de impact scherper kunnen worden gesteld. Evenwel blijft de verwachting staan dat het e-Evidence pakket in principe een efficiënter werkproces zal opleveren waarmee de doorlooptijd (sterk) afneemt, maar dat dit niet per se tot een verminderde werkdruk zal leiden. In het begin zal dit met name liggen aan het opdoen van ervaring met het nieuwe werkproces en de automatisering. Naar verloop van tijd, wanneer deze ervaring wel is opgedaan, is de verwachting dat er meer bevelen kunnen worden uitgestuurd dan nu gebeurt onder het klassieke rechtshulpstelsel. Omdat e-Evidence ervoor zorgt dat meer bedrijven dan voorheen rechtstreeks benaderbaar zijn, zal het aantal kansen voor de opsporing ook toenemen. Hierbij dient vermeld te worden dat de snelheid van reactie leidt tot het eerder beschikbaar

komen van relevante opsporingsinformatie, wat tot meer opsporingskansen kan leiden. Meer relevante informatie kan ook leiden tot meer specifieke of uitgebreidere rechtshulpverzoeken. Bovenstaande effecten die leiden tot meer opsporingskansen kunnen vervolgens voor een hogere werkdruk zorgen.

Bij de eerdere impactanalyse is de aanbeveling gedaan om vanaf de inwerkingtreding de volumes van het Europees verstrekkings- en bewaringsbevel te meten zodat zicht komt op daadwerkelijke veranderingen in de werkprocessen en de werklast. Deze aanbeveling heb ik overgenomen. Op basis hiervan kan worden bekeken of de processen en IT-systemen moeten worden aangepast en of er voldoende menskracht beschikbaar is.

De leden van de GroenLinks-PvdA-fractie menen dat in het kader van onderlinge rechtshulp binnen de EU tot nu toe het uitgangspunt van dubbele strafbaarheid geldt. De aan het woord zijnde leden zouden niet graag zien dat een justitiële autoriteit uit een land waar bijvoorbeeld euthanasie of abortus wordt vervolgd met behulp van in Nederland verkregen digitale gegevens iemand zou kunnen vervolgen. Of dat een officier van justitie uit een uitvaardigende lidstaat waar de rechtsstaat onder druk staat met behulp van uit Nederland verkregen gegevens een politieke tegenstander kan vervolgen. Deelt de regering deze mening? Zo ja, welke waarborgen gelden er om te voorkomen dat het Europees verstrekkingsbevel/bewaringsbevel voor dergelijke doelen wordt gebruikt? Zo nee, waarom deelt de regering deze mening niet?

Op basis van de e-Evidence verordening is een dienstaanbieder gehouden om gehoor te geven aan een Europees verstrekkingsbevel, behoudens de in de verordening aangegeven gevallen. Verder kan de uitvoering van een verstrekkingsbevel alleen worden geweigerd in de gevallen dat een beroep kan worden gedaan op een weigeringsgrond. Het ontbreken van strafbaarheid in de tenuitvoerleggende lidstaat is één van die weigeringsgronden. In de meeste EU landen zijn euthanasie en abortus strafbaar. En overigens ook in Nederland. Euthanasie en abortus zijn in Nederland alleen niet strafbaar

indien deze zijn begaan door een arts en is voldaan aan wettelijke zorgvuldigheidseisen. Op de reikwijdte van de weigeringsgrond inzake dubbele strafbaarheid ga ik nader in bij de beantwoording van de hierna volgende vraag van deze leden.
Andere weigeringsgronden houden verband met de beperking van strafrechtelijke aansprakelijkheid die verband houden met de persvrijheid of de vrijheid van meningsuiting in andere media en de mogelijkheid van een kennelijke schending van een relevant grondrecht als bedoeld in artikel 6 van het Verdrag betreffende de Europese Unie en in het EU Handvest. Ik wijs in dit verband ook op overweging 11 van de verordening die luidt: “Niets in deze verordening mag worden uitgelegd als een verbod voor een tenuitvoerleggingsautoriteit een Europees verstrekkingsbevel te weigeren wanneer er redenen bestaan om op basis van objectieve elementen aan te nemen dat het Europees verstrekkingsbevel is uitgevaardigd om iemand te vervolgen of te bestraffen vanwege het gender, het ras of de etnische afkomst, de godsdienst, de seksuele geaardheid of genderidentiteit, de nationaliteit, de taal of politieke overtuigingen van die persoon, of dat de positie van die persoon om een van die redenen kan worden aangetast.”
Het is aan de officier van justitie – als de op grond van het onderhavige wetsvoorstel aangewezen tenuitvoerleggingsautoriteit – om te beoordelen of een beroep moet worden gedaan op een weigeringsgrond. Indien dat het geval is, wordt geen uitvoering gegeven aan het Europees verstrekkingsbevel en worden dientengevolge door de dienstaanbieder geen gegevens verstrekt.
Het is in het licht van het voorgaande niet aan de regering om in te gaan op allerlei verschillende casusposities die zich zouden kunnen voordoen en mogelijke gevallen waarin een Nederlandse tenuitvoerleggingsautoriteit een beslissing moet nemen over een beroep op een weigeringsgrond.

De leden van de GroenLinks-PvdA-fractie vragen tevens in welke mate de voorwaarde van dubbele strafbaarheid ook gaat gelden voor het Europees verstrekkingsbevel en het Europees bewaringsbevel. Hoe moeten deze leden in dit verband de voorwaarde dat een Europees verstrekkingsbevel/bewaringsbevel slechts kan worden uitgevaardigd indien een soortgelijk bevel zou kunnen zijn

uitgevaardigd in een soortgelijk nationaal geval (artikelen 5 en 6 van Verordening 2023/1543) lezen? En tevens in dit verband: deze leden lezen dat aan het opvragen van elektronisch bewijsmateriaal betreffende verkeersgegevens en inhoudelijke gegevens restricties zijn verbonden waaronder dat voor de uitvaardiging van een Europees verstrekkingsbevel voor dit soort gegevens de tenuitvoerleggingsautoriteit, in Nederland de officier van justitie, verplicht in kennis moet worden gesteld. Die officier van justitie kan vervolgens toetsen of er sprake is van een weigeringsgrond op grond waarvan de gevraagde gegevens niet hoeven te worden verstrekt. Een van die weigeringsgronden is als een feit niet strafbaar is in de tenuitvoerleggingsstaat, tenzij het om een van de 32 ernstige misdrijven gaat zoals vermeld in bijlage IV van Verordening 2023/1543. Betekent dat dat in het geval het niet om een van die 32 misdrijven gaat, de Nederlandse officier van justitie geen mogelijkheid heeft om een bevel te toetsen? En, zo vragen de aan het woord zijnde leden, is er als het om abonneegegevens en identificerende gegevens gaat helemaal geen mogelijkheid dat er in de uitvoerende staat een toets plaats kan vinden? Met andere woorden: als er vanuit een lidstaat aan een Nederlandse dienstaanbieder om dergelijke informatie wordt gevraagd is die direct gehouden daaraan tegemoet te komen zonder mogelijkheid van bezwaar of beroep in eigen land? Klopt het dat in het geval een dienstaanbieder bezwaar wil maken tegen het verstrekken van de gevraagde abonnee- of identificerende gegevens die aanbieder alleen bezwaar dan wel beroep kan aantekenen bij een autoriteit van het uitvaardigende land?

De voorwaarde dat een verstrekkingsbevel/bewaringsbevel slechts kan worden uitgevaardigd indien een soortgelijk bevel zou kunnen zijn uitgevaardigd in een soortgelijk nationaal geval moet als volgt worden begrepen in relatie tot dubbele strafbaarheid. Op grond van de e-Evidence verordening kunnen verstrekkingsbevelen en bewaringsbevelen uitsluitend in het kader van de toepassing van het strafrecht worden uitgevaardigd. Wordt een bevel uitgevaardigd ten behoeve van een strafrechtelijk onderzoek dan zal sprake moeten zijn van de verdenking van een strafbaar feit. Een bevel kan niet worden uitgevaardigd als in de uitvaardigende lidstaat geen sprake is van een strafbaar feit. Algemeen

bekend is dat binnen de EU veel dezelfde of vergelijkbare feiten strafbaar zijn gesteld. Niettemin is het denkbaar dat een feit in de ene lidstaat wel en in de andere lidstaat niet strafbaar is gesteld. In algemene zin geldt in EU-wetgeving betreffende de wederzijdse erkenning in strafzaken dat met betrekking tot de zogenaamde lijstfeiten dubbele strafbaarheid geen voorwaarde is. Dat wil zeggen dat het ontbreken van strafbaarheid in de uitvoerende lidstaat geen reden is om een uitgevaardigd bevel niet uit te voeren. In de e-Evidence verordening is deze gebruikelijk regeling ook opgenomen. Op grond van artikel 12 van de verordening kan in de aldaar bedoelde gevallen de tenuitvoerlegging van een verstrekkingsbevel worden geweigerd indien het feit waarvoor het bevel is uitgevaardigd op grond van het recht van de tenuitvoerleggingsstaat niet strafbaar is. Deze weigeringsgrond geldt echter niet indien het feit waarvoor het bevel is uitgevaardigd een feit is dat op de lijst staat van bijlage IV bij de verordening en waarop in de uitvaardigende staat een strafmaximum van ten minste drie jaar gevangenisstraf is gesteld. Het gaat bij deze zogenaamde lijstfeiten om de gebruikelijke strafbare feiten in de EU-wetgeving. Over het algemeen zijn deze feiten in alle lidstaten strafbaar gesteld. Hoewel voor deze feiten dus niet de voorwaarde van dubbele strafbaarheid geldt, is in de praktijk in de regel wel sprake van strafbaarheid in beide betrokken lidstaten.
Indien een verstrekkingsbevel wordt uitgevaardigd voor een strafbaar feit dat in de uitvoerende lidstaat niet strafbaar is en dit strafbare feit staat niet op de lijst van bijlage IV bij de verordening, dan kan de officier van justitie de uitvoering van het bevel om die reden weigeren. Op grond van artikel 12, tweede lid, van de verordening is de dienstaanbieder dan gehouden de uitvoering van het verstrekkingsbevel te beëindigen en de gegevens niet over te dragen en is de uitvaardigende autoriteit gehouden het bevel in te trekken.
De mogelijkheid om de uitvoering van een verstrekkingsbevel te weigeren op grond van artikel 12 van de verordening in verband met het ontbreken van strafbaarheid in de uitvoerende lidstaat bestaat in de gevallen waarin het voor de uitvaardigende autoriteit op grond van artikel 8 van de verordening is aangewezen om een kennisgeving te doen aan de tenuitvoerleggingsautoriteit. Dat is in de gevallen waarin het bevel dient om (bepaalde) verkeersgegevens en

inhoudelijke gegevens te verkrijgen. Indien het bevel ertoe strekt om andere gegevens te verkrijgen, zoals abonneegegevens en de gebruiker identificerende gegevens, vindt geen kennisgeving aan de tenuitvoerleggingsautoriteit plaats en kan ook geen beroep worden gedaan op de weigeringsgronden van artikel 12 van de verordening, waaronder het ontbreken van strafbaarheid in de uitvoerende lidstaat.
Wel voorziet de verordening in de zogenaamde tenuitvoerleggingsprocedure (artikel 16). Deze houdt in dat de uitvaardigende autoriteit de tenuitvoerleggende autoriteit kan verzoeken het Europees verstrekkingsbevel of het Europees bewaringsbevel ten uitvoer te leggen, indien de geadresseerde dienstaanbieder niet binnen de toepasselijke termijn zonder opgaaf van redenen gevolg heeft gegeven aan het bevel en de tenuitvoerleggende autoriteit (nog) geen weigeringsgronden heeft aangevoerd. De tenuitvoerleggende autoriteit kan vervolgens een beroep doen op de weigeringsgronden die in artikel 16, vierde en vijfde lid, van de verordening zijn opgenomen. Het gaat daarbij onder meer om de volgende weigeringsgronden: het is feitelijk onmogelijk om het bevel na te leven, de gevraagde gegevens worden beschermd door voorrechten of immuniteiten, de gevraagde gegevens vallen onder regels inzake de vaststelling of beperking van strafrechtelijke aansprakelijkheid die verband houden met de persvrijheid of de vrijheid van meningsuiting in andere media, er zijn gegronde redenen zijn om aan te nemen dat de uitvoering van het Europees verstrekkingsbevel een kennelijke schending van een relevant grondrecht als bedoeld in artikel 6 van het Verdrag betreffende de Europese Unie en in het EU Handvest zou inhouden. Op grond van het onderhavige wetsvoorstel beslist de officier van justitie over de tenuitvoerlegging van het bevel. Indien de officier geen beroep doet op een weigeringsgrond, beveelt hij de geadresseerde zijn verplichtingen uit hoofde van het bevel na te komen. Tegen de erkenning van het bevel kan de geadresseerde binnen twee weken na daarover in kennis te zijn gesteld nog bezwaar instellen bij de officier van justitie.
Op grond van artikel 18 van de verordening heeft iedere persoon wiens gegevens via een Europees verstrekkingsbevel werden gevraagd het recht op doeltreffende rechtsmiddelen tegen dat bevel. Indien die persoon een verdachte of beklaagde is, heeft die persoon het recht op doeltreffende

rechtsmiddelen tijdens de strafprocedure waarin de gegevens worden gebruikt. Met de mogelijkheid van beklag op grond van de artikelen 552a en 552d van het Wetboek van Strafvordering, zoals neergelegd in het nieuwe artikel 5.11.6, tweede lid, van het Wetboek van Strafvordering, zoals voorzien in het onderhavige wetsvoorstel, wordt voorts in een passend rechtsmiddel voorzien. Op het beklag wordt beslist door de raadkamer van de rechtbank. Tegen die beslissing staat beroep in cassatie open bij de Hoge Raad.
Daarnaast kan het gebruik van gegevens die door middel van een Europees verstrekkingsbevel zijn verkregen, bij de inhoudelijk behandeling van de strafzaak door de verdachte aan de orde worden gesteld, zodat de strafrechter zich daarover kan uitspreken.

Hoe verhoudt de rechtsbescherming in het geval van een Europees verstrekkingsbevel of bewaringsbevel zich tot de rechtsmiddelen die open staan bij de uitvoering of uitvaardiging van een Europees opsporingsbevel, bijvoorbeeld als het om een toetsende rol van de rechter(-commissaris) gaat, zo vragen de leden van de GroenLinks-PvdA-fractie. En aanvullend: hoe gaat de rechtsbescherming, bijvoorbeeld ten aanzien van proportionaliteit en de rechten van betrokkenen, in de praktijk werken? Welke concrete mogelijkheden zijn er om op basis van deze gronden geen gegevens te verstrekken of te bewaren?

De rechtsbescherming in het geval van een Europees verstrekkingsbevel of bewaringsbevel is op vergelijkbare manier vormgegeven als de rechtsbescherming in het geval van een Europees onderzoeksbevel. Dit houdt in dat de beklagprocedure van artikel 552a Sv als een belangrijk rechtsmiddel geldt.
Wel is het zo dat een Europees onderzoeksbevel betrekking kan hebben op een grote variëteit aan onderzoekshandelingen, terwijl een Europees verstrekkingsbevel of bewaringsbevel enkel ziet op het verkrijgen van abonneegegevens, verkeersgegevens en inhoudelijke gegevens ter zake van elektronische communicatie en andere diensten als bedoeld in artikel 3, onderdeel 3, van de verordening. Ter uitvoering van een Europees onderzoeksbevel kunnen opsporingsbevoegdheden worden toegepast onder dezelfde voorwaarden waaronder

deze kunnen worden toegepast in een Nederlands onderzoek naar dezelfde feiten op grond van het Wetboek van Strafvordering. Dit houdt in dat in voorkomend geval ook een machtiging van de rechter-commissaris moet worden verkregen. Voorts kan de rechter-commissaris zelf worden belast met de uitvoering van een onderzoeksbevel.
Voor alle genoemde bevelen geldt dat de uitvoering van een bevel alleen kan worden geweigerd op de gronden en in de gevallen die zijn voorzien in de toepasselijke EU-regelgeving. Voor zowel het Europees verstrekkingsbevel of bewaringsbevel als het Europees onderzoeksbevel is één van die weigeringsgronden dat er gegronde redenen zijn om aan te nemen dat de uitvoering van het bevel een kennelijke schending van een relevant grondrecht als bedoeld in artikel 6 van het Verdrag betreffende de Europese Unie en het EU Handvest van de grondrechten zou opleveren. In een dergelijk geval is het dus mogelijk om ter bescherming van de rechten van de betrokkene geen gegevens te verstrekken of te bewaren.

3. Hoofdlijnen van het wetsvoorstel

De leden van de D66-fractie hebben vragen over de hoofdlijnen van het wetsvoorstel. Daarbij wordt er ook een onderscheid gemaakt tussen de typen gegevens en de waarborgen die daaraan verbonden zijn: voor abonnee- of identificerende gegevens is er geen kennisgeving of tussenkomst van een officier van justitie of rechter-commissaris verplicht. Bij verkeers- en inhoudelijke gegevens is een machtiging van de rechter-commissaris vereist. Vooral de uitwerking in de praktijk van deze aspecten van de Verordening roepen enkele vragen op bij deze leden. Hoe verhouden de vorderingen voor verstrekking of bewaring van gegevens door een officier van justitie zonder tussenkomst van rechters zich tot het evenredigheidsbeginsel, effectieve rechtsbescherming en het recht op een eerlijk proces ten opzichte van partijen die enkel in Nederland gevestigd zijn? Als er geen tussenkomst is van een rechter in bepaalde gevallen, hoe kan dan van de geadresseerde verwacht worden dat er een gedegen controle komt op het 'ne bis in idem'-beginsel en tegenstrijdige verplichtingen in de betreffende lidstaat of derde landen? En gezien, de geadresseerde in sommige gevallen vorderingen ontvangt zonder rechterlijke

toetsing en direct benaderd wordt door (het buitenlandse equivalent van) de officier van justitie: hoe kan de geadresseerde dan zelf toetsen of voldoen aan de vordering feitelijk onmogelijk is, of dat weigering gegrond is? Hoe verhoudt zich dat tot het recht op een eerlijk proces en tot de geldboetes en andere straffen voor niet tijdig voorzien in verstrekking/bewaring?

In de e-Evidence verordening wordt een onderscheid gemaakt tussen verschillende categorieën van gegevens, nl. abonneegegevens, verkeersgegevens en inhoudelijke gegevens. Dit strookt met het recht van veel lidstaten, het Unierecht en de rechtspraak van het Hof van Justitie. Op basis van dit onderscheid is een toetsende rol voor de rechter wel of niet voorgeschreven. Indien een Europees verstrekkingsbevel strekt tot het verkrijgen van verkeersgegevens (met uitzondering van gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker) of inhoudelijke gegevens moet het bevel worden bekrachtigd door een rechter, rechtbank of onderzoeksrechter (artikel 4, tweede lid, van de verordening). In Nederland betekent dit dan een machtiging van de rechter-commissaris.
Er kan daarom van worden uitgegaan dat de regeling in de verordening en uitvoering in het onderhavige wetvoorstel voldoet aan de eisen in de jurisprudentie betreffende onder meer het evenredigheidsbeginsel, effectieve rechtsbescherming en het recht op een eerlijk proces. Eisen waaraan alle lidstaten van de EU moeten voldoen in het licht van het primaire en secundaire EU-recht.
Wat betreft de controle op het ‘ne bis in idem’-beginsel merk ik het volgende op. Het is in de eerste plaats aan de uitvaardigende autoriteit om te controleren dat er geen redenen zijn om aan te nemen dat het uitvaardigen van een Europees verstrekkingsbevel of bewaringsbevel strijdig zou zijn met het ne bis in idem-beginsel. Indien de uitvaardigende autoriteit redenen heeft om aan te nemen dat in een andere lidstaat mogelijk een parallelle strafprocedure wordt gevoerd, is zij gehouden de autoriteiten van die lidstaat te raadplegen (overeenkomstig EU-kaderbesluit 2009/948/JBZ dat ziet op het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht in strafprocedures). Wordt na deze controle een bevel uitgevaardigd dan is het vervolgens

niet aan de geadresseerde (dienstaanbieder) om te toetsen aan het ne bis in idem-beginsel – die beschikt immers niet over de daartoe benodigde informatie – maar aan de tenuitvoerleggingsautoriteit in het kader van een mogelijk beroep op een weigeringsgrond. Voorts merk ik nog op dat ook de strafrechter in het kader van de behandeling van de strafzaak kan beoordelen of sprake is van respectering van het ne bis in idem-beginsel.
Voor het geval dat er sprake is van tegenstrijdige verplichtingen voorziet de verordening in een toetsingsprocedure bij de rechter (artikel 17). Het gaat dan om de situatie dat een geadresseerde van mening is dat de naleving van een Europees verstrekkingsbevel in strijd zou zijn met een verplichting uit hoofde van het toepasselijke recht van een derde land. De geadresseerde kan dan zijn mening dat er sprake is van tegenstrijdige verplichtingen uiteenzetten in een zogenaamd gemotiveerd bezwaar. De uitvaardigende autoriteit moet vervolgens het Europees verstrekkingsbevel aan de hand van het gemotiveerde bezwaar toetsen en eventuele inbreng van de tenuitvoerleggingsstaat. Indien de uitvaardigende autoriteit voornemens is het Europees verstrekkingsbevel in stand te houden, moet zij een bevoegde rechter van de uitvaardigende staat verzoeken om een toetsing. De uitvoering van het Europees verstrekkingsbevel wordt opgeschort in afwachting van de voltooiing van de toetsingsprocedure. In Nederland zijn op grond van het onderhavige wetsvoorstel de rechtbanken bevoegd om te beslissen in de toetsingsprocedure.
De vaststelling dat het feitelijk onmogelijk is een bevel uit te voeren kan wel door de geadresseerde (dienstaanbieder) worden gedaan. Het gaat hierbij, zoals hierboven aangegeven in antwoord op een vraag van de leden van de CDA-fractie, bijvoorbeeld om gevallen waarin de persoon om wiens gegevens wordt gevraagd geen klant is van de dienstaanbieder of de dienstaanbieder niet over de gevorderde gegevens beschikt, omdat de gegevens niet meer worden bewaard (op grond van de door de dienstaanbieder gehanteerde termijn voor het bewaren van gegevens).

De leden van de D66-fractie lezen dat de regering aangeeft niet aan de kritiekpunten van de Afdeling advisering van de Raad van State (hierna: de Afdeling) over de 'fundamentele

kritiekpunten over rechtsbescherming en de systematiek van directe grensoverschrijdende bevelen' tegemoet te kunnen komen omdat deze punten voortvloeien uit bindende regelgeving. Dat klinkt deze leden wat tegenstrijdig in de oren. De punten waar meer fundamentele kritiek op is gegeven op het gebied van rechtsbescherming en systematiek van directe grensoverschrijdende bevelen zijn de basis waarop deze wet berust en gaan over grondrechten van betrokkenen. Het betreft bij de kritiekpunten over rechtsbescherming en de systematiek van grensoverschrijdende bevelen onder anderen: de beperkte rol van zowel Nederlandse als buitenlandse rechters bij binnenkomende en uitgaande bevelen, de positie van dienstaanbieders, de bescherming van de gegevens die uitgewisseld worden en de uitvoerbaarheid en handhaafbaarheid van de wet. Kan de regering meer context geven bij de (on)mogelijkheden van het tegemoetkomen aan de deze kritiek en hoe de rechtsbeginselen die in het geding zijn onder de Europese verordening worden geborgd? Gaat het hier om dwingend EU-recht, en hoe verhoudt zich dat tot de mogelijk verzwakte rechtspositie van betrokkenen? Zou de regering aan kunnen geven waar zij mogelijkheden ziet waarop de wet wél ingevoerd kan worden zonder mogelijk de rechtspositie van betrokkenen te schaden?

De regering heeft in het advies van de Afdeling advisering van de Raad van State over het onderhavige wetsvoorstel niet de fundamentele kritiekpunten over rechtsbescherming kunnen vinden waar de leden van de D66-fractie naar verwijzen. Er is ook geen sprake van dat de regering niet aan de punten in het advies van de Raad van State tegemoet is gekomen. Zowel aan het advies inzake rechtspersoonlijkheid van dienstaanbieders als het advies over de bevoegdheden van de ACM is tegemoet gekomen.
Ik merk hierbij op dat de e-Evidence verordening op verschillende manieren in rechtsbescherming voorziet (door betrokkenheid van rechters voor te schrijven en door te verplichten tot effectieve rechtsmiddelen). In het onderhavige wetsvoorstel is daaraan uitvoering gegeven.

De leden van de VVD-fractie constateren dat het wetsvoorstel onder andere een nieuwe titel van het vijfde boek van het Wetboek van Strafvordering introduceert. Deze leden vragen

hoe de uitvoeringswet zich verhoudt tot het nieuwe Wetboek van Strafvordering. Worden de bevoegdheden uit de uitvoeringswet direct en beleidsneutraal overgezet via de tweede aanvullingswet bij het nieuwe Wetboek of via de invoeringswet van het nieuwe Wetboek?

De wijzigingen van het Wetboek van Strafvordering waarin het onderhavige wetsvoorstel voorziet zullen deel uitmaken van de invoeringswet voor het nieuwe Wetboek van Strafvordering. Daarbij wordt de regeling in het onderhavige wetsvoorstel beleidsneutraal overgezet naar het nieuwe wetboek.

4. Uitvoering

De leden van de D66-fractie hebben de volgende vragen en opmerkingen met betrekking tot de uitvoering. Opgemerkt wordt door NLconnect, dat het beoogde systeem voor het delen van de gegevens in kwestie het Reference Implementation Systeem betreft. Dat systeem voldoet niet aan alle Nederlandse standaarden voor systemen voor dit soort gegevensdeling. Heeft de regering alternatieven verkend of gekeken hoe de vereisten om aan Nederlandse standaarden te voldoen toegepast kunnen worden op het Reference Implementation Systeem? Hoe reflecteert de regering breder op de zorgen die bij deze branche leven?

In de triloogfase van het wetgevingsproces voor het e-Evidence pakket is op instigatie van het Europees parlement in het wetsvoorstel ingevoegd dat het nieuw in te voeren rechtshulpinstrument direct ook zou moeten voldoen aan de toen parallel in onderhandeling zijnde digitaliseringsverordening (Verordening (EU) 2023/2844). Dat is neergelegd in artikel 19 van de verordening. Lidstaten hebben de opdracht aangewezen vestigingen of wettelijke vertegenwoordigers van in de lidstaat gevestigde of vertegenwoordigde bedrijven via hun nationale IT-systeem toegang te verlenen tot het EU gedecentraliseerd IT-systeem. Artikel 22 geeft aan de Europese Commissie zogenoemde *reference implementation software* zal creëren, onderhouden en beheren en dat lidstaten die software kunnen gebruiken in plaats van een nationaal systeem.

Vanwege eerdere ervaringen met dergelijke software bij het implementeren van de Verordening (EU) 2020/1784 inzake de betekening en de kennisgeving van stukken en met het oog op de implementatie van de e-Justice verordening, die meer dan twintig instrumenten op het terrein van de justitiële samenwerking in grensoverschrijdende burgerlijke, handels- en strafzaken tot 2030 digitaliseert, heeft Nederland een voorkeur voor het zelf ontwikkelen van een nationaal IT-systeem als “back-end” voor het EU gedecentraliseerd IT-systeem. Vooralsnog is Nederland de enige lidstaat die werkt aan een eigen nationaal IT-systeem. De ontwikkeling van en bekendmaking van voldoende specificaties om zelf een nationaal systeem te maken lopen moeizaam en duren erg lang. Met moeite wordt nu gewerkt aan een nationaal systeem (portaal) dat als back end voor het EU gedecentraliseerd IT systeem kan werken voor de justitiële autoriteiten. Eind februari is geconstateerd dat een nationaal IT-systeem als back end voor bedrijven echter niet meer haalbaar was gelet op de planning van het in gebruik nemen van dat systeem bij de inwerkingtreding van de verordening op 18 augustus 2026. Als alternatief is ervoor gekozen dan vooralsnog voor dit portaal de *reference implementation software* te gebruiken. Overigens is er op het moment van het schrijven van dit antwoord nog geen *reference implementation software* die geschikt is voor e-Evidence. De Europese Commissie heeft een beoogde productieversie aangekondigd voor deze maand (mei 2026).

De branche die door NLconnect wordt vertegenwoordigd kwam in het voorjaar van 2026 met een notitie dat de *reference implementation software* niet voldoet aan alle Nederlandse standaarden voor systemen voor dit soort gegevensdeling. Er wordt met name gewezen op EU eisen ten aanzien van cybersecurity en de nationale uitwerking daarvan. Van de Europese Commissie heb ik begrepen dat die strijdigheid niet wordt gezien en van andere lidstaten zijn deze geluiden ook niet gehoord.
Waar dat kon, heeft mijn ministerie bedrijven via informatiesessies, nieuwsbrieven, en andere contacten zoveel mogelijk meegenomen in de implementatie van het e-Evidencepakket. Daarbij was het een grote handicap dat niet of pas heel laat meer concrete specificaties over het systeem gedeeld konden worden. Daarom begrijp ik de zorgen van de

branche zeer zeker, herken ik ze en erken ik ze op onderdelen. Ik blijf mij inspannen om zodanig met de branche en overigens ook de vele andere branches die onder reikwijdte van het e-Evidencepakket vallen, zo goed mogelijk te informeren en waar ik dat kan te ondersteunen. Ik realiseer mij daarbij terdege dat de tijd die rest tot augustus 2026 heel kort is.
Het streven van de regering is erop gericht dat het onderhavige wetsvoorstel zo snel mogelijk de instemming van de Tweede Kamer en vervolgens de Eerste Kamer kan krijgen. Wanneer dat het geval is, zal moeten worden vastgesteld wanneer de inwerkingtreding ervan met het oog op een goede uitvoering verantwoord is.

De leden van de D66-fractie hebben vernomen dat NLconnect aangeeft dat er grote zorgen en vragen zijn over implementatie. Hoe kan verzekerd worden dat geadresseerden voorzien worden in hun recht op een eerlijk proces als randvoorwaarden voor goede uitvoer nog niet in werking zijn, maar er wel al gehandhaafd wordt?

De brancheorganisatie NLconnect heeft ook bij mij haar zorgen en vragen aangegeven. Ik begrijp deze zorgen en de vragen, erken ze op onderdelen en blijf mij inspannen om zodanig met de branche en overigens ook de vele andere branches die onder de reikwijdte van het e-Evidencepakket vallen, zo goed mogelijk te informeren en waar ik dat kan te ondersteunen.
Als ik de vraagstelling goed begrijp, gaat die ervan uit dat de bedrijven vanaf augustus 2026 met handhavende acties vanuit de toezichthouder of vanuit de justitiële autoriteiten kunnen worden geconfronteerd op basis van de artikelen 5 van de richtlijn en 15 van de verordening, terwijl de bedrijven er vanwege niet aan hen toe te rekenen omstandigheden nog niet klaar voor zijn om via de verplicht voorgeschreven digitale wijze te communiceren over e-Evidence bevelen. Dat niet klaar zijn, kan eruit bestaan dat de registratie van in Nederland gevestigde of vertegenwoordigde bedrijven nog niet rond is en uitgaande bevelen daarom nog niet via het EU gedecentraliseerd IT-systeem aan hen kunnen worden geadresseerd. Deels komt dit doordat er voor de ACM geen rechtsgrondslag is voor toezicht en handhaving zolang de onderhavige uitvoeringswet nog niet in werking is getreden.

Een en ander betekent dat bedrijven zich op dit moment wel kunnen aanmelden voor registratie, maar dat het registratieproces nog niet afgerond kan worden. Dit valt de bedrijven niet aan te rekenen. In de praktijk zal dat betekenen dat een EU lidstaat geen e-Evidence bevel kan uitsturen naar het bedrijf en zal daardoor ook niet kunnen worden toegekomen aan het opleggen van een sanctie. Andere belangrijke redenen dat bedrijven, maar ook de Nederlandse overheid, niet klaar zijn voor communicatie via de verplicht voorgeschreven digitale wijze, zijn de complexe en uit de planning gelopen voorbereidingen voor het in werking krijgen van het EU gedecentraliseerd IT-systeem, te laat kunnen beschikken over specificaties die het mogelijk maken dat de Nederlandse overheid bedrijven toegang kan verlenen tot een werkend IT-systeem en dat de bedrijven een redelijke termijn nodig hebben om hun eigen bedrijfsprocessen zodanig in te richten dat zij met behulp van het IT-systeem bevelen kunnen ontvangen en behandelen om uiteindelijk gegevens te verstrekken. Sinds enkele maanden is duidelijk geworden dat de beschikbare termijn in redelijkheid niet meer kan worden gehaald. De betrokken dienstaanbieders kan dit niet worden aangerekend. Handhaving vanuit de toezichthouder – zelfs indien dit wetsvoorstel dan in werking is getreden - kan daarom niet aan de orde zijn.

Het ligt voor de hand dat als dit op grote schaal gebeurt omdat een groot deel of zelfs de gehele in Nederland gevestigde of vertegenwoordigde industrie niet is geregistreerd, andere lidstaten Nederland daarop politiek via mij aanspreken. Naast het bovenstaande zal ik dan aangegeven dat vanwege de complexe inrichtingsvragen voor dit nieuwe systeem pas in een later stadium dan initieel gepland een geschikte toezichthouder is bevonden, en dat het voor de justitiële autoriteiten moeizamer was dan initieel gedacht om de op basis van de verordening te onderscheiden werkstromen op een goede manier in te passen in de bestaande uitvoeringspraktijk. Dit alles heeft ook geleid tot vertraging in het wetgevingsproces.

Ik heb de ACM meegegeven dat, wanneer de rechtsgrondslag er wel is, de niet aan de industrie toe te rekenen omstandigheden waardoor zij nog niet klaar zijn om e-

Evidence bevelen uit te voeren, niet zouden moeten leiden tot het opleggen van boetes.

Het vorenstaande is door mijn ministerie ook verschillende keren gedeeld met medewerkers van de Europese Commissie. Mijn beeld is dat de Commissie deze punten op zichzelf uitlegbaar vindt. Verder erkent de Commissie dat er nogal wat andere lidstaten dezelfde problemen bij implementatie ondervinden en hun zorgen uiten niet op tijd klaar te zijn. Niettemin wil de Commissie vasthouden aan de in de verordening neergelegde datum voor inwerkingtreding die ingebruikname per 18 augustus 2026 voorschrijft. Voor de Commissie is vooral van belang het momentum om op korte termijn tot uitvoering van e-Evidence te komen en daarmee bij te dragen aan een effectievere opsporing van strafbare feiten ten behoeve van de veiligheid van burgers en bedrijven in de EU. Volgens de Commissie zal de realiteit in het najaar mogelijk zijn dat een groep van 5 à 6 lidstaten wel klaar is voor inwerkingtreding en dat de andere landen later en gaandeweg zullen aansluiten. Van Nederlands zijde is daarop aangegeven dat dat moeilijk werkbaar en uitvoerbaar zal zijn. De Commissie wil nader overleg voeren om de uitvoerbaarheid van een dergelijke gefaseerde invoering van e-Evidence te vergroten.

De leden van de VVD-fractie vragen naar de verdere gevolgen van de wijze waarop het wetsvoorstel wordt uitgevoerd voor de regeldruk en administratieve lastendruk voor bedrijven. Deze leden constateren dat sommige lidstaten ervoor kiezen om bedrijven eerst te waarschuwen en hulp te bieden bij het inrichten van de wettelijk vertegenwoordiger, voordat er mogelijk miljoenenboetes worden opgelegd. Hoe kijkt de regering hiernaar?

Ten aanzien van het inrichten van de wettelijke vertegenwoordiger is in Nederland de ACM de beoogde toezichthouder. De ACM zal bij het mogelijk opleggen van boetes de gebruikelijke bestuursrechtelijke aanpak hanteren, die mede kan inhouden dat de ACM met een waarschuwing, via een gesprek of een formele brief, een bedrijf verzoekt zijn handelswijze aan te passen.

Naast de hierboven al genoemde, in het voorjaar van 2024 uitgevoerde nadere impactanalyse voor de justitieketen is ook onderzocht welke effecten de Europese e-Evidence verordening en -richtlijn gaan hebben op de regeldruk van Nederlandse dienstenaanbieders. Tijdens zowel inventariserende interviews als bij georganiseerde groepsbijeenkomsten brachten de grotere dienstenaanbieders ter sprake (op dat moment) geen uitspraken te kunnen doen over de verwachte impact die e-Evidence op hun bedrijfsvoering en werkwijze heeft. Ze gaven aan dat dit voor hen niet goed mogelijk is vanwege de grote mate van onzekerheid rondom de exacte uitwerking van e-Evidence die zij ervoeren. Over de werkwijzen van grote telecomaanbieders voor de afhandeling van een verzoek in de huidige situatie werd meegedeeld dat die dusdanig uiteenlopend zijn (van grotendeels geautomatiseerd tot ‘handmatige verwerking’ en maatwerk) dat de aanbieders geen uitspraak kunnen of willen doen over het verwachte tijdsbeslag. Met de kleinere dienstenaanbieders is het wel gelukt om een tijdsinschatting voor een ‘eenvoudig’ verzoek te bepalen, evenals een laag-midden-hoog schatting voor de meer ingewikkelde verzoeken. Het volume van verzoeken in de huidige en de toekomstige situatie is in dit regeldrukonderzoek gebaseerd op het onderzoek dat is verricht voor de impactanalyse van werkprocessen bij OM en politie.
Uit een uiteindelijke doorrekening blijkt dat de regeldruk als gevolg van e-Evidence wordt ingeschat op € 540.000 tot ongeveer € 2.160.000 in 2026 voor geheel Nederland. Deze bedragen zijn weergegeven op het verwachte prijspeil in 2026.
Al tijdens de onderhandelingen van het voorstel heeft Nederland sterk aangedrongen op een zekere bescherming van met name kleine en middelgrote ondernemingen. Mede als gevolg daarvan is in de verordening opgenomen dat dergelijke bedrijven gezamenlijk kunnen “poolen” in het organiseren van hetgeen nodig is om als bedrijf aan een bevel te voldoen.

De leden van de VVD-fractie lezen dat bij de uitvoering van het Europees verstrekkingsbevel en het bewaringsbevel gebruik zal worden gemaakt van e-Codex. Dat is een bestaande gemeenschappelijke dienst in het justitiedomein en

de Nederlandse standaard voor digitale grensoverschrijdende gegevensuitwisseling. Justid verzorgt de fysieke aansluiting. Gelet op de problemen bij Justid die de afgelopen jaren zijn ontstaan, zoals het moeten uitvoeren van een correctie bij 8% van de inzageverzoeken (bijlage bij Kamerstuk 35916, nr. 6) vragen deze leden of er een uitvoeringstoets bij Justid is gedaan en zo ja, of die met de Kamer kan worden gedeeld.

Er is geen afzonderlijke uitvoeringstoets door Justid uitgevoerd. Wel is Justid betrokken bij de voorbereiding en implementatie van e-Evidence. Sinds 2023 neemt Justid met een eigen programmaorganisatie deel aan de programma's die vanuit mijn ministerie zijn ingericht voor de implementatie van het Europees verstrekkingsbevel en het bewaringsbevel.
Justid is onder andere verantwoordelijk voor diverse digitale voorzieningen en gegevensuitwisselingssystemen binnen het justitie- en veiligheidsdomein. Vanuit deze brede rol en expertise is Justid betrokken bij de ontwikkeling, implementatie en het beheer van voorzieningen voor (grensoverschrijdende) gegevensuitwisseling, waaronder e-CODEX.
Justid heeft actief bijgedragen aan de architectuur en uitvoering van het nationale deel van het EU-gedecentraliseerde IT-systeem. Hieronder valt ook het gebruik van bestaande e-CODEX-structuren ten dienste van e-Evidence. Daarbij zijn uitvoeringsaspecten gedurende het ontwikkel- en implementatietraject doorlopend betrokken en meegewogen.

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van een brief van NLconnect, de brancheverenigingvan de telecomindustrie, waarin deze sector grote zorgen uit over de implementatie van het Europees verstrekkingsbevel en het Europees bewaringsbevel. Die zorgen richten zich met name op het ontbreken van belangrijke technische afspraken, duidelijke procesbeschrijvingen en goede beveiligingsafspraken. NLconnect meent dat daardoor een zorgvuldige invoering binnen de gestelde implementatietermijn onhaalbaar is en men voorziet spanning met bestaande cybersecurityregels. Zo stelt NLconnect dat de benodigde informatie over de werking van e-Evidence te laat is verstrekt, waardoor de sector nu te

weinig tijd heeft om systemen te ontwerpen, bouwen en testen, medewerkers op te leiden en processen goed in te richten. Zij menen daarom dat zij niet aan de nieuwe regels die 18 augustus 2026 in werking treden kunnen voldoen. Om die reden zou toezicht en handhaving pas moeten beginnen als aanbieders een redelijke termijn hebben gehad om hun systemen op orde te brengen en op een veilige manier de juiste informatie kunnen delen. Kan de regering hierop in gaan? Voorts wijst NLconnect erop dat de regels van de Nederlandse Cyberbeveiligingswet aanbieders verplicht om hun netwerken en systemen zo goed mogelijk te beschermen tegen cyberaanvallen. Dat strookt naar de mening van NLconnect niet met het wisselen van informatie ten behoeve van e-Evidence via het openbare internet. Om hackers of inbraak door buitenlandse staten te voorkomen vragen de aanbieders een fysiek gesloten en zwaarbeveiligd systeem. Deelt de regering deze mening van de sector? Zo ja, welke gevolgen heeft dit voor de invoeringstermijn of het handhaven van de wettelijke regels? Kan met het opleggen van sancties worden gewacht tot dat de sector wel in staat is gebleken om de wet veilig uit te voeren?

In het hierboven gegeven antwoord op vragen van leden van de D66-fractie is al ingegaan op het ontbreken van belangrijke technische afspraken en duidelijke procesbeschrijvingen. Ik heb aangegeven dat ik deze punten herken en op onderdelen erken. Voor mij is helder dat de bedrijven maar ook Nederlandse overheid vanwege de complexe en uit de planning gelopen voorbereidingen voor het in werking krijgen van het EU gedecentraliseerd IT-systeem te laat kunnen beschikken over de specificaties die het mogelijk maken dat de Nederlandse overheid bedrijven toegang kan verlenen tot een werkend IT-systeem. Duidelijk is ook dat de bedrijven een redelijke termijn nodig hebben om hun eigen bedrijfsprocessen zodanig in te richten dat zij met behulp van het IT-systeem bevelen kunnen ontvangen en behandelen om uiteindelijk gegevens te verstrekken. Sinds enkele maanden is duidelijk dat de beschikbare termijn in redelijkheid niet kan worden gehaald. Dat kan de dienstaanbieders niet worden aangerekend. Handhaving vanuit de toezichthouder kan daarom niet aan de orde zijn. Handhaving is eerst aan de orde wanneer de bedrijven zich

hebben kunnen voorbereiden en alsdan toch niet aan de wettelijke verplichtingen voldoen.
Waar het de mogelijke samenloop met of tegenstrijdigheid van de beveiligingseisen op basis van de e-Evidence verordening met andere informatiebeveiligingseisen betreft, wordt het standpunt van NLconnect nog nader bekeken en loopt nog overleg met NLconnect. Ik heb er hierboven al op gewezen dat de gesignaleerde strijdigheid door de Europese Commissie niet wordt gezien en dat van andere lidstaten deze geluiden ook niet zijn gehoord. Voor de Nederlandse wet- en regelgeving geldt dat deze in overeenstemming moet zijn met het toepasselijke primaire en secundaire EU-recht. Het is primair aan de Europese Commissie om ervoor te waken dat EU-regelgeving, zoals het e-Evidence pakket en de daarop gebaseerde uitvoeringsregelingen en Richtlijn (EU) 2022/2555 van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (de NIS 2-richtlijn) consistente en verenigbare beveiligingseisen stellen. Voor zover Nederlandse wet- en regelgeving niet verenigbaar zou zijn met het EU-recht dient zo mogelijk sprake te zijn van een EU-recht conforme toepassing.

De leden van de CDA-fractie lezen dat onderhavig wetsvoorstel uitvoeringsgevolgen heeft voor het Openbaar Ministerie (OM), de rechtspraak en de Autoriteit Consument en Markt (ACM). Kan de regering nader ingaan op de omvang van deze gevolgen en op de vraag of de uitvoeringsorganisaties voldoende capaciteit beschikbaar hebben om het wetsvoorstel uit te voeren?

In het antwoord op vragen van de leden van de VVD-fractie is hierboven ingegaan op de impactanalyse voor uitvoering van het e-Evidence pakket voor OM en politie uit 2024 en op de laatste stand van zaken daaromtrent.
De ACM zal taken verrichten die voortvloeien uit het onderhavige wetsvoorstel dat uitvoering geeft aan de richtlijn e-Evidence. De kosten voor het uitvoeren daarvan zijn geschat op jaarlijks € 664.000. De ACM voert deze taak uit onder opdrachtgeverschap van de minister van Justitie en Veiligheid, en deze draagt daarmee ook alle kosten die nodig zijn voor de taakuitvoering. De ACM heeft geen taak ten aanzien van de afdoening van concrete bevelen.

De Raad voor de rechtspraak heeft in zijn reactie aangegeven dat het wetsvoorstel geen hoge IT-impact heeft voor de rechtspraak. Evenmin verwacht de Raad grote werklasteffecten wat betreft eventuele effecten van bestuursrechtelijke of strafrechtelijke handhaving. Wel geeft de Raad aan dat het wetsvoorstel zorgt voor een toename van de werklast voor rechter-commissarissen en de raadkamer. In zijn reactie heeft de Raad dit werklasteffect geschat op € 737.000 per jaar structureel.

5. Toezicht en handhaving

De leden van de D66-fractie hebben de volgende vraag over toezicht en handhaving. De ACM geeft aan dat zij vier randvoorwaarden schetst voor de uitvoerbaarheid en handhaafbaarheid van het wetsvoorstel. Kan de regering inmiddels meer informatie verschaffen over de stand van zaken op deze vier benodigde randvoorwaarden (te weten: rekening houden met onvoorspelbaarheid en omvang en beweeglijkheid van het aantal marktspelers dat onder het toezicht valt; een operationeel registratieplatform; een aanpassing met duidelijke scheiding tussen bestuursrecht en strafrecht; en de opname van een rechtsgrondslag voor de samenwerking en gegevensuitwisseling tussen het OM en de ACM)?

Het aantal dienstaanbieders dat in Nederland zal worden geregistreerd en dus onder het toezicht van de ACM valt, is op voorhand niet precies te voorspellen. Dit is door de regering onderkend en besproken met de ACM. Ik zorg als opdrachtgever voor voldoende financiële middelen voor de taakuitvoering.
De ACM voert het toezicht signaalgedreven uit en richt zich daarbij dus primair op dienstaanbieders ten aanzien van wie er signalen zijn dat zij niet voldoen aan de gestelde eisen. Mocht voor deze invulling van de toezichttaak in de toekomst het eerder genoemde budget van € 664.000 onvoldoende zijn, zal in overleg tussen ACM en de minister van Justitie en Veiligheid worden bezien wat nodig is.
Ten aanzien van het registratieplatform is als randvoorwaarde gegeven dat het platform operationeel is ten tijde van de inwerkingtreding van de wet. De zorg was dat de ACM in de situatie zou komen dat ze formeel een taak zouden

hebben in het registratieproces nog voordat het platform, dat wordt beheerd door de Europese Commissie, operationeel was. Inmiddels is de situatie omgekeerd; het platform is sinds dit voorjaar operationeel, maar de wet is nog niet in werking. Het kabinet beziet op dit moment of er mogelijkheden zijn om, vooruitlopend op inwerkingtreding van het wetsvoorstel, vanuit Nederland het registratieproces niet te vertragen.
Ten aanzien van het toepasselijke recht is er op grond van het onderhavige wetsvoorstel geen rol voor de ACM bij het toepassen van het strafrecht en geen rol bij de afhandeling van concrete bevelen. Het wetsvoorstel is verder aangepast zodat de hoogte van het bedrag van de last onder dwangsom en de bestuurlijke boete aansluit bij het boeteregime van de ACM. Tot slot is na nadere bestudering gebleken dat de bestaande wetgeving al voorziet in grondslagen voor de gegevensuitwisseling tussen de ACM en het OM. Het gaat dan om grondslagen in de Wet justitiële en strafvorderlijke gegevens en in de Instellingswet ACM, verder uitgewerkt in een algemene maatregel van bestuur, de Regeling gegevensverstrekking ACM 2019.

De leden van de VVD-fractie lezen in de reactie op het verzoek voor een uitvoerbaarheids- en handhaafbaarheidstoets van de ACM dat door ABDTOPConsult een verkenning is gedaan om te verkennen welke organisatie een geschikte toezichthouder als bedoeld in de richtlijn zou zijn. Kan worden toegelicht waarom deze verkenning niet bij verzending van het wetsvoorstel naar de Kamer is gestuurd?

Het briefadvies van ABDTOPConsult is gepubliceerd op de website van de rijksoverheid op 25 november 2024.[1]

De leden van de VVD-fractie lezen in de verkenning dat ABDTOPConsult concludeerde dat er geen ideale partij is om de taken van de centrale autoriteit op zich te nemen, maar dat de ACM wel kan worden aangemerkt als de plek die zoveel mogelijk recht doet aan de opgave en aan de Haagse werkelijkheid. Deze leden vinden het vooral belangrijk dat er wordt gekeken hoe een autoriteit effectief kan bijdragen aan het oplossen van problemen van mensen en hoe in dit geval

[1] Zie https://www.rijksoverheid.nl/documenten/2024/11/25/briefadvies-verkenning-beleggen-toezicht-e-evidence-richtlijn.

de belangen van de Nederlandse burgers, van de strafrechtketen en in het bijzonder de opsporing het beste worden gediend. Deze leden constateren dat de taak die het wetsvoorstel toebedeelt aan de ACM in beginsel niet goed past bij de ACM, omdat het geen markttoezicht betreft. Ook de kennis en expertise van de strafrechtketen is bij de ACM niet direct aanwezig. Kan de regering toelichten hoe de ACM wordt ondersteund om de nieuwe taak uit te voeren zonder dat uitvoering van de bestaande wettelijke taken van de ACM onder druk komen te staan? Hoe is de ministeriële verantwoordelijkheid straks geborgd als er fouten worden gemaakt bij het uitvoeren van het toezicht op de naleving van de richtlijn? Is dat de minister van Economische Zaken die verantwoordelijk is voor de ACM of is dat de minister van Justitie en Veiligheid als opdrachtgever?

Voor de uitvoering van de nieuwe taak voor de ACM op grond van het onderhavige wetsvoorstel is kennis van de strafrechtketen niet noodzakelijk. De ACM krijgt geen rol bij de toepassing van het strafrecht en geen rol bij de afhandeling van concrete e-Evidence bevelen.
De ACM krijgt wel een rol bij het registratieproces van dienstaanbieders die onder de regelgeving vallen en hun adres in Nederland willen registeren. Daarnaast gaat zij het toezicht uitvoeren ten aanzien van de aanwijzing van een wettelijke vertegenwoordiger door die dienstaanbieders, de vastlegging van de keuze van hun voertaal, en de inrichting van hun bedrijf zodat zij in staat zijn om bevelen tijdig op te volgen. Daarbij past de ACM het bestuursrecht toe. Dit toezicht op administratieve conformiteit lijkt op een aantal de uitvoering van de Digitale dienstenverordening (DSA) betreffende taken die ook bij ACM zijn belegd. De communicatie met het Openbaar Ministerie gaat over signalen dat dienstaanbieders niet in staat (lijken te) zijn om bevelen tijdig uit te voeren, hetgeen kan wijzen op problemen in de bedrijfsinrichting. Er is geen sprake van communicatie of afstemming over concrete verstrekkings- of bewaringsbevelen en de ACM heeft daarbij dus ook geen rol.
De ACM voert de e-Evidence-taak uit onder opdrachtgeverschap van de minister van Justitie en Veiligheid. Deze minister is daarmee verantwoordelijk voor de correcte inhoudelijke uitvoering van de taak en levert de financiële middelen voor de taakuitvoering. De minister van

Economische Zaken en Klimaat heeft in het bestuurlijke model in algemene zin de eigenaarsrol ten aanzien van de ACM, en is op dit dossier slechts voor dat gedeelte de minister die de verantwoordelijkheid draagt. Deze verantwoordelijkheid omvat derhalve niet de inhoud van de taakuitvoering door de ACM en de politieke eindverantwoordelijkheid daarover.

De leden van de VVD-fractie begrijpen dat de ACM straks toeziet op de aanwezigheid van de wettelijke vertegenwoordiger en dus niet op de inhoud van de gegevensverstrekking. Wat gebeurt er straks in de praktijk als een bedrijf wel een wettelijk vertegenwoordiger heeft aangesteld, maar de wettelijk vertegenwoordiger structureel niet thuis geeft wanneer het OM Europese verstrekkingsbevelen en bewaringsbevelen uitvaardigt en bijvoorbeeld niet voldoende responsief handelt of adequaat meewerkt aan het bevel? Deze leden constateren dat de scheidslijn in de praktijk dun kan zijn. Kan de regering nader toelichten hoe de coördinatie tussen de ACM en het OM is vormgegeven? Wordt er een samenwerkingsprotocol of convenant opgesteld om afspraken te maken voor gevallen waarin een 'papieren' wettelijk vertegenwoordiger de effectieve opsporing belemmert? En welke grondslag biedt het wetsvoorstel om de kwaliteit en slagkracht van de wettelijk vertegenwoordiger te toetsen, naast de enkele formele aanwezigheid?

Wanneer het OM bevelen uitvaardigt, zijn die gericht aan buitenlandse dienstaanbieders, die niet onder het toezicht van de ACM vallen, maar onder de bevoegde toezichthouder in de tenuitvoerleggende lidstaat. Wanneer een in Nederland geregistreerde dienstaanbieder, die daartoe een wettelijke vertegenwoordiger heeft aangewezen, niet of niet tijdig reageert op een bevel van een bevoegde autoriteit uit een andere lidstaat, zal die autoriteit dat moeten melden bij het Nederlandse OM, die dan in het concrete geval op kan treden. Wanneer het OM over hetzelfde bedrijf meerdere soortgelijke meldingen krijgt, kan dit signaal aan de ACM worden gegeven, omdat het een indicatie is dat de slagkracht van de vertegenwoordiger dan wel de inrichting van het bedrijf niet goed op orde is, hetgeen onder de toezichtstaak van de ACM valt. Hierbij wordt niet gecommuniceerd over

concrete bevelen, want daarbij heeft de ACM geen rol. En dus ook niet bij de gegevensverstrekking in de betreffende zaak. Bij het uitvoeren van de toets naar de kwaliteit en slagkracht van de wettelijke vertegenwoordiger kan de ACM de gebruikelijke bestuursrechtelijke middelen inzetten, waaronder het vorderen van informatie bij de dienstaanbieder.

In de bijlage bij de reactie van de ACM op de artikelsgewijze toelichting lezen de leden van de VVD-fractie dat de ACM heeft voorgesteld om een grondslag op te nemen in het wetsvoorstel voor samenwerking en gegevensuitwisseling met het OM. Kan de regering toelichten waarom deze opmerking van de ACM niet heeft geleid tot het opnemen van een dergelijke wettelijke grondslag?

Naar aanleiding van de door de ACM uitgevoerde uitvoeringstoets is overleg geweest met de ACM. Op basis van dat overleg is geconcludeerd dat voor de gegevensuitwisseling tussen de ACM en het OM in de bestaande wetgeving afdoende grondslagen zijn. Zoals ik hierboven heb aangegeven, gaat het om grondslagen in de Wet justitiële en strafvorderlijke gegevens en in de Instellingswet ACM, verder uitgewerkt in een algemene maatregel van bestuur, de Regeling gegevensverstrekking ACM 2019.

6. Financiële gevolgen

De leden van de VVD-fractie lezen dat de gereserveerde bedragen voor de implementatie oplopen van 4.8 miljoen euro in 2024 tot 10.7 miljoen euro in 2029. Naarmate die datum dichterbij komt en de binnen het programma in te voeren werkprocessen concreter worden, zal het inzicht in de kosten scherper worden. Deze leden vragen welke aannames er worden gedaan bij het ramen van deze kosten en welke mogelijkheden er zijn om bij te sturen als de aantallen van het aantal inkomende en uitgaande Europese verstrekkingsbevelen en bewaringsbevelen veel hoger zijn dan geraamd

De gereserveerde bedragen zijn gebaseerd op inschattingen in 2024 over de impact op uitvoeringsorganisaties van de

invoering van zowel het e-Evidencepakket als de digitaliseringsverordening (e-Justice). Vanaf het moment dat de toepassing van e-Evidence daadwerkelijk mogelijk is, zullen de volumes van e-Evidence bevelen, maar ook van verzoeken en bevelen op basis van de thans voor het vergaren van dergelijke gegevens gebruikte instrumenten (rechtshulpverzoeken en Europese onderzoeksbevelen) op verschillende momenten worden gemeten. Dan zullen de daadwerkelijke impact en de financiële gevolgen daarvan kunnen worden ingeschat en kan als dat nodig is binnen de regels van de rijksbegroting mogelijk tot aanpassingen worden gekomen.

7. Reacties van het OM, de Raad voor de rechtspraak, de politie en de ACM

De leden van de D66-fractie hebben op basis van de reacties van het OM, de Raad voor de rechtspraak, de politie en de ACM de volgende vragen. In reactie op de kritiek van de Raad voor de rechtspraak en privacy-organisaties wordt gewezen op de wijze waarop rechtsbescherming van burgers geborgd wordt, in het bijzonder over het op de hoogte stellen van het opvragen van hun gegevens zodat zij gebruik kunnen maken van rechtsmiddelen. In de memorie van toelichting staat voorts dat betrokkenen in beginsel moeten worden geïnformeerd, maar dat uitstel van kennisgeving ook mogelijk is "indien het belang van het onderzoek dit dringend vereist". In de memorie van toelichting worden geen vaste termijnen genoemd waarbinnen de kennisgeving alsnog moet plaatsvinden, en dat betrokkenen achteraf beklag kunnen doen via bestaande rechtsmiddelen (en lijkt dus vooral ex post te zijn). Daar zit voor betrokkenen een afhankelijkheid in van actieve kennisgeving door de betreffende (lid)staat/het OM en een risico voor misbruik van de mogelijkheid tot uitstel van kennisgeving. Kan de regering toelichten hoe deze afhankelijkheid verholpen wordt en welke maatregelen er zijn om misbruik van de uitstelregeling te voorkomen?

In de e-Evidence verordening (artikel 13, tweede lid) is bepaald dat de uitvaardigende autoriteit, overeenkomstig het nationale recht, de kennisgeving aan de betrokkene wiens gegevens worden gevraagd, kan uitstellen, beperken of achterwege laten. Hierbij wordt verwezen naar de EU-

richtlijn inzake gegevensbescherming in het politie- en justitiedomein (richtlijn 2016/680) die een vergelijkbare regeling kent voor het uitstellen, beperken of achterwege te laten van het verstrekken van informatie. De voorwaarden hierbij zijn dat het uitstellen, beperken of achterwege te laten een noodzakelijke en evenredige maatregel is om belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen, nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen, de openbare veiligheid te beschermen, de nationale veiligheid te beschermen of de rechten en vrijheden van anderen te beschermen.
Ook in het Nederlandse strafrecht is een dergelijke regeling voor het uitstellen van het verstrekken van informatie bekend. Een strafrechtelijk onderzoek kan immers ernstig worden belemmerd indien een verdachte ontijdig op de hoogte raakt van een tegen hem of haar lopend onderzoek en de informatie die in dat kader wordt vergaard. In dit licht is in artikel 5.11.6 van het Wetboek van Strafvordering, zoals gewijzigd door het onderhavige wetsvoorstel, bepaald dat de kennisgeving aan de betrokkene over de verstrekking van gegevens op basis van het Europees verstrekkingsbevel kan worden uitgesteld indien het belang van het onderzoek dit dringend vereist. Zodra dit in het belang van het onderzoek niet meer noodzakelijk is, wordt betrokkene geïnformeerd. Mij is geen informatie bekend dat van deze mogelijkheid tot uitstel in het kader van de strafrechtspleging misbruik wordt gemaakt.
Op grond van artikel 18 van de verordening heeft iedere persoon wiens gegevens via een Europees verstrekkingsbevel werden gevraagd het recht op doeltreffende rechtsmiddelen tegen dat bevel. Indien die persoon een verdachte of beklaagde is, heeft die persoon het recht op doeltreffende rechtsmiddelen tijdens de strafprocedure waarin de gegevens worden gebruikt.
Met de mogelijkheid van beklag op grond van de artikelen 552a en 552d van het Wetboek van Strafvordering, zoals neergelegd in het nieuwe artikel 5.11.6, tweede lid, van het Wetboek van Strafvordering, zoals voorzien in het onderhavige wetsvoorstel wordt in een passend rechtsmiddel voorzien. Daarnaast kan het gebruik van gegevens die door middel van een Europees verstrekkingsbevel zijn verkregen,

bij de inhoudelijke behandeling van de strafzaak door de verdachte aan de orde worden gesteld, zodat de strafrechter zich daarover kan uitspreken.

In reactie op de opmerkingen van het OM stelt de regering in dat artikel 2, tweede lid, van Verordening 2023/1543 de reikwijdte van de Verordening is beperkt tot strafzaken. In geval van een urgente persoonsvermissing – zonder dat tevens sprake is van een verdenking van een strafbaar feit – kan daarom geen Europees verstrekkingsbevel of Europees bewaringsbevel worden uitgevaardigd. De leden van de VVD-fractie vragen naar aanleiding van deze passage of bij de totstandkoming van artikel 2, tweede lid van de Verordening expliciet is besproken dat urgente persoonsvermissingen buiten het toepassingsbereik vallen en zo ja, of de regering bereid is bij de evaluatie van het e-Evidencepakket dit punt in te brengen, zodat ook in deze gevallen een Europees verstrekkingsbevel of Europees bewaringsbevel kan worden uitgevaardigd.

De regering is van mening dat het begrijpelijk is dat de reikwijdte van de e-Evidence verordening beperkt is tot strafzaken. Het gaat immers om bevoegdheden tot het verkrijgen van gegevens die een ingrijpende inmenging kunnen zijn in de privacy van burgers. Bij de totstandkoming van het e-Evidence pakket is niet gesproken over het onderwerp urgente persoonsvermissingen. In situaties waarin bij een vermissing wél sprake is van vermoedens van een strafbaar feit kan de verordening worden toegepast.
Ter gelegenheid van de evaluatie van de e-Evidence verordening zal kunnen worden vastgesteld of er in de praktijk behoefte is aan de uitbreiding van de reikwijdte van de verordening wat betreft persoonsvermissingen zonder dat sprake is van een verdenking van een strafbaar feit. Zoals gebruikelijk zal Nederland dan relevante instanties betrekken bij die evaluatie. Dat doet de Europese Commissie, als verantwoordelijke voor de evaluatie, overigens zelf ook.

De leden van de VVD-fractie betreuren daarnaast dat vooralsnog niet is gekozen om het onderscheppen van real-time dataverkeer of te verwachten dataverkeer onder het bereik van de richtlijn en de Verordening te brengen. Datzelfde geldt voor het ontsleutelingsbevel. Klopt het dat de

politie en het OM in de praktijk hier wel om hebben gevraagd of dit behulpzaam vinden? Kan de regering bevestigen dat Europol hier ook heel erg mee geholpen zou zijn?

Het e-Evidencepakket richt zich inderdaad alleen op reeds vastgelegde gegevens en voor zover die in de normale bedrijfsvoering van de onder het pakket vallende dienstaanbieders worden bewaard. Dat op zich is al een hele stap voorwaarts. In andere verbanden hebben politie en OM inderdaad aangedrongen op het effectiever toegang verkrijgen tot real-time informatie. Omdat deze problematiek per definitie grensoverschrijdend is, wordt het debat daarover gevoerd in de EU. Zo wordt momenteel in Europees verband door een interdisciplinaire groep van experts gekeken naar technische mogelijkheden om, op een cyberveilige manier waarbij privacy-grondrechten gewaarborgd blijven, gericht toegang te verkrijgen tot versleutelde communicatie van een verdachte in een strafrechtelijk onderzoek. De regering heeft de Tweede Kamer hierover geïnformeerd op 29 augustus 2025.[2] Het is op dit moment nog moeilijk te zeggen wat de uitkomsten daarvan zullen zijn en of dit een oplossing gaat bieden voor het geschetste probleem.

Deze leden merken op dat het onderscheid tussen 'opgeslagen gegevens' en 'real-time gegevens' technisch gezien anno 2026 kunstmatig is geworden en dat onder de Amerikaanse CLOUD-act het bijvoorbeeld wel mogelijk is om vergelijkbare bevelen uit te breiden met onder andere ontsleutelingsbevelen en het onderscheppen van real-time dataverkeer. Wil de regering zich hier in EU-verband voor inzetten dat er uiterlijk bij de eerste evaluatie van de Verordening een voorstel wordt ingediend om de Verordening uit te breiden naar real-time interceptie en ontsleuteling, om te voorkomen dat de handhavingskloof tussen de opsporingsdiensten in de Verenigde Staten en de EU te groot wordt? Deze leden vragen of de regering in dit verband het belang erkent van de aanpak van de georganiseerde grensoverschrijdende misdaad en of de regering uitgebreid

[2] Zie bijlage 3 bij Kamerbrief informatievoorziening over nieuwe Commissievoorstellen d.d. 29 augustus 2025 (BNC Fiche: routekaart rechtmatige en effectieve toegang tot data ten behoeve van de opsporing). Zie ook de brief van 15 april jl. betreffende het schriftelijk overleg over het fiche Mededeling Internationale Digitale Strategie (Kamerstukken II 2025/26, nr. 4312).

wil motiveren waarom het toch onwenselijk zou zijn om voor deze uitbreidingen te pleiten.

In de voornoemde brief van 29 augustus 2025 heeft het kabinet aangegeven het belangrijk te vinden, in het kader van de discussie over rechtmatige toegang tot gegevens, dat er heldere Europese regels zijn voor rechtmatige toegang tot digitale gegevens. Opsporingspartners moeten immers hun wettelijke bevoegdheden kunnen uitoefenen, zowel offline als online, om de samenleving en burgers te beschermen. Het technologische landschap is de afgelopen jaren sterk veranderd en de gevolgen daarvan hebben grote impact gehad op de mogelijkheid van de politie om burgers effectief te kunnen beschermen. De politie geeft aan dat, door de wijze waarop versleuteling wordt uitgerold door grote techbedrijven, zij deze bescherming op termijn niet langer kunnen bieden. Geconcludeerd werd dat er een noodzaak bestaat om op Europees niveau gezamenlijk toe te werken naar een stelsel van regels en toezicht voor onder andere grote communicatiediensten. De regering onderkent deze noodzaak. Vanzelfsprekend moet dergelijke regulering vorm krijgen met inachtneming van grondrechten (waaronder privacy en vertrouwelijkheid van communicatie), de jurisprudentie van het EU-Hof en relevante wetgeving inzake gegevensbescherming – en op proportionele en evenwichtige wijze, met betrokkenheid van alle relevante stakeholders. Daarbij is het belangrijk om digitale en nationale veiligheidsrisico's te voorkomen. De regering zal daarbij in Europa blijven uitdragen dat *end-to-end* encryptie niet onmogelijk mag worden gemaakt. In dat kader zal het kabinet het belang benadrukken dat eventuele wetgeving wordt omkleed met sterke waarborgen en transparant toezicht. Gezien het grensoverschrijdende karakter van de onderliggende problematiek is het extra belangrijk dat eventuele oplossingen in gezamenlijkheid met de lidstaten grondig worden uitgewerkt.

De leden van de VVD-fractie constateren dat diverse organisaties vragen hebben gesteld over de problemen die in de praktijk mogelijk ontstaan ten aanzien van de eerbiediging van het verschoningsrecht. Deze leden merken op dat de kring van verschoningsgerechtigden groter is dan in sommige andere lidstaten en dat het verschoningsrecht in Nederland

anders wordt toegepast dan in andere lidstaten. Gegeven de toename van complexiteit van de beoordeling van de mate waarin gegevens vallen onder het Nederlandse verschoningsrecht, stellen deze leden hier nog een aantal vragen over. In Nederland krijgt de rechter-commissaris straks een rol bij de vraag of er bepaalde gegevens bij Europese verstrekkingsbevelen en bewaarbevelen onder het verschoningsrecht vallen. In veel andere lidstaten zal deze beoordeling niet plaatsvinden door een rechter-commissaris. Kan de regering een inschatting geven van het aantal extra beslissingen die straks na inwerkingtreding van de uitvoeringswet moeten worden genomen door een rechter-commissaris? Zijn hun kabinetten hierop ingericht? Wordt hier voldoende extra capaciteit voor vrijgemaakt?

In de memorie van toelichting bij het onderhavige wetsvoorstel is stil gestaan bij het uitvaardigen van e-Evidence bevelen en het eerbiedigen van het verschoningsrecht. De verordening legt de verantwoordelijkheid daarvoor eerst en vooral bij de uitvaardigende justitiële autoriteit (artikel 5, tiende lid, van de verordening). De uitvaardigende autoriteit mag geen Europees verstrekkingsbevel uitvaardigen indien zij van oordeel is dat de gevraagde verkeersgegevens of inhoudelijke gegevens worden beschermd door voorrechten of immuniteiten uit hoofde van het recht van de tenuitvoerleggingsstaat. De uitvaardigende autoriteit dient daarom de reikwijdte van het Europees verstrekkingsbevel of Europees bewaringsbevel – zo nodig na overleg met de bevoegde autoriteit in de lidstaat van tenuitvoerlegging – zodanig te beperken dat de gevraagde gegevens niet worden beschermd door het verschoningsrecht.
Indien de geadresseerde (dienstaanbieder) op basis van de informatie in het certificaat inzake het Europees verstrekkingsbevel of bewaringsbevel van oordeel is dat de tenuitvoerlegging van het bevel onverenigbaar zou kunnen zijn met het verschoningsrecht, moet hij de uitvaardigende autoriteit en de tenuitvoerleggingsautoriteit hiervan in kennis stellen. Aan de hand van de van de geadresseerde of tenuitvoerleggingsautoriteit ontvangen informatie moet de uitvaardigende autoriteit vervolgens beslissen of het bevel moet worden ingetrokken, aangepast of gehandhaafd. Indien het bevel zonder aanpassingen wordt gehandhaafd, kan de

tenuitvoerleggingsautoriteit een beroep doen op een weigeringsgrond.

Van de rechter-commissaris wordt in dit verband geen grote rol verwacht. Zoals in de memorie van toelichting is vermeld, is van een rol van de rechter-commissaris alleen sprake in een zeer specifiek geval, namelijk als toepassing van artikel 5, negende lid, van de verordening aan de orde is. De inschatting is dat deze situatie zich weinig zal voordoen en dan kan passen bij het vermogen van de huidige organisatie.

De leden van de VVD-fractie vragen ook hoe bij de kennisgeving binnen tien dagen, of bij spoed binnen 96 uur, de rechter-commissaris deze toets op verschoningsgerechtigde gegevens kan uitvoeren? Hoe beoordeelt de regering het risico dat bedrijven naar aanleiding van het wetsvoorstel beslissen om hun servers of clouddiensten in Nederland te plaatsen, omdat hier veel meer gegevens onder het verschoningsrecht vallen dan in de meeste andere EU-lidstaten? Onderkent de regering dat het wetsvoorstel in die zin rechtsongelijkheid met zich meebrengt omdat er verschillen ontstaan tussen Nederlandse verschoningsgerechtigden op basis van waar zij fysiek of juridisch hun servers of clouds hebben staan?

Als ik de vraag van deze leden goed begrijp, gaan zij ervan uit dat de rechter-commissaris binnen tien dagen een toets op verschoningsgerechtigde gegevens moet doen. Hier is echter geen sprake van. De termijn van tien dagen is opgenomen in artikel 10 van de e-Evidence verordening en betreft de termijn waarbinnen aan een Europees verstrekkingsbevel uitvoering dient te worden gegeven. Zoals ik hierboven in antwoord op de vraag van deze leden heb aangegeven, moet een uitvaardigende autoriteit de reikwijdte van het verstrekkingsbevel zodanig beperken dat de gevraagde gegevens niet worden beschermd door het verschoningsrecht. Hiertoe kan de uitvaardigende autoriteit zo nodig overleggen met de tenuitvoerleggingsautoriteit. Dit overleg gaat vooraf aan de uitvaardiging van een verstrekkingsbevel. De termijn van tien dagen is dan dus niet gaan lopen. Wordt niettegenstaande het voorgaande een bevel uitgevaardigd dat toch ziet op verschoningsgerechtigde gegevens, dan kan de tenuitvoerleggingsautoriteit een beroep doen op een

weigeringsgrond overeenkomstig de regeling in de verordening. In Nederland is de officier van justitie de tenuitvoerleggingsautoriteit. De rechter-commissaris heeft hierbij geen rol.
In voorkomend geval kan de rechter-commissaris wel uitvaardigende autoriteit zijn (artikel 5.11.2, eerste lid, Sv, zoals voorzien in het onderhavige wetsvoorstel). Verder is een machtiging van de rechter-commissaris vereist indien een Europees verstrekkingsbevel betrekking heeft op verkeersgegevens of inhoudelijke gegevens (artikel 5.11.2, tweede lid, Sv, zoals voorzien in het onderhavige wetsvoorstel). Zoals uit het voorgaande blijkt, moet de uitvaardigende autoriteit voorafgaand aan de uitvaardiging van het bevel de reikwijdte van het verstrekkingsbevel zodanig beperken dat de gevraagde gegevens niet worden beschermd door het verschoningsrecht.

In het WODC-rapport “Internationaal vergelijkend onderzoek professioneel verschoningsrecht”[3] wordt door de opstellers ervan vastgesteld dat uit de inventarisatie van hoe in verschillende jurisdicties wordt omgegaan met het verschoningsrecht, geen enkel systeem naar voren komt dat in algemene zin als *best practice* kan worden aangemerkt. De vergelijking van rechtssystemen laat zien dat Nederland – in vergelijking met de andere rechtssystemen – het verschoningsrecht in het algemeen relatief ruim interpreteert, aldus de onderzoekers. Mij zijn in dit verband echter geen signalen bekend dat bedrijven naar aanleiding van het onderhavige wetsvoorstel zouden beslissen om hun servers of clouddiensten in Nederland te plaatsen en dat dit tot rechtsongelijkheid zou leiden.

De leden van de VVD-fractie constateren dat de effectiviteit van de Verordening voor de Nederlandse opsporing valt of staat met de snelheid en kwaliteit van de kennisgevingsprocedures in andere lidstaten. Kan de regering toelichten hoe zij omgaat met lidstaten die de kennisgevingsplicht uit artikel 8 van de Verordening op een wijze hebben ingericht die minder waarborgen biedt dan de

[3] J.S. Nan, P.A.M. Mevis, N.L. Holvast en P.A.M. Verrest, *Internationaal vergelijkend onderzoek professioneel verschoningsrecht*, Erasmus Universiteit, Rotterdam 2025. Het rapport is aangeboden aan de Tweede Kamer bij brief van 8 december 2025 (Kamerstukken II 2025/26, nr. 29279, nr. 1003).

Nederlandse toets door de rechter-commissaris? Wordt er op EU-niveau gewerkt aan een geharmoniseerde kwaliteitsstandaard voor de autoriteiten die deze kennisgevingen beoordelen, om te voorkomen dat Nederlandse opsporingsonderzoeken vertraging oplopen door willekeur in andere lidstaten?

De verplichting tot kennisgeving, bedoeld in artikel 8 van de e-Evidence verordening, bestaat in het geval dat een Europees verstrekkingsbevel strekt tot het verkrijgen van verkeersgegevens of inhoudelijke gegevens. De verplichting tot kennisgeving rust op de uitvaardigende autoriteit. Op grond van artikel 4, tweede lid, van de verordening kan een Europees verstrekkingsbevel voor het verkrijgen van verkeersgegevens of voor het verkrijgen van inhoudelijke gegevens uitsluitend worden uitgevaardigd door een in de betrokken zaak bevoegde rechter, rechtbank of onderzoeksrechter, dan wel een andere strafrechtelijke onderzoeksautoriteit. In het laatste geval kan het bevel niet worden uitgevaardigd dan nadat het bevel is bekrachtigd door een rechter. Ik heb op dit moment nog geen overzicht van de keuzes die andere lidstaten hebben gemaakt wat betreft het aanwijzen van de bevoegde uitvaardigende autoriteit.
De kennisgeving aan de tenuitvoerleggingsautoriteit geschiedt door het certificaat inzake het Europees verstrekkingsbevel (het CEV) te doen toekomen aan die autoriteit op hetzelfde moment waarop het CEV wordt doorgegeven aan de geadresseerde (dienstaanbieder). In bijlage I van de verordening is het voorgeschreven model opgenomen voor het CEV. Het is aan de professionele deskundigheid van de tenuitvoerleggingsautoriteiten in de verschillende lidstaten om op basis van de informatie in het CEV te beoordelen of een beroep moet worden gedaan op een weigeringsgrond. De tenuitvoerleggingsautoriteit heeft daar tien dagen de tijd voor. Indien de tenuitvoerleggingsautoriteit binnen tien dagen na ontvangst van het CEV geen weigeringsgrond heeft aangevoerd, moet de geadresseerde dienstaanbieder ervoor zorgen dat de gevraagde gegevens rechtstreeks aan de in het CEV vermelde uitvaardigende autoriteit of rechtshandhavingsautoriteiten worden toegezonden.

Omdat voor alle lidstaten op basis van de verordening dezelfde weigeringsgronden en termijnen gelden, heb ik op voorhand geen reden om aan te nemen dat Nederlandse opsporingsonderzoeken vertraging zullen oplopen. Integendeel, de e-Evidence verordening is juist bedoeld als een doeltreffender mechanisme om elektronisch bewijsmateriaal te verkrijgen waarbij als uitgangspunt geldt dat dienstaanbieders verplicht zijn om direct te reageren op bevelen van autoriteiten in een andere lidstaat.
Artikel 33 van de verordening schrijft voor dat de toepassing van de verordening en de daarmee bereikte resultaten worden geëvalueerd. Op basis van die evaluatie zal kunnen blijken of de verordening het beoogde doel heeft bereikt.

De leden van de VVD-fractie vragen of zowel de overheid als de telecomaanbieders in Nederland voldoende in staat zijn en worden gesteld om tijdig systemen te bouwen of aan te passen om het wetsvoorstel uit te voeren. Voor zover deze leden kunnen overzien, zijn er tot nu toe te weinig technische specificaties verstrekt om alle dienstaanbieders in staat te stellen dit te doen. Graag ontvangen deze leden een reactie hierop van de regering en ook een overzicht van de overleggen en inbreng die er zijn geweest vanuit de dienstaanbieders. In het verlengde hiervan vragen zij of er is voorzien in een adequaat implementatieprogramma en op welke wijze aanbieders worden geïnformeerd over de uitvoering van het wetsvoorstel. Welke rol ziet de regering om aanbieders voor te lichten over niet alleen de uitvoeringswet maar ook de adequate toepassing ervan? Is de regering bijvoorbeeld voornemens een handreiking op te stellen voor de aanbieders?

In het hierboven gegeven antwoord op vragen van de leden van de D66-fractie ben ik ingegaan op het ontbreken van belangrijke technische afspraken en duidelijke procesbeschrijvingen. Ik heb aangegeven dat ik deze punten herken en op onderdelen erken. Duidelijk is dat dat de bedrijven maar ook Nederlandse overheid vanwege de complexe en uit de planning gelopen voorbereidingen voor het in werking krijgen van het EU gedecentraliseerd IT-systeem te laat kunnen beschikken over specificaties die het mogelijk maken dat de Nederlandse overheid bedrijven toegang kan verlenen tot een werkend IT systeem. De

bedrijven hebben een redelijke termijn nodig om hun eigen bedrijfsprocessen zodanig in te richten dat zij met behulp van het IT systeem bevelen kunnen ontvangen en behandelen. Pas sinds enkele maanden is duidelijk dat de beschikbare termijn in redelijkheid niet meer kan worden gehaald.
Er wordt gewerkt aan een evenwichtig implementatieplan en er is structureel overleg met de Europese Commissie.

De leden van de GroenLinks-PvdA-fractie lezen dat omdat het wetsvoorstel over implementatie van het EU-recht gaat consultatie niet voorgeschreven was. Wel heeft de regering over het concept van de voorliggende uitvoeringswet het OM, de Raad voor de rechtspraak, de politie en de ACM om commentaar heeft gevraagd. De aan het woord zijnde leden zouden het op prijs stellen indien de regering ook de Nederlandse Orde van Advocaten en de Autoriteit Persoonsgegevens om commentaar zou vragen. Is de regering daartoe bereid en zouden die commentaren uiterlijk tegelijkertijd met de nota naar aanleiding van het verslag aan de Kamer kunnen worden gestuurd?

Bij de verplichte implementatie van EU-regelgeving is het uitgangspunt dat over het ontwerp van een implementatieregeling geen advies wordt gevraagd of extern overleg wordt gevoerd (Aanwijzing 9.16, tweede lid, van de Aanwijzingen voor de regelgeving). Aan het College van procureurs-generaal van het Openbaar Ministerie, de Raad voor de rechtspraak, de politie en de Autoriteit Consument en Markt is gevraagd om een reactie op het wetsvoorstel met het oog op het vaststellen van eventuele uitvoeringsgevolgen. Nu het wetsvoorstel dient ter verplichte implementatie van het e-Evidence pakket van de EU en het voorstel ook daartoe is beperkt, is er geen aanleiding om het wetsvoorstel voor commentaar voor te leggen aan de Nederlandse Orde van Advocaten en de Autoriteit Persoonsgegevens.

De leden van de CDA-fractie lezen dat het OM opmerkt te veronderstellen dat de bevoegdheid van de officier van justitie tot de uitvaardiging van een Europees verstrekkingsbevel of Europees bewaringsbevel ruimte laat voor de voorbereiding door de opsporingsambtenaar. De regering geeft aan dat wordt beoogd dat de officier van justitie de beslissing neemt en de verantwoordelijkheid

draagt over de uitoefening van de bevoegdheid, maar dat vereist niet dat de officier van justitie deze eigenhandig opstelt. Deze leden vragen of het feitelijk wel mogelijk is dat de officier van justitie het bevel opstelt, of dat dit in de praktijk altijd een opsporingsambtenaar zal zijn. En zo ja, wat houdt dit in voor de toename van de werklast voor de politie?

In de werkprocessen die zijn en worden ontwikkeld, stelt in zeer algemene termen geformuleerd de politie het bevel op en doet het OM een juridische toets en ondertekent het bevel. In de gemaakte impactanalyse is daarom voor zogenoemde uitgaande bevelen ook belasting bij de politie meegenomen. Werklast aan de inkomende kant verdwijnt echter bij de politie. Niettemin herijken politie en OM op basis van de laatste inzichten van de wenselijke toekomstige werkprocessen de gemaakte inschattingen van de werklast. De uitkomsten van deze herijking heb ik nog niet ontvangen.

De leden van de CDA-fractie lezen dat de politie en het OM de vraag stellen of het niet wenselijk is om ook de opsporingsambtenaar als bevoegde autoriteit aan te wijzen omdat dit behulpzaam kan zijn in noodsituaties. De regering antwoordt hierop dat dit niet voor de hand ligt omdat het Europees verstrekkingsbevel en bewaringsbevel instrumenten zijn in het kader van de justitiële samenwerking in strafzaken tussen bevoegde autoriteiten, en dat dit het domein is van de officier van justitie. Deze leden vragen of andere lidstaten de opsporingsambtenaar wel hebben aangewezen als bevoegde autoriteit, nu de lidstaten de vrijheid hebben om zelf een autoriteit aan te wijzen.

Het is de regering niet bekend dat andere lidstaten opsporingsambtenaren hebben aangewezen als bevoegde autoriteit. Ik wijs er in dit verband op dat de e-Evidence verordening wel regels geeft voor het aanwijzen van een bevoegde autoriteit (artikel 4). Zo kan een autoriteit die in de betrokken zaak optreedt als strafrechtelijke onderzoeksautoriteit en overeenkomstig het nationale recht bevoegd is opdracht te geven tot het vergaren van bewijsmateriaal wel worden aangewezen als uitvaardigende autoriteit, maar moet een verstrekkingsbevel van die autoriteit wel worden bekrachtigd door een rechter, rechtbank, onderzoeksrechter of openbare aanklager in de

uitvaardigende lidstaat of, in het geval van het bevel strekt tot het verkrijgen van verkeersgegevens of inhoudelijke gegevens, door een rechter, rechtbank of onderzoeksrechter in de uitvaardigende lidstaat.

Daarnaast lezen de leden van de CDA-fractie dat de Verordening uitsluitend ziet op strafzaken en daarom niet kan worden toegepast bij urgente persoonsvermissingen zonder verdenking van een strafbaar feit. Deze leden vragen de regering of zij, juist in situaties waarin bij een vermissing wél sprake is van een verdenking van een strafbaar feit en snelheid cruciaal is, mogelijkheden ziet om opsporingsambtenaren een duidelijkere rol te geven in het proces rond het Europees verstrekkings- of bewaringsbevel.

In situaties waarin bij een vermissing wél sprake is van een verdenking van een strafbaar feit kan de verordening worden toegepast. Zoals aangegeven in de memorie van toelichting bij het onderhavige wetsvoorstel laat de bevoegdheid van de officier van justitie tot het uitvaardigen van een Europees verstrekkingsbevel of Europees bewaringsbevel ruimte voor de voorbereiding van zo'n bevel door een opsporingsambtenaar. Dat is ook staande praktijk bij de uitoefening van de bevoegdheden die de officier van justitie heeft op grond van het Wetboek van Strafvordering. Indien de situatie daarom vraagt, kunnen de officier van justitie en de opsporingsambtenaar ook snel in actie komen. Zo nodig kan in een aanwijzing van het Openbaar Ministerie worden voorzien in een werkwijze in geval van spoed.

De leden van de CDA-fractie vragen aan de regering wat het wetstraject rondom de modernisering van het Wetboek van Strafvordering betekent voor onderhavige wet, nu er verschillende verwijzingen zijn opgenomen naar artikelen uit dat betreffende wetboek.

Vanwege de Europeesrechtelijk voorgeschreven termijnen kan niet worden volstaan met de uitvoering en implementatie van de e-Evidence verordening en richtlijn in het nieuwe Wetboek van Strafvordering, dat niet eerder dan 1 april 2029 in werking zal treden. Daarom voorziet het onderhavige wetsvoorstel in wijziging van het huidige Wetboek van Strafvordering. Door middel van de invoeringswet voor het

nieuwe Wetboek van Strafvordering zal de regeling in het onderhavige wetsvoorstel beleidsneutraal worden overgezet naar het nieuwe wetboek.

8. Overgangsrecht en inwerkingtreding

De leden van de D66-fractie hebben vernomen dat vanuit de telecom- en internetaanbieders in Nederland grote zorgen zijn geuit over de implementatie van de wet in augustus 2026. Hoe is de regering van plan de zorgen voor de beoogde inwerkingtreding weg te nemen? En indien dat niet lukt, welk tijdspad ziet de regering voor zich om openstaande vragen en zorgen over de implementatie van de wet weg te nemen?

In het hierboven gegeven antwoord op vragen van de leden van de D66-fractie ben ik ingegaan op het ontbreken van belangrijke technische afspraken en duidelijke procesbeschrijvingen. Ik heb aangegeven dat ik deze punten herken en op onderdelen erken. De zorgen van de industrie trek ik mij aan. Via voorlichtings- en expertsessies, alsook in bilateraal contact, stel ik de informatie zoals ik die heb ter beschikking. Daarnaast heeft mijn ministerie ook een specifieke webpagina gecreëerd waarop allerhande informatie is terug te vinden (https://www.eevidence.nl/). Mede op basis van hetgeen in overleg met de Europese Commissie en andere lidstaten nader en concreter kan worden besloten over een mogelijke gefaseerde invoering van e-Evidence zal ik het communicatieproces met de industrie intensiveren.

De leden van de CDA-fractie constateren dat de implementatiedeadline van 18 februari 2026 niet is gehaald. Wat zijn hiervan de consequenties en lopen andere lidstaten ook achter op schema? Is de regering van mening dat de deadline van 18 augustus 2026, waarop de Verordening in werking treedt en rechtstreeks werkt, wel wordt gehaald?

Uit informele overleggen in EU-verband blijkt inderdaad dat meerdere lidstaten de deadline niet hebben gehaald, en ook de deadline van 18 augustus a.s. naar verwachting niet zullen halen. Nederland heeft in maart 2026 een brief van de Europese Commissie ontvangen waarin gevraagd is om het

niet halen van de deadline uit te leggen. Eind mei zal de regering deze brief beantwoorden.
De deadline van februari 2026 is in de praktijk op dit moment vooral relevant voor het aanwijzen van een geadresseerde door dienstaanbieders die in Nederland zullen worden geregistreerd. Zoals in de memorie van toelichting is aangegeven, is afgesproken met de Europese Commissie dat dienstaanbieders hun registratie kunnen indienen bij een centraal punt van de Europese Commissie. Het kabinet beziet op dit moment of er mogelijkheden zijn om, vooruitlopend op inwerkingtreding van het wetsvoorstel, vanuit Nederland dit proces niet te vertragen.

II ARTIKELSGEWIJS

Artikel 8 (bestuurlijke boete)
De leden van de VVD-fractie constateren dat artikel 7 de grondslag biedt voor de ACM een last onder dwangsom op te leggen en dat artikel 8 de grondslag biedt voor oplegging van een bestuurlijke boete. Deze leden vragen of de opbrengst van de lasten onder dwangsom en bestuurlijke boetes toe komt aan de ACM conform de algemene regeling in de Algemene wet bestuursrecht in de artikelen 5:10, eerste lid jo. 1:1, vierde lid. Kan de regering bevestigen dat bedoeld is dat de opbrengsten van de sancties integraal terugvloeien naar de algemene middelen? Ook vragen deze leden of de ACM bij het vaststellen van de hoogte van de last onder dwangsom en bestuurlijke boetes rekening houdt met de grootte van het bedrijf. Deze leden vinden het in dat licht redelijk dat een last onder dwangsom of een boete in verhouding staat tot de gevolgen voor het bedrijf. Iemand uit het midden- en kleinbedrijf (mkb) zal eerder failliet worden verklaard na oplegging van een boete dan een grote onderneming met duizenden werknemers. Kan de regering hierop reageren?

Op grond van artikel 6a, tiende lid, van de Instellingswet Autoriteit Consument en Markt komt, indien een door de Autoriteit Consument en Markt een verplichting tot betaling van een geldsom is opgelegd, deze geldsom toe aan de Staat der Nederlanden.
Voor zowel het vaststellen van de hoogte van de dwangsom als van de bestuurlijke boete geldt dat rekening kan worden

gehouden met de grootte van een bedrijf. Dat vloeit voort uit de artikelen 7 en 8 van het onderhavige wetsvoorstel waarin de maximale hoogte van een dwangsom en bestuurlijke boete is bepaald. Indien de in die artikelen genoemde zesde categorie van bedragen, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht geen passende dwangsom of boete toelaat, kan een dwangsom of boete worden opgelegd van ten hoogste tien procent van de jaaromzet van de dienstaanbieder in het boekjaar voorafgaande aan de beschikking waarin de last onder dwangsom of bestuurlijke boete is opgelegd.
Ik wijs in dit verband ook naar de boetebeleidsregels die de ACM heeft opgesteld en die te raadplegen zijn via wetten.nl.

De Minister van Justitie en Veiligheid,
D.M. van Weel