Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

398

Vragen van de leden **Kathmann** (GroenLinks-PvdA) en **Six Dijkstra** (Nieuw Sociaal Contract) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de oproep van Europese politiechefs om end-to-endencryptie te verzwakken* (ingezonden 30 april 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 25 oktober 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 1796.

Vraag 1
Bent u bekend met het bericht «Politiechefs spreken zich uit tegen versleutelde chatberichten» (NU.nl, 22 april)?[1]

Antwoord 1
Ja

Vraag 2 (i)
Wat is uw reactie op de oproep van Europese politiechefs om actie te ondernemen tegen online platforms die berichten end-to-end versleutelen?

Antwoord 2 (i)
Allereerst wil ik graag het belang benadrukken van het signaal dat de politiechefs afgeven. Het is de taak van de politie om burgers te beschermen en om strafbare feiten op te sporen. De politiechefs geven aan dat de manier waarop end-to-end-encryptie wordt uitgerold, hen zodanig belemmert dat zij hun wettelijke taak om burgers te beschermen niet meer goed kunnen uitoefenen («*[a]s a result, we will simply not be able to keep the public safe*»). Dat is een zeer serieus signaal, dat ik ook als zodanig wil behandelen. De politiechefs roepen niet op om «actie te ondernemen tegen platforms». Zij richten zich primair tot de platforms zelf. Zij vragen de platforms om goed te kijken op welke manier privacybeschermende technologie kan worden ingezet, zonder dat zij zelf en de politie daardoor blind worden voor de criminaliteit op hun platform. Zij hebben daar ook een maatschappelijke

[1] Nu.nl, 22 april 2024, Politiechefs spreken zich uit tegen versleutelde chatberichten (www.nu.nl/tweakers/6310039/politiechefs-spreken-zich-uit-tegen-versleutelde-chatberichten.html)

ah-tk-20242025-398
ISSN 0921 - 7398
's-Gravenhage 2024

verantwoordelijkheid. De politiechefs spreken hen daarop – terecht – aan en geven blijk van het besef dat dit per platform maatwerk kan betekenen. Daarnaast worden overheden opgeroepen om te werken aan oplossingen. Dat vind ik een terechte oproep. Ik zal daar in het antwoord op de volgende vraag nader op in gaan.

Vraag 2 (ii)
Heeft u hierover contact gehad met uw Europese collega's? Welke acties verbinden u en uw collega's aan deze oproep?

Antwoord 2 (ii)
Ik heb geen direct contact gehad met mijn Europese collega's over deze verklaring, en vooralsnog verbind ik geen acties aan deze oproep. Wel worden de uitdagingen voor de opsporing bij de rechtmatige toegang tot gegevens veelvuldig besproken in Europese fora. Experts vanuit Europa hebben zich over deze kwestie gebogen, met het doel om de nieuwe Commissie werkbare handvatten aan te reiken waarmee zij aan de slag kunnen gaan.[2] Vanwege het sterk grensoverschrijdende karakter van dit probleem, acht ik het belangrijk dat wij dit in Europees verband oplossen.

Vraag 3
Wat is uw standpunt en wat is het standpunt de Nederlandse politie over end-to-end versleuteling? Onder welke concrete voorwaarden vindt u het verbreken van end-to-end versleuteling gerechtvaardigd, zowel individueel gericht als via het inbouwen van een generieke achterdeur bij versleutelde berichtenplatforms?

Antwoord 3
De Kamer heeft in juli 2022 middels de motie van het lid Van Raan c.s. de regering verzocht end-to-end-encryptie in stand te houden en voorstellen die dat onmogelijk maken niet te steunen. Het vorige kabinet heeft, in antwoord op dit verzoek, toegezegd uitvoering te geven aan deze motie.[3] Dit standpunt staat hier niet ter discussie.
Wel wil ik, zoals mijn voorganger vaak heeft benadrukt, het belang onderstrepen dat wij moeten blijven zoeken naar mogelijkheden om rechtmatige toegang tot gegevens mogelijk te maken en/of te behouden. Zoals de Kamer is geïnformeerd wordt onder andere in Europees verband naar oplossingen gezocht.[4] Dat is echter een lang proces, waarbij nog geen concrete oplossingen in zicht zijn.
Overigens geeft (vooral) het Wetboek van Strafvordering bevoegdheden voor de opsporing van strafbare feiten. Deze bevoegdheden, zoals de bevoegdheid tot binnendringen in een geautomatiseerd werk, kunnen leiden tot een inbreuk op de persoonlijke levenssfeer en zijn daarom met voorwaarden en waarborgen omkleed. Deze wettelijke bepalingen zijn in beginsel techniekneutraal. Of een inbreuk op de persoonlijke levenssfeer gerechtvaardigd is, wordt derhalve niet bepaald door de keuze van de beveiligingstechniek van de verdachte.

Vraag 4 (i)
Heeft u contact gehad met Europol en de nationale politie over deze gezamenlijke oproep?

---

[2] De Kamer is eerder geïnformeerd dat in Europees verband de zogenaamde «High Level Group» de opdracht heeft gekregen om de uitdagingen, die handhavingsautoriteiten in de praktijk ervaren, nader te verkennen en effectieve methoden en technieken voor de rechtshandhaving te formuleren. Daarbij richt de groep zich op adequate toegang tot gegevens. Gevoed door experts uit heel Europa werkt deze groep aan een toekomstgerichte visie op de uitdagingen voor de handhaving met inachtneming van de technologische ontwikkelingen en aan aanbevelingen voor de verdere ontwikkelingen van EU-beleid en -regelgeving. Zie Kamerstukken II, 2022–2023, 32 317, nr. 845; Kamerstukken II, 32 317, nr. 830 en 879.

[3] Kamerstukken II, 2022–2023, 26 643, nr. 908.

[4] Zie o.a. Kamerstukken II, 2022–2023, 32 317, nr. 845; Kamerstukken II, 2022–2023, 32 317, nr. 830.

Antwoord 4 (i)
Nee. Mijn ministerie heeft wel regelmatig contact met Europol over handhavingsvraagstukken, waaronder het onderhavige vraagstuk.

Vraag 4 (ii)
Ontvangt u dergelijke signalen ook van Nederlandse politiechefs? Zo ja, wat is uw reactie?

Antwoord 4 (ii
Ja. Ik onderken hun zorgen en deel deze. Daarom zoek ik, zoals ook aangegeven in mijn antwoord op vraag 3, in Europees verband naar oplossingen voor dit handhavingsprobleem.

Vraag 5
Deelt u de mening van politiechefs dat end-to-end versleuteling in stand kan blijven met een achterdeurtje die alleen voor de politie beschikbaar is? Zo ja, hoe ziet u dat voor zich? Hoe stelt u voor dat dit technisch kan zonder dat deze achterdeur algemeen beschikbaar komt en daarmee een einde maakt aan end-to-end versleuteling?

Antwoord 5
De hoofden van politie wijzen op de uitdagingen voor de opsporing bij de rechtmatige toegang tot gegevens. Zij roepen op tot het mogelijk houden dan wel maken van die rechtmatige toegang, waarbij zij tevens vermelden dat de technische oplossingen hiervoor kunnen verschillen voor diverse platforms of vormen van toegang. Zoals gemeld wordt momenteel onder andere in Europees verband naar oplossingen gezocht.
De politie geeft in haar verklaring niet aan dat «end-to-end versleuteling in stand kan blijven met een achterdeurtje die alleen voor de politie beschikbaar is». Het is van belang te zoeken naar mogelijkheden om te voorkomen dat er vrijplaatsen voor criminele activiteiten ontstaan, die tevens recht doen aan het belang van het in stand houden van end-to-end encryptie.

Vraag 6
In de Staat van de Unie 2023[5] schrijft u dat «end-to-end encryptie niet onmogelijk (mag) worden gemaakt,» tegelijkertijd stelt u in eerdere antwoorden op Kamervragen van de leden Kuik en Slootweg[6] dat «het van belang [is] dat er mogelijkheden zijn om onder bepaalde omstandigheden toegang tot (end-to-end versleuteld) berichtenverkeer te krijgen, onder passende voorwaarden en waarborgen.» Hoe verenigt u deze standpunten? Zou toegang onder bepaalde voorwaarden en waarborgen end-to-end versleuteling niet per definitie onmogelijk maken?

Antwoord 6
Een inperking van de privacy door de overheid moet steeds voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Waar nodig worden in wettelijke regelingen daarover waarborgen opgenomen, zoals een rechterlijke machtiging voor het inperken van de vertrouwelijkheid van communicatie. In het kader van de opsporing van strafbare feiten betreft dergelijke wetgeving vooral het Wetboek van Strafvordering. Deze wettelijke bepalingen zijn in beginsel techniek-neutraal geformuleerd. Welke beveiligingsmethodiek wordt toegepast, is niet van belang voor de vraag of een inbreuk op de privacy gerechtvaardigd is.
Toegang tot informatie in specifieke gevallen leidt niet noodzakelijkerwijs tot het onmogelijk maken van end-to-end-encryptie. Wanneer informatie wordt getransporteerd tussen twee punten («end-to-end») kan deze worden beveiligd (versleuteld) worden met end-to-end-encryptie. Deze beveiligingsmethode zorgt er voor dat tijdens het transport van die informatie derden dit bericht niet in leesbare vorm kunnen onderscheppen. Om toch toegang tot het berichtenverkeer te verkrijgen, bijvoorbeeld omdat op grond van wettelijke bevoegdheden tot toegang tot de berichten van een verdachte in het kader van een opsporingsonderzoek is besloten, zijn er in theorie diverse

[5] Kamerstuk 36 259, nr. 1
[6] Aanhangsel Handelingen II, vergaderjaar 2022–2023, nr. 3180

mogelijkheden. Het bericht kan bijvoorbeeld versleuteld worden onderschept en later worden ontsleuteld. Dit blijkt echter tegenwoordig in de praktijk vaak technisch niet mogelijk. Een andere mogelijkheid is dat de aanbieder van de communicatiedienst de encryptie voor de berichten van een specifieke verdachte niet toepast en de berichten onversleuteld aan de autoriteiten verstrekt, zoals ook aanbieders van openbare telecommunicatiediensten verplicht zijn de versleuteling ongedaan te maken in het geval van het aftappen van telecommunicatie. De end-to-end-versleuteling wordt voor berichten van en naar deze specifieke verdachte dan uitgezet. Zoals eerder is toegelicht aan uw Kamer staat deze methode los van andere processen die plaatsvinden op een apparaat.[7] Een manieren waarop inzicht in informatie kan worden verkregen op het apparaat is bijvoorbeeld het binnendringen in een geautomatiseerd werk. Met een dergelijke methode is er toegang tot de gegevens op het apparaat in plaats van tijdens het transport. De berichten zijn dan veelal in leesbare vorm, omdat deze op het apparaat nog niet zijn versleuteld voor het transport, of reeds zijn ontsleuteld na het transport. Deze mogelijkheden kunnen een meer dan geringe inbreuk op de privacy opleveren en zijn daarom met passende wettelijke voorwaarden en waarborgen omkleed. Zo moeten zij onder meer voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Voor een nadere toelichting wil ik verwijzen naar brieven van 8 mei, 28 juni en 18 september 2023 aan uw Kamer.[8]

Vraag 7
Bent u bekend met cryptotelefoons? Zo ja, hoe denkt u te voorkomen dat criminelen gebruik maken van deze devices in plaats van reguliere end-to-end versleutelde berichtenplatforms? Hoe weegt u de effectiviteit van de inbreuk op de privacy van miljoenen mensen tegenover de georganiseerde misdaad die vervolgens via cryptotelefoons anoniem kan blijven communiceren?

Antwoord 7
Ja, ik ben bekend met cryptotelefoons. Deze zijn op zichzelf niet verboden. Voor handhavingsautoriteiten is het probleem bij cryptotelefoons niet anders dan bij andere sterk versleutelde diensten: iedereen, inclusief gerechtelijke autoriteiten in Europese lidstaten die handelen op basis van wettelijke bevoegdheden, wordt toegang ontzegd tot de inhoud van deze berichten door het platform dat de communicatie mogelijk maakt. Dit gebrek aan rechtmatige toegang tot digitale gegevens raakt tevens de kern van de zorg die wordt uitgesproken door de nationale hoofden van politie in hun verklaring d.d. 18 april.[9]

Vraag 8
Wat is het staande beleid ten opzichte van de strategie «store-now-decrypt-later»? Wordt er nu al door veiligheidsdiensten versleutelde informatie opgeslagen, om deze op een later moment te ontsleutelen? Hoe lang mag de politie deze informatie dan hiervoor opslaan?

Antwoord 8
Ik ben bekend met het *store-now-decrypt-later*-begrip en de mogelijkheid om versleutelde informatie op te slaan om deze op een later moment te kunnen ontsleutelen indien er in de toekomst een kwantumcomputer beschikbaar komt. In dat verband wil ik wijzen op de strategie die de rijksoverheid heeft ontwikkeld om organisaties te helpen de risico's van kwantumtechnologie op cryptografie op tijd te beheersen, door tijdig te migreren naar zogenaamde

---

[7] Zie o.a. Kamerstukken II, 2022–2023, 26 643, nr. 968, (Verslag van een schriftelijk overleg); Kamerstukken II, 26 643, nr. 1064, p. 22; Kamerstukken II, 2022–2023, 26 643/34 843, nummer 1022.

[8] Kamerstukken II 2022–2023, 26 643, nr. 1022; Kamerstukken II 2022–2023, 26 643, nr. 1043; Kamerstukken II 2022–2023, 26 643, nr. 1011.

[9] Over de afweging met betrekking tot de privacy bij het eventueel detecteren van beeldmateriaal van online seksueel kindermisbruik en *grooming* wordt verwezen naar de kabinetsbrieven van 8 mei, 28 juni en 18 september 2023 aan uw Kamer (Kamerstukken II 2022–2023, 26 643, nr. 1022; Kamerstukken II 2022–2023, 26 643, nr. 1043; Kamerstukken II 2022–2023, 26 643, nr. 1011).

post-quantum cryptografie.[10] Deze vorm van cryptografie biedt weerstand tegen het eerder genoemde *store-now-decrypt-later*-scenario.
Op uw vraag over de veiligheidsdiensten wijs ik erop dat over de precieze werkwijze van de inlichtingen- en veiligheidsdiensten in het openbaar geen uitspraken worden gedaan. Voor de politie in Nederland geldt dat zij in het kader van de opsporing versleutelde persoonsgegevens rechtmatig kunnen vergaren op grond van diverse bevoegdheden uit het Wetboek van Strafvordering. De wettelijke bewaartermijnen voor politiegegevens, zoals onder andere opgenomen in de Wet politiegegevens, maken geen onderscheid tussen versleutelde en onversleutelde gegevens.

Vraag 9
Bent u bekend met de uitspraak van het Europese Hof voor de Rechten van de Mens (EHRM) op 13 februari 2024 in de zaak Podchasov v. Rusland?[11] Bent u eveneens bekend met de gezamenlijke reactie van de European Data Protection Board (EDPB) van 13 februari 2024 op de Verordening ter voorkoming en bestrijding van seksueel kindermisbruik (CSAM)?[12] Bent u bovendien bekend met het standpunt van het Europese Hof van Justitie dat generieke toegang tot versleutelde berichten nooit rechtmatig kan zijn?[13]

Antwoord 9
Ja, ik ben bekend met de uitspraak in de zaak *Podchasov v. Rusland*. Daarnaast ben ik bekend met de verklaring van het Europees Comité voor gegevensbescherming van 13 februari 2024. Dit betreft echter geen reactie op de Verordening ter bestrijding en voorkoming van seksueel kindermisbruik zoals voorgesteld door de commissie, maar op het (tegen)voorstel zoals gedaan door het Europees Parlement op 22 november 2023.[14] Ten slotte ben ik bekend met de uitspraak van het Europese Hof in de zaak *Schrems*. Versleutelde berichten of versleuteling speelden echter geen rol in deze zaak.

Vraag 10
Onderschrijft u de conclusies van deze zwaarwegende uitspraken omtrent end-to-end versleuteling volledig? Kunt u op de uitspraken en standpunten van de drie organisaties afzonderlijk reageren?

Antwoord 10

Europees Hof voor de Rechten van de Mens (EHRM)
In de zaak *Podchasov v. Rusland* is klager een Russische onderdaan, en gebruiker van de berichtenapplicatie Telegram. Telegram is door de Russische staat aangemerkt als «Internet organisator van communicatie». Als gevolg hiervan is het bij wet verplicht om alle communicatiegegevens op te slaan voor de duur van een jaar en de inhoud van alle communicatie gedurende zes maanden. Verder is bepaald dat deze gegevens kunnen worden voorgelegd aan de rechtshandhavingsinstanties of veiligheidsdiensten, samen met de informatie die nodig is om versleutelde berichten te kunnen ontsleutelen.[15] Het EHRM overweegt dat het opslaan van de gegevens van klager een inmenging is in het recht op privéleven (artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM)). Deze inmenging kan gerechtvaardigd zijn indien deze heeft plaatsgevonden in overeenstemming met de wet, een

---

[10] Kamerstukken II, 26 643, nr. 1085; Kamerstukken II, 2023–2024, Aanhangsel van de Handelingen, nummer 1178.

[11] European Court of Human Richts, 13 februari 2024, PODCHASOV v. RUSSIA (hudoc.echr.coe.int/eng/#%7B%22itemid%22:%5B%22001-230854%22%5D%7D).

[12] European Data Protection Board, 13 februari 2024, Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf.pdf (Europa.eu)).

[13] Van Daalen, 22 april 2023, Fundamental rights assessment of the framework for detection orders under the CSAM proposal (https://www.ivir.nl/publicaties/download/CSAMreport.pdf). paragraaf 3.2

[14] Zie https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf.

[15] De samenvatting van deze Hofuitspraak is mede ontleend aan de Nieuwsbrief Rechtspraak Europa, aflevering 3, 2024, gepubliceerd ten behoeve van de Rechtspraak op rechtspraak.nl.

legitiem doel dient en noodzakelijk is in een democratische samenleving. Het EHRM overweegt dat nationale wetgeving voldoende waarborgen moet bieden met betrekking tot onder andere de duur, de opslag, het gebruik, de toegang van derden, procedures voor het bewaren van de integriteit en vertrouwelijkheid van gegevens en procedures voor de vernietiging ervan, zodat er voldoende garanties zijn tegen het risico van misbruik en willekeur, om te voorkomen dat persoonsgegevens in strijd met artikel 8 EVRM worden gebruikt. De nationale wetgeving moet er met name voor zorgen dat de bewaarde gegevens relevant en niet buitensporig zijn in verhouding tot de doeleinden waarvoor ze worden bewaard, en dat ze in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor ze worden bewaard. Daarnaast moet de wetgeving aan het voorzienbaarheidsvereiste voldoen.
Het EHRM overweegt dat Russische wetgeving communicatieaanbieders verplicht tot het installeren van technieken die directe toegang door de Russische veiligheidsdiensten tot de communicatie mogelijk maken. De Russische opsporingsautoriteiten moeten weliswaar een rechterlijke machtiging verkrijgen alvorens deze gegevens te kunnen raadplegen, maar er bestaat geen verplichting om die machtiging ook aan de communicatieaanbieder te tonen.[16] Gezien het risico van misbruik dat een dergelijke regeling in het leven roept, moet de wet voldoende waarborgen bevatten tegen willekeur en misbruik. Het EHRM oordeelt dat daar in deze zaak onvoldoende sprake van is.
Met betrekking tot de verplichting tot medewerking van Telegram aan het ontsleutelen van alle end-to-end versleutelde communicatie overweegt het EHRM:
«Deze maatregelen kunnen naar verluidt niet worden beperkt tot specifieke individuen en zouden zonder onderscheid iedereen treffen, inclusief individuen die geen bedreiging vormen voor een legitiem overheidsbelang. Het verzwakken van de encryptie door het creëren van achterdeuren zou het blijkbaar technisch mogelijk maken om routinematige, algemene en willekeurige surveillance van persoonlijke elektronische communicatie uit te voeren.»
Het EHRM overweegt dat onder die omstandigheden de bovengenoemde verplichting die Rusland oplegde aan Telegram niet proportioneel is ten aanzien van het beoogde doel.[17] Het EHRM concludeert dat de bestreden Russische wetgeving onvoldoende adequate waarborgen tegen misbruik bevat en de kern van artikel 8 EVRM aantast – het recht op eerbiediging van het privéleven.
Het vorige kabinet heeft aangegeven uitvoering te geven aan de motie-Van Raan en heeft dit standpunt uitgebreid weergegeven en onderbouwd. Dit standpunt, dat hier niet ter discussie staat, staat haaks op het creëren van enige verplichting tot afzwakking, uitschakeling of algehele ontsleuteling van end-to-end versleutelde informatie.

Europees Hof van Justitie
Het Europese Hof in de zaak *Schrems* schreef dat «een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie [moet] worden beschouwd als een aantas-

[16] Zie Annotatie bij Europees Hof voor de Rechten van de Mens, 13-02-2024, ECLI:CE:ECHR:2024:0213JUD003369619 (EHRC-2024–0077).
[17] Ibid, p. 4. De Engelse tekst in overweging 77 van de uitspraak van het EHRM luidt als volgt «[...] it appears that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's «secret chats», it would be necessary to weaken encryption for all users. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications.»

ting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd».[18]
Hoewel ik deze conclusie van het Hof onderschrijf, wil ik erop wijzen dat versleutelde berichten of versleuteling als zodanig geen rol speelde in deze zaak.

Europees Comité voor gegevensbescherming
Het kabinet onderschrijft de conclusie van het Europees Comité voor gegevensbescherming dat end-to-end versleuteling een belangrijk middel is om de vertrouwelijkheid van elektronische communicatie te kunnen bewerkstelligen.

Vraag 11
Is uw standpunt over end-to-end versleuteling veranderd naar aanleiding van de recente uitspraken van het EHRM en EDPB? Zo ja, op welke wijze draagt u dit uit bij lopende onderhandelingen in Europa en het binnenland over wet- en regelgeving? Zo niet, kan u met voorbeelden onderbouwen dat het huidige kabinetsstandpunt voldoende invulling geeft aan de uitspraken van de rechter en de EDPB?

Antwoord 11
Nee. Dit standpunt, zoals aangehaald en beschreven in mijn beantwoording op uw vorige vragen, is niet strijdig met voornoemde uitspraken.

Vraag 12
Biedt het geactualiseerde Grondwetsartikel 13 over het brief- en telecommunicatiegeheim een absolute garantie dat er geen verzwakkingen van end-to-end versleuteling mogen plaatsvinden in Nederland? Zijn de aanbevelingen van de staatscommissie-Grondwet 2010 hiermee volledig geïmplementeerd?[19]

Antwoord 12
De doelstelling van artikel 13 Grondwet (Gw) betreft het beschermen van de vertrouwelijkheid van communicatie. Die bescherming geldt met en zonder encryptie: ook als de inhoud van communicatie niet versleuteld is, mag die niet zomaar worden bekeken. Encryptie is een technische manier om de inhoud van de communicatie te beschermen tegen inzage door anderen, naast andere manieren om daartegen te beschermen. Artikel 13 schrijft niet voor of en op welke wijze private partijen hun communicatie dienen te beschermen.[20] Dat een beveiligingsmethode eventueel gekraakt kan worden doet aan de juridische bescherming niet af.[21] Overigens biedt artikel 13 Gw expliciet de mogelijkheid inperkingen te maken op het communicatiegeheim. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Een voorbeeld van een dergelijke beperking is inzet van de interceptiebevoegdheid ten behoeve van de opsporing van strafbare feiten. Voorafgaande machtiging van de rechter is dan vereist.
In 2010 adviseerde de Staatscommissie om de bescherming van artikel 13 Gw te beperken tot de transportfase van de informatie en de inhoud van de communicatie buiten de bescherming van artikel 13 te laten vallen.[22] In de memorie van toelichting bij de herziening van dit grondwetsartikel, alsmede tijdens debatten over het wetsvoorstel in de Tweede Kamer, is toegelicht waarom voor een andere, tevens techniek-onafhankelijke benadering is gekozen bij de vormgeving van dit grondwetsartikel.[23] In de kern komt het

---

[18] Uitspraak van het Hof van Justitie in de zaak Schrems I (C-362/14), 6 oktober 2015, paragraaf 94.
[19] Bijlage bij Kamerstuk 31 570, nr. 17. paragraaf 8.6
[20] Zie o.a. verslag van een debat in de Eerste Kamer over het wetsvoorstel Verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim, Kamerstuk HTK20212022-66-5 (30-03-2022).
[21] Deze grondgedachte is door de tijd heen in feite hetzelfde gebleven, zie o.a. Kamerstukken II, 1997–1998, 25 443, nummer 5.
[22] Kamerstukken II, 2010–2011, 31 570, nr. 17, pp. 86–87.
[23] Zie o.a. Kamerstukken II, (2013–2014), 33 989, nr. 3.

erop neer dat bij de bescherming van het telecommunicatiegeheim is gekozen om niet het middel dat bescherming kan bieden, maar bescherming van de inhoud van de communicatie zelf centraal te stellen.[24]

Vraag 13
Bent u bereid om samen met de nationale politie en de Autoriteit Persoonsgegevens tot een eenduidig standpunt te komen over het borgen van end-to-end versleuteling, dat recht doet aan de uitspraken van het EHRM, EHJ en de EDPB, en dit blijvend uit te dragen in Nederland en Europa?

Antwoord 13
Zoals gezegd is voornoemd standpunt inzake end-to-end-encryptie niet strijdig met voornoemde uitspraken. Voor nadere uitleg verwijs ik naar mijn puntsgewijze beantwoording van vraag 10.

Vraag 14
Kunt u deze vragen apart van elkaar beantwoorden?

Antwoord 14
Ja.

[24] Zie o.a. Kamerstukken II, (2013–2014), 33 989, nr. 3.