26 643 **Informatie- en communicatietechnologie (ICT)**

Nr. 968 **Verslag van een schriftelijk overleg**
Vastgesteld 2 februari 2023

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de minister van Justitie en Veiligheid over de brief van 23 september 2023 over uitvoering van de motie van het lid Van Raan c.s. over end-to-endencryptie in stand houden (Kamerstuk 26 643, nr. 885) (Kamerstuk 26 643, nr. 908).

De vragen en opmerkingen zijn op 2 december 2022 aan de minister van Justitie en Veiligheid voorgelegd. Bij brief van 31 januari 2023 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Van Tilburg

Inleiding

Hierbij bied ik uw Kamer de antwoorden aan op de nadere vragen van 4 december 2022 van de leden van de fracties van Democraten 66 (D66), Christen-Democratisch Appèl (CDA), Socialistische Partij (SP) en Partij voor de Dieren (PvdD) naar aanleiding van mijn brief van 23 september 2022 over de uitvoering van de motie van het lid Van Raan c.s. (Kamerstuk 26 643, nr. 885) over end-to-end encryptie (Kamerstuk 26 643, nr. 908).

Ik heb met belangstelling kennisgenomen van de vragen van de leden van deze fracties. De vragen beantwoord ik hierna. Bij de volgorde van de beantwoording is de volgorde van de brief van 4 december 2022 aangehouden. Vanwege de omvang van het aantal vragen en het detailniveau van de beantwoording daarvan, heb ik de afzonderlijke vragen en antwoorden zoveel mogelijk bij elkaar gehouden.

Vragen van de leden van de D66-fractie en antwoorden

De leden van de D66-fractie hebben kennisgenomen van de kabinetsreactie op de motie van het lid Van Raan c.s. (Kamerstuk 26 643, nr. 885) en hebben hier over enkele vragen. Allereerst vragen de leden van de D66-fractie er wederom aandacht voor dat er geen tussenweg bestaat tussen veilige encryptie en een achterdeur voor veiligheidsdiensten. Met onderzoek naar een niet bestaande technische oplossing voor dit probleem staat het recht op veilige encryptie onder druk met grote gevolgen voor het beschermen van kennis bij bedrijven en het werk van journalisten, wetenschappers, activisten, advocaten en vele anderen.

Vraag
Kan de minister de positie van Duitsland en het Oostenrijkse parlement ten opzichte van het onderdeel chatcontrol in het commissievoorstel toelichten?

Antwoord
In algemene zin zien lidstaten de noodzaak van een Europese aanpak om (online) seksueel kindermisbruik tegen te gaan. De Duitse minister van Justitie heeft via sociale media aangegeven kritisch te zijn op wat hij chatcontrol noemt.[1] De term chatcontrol als zodanig wordt niet genoemd in de Verordening. In Oostenrijk heeft het parlement een motie aangenomen waarin het de minister van Binnenlandse Zaken, de minister van Justitie en de minister voor Vrouwen, Familie, Integratie en Media oproept om in het kader van de onderhandelingen over de verordening ervoor te zorgen dat deze in overeenstemming is met de grondrechten.

Vraag
Acht de minister het mogelijk om aan te sluiten bij de Duitse en Oostenrijkse inzet om chatcontrol uit de motie te weren? Zo nee, waarin verschillen de posities van Nederland ten opzichte van deze landen? Deze leden zullen op dit onderwerp een motie indienen om hierbij aan te sluiten tijdens de eerste volgende Raad Justitie en Binnenlandse Zaken (JBZ-raad).

[1] Een nadere duiding van hetgeen de Duitse Minister bedoelt met deze term wordt gegeven in een online artikel van ‘Zeit online’ d.d. 13 oktober 20222: https://www.zeit.de/digital/internet/2022-10/kindesmissbrauch-netz-chatkontrolle-eu-marco-buschmann.

Antwoord
Het Nederlandse standpunt blijkt uit het BNC-fiche en de brief over de uitvoering van de motie van het lid Van Raan c.s. (Partij van de Dieren). Het Nederlandse standpunt met betrekking tot monitoring van materiaal van seksueel kindermisbruik en grooming is duidelijk. Het kabinet vindt het tegengaan van (materiaal van) seksueel kindermisbruik van groot belang. Het kabinet ziet voor detecteren mogelijkheden voor bijvoorbeeld het gebruik van hashdatabases, waarmee onmiskenbaar materiaal van seksueel kindermisbruik kan worden onderkend om vervolgens ontoegankelijk gemaakt te worden. Het kabinet wil niet dat het voorstel leidt tot algemene monitoring. Dit staat ook vermeld in het BNC-fiche (Kamerstuk 22 112, nr. 3455).

Een ander specifiek aandachtspunt voor het kabinet zijn de voorstellen op het gebied van grooming. De opsporing van grooming is complex, omdat het hierbij gaat om tekst waarbij de inhoud en de interpretatie afhankelijk zijn van de context. In Nederland is het detecteren van grooming exclusief belegd bij opsporingsinstanties. Nederland wil dit zo houden. In de onderhandelingen wordt dit standpunt actief uitgedragen.

Wanneer het gaat om versleuteling heeft Nederland ook een duidelijk standpunt ingenomen. Het kabinet zal (Europese) voorstellen die end-to end encryptie onmogelijk maken niet steunen. Hoe men binnen de kaders van bovengenoemde standpunten toegang kan krijgen tot informatie wordt nader onderzocht. Naast de mogelijke zorgen wil ik ook dat we goed kijken naar wat wél mogelijk is in dit complexe vraagstuk.

Het kabinet kijkt kritisch naar de aspecten van het voorstel waarmee inbreuk wordt gemaakt op een aantal grondrechten en beoogt te voorkomen dat het voorstel leidt tot algemene monitoring.[2] Een inbreuk op het recht op privéleven, het recht op gegevensbescherming, het recht op vrijheid van meningsuiting en het communicatiegeheim van burgers mag alleen als deze noodzakelijk is en voldoet aan de eisen van proportionaliteit en subsidiariteit en de bijzondere eisen van de grondwet en de desbetreffende internationale verdragen.

Samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken waarbij fundamentele rechten zijn geborgd.

Vragen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van de brief over de uitvoering van de motie van het lid Van Raan c.s. (Kamerstuk 26 643, nr. 885) over het in stand houden van end-to-end-encryptie. Deze leden hebben hierover nog enkele vragen. Zij willen ten eerste markeren dat zij tegen de betreffende motie hebben gestemd.

De leden van de CDA-fractie constateren dat de uitvoering van de motie invloed heeft op de onderhandelingen over de Conceptverordening inzake het tegengaan van online seksueel kindermisbruik. Deze leden maken zich grote zorgen over het grote aantal meldingen dat jaarlijks wordt gedaan van online seksueel kindermisbruik.

---

[2] Zie tevens artikel 8 van de Verordening Digitale Diensten (‘Digital Services Act): “Aan aanbieders van tussenhandeldiensten wordt geen algemene verplichting opgelegd tot monitoring van de door hen doorgegeven of opgeslagen informatie noch tot actief onderzoek naar de feiten of omstandigheden die duiden op illegale activiteiten.”

Vraag
Deze leden vragen of de minister het met deze leden eens is dat het belang van het terugdringen van online seksueel kindermisbruik voorop moet staan en dat dit belang zwaarder weegt dan de privacy van betrokkenen.

Antwoord
Het is van groot belang dat (online) seksueel kindermisbruik wordt voorkomen en bestreden. Het kabinet heeft zich de afgelopen jaren hard ingezet om materiaal van seksueel kindermisbruik effectief te bestrijden. Tegelijkertijd is het van belang dat de inbreuk op grondrechten alleen plaatsvindt wanneer deze strikt noodzakelijk is, voldoet aan de eisen van proportionaliteit en subsidiariteit, is omkleed met waarborgen en voldoet aan de bijzondere eisen van de Grondwet. Het gaat daarbij niet alleen om de bescherming van de privacy, maar bijvoorbeeld ook om de bescherming van het telecommunicatiegeheim. Het betreft mogelijk ook rechten van mensen die niets te maken hebben met (online) seksueel kindermisbruik. Het kabinet onderzoekt effectieve oplossingen die noodzakelijk, proportioneel en subsidiair zijn om online seksueel kindermisbruik aan te pakken en maakt daarbij steeds een weging van alle betrokken belangen.

Vraag
De leden van de CDA-fractie vragen ook of de minister vindt dat opsporingsdiensten adequate wettelijke bevoegdheden moeten hebben om online seksueel kindermisbruik te detecteren en meldingen op te volgen. Deze leden verwijzen in dit verband naar het genoemde verschil tussen Facebook (geen end-to-end-encryptie en 11 miljoen meldingen) en WhatsApp (wel end-to-end-encryptie en 400.000 meldingen). Deze leden concluderen hieruit dat end-to-end-encryptie een grote belemmering vormt voor het opsporen van online seksueel kindermisbruik en vragen of de minister het hiermee eens is.

Antwoord
Hoogwaardige encryptie is van groot belang. End-to-end encryptie is hier een voorbeeld van. Om het vertrouwelijke karakter van hun diensten te waarborgen passen steeds meer communicatiedienstverleners, zoals de aanbieders van Over-The-Top diensten, sterke encryptie toe. Sterke encryptie is cruciaal voor onze digitale samenleving en beschermt onze maatschappij tegen derden met kwaadwillende doeleinden zoals statelijke actoren en cybercriminelen. Bovendien is encryptie van groot belang voor de cybersecurity van systemen, onder meer door de communicatie tussen systemen van overheid, bedrijven en burgers te beveiligen. Encryptie draagt mede om deze redenen bij aan het beschermen van de nationale veiligheid.

Versleuteling heeft tegelijkertijd nadelige gevolgen voor de uitvoering van de wettelijke taak van opsporings- en inlichtingen en veiligheidsdiensten. Deze diensten geven regelmatig aan dat informatie die van belang is voor hun taakuitvoering vrijwel altijd van encryptie is voorzien en het steeds lastiger blijkt, en vaak onmogelijk, om deze te doorbreken. Dat belemmert de diensten in hun wettelijke taak de samenleving veilig te maken. Dit probleem is de afgelopen jaren steeds groter geworden, onder meer door het gebruik van communicatieapps en de standaard sterke versleuteling daarop. Waar openbare aanbieders van telecommunicatie reeds lange tijd zijn verplicht de afgetapte communicatie onversleuteld aan te leveren, is dit voor communicatieapps niet het geval.

De Europese Commissie heeft enkele voorbeelden genoemd van mogelijkheden hoe materiaal dat seksueel kindermisbruik bevat kan worden gedetecteerd. De voorstellen worden

bezien en samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken. Voorstellen die end-to-end encryptie onmogelijk maken worden daarbij niet gesteund.

Ik ben het met de leden van de CDA-fractie eens dat de bevoegdheden en middelen die de diensten tot hun beschikking hebben, moeten zijn toegerust op de huidige en toekomstige digitale realiteit en zeker op de bestrijding van seksueel kindermisbruik. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld. Daarbij blijven we openstaan voor nieuwe inzichten bij de vormgeving van beleid in het digitale domein.

Vraag
Deze leden vragen de minister daarom hoe zij het belang van de uitvoering van de motie weegt ten opzichte van de constatering dat het voor opsporingsdiensten vanwege end-to-end-encryptie steeds moeilijker wordt om informatie over strafbare feiten te detecteren en ontcijferen.

Antwoord
Integraal beleid is belangrijk in het digitale domein en hierin moeten verschillende belangen afgewogen worden en in evenwicht worden gebracht. In de discussie van rechtmatige toegang tot versleutelde opsporingsinformatie spelen verschillende zwaarwegende belangen een rol, waaronder die van de opsporing, privacy, het telecommunicatiegeheim en cybersecurity. Voor de opsporing is tijdige en effectieve toegang tot informatie van groot belang. Daarom wordt geanalyseerd wat de impact van encryptie op de opsporing is. Hierover verwacht ik in het eerste kwartaal van dit jaar een WODC-rapport naar uw Kamer te sturen. Bovendien is het noodzakelijk om te kijken welke opsporingsmiddelen effectiever kunnen worden ingezet. Op dit moment wordt gewerkt aan de reactie op de wetsevaluatie van de Wet Computercriminaliteit III die uw Kamer in het voorjaar ontvangt. Daarnaast blijft onderzoek mogelijk naar proportionele mogelijkheden voor rechtmatige toegang tot versleutelde opsporingsinformatie. Op deze manieren wordt invulling gegeven aan het opsporingsbelang binnen de encryptie discussie.

Vraag
Deze leden zijn van mening dat het uitvoeren van de motie een stap achteruit betekent in de aanpak van online seksueel kindermisbruik, en vragen welke stappen de minister neemt om dit te voorkomen.

Antwoord
Per brief van 23 september jl. is uw Kamer geïnformeerd dat het kabinet uitvoering zal geven aan de motie van het lid Van Raan c.s.[3] Dit betekent dat Nederland voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Wel wil ik blijven kijken naar wat wél mogelijk is (binnen- en buiten het encryptie dossier) om het werk van de opsporings-, inlichtingen- en veiligheidsdiensten effectief te houden. Eventuele maatregelen – die end-to-end encryptie niet onmogelijk maken – worden telkens bezien vanuit grondrechtelijk perspectief en beoordeeld op noodzakelijkheid, proportionaliteit en subsidiariteit.

[3] Kamerstuk 26 643, nr. 908, d.d. 23 september 2022.

Vraag
De leden van de CDA-fractie lezen in de beslisnota dat organisaties die in hun taakuitvoering nadelen ondervinden van end-to-end-encryptie, zoals de politie, bezwaren hebben geuit. Deze leden vragen hoe zwaarwegend de stem van de uitvoerende organisaties en mensen is voor de minister, aangezien zij dagelijks te maken krijgen met de schokkende inhoud van kinderporno en de uitdagingen die het terugdringen hiervan met zich meebrengt.

Antwoord
De stem van de uitvoerende organisaties en de mensen die daar werken is zeer zwaarwegend voor mij. Opsporings-, inlichtingen- en veiligheidsdiensten moeten nu en in de toekomst effectief gebruik kunnen maken van hun wettelijke bevoegdheden, zodat zij de nationale veiligheid kunnen beschermen, criminaliteit kunnen bestrijden en slachtoffers genoegdoening kan worden gegeven. Het is zaak om de beschermende waarde van versleuteling te behouden, terwijl de negatieve effecten voor opsporings- en inlichtingen en veiligheidsdiensten worden verminderd.

Daarom blijft wetenschappelijk onderzoek naar rechtmatige toegang tot versleutelde informatie mogelijk en gaat onze zoektocht naar alternatieve mogelijkheden tot het verkrijgen van informatie voor het tegengaan en opsporen van strafbare feiten en het beschermen van de nationale veiligheid door.

Vraag
Deze leden vragen hoe de minister ervoor zorgt dat deze organisaties en mensen, ondanks de aangenomen motie, niet worden belemmerd in hun belangrijke werk.

Antwoord
In opsporingsonderzoeken wordt gebruik gemaakt van diverse juridische en technische mogelijkheden. De inzet daarvan is steeds afhankelijk van de specifieke zaak en de afwegingen die daarin worden gemaakt. De uitdagingen waar sterke encryptie de opsporing voor stelt kunnen leiden tot (sterk) verminderde effectiviteit van de inzet van bepaalde bevoegdheden. Tijdens onderzoeken wordt per geval bezien of andere bevoegdheden en/of technische middelen in de informatiebehoefte kunnen voorzien. Naar verwachting is dat niet altijd het geval.

Vragen van de leden van de SP-fractie
De leden van de SP-fractie hebben de reactie van de minister over de uitvoering van de motie van het lid Van Raan c.s. (Kamerstuk 26 643, nr. 885) gelezen en hebben hierover nog enkele vragen en opmerkingen.

De leden van de SP-fractie vinden het in stand houden van end-to-end-encryptie van groot belang en vinden het daarom goed dat een Kamermeerderheid zich achter de motie van het lid Van Raan c.s. heeft geschaard. Het zou vanzelfsprekend moeten zijn dat het kabinet deze motie uitvoert. Deze leden hebben nog wel enkele zorgen, die overeenkomen met de zorgen die ook de Autoriteit Persoonsgegevens (AP) uit.

Vraag
De AP formuleert het als volgt:
"- Er ontstaat een te groot risico dat communicatiediensten bij alle communicatie van alle burgers in de Europese Economische Ruimte (EER) mee zullen kijken én luisteren.

- Er is een groot risico op ondermijning van het gebruik van versleutelde communicatie (zogeheten end-to-end encryptie);
- De AI-software die waarschijnlijk wordt ingezet maakt fouten en kan vooroordelen bevatten, waardoor burgers ten onrechte als potentieel 'verdacht' worden aangemerkt."
Kan de minister uitgebreid ingaan op deze zorgen?

Antwoord
Het kabinet heeft kennisgenomen van de brief van de Autoriteit Persoonsgegevens. De Autoriteit vindt het vanzelfsprekend dat seksueel kindermisbruik hard moet worden aangepakt, maar het huidige voorstel vormt naar de mening van de Autoriteit een te groot risico voor de rechten en vrijheden van burgers. Het kabinet is het met de Autoriteit eens dat seksueel kindermisbruik hard moet worden aangepakt en zet zich ervoor in dat materiaal van seksueel kindermisbruik effectief kan worden bestreden. Daarbij deelt het kabinet met de Autoriteit de zorgen over de inbreuk op de grondrechten die door het voorstel wordt gemaakt. Een inbreuk kan alleen plaatsvinden wanneer deze strikt noodzakelijk is, voldoet aan de eisen van proportionaliteit en subsidiariteit en omkleed is met waarborgen.

Volgens de Autoriteit ontstaat een te groot risico dat communicatiediensten bij alle communicatie van alle burgers in de Europese Economische Ruimte (EER) mee zullen kijken én luisteren. Aanbieders van hostingdiensten en interpersoonlijke communicatiediensten worden verplicht om mitigerende maatregelen te treffen en een beoordeling te maken van het risico op misbruik van hun diensten voor de verspreiding van materiaal van seksueel kindermisbruik of grooming. Dit rapporteren zij aan een door de lidstaten aangewezen coördinerende autoriteit. Als de coördinerende autoriteit vaststelt dat er een aanzienlijk risico op misbruik van de dienst blijft bestaan kunnen zij een rechtbank of een onafhankelijke nationale autoriteit vragen een detectiebevel uit te vaardigen. Dit bevel verplicht alleen aanbieders met een significant risico op misbruik van hun diensten om bekend of nieuw materiaal van seksueel kindermisbruik of grooming te detecteren. Het kabinet zal de voorgestelde maatregelen steeds kritisch bezien, in het bijzonder die maatregelen die ook zien op interpersoonlijk berichtenverkeer. In dit verband geldt dat het kabinet voorstellen die end-to-end encryptie onmogelijk maken niet steunt, conform de motie van het lid Van Raan c.s. Een ander specifiek aandachtspunt voor het kabinet zijn de voorstellen op het gebied van grooming. De opsporing van grooming is complex, omdat het hierbij gaat om tekst waarbij inhoud en interpretatie afhankelijk zijn van de context. In de onderhandelingen zal het kabinet het standpunt uitdragen dat Nederland het detecteren van grooming exclusief bij de opsporingsinstanties wil houden.

De Autoriteit raadt aan om expliciet in het voorstel op te nemen dat het voorstel niet als doel heeft end-to-end encryptie te verbieden of te verzwakken. Per brief van 23 september jl. is uw Kamer geïnformeerd dat het kabinet uitvoering zal geven aan de motie van het lid Van Raan c.s.[4] In de onderhandelingen over de voorgestelde verordening wordt uitgedragen dat het kabinet Europese voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen waarmee wordt beoogd dit standpunt te bestendigen in de verordening.

Volgens de Autoriteit is meer informatie nodig over de effectiviteit en de risico's van technologieën die gebruik maken van algoritmische software en de criteria waaraan deze software moet voldoen. Het voorstel is technologisch neutraal opgesteld en geeft geen

[4] Kamerstuk 26 643, nr. 908, d.d. 23 september 2022.

specificatie welke technologie moet worden gebruikt. Tegelijkertijd moet goed worden gekeken naar bepaalde randvoorwaarden waaraan de software moet voldoen. Hierbij valt o.a. te denken aan de voorwaarde dat deze end-to-end encryptie niet onmogelijk maakt of aan strenge voorwaarden ten aanzien van vals positieve marges. Het kabinet zal zich ervoor inzetten dat het voorstel niet leidt tot algemene monitoring en zet zich in voor goede waarborgen om te voorkomen dat materiaal onterecht als seksueel kindermisbruik wordt aangemerkt, zeker wanneer hierbij automatische middelen worden toegepast. Op dit moment wordt verkend met behulp van welke technologieën de verplichtingen uit de voorgestelde verordening zouden kunnen worden vervuld. Samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken waarbij fundamentele rechten zijn geborgd.

Ik wil hierbij wel opmerken dat, los van de beschermende waarde die sterke encryptie heeft voor onze samenleving, de toename van communicatie die end-to-end versleuteld is ook effecten heeft op de effectieve bestrijding van criminaliteit. Opsporingsonderzoeken zijn steeds meer afhankelijk van digitale opsporingsinformatie, terwijl de communicatie van verdachten steeds meer verloopt via ‘over the top’ communicatiediensten zoals Whatsapp of Signal. De praktische gevolgen van een praktijk waarin ‘niemand kan meekijken’, zoals de Autoriteit dit in haar advies verwoord, zijn steeds meer voelbaar in de rechtspraktijk.[5]

Vraag
Kan de minister verder toelichten wat het betekent dat Nederland het onmogelijk maken van end-to-end-encryptie niet zal steunen?

Antwoord
De Kamer heeft middels de motie van het lid Van Raan c.s. de regering verzocht end-to-end encryptie in stand te houden en Europese voorstellen die dat onmogelijk maken niet te steunen. Ik heb toegezegd uitvoering te geven aan de motie. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen voor aanpassingen van de conceptverordening, waarmee wordt beoogd dit standpunt te bestendigen in de verordening – óók als dat betekent dat de bepalingen uit de Verordening niet meer technologisch neutraal van aard zijn. Samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken.

Vraag
Steunt het kabinet wel maatregelen die end-to-end-encryptie nagenoeg onmogelijk zou maken of ernstig zouden bemoeilijken? Hoe wordt dit gewogen?

Antwoord

[5] Het brief- en telecommunicatiegeheim betreft, net als andere grondrechten, geen ongelimiteerd recht waarvoor alle andere grondrechten moeten wijken. Beperkingen op dit grondrecht zijn mogelijk in gevallen bij wet bepaald met machtiging van de rechter, met uitzondering van die gevallen waarin de nationale veiligheid in het geding is. Voor deze laatste categorie zijn beperkingen van het brief- en telecommunicatiegeheim toegestaan met machtiging van een of meer ministers die daartoe bij de wet zijn aangewezen. Zie o.a. Kamerstuk 33 989, nr. 3, paragraaf 3.2.

Voorstellen die end-to-end encryptie nagenoeg onmogelijk maken zijn niet in lijn met de motie van het lid Raan en worden niet gedragen door uw Kamer en dit kabinet. Er zijn echter maatregelen denkbaar (in de vorm van technische oplossingen op het apparaat zelf) die weliswaar end-to-end encryptie ongemoeid laten, maar toch een meer dan geringe privacy-inbreuk kunnen opleveren. In die gevallen is het belangrijk om vooraf scherp te bepalen welke mogelijke inbreuken proportioneel, subsidiair en noodzakelijk ten aanzien van het beoogde doel én voldoende omkleed zijn van de nodige waarborgen - zoals toetsing door een gerechtelijke instantie. Voor alle voorstellen geldt dat deze moeten worden beoordeeld wanneer zij worden gedaan, waarbij de motie van het lid Van Raan c.s. het uitgangspunt blijft.

Vraag
Kan de minister ingaan op wat de strategie van het kabinet is indien er in de verordening wel maatregelen worden genomen die end-to-end-encryptie onmogelijk maken? Kan de minister de procedure dan schetsen?

Antwoord
Op dit moment wordt onderhandeld over het voorstel en worden de bepalingen nauwkeurig en kritisch bezien. Daarbij wordt ook gekeken naar de effecten van het detectiebevel op end-to-end encryptie. In de onderhandelingen over de voorgestelde verordening wordt uitgedragen dat het kabinet Europese voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen waarmee wordt beoogd dit standpunt te bestendigen in de verordening (concreet: aanpassingen van de concept verordening). Samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken waarbij fundamentele rechten zijn geborgd. De besluitvormingsprocedure van de verordening is op basis van een gekwalificeerde meerderheid. Dit betekent dat als de verordening wordt aangenomen dat dit voor alle lidstaten geldt.

Vragen van de leden van de PvdD-fractie

De leden van de PvdD-fractie danken de minister voor haar brief over de aangenomen motie van het lid Van Raan c.s. (Kamerstuk 26643, nr. 885) over het in stand houden van encryptie. Deze leden hebben wel nog enige vragen over de uitvoering daarvan.

De leden van de PvdD-fractie zijn verheugd te horen dat de minister onderschrijft dat encryptie belangrijk is voor onder andere de vrijheid van meningsuiting en bijdraagt aan het beschermen van de nationale veiligheid maar zij zijn benieuwd hoe stellig de minister positie kiest binnen de Europese Unie bij voorstellen die encryptie ondermijnen.

Vraag
Deze leden vragen de minister of zij bereid is om bij de komende JBZ-raad op 8 en 9 december in Brussel en in de verdere toekomst actief steun te zoeken voor de Nederlandse positie omtrent encryptie. Naar mening van deze leden is het wenselijk dat Nederland niet alleen de positie inneemt dat encryptie niet onmogelijk gemaakt mag worden maar ook actief steun zoekt voor de positie dat de ontwikkeling, beschikbaarheid en toepassing van encryptie niet ingeperkt wordt. Is de minister daartoe bereid?

Antwoord

Per brief van 23 september is uw Kamer geïnformeerd dat het kabinet uitvoering zal geven aan de motie van het lid Van Raan c.s. Dit betekent ook dat Nederland samen met lidstaten met een gelijkluidende opvatting zal zoeken naar oplossingen om op een noodzakelijke, proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken.

Vraag
Draagt zij actief uit dat pogingen tot afzwakking of belemmering van encryptie op Nederlands verzet zullen stuiten?

Antwoord
In de onderhandelingen over de voorgestelde verordening wordt uitgedragen dat het kabinet Europese voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen waarmee wordt beoogd dit standpunt te bestendigen in de verordening. Het kabinet draagt het Nederlandse standpunt ook uit in gesprekken met Europese partners.

Vraag
Kan de minister het Europese krachtenveld op deze punten uitgebreider schetsen en kan zij de Kamer proactief verslag doen van Europese ontwikkelingen?

Antwoord
De lidstaten hebben in het algemeen een overwegend positieve houding ten opzichte van het voorstel van de Europese Commissie. De lidstaten zien de noodzaak van een Europese aanpak om (online) seksueel kindermisbruik tegen te gaan. Er zijn zowel lidstaten die van mening zijn dat end-to-end encryptie niet mag worden verzwakt als lidstaten die vinden dat end-to-end encryptie niet in de weg mag staan van de werking van de verordening. Wanneer het onderwerp op de JBZ-raad wordt geagendeerd, wordt het parlement via de geannoteerde agenda voor de Raad geïnformeerd.

Vraag
Wat bedoelt de minister precies als ze schrijft dat “Nederland voorstellen die end-to-end-encryptie onmogelijk maken niet steunt”? Betekent dat ook dat als er in de verordening artikelen zijn opgenomen die in potentie kunnen leiden tot een inperking van end-to-end-encryptie, Nederland zich hier tegen zal verzetten?

Antwoord
In de onderhandelingen over de voorgestelde verordening wordt uitgedragen dat het kabinet Europese voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen waarmee wordt beoogd dit standpunt te bestendigen in de verordening.

Vraag
De leden van de PvdD-fractie vragen of de minister de mening deelt dat het huidige Europese voorstel ter voorkoming en bestrijding van online seksueel kindermisbruik (CSA-voorstel) nog geen garanties bevat dat encryptie in stand kan blijven. Sterker nog, deelt de minister de mening dat het CSA-voorstel verplichtingen bevat die encryptie onmogelijk maken? Bijvoorbeeld doordat het communicatiediensten verplicht om berichten te bekijken, en zelfs verplicht om gesproken communicatie af te luisteren

Antwoord

De Kamer heeft middels de motie van het lid Van Raan c.s. de regering verzocht end-to-end encryptie in stand te houden en Europese voorstellen die dat onmogelijk maken niet te steunen. Tijdens de onderhandelingen geeft het kabinet hier actief gevolg aan in de vorm van concrete voorstellen (concreet: aanpassingen van de concept verordening) waarmee wordt beoogd dit standpunt te bestendigen in de verordening – óók als dat betekent dat de bepalingen uit de Verordening niet meer technologische- neutraal van aard zijn. Samen met lidstaten met een gelijkluidende opvatting zal worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele, subsidiaire en effectieve manier online seksueel kindermisbruik aan te pakken.

Bij de beoordeling van de beoogde maatregelen genoemd in de verordening is het belangrijk om onderscheid te maken tussen enerzijds zorgen omtrent de beveiligingsmethodiek (end-to-end encryptie) en anderzijds de mogelijke privacy inbreuk die een beoogde maatregel kan opleveren. De maatregelen genoemd in de verordening kunnen worden uitgevoerd met behulp van technische middelen die end-to-end encryptie niet aantasten. Een expert van het Nederlands Forensisch Instituut heeft dit, in antwoord op vragen van uw Commissie tijdens een technische briefing over de verordening, desgevraagd ook toegelicht.[6] Het gaat hierbij uitsluitend om een beperkt aantal technische oplossingen – zoals opgesomd en uitgebreid toegelicht door de Commissie in de 'impact assessment' behorende bij de Verordening - die zien op 'on device scanning'. Echter, het feit dat bepaalde maatregelen kunnen worden uitgevoerd met behulp van technische middelen die end-to-end encryptie niet aantasten, betekent níet dat het kabinet zonder meer steun kan verlenen aan elk van deze maatregelen. Bij elk van de voorgestelde maatregelen moet immers afzonderlijk worden bepaald of de inbreuk die daarbij gepaard gaat (a) proportioneel, subsidiair en noodzakelijk is ten aanzien van het beoogde doel én (b) voldoende omkleed is van de nodige waarborgen – waaronder bijvoorbeeld toetsing door een gerechtelijke instantie. Zo is op basis van het huidige voorstel dit kabinet kritisch ten aanzien van het detectiebevel waarmee grooming kan worden opgespoord. Hierbij gaat het concreet om het scannen van geschreven berichten. Als dit enkel gebeurt op het apparaat waarvan het bericht wordt verstuurd en vóórdat het bericht wordt versleuteld, dan zou deze maatregel in potentie geen belemmering vormen voor de toepassing- en beschikbaarheid van end-to-end encryptie. Echter, de privacy-inbreuk die deze maatregel oplevert staat - op basis van het huidige voorstel – hoogstwaarschijnlijk niet meer in verhouding tot het beoogde doel daarvan. Mede hierom zal het kabinet in de onderhandelingen het standpunt uitdragen dat Nederland het detecteren van grooming exclusief bij de opsporingsinstanties wil houden.

Vraag
Heeft de minister kennisgenomen van de zeer kritische brief van de gezamenlijke privacy toezichthouders? Deelt de minister hun positie dat het voorliggende voorstel een te groot risico bevat dat communicatiediensten bij alle communicatie van alle burgers in de Europese Economische Ruimte (EER) mee zullen kijken én luisteren? Deelt de minister hun stelling dat er een groot risico is op ondermijning van het gebruik van end-to-end-encryptie? Deelt de minister hun positie dat het huidige voorstel niet voldoet aan de vereiste van noodzakelijkheid en proportionaliteit en dit gevaren met zich meebrengt?

Antwoord
Het kabinet heeft kennisgenomen van gezamenlijk brief van de European Data Protection Supervisor (EDPS) en European Data Protection Board (EDPB). De EDPS en de EDPB

[6] https://debatgemist.tweedekamer.nl/node/29579

geven in de conclusie van het rapport aan dat zij van mening zijn dat het voorstel ernstige problemen oplevert op het gebied van gegevensbescherming en privacy. Zij verzoeken de medewetgevers de voorgestelde verordening te wijzigen, met name om ervoor te zorgen dat de beoogde detectieverplichtingen voldoen aan noodzakelijkheid en evenredigheid en niet leiden tot een verzwakking of verslechtering van de encryptie in het algemeen. In de onderhandelingen over de voorgestelde verordening wordt duidelijk gemaakt dat het kabinet voorstellen die end-to-end encryptie onmogelijk maken niet steunt, conform de motie van het lid Van Raan c.s. en hetgeen daarover eerder met uw Kamer is gecommuniceerd. Bovendien zijn de kaders uit het kabinetsstandpunt over encryptie leidend voor de Nederlandse inbreng. Het kabinet kijkt kritisch naar de aspecten van het voorstel waarmee inbreuk wordt gemaakt op een aantal grondrechten en beoogt bijvoorbeeld te voorkomen dat het voorstel leidt tot algemene monitoring. Een inbreuk op het recht op privéleven, het recht op gegevensbescherming, het recht op vrijheid van meningsuiting en het telecommunicatiegeheim van burgers mag alleen als deze noodzakelijk is en voldoet aan de eisen van proportionaliteit en subsidiariteit en de bijzondere eisen van de Grondwet.

Vraag
Dan hebben de leden van de PvdD-fractie nog enige vragen over de cijfers waar de minister en de Europese Commissie zich op lijken te baseren. Hoeveel zicht is er op de meldingen en het verificatieproces om bijvoorbeeld vertekening door vals positieven of doublures te voorkomen? Welk deel van de genoemde cijfers gaat over de Europese Unie?

Antwoord
De Commissie refereert in haar ‘impact assessment’ behorende bij de concept Verordening aan Europese cijfers van seksueel kindermisbruik die jaarlijks beschikbaar worden gemaakt door het ‘National Centre for Missing and Exploited Children’ (NCMEC).[7] Zoals toegelicht in de Kamerbrief Uitvoering motie van het lid van Raan c.s. is dit centrum een van de belangrijkste bronnen van informatie over gevallen van seksueel kindermisbruik.[8] Omdat het merendeel van de elektronische communicatiediensten (waaronder sociale media) in de VS is gevestigd waar een strenge meldplicht bestaat om seksueel kindermisbruikmateriaal te rapporteren, komen jaarlijks tientallen miljoenen meldingen van seksueel kindermisbruik binnen via het NCMEC. Om te voorkomen dat vertekening plaatsvindt door vals positieven of doublures, wordt volgens het NCMEC - die de hierboven genoemde cijfers heeft gepubliceerd - meldingen beoordeeld voordat deze worden doorgegeven aan wetshandhavingsinstanties.[9]

Bij het geautomatiseerd controleren van berichten op materiaal van seksueel kindermisbruik kan het aantal vals positieven, indien nodig, tot een zeer laag percentage (bijvoorbeeld 0.01 procent) worden gebracht. Voor de detectie van bekend materiaal van seksueel kindermisbruik levert een dergelijk rigide standaard geen problemen op. Echter, voor onbekend materiaal van seksueel kindermisbruik zou een dergelijke standaard in de praktijk betekenen dat dit type materiaal maar marginaal wordt gedetecteerd. Indien gewenst is dat een aanzienlijk deel van het online seksueel kindermisbruik ook daadwerkelijk gedetecteerd wordt, zal bij het geautomatiseerd controleren van berichten op onbekend materiaal van seksueel kindermisbruik significante hoeveelheden vals positieven te verwachten zijn.[10]

---

[7] Zie https://www.missingkids.org/content/dam/missingkids/pdfs/pdf-thumbs/EU-2020v2021CyberTiplineData.pdf.
[8] Kamerstuk 26 643, nr. 908, d.d. 23 september 2022.
[9] Zie https://www.missingkids.org/gethelpnow/cybertipline.
[10] Anders gezegd is hier sprake van communicerende vaten, waarbij vooraf ingestelde marge vals-positieven

Mede hierom wordt door de Commissie, naast technische oplossingen om de effecten van vals positieven te verminderen, in haar voorstel aanbevolen om deze negatieve effecten te ondervangen middels oprichting van een Europees centrum. Met dit centrum wordt onder andere beoogd te voorkomen dat deze vals positieven de wetshandhavers bereiken en meer focus kan worden bereikt ten aan zien van de gevallen die hen wel bereiken. Ook kan het centrum optreden als schakel naar de dienstaanbieders en hen van de nodige informatie voorzien. Tenslotte kan het centrum de rechtshandhaving noodzakelijke inzichten bieden door, onder andere, betrouwbare statistieken te genereren met betrekking tot seksueel kindermisbruik.

Vraag
Tot slot, wanneer verwacht de minister het rapport van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) over de impact van encryptie op de opsporing en wanneer verwacht zij een appreciatie naar de Kamer te kunnen sturen?

Antwoord
Dit verwacht ik in het eerste kwartaal van 2023 aan uw Kamer te sturen. De vraag of dit rapport vergezeld zal worden van een beleidsreactie zal afhangen van de inhoud van het rapport.

(bijvoorbeeld: het gedetecteerde materiaal mag maximaal 0,01 procent vals positieven bevatten) bepalend is voor de detectiegraad van materiaal van seksueel kindermisbruik: hoe strenger de marge wordt ingesteld, hoe lager de detectiegraad zal zijn.