Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

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)

Nr. 5

VERSLAG

Vastgesteld 15 maart 2016

De vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

Inhoudsopgave

kst-34388-5
ISSN 0921 - 7371
's-Gravenhage 2016

Algemeen

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel betreffende 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, hierna: het wetsvoorstel). Zij vinden het goed dat er met dit wetsvoorstel, dat voortvloeit uit de motie-Hennis-Plasschaert c.s. (Kamerstuk 26 643, nr. 202), een wettelijke verplichting tot het melden van een inbreuk op de veiligheid komt. Het delen van kennis over cyberdreigingen is immers van groot belang om de digitale veiligheid te verhogen. Eigen verantwoordelijkheid is mooi, maar vrijblijvendheid in dit geval niet. Aangezien het niet melden van een inbreuk op de veiligheid verstrekkende gevolgen kan hebben, is het belangrijk dat het melden ervan verplicht wordt gesteld voor vitale aanbieders. Dit om maatschappelijke ontwrichting door ICT-inbreuken te voorkomen of in ieder geval te beperken. Deze leden hebben nog enkele vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij zien het belang van dit wetsvoorstel, te weten veilige en continue levering van vitale producten en diensten. Daarbij is het waarborgen van de bewaking van de privacy voor deze leden van groot belang.

De leden van de SP-fractie hebben met belangstelling kennisgenomen van de inhoud van het wetsvoorstel. Zij hebben hierover een aantal vragen en opmerkingen.

De leden van de CDA-fractie hebben kennisgenomen van het wetsvoorstel. Zij hebben hierover nog enkele vragen.
Deze leden merken op dat het wetsvoorstel weliswaar een meldplicht in het leven roept, maar dat de regering over de belangrijkste onderdelen hiervan nog geen duidelijkheid verschaft, te weten de reikwijdte van de meldplicht en de producten en diensten die hieronder zullen vallen. Is de regering voornemens de Kamer te betrekken bij de beoordeling van de in voorbereiding zijnde algemene maatregel van bestuur (amvb)?
Deze leden vragen of de regering ook van mening is dat de noodzaak tot onderhavig wetsvoorstel substantieel is veranderd sinds de aangenomen motie-Hennis-Plasschaert in 2011. Zij vragen de regering een overzicht te geven van het aantal meldplichten, per sector waarop het wetsvoorstel betrekking heeft, dat sinds 2011 in het leven is geroepen. Herkent de regering in dat kader de opmerking van Business Communication Providers Alliance (BCPA) dat in de telecomsector bijvoorbeeld een wildgroei van meldplichten is ontstaan?
De leden van de CDA-fractie vragen of het klopt dat er in 2011 nog geen sprake was van een voorstel van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt aan het verhogen van de digitale veiligheid. Ook wijzen zij op de Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp), waardoor er vanaf 1 januari 2016

een meldplicht geldt bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens.
De aan het woord zijnde leden vragen of het klopt dat met het wetsvoorstel in de praktijk een tweeledige meldplicht ontstaat (sectorale toezichthouder en het National Cyber Security Centre (NSCS)) en in geval van verlies van persoonsgegevens een driedubbele meldplicht voor de betreffende bedrijven en organisaties (sectorale toezichthouder, NSCS en Autoriteit Persoonsgegevens)? Is dat niet een beetje teveel van het goede?
De aan het woord zijnde leden worden hierin bevestigd door niet alleen de Afdeling advisering van de Raad van State (hierna: de Afdeling advisering), die een nadere onderbouwing van de extra meldplicht mist, maar ook door de adviezen van de betreffende organisaties, die in het algemeen vraagtekens zetten bij de toegevoegde waarde van het wetsvoorstel en lastenverhoging die dit met zich meebrengt. Heeft de regering overwogen, in afwachting van de implementatie van het genoemde EU-voorstel, enkel voort te bouwen op de zogeheten «just culture», een publiek-private uitwisseling waarin het gezamenlijk bijdragen op basis van vrijwillige afspraken de voorkeur krijgt boven het afdwingen van samenwerking door middel van wettelijke regels?

De leden van de PVV-fractie hebben kennisgenomen van het wetsvoorstel. Naar aanleiding hiervan hebben zij enkele vragen.
Deze leden lezen dat de voorgestelde meldplicht beperkt zal blijven tot ICT-inbreuken die een serieuze bedreiging voor de Nederlandse samenleving inhouden. Hoe vaak komen dit soort serieuze bedreigingen naar schatting jaarlijks voor? Worden deze ICT-inbreuken nu zonder meldplicht en hulp van het NCSC netjes opgelost of zijn er aanwijzingen waaruit blijkt dat dit niet of onvoldoende is gebeurd?

De leden van de D66-fractie hebben kennisgenomen van het wetsvoorstel. Zij onderschrijven het belang dat ICT-inbreuken in de informatiesystemen van vitale aanbieders die gevolgen kunnen hebben voor de samenleving, actief worden gemeld. Het wetsvoorstel lijkt echter nog geen volledige invulling te geven aan de meldplicht, waardoor het zicht op omvang en impact daarvan onvolledig is. De aan het woord zijnde leden hebben zodoende vele vragen en opmerkingen bij het wetsvoorstel. Zij zijn vooralsnog niet overtuigd van de noodzaak om de meldplicht op deze onvolledige wijze aan de Kamer voor te leggen.
De leden van de D66-fractie zijn van mening dat een meldplicht bij ICT-inbreuken voor zogenoemde vitale aanbieders kan bijdragen aan de online veiligheid in Nederland. Echter, niet alleen goede procedures achteraf zijn belangrijk, ook preventieve maatregelen kunnen van groot belang zijn, bijvoorbeeld door middel van risicoanalyses. Deze leden vragen de regering nader toe te lichten op wat voor manier vitale aanbieders vooral ook preventief geholpen worden om ICT-inbreuken te voorkomen.
De aan het woord zijnde leden lezen dat de doelgroep van het NCSC breder is dan alleen vitale aanbieders: het NCSC richt zich ook op de niet-vitale aanbieders die onderdeel zijn van de rijksoverheid. Kan de regering toelichten in hoeverre dit wetsvoorstel ook van toepassing is op deze bredere doelgroep? Zo nee, kan de regering toelichten wat met deze zinsnede bedoeld wordt?
Deze leden vragen of de regering voornemens is het wetsvoorstel te voorzien van een evaluatiebepaling.

2. Meldplicht

2.1 Inleiding

De leden van de VVD-fractie lezen dat voorgesteld wordt het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties). Toezicht en sancties worden voorgeschreven in het voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (NIB-richtlijn). Zij vragen of het, nu in dit wetsvoorstel een meldplicht opgenomen is, niet van belang is dat een sanctie op het schenden van die meldplicht tegelijkertijd op te nemen. Deze leden lezen dat als een vitale aanbieder niet weet dat er sprake is van een ICT-inbreuk, die ook niet kan worden gemeld. Hoe wordt vastgesteld of een vitale aanbieder had kunnen of moeten weten dat er sprake was van een ICT-inbreuk?

De leden van de PvdA-fractie lezen dat het bewerkstelligen van een cultuur om in gezamenlijkheid bij te dragen aan veiligheid centraal staat. Deze leden vinden dat het werken aan een «just culture», waarmee de luchtvaartsector werkt, hoog in het vaandel moet staan. Hoe gaat de regering dit bewerkstelligen? Worden de relevante sectoren actief gewezen op de benchmark? Welke andere maatregelen treft de regering om een veilige cultuur voor het doen van meldingen te stimuleren? De wet kan immers niet (goed) functioneren als een veilige meldcultuur ontbreekt in een organisatie. Kan de regering dit beamen? Kan de regering aangeven welke consequenties zij daaruit trekt?
Voor de aan het woord zijnde leden is het in de toekomst vermijden van kwetsbaarheden eveneens van groot belang, want het is beter te voorkomen dan te genezen. Welk specifieke maatregelen heeft de regering in gedachten om dit streven waar te maken? Wat doet de regering om aanbieders, zoals bijvoorbeeld softwareleveranciers in de telecomsector, te verplichten om de geleverde software te allen tijde bijgewerkt te houden en blijvend aan de hoogste («state of the art») veiligheidsnormen te laten voldoen? Deze leden zijn in algemene zin van mening dat een softwareleverancier nooit mag stoppen met het bieden van software-updates. Is de regering het met deze leden eens? Zo nee, waarom niet? Zo ja, welke maatregelen treft de regering om dit te bewerkstelligen bij de desbetreffende bedrijven?

De leden van de SP-fractie constateren dat de meldplicht alleen geldt bij een inbreuk op de veiligheid of daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Het moet dan gaan om ongeoorloofde toegang door een niet-geautoriseerd persoon. Interne fouten van een medewerker vallen alleen onder de meldplicht als deze fout heeft geleid tot ongeoorloofde toegang door een persoon van buitenaf. Maar geldt de meldplicht ook als bijvoorbeeld het handelen of nalaten van een medewerker heeft gezorgd voor inbreuk op de veiligheid of verlies van integriteit, ongeacht of er nu wel of niet ongeoorloofd toegang is geweest? Moet het uiteindelijk niet uitsluitend gaan om de gevolgen van een bepaalde handeling?
Hoe kijkt de regering aan tegen de mogelijkheid om ook te kunnen leren van kleinere inbreuken of van zaken waarin men zogezegd langs de rand van de afgrond is gescheerd en die evengoed tot grote problemen hadden kunnen leiden? Geniet de grootst mogelijke mate van transparantie niet juist de voorkeur? Zou dit niet veel meer toekomen aan een goede werking van bijvoorbeeld de markt, omdat (potentiele) klanten van bedrijven dan een beter geïnformeerde keuze kunnen maken voor een bepaalde dienst of product?

De leden van de SP-fractie vragen hoe de regering het risico inschat dat dienstverleners kunnen trachten om een onwelgevallig incident, dat publicitair onopgemerkt is gebleven en dat reputatieschade zou veroorzaken bij bekendwording, onder de pet te houden. In welke mate biedt de op diverse wijzen uit te leggen kwalificatie «in belangrijke mate» voldoende duidelijkheid om dit tegen te gaan? Biedt de kwalificatie «in belangrijke mate» afdoende rechtszekerheid voor zowel dienstverleners als hun klanten?

De leden van de D66-fractie constateren dat het NCSC belast wordt met het bieden van hulp na een melding van een ICT-inbreuk. In hoeverre is de melder van een ICT-inbreuk ook verplicht om het advies van het NCSC op te volgen? Welke stappen kan het NCSC nemen als een melder van een ICT-inbreuk geen navolging geeft aan de gegeven adviezen? De Afdeling advisering wijst in zijn advies op het belang van handhaving van de meldplicht, van het toezicht op de naleving van de meldplicht en van het opleggen van een sanctie bij niet nakomen van de verplichting. De keuze is gemaakt om in afwachting van de implementatie van de Europese NIB-richtlijn voorlopig een wettelijke meldplicht zonder toezicht en handhaving te realiseren. Dat roept bij deze leden de vraag op wat dan de toegevoegde waarde is van de voorgestelde wettelijke meldplicht als deze voorlopig niet handhaafbaar is. Blijft daarmee niet feitelijk de huidige praktijk van vrijblijvend melden gewoon voort bestaan? Wat maakt het regelen van het toezicht en een sanctie nu precies zo lastig? Kan de regering toelichten waarom zij er dan niet voor kiest om helemaal te wachten totdat de Europese NIB-richtlijn geïmplementeerd is? De reden die de regering daar nu voor geeft, vinden de leden van de D66-fractie onvoldoende onderbouwing, aangezien het feitelijk niets lijkt te veranderen aan de reeds bestaande praktijk waarin aanbieders van vitale diensten al melding maken. Omdat de precieze invulling van de meldplicht niet in het wetsvoorstel wordt gegeven en daardoor de omvang en impact niet duidelijk is, vragen deze leden om een nadere overweging op dit punt. De aan het woord zijnde leden vragen tevens wanneer de regering verwacht dat de Europese NIB-richtlijn gereed zal zijn voor implementatie. Waarom is er niet voor gekozen in de tussentijd in overleg met de betreffende sectoren afspraken te maken over toezicht en sancties zodat alles in een keer geregeld kan worden? In hoeverre wordt naast de wettelijke regeling erin voorzien dat toezichthouders op andere meldplichten een notificatie sturen aan het NCSC, zodat het NCSC kan nagaan of een melding ook daar had moeten plaatsvinden en of dat ook is gebeurd om daarmee ten minste te ondervangen dat de voorliggende wettelijke regeling vooralsnog niet voorziet in toezicht en sancties op naleving van de meldplicht?
De leden van de D66-fractie vragen de regering hoe dit wetsvoorstel zich verhoudt tot het wetsvoorstel Computercriminaliteit III (Kamerstuk 34 372). Wat gebeurt er als de politie bedoeld of onbedoeld een ICT-systeem van een vitale aanbieders hackt? Wat gebeurt er met de kwetsbaarheden die voor een dergelijke hack gebruikt worden als zij vitale producten of diensten onveiliger maken? Wat gebeurt er met software kwetsbaarheden die in het kader van een melding van een ICT-inbreuk gevonden worden? Worden zij altijd zo snel mogelijk gedicht of bestaat de mogelijkheid dat de politie de kwetsbaarheid eerste misbruikt in het kader van de hackbevoegdheid?

2.2 Te melden ICT-inbreuken

De leden van de VVD-fractie merken op dat in richtsnoeren kan worden vastgelegd wat moet worden verstaan onder «in belangrijke mate». Is al duidelijk of deze richtsnoeren er daadwerkelijk gaan komen? Is al duidelijk wat de definitie van «in belangrijke mate» zal zijn?

De leden van de PvdA-fractie lezen dat de meldplicht gaat gelden voor aanbieders van vitale producten of diensten en dat het meldingen van daadwerkelijke inbreuken op de ICT-systemen betreft. Zij lezen dat het criterium om te moeten melden is dat de beschikbaarheid van de dienst of het product wordt of kan worden onderbroken, omdat dit tot maatschappelijke ontwrichting zou kunnen leiden. DDos-aanvallen vallen buiten de meldplicht. Dergelijke aanvallen hebben echter al tot dagenlange problemen geleid bij banken en heeft veel overlast bezorgd. Deze leden menen dat het niet denkbeeldig is dat de aanvallers (sterk) maatschappelijk ontwrichtende problemen weten te veroorzaken, zoals bijvoorbeeld langdurige onbereikbaarheid van financiële diensten. Dergelijke aanvallen zouden daarom wel onder de meldplicht moeten kunnen vallen, zo menen de aan het woord zijnde leden. Kan de regering uitleggen waarom toch niet is gekozen voor een meldplicht? Kan dit in de toekomst eventueel wel gebeuren? Zo ja, waar hangt dit vanaf? Overweegt de regering criteria of richtsnoeren voor uitbreiding van de meldplicht?

De leden van de SP-fractie begrijpen dat er discussie is over de invulling van «in belangrijke mate» als drempel om een ICT-inbreuk te melden. Waarom is hier niet reeds over gesproken met de betrokken sectoren en departementen? Kan worden aangegeven wat de visie van het Ministerie van Veiligheid en Justitie zelf is? Van belang zal zijn of en wanneer sprake is van maatschappelijke ontwrichting of niet. Betekent dit ook dat een inbreuk niet gemeld hoeft te worden als een inbreuk alleen ontwrichtend is in individuele gevallen? Hoe gaan betrokken sectoren en ministeries om met ICT-inbreuken die slechts zeer negatieve gevolgen hebben voor een kleinere groep betrokkenen?

De leden van de CDA-fractie vragen de regering wat zij, los van het overleg met de betrokken sectoren en departementen, zelf verstaat onder «in belangrijke mate» en bijbehorende criteria bij de meldplicht. Voor de beoordeling van het onderhavige wetsvoorstel lijkt het deze leden van belang dat de regering, voordat de amvb hierover wordt opgesteld, in het wetsvoorstel een nadere duiding geeft van de voorwaarden waaronder de meldplicht moet worden nageleefd en van organisaties waarop de meldplicht van toepassing is. Graag zien zij een reactie van de regering op dit punt tegemoet.

De leden van de D66-fractie constateren dat de verplichting tot melden alleen geldt als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Bij veel ICT-inbreuken is het in eerste instantie vaak onduidelijk wat het effect van de inbreuk is op de beschikbaarheid of betrouwbaarheid van het product of dienst. Hoe moeten vitale aanbieders de inschatting maken of een inbreuk wel of niet gevolgen heeft voor de beschikbaarheid of betrouwbaarheid van het product of dienst? Heeft de regering overwogen om de verplichting tot melden te laten gelden voor alle ICT-inbreuken? De voornoemde leden lezen voorts dat in overleg met de betrokken sectoren en departementen nader zal worden uitgewerkt wat voor de verschillende betrokken producten en diensten moet worden verstaan onder «in belangrijke mate». Wanneer zullen deze gesprekken plaatsvinden?

De leden van de D66-fractie vragen de regering nader toe te lichten waarom ervoor gekozen is om DDoS-aanvallen uit te sluiten van de meldplicht. Is de regering het met de leden van de D66-fractie eens dat een DDoS-aanval ook een maatschappelijk ontwrichtende werking kan hebben en dat het NCSC bijstand kan bieden bij het mitigeren van dergelijke aanvallen. Waarom is desalniettemin ervoor gekozen om DDoS-aanvallen buiten de strekking van dit wetsvoorstel te laten vallen?

2.3 Verhouding tot sectorale meldplichten

De leden van de SP-fractie lezen dat de administratieve lasten door samenloop met sectorale meldplichten zo beperkt mogelijk zullen worden gehouden doordat betrokken instanties dezelfde gegevens moeten aanleveren op grond van de voorgestelde meldplicht als op grond van de sectorale meldplichten. Hoe kijken betrokken sectoren hiertegen aan? Wordt er bij het toewijzen van sectoren, die onder de meldplicht vallen, ook gekeken of zij aan deze (extra) meldplicht kunnen voldoen en wat zij moeten ondernemen om hier wel aan te kunnen voldoen? Zo nee, waarom niet?
Deze leden begrijpen dat het zeker voor kan komen dat het advies van het NCSC door eerder genoemde samenloop van meldplichten afwijkt van de aanwijzing van de sectorale toezichthouder. De aanwijzing van de toezichthouder prevaleert dan, omdat adviezen van het NCSC niet bindend zijn. Maar wat gebeurt er vervolgens? Wordt dan ook onderzocht waar het verschil in inzicht vandaan komt en eventueel kan worden opgelost?

De leden van de CDA-fractie vragen aan de regering een overzicht te geven van alle bestaande sectorale toezichthouders en daaraan gelieerde organisaties die ook onder de reikwijdte van onderhavig wetsvoorstel vallen.
Deze leden vragen of de regering heeft overwogen het wetsvoorstel op zo'n manier in te richten dat de sectorale toezichthouders meldingen, die zij ontvangen van vitale aanbieders, doorspelen naar het NCSC in plaats van aanbieders een dubbele meldplicht en in sommige gevallen een driedubbele meldplicht op te leggen. Zij vragen of de regering de voordelen van een dergelijk stelsel ziet en/of ook wat de nadelen hiervan zouden zijn. Maakt een dergelijk systeem niet ook de weg vrij voor (andere) keuzes ten aanzien van gevoelige gegevensverstrekking door het NCSC aan derden? Ook hierover leven de nodige zorgen, zo merken deze leden op naar aanleiding van de ingediende adviezen bij het wetsvoorstel. Zoals bepleit door De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM), zou met de keuze voor een dergelijk systeem het ook logischer zijn dat de sectorale toezichthouder beslist over het verstrekken van gegevens aan derden en niet het NCSC, uitgezonderd de informatievoorziening aan inlichtingen-, veiligheids- en opsporingsdiensten voor wat de leden van de CDA-fractie betreft. Graag vernemen zij een reactie van de regering hierop
De aan het woord zijnde leden vragen hoe de stellingname dat de Minister van Veiligheid en Justitie (ingevolge de huidige portefeuilleverdeling: de Staatssecretaris) «een eigen verantwoordelijkheid heeft om de digitale weerbaarheid van de samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen» zich verhoudt tot de beperkte mogelijkheden die het NCSC worden toegekend. Immers, het NCSC heeft geen handhavingsbevoegdheid en ingeval van tegenstrijdige adviezen prevaleert het advies van de sectorale toezichthouder. Deze leden hebben begrip voor beide keuzes, maar is daarmee de Minister van Veiligheid en Justitie geen tandeloze tijger? Zou de Minister van Veiligheid en Justitie met onderhavig wetsvoorstel meer verantwoordelijk moeten zijn en kunnen worden bij schade door ICT-inbreuken in vitale informatiesystemen, ook wanneer dit een branche en toezichthouder betreft die onder een andere bewindspersoon valt? De aan het woord zijnde leden vragen de regering bij haar reactie te betrekken het gegeven dat veel vitale aanbieders via sectorale toezichthouders al onder ministeriële verantwoordelijkheid staan en of hiermee de hierboven genoemde verantwoordelijkheid niet al voldoende is geborgd.

De leden van de D66-fractie lezen dat de voorziene meldplicht van het NCSC wezenlijk verschilt van de sectorale meldplichten gericht op toezicht op een wettelijke zorgplicht. In hoeverre is dat wezenlijke verschil een keuze van de regering zelf, die niet voortvloeit uit de voorziene NIB-richtlijn? Onderschrijft de regering dat toezicht en hulpverlening elkaar niet hoeven te bijten en beide georganiseerd kunnen en zelfs moeten worden? In hoeverre kan het zijn dat vitale aanbieders met een samenloop van meldplichten worden geconfronteerd? Welke meldplicht-instantie is dan leidend in de behandeling daarvan? Is in kaart gebracht in hoeverre daarbij sprake kan zijn van conflicterende aanwijzingen en adviezen?
Deze leden vragen of het NCSC als enige hulp kan en zal aanbieden bij ICT-inbreuken bij vitale aanbieders die tot maatschappelijke ontwrichting kunnen leiden of is een hulp biedende taak ook belegd bij andere instanties die uitvoering geven aan een meldplicht?
De leden van de D66-fractie lezen dat in geval van aanwijzingen van een toezichthouder die tegenstrijdig is aan het advies van het NCSC, de aanwijzing van de toezichthouder prevaleert. Hoe verhoudt zich dat tot de constatering van de regering dat de coördinerend bewindspersoon voor cybersecurity een eigen verantwoordelijkheid heeft om de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen? Hoe meent de coördinerend bewindspersoon maatschappelijke ontwrichting van vitale systemen te voorkomen wanneer een aanwijzing van een toezichthouder conflicteert met het advies van de NCSC en die eerste voorrang krijgt? Indien dit het uitgangspunt is, op welke wijze verwoord de wettekst dan expliciet dat het advies van het NCSC ondergeschikt is aan het advies van de sectorale toezichthouder?

2.4 Verhouding tot meldplicht datalekken

De leden van de SP-fractie lezen dat er ook kans is op samenloop met het meldplicht datalekken. Dat brengt deze leden op de vraag wat er precies gebeurt als een toezichthouder of een instantie als het NCSC of de Autoriteit persoonsgegevens (AP) bij het onderzoek naar een melding erachter komen dat verkeerd gemeld is. Zullen zij de melding dan actief doorgeleiden naar de juiste instantie? Indien het NCSC er bijvoorbeeld achter komt dat er ook persoonsgegevens in het geding zijn, zal het de zaak dan ook actief doorgeven aan de AP? De leden kunnen zich namelijk goed voorstellen dat betrokken instanties niet altijd goed kunnen inschatten wat de gevolgen zijn van een inbreuk.

De leden van de CDA-fractie vragen de regering in te gaan op de ministeriële verantwoordelijkheid die geldt ten aanzien van de bescherming van persoonsgegevens. In het bijzonder vragen zij om een reactie op de wijze waarop de Minister van Volksgezondheid, Welzijn en Sport onlangs heeft gereageerd op de berichtgeving dat Belgische gevangenen gewerkt hebben met Nederlandse patiëntendossiers. Zij verwees in beantwoording van Kamervragen enkel en alleen naar de AP als het gaat om controle en toezicht hierop (Aanhangsel van de Handelingen, vergaderjaar 2015–2016, nr. 1590 en Aanhangsel van de Handelingen, vergaderjaar 2015–2016, nr. 1559). Is dat niet wat mager, gelet op de gevoeligheid van dergelijke gegevens? Daar zou toch ook de betrokken Minister direct verantwoordelijkheid voor dienen te nemen? In dat kader wijzen deze leden de regering ook op een Kamerbreed gesteund verzoek om met de Minister van Volksgezondheid, Welzijn en Sport in debat te gaan over berichtgeving dat tien ziekenhuizen in Nederland gevangenen in België medische gegevens laat verwerken en erger nog, dat gevangenen die gegevens ook gewoon weggooien. Kan de regering aangeven hoe de ministeriële verantwoordelijkheid haar uitwerking krijgt in relatie

tot het wetsvoorstel datalekken en het onderhavige wetsvoorstel, ook voor wat betreft andere ministeries dan het Ministerie van Veiligheid en Justitie?

2.5 Naleving

De leden van de PvdA-fractie lezen dat als het advies van de NCSC niet (voldoende) wordt opgevolgd door de getroffen organisatie, de voor de sector verantwoordelijke bewindspersoon op de hoogte kan worden gebracht van zowel het advies van de NCSC als het uitblijven van het nemen van effectieve maatregelen. Kan de regering voorbeelden geven van dergelijke situaties? Welke criteria gelden dan en welke maatregelen kunnen vervolgens worden getroffen, vooral richting de niet-coöperatieve organisatie, om escalatie te voorkomen? Wat verstaat de regering onder «passend invulling geven» aan zijn sectorale verantwoordelijkheid? Hoe is in dergelijke gevallen de aansprakelijkheid geregeld? Welke sancties gelden bij in gebreke blijven?

De leden van de SP-fractie krijgen enigszins het idee dat niet heel veel is nagedacht over toezicht en handhaving van de meldplicht of dat daar in ieder geval te snel overheen gestapt wordt. Wordt dit pas geregeld bij inwerkingtreding van de NIB-richtlijn? Hoe wordt tot die tijd nu precies gezorgd dat gecontroleerd wordt of de meldplicht wordt nageleefd of niet? Zal de Staatssecretaris van Veiligheid en Justitie hier zorg voor dragen? Op welke manier zal praktische invulling aan toezicht en handhaving worden gegeven? Welke waarborgen zijn er voor de naleving van de meldplicht? Hier lezen de leden zeer weinig over.

De leden van de PVV-fractie merken op dat het advies van het NCSC niet bindend is. Indien op grond van het verstrekte advies geen of onvoldoende maatregelen zijn getroffen om (verdere) verstoring van de betrouwbaarheid of beschikbaarheid van de getroffen producten of diensten te voorkomen, kan de voor de betreffende sector verantwoordelijke bewindspersoon hiervan op de hoogte worden gebracht. Zo is hij in staat om passend invulling te geven aan zijn sectorale verantwoordelijkheid. Welke maatregelen kan een bewindspersoon vervolgens nemen?

De leden van de D66-fractie vragen de regering toe te lichten op wat voor manier gerapporteerd wordt aan de Tweede Kamer door het NCSC over de meldplicht. Is de regering bereid de Kamer een overzicht toe te sturen van het aantal meldingen en in hoeverre de adviezen van het NCSC zijn opgevolgd?

3. Wettelijke grondslag voor taken en gegevensverwerking NCSC

De leden van de VVD-fractie lezen dat het NCSC niet bevoegd is om dadergericht onderzoek te doen. In hoeverre kan het NCSC wel informatie delen met de inlichtingen- en veiligheidsdiensten, de politie en het Openbaar Ministerie (OM) die wel over opsporingsbevoegdheden beschikken?

De leden van de PvdA-fractie hebben al gewezen op het belang dat zij hechten aan de eigen verantwoordelijkheid van aanbieders voor wat betreft de veiligheid van hun informatiesystemen. In hoeverre kan en wil de regering deze verantwoordelijkheid afdwingen?
Deze leden merken op dat het NCSC als taak heeft analyses en technisch onderzoek te verrichten. Zij willen weten of het mogelijk is daarvoor jongeren in te zetten, die uitgevallen zijn in het VMBO en soms ook MBO/HBO. Het gaat om (meestal) jongens met een storing in het autistisch spectrum. Onder die enorme grote groep jongeren zijn er veel

die heel slim zijn met computers, internet en veiligheidslekken, maar niet pasten in het reguliere onderwijs.

De leden van de CDA-fractie vragen of het wenselijk is, ook gelet op de verantwoordelijkheid die de regering bij de Minister van Veiligheid en Justitie wil neerleggen om de maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen, dat het NCSC niet bevoegd wordt gesteld om de identiteit van bijvoorbeeld hackers te achterhalen. Deze leden erkennen dat het strafrechtelijke opsporingsonderzoek is belegd bij politie en justitie, maar zij vragen of de regering de mening deelt dat medewerkers van het NCSC in elk geval hun ogen niet kunnen sluiten als zij op de identiteit van personen stuiten die (mogelijk) strafbare feiten hebben gepleegd of nog zullen plegen. Wat is de regering voornemens hierover te regelen bij amvb? In dat kader maken deze leden zich zorgen over de opmerking dat indien aan het NCSC een dataset is overhandigd, waarin bijzondere persoonsgegevens blijken te zijn opgenomen, deze onmiddellijk dient te worden vernietigd. Hoe verhoudt zich dit tot de effectiviteit van opsporing en vervolging dat uit NCSC-onderzoek naar datalekken kan voortvloeien?
De leden van de CDA-fractie vragen of de regering de mening deelt dat ook het OM en de politie geschaard kunnen worden onder organisaties die tot taak hebben om andere organisaties of het publiek over dreigingen of incidenten te rapporten. Zo ja, kan de regering dan ook bevestigen dat de genoemde eventuele bijvangst met al deze organisaties gedeeld kan worden door het NCSC? Zo nee, waarom niet? Op dit punt sluiten deze leden zich aan het advies van de Afdeling advisering om gegevens door het NCSC uit eigen beweging herleidbare gegevens te kunnen doorgeleiden naar het OM. Beschikt de regering over indicaties dat vitale aanbieders hier bezwaren tegen zouden hebben? Zo nee, waarom beslist zij dit dan op die wijze voor de vitale aanbieders in het voorgestelde artikel 9?

4. Verstrekking van vertrouwelijke gegevens

De leden van de PvdA-fractie zien in dat herleidbare gegevens soms aan andere organisaties of aan het publiek moeten worden verstrekt. Kan de regering aan de hand van voorbeelden, wellicht ook uit het verleden, toelichten wanneer hiertoe moet worden overgegaan? Welke rol kunnen specifieke organisaties met bijzondere expertise, zoals de Fraudehelpdesk, hebben? Deze leden vinden het van groot belang dat een streng criterium geldt, in verband met de privacygevoeligheid. Deze leden willen tevens benadrukken dat de tijdsdruk niet ten koste mag gaan van de belangenafweging. Hoe gaat de regering hiervoor waken, anders dan het streng houden aan het criterium «voorkómen van ernstige maatschappelijke gevolgen»? Kan de regering een voorbeeld noemen waarin meteen het belang van het publiek de doorslag geeft? Hoe wordt in het algemeen het publiek op de hoogte gebracht en gehouden van de publieksmededelingen en voorlichting van het NCSC? Wordt daarvoor een apart medium en/of alert-systeem overwogen?

De leden van de D66-fractie hebben kennisgenomen van de opmerkingen zoals gemaakt door de Afdeling advisering en de AP over de onwenselijkheid om zonder enige precisiering af te wijken van het doelbindingsvereiste zoals dat wettelijk geldt voor de verwerking van persoonsgegevens. De regering schrijft in reactie op het advies van de Afdeling advisering en de AP dat het NCSC slechts mag verzoeken om verstrekking van gegevens die noodzakelijk zijn voor de vervulling van de in artikel 2, eerste lid, omschreven taken. Waarvoor is het dan nog nodig om afwijking van doelbinding voor te stellen zoals thans gebeurt in artikel 4, tweede lid? Op welke grond is afwijking van doelbinding dan nog noodzakelijk? En als

artikel 2 juist bindt aan een specifiek doel, namelijk hetgeen past bij de wettelijk omschreven taken, wat bedoelt het kabinet dan precies met de, naar opvatting van D66 contradictoire, zinsnede dat artikel 2 «voorziet in een alternatief om wettelijk te preciseren in welke categorieën van gevallen van het doelbindingsvereiste kan worden afgeweken»?

5. Totstandkoming van dit wetsvoorstel

5.1 Bespreking van de reacties op hoofdlijnen

5.1.1 Zorgplichten en handhaving

De leden van de CDA-fractie vragen of de regering heeft overwogen in geval er geen sprake is van publiek-private samenwerking maar alleen van publiekrechtelijke organisaties, wel nadere interventiebevoegdheden voor het NCSC mogelijk te maken.
Deze leden vragen met betrekking tot de advisering omtrent installatie van detectiesoftware of ingeval van tegenstrijdige adviezen of het advies van de sectorale toezichthouder altijd prevaleert boven dat van het NCSC. Immers, de keuze de installatie van dergelijke programmatuur wel of niet te eisen van de betreffende vitale aanbieder, kan verstrekkende gevolgen hebben bij (latere) ICT-inbreuken. De leden van de CDA-fractie vragen de regering daarom op dit punt nader aandacht te besteden aan de verhouding tussen het NCSC en de sectorale toezichthouders. Ook vragen zij of de regering kan verzekeren dat momenteel alle bekende vitale aanbieders in Nederland beschikken over een detectiesoftware. Indien dat niet het geval is, dient daar snel werk van te worden gemaakt.

5.1.2 Administratieve lasten

De leden van de VVD-fractie lezen dat in diverse reacties op het wetsvoorstel bezorgdheid is uitgesproken over de administratieve lasten. Kan toegelicht worden wat een melding van een ICT-inbreuk in de praktijk precies behelst voor de betrokken vitale aanbieder?

5.1.3 Reikwijdte meldplicht

De leden van de VVD-fractie vragen hoe gezondheidsinstellingen, zoals ziekenhuizen, zich verhouden tot de definitie van vitale aanbieders.

De leden van de PvdA-fractie lezen dat de reikwijdte van de meldplicht een gevoelig punt is voor bedrijven en lastig is af te bakenen. Zij zijn van mening dat het criterium «in belangrijke mate» zorgvuldig moet worden ingevuld en heldere, niet voor discussie vatbare, criteria moet bevatten. Al dan niet melden mag niet in discussie of onderhandeling ontaarden, zeker als het maatschappelijk belang daarom vraagt. Onder tijdsdruk moet snel en helder een afweging kunnen plaatsvinden aan de hand van een concrete checklist of beslisboom, menen de aan het woord zijnde leden. Hoe gaat de regering dit in samenspraak met de desbetreffende sectoren vormgeven en hoe wordt de Tweede Kamer van de uitkomst op de hoogte gebracht?
Deze leden lezen dat de gezondheidszorg buiten de reikwijdte van het w etsvoorstel valt vanwege het geringe risico van cascade-effecten. Zij vragen waarom (hooggespecialiseerde) ziekenhuiszorg als voor de samenleving niet-vitale dienst wordt gekwalificeerd? Uitval van zorg door ICT-problemen kan ook leiden tot maatschappelijke ontwrichting, zo menen zij. Het welzijn van het land is in dit geval in het geding. Kan de regering een toelichting geven?

5.1.4 Te melden ICT-inbreuken

De leden van de SP-fractie vragen extra aandacht voor de opmerking van Bits of Freedom dat DDoS-aanvallen wel degelijk tot maatschappelijke ontwrichting kunnen leiden. Het kan bijvoorbeeld leiden tot de situatie waarin persoonlijke gegevens van mensen op straat komen te liggen. Dergelijke aanvallen vallen echter niet onder de meldplicht. Kan de regering deze afweging uitgebreid toelichten?

5.1.5 Vertrouwelijkheid

De leden van de SP-fractie lezen dat er een geheimhoudingsplicht voor het NCSC komt die vergelijkbaar is met de geheimhoudingsplicht van sectorale toezichthouders. Wie controleert of deze geheimhoudingsplicht wordt nageleefd en wat gebeurt er bij schending hiervan?

6. Grondrechtentoets

De leden van de SP-fractie lezen dat het NCSC ten behoeve van gegevensverwerking een dataset met IP-adressen, e-mailadressen en domeinnamen. Deze gegevens zijn nodig om aan het voorgestelde artikel 2 te kunnen voldoen, namelijk het dienen van onder meer de nationale veiligheid, openbare veiligheid en het economisch welzijn van het land. Echter, op welke manier leiden deze datasets hiertoe? Hoe kan het NCSC op basis van sec de IP-adressen nader onderzoek doen zonder dat men ook te maken krijgt met (bijzondere) persoonsgegevens? Hoe wordt kortom voorkomen dat er een (forse) inmenging plaatsvindt in het recht op respect voor iemands privéleven?

De leden van de CDA-fractie vragen de regering waarom zij voorschrijft dat persoonsgegevens onmiddellijk verwijderd moeten worden wanneer deze door het NCSC worden aangetroffen in datasets. Gelet op de mogelijke dreiging van een ICT-inbreuk, zou de focus van het NCSC toch vooral moeten zijn het oplossen hiervan en in elk geval niet het uitkammen van datasets op de aanwezigheid van bijzondere persoonsgegevens? Deelt de regering in elk geval deze mening van deze leden? In dit kader vragen de aan het woord zijnde leden hoe het voornemen tot het onmiddellijk verwijderen van datasets zich verhoudt tot de opmerking van de regering dat het NCSC zijn taken niet kan uitoefenen wanneer het niet zou beschikken over de persoonsgegevens die vaak deel uitmaken van datasets die het NCSC verkrijgt bij de melding van een incident. Deelt de regering de mening dat juist bij het overhandigen van de datasets nog niet altijd duidelijk kan en zal zijn voor zowel de vitale aanbieder als het NCSC welke daarin aanwezige persoonsgegevens noodzakelijk zijn voor het uitvoeren van de NCSC-taken? Is de regering bereidt het NCSC dan ook de nodige ruimte te verschaffen in de uitoefening van haar taken bij het aantreffen van bijzondere persoonsgegevens en deze dus niet in alle gevallen direct hoeven te worden verwijderd?

De leden van de D66-fractie lezen dat de AP van mening is dat de regering niet kan volstaan met slechts enkele waarborgen voor verstrekking van vertrouwelijke gegevens door de NCSC. Gelet op de verwerking van bijzondere persoonsgegevens, het buiten toepassing verklaren van het doelbindingsbeginsel en de geheimhoudingsplicht uit de Wet bescherming persoonsgegevens, acht de AP het treffen van extra waarborgen essentieel is. Heeft de regering de aangevulde toelichting in paragraaf 6 van de toelichting bij het wetsvoorstel nadien nog voorgelegd aan de AP? In hoeverre heeft de regering van de AP vernomen dat hiermee sprake is van afdoende tegemoetkoming aan het dringende advies voor extra waarborgen?

7. Privacy impact assessment

De leden van de SP-fractie lezen dat een betrokkene inzicht kan verkrijgen in de persoonsgegevens die het NCSC (heeft) verwerkt door een verzoek in te dienen bij het Ministerie van Veiligheid en Justitie. Worden betrokkenen actief op deze mogelijkheid gewezen of moeten zij hier zelf achter komen? Indien van dat laatste sprake is, op welke manier kunnen betrokkenen afweten van deze gegevensverwerking? Indien het ministerie een verzoek afwijst, staat dan bezwaar en beroep bij de bestuursrechter open?

De leden van de D66-fractie lezen in het voorstel dat een privacy impact assessment heeft plaatsgevonden. Deze leden vragen de regering de privacy impact assessment aan de Kamer te doen toekomen.

8. Regeldruk

De leden van de CDA-fractie vragen of de regering goede nota heeft genomen van de administratieve lasten die de betrokken vitale aanbieders verwachten als gevolg van onderhavig wetsvoorstel. In dat kader vragen zij de regering een indicatie te geven van de administratieve lasten die aanbieders kwijt zijn in geval zij een dubbele of driedubbele melding van een inbreuk moeten maken. In dat geval zouden de lasten ver boven de genoemde 17.000 euro per jaar (acht aanbieders, tien meldingen per jaar) uitkomen. Acht de regering de kosten en baten hiervan niet te hoog, zeker voor het midden- en kleinbedrijf?
Ook vragen deze leden om een reactie op het risico dat aanbieders bij invoering van de meldplicht veel tijd en middelen kwijt zijn aan het managen van processen in plaats van het oplossen van de betreffende ICT-problemen. In dat kader behoeft ook de opmerking van de regering in reactie op het advies van de Afdeling advisering dat dit wetsvoorstel zal leiden tot een verdere vergroting van de meldingsbereidheid enige toelichting. Waarop baseert de regering deze verwachting, mede gezien de toename van administratieve lasten van de zijde van de vitale aanbieders bij het doen van melding?

Het verbaast de leden van de D66-fractie zeer dat nog geen zicht bestaat op de regeldruk doordat nog niet vaststaat voor welke vitale aanbieders en voor welke producten en diensten de meldplicht zal gelden en welke inbreuken ernstig genoeg zijn om onder de meldplicht te vallen. Daarmee ontbreekt voor zowel de vitale aanbieders die het treft als voor de Kamer als medewetgever het zicht op de concrete invulling en op de gevolgen van het voorstel.
Bovendien constateren voornoemde leden dat de concrete invulling van de meldplicht wel van invloed is op de omvang van de administratieve lasten. Net als de vele organisaties die in consultatie hun opmerkingen hebben geplaatst bij het wetsvoorstel, zijn deze leden van mening dat de invulling van de meldplicht daarmee onvoldoende concreet is en het voor zowel de Kamer als de vitale aanbieders niet mogelijk is om te voorzien wat deze meldplicht precies gaat betekenen voor administratie lasten en risico's. Indien alle potentieel maatschappij ontwrichtende incidenten gemeld dienen te worden, bestaat het risico dat een grote stroom van meldingen kan ontstaan. De leden van de D66-fractie delen dan ook de constatering van onder meer VNO-NCW dat dit nadrukkelijk vragen oproept over de capaciteit van het NCSC om bij een potentieel grote stroom aan meldingen daadwerkelijk hulp te bieden aan vitale aanbieders. Hoe denkt de regering in die capaciteit te voorzien?
In dit licht merken deze leden ook op dat het onwenselijk is dat het wetsvoorstel geen financiële paragraaf bevat. Welke kosten verwacht de

regering ten behoeve van het adequaat kunnen uitvoeren van de voorgestelde meldplicht door het NCSC?
De leden van de D66-fractie vragen waarom de regering er niet voor heeft gekozen eerst de uitwerking met betrokken sectoren en departementen ter hand te nemen en deze dan vervolgens mee te nemen in artikel 6 van het voorliggende wetsvoorstel, dan wel de aanvullende richtsnoeren en amvb's gezamenlijk met het wetsvoorstel aan de Kamer voor te leggen zodat een integrale beoordeling van inhoud en impact kan plaatsvinden.

Artikelsgewijze toelichting

Artikel 1

De leden van de CDA-fractie vragen in verband met de herijkte lijst vitale infrastructuur of gemeenten ook onder de reikwijdte van onderhavig wetsvoorstel vallen (Kamerstuk 30 821, nr. 23), dit omdat digitale overheid ook op deze lijst (onder categorie B) staat. Los hiervan vragen deze leden de regering nader in te gaan op de wijze waarop gemeenten zich hebben voorbereid op de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp die op januari 2016 in werking is getreden. Herkent de regering het beeld dat de digitale infrastructuur van gemeenten nog onvoldoende is toegerust op voorkomen van datalekken door gebrek aan expertise en financiële middelen? Hoe ondersteunt de regering gemeenten hierin, juist nu gemeenten door onder meer de transities in de zorg steeds meer bijzondere persoonsgegevens verwerken? Kan de regering aangeven in hoeverre gemeenten de adviezen van de Informatie Beveiligingsdienst (IGB) hebben opgevolgd om voorbereid te zijn op deze nieuwe meldplicht omtrent het datalekken? Lopen zij hierin tegen (financiële) problemen aan? Het betreft onder andere het uitvoeren van een baselinetoets BIG en een privacy impact assessment, het afsluiten van gebruikersovereenkomst met een cloud-dienstverleners, het aanpassen van de bewerkersovereenkomsten, het benoemen van verantwoordelijke ambtenaren op het terrein van gemeentelijk informatiebeveiligingsbeleid, het inrichten van een incident-managementproces, het registreren van alle gegevensverzamelingen, het loggen en monitoren van verzamelde gegevens en het vergroten van bewustwording onder medewerkers (https://www.ibdgemeenten.nl/wp-content/uploads/2016/01/Leaflet-Meldplicht-Datalekken.pdf). Graag vernemen deze leden hierop een reactie van de regering.

Artikel 4

De leden van de SP-fractie begrijpen dat persoonsgegevens niet aan het NCSC mogen worden verstrekt als dat niet verenigbaar is met de doeleinden waarvoor die gegevens zijn verkregen. Afwijking hiervan is mogelijk op grond van artikel 43 Wbp, maar dat artikel is volgens de regering onvoldoende, aangezien gegevens ook moeten worden verstrekt ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van elektronische informatiesystemen van vitale aanbieders die niet behoren tot de rijksoverheid. Eerder had de AP kritiek op deze uitzonderingen, omdat volgens deze instantie artikel 43 Wbp voldoende soelaas zou moeten bieden. Wat is de reactie van de AP nu de memorie van toelichting op dit punt is aangepast? Kan de regering daarbij ook weer reageren op deze vervolgreactie?

De leden van de CDA-fractie vragen aan wie in eerste instantie beoordeelt dat de verstrekking van bepaalde gegevens aan het NCSC past binnen de uitoefening van de taken van het NCSC. Deelt de regering de mening dat dit in eerste instantie aan het NCSC zelf is omdat het het NCSC is dat de aanvraag doet? Maar wat als het NCSC en de betrokken aanbieder van

mening verschillen of de verstrekking van gegevens past binnen deze taakuitoefening? Deelt de regering de analyse dat het NCSC dan altijd aan het korte eind trekt omdat de gegevensverstrekking op vrijwillige basis geschiedt? Zou niet een vangnetconstructie, bijvoorbeeld door middel van een beoordeling van de betrokken sectorale toezichthouder, een oplossing kunnen bieden in een dergelijke situatie?

Artikel 5

De leden van de PvdA-fractie lezen dat meldplichtige aanbieders van vitale producten of diensten ook buiten Nederland gevestigd kunnen zijn. Hoe komen en blijven deze vestigingen op de hoogte van de meldplicht en de daaraan verbonden eisen en verantwoordelijkheden? Heeft de regering een mogelijk risico van vertraging door (onder meer) communicatieproblemen in het vizier? Zo ja, welke consequenties trekt zij daaruit, gezien voor een melding geldt dat die zo spoedig mogelijk gedaan wordt?

Artikel 10

De leden van de VVD-fractie vragen of toegelicht kan worden welke redenen er zouden kunnen zijn om te besluiten tot gedifferentieerde inwerkingtreding van onderhavige wet.

De leden van de PvdA-fractie vragen wanneer (en onder welke voorwaarden) de wet gedifferentieerd in werking treedt.

De voorzitter van de commissie,
Ypma

De griffier van de commissie,
Nava