Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

36 084

Wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders

Nr. 6

VERSLAG

Vastgesteld 2 juni 2022

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van bovenstaand wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering op de gestelde vragen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

Inhoudsopgave

I. ALGEMEEN DEEL

1. Inleiding

De leden van de VVD-fractie merken op dat de behandeling van deze wetswijziging bij de Minister van Justitie en Veiligheid ligt, maar dat het toezicht van deze wijziging bij de Minister van Economische Zaken en Klimaat ligt. Kan de regering uiteenzetten hoe de verdeling van taken en verantwoordelijkheden ligt bij de ministers en of er knelpunten worden

kst-36084-6
ISSN 0921 - 7371
's-Gravenhage 2022

ervaren? Deze leden volgen de ontwikkelingen omtrent de richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn) op de voet. Kan de regering uiteen zetten of en welke gevolgen dit gaat hebben voor de uitvoering van deze wet?

De leden van de PVV-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en hebben nog enkele vragen en opmerkingen over het wetsvoorstel. Deze leden signaleren dat de Afdeling Advisering van de Raad van State van mening is dat in het wetsvoorstel onvoldoende wettelijk is gewaarborgd dat schakelorganisaties het vereiste niveau van beveiliging en privacybescherming hebben op het moment dat zij worden aangewezen. Toch ziet de regering geen reden beveiligingsverplichtingen voor organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's) in de wet op te nemen. Deze leden vragen waarom de regering van dit advies is afgeweken en hoe nu kan worden gegarandeerd dat de schakelorganisaties aan het vereiste niveau van beveiliging en privacybescherming (blijven) voldoen.

De leden van de CDA-fractie hebben met instemming kennisgenomen van het onderhavige wetsvoorstel. Deze leden hebben naar aanleiding hiervan geen vragen.

De leden van de SP-fractie hebben het voorstel voor wijziging van de Wet beveiliging- en informatiesystemen gelezen en hebben hierover nog enkele vragen en opmerkingen. Deze leden maken van de gelegenheid gebruik eerst een opmerking te maken over het doorlopen proces. De regering heeft verzocht vooruit te kunnen lopen op deze wetswijziging vanwege de toenemende digitale dreiging door de oorlog in Oekraïne. Hoewel deze leden deze digitale dreiging erkennen, zijn zij verbaasd over deze argumentatie. Er is veelvuldig door verschillende organisaties gewaarschuwd voor digitale dreigingen, onder meer door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Daarbij zijn er inmiddels meerdere aanvallen geweest, ook al in eerdere jaren. Waarom heeft deze wijziging dan zo lang op zich laten wachten?

De leden van de GroenLinks-fractie zien cybersecurity als randvoorwaarde van een digitaliserende samenleving en overheid, en het uitwisselen van informatie is hier onderdeel van. Maar bij meer verantwoordelijkheden, hoort ook gepast toezicht en gepaste verantwoordingsmechanismen. Deze leden zien dat de groei in digitale aanvallen op «andere aanbieders» gelijk gaat met een groeiende afhankelijkheid van meer aanbieders en minder ICT-leveranciers.

De leden van de Volt-fractie hebben met interesse kennisgenomen van het wetsvoorstel tot Wijziging van de Wet beveiliging netwerk- en informatiesystemen. Dit wetsvoorstel komt tegemoet aan een wens om organisaties en bedrijven beter op de hoogte te kunnen brengen van dreigingssituaties, met als doel de cyberweerbaarheid van Nederland te vergroten. Dat kan alleen met de juiste waarborgen. Over het wetsvoorstel hebben deze leden dus nog enkele vragen.

2. Aanleiding voor het wetsvoorstel

De leden van de GroenLinks fractie vragen of het begrip «andere aanbieders» voldoende afgebakend is in de voorgestelde wetswijziging.

3. Inhoud van het wetsvoorstel

3.1 Delen van dreigings- en incidentinformatie met andere aanbieders

De leden van de VVD-fractie vragen of de regering kan toelichten of bedrijven zoals grote toeleveranciers van firewalls ook onder «andere aanbieders» zouden kunnen vallen.

De leden van de SP-fractie zien het belang van het voortijdig informeren van bedrijven en andere belanghebbenden in het geval van een digitale dreiging. Deze leden hebben daarom zelf gepleit voor de oprichting van het Digital Trust Center (DTC). Deze leden zien echter ook het gevaar dat er veel werk dubbel wordt gedaan, of werk blijft liggen omdat geen van de organisaties zich verantwoordelijk voelt, of organisaties zelfs elkaar gaan tegenwerken. Waarom is er niet gekozen voor één verantwoordelijke organisatie?

De leden van de GroenLinks-fractie vinden het opmerkelijk dat informatie van «andere aanbieders» die nu verkregen wordt «rest data» of «bijvangst» genoemd wordt. Betekent dit dat het Nationaal Cyber Security Centrum (NCSC) niet op zoek was naar gegevens over «andere aanbieders», maar dit nu toevallig tegenkomt? Hoe past dit in de principes van doelbinding en dataminimalisatie van de Algemene verordening gegevensbescherming (AVG)?

De leden van de Volt-fractie merken allereerst op dat de definitie «andere aanbieders» erg ruim is. Hierdoor wordt het in theorie mogelijk om alle bedrijven en organisaties in Nederland te informeren. Dat betekent tegelijkertijd dat er een omvangrijke verwerkingsgrondslag wordt gecreëerd. Daarover maken deze lezen zich, in lijn met de Autoriteit Persoonsgegevens, zorgen. De bepaling is onvoldoende gespecificeerd en daarmee onvoldoende kenbaar en voorzienbaar, zoals wordt bedoeld in rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), zeker nu er nog geen besluit is genomen waarin de OKTT's worden aangewezen. Kan de regering toelichten welke aanbieders zij voor ogen heeft met dit wetsvoorstel? Kan dit nader gespecificeerd worden, wellicht niet op individueel niveau, maar wel op het niveau van categorieën? Is er vanuit het verleden kennis opgebouwd over het type aanbieders dat met dit wetsvoorstel beoogd wordt? Zo ja, welk type aanbieder is dit? Wat bedoelt de regering concreet met «andere aanbieders»?

3.2 Delen van vertrouwelijke herleidbare gegevens over aanbieders met OKTT's

De leden van de PVV-fractie hebben kennisgenomen van de verwachting van de regering dat de wijzigingen geen aanpassingen van ICT-systemen zouden vergen. Wel moeten een aantal werkprocessen worden aangepast. De leden vragen of dit ook geldt voor de OKTT's. Volgens de regering zijn er geen financiële gevolgen voor de OKTT's, omdat het aan deze partijen zelf is om te bepalen hoe zij omgaan met de ontvangen dreigings- en incidentinformatie. De leden vragen of de regering wel voorbereid is op eventuele logistieke en financiële ondersteuning van OKTT's.

De leden van de VVD-fractie lezen dat de regering geen aanleiding ziet om beveiligingsverplichtingen voor OKTT's in de wet op te nemen. Welke negatieve gevolgen ziet de regering om deze beveiligingsverplichtingen in de wet op te nemen?

De leden van de GroenLinks-fractie vragen of de regering nader kan definiëren welke organisaties zij als OKTT's ziet. Is dit bijvoorbeeld altijd een stichting? Waarom is er gekozen om OKTT's aan te wijzen per ministeriele aanwijzing, in plaats van ministeriele regeling? Deze leden lezen dat er bij het aanwijzen van een OKTT getoetst wordt of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen met betrekking tot de netwerk- en informatiesystemen hebben genomen. Wordt dit na deze initiële toets, daarna stelselmatig gecontroleerd? Zo ja, door wie? Ook lezen deze leden dat er wordt beoordeeld of de betrokken schakelorganisatie afdoende maatregelen heeft genomen om persoonsgegevens rechtmatig te verwerken. Door wie wordt dit beoordeeld? Is dit wellicht een taak voor de Autoriteit Persoonsgegevens, die de kennis en kunde hebben hiervoor? Waarom is deze grote hoeveelheid organisaties die geen vitale aanbieder of aanbieder is die onderdeel is van de rijksoverheid, niet aangesloten bij een, bij minsteriele regeling aangewezen, computercrisisteam? Hoe voorkomt de regering dat er overlap in verantwoordelijkheden komt door de toename van schakelorganisaties die als OKTT of computercrisisteam worden aangewezen? Is de AVG, volgens de regering, van toepassing op het verstrekken van persoonsgegevens door OKTT's?

De leden van de Volt-fractie merken op dat voor zover herleidbare gegevens over aanbieders met OKTT's worden gedeeld kan hier ook sprake zijn van persoonsgegevens, waaronder persoonsgegevens betreffende strafbare feiten als bedoeld in art. 10 AVG. Welke aanvullende maatregelen treft de regering om het verwerken van deze gegevens toe te staan, nu de verwerking ervan in beginsel verboden is? Hoe wordt bijvoorbeeld omgegaan met restdata en bijvangst en wie is daarvoor de verwerkingsverantwoordelijke? Kan de regering een lijst geven van de schakelorganisaties, OKTT's, computercrisisteams en andere aanbieders die vallen onder artikel 3, tweede lid a t/m e? Hoe wordt bepaald welke organisaties hier tot toe mogen treden? Wat is het toetsingskader aan de hand waarvan organisaties kunnen worden toegevoegd aan de lijst? De regering geeft in de memorie van toelichting aan dat zowel publieke als private organisaties, zoals bedoeld in het voorgestelde artikel 3, tweede lid, onder e, zelf verantwoordelijk zijn voor het bepalen van de basis waarop zij die informatie verder verwerken. Vertrouwt de regering erop dat de juiste waarborgen in acht worden genomen door deze organisaties om de rechtmatigheid en veiligheid van de verdere verwerking te garanderen? Hoe kan dat worden gecontroleerd?

4. Verhouding NCSC – Digital Trust Center (DTC)

De leden van de VVD-fractie zouden graag willen weten hoe de «andere aanbieders» worden geïnformeerd over deze wetswijziging. Kan er met deze wetswijziging onduidelijkheid ontstaan voor «andere aanbieders» over waar ze terecht moeten wanneer er een cyberdreiging is? Zo ja, hoe wordt dit opgelost? Zo nee, waarom niet? Deze leden vragen daarnaast of deze wetswijziging juist niet een mooi moment kan zijn om het NCSC en DTC nog beter en intensiever samen te laten werken. Zo ja, op welke manier gaat dit ingevuld worden? Zo nee, waarom niet?

De leden van de PVV-fractie merken op dat het door de overlap in taakstelling tussen het NCSC en het DTC kan zijn dat er in tijden van crisis onduidelijkheden ontstaan omtrent de taken, bevoegdheden en/of rolverdeling van de organisaties. In de memorie van toelichting heeft de regering dit nader geprobeerd te concretiseren en wordt aangegeven dat de Wet bevordering digitale weerbaarheid bedrijven de taken van het DTC verder zal verduidelijken. Voor deze leden blijft het dan ook de vraag of, ook los van de Wet bevordering digitale weerbaarheid, de taken,

bevoegdheden en/of rolverdeling van de respectievelijke organisaties met dit wetsvoorstel wel voldoende zijn geconcretiseerd en welke mogelijke aanpassingen van organisatorische aard de regering overweegt om een einde te maken aan de overlap in taakstelling.

5. Verhouding tot hoger recht

5.1 Inleidende opmerkingen

De leden van de Volt-fractie merken op dat het concept van de NIB-richtlijn op 13 mei 2022 gereed was en nu ter beoordeling ligt. Het is aannemelijk dat hier weinig aan veranderd wordt, aangezien de BNC-fiches hier al in zijn verwerkt. Is het huidige wetsvoorstel van de Wbni voldoende voorbereid op de implementatie van deze richtlijn?

5.2 EVRM

De leden van de Volt-fractie merken op dat de regering in de memorie van toelichting schrijft, ten aanzien van de dringende maatschappelijke behoefte, dat de samenleving in grote mate afhankelijk is van elektronische informatiesystemen, die onderling verweven zijn. Daarbij is het voorstelbaar dat het NCSC dreigingsinformatie moet delen, maar het gegeven – dat er grote afhankelijkheid bestaat – alleen, zegt nog niets over de maatschappelijke behoefte. Kan de regering aangeven in hoeverre er een concrete dreiging is die het NCSC noodzaakt om informatie te delen? Waaruit bestaat die dreiging precies? Of is het slechts een potentiële dreiging? Welke andere maatregelen kunnen eveneens getrokken worden om dreigingen te verminderen? In de memorie van toelichting schrijft de regering dat de voorgestelde nieuwe taak om persoonsgegevens aan andere aanbieders te verstrekken, gelet op de aard ervan, het doel en de overige waarborgen waarmee deze verwerking is omkleed, geen forse inmenging in het recht op respect voor iemands privéleven oplevert. Kan de regering dit nader toelichten? Welke waarde hecht zij aan de aard, het doel en de verschillende waarborgen? Met andere woorden, hoe worden deze factoren ingekleurd? Door het ontbreken van de toelichting daarop, kan deze conclusie niet worden gewaardeerd door deze leden.

6. Toezicht en handhaving

Het verbaast de leden de GroenLinks-fractie dat er geen sprake zou zijn van toezicht op en handhaving van de naleving van verplichtingen. Worden hier geen gegevens uitgewisseld en verwerkt? Krijgen de OKTT's aanzienlijke bevoegdheden, zonder toezicht op de wijze waarop zij dit gaan uitvoeren? Deze leden lezen dat er bij aanwijzing als OKTT, de schakelorganisatie een verklaring ondertekent waarin is opgenomen dat aan het NCSC melding wordt gemaakt van onder meer belangrijke wijzigingen van de getroffen (technische en organisatorische) beveiligingsmaatregelen of van de doelgroep en de taken die ten behoeve van die doelgroep worden verricht. Acht de regering deze zelfrapportage voldoende op rechtmatige omgang met persoonsgegevens te garanderen?

7. Advies en consultatie

7.1 Autoriteit Persoonsgegevens

De leden van de GroenLinks-fractie lezen dat de regering IP-adressen in dit verband niet ziet als persoonsgegevens betreffende strafbare feiten in de zin van artikel 10 AVG. Kan de regering nader motiveren waarom dit niet het geval zou zijn? Deze leden lezen dat het doel niet is om

handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. Betekent dit dat er niet strafrechtelijk opgetreden gaat worden tegen deze partijen wanneer blijkt dat zij aanvallen plegen op de informatiehuishouding van «andere aanbieders»? Daarnaast verbaast het deze leden dat de regering het advies van de Autoriteit Persoonsgegevens om met een betere afbakening van het begrip «andere aanbieders» te komen, afwijst. Dit vinden deze leden kwalijk. Het is van groot belang om expliciet en concreet te zijn in het geval van gegevensuitwisseling. Op dit moment, worden «andere aanbieders» voornamelijk gedefinieerd op kenmerken die zij niet hebben, zoals «niet een vitale aanbieder» of «een aanbieder die geen schakelorganisatie heeft». Kan de regering nader uitleggen waarom er gekozen is deze organisaties te definiëren met kenmerken die zij niet hebben, in plaats van kenmerken die zij wel hebben? Deze leden zien ook dat de Autoriteit Persoonsgegevens adviseert aan te geven welke grondslag van verwerking van toepassing is op de verwerking door publieke aanbieders. De regering geeft aan dat de voorliggende wet de grondslag voor het delen van deze gegevens regelt en dat organisaties zelf verantwoordelijk zijn voor de grondslag waarop zij dat verwerken. Waarom is er gekozen om organisaties zelf verantwoordelijk te stellen voor het bepalen van de grondslag op basis waarvan zij informatie verwerken? Dreigt hierdoor niet een lappendeken aan wettelijke grondslagen? Vindt de regering dit wenselijk?

7.2 Cyber Security Raad (CSR)

De leden van de PVV-fractie hebben kennisgenomen van het advies van de Cyber Security Raad (CSR) die adviseert om meer helderheid te verschaffen richting bedrijven en maatschappelijke organisaties over wat zij van de verschillende partijen in het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden (LDS) kunnen verwachten. Daarbij heeft de CSR het advies herhaald om, in afwachting van de afwikkeling van de wijziging van de Wbni, nu al tot het delen van incidentinformatie met OKTT's over te gaan. De leden vragen of de regering van plan is om aan dit advies invulling te geven en hoe de regering dit gaat doen. Wat zijn de concrete plannen van de regering op dit punt?

7.3 OKTT's

De leden van de GroenLinks-fractie delen de zorg dat «bijzondere gevallen» een onvoldoende objectief en onvoldoende duidelijk criterium betreft. Het NCSC beoordeelt per geval of wordt voldaan aan de genoemde vereisten. Hoe garandeert de regering het voorkomen van willekeur bij deze beoordeling?

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Tilburg