Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 908

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 september 2022

Op 5 juli heeft uw Kamer de motie met Kamerstuk 26 643, nr. 885, ingediend door het lid Van Raan (PvdD), aangenomen (Handelingen II 2021/22, nr. 100, item 28). De motie is mede ingediend door de leden Van Baarle (DENK), Van Ginneken (D66), Leijten (SP) en Van Weerdenburg (PVV).

De motie verzoekt de regering end-to-end encryptie in stand te houden en (Europese) voorstellen die dat onmogelijk maken niet te steunen.

Aan het begin van deze brief wil ik duidelijk stellen dat we deze motie zullen uitvoeren. Echter, zoals geschetst in het Commissiedebat Online veiligheid en cybersecurity, is dit niet zonder dilemma's. Conform mijn toezegging tijdens het commissiedebat, schets ik deze hier beknopt.

End-to-end encryptie heeft een belangrijke rol in onze digitale maatschappij. Encryptie beveiligt informatie en communicatie en helpt daarmee het recht op eerbieding van de persoonlijke levenssfeer en het communicatiegeheim te borgen. Dat beschermt organisaties, bedrijven en burgers, waaronder kwetsbare groepen in landen met een repressief regime, tegen kwaadwillende actoren. Dit is ook belangrijk voor de uitoefening van de vrijheid van meningsuiting in binnen- en buitenland. Het stelt bijvoorbeeld burgers, maar ook beroepen met een belangrijke democratische functie zoals journalisten, in staat om vertrouwelijk te communiceren. 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. Encryptiemethoden zijn steeds sterker geworden en op veel apparaten en applicaties is het vaak standaard ingesteld. Dat biedt de samenleving grote voordelen.

Aan de andere kant stelt encryptie kwaadwillenden in staat om de inhoud van hun communicatie buiten het zicht van de opsporings-, inlichtingen-

kst-26643-908
ISSN 0921 - 7371
's-Gravenhage 2022

en veiligheidsdiensten te houden. Deze diensten vergaren informatie voor het opsporen van criminelen of het beschermen van onze nationale veiligheid. Dat doen zij op grond van wettelijke bevoegdheden, voorzien van passende voorwaarden en waarborgen. Voorbeelden daarvan zijn het onderzoeken van inbeslaggenomen telefoons en het aftappen van telecommunicatie. Deze diensten geven regelmatig aan dat dergelijke informatie vrijwel altijd van encryptie is voorzien en 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 uitvoering van de motie-Van Raan c.s. is relevant voor een aantal trajecten, waarvan ik er twee zal uitlichten: de onderhandelingen over de Conceptverordening inzake het tegengaan van online seksueel kindermisbruik en de inventarisatie naar rechtmatige toegang tot versleutelde informatie. Hieronder volgt een toelichting hoe bovenstaande dilemma's van toepassing zijn op deze trajecten en wordt aangegeven wat de uitvoering van de motie-Van Raan c.s. daarvoor betekent.

Conceptverordening inzake het tegengaan van online seksueel kindermisbruik

Het voorstel voor een Europese verordening ter voorkoming en bestrijding van online seksueel kindermisbruik bevat een regeling voor bevelen aan dienstverleners om bij specifieke diensten, waarvan is vastgesteld dat deze een hoog risico hebben om voor de verspreiding van beeldmateriaal van seksueel kindermisbruik en voor grooming te worden gebruikt, deze activiteiten te detecteren. De noodzaak van de voorstellen is volgens de Commissie onder meer gelegen in het groot aantal meldingen van online seksueel kindermisbruik dat jaarlijks wordt gedaan. Omdat het merendeel van de elektronische communicatiediensten (waaronder sociale media) in de VS is gevestigd, komen veel meldingen over seksueel kindermisbruik binnen via het Amerikaanse National Center for Missing & Exploited Children (NCMEC). Het NCMEC ontvangt jaarlijks miljoenen meldingen van beeldmateriaal van seksueel kindermisbruik. Daarbij valt het verschil zoals vermeld in het *impact assessment* van de Europese Commissie in het aantal meldingen op tussen vergelijkbare diensten met en zonder end-to-end versleuteling. Zo is Facebook Messenger – een dienst die niet end-to-end versleuteld is en maatregelen heeft geïmplementeerd om proactief materiaal van seksueel kindermisbruik te detecteren – de bron van meer dan de helft van de meldingen aan het NCMEC (meer dan 11 miljoen meldingen). WhatsApp, een dienst die wel end-to-end versleuteld is, is de bron van 400.000 meldingen.[1]

De Europese Commissie heeft enkele voorbeelden genoemd van mogelijkheden hoe materiaal dat seksueel kindermisbruik bevat kan worden gedetecteerd. Via het BNC-fiche is uw Kamer geïnformeerd dat er nog veel onduidelijkheid bestaat over de gevolgen van deze voorstellen voor de versleuteling van berichten, de inbreuk op de privacy en de waarborg van het briefgeheim.[2] Daarom neemt het kabinet een vragende, maar kritische, houding aan. Daarbij zal, samen met lidstaten met een gelijkluidende opvatting, worden gezocht naar oplossingen die recht doen

[1] Zie o.a. van de impact assessment (SWD(2022) 209) behorende bij de concept verordening ter voorkoming en bestrijding van seksueel kindermisbruik pp. 24–30.
[2] Kamerstuk 21 112, nr. 3455.

aan de wens om op een proportionele en effectieve manier online seksueel kindermisbruik te willen aanpakken en verschillende mogelijkheden inhoudelijk zorgvuldig te beoordelen.

In de uitvoering van de motie-Van Raan c.s. worden bij de onderhandelingen over de conceptverordening over het tegengaan van online seksueel kindermisbruik een aantal acties ondernomen. Zo wordt in de onderhandelingen duidelijk gemaakt dat Nederland voorstellen die end-to-end encryptie onmogelijk maken niet steunt. Daarnaast wordt in de Raad actief aansluiting gezocht bij lidstaten met een gelijkluidende opvatting als Nederland. Bij nieuwe ontwikkelingen zal uw Kamer geïnformeerd worden.

Alternatieven voor toegang tot versleuteld materiaal

De Cyber Security Raad (CSR) stelt in zijn advies over alternatieven voor het beperken van encryptie dat op korte dan wel middellange termijn geen oplossingen te verwachten zijn die aan alle verschillende belangen volledig tegemoet kunnen komen. Alternatieven voor het beperken van encryptie zijn daarom zeer wenselijk. In de uitvoering van de motie-Van Raan c.s. en in opvolging van het advies van de CSR zal ik mij namens het kabinet sterk inzetten voor alternatieve mogelijkheden die encryptie niet aantasten. Het advies van de CSR biedt hiervoor waardevolle aanknopingspunten, waarbij alle alternatieven die in het advies worden aanbevolen zullen worden bestudeerd. Tevens is recent de evaluatie van de bevoegdheid uit de Wet CCIII tot het binnendringen in een geautomatiseerd werk voltooid.[3]

De CSR stelt ook dat de geschetste alternatieven qua schaalbaarheid en voorspelbaarheid van de opbrengst niet te vergelijken zijn met het aftappen van reguliere telefonie via medewerking van aanbieders van openbare telecommunicatienetwerken en -diensten. Om de afweging tussen de beschermende waarde van encryptie en de beschermende waarde van de interceptiebevoegdheid goed te kunnen maken zal onderzoek worden gedaan naar technische oplossingen voor de toegang tot informatie voor de opsporings-, inlichtingen- en veiligheidsdiensten.

Conclusie

Het kabinet voert de motie-Van Raan uit en zal (Europese) voorstellen die end-to-end encryptie onmogelijk maken niet steunen. Ons gezamenlijke standpunt om end-to-end-encryptie niet onmogelijk te maken zal ik actief in de EU uitdragen, ook in het kader van het voorstel voor een verordening ter voorkoming en bestrijding van seksueel kindermisbruik.

Ondertussen blijft wetenschappelijk onderzoek naar rechtmatige toegang tot versleuteld materiaal mogelijk en gaat onze zoektocht naar mogelijkheden tot het verkrijgen van informatie voor het tegengaan en opsporen van strafbare feiten en het beschermen van de nationale veiligheid door. Bij nieuwe ontwikkelingen zal uw Kamer geïnformeerd worden.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

[3] WODC rapport «De hackbevoegdheid in de praktijk, een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)», 16 september 2022. Bijlage bij Kamerstuk 34 372, nr. 30.