Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 729

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 december 2020

Op 14 december heeft de Raad een resolutie aangenomen welke het startpunt vormt om tezamen met internet dienstverleners een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs. In opvolging van mijn toezegging richting het lid Yeşilgöz-Zegerius (VVD) tijdens de begrotingsbehandeling van 26 november jl. informeer ik bij deze uw Kamer over de voorgenomen inventarisatie.

Sterke encryptie is en blijft een belangrijk beginsel voor de veiligheid van onze maatschappij, het bedrijfsleven en de overheid. Tegelijkertijd moeten we oog hebben voor het effect van encryptie op het werk van opsporingsinlichtingen en veiligheidsdiensten. Daarom steun ik het initiatief om in EU verband gezamenlijk te onderzoeken of technische oplossingen mogelijk zijn. Met deze resolutie worden geen onomkeerbare stappen gezet. Uit de inventarisatie van de Commissie komen hopelijk meerdere technische mogelijkheden die vervolgens kunnen worden afgewogen. Deze technische oplossingen moeten adequaat en evenwichtig zijn. Hierbij is het beginsel van de proportionaliteit van groot belang bij de beoordeling van eventuele mogelijkheden. Tevens moeten technische oplossingen werkbaar zijn, om deze reden worden technologie bedrijven bij de inventarisatie betrokken. Dit wordt hieronder nader toegelicht.

Noodzaak van toegang tot versleutelde data

De beschikbaarheid, het gebruik en de ontwikkeling van sterke encryptie moet blijvend worden aangemoedigd. Dit is belangrijk voor de systeem- en informatiebeveiliging van de maatschappij, bedrijven en overheid. Eveneens is dit belangrijk voor de bescherming van fundamentele rechten, zoals het recht op de persoonlijke levenssfeer en het communicatiegeheim. Tegelijkertijd kan het nadelige effect van versleuteling op de uitvoering van de wettelijke taak van opsporings- en inlichtingen en veiligheidsdiensten niet worden genegeerd. De resolutie van 14 december

kst-26643-729
ISSN 0921 - 7371
's-Gravenhage 2020

is de eerste stap in de inventarisatie of een betere balans in de afweging van beide gerechtvaardigde belangen mogelijk is.

Rechtmatige toegang tot digitale gegevens is steeds belangrijker voor bevoegde autoriteiten om strafbare feiten op te sporen en de nationale veiligheid te beschermen. Dit geldt bijvoorbeeld voor de aanpak van zware en ernstige criminaliteit en terrorisme. In onze digitale samenleving is bewijs immers steeds vaker alleen digitaal beschikbaar. Tegelijkertijd wordt toegang tot deze informatie door encryptie belemmerd of is dit praktisch onmogelijk. Bijvoorbeeld wanneer door encryptie geen effectieve toegang tot gegevens kan worden verkregen via een vordering aan een dienstverlener. Dit beperkt ook de mogelijkheden van dienstverleners zelf om criminele actoren via hun dienst te weren en criminele activiteiten tegen te gaan. Tevens zijn de uitkomsten van de EU inventarisatie relevant voor het onderzoek naar mogelijkheden om toegang te verkrijgen tot communicatie via OTT-diensten[1].

Om deze redenen beoogt de inventarisatie naar technische oplossingen de beschermende waarde van versleuteling hoog te houden, terwijl de negatieve effecten voor opsporings- en inlichten en veiligheidsdiensten worden verminderd.

Adequaat en evenwichtig

Een technische oplossing moet adequaat en evenwichtig zijn. Belangrijk hierbij zijn de principes van proportionaliteit en subsidiariteit. Ten eerste moet de technische oplossing proportioneel zijn en bijdragen aan een veilige maatschappij of de bescherming van kwetsbaren in onze samenleving. Het middel moet aanvaardbaar zijn, dit betekent dat er geen onverantwoorde beslissingen worden genomen wanneer het de (digitale) veiligheid van burgers, het bedrijfsleven en de overheid aangaat. In de besluitvorming omtrent een eventuele technische oplossing is ook het effect op de uitvoering van fundamentele rechten belangrijk, zoals het recht op eerbiediging van de persoonlijke levenssfeer, het communicatiegeheim en de uitoefening van de vrijheid van meningsuiting. Dit geldt ook voor de bescherming van journalisten en de verdedigers van mensenrechten in repressieve regimes.[2] Het recht op privacy is echter niet absoluut. Artikel 8 van het EVRM bepaalt dat een staat dit recht mag beperken, als dat bij de wet is voorzien en in een democratische samenleving noodzakelijk is op grond van een aantal nader aangegeven gronden, waaronder de nationale veiligheid en het voorkomen van strafbare feiten.[3]

Indien een acceptabele technische oplossing wordt gevonden, moet ten tweede de inzet van de eventuele technische oplossing proportioneel en subsidiair zijn in de opsporingspraktijk. Een technische oplossing zou moeten kunnen worden ingezet ter bestrijding van zware criminaliteit zoals ernstige of georganiseerde misdrijven, cybercrime, zedendelicten als kinderporno of terrorisme. Ook moet de inzet van de bevoegdheid door de opsporing – zoals voor alle opsporingsbevoegdheden geldt – niet met minder ingrijpende bevoegdheden hetzelfde resultaat kunnen bereiken.

In de geannoteerde agenda voor de JBZ-raad van december als in het schriftelijk overleg heb ik reeds de voorwaarden en waarborgen geschetst die bij de inventarisatie in acht worden genomen.[4] In de Raadsresolutie

---

[1] Kamerstuk 28 684, nr. 621
[2] Kamerstukken 32 317, 22 112, 35 535 en 29 279, nr. 662
[3] Kamerstuk 32 761, nr. 174
[4] Kamerstuk 32 317, nr. 661; Kamerstukken 32 317, 22 112, 35 535 en 29 279, nr. 662

wordt ook opgeroepen om de EU-coördinatie te verbeteren op onderwerpen zoals het vinden van innovatieve mogelijkheden bij nieuwe technologieën en het analyseren van technische en operationele oplossingen om digitale opsporingsmogelijkheden te verbeteren.

Kabinetsstandpunt 2016

Ten slotte geef ik een toelichting over hoe dit traject zich verhoudt tot het kabinetsstandpunt inzake encryptie.[5] In het kabinetsstandpunt staat dat er geen zicht is op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. De conclusie in het standpunt luidt dat «het kabinet van mening [is] dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.»[6]

Tegelijkertijd heeft «het kabinet tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie.»[7] Daarnaast werd geconstateerd dat gelet op dit belang dat encryptie noopt tot het zoeken naar nieuwe oplossingen. Gegeven de afhankelijkheid van samenwerking met aanbieders, is overleg nodig met hen over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.[8]

Via de EU-inventarisatie naar rechtmatige toegang tot versleuteld bewijs wordt invulling gegeven aan het zoeken naar nieuwe oplossingen voor effectieve gegevensverstrekking. Zoals eerder aan uw Kamer gemeld wordt bij inventarisaties gestreefd om binnen het kabinetsstandpunt te blijven.[9]

Uit het bovenstaande blijkt dat in het kabinetsstandpunt van 2016 het grote belang van encryptie wordt benadrukt en daarbij erkent dat dit (tijdig) inzicht door bevoegde autoriteiten in digitale gegevens bemoeilijkt, vertraagt of het geheel onmogelijk maakt. Sinds 2016 heeft de digitale ontwikkeling niet stilgestaan, zowel op het vlak van versleuteling als nieuwe bevoegdheden van de opsporing. Daarom heb ik het WODC gevraagd om het effect van encryptie op de opsporing nader te onderzoeken. Dit geactualiseerde beeld helpt bij de weging van de proportionaliteit van een eventuele oplossing.

Motie inzake het verbieden van encryptie

Op 11 november jl. heeft het lid Baudet(FvD) een motie ingediend die constateert dat binnen de EU stemmen opgaan om het versleutelen van digitale berichten te verbieden, zodat overheden mee kunnen lezen.[10] De motie roept de regering op zich tegen deze ontwikkeling te verzetten en niet akkoord te gaan met enig voorstel om versleuteling van berichtgeving te verbieden. Deze motie is door uw Kamer aangenomen.

---

[5] Kamerstuk 26 643, nr. 383
[6] Idem.
[7] Idem.
[8] Idem.
[9] Aanhangsel Handelingen II 2019/20, nrs. 758 en 1095
[10] Kamerstuk 21 501-02, nr. 2232

Er is geen sprake van een voornemen om versleuteling te verbieden en het kabinet zal het verbieden van encryptie in de toekomst niet steunen.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus