Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

2095

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *de vacature «Senior beleidsmedewerker interceptie en digitale opsporing»* (ingezonden 4 februari 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 16 maart 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1922.

Vraag 1
Bent u bekend met bovenstaande vacature?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat de functie onder andere het onderzoeken naar de (voor- en nadelen van) mogelijkheden om communicatie van OTT-communicatiediensten, zoals Whatsapp, Signal e.d. op een proportionele wijze aftapbaar te maken, omvat? Zo ja, kunt u deze te verrichten werkzaamheden toelichten?

Antwoord 2
Ja, dat klopt. Als onderdeel van het onderzoek dat in de vacaturetekst wordt genoemd is er een inventarisatie gaande om mogelijkheden te onderzoeken voor rechtmatige toegang tot versleutelde digitale communicatie, om vervolgens de voor- en nadelen daarvan voor alle betrokken zwaarwegende belangen te analyseren. Daardoor wordt geïnformeerde en zorgvuldige besluitvorming door het kabinet en uw Kamer mogelijk. Tijdens deze inventarisatie wordt expliciet de mogelijkheid opengehouden dat geen proportionele oplossing zich aandient, waardoor voortgang op dit traject op dat moment niet prudent is. Hieronder volgt een nadere onderbouwing. Politie, het OM en de inlichtingen- en veiligheidsdiensten (IenV-diensten) geven al langere tijd aan dat het wijdverspreide gebruik van digitale communicatiediensten een negatieve impact heeft op de effectiviteit van de interceptiebevoegdheden. Dat komt onder meer door het volgende. Over-The-

[1] Werken voor Nederland, 25 januari 2022, «Senior beleidsmedewerker interceptie en digitale opsporing», www.werkenvoornederland.nl/vacatures/senior-beleidsmedewerker-interceptie-en-digitale-opsporing-JUSB-2022-0027#0

ah-tk-20212022-2095
ISSN 0921 - 7398
's-Gravenhage 2022

Top (OTT) communicatiediensten (OTT-communicatiediensten) worden praktisch door iedereen gebruikt. Deze OTT-communicatiediensten kennen geen wettelijke medewerkings- en aftapbaarheidsverplichtingen zoals aanbieders van openbare telecommunicatiediensten en -netwerken die wel hebben. Bovendien is er geen sprake van een ontsleutelplicht voor dergelijke aanbieders van communicatiediensten. Daarbovenop maken zij gebruik van een type versleuteling waardoor niet alleen opsporings- en IenV-diensten zijn uitgesloten van toegang tot deze communicatie, maar ook de aanbieders van de diensten zelf. Rechtmatige toegang is hierdoor niet mogelijk, ongeacht de bevoegdheden daartoe, passende juridische waarborgen of de ernst van het criminele feit of de dreiging.
De zorgen geuit door de opsporings- en IenV-diensten over de effectieve uitvoering van hun wettelijke taak neem ik serieus. Het betreft hier het vermogen van deze diensten om hun kerntaken uit te voeren: criminaliteit opsporen, verdachten voor de rechter brengen en de Nederlandse veiligheid bewaken.
Tegelijkertijd ben ik mij er zeer van bewust dat het een bijzonder complex vraagstuk is met veel betrokken vakgebieden en belangen. Ook door dit kabinet wordt de noodzaak voor goede, sterke versleuteling van digitale communicatie onderschreven alsook het belang hiervan voor cybersecurity, nationale veiligheid en de bescherming van fundamentele rechten en vrijheden. Zie hiervoor ook het antwoord op vraag vier.
Uw Kamer is bekend met de initiatieven die door het vorige kabinet met betrekking tot de interceptie van communicatie via OTT-communicatiediensten in gang zijn gezet en de motivatie daarvoor, alsook de dilemma's die in dit vraagstuk naar voren komen en in deze beantwoording verder worden toegelicht. Naast deze nationale verkenning is in dit traject ook een initiatief op EU-niveau in gang gezet. Nederland staat niet alleen in de zoektocht naar een passende, rechtstatelijke oplossing voor dit bijzonder complexe vraagstuk. De Commissie heeft aangegeven in 2022 een «way forward» te willen voorstellen op dit dossier. Daarbij pleit ik ook structureel, mede in EU verband, voor een transparant proces waarbij de samenwerking met het bedrijfsleven, opsporingsdiensten, het maatschappelijk middenveld en de wetenschap wordt gezocht. Gedurende het EU traject vindt ook afstemming plaats tussen mijn Ministerie en de I&V-diensten.

Vraag 3
Wat is volgens u het uiteindelijke doel van het onderzoeken naar de mogelijkheden om communicatie van OTT-diensten op een proportionele wijze aftapbaar te maken? Hoe verhoudt dit doel zich tot het bredere cybercrime beleid?

Antwoord 3
Zoals ik in mijn antwoord op vraag 2 heb aangegeven is het doel van de inventarisatie om geïnformeerde en zorgvuldige besluitvorming mogelijk te maken door dit kabinet en uw Kamer. Indien een mogelijke oplossing voor interceptie van versleutelde communicatie via OTT-communicatiediensten wordt gevonden, dan moet men goed inschatten wat de impact is op de cybersecurity, nationale veiligheid en bescherming van fundamentele rechten en vrijheden, zoals eerbiediging van de privacy. Indien een proportionele oplossing zich niet aandient, moeten we bijvoorbeeld ook goed analyseren wat dit betekent voor de mogelijkheden van de opsporing en IenV-diensten om criminaliteit op te sporen en onze maatschappij veilig te houden.
Dit traject staat los van het cybercrime beleid. De beschermende waarde van encryptie om te voorkomen dat criminelen toegang krijgen tot persoonlijke gegevens staat niet ter discussie. Daarbij moet ook worden bedacht dat rechtmatige toegang tot versleutelde communicatie ook de veiligheid van de maatschappij en burgers kan verbeteren doordat illegale inhoud kan worden erkend, onderschept, verwijderd en slachtofferschap wordt voorkomen of geminimaliseerd. De interceptiebevoegdheid kan worden gebruikt voor de bestrijding van vele soorten criminaliteit. Daarbij gelden passende juridische waarborgen: er moet toestemming worden verleend door een bevoegde autoriteit – de rechter-commissaris bij de inzet ten behoeve van de opsporing – die in concrete gevallen telkens een proportionaliteitsafweging maakt.
Ook in opsporingsonderzoeken naar misdrijven die alleen in de fysieke wereld worden gepleegd communiceren verdachten onderling of met derden

over de planning of uitvoering van het misdrijf via OTT-communicatiediensten. Gegeven het belang van de interceptiebevoegdheid voor vele typen criminaliteit en de ontwikkeling in het gebruik van OTT-communicatiediensten is het WODC gevraagd om onderzoek te doen naar de impact van encryptie op de opsporing. Dit onderzoek kan helpen bij de weging van de proportionaliteit van een eventuele oplossing.

Vraag 4
Hoe kijkt u naar het gebruik van end-to-end encryptie door OTT-communicatiediensten zoals Whatsapp en Signal? Wat zijn volgens u hier de voor- en nadelen van?

Antwoord 4
Ook dit kabinet erkent het belang van de ontwikkeling, beschikbaarheid en het gebruik van encryptie. Het is van groot belang de vertrouwelijkheid en integriteit van digitale communicatie en opgeslagen data te beschermen. Dat is belangrijk voor de eerbiediging van de persoonlijke levenssfeer, het vertrouwen van mensen in digitale producten en diensten en voor de Nederlandse economie in het licht van de digitale maatschappij. Dit kabinet stelt zich in het coalitieakkoord ook ten doel om privacy van burgers te verbeteren, fundamentele burgerrechten online te erkennen en veilige digitale communicatie te versterken.
In het coalitieakkoord wordt echter ook een ambitieuze agenda neergelegd voor de aanpak van ondermijnende criminaliteit, radicalisering en extremisme, cybercriminaliteit en de slagkracht van de opsporings- en IenV-diensten. Interceptie van communicatie is voor het realiseren van deze doelen van belang.
De voor- en nadelen die gelden voor de versleuteling in het algemeen gelden ook voor end-to-end versleuteling. Zoals ik in antwoord op vraag twee reeds benoemd heb, zijn door de implementatie van dit type versleuteling opsporings- en IenV-diensten uitgesloten van rechtmatige toegang tot deze communicatie via de aanbieder. Ongeacht de passende juridische waarborgen of de ernst van het criminele feit of de dreiging. Dit heeft tot gevolg dat opsporings- en IenV-diensten meer aangewezen zijn op alternatieve mogelijkheden om alsnog toegang tot de informatie te verkrijgen, zoals bijvoorbeeld de bevoegdheid tot Opname van Vertrouwelijke Communicatie (OVC) of het op afstand binnendringen in een geautomatiseerd werk.
De effectiviteit van de wet die deze laatste bevoegdheid mogelijk maakt wordt op dit moment geëvalueerd door het WODC, het rapport verwacht ik in de eerste helft van 2022. In het algemeen kan worden gesteld dat deze bevoegdheden minder schaalbaar en de effectiviteit er van beperkt voorspelbaar zijn vanwege de vereiste expertise, de kostbaarheid van de uitvoering, de capaciteit die dit vraagt en de vraag of het de opsporings- en inlichtingendiensten überhaupt lukt om toegang te krijgen en te houden tot de gewenste communicatie. Betrouwbare en voorspelbare toegang tot informatie is een belangrijk element in dit vraagstuk.

Vraag 5
Wat zijn volgens u de voor- en nadelen van het aftappen van OTT-communicatiediensten zoals Whatsapp? Kunt u deze toelichten?

Antwoord 5
Dit is de kernvraag van de inventarisatie die in gang is gezet en hangt af van de mogelijke oplossingen, indien zich een proportionele oplossing aandient. Nederland zet nu primair in op het eerdergenoemde EU-traject. In de tussentijd zal nationale gedachtevorming doorgaan om onder andere een betekenisvolle rol te spelen in dit traject. Daarbij zet ik mij in, zowel nationaal in EU-verband, voor een transparant proces waarbij de samenwerking met het bedrijfsleven, het maatschappelijk middenveld en de wetenschap wordt gezocht.

Vraag 6
Op welke wijze zou volgens u überhaupt de communicatie van deze OTT-diensten op proportionele wijze aftapbaar kunnen worden gemaakt? Kunt u dit toelichten?

Antwoord 6
Dit punt is onderwerp van de inventarisatie. Ik kan hierop nog geen antwoord geven. Ik zal uw Kamer indien het onderzoek resultaten heeft opgeleverd informeren over de uitkomsten en meenemen in de weging en verdere gedachtenvorming. Dat doe ik ook met een zeer brede groep van stakeholders: academici, het maatschappelijk middenveld, OTT-communicatiediensten, opsporings- en IenV-diensten.