Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

34 388 Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)

A

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR VEILIGHEID EN JUSTITIE[1]

Vastgesteld 17 januari 2017

Het voorbereidend onderzoek heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de **VVD**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity. Zij hebben nog enkele vragen.

De leden van de fractie van **D66** hebben met belangstelling kennisgenomen van het wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity. Zij erkennen het belang van het adequaat beschermen van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving, maar hebben wel vragen en zorgen bij dit wetsvoorstel.

De leden van de **PvdA**-fractie hebben met belangstelling kennisgenomen van dit wetsvoorstel. Zij zien het belang van het creëren van een wettelijke verplichting tot het melden van ICT-inbreuken die een serieuze bedreiging kunnen vormen voor de beschikbaarheid of betrouwbaarheid van voor de Nederlandse samenleving vitale producten of diensten. Zij hebben echter wel nog enkele vragen bij de uitwerking van het wetsvoorstel.

[1] **Samenstelling:**
Kox (SP), Engels (D66), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA) (*vicevoorzitter*), Duthler (VVD) *(voorzitter),* Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Backer (D66), Knip (VVD), Barth (PvdA), Beuving (PvdA), Hoekstra (CDA), Popken (PVV), Schouwenaar (VVD), Schrijver (PvdA), Bredenoord (D66), Van Dijk (SGP), Markuszower (PVV), Van Rij (CDA), Rombouts (CDA), Van Weerdenburg (PVV), Wezel (SP), Van de Ven (VVD), Bikker (CU)

kst-34388-A
ISSN 0921 - 7371
's-Gravenhage 2017

2. Effectiviteit meldplicht

Ingevolge het wetsvoorstel geeft een vitale aanbieder de Minister van Veiligheid en Justitie onverwijld kennis van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken. Er bestaat reeds al een publiek-private samenwerking tussen relevante partijen, waarbinnen nut en noodzaak van het delen van vertrouwelijke gegevens met betrekking tot de ICT-inbreuken bovendien breed wordt gedragen. Op grond daarvan zette de Afdeling advisering van de Raad van State in haar advies vraagtekens bij de toegevoegde waarde van de voorgestelde meldplicht.[2] Op welke concrete gronden acht de regering de huidige publiek-private samenwerking ontoereikend, zo vragen de fractieleden van **D66**. Heeft zij onderzoek gedaan naar deze huidige samenwerking? Kan de regering toelichten op welke specifieke gronden het voorgestelde wetsvoorstel wél ertoe gaat leiden dat partijen behorend tot de doelgroep van dit wetsvoorstel, alle ICT-inbreuken aan het Nationaal Cyber Security Centrum (hierna: NCSC) zullen melden?

In reactie op het advies van de Afdeling advisering van de Raad van State stelde de regering dat het breed gedragen besef binnen de doelgroep van het wetsvoorstel met betrekking tot nut en noodzaak van het delen van vertrouwelijke gegevens over ICT-inbreuken met het NCSC, niet betekent dat alle ICT-inbreuken waarop de voorgestelde meldplicht ziet nu reeds aan het NCSC worden gemeld. Kan de regering aangeven hoe groot de problematiek met betrekking tot niet-gemelde ICT-inbreuken is, in het bijzonder de frequentie en omvang van niet-gemelde ICT-inbreuken waarop de voorgestelde meldplicht ziet? Zo niet, welke concrete aanwijzingen heeft zij met betrekking tot de door haar gestelde problematiek van niet-gemelde ICT-inbreuken, zo vragen de D66-fractieleden.

Daarnaast stelde de regering, zo merken de leden van de D66-fractie op, dat een wettelijke meldplicht zoals vervat in dit wetsvoorstel naar haar verwachting zal leiden tot een verdere vergroting van de meldingsbereidheid van vitale aanbieders, doordat het maatschappelijke belang van deze meldingen wordt benadrukt. Op welke concrete gronden baseert de regering haar stelling dat de meldingsbereidheid van vitale aanbieders wordt vergroot door een meldplicht op basis van een wet, ook zonder dat die wet voorziet in toezicht en sancties bij het niet voldoen aan die meldplicht? Heeft de regering onderzoek hiernaar gedaan?

3. Melding inbreuk

Bij de brief van 4 oktober 2016 heeft de Minister van Veiligheid en Justitie de nadere informatie verschaft aan de Tweede Kamer over de rol van het NCSC bij databeveiliging.[3] De leden van de **VVD**-fractie hechten grote waarde aan de voortgang om te komen tot een goede Wet gegevensverwerking en meldplicht cybersecurity. Gezien het belang van tijdig efficiënt handelen met betrekking tot ICT-inbreuken, vragen de voornoemde leden aan de regering binnen welke termijn deze inbreuken bij de Minister van Veiligheid en Justitie en de NCSC gemeld dienen te worden.
De memorie van toelichting stelt dat een inbreuk op de ICT-systemen van aanbieders slechts moeten worden gemeld wanneer «[deze] tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van deze producten of diensten in belangrijke mate wordt of kan worden onder-

[2] Kamerstukken II 2015/16, 34 388, nr. 4, p. 2–3.
[3] Kamerstukken II 2016/17, 34 388, nr. 7.

broken.»[4] Per sector zullen drempelwaarden worden vastgesteld om te bepalen of sprake is van «in belangrijke mate», zoals bedoeld in artikel 6 van het wetsvoorstel. De regering heeft in de nota naar aanleiding van het verslag aangegeven dat deze drempelwaarden per sector nader zullen worden uitgewerkt in richtsnoeren en uiteindelijk geformuleerd in criteria.[5] De voornoemde leden vragen de regering aan de hand van welke criteria deze drempelwaarden zullen worden vastgesteld en zij ontvangen graag het betreffende beleidsbesluit.

Dit wetsvoorstel regelt een meldplicht voor beveiligingsinbreuken. De VVD-fractieleden merken op dat de algemene verordening gegevensbescherming ook een meldplicht kent voor beveiligingsinbreuken die verband houden met persoonsgegevens, evenals onder meer de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp. Deze regelgeving kent een termijn van 72 uur waarbinnen deze inbreuken gemeld moeten worden. Onderhavige wet kent een termijn van «onverwijld». Als er sprake is van samenloop tussen beveiligingsincidenten die tevens verband houden met persoonsgegevens, bij wie moet de vitale aanbieder de inbreuken melden? Is dat slechts bij de Minister van Veiligheid & Justitie/NCSC, of ook bij de Autoriteit Persoonsgegevens? Dat laatste lijkt het meest voor de hand te liggen. Betrokkenen moeten immers ook op de hoogte kunnen worden gesteld indien het gaat om ernstige inbreuken op de beveiliging die mogelijk gevolgen hebben voor de bescherming van de persoonlijke levenssfeer.
De leden van de VVD-fractie voorzien dat organisaties te maken gaan krijgen met een veelvoud aan instanties waar gemeld moet gaan worden. Naast de NCSC en Autoriteit Persoonsgegevens moeten financiële instellingen immers beveiligingsincidenten onder bepaalde omstandigheden ook melden bij De Nederlandsche Bank (DNB) of de Autoriteit Financiële Markten (AFM) en telecombedrijven aan de Autoriteit Consument en Markt (ACM). Hoe wordt ervoor gezorgd dat steeds voldoende bekend is wie welke incidenten waar moet melden, en hoe wordt voorkomen dat de meldplicht een «administratief circus» wordt?

4. Vitale aanbieders

De normadressaten van het onderhavige wetsvoorstel betreffen vitale aanbieders die zijn aangewezen bij AMvB of behoren tot een daarbij omschreven categorie, voor wat betreft de producten of diensten die bij die maatregel zijn aangewezen of behoren tot een daarbij omschreven categorie[6]. Is de concepttekst van de AMvB reeds bekend, en zo ja, wil de regering die de leden van de **VVD**-fractie doen toekomen? Zo nee, wil zij aangeven van welke aanbieders zij voorziet dat deze in de AMvB worden aangewezen? Om een goed begrip van de reikwijdte van dit wetsvoorstel te kunnen krijgen, is inzicht in de voorgenomen normadressaten zeer wenselijk.

Ingevolge het wetsvoorstel bestaat een meldplicht voor vitale aanbieders (overheid en private sector) waarbij een ICT-inbreuk direct of indirect kan leiden tot maatschappelijke ontwrichting. Uit de memorie van toelichting volgt dat de (categorieën van) vitale aanbieders en hun concrete producten of diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij AMvB. Ook volgt uit de memorie van toelichting een aantal voorbeelden van sectoren met vitale aanbieders: elektriciteit, gas, drinkwater, telecom, financiën, overheid (waaronder in ieder geval primaire waterkeringen), transport (mainports Rotterdam en Schiphol) en

[4] Kamerstukken II 2015/16, 34 388, nr. 3, p. 1.
[5] Kamerstukken II 2015/16, 34 388, nr. 6, p. 8.
[6] Artikel 5 van het wetsvoorstel.

de nucleaire sector. De memorie van toelichting geeft ook enkele voorbeelden van vitale aanbieders: energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, banken en Rijkswaterstaat als beheerder van primaire waterkeringen.[7]
De leden van de fractie van **D66** maken uit de bewoordingen van de regering op dat de bovenstaande opsomming niet limitatief is. Welke onderdelen van de rijksoverheid en welke private organisaties worden precies als vitale aanbieders (privaat en publiek) aangemerkt? Mocht de regering deze duidelijkheid nog niet kunnen verschaffen, wanneer verwacht zij hierover meer duidelijkheid te kunnen verschaffen?

5. Verhouding tot Wet bescherming persoonsgegevens

De **PvdA**-fractieleden krijgen niet goed vat op de voorgestelde regeling in artikel 4 van het wetsvoorstel. Enerzijds is een op artikel 4, eerste lid, van het wetsvoorstel gebaseerd verzoek vrijblijvend, in die zin dat het voor de rechtspersoon (of het orgaan daarvan) tot wie het verzoek is gericht geen verplichting oplevert tot verstrekking van de gevraagde gegevens. Uit de memorie van toelichting blijkt dat de regering een dergelijke verplichting niet nodig acht. Een verplichting wordt alleen nodig gevonden voor een bij AMvB aangewezen vitale aanbieder die bij het NCSC een meldplichtige ICT-inbreuk heeft gemeld, in welke verplichting artikel 7 van het wetsvoorstel voorziet.[8] Anderzijds wordt een op artikel 4, eerste lid, van het wetsvoorstel gebaseerd verzoek door de regering toch weer zo belangrijk geacht, dat in het tweede lid van artikel 4 het doelbindingsvereiste van de Wet bescherming persoonsgegevens (hierna: Wbp) buiten toepassing wordt gesteld. Uit de memorie van toelichting en de inhoud van het wetsvoorstel blijkt dat het bij een op artikel 4, eerste lid, van het wetsvoorstel gebaseerd verzoek zelfs moet gaan om gegevens die *noodzakelijk zijn* voor het vervullen van de in artikel 2, eerste lid, van het wetsvoorstel genoemde taken («[...] ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van elektronische informatiesystemen van vitale aanbieders [...]»[9]). En met name als die vitale aanbieder niet tot de rijksoverheid behoort, meent de regering dat artikel 43 van de Wbp onvoldoende ruimte biedt om artikel 9, eerste lid, van de Wbp buiten toepassing te laten. Naar het oordeel van de regering rechtvaardigt het zwaarwegend algemene belang dat het NCSC zijn wettelijke taken kan vervullen, de voorgestelde afwijking van de Wbp.

De voornoemde leden vragen de regering hoe dit te rijmen is met het feit dat zij ervoor gekozen heeft het op artikel 4, eerste lid, van het wetsvoorstel gebaseerde verzoek vrijblijvend te laten zijn, in die zin dat de betreffende rechtspersoon (of een orgaan daarvan) niet verplicht is daaraan te voldoen. Zien zij het goed dat het belang dat het NCSC zijn wettelijke taken kan vervullen volgens de regering wel zo zwaarwegend is dat het doelbindingsvereiste van de Wbp geheel buiten toepassing kan worden gesteld, doch niet zo zwaarwegend dat een verplichting tot medewerking kan worden opgelegd aan de rechtspersoon tot wie het verzoek is gericht? En wat is dan nog de betekenis van het buiten toepassing stellen van het doelbindingsvereiste, als de betreffende rechtspersonen (of organen daarvan) toch zonder opgaaf van redenen kunnen weigeren om de gevraagde gegevens te verstrekken? De PvdA-fractieleden vragen de regering om bij het beantwoorden van deze vragen zo concreet mogelijk voorbeelden te geven van situaties waarin een verzoek als bedoeld in het voorgestelde artikel 4, eerste lid kan worden gedaan, waarin voldaan wordt aan de in dit artikel en in het

---

[7] Kamerstukken II 2015/16, 34 388, nr. 3, p. 4.
[8] Kamerstukken II 2015/16, 34 388, nr. 3, p. 26.
[9] Artikel 2, eerste lid, van het wetsvoorstel.

voorgestelde artikel 2, eerste lid, aanhef geformuleerde vereisten, waarin het belang dat het NCSC zijn wettelijke taken kan vervullen niet zo zwaarwegend is dat het nodig is dat de benodigde gegevens bij de betreffende rechtspersoon kunnen worden gevorderd, maar waarin dat belang weer wel zo zwaarwegend is dat een terzijdestelling van het doelbindingsvereiste uit de Wbp gerechtvaardigd is, terwijl artikel 43 van de Wbp in de gegeven situaties daartoe onvoldoende mogelijkheden biedt.

6. Netwerk en InformatieBeveiliging-richtlijn

Deze wet loopt gedeeltelijk vooruit op de implementatie van de Netwerk en InformatieBeveiliging-richtlijn (hierna: NIB-richtlijn), merken de fractieleden van de **VVD** op. Wanneer verwacht de regering de implementatiewet van de NIB-richtlijn aan te kunnen bieden aan de Tweede Kamer?

De komende NIB-richtlijn onderstreept – net als dit wetsvoorstel – het belang van een wettelijke meldplicht bij ICT-inbreuken. Lidstaten zullen worden verplicht om een dergelijke meldplicht in te voeren. Kan de regering de **D66**-fractieleden toelichten op welke punten de wettelijke meldplicht, zoals vervat in dit wetsvoorstel, afwijkt van de wettelijke meldplicht zoals vervat in de NIB-richtlijn?

7. Toezicht en handhaving

Ten aanzien van toezicht en sancties hebben de leden van de **VVD**-fractie kennisgenomen van het voorstel om het NCSC niet te belasten met de handhaving van de meldplicht. Toezicht en sancties worden voorgeschreven in de NIB-richtlijn, welke uiterlijk op 9 mei 2018 dient te zijn geïmplementeerd. De regering geeft in de nota naar aanleiding van het verslag aan dat het wenselijk is de meldplicht bij het NCSC eerder in te voeren dan dat de richtlijn vereist, en dat het toezicht op de naleving van de meldplicht bij het NCSC zal worden geregeld in het kader van de implementatie van de NIB-richtlijn. Tevens verwacht de regering dat de opgenomen meldplicht goed zal werken zonder toezicht en sancties op niet-naleving daarvan.[10] De voornoemde leden vragen welke garanties er zijn opdat de meldplicht efficiënt functioneert zonder toezicht en sancties, en op welke wijze de regering de naleving van de Wet gegevensverwerking en meldplicht cybersecurity zal borgen.

Hoewel er volgens het wetsvoorstel een meldplicht in bepaalde gevallen geldt, wordt het NCSC noch een andere toezichthouder belast met de handhaving van deze meldplicht, merken de leden van de **D66**-fractie op. De Afdeling advisering van de Raad van State stelde in haar advies: «Als de voorgestelde meldplicht daadwerkelijk noodzakelijk is om de eigen verantwoordelijkheid van de Minister van Veiligheid en Justitie voor de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen, mag worden verwacht dat toezicht wordt gehouden op de naleving van de meldplicht en een sanctie wordt gesteld op het niet nakomen van de verplichting.»[11] De voornoemde leden delen de verbazing van de Afdeling dat in het wetsvoorstel geen toezicht en handhaving met betrekking tot de meldplicht wordt ingesteld. Zij delen daarom de zorg van deze Afdeling dat de voorgestelde meldplicht ineffectief zou kunnen zijn. Kan de regering toelichten waarom zij verwacht dat de voorgestelde meldplicht wel effectief zal zijn?

---

[10] Kamerstukken II 2015/16, 34 388, nr. 6, p. 2–3.
[11] Kamerstukken II 2015/16, 34 388, nr. 4, p. 2.

Daarnaast zijn de adviezen van het NCSC niet bindend. Kan de regering toelichten waarom zij voorstander is van een vrijblijvende houding voor vitale aanbieders na een ICT-inbreuk?

Het onderhavige wetsvoorstel voorziet niet in een regeling op grond waarvan toezichthouders naar aanleiding van andere meldplichten het NCSC kunnen informeren over meldingen die zij hebben ontvangen. Kan de regering toelichten waarom is afgezien van een dergelijke regeling, zo vragen de fractieleden van D66.

8. Overige

Vertrouwelijke gegevens kunnen worden verstrekt, conform het voorgestelde artikel 9 van het wetsvoorstel, aan computercrisisteams en de inlichtingen- en veiligheidsdiensten. Laatstgenoemde diensten hebben een wettelijke geheimhoudingsplicht. De leden van de **VVD**-fractie vragen de regering hoe wordt gewaarborgd dat de leden van de computercrisisteams ook tot geheimhouding worden gehouden.

In de memorie van toelichting wordt gesteld dat ingevolge het wetsvoorstel de bevoegdheid van het NCSC in het kader waarvan persoonsgegevens worden verwerkt, van een steviger wettelijke grondslag wordt voorzien.[12] Acht de regering deze stevigere wettelijke grondslag op het terrein van de bescherming van privacy met voldoende waarborgen omkleed, zo vragen de leden van de **D66**-fractie.

Tot slot wensen de **PvdA**-fractieleden van de regering te vernemen hoe het voorliggende wetsvoorstel zich verhoudt tot het initiatiefvoorstel-Voortman en Van Weyenberg Wet open overheid[13], zoals dat inmiddels in de Tweede Kamer is aangenomen.

De leden van de vaste commissie voor Veiligheid en Justitie zien de reactie van de regering – bij voorkeur binnen vier weken – met belangstelling tegemoet.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Duthler

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren

[12] Kamerstukken II 2015/16, 34 388, nr. 3, p. 2.
[13] Kamerstukken 33 328.