

Vergaderjaar 2024–2025

22 112

Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4116

BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 augustus 2025

Overeenkomstig de bestaande afspraken ontvangt u hierbij 5 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Wijziging EU-klimaatwet (EU-klimaatdoelstelling 2040) (Kamerstuk 22 112, nr. 4114)

Fiche: Omnibus VI – vereenvoudiging eisen en procedures chemische producten (Kamerstuk 22 112, nr. 4115)

Fiche: Routekaart rechtmatige en effectieve toegang tot data ten behoeve van de opsporing

Fiche: Verordening voor de EU Space Act (Kamerstuk 22 112, nr. 4117)

Fiche: Mededeling over a Vision for the European Space Economy (Kamerstuk 22 112, nr. 4118)

De Minister van Buitenlandse Zaken,
R.P. Brekelmans

Fiche: Routekaart rechtmatige en effectieve toegang tot data ten behoeve van de opsporing

1. Algemene gegevens

- a) *Titel voorstel*
Communication: Roadmap for lawful and effective access to data for law enforcement
- b) *Datum ontvangst Commissiedocument*
juni 2025
- c) *Nr. Commissiedocument*
COM(2025) 349
- d) *EUR-Lex*
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0349>
- e) *Nr. impact assessment Commissie en Opinie*
Niet van toepassing
- f) *Behandelingstraject Raad*
Nog onbekend
- g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid

2. Essentie mededeling

De Europese Commissie (hierna: Commissie) heeft op 24 juni jl. de mededeling «*Roadmap for lawful and effective access to data for law enforcement*» uitgebracht. De Commissie reageert hiermee op de oproep van de JBZ-Raad in december 2024¹ om in het tweede kwartaal van 2025 met een routekaart te komen met betrekking tot de aanbevelingen van de *High Level Group on access to data* (hierna: HLG). In juni 2023 is onder het Zweedse voorzitterschap de HLG opgericht ten behoeve van de effectieve rechtshandhaving. De HLG had als doel om met experts vanuit heel Europa problemen in kaart te brengen en tot oplossingsrichtingen te komen voor de uitdagingen die rechtshandhavingpartners ervaren bij het verkrijgen van digitale gegevens voor opsporing. De belangrijkste thema's waar de HLG zich op richtte betroffen dataretentie en versleuteling.²

Op het gebied van dataretentie geeft de Commissie aan dat sinds het *Digital Rights Ireland* arrest van het Hof van Justitie van de Europese Unie (hierna: EU-Hof) uit 2014,³ op basis waarvan de EU-richtlijn inzake gegevensbewaring in 2014 ongeldig is verklaard, het EU-wetgevingslandschap met betrekking tot de verplichting voor dienstverleners om gegevens te bewaren sterk gefragmenteerd is geraakt. De kaders voor gegevensbewaring van de lidstaten lopen sterk uiteen voor wat betreft de soorten elektronische data die dienstverleners moeten bewaren, de categorieën gegevens die deze bestrijken en de duur van de vereiste bewaartermijnen. Rechtshandavings- en gerechtelijke autoriteiten worden geconfronteerd met juridische en operationele obstakels bij het uitvoeren van hun werkzaamheden. Daarnaast worden aanbieders van elektronische communicatie, met name kleinere aanbieders, geconfronteerd met extra kosten en obstakels bij het aanbieden van hun diensten in de hele EU, omdat zij moeten voldoen aan verschillende wettelijke vereisten in verschillende lidstaten. In lijn met de aanbevelingen van de HLG om dataretentie-wetgeving in Europa te harmoniseren, kondigt de Commissie een impact assessment aan waarin zij gaat onderzoeken of, en

¹ Zie Raadsconclusies d.d. 12 december 2024 (no. 16448/24) «Council conclusions on access to data for effective law enforcement».

² Zie o.a. Kamerstuk 32 317, nr. 879, pp. 15–16.

³ HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland).

zo ja, welke nieuwe wet- en/of regelgeving nodig is op het gebied van dataretentie.

Met betrekking tot de interceptiebevoegdheid van rechtshandavingsautoriteiten wil de Commissie, conform de aanbevelingen van de HLG, maatregelen onderzoeken om de efficiëntie van rechtshulpverzoeken via bestaande instrumenten te verbeteren en waar nodig te versterken, waaronder het Europees onderzoeksbevel. Ook wil de Commissie, in lijn met de aanbevelingen van de HLG, maatregelen verkennen om een meer gelijk speelveld te creëren voor communicatieaanbieders vis-a-vis de rechtshandhaving. Daarbij zal de Commissie bezien wat de meest efficiënte aanpak zou zijn in de omgang met niet-coöperatieve communicatieaanbieders. Ook zal de Commissie mogelijkheden onderzoeken om de inzet van beveiligde capaciteiten voor informatie-uitwisseling tussen lidstaten, Europol en andere veiligheidsdiensten te ondersteunen. Tenslotte reageert de Commissie op het advies van de HLG om een technologische routekaart te ontwikkelen om, waar nodig, gerichte rechtmatige toegang tot versleutelde informatie mogelijk te maken, waarbij *cybersecurity* en de bescherming van grondrechten gewaarborgd blijven. De Commissie kondigt aan een deskundigengroep te organiseren en faciliteren en verwacht deze technologische routekaart op te kunnen leveren in het tweede kwartaal van 2026.

Betreffende digitale forensische toepassingen en standaardisatie geeft de Commissie aan, conform de aanbevelingen van de HLG, dat zij de komende jaren zal werken aan een meer gecoördineerde EU-aanpak voor standaardisatie op het gebied van interne veiligheid en handhavingsautoriteiten meer wil ondersteunen bij de (meer) gezamenlijke ontwikkeling van digitale forensische toepassingen. De Commissie benoemt dat standaarden essentieel zijn in digitale communicatie en zorgen voor interoperabiliteit tussen systemen en apparaten die door technologieleveranciers zijn ontwikkeld. Daarnaast faciliteren standaarden de naleving van wettelijke verplichtingen door technologieën, waaronder rechtmatige toegang voor wetshandavingsdoeleinden.

De Commissie benoemt in relatie tot decryptie van gegevens ten behoeve van (grote) strafzaken dat het decryptieplatform van Europol zijn nut heeft bewezen bij de ondersteuning van belangrijke strafzaken, waaronder die in de Sky-ECC en EncroChat-zaken. De Commissie bepleit dat verbeterde decryptiecapaciteiten nodig zijn om ervoor te zorgen dat rechtshandhavingautoriteiten de capaciteit hebben om steeds complexere algoritmen te ontsleutelen. De HLG heeft aanbevolen om de financiering te verhogen ter ondersteuning van innovatie op het gebied van datatoegang bij (grote) strafzaken. Als reactie hierop geeft de Commissie aan het onderzoek naar en de ontwikkeling van nieuwe decryptiecapaciteiten te ondersteunen om ervoor te zorgen dat Europol na 2030 goed is toegerust om de lidstaten te ondersteunen, in het licht van nieuwe technologische ontwikkelingen op dit gebied.

De Commissie kondigt verschillende acties aan die zij zal ondernemen op het gebied van AI. Ten eerste: het stimuleren van innovatie voor AI-oplossingen voor het filteren en analyseren van digitaal bewijsmateriaal, door zowel de ontwikkeling van nieuwe tools als de verbetering van bestaande toepassingen te ondersteunen. Hierbij dient gebruik te worden

gemaakt van de *AI regulatory sandboxes*⁴ zoals voorzien in de AI-verordening, voor veilige ontwikkeling, testen en evaluatie. Verder stelt de Commissie voor om een gestructureerde dialoog met wetshandhavingsinstanties en andere relevante stakeholders aan te gaan om operationele behoeften en uitdagingen te identificeren, voortbouwend op het werk van de *Innovation Lab* van Europol en de *EU Innovation Hub for Internal Security* (die door Europol wordt gehost).⁵ Ook kondigt de Commissie aan de ontwikkeling van duidelijke en praktische richtsnoeren voor rechtmatig, ethisch en doeltreffend gebruik van AI in de rechtshandhaving te ondersteunen, met inachtneming van grondrechten en het juridische kader. Tot slot: het ondersteunen en financieren van proefprojecten gericht op de ontwikkeling, training en validering van juridisch conforme en technisch betrouwbare AI-toepassingen voor digitaal forensisch onderzoek, data-analyse en andere onderzoeksinstrumenten voor rechtshandhaving.

3. Nederlandse positie ten aanzien van de mededeling

a) Essentie Nederlands beleid op dit terrein

Het kabinet acht het belangrijk, in het kader van de discussie over rechtmatige toegang tot gegevens, dat er heldere Europese regels zijn voor rechtmatige toegang tot digitale gegevens.⁶ Opsporingspartners moeten immers hun wettelijke bevoegdheden kunnen uitoefenen, zowel *offline* als *online*, om onze samenlevingen 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.⁷ Een van de belangrijke aanbevelingen van de HLG betreft dan ook de noodzaak om op Europees niveau gezamenlijk toe te werken naar een stelsel van regels en toezicht voor o.a. grote communicatiediensten. Het kabinet 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. Het kabinet zal daarbij in Europa blijven uitdragen dat end-to-end encryptie niet onmogelijk mag worden gemaakt⁸ en het kabinetsstandpunt in acht nemen.⁹ In dat kader zal het kabinet het belang benadrukken dat eventuele wetgeving wordt omkleed met sterke waarborgen en transparant toezicht.

⁴ Regulatory sandboxes zijn gecontroleerde omgevingen («proeftuinen») waarbinnen AI systemen ontwikkeld, getest en gevalideerd kunnen worden, met betrokkenheid van toezicht-houders, voordat publicatie op de markt plaatsvindt. Het doel van sandboxes is om innovatie te bevorderen en risico's tijdig te identificeren en mitigeren, met name op het gebied van veiligheid en grondrechten.

⁵ De «EU Innovation Hub on Internal Security» betreft een Europees netwerk van innovatielabs gericht op coördinatie en samenwerking op innovatie tussen actoren die bezighouden interne veiligheid in de EU (o.a. rechtshandhaving, justitie, grondrechten, grensbeveiliging, immigratie, douane).

⁶ Zie o.a. geannoteerde agenda van de informele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 13 en 14 juni 2024, p. 7.

⁷ Beantwoording van Kamervragen d.d. 24 oktober 2024, (Aanhangsel Handelingen II 2024/25, nr. 398, p. 1).

⁸ Uitvoering van de motie van het lid Van Raan c.s. over end-to-endencryptie in stand houden (Kamerstuk 26 643, nr. 885)

⁹ Kabinetsstandpunt encryptie (Kamerstuk 26 643, nr. 383)

Gezien het grensoverschrijdende karakter van de onderliggende problematiek is het extra belangrijk dat eventuele oplossingen in gezamenlijkheid met de lidstaten grondig worden uitgewerkt.

Alvorens in te gaan op de voorgenomen stappen die de Commissie heeft aangekondigd in de mededeling kan worden opgemerkt dat alle voorstellen die de Commissie aandraagt direct voortvloeien uit de aanbevelingen van de HLG. Derhalve is het belangrijk om te benoemen welk standpunt Nederland heeft uitgedragen met betrekking tot het werk van dit gremium.

In 2023 en 2024 zijn de onder de HLG hangende expertgroepen bijeengekomen. De expertgroepen bestonden veelal uit ervaren experts vanuit de uitvoeringspartners, zoals politie en OM. Nederland heeft aan alle werkgroepen deelgenomen.¹⁰

Veel lidstaten, waaronder Nederland, hebben het werk en de aanbevelingen van de HLG verwelkomd en gesteund tijdens de JBZ-Raden van zowel juni als juli 2024.¹¹ Op 18 november is het definitieve rapport van de HLG gepresenteerd, met aanbevelingen met betrekking tot knelpunten en mogelijke oplossingen op drie deelonderwerpen: digitale opsporing, dataretentie en toegang tot data. Tijdens de JBZ-Raad van 12 en 13 december hebben de lidstaten, waaronder Nederland, hun brede steun uitgesproken voor het eindrapport van de HLG en heeft de JBZ-Raad Raadsconclusies aangenomen. Met deze Raadsconclusies worden de HLG conclusies onderschreven en werd de Commissie opgeroepen om een routekaart te presenteren waarin deze conclusies concreet worden uitgewerkt.¹²

b) Beoordeling en inzet ten aanzien van dit voorstel

Het kabinet verwelkomt de routekaart en ondersteunt het doel en de algemene strekking van de stappen die de Commissie zal ondernemen, waarbij het van belang is gedegen, prudente en concrete stappen te nemen. Hiermee herhaalt het kabinet het standpunt dat eerder uitgedragen is tijdens de JBZ-raad.

Op het gebied van dataretentie acht het kabinet geharmoniseerde dataretentie regelgeving nodig, gezien de sterk uiteenlopende wetgeving in de lidstaten, om de door de Commissie en HLG genoemde rechtsongelijkheid die is ontstaan in het beschermingsniveau van EU-burgers en bedrijven aan te pakken en de retentie van gegevens ten behoeve van de strafrechtspleging onder strenge voorwaarden mogelijk te maken. Gezien het feit dat gegevens vaak buiten de landsgrenzen worden opgeslagen is het belangrijk dat regelgeving omtrent het bewaren van die gegevens gelijk is (en indien noodzakelijk beschikbaar is op basis van een gerechtelijke vordering) in de lidstaten. Daarnaast is het belangrijk dat regels in de EU omtrent de wijze waarop data worden opgeslagen beter op elkaar aansluiten. Dat zorgt niet alleen voor duidelijkheid, maar ook voor betere kwaliteit en beschikbaarheid van data. Het kabinet vindt het positief dat de Commissie een impact assessment gaat uitvoeren op dit terrein.

¹⁰ Zie o.a. Kamerstuk 32 317, nr. 879, pp. 15–16; Verslag van de bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 12 en 13 juni 2025, p. 6.

¹¹ Verslag van de formele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 13 en 14 juni 2024, p. 3; Verslag van de informele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 22 en 23 juli 2024 te Boedapest, p. 2.

¹² Verslag van de formele bijeenkomst van de Raad Justitie en Binnenlandse Zaken, 12 en 13 december 2024, p. 7.

Het kabinet heeft vaak bepleit dat het instrument van de «*impact assessment*» een noodzakelijk onderdeel zou moeten uitmaken van besluitvorming omtrent nieuwe EU wet- en regelgeving. Hoewel het kabinet voorstander is van geharmoniseerde dataretentie wet- en regelgeving, is het belangrijk dat de noodzaak en vormgeving van dergelijke wetgeving deugdelijk wordt getoetst en onderbouwd. Een *impact assessment* is hiervoor bij uitstek het meest geschikte middel. Het kabinet kan zich derhalve positief uitspreken ten aanzien van deze voorgenomen stap. Uiteraard zal, in lijn met de daartoe strekkende HLG-aanbevelingen, eventuele dataretentiewetgeving in lijn moeten zijn met grondrechten en de jurisprudentie van het Europees Hof van Justitie.¹³

Betreffende interceptiebevoegheden onderstreept het kabinet in algemene zin dat opsporingspartners hun wettelijke bevoegdheden moeten kunnen uitoefenen, zowel offline als online, om onze samenlevingen en burgers te beschermen. Het kabinet ondersteunt het voornemen van de Commissie om de onderlinge samenwerking tussen rechtshandhavinginstanties te verbeteren alsmede middelen en instrumenten, waaronder het Europees onderzoeksbevel, te verbeteren en te versterken. Echter, omdat nog niet wordt aangekondigd op welke wijze de Commissie dit wil bewerkstelligen, kan daarover op dit moment inhoudelijk weinig worden opgemerkt. Ook kondigt de Commissie, conform de aanbevelingen van de HLG, aan dat zij een technologische routekaart zal uitwerken. Hiermee zal, waar nodig, de mogelijkheid en haalbaarheid worden onderzocht van gerichte rechtmatige toegang tot versleutelde informatie, waarbij *cybersecurity* en de bescherming van grondrechten gewaarborgd blijven. De HLG adviseerde een voorzichtige aanpak te hanteren bij het ontwerpen van oplossingen voor rechtmatige toegang tot systemen. De industrie mag niet worden gevraagd systemen te integreren die de encryptie op een algemene of systematische manier voor alle gebruikers van een dienst kunnen verzwakken. Rechtmatige toegang tot gegevens moet gericht blijven en beperkt blijven tot specifieke communicatie, van geval tot geval. Het kabinet onderschrijft de noodzaak dat de technische haalbaarheid van dergelijke maatregelen grondig wordt onderzocht. Er moet worden voorkomen dat enige verplichting in het leven wordt geroepen die, in de praktijk, schadelijk zou uitpakken voor de cybersecurity van burgers en bedrijven, danwel de bescherming van privacy en andere grondrechten onvoldoende zou waarborgen. Ook in het kader van de beoordeling van de proportionaliteit en subsidiariteit van eventuele nieuwe regelgeving is een dergelijke analyse noodzakelijk. Het kabinet acht het essentieel dat de aangekondigde technologische routekaart deugdelijk wordt uitgewerkt. Daarbij mag niet uit het oog worden verloren dat zonder effectieve opsporingsbevoegdheden de politie, onder leiding van het OM, burgers niet effectief kan beschermen en dat het vinden van concrete oplossingen hard nodig is.¹⁴

Tenslotte zal de Commissie bezien, conform de daartoe strekkende HLG aanbevelingen, of en hoe een gelijk speelveld kan worden bewerkstelligd tussen de aanbieders van communicatiediensten ten aanzien van rechtshandhavinginstanties. Op dit moment zijn telecomaانبieders aan een stelsel van wettelijke regels en toezicht gebonden,¹⁵ terwijl voor andere communicatiediensten juist weinig of geen regels gelden en zij

¹³ Zie o.a. HvJ EU 8 april 2014, nrs. C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland).

¹⁴ Zie tevens Beantwoording van Kamervragen d.d. 24 oktober 2024, (Aanhangsel Handelingen II 2024/25, nr. 398, p. 1).

¹⁵ In Nederland is dit met name op basis van de verplichtingen die voortvloeien uit hoofdstuk 13 van de Telecommunicatiewet.

niet onderhevig zijn aan enige (of een vergelijkbare) vorm van toezicht. Dat is, ook vanuit het concurrerend vermogen bezien, op zichzelf een onwenselijke situatie. Het kabinet steunt daarom dit voornemen van de Commissie. De Commissie onderzoekt nog hoe een gelijk speelveld kan worden bewerkstelligd. Het kabinet zal kritisch meekijken naar eventuele maatregelen die voortvloeien uit dit voornemen van de Commissie. Gezien de onderlinge samenhang is het te verwachten dat eventuele maatregelen pas kunnen worden uitgewerkt wanneer de tevens aangekondigde technologische routekaart deugdelijk is uitgewerkt.

Het kabinet steunt initiatieven met betrekking tot het stimuleren van innovatie van AI binnen het rechtshandavingsdomein, wanneer zij binnen de reikwijdte van de AI-verordening en andere relevante (EU-)wetgeving worden uitgevoerd. De inzet van het kabinet is om via onder andere de *subgroup Law Enforcement and Security* van het *AI Office*, de Commissie te voorzien van input om zo tot duidelijke en praktische richtsnoeren te komen.

Proefprojecten ten aanzien van de ontwikkeling, training en validering kunnen worden ondersteund door het kabinet wanneer deze levensvatbaar zijn en leiden tot een bruikbare en praktische toepassing. AI is onmisbaar om snel en gericht te zoeken in gegevens, maar moet betrouwbaar, transparant en wettelijk geborgd zijn. Daarom is het goed om proefprojecten uit te voeren binnen zogenaamde «*AI Sandboxes*» – veilige testomgevingen. Het gebruik van gestandaardiseerde dataformaten is daarbij belangrijk.

De aangekondigde stappen van praktische aard vloeien direct voort uit de aanbevelingen van de HLG, zoals de ontwikkeling van forensische digitale toepassingen, de ondersteuning van faciliteiten bij Europol die de ontsleuteling van data in grote strafrechtelijke onderzoeken mogelijk maken en de bevordering van een (meer) gecoördineerde betrokkenheid van rechtshandavingsinstanties (alsmede de benodigde training daartoe) bij de ontwikkeling van technische standaarden. Het kabinet verwacht dat deze maatregelen een praktische bijdrage kunnen leveren aan een verbeterde toegang tot data ten behoeve van de opsporing en kan deze stappen ondersteunen.

c) Eerste inschatting van krachtenveld

Naar verwachting wordt de routekaart in algemene zin breed ondersteund door de EU-lidstaten. Alle voorgenomen stappen die de Commissie heeft aangekondigd in de «*Roadmap on lawful and effective access to data*» volgen uit de aanbevelingen van de HLG. Deze aanbevelingen worden breed ondersteund door de lidstaten, waaronder door Nederland. De positie van het Europees parlement is nog niet bekend.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

De grondhouding van het kabinet is positief. Het betreft een mededeling, waarin verschillende voorstellen worden aangekondigd die vooral betrekking hebben op verschillende beleidsterreinen, zoals de ruimte van vrijheid, veiligheid en recht en werking van de interne markt. Op deze terreinen is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, lid 2, sub a, sub f, sub j, VWEU). Daarnaast heeft de mededeling betrekking op het terrein van onderzoek en technologische

ontwikkeling. Dit betreft een parallelle bevoegdheid tussen de EU en lidstaten (artikel 4, lid 3 VWEU).

b) Subsidiariteit

De grondhouding ten aanzien van de subsidiariteit is positief. De mededeling heeft tot doel via een voorstel tot een strategie en aangekondigde initiatieven bij te dragen aan een effectieve en gemeenschappelijke aanpak van lidstaten tegen (georganiseerde) criminaliteit en factoren die criminaliteit in de hand werken.¹⁶ Gezien de grensoverschrijdende aard van veel vormen van criminaliteit en de sterk uiteenlopende dataretentie wet- en regelgeving wetgeving op nationaal niveau, kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Daarom is een EU-aanpak nodig. Gelet op deze grensoverschrijdende aard van (georganiseerde) criminaliteit, samen met de internationale dimensies van de wijze waarop burgers met elkaar communiceren, kan (georganiseerde) criminaliteit het beste worden bestreden door een multidisciplinaire Uniebrede aanpak.¹⁷ Om die redenen is optreden op het niveau van de Unie gerechtvaardigd.

c) Proportionaliteit

De grondhouding ten aanzien van de proportionaliteit is positief. De mededeling heeft tot doel via een voorstel tot een strategie en aangekondigde initiatieven bij te dragen aan een effectieve en gemeenschappelijke aanpak van lidstaten tegen (georganiseerde) criminaliteit en factoren die criminaliteit in de hand werken. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, omdat de verscheidene beschreven maatregelen omtrent dataretentie en een gemeenschappelijke aanpak voor rechtshandhavend optreden in het digitale domein wezenlijk zullen bijdragen aan de gemeenschappelijke aanpak tegen (grensoverschrijdende) criminaliteit. Bovendien gaat het voorgestelde optreden niet verder dan noodzakelijk omdat de initiatieven en het bieden van een strategische visie op rechtmatige toegang tot data nog wel voldoende ruimte laat aan de EU-lidstaten om hier invulling aan te geven en door de uitwerking daarvan mede vorm te geven en grondrechten te borgen.

d) Financiële gevolgen

De mededeling op zichzelf heeft geen directe financiële gevolgen, maar bevat wel vermeldingen van beoogde concrete investeringen van de EU of van lidstaten. De Commissie geeft aan dat ondersteuning van Europol in het versterken van, onder andere, haar decryptie faciliteiten, financiële gevolgen kan hebben. Hierbij worden echter geen bedragen genoemd of doorrekening gegeven. Het kabinet onderkent het belang van samenwerking op dit terrein, waar de kosten voor doorontwikkeling worden aangejaagd door de snelheid van technologische ontwikkelingen. De Commissie geeft op dit punt aan dat lidstaten nauw betrokken zullen worden om hun specifieke behoeften te delen. Het kabinet zal de Commissie vragen aan te geven wat het financieel beslag van de aangekondigde voorstellen zal zijn. Het kabinet is van mening dat

¹⁶ Het thema «rechtmatige toegang tot gegevens» wordt ten behoeve van de opsporing tevens uitgebreid beschreven in de EU interne veiligheidsstrategie, zie «ProtectEU: een Europese strategie voor interne veiligheid» (COM(2025) 148 final) d.d. 1 april 2025 onder punt (3).

¹⁷ Hierbij moet bijvoorbeeld worden gedacht aan de vele, vaak buiten de EU gevestigde bedrijven die nodig zijn om een communicatieverbinding tot stand te brengen. Hierbij moet bijvoorbeeld worden gedacht aan de vele, vaak buiten de EU gevestigde bedrijven die nodig zijn om een communicatieverbinding tot stand te brengen. Denk bijvoorbeeld aan het bedrijf waar de desbetreffende applicatie kan worden gedownload; het bedrijf dat de applicatie aanbiedt en het bedrijf dat de communicatie over het internet mogelijk maakt.

eventueel benodigde middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

Eventuele budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

Met betrekking tot de aangekondigde plannen omtrent standaardisatie maakt de Commissie melding van het verstrekken van financiële ondersteuning via het Fonds voor Interne Veiligheid aan experts die deelnemen aan relevante standaardisatiefora. Dit komt overeen met het advies van de HLG om dergelijke inspanningen van de Commissie te financieren in het kader van bestaande EU-instrumenten (Horizon Europe, het Digital Europa programma, en het Fonds voor interne veiligheid) en gelijksoortige instrumenten in het kader van de volgende langetermijnbegroting van de EU (meerjarig financieel kader). Het kabinet wil niet vooruit lopen op de integrale afweging van middelen na 2027. Voor wat betreft het standaardiseren van interceptiemogelijkheden moet worden opgemerkt dat een wettelijke bevoegdheid tot het creëren van dergelijke mogelijkheden altijd noodzakelijk is alvorens deze kunnen worden geagendeerd in de desbetreffende standaardisatiefora (waaronder ETSI en 3GPP). Anders gezegd: interceptiemogelijkheden worden niet in standaarden opgenomen indien de bevoegdheid daartoe niet bij wet is voorzien.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

De mededeling bevat enkel aankondigingen van voorgenomen initiatieven van wetgevende, beleidsmatige of praktische aard waarvan net als bij de financiële gevolgen, de gevolgen voor de regeldruk zonder uitwerking nu niet zijn in te schatten. Waar het gaat om de impact van de voorgestelde maatregelen op grensoverschrijdende strafrechtelijke onderzoeken en handhavende acties is het mogelijk dat de voorgestelde initiatieven effect hebben op de vraag- en aanbodkant van rechtshulp en de doorlooptijd van onderzoeken. Rechtshulpverzoeken veroorzaakt door weinig gestroomlijnde samenwerking zullen mogelijk afnemen. Meer geharmoniseerde regels op het gebied van dataretentie en de beoogde technische ondersteuning kunnen verder bijdragen aan een verlaging van de regeldruk. Bij de uitwerking van (wetgevings-)voorstellen moet volgens het kabinet het uitgangspunt zijn dat deze zo lastenluw mogelijk worden vormgegeven zodat hun haalbaarheid wordt vergroot en rekening wordt gehouden met de beperkingen in capaciteit en middelen bij organisaties verantwoordelijk voor hun uitvoering.

De voorgestelde maatregelen die betrekking hebben op het bundelen van onderzoeks- en ontwikkelinitiatieven inzake innovaties voor veiligheidsdoeleinden worden positief beoordeeld in het kader van de geopolitieke positie van de EU, indien daarbij de open strategische autonomie (veiligheidsbelangen) van Nederland te allen tijde goed wordt bewaakt. Innovaties die voortvloeien uit deze bundeling kunnen het concurrentievermogen binnen deze sector vergroten.