8 december 2011

Juridisch kader

Cyber Security

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

In het afgelopen decennium is een groot deel van de computersystemen van de Rijksoverheid, lagere overheden en het bedrijfsleven met elkaar verbonden via het Internet. Dit heeft ertoe geleid dat overheidsdiensten beter in staat zijn om onderling en met bedrijven en burgers informatie uit te wisselen, wat doeltreffender beleidsvorming en beleidsuitoefening mogelijk heeft gemaakt. Het bedrijfsleven is door deze ontwikkeling voorts in staat gesteld om geografisch verspreide activiteiten centraal te coördineren, wat productiviteit en efficiëntie heeft bevorderd. Bovendien heeft de koppeling van computersystemen aan het Internet maatschappelijk wenselijke ontwikkelingen zoals thuis- en deeltijdwerken gestimuleerd.

Het aan elkaar koppelen van systemen via het Internet brengt echter ook risico's met zich. Het Internet is wereldwijd toegankelijk voor een algemeen publiek. Dit brengt mee dat activisten, georganiseerde criminaliteit en buitenlandse mogendheden er toegang toe hebben en er misbruik van kunnen maken. Daarnaast brengen ook onbedoelde cyberincidenten risico's met zich.

1.2 Aanleiding en definitie

De Tweede Kamer heeft in het algemeen overleg van 1 juli 2011 de Minister van Veiligheid en Justitie vragen gesteld over het juridisch instrumentarium dat de Rijksoverheid met betrekking tot cyber security ter beschikking staat. De Minister van Veiligheid en Justitie heeft vervolgens aangekondigd een onderzoek te laten uitvoeren naar het juridisch kader met betrekking tot cyber security. Dit document is daarvan het resultaat.

In het kader van een dergelijk onderzoek is allereerst van belang wat onder "cyber security" moet worden verstaan. In dit document wordt aangesloten bij de definitie zoals gehanteerd in de Nationale Cyber Security Strategie. Cyber security wordt hierin omschreven als het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie en schade aan de integriteit van die informatie. Cyber security ziet derhalve zowel op opzettelijke als onopzettelijke incidenten en verstoringen van ICT-netwerken.

1.3 Opzet en indeling

Dit document beoogt, zoals toegezegd door de Minister van Veiligheid en Justitie, het juridisch kader met betrekking tot cyber security inzichtelijk te maken. Het document dient als basis om te identificeren waar knelpunten optreden, met als doel mogelijkheden tot verbetering in kaart te brengen. Cyber security is een breed terrein dat vele raakvlakken kent met andere beleidsterreinen, waaronder het privacybeleid en het buitenlands veiligheid- en defensiebeleid.

Deze terreinen zijn waar relevant meegenomen in dit juridisch kader. Voor het privacybeleid, waaronder de meldplicht datalekken (persoonsgegevens) verwijs ik u naar de brief aan uw kamer getiteld: Verwerking en bescherming persoonsgegevens (TK 2010-2011, 32 761 nr. 1) en de toezeggingen die ik heb gedaan tijdens het AO van 15 september 2011 Ten aanzien van de implicaties van de ontwikkelingen in het cyberdomein voor het buitenlands veiligheid- en defensiebeleid loopt er momenteel een adviesaanvraag bij de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagsstukken. Uw Kamer wordt hierover op korte termijn geïnformeerd.
De doelstelling van dit document vraagt om een praktische aanpak. Het document is hierom niet ingedeeld op juridische grondslag, maar op praktische toepassing. Het omvat ook geen uitputtend overzicht van wetgeving, maar legt de nadruk op wetgeving met een hoge mate van praktische relevantie.

Allereerst gaat het document in op het relevante grondwettelijk en verdragsrechtelijk kader. Vervolgens worden de verschillende fasen van het bevorderen van cyber security als uitgangspunt genomen: preventie, toezicht, meldplichten, interventie, opsporing en repressie. Tot slot worden de waarborgen besproken die gelden ten aanzien van overheidsoptreden op deze terreinen.

Deze thema's worden in het document in de volgende hoofdstukkenindeling besproken: grondwettelijk en verdragsrechtelijk kader (hoofdstuk 2), preventie en toezicht (hoofdstuk 3), meldplichten en maatregelen (hoofdstuk 4), opsporings- en interventiebevoegdheden (hoofdstuk 5) en repressie (hoofdstuk 6). Tot slot bespreekt deze analyse als gezegd de reeds genoemde waarborgen (hoofdstuk 7).

2 GRONDWETTELIJK EN VERDRAGSRECHTELIJK KADER

2.1 Inleiding

Het grondwettelijk en verdragsrechtelijk kader omschrijft de rechten en plichten van de overheid ten opzichte van burgers. Het grondwettelijk en verdragsrechtelijk kader is met name relevant als de wetgever besluit om aanvullende wet- en regelgeving met betrekking tot cyber security vast te stellen. In deze gevallen dient de wetgever te beoordelen of de wet- en regelgeving die is voorgesteld, past binnen dit kader.

Voor huidige wet- en regelgeving met betrekking tot cyber security geldt, dat deze reeds bij totstandkoming aan het grondwettelijk en verdragsrechtelijk kader is getoetst. In beginsel wordt wet- en regelgeving en overheidsoptreden na inwerkingtreding niet door de rechter aan het grondwettelijk kader getoetst: artikel 120 Grondwet ("**Gw**") sluit een dergelijke toetsing uit. Wel kan de rechter beoordelen of wet- en regelgeving en overheidsoptreden in lijn is met verdragen waarop een algemeen beroep kan worden gedaan, zoals het Internationaal Verdrag inzake burgerrechten en politieke rechten ("**IVBPR**"), het Europees Verdrag voor de Rechten van de Mens ("**EVRM**") en het Handvest van de grondrechten van de Europese Unie ("**Handvest**"). In dit Juridisch Kader zal hoofdzakelijk worden verwezen naar het EVRM en de Grondwet.

Het grondwettelijk en verdragsrechtelijk kader van cyber security valt uiteen in *positieve verplichtingen* en *grondrechten*. De positieve verplichtingen of zorgplichten bestaan uit verplichtingen voor de overheid om zorg te dragen voor bewoonbaarheid en infrastructuur van Nederland. Hieronder valt het waarborgen van de veiligheid van informatiesystemen en het adequaat reageren op incidenten en noodsituaties. Deze positieve verplichtingen worden hierna in paragraaf 2.2 behandeld.

De grondrechten bestaan uit de bescherming van persoonlijke levenssfeer, strafrechtelijk waarborgen zoals legaliteit en fair trial en bescherming van eigendom. Zij stellen grenzen aan de mogelijkheden voor de overheid om informatie over burgers te verzamelen, burgers te straffen of hun vrijheid te ontnemen en om, bijvoorbeeld in het kader van incidenten of noodsituaties, zaken te onteigenen. De grondrechten komen in paragraaf 2.3 aan de orde. Tot slot wordt in paragraaf 2.4 kort stil gestaan bij verdragsrechtelijke afspraken die specifiek zien op cyber security.

2.2 Positieve verplichtingen

2.2.1 Bewoonbaarheid land

Artikel 21 van de Gw legt een zorgplicht op aan de overheid met betrekking tot de bewoonbaarheid van het land en de bescherming en verbetering van het leefmilieu. Onder de bewoonbaarheid van het land valt onder meer het aanleggen van infrastructurele voorzieningen voor verkeer, industrie, wonen en recreatie.[1]

[1] Zie Kamerstukken *II*, 1975/76, nr. 3, p. 31.

Dit artikel dateert nog uit een tijd (1976) dat digitale informatiesystemen schaars waren en het maatschappelijk belang van dergelijke systemen beperkt was. Inmiddels hebben het Internet en diverse informatiesystemen die daarmee zijn verbonden echter een groot maatschappelijk belang[2] en behoren zij tot de vitale infrastructuur van Nederland. Het mag daarom worden aangenomen dat er op de wetgever een verplichting rust om wetgeving op te stellen die aan deze zorgplicht met betrekking tot informatiesystemen invulling geeft.[3] Strafbepalingen en opsporingsbevoegdheden met betrekking tot computercriminaliteit in het Wetboek van Strafrecht ("**Sr**") en Wetboek van Strafvordering ("**Sv**") vormen hiervan een voorbeeld.

2.2.2 Incidenten en noodtoestanden

Het maatschappelijk belang van Internet en digitale informatiesystemen maakt dat zich op Internet of op die informatiesystemen zich ook noodsituaties kunnen voordoen, die de in- of uitwendige veiligheid van Nederland kunnen aantasten. Hierbij kan bijvoorbeeld worden gedacht aan cyberaanvallen die nutsvoorzieningen of de staatsveiligheid bedreigen.

Artikel 103 Gw zet uiteen dat bij wet dient te worden bepaald in welke gevallen ter handhaving van de uit- of inwendige veiligheid een beperkte of algemene uitzonderingstoestand kan worden afgekondigd. De overheid heeft uitvoering gegeven aan deze grondwettelijke verplichting door invoering van de Coördinatiewet uitzonderingstoestanden.[4]

Hoewel deze wet niet is opgesteld met het oog op cyber security als zodanig, zou zij in zeer ernstige situaties wel in dat kader kunnen worden gebruikt. Dit geldt als een cyberincident leidt tot (i) bedreiging van een vitaal belang en de overheid kampt met (ii) ontoereikendheid van de normale bevoegdheden. In een dergelijk geval vallen bijzondere bevoegdheden vrij onder een veelheid aan wetten,[5] waaronder de Wet bescherming staatsgeheimen, de Onteigeningswet, de Telecommunicatiewet en de Luchtvaartwet. Op deze bevoegdheden komen wij in deze analyse nog nader terug (zie paragraaf 5.1.4).

In de regel zullen ook in een noodsituatie te nemen maatregelen aan het EVRM moeten worden getoetst. Artikel 15 EVRM[6] bepaalt echter dat Nederland bevoegd is af te wijken van de rechten en vrijheden in het EVRM, als zich een algemene noodtoestand voordoet die het bestaan van het land bedreigt.[7] Het artikel kan uitsluitend worden ingeroepen als de ernst van de situatie de te treffen maatregelen strikt noodzakelijk maakt en op voorwaarde dat deze niet in strijd zijn met

---

[2] Zie ook MvT Wijziging Telecommunicatiewet, 2010-2011, Kamerstukken *II* 32 549, nr. 3, par. 1.7.

[3] Vgl. Kamerstukken *II*, 1975/76, 13 873, nr. 3, p. 13-14.

[4] Coördinatiewet uitzonderingstoestanden, 3 april 1996, *Stb.* 1996, 365, zoals laatstelijk gewijzigd bij Wet van 17 mei 2010, *Stb.* 2010, 350.

[5] Bijlage A en B bij de Coördinatiewet uitzonderingstoestanden.

[6] Vergelijk artikel 4 IVBPR, dat een enigszins beperktere afwijkingsbevoegdheid schept ten opzichte van de rechten en vrijheden verwoord in het EVRM.

[7] Dit met uitzondering van artikel 2, behalve ingeval van dood als gevolg van rechtmatige oorlogshandelingen, en van de artikelen 3, 4, eerste lid en 7 EVRM.

andere verplichtingen die voortvloeien uit het internationale recht. Een dergelijke situatie zou zich bijvoorbeeld kunnen voordoen bij een cyberaanval van een vreemde mogendheid, die al dan niet wordt gecombineerd met (andersoortige) militaire actie.

2.3 Grondrechten

2.3.1 Persoonlijke levenssfeer

Op grond van artikel 10 Gw en artikel 8 van het EVRM[8] heeft iedereen recht op eerbiediging van zijn of haar persoonlijke levenssfeer. De persoonlijke levenssfeer omvat tal van terreinen, welke zeer uiteenlopend van aard zijn.[9] Sommige van deze deelterreinen genieten zelfstandige verdragsrechtelijke of grondwettelijke bescherming. Zo is het recht op bescherming van persoonsgegevens zelfstandig geregeld in artikel 8 van het Handvest van de grondrechten van de Europese Unie en artikel 16 van het Verdrag betreffende de werking van de Europese Gemeenschap. In de Grondwet zijn onder andere het recht op eerbiediging van de woning (artikel 12 Gw) en de communicatie via brief, telefoon en telegraaf (artikel 13 Gw) zelfstandig geregeld. Opgemerkt zij dat artikel 13 Gw thans niet van toepassing wordt geacht op digitale communicatie, bijvoorbeeld communicatie per e-mail.[10]

Uitgangspunt van deze bepalingen is dat de overheid uitsluitend beperkingen kan stellen aan de persoonlijke levensfeer in gevallen die bij of krachtens de wet zijn bepaald. Op grond van artikel 8 EVRM zijn beperkingen voorts alleen toegestaan indien deze noodzakelijk zijn ter bescherming van bepaalde belangen, waaronder de nationale en de openbare veiligheid, het economisch welzijn van een land en het voorkomen van wanordelijkheden en strafbare feiten. Artikel 10 lid 2 Gw vereist voorts dat de wet regels stelt met betrekking tot het vastleggen en verstrekken van persoonsgegevens.

De bovenstaande normen beogen individuen te beschermen tegen willekeurige inmenging door de overheid in hun persoonlijke levenssfeer. Deze normen zijn ook van belang in het kader van het bevorderen van cyber security. Ter opsporing van cyberaanvallen zullen immers mogelijk maatregelen worden genomen, die gevolgen hebben voor de persoonlijke levenssfeer van burgers. Uit bovenstaande grondrechten vloeit voort dat toepassing van dergelijke maatregelen alleen is toegestaan voor zover er hiertoe een wettelijke bevoegdheid bestaat. Daarnaast dient de overheid de door haar verkregen persoonsgegevens zorgvuldig en binnen de daartoe opgestelde wettelijke kaders (bijvoorbeeld de Wet bescherming persoonsgegevens) te behandelen.

---

[8] Vergelijk artikel 17 IVBPR en artikel 7 Handvest.

[9] Zie Kamerstukken *II*, 1975/76, 13 872, nr. 3 p. 40.

[10] De Staatscommissie Grondwet heeft in haar rapport van november 2010 een voorstel gedaan tot een nieuw artikel 13 Gw dat van toepassing zou moeten zijn op communicatie, ongeacht het communicatiemedium, zie: Staatscommissie Grondwet, Rapport Staatscommissie Grondwet, z.pl., november 2010, p. 85-88. Het rapport is beschikbaar op: http://www.staatscommissiegrondwet.nl/userfiles/files/Rapport%20Staatscommissie%20Grondwet_lowres(1).pdf.

2.3.2 Strafvervolging

De Grondwet omvat twee bepalingen die burgers beschermen tegen willekeurige vervolging en vrijheidsontneming door de overheid. Hierbij is uitgangspunt dat burgers uitsluitend mogen worden vervolgd ter zake van strafbare feiten. Op grond van artikel 16 Gw geldt dat geen feit strafbaar is dan uit kracht van een daaraan voorafgaande wettelijke bepaling. Hieruit volgt dat gedragingen niet met terugwerkende kracht strafbaar mogen worden gesteld of bestraft en dat de strafrechtelijke norm moet zijn bekendgemaakt voordat deze van kracht kan worden.[11]

Op grond van artikel 15 lid 1 Gw mag voorts aan niemand zijn vrijheid worden ontnomen zonder dat dit bij of krachtens de wet is geregeld. Onder vrijheidsontneming valt niet alleen het uitzitten van een vrijheidsstraf, maar ook het voorarrest Indien iemand zijn of haar vrijheid is ontnomen op basis van voorarrest, dient zijn of haar berechting op grond van artikel 15 lid 3 Gw binnen een redelijke termijn plaats te vinden. Op grond van het bovenstaande dient de overheid bij uitoefening van strafrechtelijke bevoegdheden in het kader van cyber security zeker te stellen dat de gedraging strafbaar is gesteld en (voorlopige) hechtenis is toegelaten.

2.3.3 Eerlijk proces

Op grond van artikel 6 lid 1 EVRM[12] heeft eenieder tegen wie vervolging is ingesteld recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij wet is ingesteld. Hiermee wordt de verdachte beschermd tegen willekeurig optreden van de overheid. Deze bescherming wordt nader ingevuld door het toekennen van een aantal verdedigingsrechten aan de verdachte in lid 3 van artikel 6 EVRM.[13]

Op grond van lid 2 van artikel 6 EVRM[14] dient de *onschuldpresumptie* in acht te worden genomen. Hieruit volgt dat van een ieder tegen wie vervolging is ingesteld, de onschuld wordt aangenomen, totdat zijn schuld in rechte is komen vast te staan. In de jurisprudentie van het EHRM is uitgemaakt dat ook het recht om niet mee te hoeven werken aan de eigen veroordeling en het zwijgrecht onderdeel uitmaken van het recht op een eerlijk proces in de zin van artikel 6 EVRM (*nemo tenetur*). De overheid dient in het kader van opsporing van cybercrime te voorkomen dat zij dwangmiddelen inzet op een wijze die in strijd is met de uit artikel 6 EVRM voortvloeiende rechten.

De rechten die volgen uit artikel 6 EVRM zijn toegekend aan een ieder zodra sprake is van een zogeheten "*criminal charge*". Hiervan is sprake indien de overtreder uit de handelingen van het

---

[11] Zie Kamerstukken *II*, 1975/76, 13 873, nr. 3, p. 51.

[12] Vergelijk artikel 14 IVBPR, dat een enigszins ruimere bescherming biedt dan artikel 6 EVRM, en artikel 47 Handvest.

[13] Zo heeft de verdacht onder meer het recht te beschikken over de tijd en faciliteiten die nodig zijn voor de voorbereiding van zijn verdediging en heeft hij, indien hij over onvoldoende middelen beschikt, het recht kosteloos door een toegevoegde advocaat te worden bijgestaan.

[14] Vergelijk artikel 14 IVBPR en artikel 47 Handvest.

overheidsorgaan redelijkerwijs kan afleiden dat tegen hem een strafproces in gang gezet zal worden of dat hem mogelijk een punitieve sanctie zal worden opgelegd. Hiervan kan niet alleen sprake zijn bij de strafrechtelijke vervolging van cybercrime, maar bijvoorbeeld ook in geval van het opleggen van een bestuurlijke boete wegens schending van in het kader van cyber security relevante zorg- of meldplicht.

2.3.4 Eigendom

Artikel 1 van het Eerste Protocol van het EVRM geeft iedere natuurlijke persoon of rechtspersoon het recht op een ongestoord genot van zijn eigendom. Het EVRM zet in dit kader uiteen dat alleen inbreuk kan worden gemaakt op een eigendomsrecht ten behoeve van het algemeen belang en onder de voorwaarden voorzien in de wet. In artikel 14 van de Gw is vastgelegd dat onteigening alleen kan geschieden bij wet, in het algemeen belang en tegen vooraf verzekerde schadeloosstelling. Indien het recht op eigendom in het algemeen belang enkel wordt beperkt, bestaat het recht op schadevergoeding op grond van artikel 14 lid 3 Gw alleen indien dit bij of krachtens de wet is bepaald. Het begrip "algemeen belang" wordt ruim uitgelegd.

Het kan in het kader van cyber security voorkomen dat de overheid zich genoodzaakt ziet om inbreuk te maken op de eigendomsrechten van personen of rechtspersonen. Te denken valt aan situaties waarin de overheid de controle over computersystemen of zelfs een onderneming zou willen overnemen, bijvoorbeeld bij de bestrijding van een cyberaanval die de in- of uitwendige veiligheid van Nederland kan aantasten (zie ook paragraaf 5.1.4). In een dergelijk geval dient de overheid zich ervan te vergewissen dat zij bevoegd is inbreuk te maken op het eigendomsrecht en dat dit in het algemeen belang vereist is.

2.4 Internationale afspraken

Het Cybercrimeverdrag[15] vormt een internationale basis voor de gecoördineerde aanpak van strafbare feiten verbonden met elektronische netwerken. In het verdrag zijn afspraken gemaakt over de materieel-strafrechtelijke gedragingen die de aangesloten landen in hun nationale wetgeving strafbaar dienen te stellen en over een aantal strafvorderlijke bevoegdheden dat zij in hun nationale wetgeving moet toekennen aan de met opsporing van strafbare feiten belaste organen. Daarnaast bevat het verdrag bepalingen over internationale samenwerking.

Een andere belangrijke internationale afspraak betreft het EU Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen. Dit Kaderbesluit heeft tot doel de samenwerking tussen justitiële en andere bevoegde autoriteiten van de lidstaten, zoals de politie en andere gespecialiseerde rechtshandhavingsinstanties, te verbeteren door middel van onderlinge afstemming van de strafrechtelijke bepalingen van de lidstaten op het gebied van aanvallen op informatiesystemen. Nederland heeft dit kaderbesluit geïmplementeerd in de Wet computercriminaliteit II.[16]

[15] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18.

[16] Wet van 1 juni 2006, *Stb.* 2006, 300.

Momenteel is een nieuw voorstel voor een Europese richtlijn over aanvallen op informatiesystemen aanhangig. Het voorstel strekt tot vervanging van Kaderbesluit 2005/222/JBZ,[17] dat op bepaalde punten tekort zou schieten door de toename van cyberaanvallen in zowel ernst als aantal. De voorgestelde richtlijn strekt tot verdergaande maatregelen ter bestrijding van cybercriminaliteit en verplicht lidstaten onder meer tot het instellen van hogere straffen op cybergerelateerde delicten zoals computervredebreuk en *denial-of-service* aanvallen.[18] Daarnaast adresseert het voorstel specifiek het probleem van botnets[19] en stelt het onder meer de productie, de verkoop en de invoer van instrumenten voor het plegen van strafbare feiten strafbaar.

[17] COM (2010)517 - Voorstel voor een Richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ.

[18] Aanval waarbij een groot aantal verzoeken of gegevens aan een computersysteem wordt gestuurd teneinde de werking daarvan negatief te beïnvloeden.

[19] Netwerk van computersystemen die zijn geïnfecteerd met kwaadaardige software en hierdoor onder controle staan van één persoon of organisatie.

3 PREVENTIE EN TOEZICHT

3.1 Inleiding

Dit hoofdstuk schetst het juridisch kader dat betrekking heeft op preventie en toezicht in het kader van cyber security. Het gaat hier om de fase voorafgaand aan een cyberincident of cyberaanval. Het is de fase waarin:

- door controle en verbetering van informatiebeveiliging potentieel een mogelijkheid bestaat om een cyberincident te voorkomen of een cyberaanval te verijdelen;
- door verzamelen van informatie risico's in kaart kunnen worden gebracht en kunnen worden bestreden voordat ze zich verwezenlijken;
- het NCSC een belangrijke taak zal vervullen bij het faciliteren van informatieuitwisseling tussen partijen met betrekking tot toe te passen beveiligingsmaatregelen.

Dit hoofdstuk gaat ten eerste in op wetgeving van algemene aard (paragraaf 3.2), waarbij het civiele recht, de bescherming van persoonsgegevens en de bevoegdheden van inlichtingen- en veiligheidsdiensten worden besproken. Ten tweede wordt in dit hoofdstuk een beschrijving gegeven van zorg- en preventieplichten in sectoren met grote maatschappelijke relevantie en bevoegdheden van toezichthouders om hierop toezicht uit te oefenen (paragraaf 3.3).

3.2 Wetgeving van algemene aard

3.2.1 Civiel recht

Het Burgerlijk Wetboek ("**BW**") en aanverwante wetgeving is relevant in situaties waarin de overheid of het bedrijfsleven (een gedeelte van) het onderhoud of de *hosting* van haar informatiesystemen uitbesteedt aan een externe leverancier. In die gevallen maken partijen in de regel onder meer contractuele afspraken met betrekking tot informatiebeveiliging, die onder andere kunnen zien op:

(a) het beveiligingsniveau dat de IT dienstverlener zal toepassen;
(b) controle die op het beveiligingsniveau kan worden uitgeoefend; en
(c) aansprakelijkheid van de IT dienstverlener bij niet-nakoming.

De contractuele afspraken vormen in een dergelijke opdrachtgever-opdrachtnemer relatie voor zowel de overheid als het bedrijfsleven een belangrijk preventief middel om het niveau van informatiebeveiliging te bevorderen. De hierboven genoemde aspecten worden hierna besproken.

(a) Beveiligingsniveau

Sommige IT overeenkomsten – met name standaardvoorwaarden van leveranciers – bevatten enkel een verplichting voor de leverancier om zich in te spannen om informatie op een passende wijze te beveiligen. In uitzonderingsgevallen is zelfs in het geheel niets over informatiebeveiliging bepaald. In deze gevallen kan van het Burgerlijk Wetboek een aanvullende werking uitgaan.

Hierbij kan worden gedacht aan artikel 7:401 BW, dat een opdrachtnemer verplicht om bij zijn werkzaamheden de zorg van een goed opdrachtnemer in acht te nemen. Ook kan worden gedacht aan de aanvullende werking van de redelijkheid en billijkheid van artikel 6:248 BW.

Veel uitonderhandelde IT overeenkomsten bevatten tegenwoordig een bepaling die uiteenzet dat het niveau van informatiebeveiliging zal voldoen aan een standaard, zoals de Code voor Informatiebeveiliging (ISO 27001 en 27002), SAS 70 en PCI DSS. Deze standaarden worden vastgesteld door onafhankelijke instituten en omvatten *controls* en *best practices* die door de dienstverlener dienen te worden gevolgd. Deze standaarden gelden overigens niet, althans niet zonder meer als in de overeenkomst met de dienstverlener daaromtrent niets is bepaald.

Om daadwerkelijke handhaving van het afgesproken beveiligingsniveau te bevorderen kan een contractuele boete worden overeengekomen op niet-nakoming van deze afspraken. Een boeteclausule vooronderstelt de instemming van de betrokken contractspartijen. De mate waarin een dienstverlener bereid en in staat is een boete overeen te komen houdt verband met diverse factoren, zoals (i) de mate van concreetheid van de gedraging waarop de boete wordt gesteld, (ii) de mate van 'control' die de dienstverlener heeft, (iii) verzekeringsaspecten, (iv) de hoogte van de boete, mede in samenhang met mogelijke andere contractuele sancties (zoals aanvullende schadevergoeding) en (v) de mate waarin subcontractors van de dienstverleners bereid en in staat zijn verantwoordelijkheden te dragen. Doorgaans wensen leveranciers geen boetes te aanvaarden voor risico's die 'beyond' hun control zijn of voor verantwoordelijkheden die contractueel in vage termen zijn omschreven.

(b) Controle

In veel uitonderhandelde overeenkomsten komt een bepaling voor die de opdrachtgever in staat stelt om het niveau van beveiliging zelf te controleren of dit door een externe derde te laten doen. Bij het uitonderhandelen van een dergelijke controlebevoegdheid is van belang dat de uitbestedende organisatie zich ervan bewust is dat de hiervoor genoemde beveiligingsstandaarden een grote mate van eigen beoordeling en invulling toelaten. Ook in gevallen waarin dit soort normen worden toegepast, is daarom van belang dat niet alleen toepassing van de norm zelf, maar ook het niveau van beveiliging wordt gecontroleerd.

(c) Aansprakelijkheid bij niet-nakoming

Civielrechtelijke afspraken zijn uitsluitend zoveel waard als de dienstverlener zelf. Zo bood DigiNotar geen verhaal meer, toen moederbedrijf Vasco enkele maanden na het beveiligingsincident het faillissement van haar dochteronderneming DigiNotar aanvroeg. De kredietwaardigheid van de dienstverlener is daarom van groot belang.

Daarnaast is ook de aansprakelijkheid die de dienstverlener aanvaardt zeer relevant. Bij het aangaan van een IT-overeenkomst is van belang om zeker te stellen dat de IT-dienstverlener

aansprakelijkheid voor beveiligingsincidenten of verlies van dan wel onbevoegde toegang tot gegevens niet geheel uitsluit of kwalificeert als overmacht indien de desbetreffende incidenten in de controlesfeer van de leverancier liggen. Voor incidenten welke het gevolg zijn van factoren die geheel of nagenoeg geheel buiten de controlesfeer van de leverancier liggen – bijvoorbeeld het uitvallen van het internet - ligt een uitsluiting of beperking van aansprakelijkheid of de contractuele kwalificatie tot overmacht wel voor de hand. De meeste IT-overeenkomsten bevatten een uitgebreide aansprakelijkheidsregeling, waarin aansprakelijkheid wordt gemaximeerd. In evenwichtige IT-contracten staat een dergelijke aansprakelijkheidsbeperking veelal in een juiste verhouding tot de opdrachtsom.

Opdrachtnemers zullen zich veelal tegen aansprakelijkheid wegens wanprestatie verzekeren. De praktijk leert echter dat een deel van de verzekeringsmarkt in meer of mindere mate dekking in verband met cyber risico's uitsluiten. Deze markt is thans sterk in beweging en thans geldt dat zeker niet alle risico's zonder meer verzekerbaar zijn. Echter, in geval van faillissement zullen de aan de opdrachtnemer uit te keren verzekeringspenningen in beginsel in de failliete boedel vallen, met als gevolg dat de opdrachtgever zich daarop niet kan verhalen. Men kan pogen dit via een cessie bij voorbaat van de verzekeringspenningen te voorkomen.

Een ander aspect van de aansprakelijkheid betreft de verplichting van de overheid om zelf, vanuit haar eigen verantwoordelijkheid en vanwege haar verplichtingen op grond van artikel 6:101 BW, binnen grenzen van redelijkheid de schade te beperken in de gevallen waarin een leverancier onverhoopt zijn contractuele verplichtingen inzake beveiliging zou schenden. Op de overheid rust, als afnemer van IT-diensten en producten, in dat opzicht een eigen wettelijke verplichting. Als goed opdrachtgever/afnemer zal de overheid in de regel haar schadebeperkende maatregelen tevoren moeten afstemmen of bespreken met de leverancier of dienstverlener in kwestie.

3.2.2 Bescherming persoonsgegevens

De Wet bescherming persoonsgegevens ("**Wbp**") beschermt de persoonlijke levenssfeer van natuurlijke personen bij verwerking van zogeheten "persoonsgegevens". Persoonsgegevens zijn gegevens die een natuurlijk persoon direct of indirect kunnen identificeren. De Wbp bepaalt onder meer dat persoonsgegevens uitsluitend in overeenstemming met de wet, op zorgvuldige wijze en voor welbepaalde doeleinden mogen worden verwerkt (zie hierover paragraaf 7.4.1). Artikel 14 Wbp verplicht verantwoordelijken een schriftelijke bewerkersovereenkomst te sluiten met een bewerker (derde partij).Het College Bescherming Persoonsgegevens ("**CBP**") houdt toezicht op de naleving van de Wbp.

Artikel 13 Wbp omvat de specifieke verplichting dat degene die de verantwoordelijke[20] is voor een gegevensverwerking passende technische- en organisatorische maatregelen dient te treffen om persoonsgegevens te beschermen tegen verlies of tegen enige vorm van onrechtmatige

[20] "Verantwoordelijke" is degene die doel en middelen van de gegevensverwerking vaststelt. Zie ook artikel 1 sub d Wbp.

verwerking. Dit beveiligingsvoorschrift strekt zich uit tot alle onderdelen van het proces van de gegevensverwerking en is gericht op voorkoming van "verlies of onrechtmatige verwerking". Met "onrechtmatige verwerking" wordt gedoeld op iedere verwerking die niet aan de Wbp voldoet. In de praktijk komt dit vooral neer op het voorkomen van de aantasting van gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

De beveiligingsplicht vereist dat de verantwoordelijke twee soorten maatregelen treft: technische en organisatorische. Onder technische maatregelen vallen bijvoorbeeld beveiliging van gegevens met een wachtwoord en encryptie bij opslag of verzending. Een voorbeeld van een organisatorische maatregel betreft een beperking van het aantal personen dat toegang heeft tot een bestand met persoonsgegevens. Deze organisatorische en technische maatregelen dienen een niveau van beveiliging te garanderen, dat gelet op de risico's van de verwerking en de aard van de te beschermen gegevens "passend" is.

Opgemerkt zij overigens dat op grond van artikel 2 Wbp deze wet niet van toepassing is op de verwerking van gegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten[21], ten behoeve van de uitvoering van de politietaak[22] en ter uitvoering van de Wet justitiële en strafvorderlijke gegevens[23] ("**Wjsg"**).[24] Het toezicht op de verwerking van persoonsgegevens ter uitvoering van de politietaak en de Wjsg is echter wel toebedeeld aan het CBP.[25]

3.2.3 Verplichtingen met betrekking tot informatieverwerking en -uitwisseling door de overheid

Voor de uitwisseling van informatie binnen de rijksdienst gelden diverse regels ten aanzien van de beveiliging van deze informatie. Als eerste kan worden gewezen op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 ("**Vir**"). Dit schrijft voor dat er technische en organisatorische maatregelen getroffen worden ter bevordering van de beveiliging van binnen de rijksdienst gedeelde informatie. Ten tweede kan worden gewezen op het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie ("**Vir-bi**") met betrekking tot "staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries". Dit Besluit kent vier categorieën van

[21] De verwerking van persoonsgegevens in dit kader is geregeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002. Zie paragraaf 7.4.2.

[22] De verwerking van persoonsgegevens in dit kader is geregeld in de Wet Politiegevens. Zie paragraaf 7.4.3.

[23] Over de verwerking van persoonsgegevens in dit kader zie paragraaf 7.4.4.

[24] Artikel 16 van het Verdrag betreffende de werking van de Europese Gemeenschap ("Verdrag van Lissabon") voorziet in een algemene rechtsgrondslag voor de bescherming van persoonsgegevens. Deze bescherming is ook van toepassing op de verwerking van persoonsgegevens in het kader van de politiële en justitiële samenwerking. De Privacyrichtlijn (95/46/EG) dient hieraan nog te worden aangepast. Zie daarover de Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de regio's, Brussel, 4 november 2010, (COM2010)609, paragraaf 2.3. Uiteindelijk zal deze aanpassing in de Nederlandse wet moeten worden geïmplementeerd.

[25] Zie artikel 27 en 39r Wjsg en artikel 35 Wpg.

bijzondere informatie, te weten (in afnemende mate van vertrouwelijkheid): zeer geheim, geheim, confidentieel en vertrouwelijk. In bijlage 3 bij dit Besluit staat per categorie aangegeven welk niveau van beveiliging gehandhaafd dient te worden en welke concrete maatregelen daarvoor moeten worden getroffen. Tot slot zij erop gewezen dat, indien de rijksdienst een IT-dienst uitbesteedt aan een externe dienstverlener, zij in de regel de Algemene rijksvoorwaarden bij IT-overeenkomsten ("**ARBIT**") dient op te leggen. Deze voorwaarden schrijven passende technische en organisatorische maatregelen voor omtrent de verwerking van persoonsgegevens. Er bestaat echter geen wettelijke verplichting tot gebruik van deze voorwaarden en de ARBIT is bovendien niet geschikt of bestemd voor complexe IT-transacties.

3.2.4 Inlichtingen- en veiligheidsdiensten

De Wet op de Inlichtingen en Veiligheidsdiensten 2002 ("**WIV**") omschrijft de taken en regelt de bevoegdheden van de Algemene Inlichtingen en Veiligheidsdienst ("**AIVD**") en de Militaire Inlichtingen- en Veiligheidsdienst ("**MIVD**"). Binnen de kaders van hun taken en bevoegdheden zijn de AIVD en de MIVD (samen aan te duiden als de "**Diensten**") bevoegd inlichtingen en informatie te verzamelen met betrekking tot cyber security. Daarom worden zij in dit hoofdstuk besproken.

Taken AIVD

De AIVD heeft op grond van artikel 6 lid 2 WIV de volgende taken in het belang van de nationale veiligheid:
a. het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat;
b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;
c. het bevorderen van maatregelen ter bescherming van de onder a genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheidsdienst en van het bedrijfsleven die naar het oordeel van Onze ter zake verantwoordelijke Ministers van vitaal belang zijn voor de instandhouding van het maatschappelijk leven;
d. het verrichten van onderzoek betreffende andere landen ten aanzien van onderwerpen die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers zijn aangewezen;
e. het opstellen van dreigings- en risicoanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 6, derde lid, onderdeel b, en 38, eerste lid, onderdeel c, van de Politiewet 1993 en de bewaking en de beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 15a van die wet.

In het kader van cyber security zijn met name de taken onder (a), (c) en onder (d), algemeen aangeduid als de "A-taak", de "C-taak", en de "D-taak", van belang.

De A-taak omvat het verrichten van onderzoek met betrekking tot organisaties en personen die door hun activiteiten of de doelen die zij nastreven worden vermoed een gevaar te vormen voor de democratische rechtsorde of voor de veiligheid of voor andere gewichtige belangen van de staat. Niet vereist is dat sprake is van een daadwerkelijke bedreiging van de nationale veiligheid: een potentiële bedreiging is voldoende voor het rechtvaardigen van een onderzoek. De (potentiële) dreiging van een cyberaanval kan, afhankelijk van het doel van die cyberaanval, hieronder vallen.

De focus van de onderzoeken in het kader van de A-taak wordt jaarlijks door de AIVD zelf bepaald op basis van een risico- en trendanalyse en kan derhalve ieder jaar veranderen. De AIVD heeft een duidelijke toename van incidenten betreffende cyber security waargenomen en besteedt hieraan dan ook aandacht.[26]

De C-taak van de AIVD ziet op het bevorderen van maatregelen ter bescherming van de in artikel 6 lid 2 sub (a) WIV genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens waarvan geheimhouding door de nationale veiligheid wordt geboden. Deze gegevens kunnen afkomstig zijn van onderdelen van de overheid en van vitale sectoren van het bedrijfsleven. De AIVD geeft uitvoering aan zijn C-taak door vanuit zijn specifieke kennis en expertise dreigingsinformatie te verstrekken ten behoeve van de organisaties die blijkens operationeel onderzoek blootstaan aan dreiging.[27] In het kader van cyber security adviseert de AIVD bijvoorbeeld over de bescherming van bijzondere informatie en maatschappelijk kritische processen tegen ICT-gerelateerde dreigingen.[28]

De D-taak van de AIVD heeft betrekking op het verrichten van onderzoek naar andere landen. De zogeheten inlichtingenbehoefte van de Nederlandse Regering wordt opgesteld door de Minister-president in samenspraak met de Minister van Binnenlandse Zaken en Koninkrijkrelaties, de Minister van Defensie en de Minister van Buitenlandse Zaken en vastgelegd in een Aanwijzingsbesluit.[29] Het huidige Aanwijzingsbesluit loopt van 2008 tot 2012 en richt de onderzoeken van de AIVD op (i) het inwinnen van inlichtingen omtrent de politieke intenties van regeringen, instellingen en inwoners van specifiek benoemde landen of regio's en (ii) het signaleren van en reageren op ontwikkelingen in landen of regio's die een potentiële dreiging ten aanzien van de nationale veiligheid vormen.[30] In het kader van cyber security kan hierbij worden gedacht aan informatie omtrent de voornemens en de capaciteit van personen of groeperingen om, al dan niet in opdracht van overheden of lokale machthebbers, een cyberaanval op Nederlandse overheden uit te voeren.

---

[26] Zie de brief van de Minister van Binnenlandse Zaken, 2 februari 2010, Kamerstukken *II*, 2009-2010, 30 977, nr.30.

[27] Zie http://www.aivdkennisbank.nl/jaarverslag/aDU3387_Veiligheidsbevordering.aspx.

[28] Zie Kamerstukken *II*, 2009-2010, 30 977, nr.30, p. 6.

[29] Jaarverslag AIVD 2010, p. 33.

[30] Jaarverslag AIVD 2010, p. 33.

Taken MIVD

De MIVD heeft op grond van artikel 7 lid 2 WIV de volgende taken in het belang van de nationale veiligheid:

(a) het verrichten van onderzoek naar:
- het potentieel en de strijdkrachten van andere mogendheden en
- factoren die van invloed kunnen zijn op de handhaving en bevordering van de internationale rechtsorde, voor zover de krijgsmacht daarbij betrokken kan worden;

(b) het verrichten van veiligheidsonderzoeken;

(c) het verrichten van onderzoek dat nodig is om maatregelen te treffen:
- om activiteiten te voorkomen die tot doel hebben de veiligheid of paraatheid van de krijgsmacht in gevaar te brengen,
- ter bevordering van een juist verloop van de mobilisatie en concentratie der strijdkrachten,
- voor een ongestoorde voorbereiding en inzet van de krijgsmacht, als bedoeld in onderdeel a, tweede bullet;

(d) het bevorderen van maatregelen ter bescherming van de onder (c) genoemde belangen, waaronder begrepen veiligheidsmaatregelen ten behoeve van de vertrouwelijke gegevens van de krijgsmacht;

(e) het verrichten van onderzoek naar andere landen ten aanzien van onderwerpen met een militaire relevantie die door de Minister-President zijn aangewezen; en

(f) het opstellen van dreigingsanalyses ter beveiliging van personen en objecten.[31]

---

[31] De volledige tekst van artikel 7 lid 2 WIV luidt als volgt.

De Militaire Inlichtingen- en Veiligheidsdienst heeft in het belang van de nationale veiligheid tot taak:

a. het verrichten van onderzoek:

1°. omtrent het potentieel en de strijdkrachten van andere mogendheden, ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht;

2°. naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden;

b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;

c. het verrichten van onderzoek dat nodig is voor het treffen van maatregelen:

1°. ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden;

2°. ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten;

3°. ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht als bedoeld in onderdeel a, onder 2°.

d. het bevorderen van maatregelen ter bescherming van de onder c genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens betreffende de krijgsmacht waarvan de geheimhouding is geboden;

e. het verrichten van onderzoek betreffende andere landen, ten aanzien van onderwerpen met een militaire relevantie die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers, zijn aangewezen;

f. het opstellen van dreigingsanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 6, derde lid, onderdeel b, en 38, eerste lid, onderdeel c, van de Politiewet 1993 en de bewaking en de beveiliging van de objecten

In het kader van cyber security zijn met name de taken onder (a), (c), (d) en (e), algemeen aangeduid als de "A-taak" , de "C-taak" , de "D-taak" en de "E-taak" van de MIVD, van belang.

De A-taak betreft het verrichten van onderzoek omtrent het potentieel van strijdkrachten van andere mogendheden en naar factoren die van invloed zijn op de internationale rechtsorde voor zover de krijgsmacht daarbij betrokken is of kan zijn. Ten aanzien van cyber kan gedacht worden aan de ontwikkeling van cybercapaciteiten van andere strijdkrachten en de eventuele dreiging die hier uit voortvloeit.

De C-taak van de MIVD voorziet in de bevoegdheid onderzoek te doen naar potentiële dreigingen ten aanzien van de veiligheid en paraatheid van de krijgsmacht.[32] In 2009 heeft de MIVD een begin gemaakt met het opbouwen van een normbeeld aangaande cyber security.[33] Al in 2009 werd er gesproken van een reële dreiging van een cyberaanval.

In het kader van haar D-taak stelt de MIVD zich ten doel bij te dragen aan de bescherming van Defensiebelangen tegen interne en externe bedreigingen. In dat kader tracht de MIVD dreigingen tegen Defensie en de defensie-industrie te onderkennen en te identificeren en het op basis hiervan (laten) treffen van maatregelen ter bescherming van de te behartigen belangen.[34] In dat kader adviseert de MIVD ook op het gebied van gegevensbeveiliging.[35]

De E-taak van de MIVD heeft betrekking op het verrichten van onderzoek naar andere landen. De inlichtingenbehoefte is vastgelegd in het Aanwijzingsbesluit. Deze aanwijzing wordt aan beide diensten verstrekt waarin beide diensten een aantal landen toegewezen krijgt. Het betreft hier informatie die via andere, bijvoorbeeld diplomatieke, kanalen niet of moeilijk te verkrijgen is. Met betrekking tot cyber security kan gedacht worden aan de cybercapaciteiten van landen en of groeperingen die door middel van hun cyberactiviteiten een bedreiging kunnen vormen ten aanzien van de nationale veiligheid.

Bevoegdheden AIVD/MIVD

De Diensten hebben op grond van artikel 12 WIV een algemene bevoegdheid tot gegevensverwerking, die echter wordt begrensd door de eisen gesteld in artikel 13 WIV. Binnen deze context zijn de Diensten op grond van artikel 17 WIV bevoegd zich voor het verzamelen

---

en de diensten die zijn aangewezen op grond van artikel 15a van die wet, voor zover het betreft personen, objecten en diensten met een militaire relevantie.

[32] De Commissie van Toezicht betreffende de Inlichtingen- en VeiligheidsDiensten ("**CTIVD**") stelt zich op het standpunt dat in dit verband geen sprake hoeft te zijn van een concrete aanleiding. Zie Kamerstukken *II*, 2010-2011, 29 924, nr. 61, p. 12.

[33] Jaarverslag 2009 Militaire Inlichtingen- en Veiligheidsdienst 2009, p. 47, beschikbaar op: http://www.defensie.nl/mivd/publicaties_en_formulieren/publicaties/.

[34] Jaarverslag MIVD 2010, p. 11.

[35] Jaarverslag MIVD 2010, p. 11.

van gegevens te wenden tot eenieder die wordt gedacht de benodigde gegevens te kunnen verstrekken, waaronder bestuursorganen en de verantwoordelijke voor een gegevensverwerking. Daarnaast zijn de Diensten bevoegd gegevens te verzamelen uit publiek beschikbare bronnen, hetgeen ook wel bekend staat als open-source intelligence ("**OSINT**").

De Diensten hebben met betrekking tot een aantal taken tevens bijzondere bevoegdheden. Voor de AIVD geldt dit voor de A- en de D-taak en voor de MIVD geldt dit voor de A-, de C-, en de E-taak.

Verplichtingen met betrekking tot gegevensverwerking door de Diensten

Artikel 16 WIV legt de Diensten enkele verplichtingen op met betrekking tot de verwerking van gegevens. Met name artikel 16 sub b verplicht de Diensten de nodige technische en organisatorische voorzieningen te treffen tegen onbevoegde gegevensverwerking en ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens.

3.3 Sectorale verplichtingen

Naast bovengenoemde algemene regelgeving bestaat ook op sectoraal niveau relevante regelgeving in het kader van de preventie van cyberincidenten. Deze regelgeving is toegespitst op de specifieke risico's en omstandigheden in sectoren met een groot maatschappelijk belang. Wij gaan hierna in op preventie en toezicht met betrekking tot cyber security bij:

(a) financiële instellingen;
(b) nutsvoorzieningen;
(c) telecommunicatiediensten;
(d) zorginstellingen;
(e) spoorvervoer en luchtvaart.

(a) Financiële instellingen

Financiële instellingen die uit hoofde van de Wet op het financieel toezicht ("**Wft**") onder toezicht staan van De Nederlandse Bank ("**DNB**") en/of de Autoriteit Financiële Markten (de "**AFM**") dienen ingevolge artikel 3:17[36] en artikel 4:14[37] Wft hun bedrijfsvoering zodanig in te richten dat zij voorzien in een beheerste en integere bedrijfsuitoefening.

Hieronder valt tevens het beheersen van bedrijfsprocessen en bedrijfsrisico's. In dit verband bepalen artikel 20 lid 2 Besluit prudentiële regels Wft ("**Bpr Wft**") en artikel 30 lid 1 sub c Besluit gedragstoezicht financiële ondernemingen Wft ("**Bgfo**") dat financiële instellingen over procedures en maatregelen dienen te beschikken om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen. In dit

[36] Dit artikel geldt voor een betaalinstelling, clearinginstelling, entiteit voor risicoacceptatie, kredietinstelling, premiepensioeninstelling of verzekeraar met een zetel in Nederland.

[37] Dit artikel geldt voor een beheerder, beleggingsinstelling, beleggingsonderneming, bewaarder of pensioenbewaarder.

verband kan blijkens de parlementaire geschiedenis worden gedacht aan het maken van veiligheidskopieën, herstelmaatregelen en een calamiteitenplan dat regelmatig wordt geactualiseerd en op een goede werking wordt getest.[38]

Het toezicht op de naleving van bovenstaande artikelen wordt uitgeoefend door DNB en de AFM. Welke van deze twee toezichthouders bevoegd is, is afhankelijk van de financiële onderneming in het specifieke geval.

In het kader van hun toezichthoudende taken beschikken de AFM en DNB over de toezichtbevoegdheden uit de Algemene wet bestuursrecht ("**Awb**"), zoals:

- het betreden van plaatsen, met uitzondering van de woning zonder toestemming van de bewoner (5:15 Awb);
- het vorderen van inlichtingen (5:16 Awb);
- het vorderen van inzage in zakelijke gegevens en bescheiden (5:17 Awb); en
- het onderzoeken en aan op- of monsterneming onderwerpen van zaken (5:18 Awb).

Een ieder is op grond van artikel 5:20 Awb verplicht hieraan medewerking te verlenen.

(b) Nutsvoorzieningen

Voor energiebedrijven gelden algemeen geformuleerde zorgplichten ten aanzien van kwaliteit, betrouwbaarheid en beveiliging. De netbeheerders van gas- en elektriciteitsnetwerken dienen over doeltreffende systemen te beschikken om de veiligheid en de betrouwbaarheid van het transport van elektriciteit en gas te waarborgen.[39] De vergunninghouder van een kerncentrale dient de beveiligingsmaatregelen te treffen die redelijkerwijs noodzakelijk zijn om de inrichting te beveiligen tegen de dreigingen zoals omschreven in de referentiedreiging.[40] Voor drinkwaterbedrijven – allen bestuursorganen[41] – gelden voorts verplichtingen om de productie, distributie, kwaliteit en duurzaamheid van drinkwater zeker te stellen.[42]

De voornoemde verplichtingen zien niet specifiek op cyber security en preventie van cyberincidenten. Er kan echter wel een verplichting in worden gelezen om een toereikend niveau van informatiebeveiliging te hanteren, voor zover de betrouwbaarheid van de betreffende nutsvoorziening van een informatiesysteem afhankelijk is.

De Raad van Bestuur van de Nederlandse Mededingingsautoriteit ("**RvB NMa**") is belast met het

[38] Zie Nota van toelichting Bpr Wft, Staatsblad 2006, 519, p. 112.

[39] Zie artikel 16 lid 1 sub b Elektriciteitswet en artikel 8 Gaswet.

[40] Zie artikel 3 Regeling beveiliging nucleaire inrichtingen en splijtstoffen, *Stcrt*, 2010, nr. 19950. De referentiedreiging is een langetermijnanalyse van dreigingen van diefstal van categorie I, II of III-materiaal dan wel van sabotage van dat materiaal, of van inrichtingen. De vastgestelde referentiedreiging is niet openbaar.

[41] Zie artikel 3 Drinkwaterwet.

[42] Zie artikel 7 Drinkwaterwet.

toezicht op de naleving van de zorgplichten van gas- en elektriciteitsnetbeheerders.[43] De RvB NMa beschikt in dit verband over de toezichtbevoegdheden uit de Awb, zoals hierboven onder (a) beschreven. De ambtenaren zoals aangewezen in het Besluit aanwijzing toezichtambtenaren zijn daarnaast belast met handhaving van de Kernenergiewet.[44] Ook deze ambtenaren beschikken in dit verband over de toezichtbevoegdheden uit de Awb, zoals hierboven onder (a) uiteen gezet. In aanvulling daarop beschikken de ambtenaren over de bevoegdheid, met medeneming van de benodigde apparatuur, een woning binnen te treden zonder toestemming van de bewoner.[45]

Het Besluit aanwijzing ambtenaren VROM-regelgeving wijst ambtenaren aan die zijn belast met het toezicht op de Drinkwaterwet.[46] In het kader van hun toezichthoudende taak beschikken deze ambtenaren over de toezichtbevoegdheden uit de Awb, zoals hierboven onder (a) uiteen gezet.

(c) Telecommunicatiediensten

Aanbieders van communicatienetwerken en -diensten zijn onderworpen aan een zorgplicht ex artikel 11.3 Telecommunicatiewet ("**Tw**") om passende technische en organisatorische maatregelen ten behoeve van de veiligheid en de beveiliging van de door hen aangeboden netwerken en diensten te treffen. Dit met het oog op de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.[47]

Op grond van artikel 14.6 Tw is de Minister van Economische Zaken bevoegd regels te stellen ten behoeve van de voorbereiding van het verzorgen van elektronisch transport van gegevens in buitengewone omstandigheden.[48] Deze regels kunnen ook zien op de daaromtrent aan de

---

[43] Zie artikel 59 lid 1 Gaswet en artikel 5 lid 1 Elektriciteitswet 1998.

[44] Zie artikel 58 Kernenergiewet jo. het Besluit aanwijzing toezichtsambtaren Kernenergiewet.

[45] Zie artikel 59 lid 2 Kernenergiewet.

[46] Zie artikel 48 jo. Besluit aanwijzing ambtenaren VROM-regelgeving.

[47] Op grond van artikel 15.1 lid 3 Tw zijn de door het College van de Onafhankelijke Post en Telecommunicatie Autoriteit aangewezen ambtenaren belast met het toezicht op de zorgplicht ex artikel 11.3 Tw. Zij kunnen in dit verband gebruik maken van de toezichtsbevoegdheden in de Awb, zoals hierboven onder (a) omschreven.
Overigens zijn aanbieders van communicatienetwerken en -diensten op grond van artikel 11.2 Tw tevens gehouden zorg te dragen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van hun netwerk en/of diensten. Het toezicht hierop is eveneens op grond van artikel 15.1 lid 3 Tw toebedeeld aan de door het College van de OPTA aangewezen ambtenaren.
Het toezicht op de verwerking van verkeers- en locatiegegevens, als bedoeld in artikel 11.5, 11.5a en 11.13, is op grond van artikel 15.1 lid 1 sub h jo. artikel 2 lid 1 van het Besluit aanwjzing toezichthouders Telecommunicatiewet toebedeeld aan het Agentschap Telecom.

[48] De Minister van Economische Zaken is hiertoe slechts bevoegd na overleg met de Ministers van Binnenlandse Zaken en van Defensie.

Minister te verstrekken informatie. Op grond van artikel 14.6 lid 2 Tw zijn deze regels alleen van toepassing op door de Minister aangewezen telecomaanbieders. Bij beleidsregel is bepaald dat als zodanig worden aangewezen aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten die de volgende diensten aanbieden: (a) openbare vaste spraaktelefonie, (b) openbare mobiele spraaktelefonie of (c) toegang tot breedbandinternet.[49] Op grond van artikel 4 van de Regeling voorbereiding buitengewone omstandigheden sector telecommunicatie 2007 zijn de aangewezen aanbieders gehouden de Minister jaarlijks te informeren over in het kader van artikel 14.6 lid 1 Tw getroffen voorbereidingen.[50]

In het op artikel 18.2 Tw gebaseerde Besluit universele dienstverlening en eindgebruikers ("**Bude**") is een bepaling opgenomen ten aanzien van zogeheten "*cookies*" en vergelijkbare software. Een cookie is een stukje informatie dat door een website kan worden geplaatst op de computer van een bezoeker, waardoor onder meer het surfgedrag van deze bezoeker kan worden gevolgd. Op grond van artikel 4.1 Bude is het plaatsen van cookies enkel toegestaan indien de gebruiker hierover is geïnformeerd en op kenbare wijze in de gelegenheid is gesteld dit te weigeren.

In artikel 18.8 Tw is de mogelijkheid opgenomen voor de Minister van Economische Zaken om met betrekking tot de veiligheid en de beveiliging van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten regels te stellen. Deze regels kunnen technische en organisatorische eisen bevatten die aan Telecomaanbieders kunnen worden gesteld. Aan deze bevoegdheid is echter vooralsnog geen uitvoering gegeven.[51]

Met betrekking tot alle bij of krachtens de Tw te nemen maatregelen en regels geldt op grond van artikel 18.13 Tw dat hierbij het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer alsmede de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken in acht dient te worden genomen.

Momenteel is een wetsvoorstel tot wijziging van de Telecommunicatiewet aanhangig.[52] In dit wetsvoorstel is onder meer een uitbreiding van de beveiligingsplicht opgenomen, in die zin dat Telecomaanbieders ingevolge het voorgestelde artikel 11a.1 lid 1 Tw passende technische en organisatorische maatregelen dienen te nemen om de risico's voor de veiligheid en integriteit van

---

[49] Beleidsregel aanwijzen aanbieders telecommunicatie in verband met buitengewone omstandigheden, *Stcrt* 2011, 5400.

[50] Op grond van artikel 15 lid 1 sub j Tw jo artikel 2 lid 2 van het Besluit aanwjjzing toezichthouders Telecommunicatiewet wordt toezicht gehouden op de naleving van de verplichtingen ex artikel 14.6 Tw door de senior beleidsmedewerkers van de directie Telecommarkt van het directoraat-generaal voor Energie, Telecom en Markten.

[51] Indien de Minister van Economische Zaken ervoor zou kiezen regels te stellen op grond van deze bevoegdheid, dan komt het toezicht op de naleving van deze regels op grond van artikel 15.1 lid 3 Tw toe aan de bij besluit van het College van de OPTA aangewezen ambtenaren.

[52] Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, Kamerstukken *II*, 32 549, nr. 2. is op 25 juli 2011 door de Tweede Kamer aangenomen en ligt op dit moment bij de Eerste Kamer ter inzage.

hun netwerken en diensten te beheren.[53] Door middel van het woord "passend" wordt gewaarborgd dat de maatregelen geschikt zijn, gezien de stand van de techniek en de risico's die zich voordoen.[54] In het voorgestelde Besluit continuïteit telecommunicatie worden nadere regels gesteld met betrekking tot onder meer de technische en organisatorische maatregelen en eisen als bedoeld in het voorgestelde artikel 11a.1 Tw.[55]

(d) Zorginstellingen

In de zorgsector geldt een algemene zorgplicht uit hoofde van artikel 3 van de Kwaliteitswet zorginstellingen ("**Kzi**"). Dit artikel zet uiteen dat de zorgaanbieder de zorgverlening op zodanige wijze dient te organiseren, van zodanig personeel en materieel dient te voorzien en zorg dient te dragen voor een zodanige verantwoordelijkheidstoedeling, dat een en ander leidt of redelijkerwijs moet leiden tot een verantwoorde zorg.[56] Deze verplichting ziet niet specifiek op cyber security en preventie van cyberincidenten. Er kan echter wel een verplichting in worden gelezen om een toereikend niveau van informatiebeveiliging te hanteren, als de zorgverlening van het betreffende informatiesysteem afhankelijk is.

De Nederlandse norm (NEN) 7510, "Medische informatica - Informatiebeveiliging in de zorg - Algemeen" ("**NEN 7510**"), voorziet in uitgebreide voorschriften betreffende de beveiliging van informatie in zorginstellingen. Naleving van deze norm is verplicht op grond van artikel 10 van de Wet gebruik burgerservicenummer in de zorg en artikel 2 van de Regeling gebruik burgerservicenummer in de zorg.

Het toezicht op deze algemene zorgplicht wordt uitgeoefend door ambtenaren van het Staatstoezicht op de volksgezondheid, ook wel bekend als de Inspectie voor de gezondheidszorg ("**IGZ**").[57] De IGZ hanteert daarbij de NEN 7510 als referentiekader[58] en kan in dit verband gebruik maken van de toezichtsbevoegdheden in de Awb, zoals omschreven onder (a). In aanvulling hierop zijn de ambtenaren bevoegd een woning binnen te treden zonder toestemming van de bewoner, voor zover de woning deel uitmaakt van een instelling.[59] Zij zijn voorts bevoegd

[53] Artikel 11a.1 lid 2 voorziet bovendien in een verplichting om aanbieders van openbare telefoondiensten en aanbieders van openbare elektronische communicatienetwerken, waarover openbare telefoondiensten worden aangeboden, om alle noodzakelijke maatregelen te nemen om de beschikbaarheid van de openbare telefoondiensten over de openbare elektronische communicatienetwerken zo volledig mogelijk te waarborgen in geval van een technische storing of uitval van het elektriciteitsnetwerk.

[54] Zie Kamerstukken *II*, 2010-2011, 32 549, nr. 3, p. 82.

[55] Op grond van artikel BF sub b van het wetsvoorstel zal het toezicht op de zorgplicht ex artikel 11a.1 Tw op grond van artikel 15.1 lid 1 sub j jo. artikel 2 lid 2 van het Besluit aanwijzing toezichthouders Telecommunicatiewet worden uitgeoefend door de senior beleidsmedewerkers van de directie Telecommarkt van het directoraat-generaal voor Energie, Telecom en Markten.

[56] Zie artikel 3 Kzi.

[57] Zie artikel 7 lid 1 Kzi.

[58] Zie Kamerstukken *II*, 2010-2011, 27 529, nr. 82.

[59] Zie artikel 7 lid 2 Kzi.

tot inzage van de patiëntendossiers.[60]

(e) Spoorvervoer en luchtvaart

Ook in de spoorwegsector en de luchtvaartsector gelden algemene zorgplichten met betrekking tot kwaliteit, duurzaamheid en veiligheid.[61] In deze algemene zorgplichten kan de verplichting worden gelezen om een adequaat beveiligingsniveau te hanteren ter preventie van cyberincidenten, in die gevallen dat de kwaliteit en veiligheid van het spoor respectievelijk de luchtvaart afhankelijk is van elektronische informatiesystemen.

Spoorvervoer

De beheerder van een hoofdspoorweginfrastructuur dient op grond van artikel 16 lid 1 Spoorwegwet zorg te dragen voor de kwaliteit, betrouwbaarheid en beschikbaarheid van de infrastructuur. De minister van Verkeer en Waterstaat verleent concessies aan een of meerdere beheerders. Aan deze concessie wordt in elk geval het voorschrift verbonden om de risico's van het gebruik en beheer voor de veiligheid van hoofdspoorwegen te analyseren en passende maatregelen te nemen, waaronder het zo nodig buiten dienst stellen van een gedeelte van de hoofdspoorweg, om deze risico's afdoende te beheersen, waarbij rekening wordt gehouden met de specifieke vereisten van de te verwachten bedrijfsvoering en de stand der techniek.[62]

Een spoorwegonderneming heeft ingevolge artikel 27 Spoorwegwet onder meer een zogeheten veiligheidsattest nodig om gebruik te mogen maken van de hoofdspoorwegen. Teneinde dit veiligheidsattest te krijgen dient de spoorwegonderneming onder andere aan te tonen dat deze door toepassing van een adequaat veiligheidszorgsysteem veilig gebruik kan maken van de spoorweg.[63] In dit verband dient de spoorwegonderneming de aan de bedrijfsvoering verbonden risico's te onderkennen en passende maatregelen te nemen om deze afdoende te beheersen, daarbij rekening houdend met de stand der techniek en de binnen de bedrijfstak aanwezige kennis en richtsnoeren voor een veilige bedrijfsvoering.[64]

Ambtenaren van de Inspectie van Verkeer en Waterstaat zijn belast met het toezicht op bovenstaande eisen.[65] Zij kunnen in dit verband gebruik maken van de toezichtsbevoegdheden in de Awb, zoals omschreven onder (a).

Luchtvaart

Op grond van artikel 1.3 van de Wet Luchtvaart is een luchtvaartmaatschappij verplicht ervoor

[60] Zie artikel 7 lid 3 Kzi.

[61] Zie artikelen 16, 16a en 32 Spoorwegwet, en artikelen 1.3 en 5.23 Wet Luchtvaart.

[62] Zie artikel 17 Spoorwegwet.

[63] Zie artikel 32 Spoorwegwet.

[64] Zie artikel 33 lid 2 sub c Spoorwegwet. Nadere regels met betrekking tot de bedrijfsvoering staat in het Besluit bedrijfsvergunning en veiligheidsattest hoofdspoorwegen.

[65] Zie artikel 69 Spoorwegwet jo. Besluit aanwijzing toezichthouders spoorwegen.

zorg te dragen dat de door haar geëxploiteerde luchtvaartuigen in een zodanige staat zijn, dat daarmee veilig gevlogen en vervoerd kan worden. Luchtverkeersleiding Nederland ("**LVNL**") is voorts, ter bevordering van een zo groot mogelijke veiligheid van het luchtverkeer, belast met een aantal specifieke taken. In dit verband kan worden gedacht aan het verlenen van communicatie-, navigatie- en plaatsbepalingsdiensten.[66] In het kader van deze taken is de LVNL grotendeels afhankelijk van elektronische (informatie)systemen.

Belast met het toezicht op de veiligheidstaken van de LVNL zijn de ambtenaren van het Ministerie van Verkeer en Waterstaat die op grond van artikel 11 lid 1 sub b van de Wet Luchtvaart bij het Besluit aanwijzing toezichthouders luchtvaart zijn aangewezen. Zij maken hierbij gebruik van de toezichtsbevoegdheden in de Awb, zoals omschreven onder (a).

[66] Zie artikel 5.23 Wet Luchtvaart.

4 MELDPLICHTEN EN MAATREGELEN

4.1 Inleiding

Dit hoofdstuk schetst het juridisch kader dat betrekking heeft op meldplichten en overige op eigen initiatief te treffen maatregelen. Het gaat hier om de fase dat zich een cyberincident voordoet of (zeer) kort geleden heeft voorgedaan. In deze fase:

- is het van groot belang dat de juiste partijen worden opgelijnd;
- kunnen er bij beursgenoteerde instellingen koerseffecten optreden als nieuws over de cyberincident bekend wordt;
- kunnen interne maatregelen het verschil maken tussen een beheersbaar incident en oncontroleerbare gevolgschade; en
- kunnen sporen worden veiliggesteld die kunnen leiden tot opsporing en vervolging van eventuele daders;

Het hoofdstuk bespreekt ten eerste wetgeving van algemene aard (paragraaf 4.2), waarbij de strafrechtelijke aangifteplicht, het civiel recht en de bescherming van persoonsgegevens aan bod komen. Het hoofdstuk geeft ten tweede een beschrijving van meldplichten in sectoren met grote maatschappelijke relevantie en bevoegdheden van toezichthouders om hierop toezicht uit te oefenen (paragraaf 4.3).

4.2 Wetgeving van algemene aard

4.2.1 Strafrechtelijke aangifteplicht

Artikel 160 Sv verplicht eenieder die kennis draagt van bepaalde bijzondere misdrijven om daarvan onverwijld aangifte te doen. In het kader van cyber security lijkt in twee gevallen sprake te zijn van een aangifteverplichting, te weten:

- **Schending van een staatsgeheim** – Schending of ongerechtvaardigd bezit van een staatsgeheim is strafbaar gesteld in artikel 98-98c Sr. Als staatsgeheim moet worden aangemerkt informatie "waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat of zijn bondgenoten".[67] Dergelijke informatie kan bijvoorbeeld worden buitgemaakt bij een cyberaanval op een overheidsinstantie of een door die overheidsinstantie ingeschakelde (onder)aannemer. De Staat stelt de rubricering van gegevens vast. Uiteindelijk kan door de rechter worden getoetst of er daadwerkelijk sprake is van een staatsgeheim.[68]

- **Levensgevaar** – Bepaalde aantastingen van computersystemen kunnen levensgevaar veroorzaken. Deze aantastingen van computersystemen zijn strafbaar gesteld in artikel 161sexies lid 1 sub 3 of 4 Sr en artikel 161septies sub 2 of 3 Sr. Men kan hierbij

[67] Artikel 1 sub a en b Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie.

[68] Vgl. Vz Rb Amsterdam 14 juni 2004, LJN: AP4278.

bijvoorbeeld denken aan de aantasting van de administratie van een ziekenhuis, waardoor patiënten niet meer kunnen worden behandeld of verkeerde behandelingen krijgen. Ook kan men denken aan een aantasting van een systeem dat het lucht-, spoor- of wegverkeer regelt, waardoor zich botsingen met dodelijke afloop kunnen voordoen.

De plicht tot het doen van aangifte ontstaat door kennis van een feitencomplex dat in redelijkheid kan worden gekwalificeerd als een van de bovengenoemde misdrijven. Ook kennis van medeplichtigheid, poging tot het plegen of voorbereiding van een van deze misdrijven resulteert in een aangifteverplichting.[69] Een aangifteverplichting bestaat niet voor personen die door het doen van aangifte het gevaar lopen zelf vervolgd te worden en personen die een verschoningsrecht toekomt.

Het niet doen van aangifte in strijd met de aangifteplicht is op grond van artikel 135 Sr strafbaar gesteld. De strafbaarheid treedt echter alleen in, als het misdrijf ook daadwerkelijk heeft plaatsgevonden en komt vast te staan dat door het doen van aangifte het misdrijf had kunnen worden voorkomen.

4.2.2 Civiel recht

Contractuele meldplichten

IT-overeenkomsten bevatten in toenemende mate een bepaling, die de dienstverlener verplicht om cyberincidenten aan de klant te melden. Probleem met het maken van een dergelijke afspraak is dat een beveiligingsincident in de ogen van een IT-dienstverlener nog beheersbaar kan zijn, terwijl dit in de ogen van de klant al lang niet meer het geval is.

IT-overeenkomsten bevatten in veel gevallen een geheimhoudingsbeding, waaraan tevens de verplichting is gekoppeld de andere partij te informeren als de geheimhouding van gegevens niet langer kan worden gewaarborgd. Als bij (bijvoorbeeld) een cyberaanval een hacker (mogelijkerwijs) toegang heeft tot gegevens die vallen onder een dergelijke bepaling, is degene die zich tot geheimhouding heeft verplicht, verplicht hiervan aan de andere contractspartij melding te doen. In de praktijk is bij een cyberaanval vaak onduidelijk tot welke gegevens een hacker toegang heeft. In een dergelijk geval kan de IT-dienstverlener die zich tot geheimhouding heeft verplicht, zich mogelijk met succes op overmacht (artikel 6:75 BW) beroepen. Niet-nakoming van een meldplicht kan de IT-dienstverlener in dit geval niet worden toegerekend.

Overigens kan in gevallen dat niet is overeengekomen dat een IT-dienstverlener een aantasting van haar informatiebeveiliging dient te melden, een dergelijke verplichting onder omstandigheden wel worden afgeleid uit de aanvullende werking van de redelijkheid en billijkheid (artikel 6:248 BW) en de verplichting van de IT-dienstverlener om als goed opdrachtnemer te handelen (artikel 7:401 BW).

[69] Dit vloeit voort uit 139 Sv, dat bepaalt dat waar in Sv van een misdrijf gesproken wordt, tevens wordt gedoeld op medeplichtigheid aan, poging tot, of voorbereiding van dat misdrijf, tenzij waar de wet anders bepaalt.

Onrechtmatige daad

Onder omstandigheden zal het niet melden van een aantasting van informatiebeveiliging, in het bijzonder wanneer dit gepaard gaat met een verlies van persoonsgegevens, een onrechtmatige daad (artikel 6:162 BW) opleveren tegen degenen die daardoor schade lijden. Er kan worden betoogd, dat de partij die voorwerp is van de cyberaanval en nalaat om belanghebbenden op de hoogte te stellen, in strijd handelt met ongeschreven betamelijkheids- of zorgvuldigheidsnormen. Een voorbeeld van een dergelijke situatie zou kunnen zijn, dat een beheerder van een gecompromitteerde database met creditcard gegevens nalaat om de financiële instellingen die die creditcards hebben uitgegeven te informeren. In een dergelijk geval is goed mogelijk dat een rechter zal oordelen dat de beheerder van die database toerekenbaar onrechtmatig heeft gehandeld en verplicht is om de schade (bijvoorbeeld ontstaan door creditcardfraude) te vergoeden.

4.2.3 Wet bescherming persoonsgegevens

De Wbp omvat op dit moment geen verplichting om het verlies van controle over persoonsgegevens te melden. Wel geldt uit hoofde van de Wbp een informatieplicht met betrekking tot de verwerking van persoonsgegevens.[70] De informatieplicht brengt mee dat degene die verantwoordelijk is voor een verwerking van persoonsgegevens, de personen op wie de persoonsgegevens betrekking hebben (betrokkenen) op de hoogte dient te stellen van informatie die nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen jegens betrokkenen (zie ook paragraaf 7.4.1).[71]

De gewijzigde e-privacy richtlijn (2009/136/EG) stelt dat als er (waarschijnlijk) sprake is van ‘adverse effects’ de betrokkene moet worden geïnformeerd. Een wijizigingsvoorstel van de Telecommunicatiewet ter implementatie van die richtlijn ligt op dit moment voor in de Eerste Kamer.

Een verantwoordelijke die in strijd handelt met de informatieplicht uit de Wbp handelt in strijd met de wet en daarom onrechtmatig (artikel 6:162 BW, zie ook hiervoor). Voor zover deze onrechtmatige daad de verantwoordelijke kan worden toegerekend, dient de verantwoordelijke de schade die als gevolg daarvan ontstaat te vergoeden.

4.3 Sectorale verplichtingen

Naast bovengenoemde algemene regelgeving bestaat ook op sectoraal niveau relevante regelgeving met betrekking tot meldplichten en interne maatregelen. Hierna gaan wij in op de verschillende sectoren met een groot maatschappelijk belang, die ook reeds in paragraaf 3.3 werden geïdentificeerd.

[70] Artikel 33 en 34 Wbp.

[71] Artikel 34 lid 3 Wbp.

Wij beginnen de bespreking echter met een uiteenzetting van meldplichten, of beter gezegd: openbaarmakingsverplichtingen van beursgenoteerde instellingen.

(a.1) Beursgenoteerde instellingen

Ingevolge artikel 5:25i lid 2 Wft dient een Nederlandse beursgenoteerde onderneming koersgevoelige informatie onverwijld openbaar te maken. Van koersgevoelige informatie is kort gezegd sprake wanneer een redelijk handelende belegger waarschijnlijk ten dele gebruik zou maken van deze informatie bij het nemen van een beleggingsbeslissing. De beursgenoteerde onderneming mag op grond van artikel 5:25i lid 3 Wft de openbaarmaking van koersgevoelige informatie enkel uitstellen indien:

(i) het uitstel een rechtmatig belang dient;
(ii) van uitstel geen misleiding van het publiek te duchten is; en
(iii) de vertrouwelijkheid van de informatie kan worden gewaarborgd.

De vraag is onder welke omstandigheden een cyberincident kan leiden tot openbaarmakingsverplichtingen onder deze regeling.

Een eerste reden kan zijn dat (niet kan worden uitgesloten dat) hackers zichzelf toegang hebben verschaft tot koersgevoelige informatie, waarvan bekendmaking door de onderneming is uitgesteld. Op dat moment wordt niet langer voldaan aan de zojuist genoemde voorwaarde sub (iii). De onderneming moet in dat geval de koersgevoelige informatie onmiddellijk openbaar maken.

Een tweede reden kan zijn dat de computercriminaliteit zelf resulteert in koersgevoelige informatie. Bij ondernemingen die geconfronteerd worden met een cyberincident bestaat vaak grote onzekerheid over het moment waarop het cyberincident resulteert in koersgevoelige informatie. Het enkele feit dat er computercriminaliteit plaatsvindt of heeft plaatsgevonden, levert vermoedelijk geen openbaarmakingsverplichting op, omdat een redelijk handelend belegger dat enkele feit in de regel niet van invloed zal laten zijn op een investeringsbeslissing. Dit is anders wanneer de computercriminaliteit ernstige gevolgen heeft of kan hebben voor de onderneming. Voorbeelden van situaties waarin openbaarmakingsverplichtingen zouden kunnen ontstaan zijn:

- **verlies van controle over financiële verslaglegging** – als de betrouwbaarheid van de financiële rapportage richting aandeelhouders ter discussie komt te staan, bijvoorbeeld omdat de hacker toegang heeft tot de administratie van de onderneming;
- **aantasting winstpotentieel of winstverwachting** – als het winstpotentieel van de onderneming of de winstverwachting materieel moet worden bijgesteld, bijvoorbeeld door reputatieschade of diefstal van intellectueel eigendom en bedrijfsgeheimen;

- **materiële schadeclaims** – als er materiële schadeclaims worden verwacht, bijvoorbeeld van beleggers of klanten wier gegevens zijn gelekt of van partijen met wie een geheimhoudingsbeding is gesloten dat wordt geschonden;[72]
- **strategische koerswijziging** – als de computercriminaliteit noopt tot een strategische koerswijziging of ingrijpende wijziging van activiteiten, bijvoorbeeld doordat een online dienst niet meer kan worden aangeboden;[73] en
- **materiële kosten** – als er materiële kosten worden verwacht, bijvoorbeeld juridische kosten, kosten om de informatiebeveiliging van de onderneming te herstellen of kosten om klanten te informeren.

De beslissing of daadwerkelijk sprake is van koersgevoelige informatie wordt genomen door het bestuur van de onderneming. In de Verenigde Staten heeft een groep leden van het Congres recentelijk Mary Shapiro, de voorzitter van de Securities and Exchange Commission (SEC), in een open brief opgeroepen om duidelijk te maken onder welke omstandigheden ondernemingen investeerders moeten informeren over een cyberincident.[74] Vooralsnog heeft de SEC aan deze oproep geen gevolg gegeven.

(a.2) Financiële instellingen

Op grond van de artikelen 3:10 lid 3[75] of 4:11 lid 4 Wft[76] dient een onder toezicht staande financiële onderneming DNB of de AFM onverwijld te informeren over zogeheten incidenten.

Indien een cyberaanval heeft plaatsgevonden waardoor de (controle)systemen van de financiële onderneming niet meer naar behoren functioneren en/of niet meer betrouwbaar zijn kan een onderneming mogelijk haar integriteit niet meer waarborgen. In dit verband kan bijvoorbeeld worden gedacht aan systemen waarmee in een financiële onderneming wordt geregistreerd welke werknemer welke transacties verricht of aan systemen waarmee (wettelijk vereiste) *customer due diligence* wordt uitgevoerd.

Door het niet of gebrekkig functioneren van deze systemen verliest de financiële onderneming mogelijk (een deel van) haar zicht op en controle over de integriteit van haar bedrijfsprocessen. Indien dit het geval is, bestaat een ernstig gevaar voor de integere bedrijfsvoering van de onderneming en dient het cyberincident als incident bij de AFM of DNB te worden gemeld. Naast

[72] Zie ook brochure "Koersgevoelige Informatie", Autoriteit Financiële Markten, pagina 8, te vinden via http://www.afm.nl/layouts/afm/default.aspx~/media/files/brochures/2009/kgi.ashx.

[73] Een voorbeeld hiervan is het Sony PlayStation-incident, dat ertoe heeft geleid dat het PlayStation netwerk niet in zijn oude vorm kon worden voortgezet. Zie ook brochure "Koersgevoelige Informatie", Autoriteit Financiële Markten, pagina 9.

[74] http://online.wsj.com/article/SB10001424052748704681904576317571066403808.html?mod=WSJ_Tech_LEFTTopNews

[75] Dit artikel geldt voor een betaalinstelling, clearinginstelling, entiteit voor risicoacceptatie, kredietinstelling, premiepensioeninstelling of verzekeraar met een zetel in Nederland.

[76] Dit artikel geldt voor een beheerder, beleggingsinstelling, beleggingsonderneming, bewaarder of pensioenbewaarder.

het melden van het incident dient de onder toezicht staande financiële onderneming maatregelen te treffen om de aan het incident verbonden risico's te beheersen en herhaling te voorkomen.[77]

(b) Nutsvoorzieningen

Indien zich met betrekking tot een gastransportnet een voorval voordoet of heeft voorgedaan, waardoor nadelige gevolgen voor de mens of het milieu zijn ontstaan of dreigen te ontstaan, dient de netbeheerder dit voorval zo spoedig mogelijk te melden aan de Minister van Economische Zaken.[78] Deze verplichting kan met zich brengen dat de gasnetbeheerder een cyberincident dient te melden, als hieruit nadelige gevolgen voor mens of milieu (dreigen te) ontstaan. In de Elektriciteitswet zijn geen specifieke meldplichten opgenomen.[79]

Inrichtingen die betrokken zijn bij het produceren of verwerken van (grondstoffen voor) kernenergie[80] hebben bepaalde plichten op grond van artikel 39 Kernenergiewet. Op grond van dit artikel is eenieder verplicht de burgemeester te informeren indien men weet of redelijkerwijs kan vermoeden dat een ongeval zich voordoet met een kernenergie-inrichting. De burgemeester meldt dit onverwijld aan de Minister van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer. Daarnaast staat het de exploitant van de inrichting vrij om zelf informatie te verschaffen aan de burgemeester. Dit artikel kan van belang zijn in het geval dat er bij een cyberaanval een inbreuk wordt gemaakt op de elektronische controlesystemen van een dergelijke inrichting of de ordelijke werking daarvan niet meer gegarandeerd is als gevolg van een cyberincident.

Op grond van artikel 49 Drinkwaterwet dient de eigenaar van een drinkwaterbedrijf, collectieve watervoorziening of collectief leidingnet onmiddellijk kennis te geven aan de toezichthouder[81] van omstandigheden die, naar hij redelijkerwijs kan vermoeden, gevaar of beletsel voor de kwaliteit van het drinkwater kunnen opleveren. Indien een cyberincident dergelijke gevolgen teweeg kan brengen door bijvoorbeeld een ernstige aantasting van het functioneren van zuiveringsinstallaties, dient de eigenaar dit te melden aan de toezichthouder.

(c) Telecommunicatiediensten

Telecomaanbieders zijn op grond van artikel 11.2 en 11.3 Tw verplicht zorg te dragen voor de vertrouwelijkheid van de gegevens van abonnees en zijn verplicht abonnees te informeren als deze vertrouwelijkheid in gevaar komt.

---

[77] Artikel 17 lid 6 en artikel 19 lid 2 Besluit gedragstoezicht financiële ondernemingen Wft.

[78] Zie artikel 8a Gaswet.

[79] Mogelijk vallen energie-inrichtingen onder andere wetten, zie bijvoorbeeld de Kernenergiewet.

[80] Zie voor definities artikel 38 Kernenergiewet.

[81] Op grond van artikel 48 jo. 49 Drinkwaterwet jo. artikel 3 Besluit aanwijzing ambtenaren VROM-regeling zijn als toezichthouders aangewezen De inspecteur-generaal, de hoofddirecteur Uitvoering en de directeuren-inspecteur van het Inspectoraat-Generaal VROM en de door hen daartoe aangewezen, onder hun bevelen werkzame ambtenaren.

Er zijn voorts twee meldplichten voor cyberincidenten voor Telecomaanbieders in voorbereiding.[82]

Het wetsvoorstel voorziet (onder voorbehoud van behandeling door de Eerste Kamer) allereerst in een nieuw artikel 11a.2, dat Telecomaanbieders verplicht om de Minister van Economische Zaken onverwijld in kennis te stellen van een inbreuk op de veiligheid of een verlies van integriteit, waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke
mate werd onderbroken. Ten tweede voorziet het wetsvoorstel in een nieuw artikel 11.3a Telecommunicatiewet dat aanbieders van openbare elektronische communicatiediensten verplicht om:

- de Onafhankelijke Post en Telecommunicatie Autoriteit ("**OPTA**") te informeren als er sprake is van een inbreuk op de beveiliging van een elektronische communicatiedienst, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens;
- betrokkenen te informeren als een dergelijke inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer; en
- een overzicht bij te houden van alle inbreuken in verband met persoonsgegevens.

Deze meldplichten hebben uitsluitend betrekking op Telecomaanbieders. De laatstgenoemde meldplicht is echter ook relevant voor ondernemingen die diensten bij Telecomaanbieders afnemen. Als gevolg van een cyberincident kunnen immers naast persoonsgegevens van de Telecomaanbieder zelf ook persoonsgegevens van ondernemingen die diensten afnemen worden gelekt. Het kan hierbij (bijvoorbeeld) gaan om gegevens van personeelsleden of klanten van de onderneming.

(d) Zorginstellingen

Op grond van artikel 4a van de Kzi dient een zorgaanbieder iedere calamiteit binnen de instelling, waaronder verstaan dient te worden een niet-beoogde of onverwachte gebeurtenis, die betrekking heeft op de kwaliteit van de zorg en die tot de dood van of een ernstig schadelijk gevolg voor een patiënt of cliënt van de instelling heeft geleid,[83] onverwijld aan de IGZ te melden.

Deze meldplicht ziet niet specifiek op cyber security, maar dekt wel cyberincidenten die de dood of een ernstig schadelijk gevolg voor een patiënt of cliënt van de instelling hebben. De melding heeft onder meer tot doel dat, indien de calamiteit verder gaat dan het incidentele geval, speciale maatregelen kunnen worden getroffen om uitbreiding van de calamiteit of herhaling van de calamiteit elders te voorkomen.[84]

---

[82] Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, Kamerstukken *II*, 32 549, nr. 2. is op 25 juli 2011 door de Tweede Kamer aangenomen en ligt op dit moment bij de Eerste Kamer ter inzage.

[83] Zie artikel 4a lid 2 Kzi.

[84] Zie Kamerstukken *II*, 2001-2002, 28 498, nr. 3, p. 2.

De NEN 7510 schrijft in paragraaf 13.1.1 voor dat, wanneer patiëntgegevens onbedoeld openbaar zijn geraakt, de zorginstelling patiënten die het betreft daarvan in kennis behoort te stellen.[85]

(e) Spoorvervoer en luchtvaart

Op grond van artikel 7.1 van de Wet Luchtvaart dienen voorvallen, waaronder dient te worden verstaan een operationele onderbreking, defect, fout of andere onregelmatigheid, waardoor de vliegveiligheid wordt of kan worden beïnvloed (met uitzondering van "ongevallen" in de zin van richtlijn 94/56/EG[86]), door de exploitant of de gezagvoerder van een luchtvaartuig en een bedrijfsleider van een luchthaven[87] te worden gemeld bij de Minister van Verkeer en Waterstaat. In de Regeling melding voorvallen in de burgerluchtvaart (van 12 december 2006) wordt geregeld dat de melding verder dient te geschieden aan het Analyse Bureau Luchtvaartvoorvallen van de Inspectie Verkeer en Waterstaat ("**ABL**"). Bij het ABL kunnen ook voorvallen worden gemeld waarvoor geen meldplicht bestaat, maar die door de melder als reëel of mogelijk gevaar worden beschouwd.[88] Hoewel deze meldplichten niet specifiek zien op cyber security, worden bedreigingen van informatiesystemen die noodzakelijk zijn voor de vliegveiligheid er wel door gedekt.

[85] Zie ook paragraaf 3.3 (d) Zorginstellingen.

[86] Zie artikel 1.1 Wet Luchtvaart. Ongevallen in de zin van Richtlijn 94/56/EG zijn ongevallen die plaatsvinden tussen het tijdstip van instappen en uitstappen van de passagiers en waarbij een persoon – als gevolg van bepaalde oorzaken- dodelijk of ernstig gewond raakt, het luchtvaartuig schade of een structureel defect oploopt of het luchtvaartuig wordt vermist of volledig onbereikbaar is.

[87] Besluit melding voorvallen in de burgerluchtvaart (van 24 november 2006, zoals laatstelijk gewijzigd bij Besluit van 1 september 2008).

[88] Zie artikel 4 van de Regeling melding voorvallen in de burgerluchtvaart.

5 INTERVENTIE EN OPSPORING

Dit hoofdstuk schetst het juridische kader dat betrekking heeft op interventie en opsporing. Het gaat hier om de fase dat zich een cyberincident voordoet of (zeer) kort geleden heeft voorgedaan en de overheid een noodzaak ziet tot ingrijpen. In deze fase:

- heeft de overheid onder bepaalde omstandigheden de bevoegdheid in te grijpen als de organisatie die voorwerp is van het incident er zelf niet in slaagt deze onder controle te brengen;
- kunnen daders worden opgespoord; en
- kunnen bewijsmiddelen worden veiliggesteld.

Hieronder volgt een inventarisatie van de interventie- en opsporingsbevoegdheden die de overheid in een dergelijk geval toekomen. Deze bevoegdheden zijn van strafvorderlijke, bestuursrechtelijke en (in beperkte mate) van civielrechtelijke aard. De belangrijkste algemene en sectorale bestuursrechtelijke bevoegdheden zullen tevens aan de orde komen in het hierop volgende hoofdstuk over handhaving en repressie. Bestuursorganen kunnen hun bevoegdheden immers aanwenden zowel voor preventief toezicht als voor onderzoek na een incident.

De inhoud van dit hoofdstuk is als volgt. Eerst wordt in paragraaf 5.1 ingegaan op de algemene mogelijkheden voor de overheid om te interveniëren ingeval van een cyberincident. Daarna wordt in paragraaf 5.2 ingegaan op de mogelijkheden tot interventie zoals deze zijn opgenomen in de sectorale wetgeving. Tot slot worden in paragraaf 5.3 de meest relevante strafvorderlijke opsporingsbevoegdheden in het kader van cybercriminaliteit besproken.

5.1 Algemene interventiebevoegdheden

In deze paragraaf komen de algemene bevoegdheden van de overheid aan de orde, waarmee de overheid kan ingrijpen in het geval zich een cyberincident voordoet bij een organisatie met maatschappelijke relevantie. In dit verband worden achtereenvolgens de mogelijkheden in het bestuursrecht, het strafvorderlijk kader en het civiele recht behandeld. Daarna wordt ingegaan op de bevoegdheden die de overheid heeft in het geval van een zogeheten noodtoestand.

5.1.1 Bestuursrecht

De Awb voorziet in één bevoegdheid die zich goed leent voor interventie. Op grond van artikel 5:31 Awb is een bestuursorgaan dat bevoegd is om een last onder bestuursdwang op te leggen in spoedeisende gevallen bevoegd om te besluiten dat de bestuursdwang zal worden toegepast zonder voorafgaande last. De vereiste onderliggende bevoegdheid tot het opleggen van een last onder bestuursdwang kan niet aan de Awb worden ontleend, maar moet in een bijzondere wet zijn voorzien. De nadruk bij interventie komt aldus duidelijk te liggen bij bijzondere wetgeving.

5.1.2 Strafvordering

Het Wetboek van Strafvordering bevat sommige opsporingsbevoegdheden die gebruikt kunnen

worden voor interventie. Een voorbeeld hiervan is de bevoegdheid tot het ontoegankelijk maken van gegevens, zoals in het volgende deel van dit hoofdstuk wordt besproken. Het grootste deel van de dwangmiddelen opgenomen in het Wetboek van Strafvordering is echter primair gericht op het nemen van strafvorderlijke beslissingen.

Dit ligt enigszins anders bij de Wet op de Economische Delicten ("**WED**"). Deze wet voorziet in een (beperkte) interventiemogelijkheid, namelijk in de vorm van voorlopige maatregelen. Op grond van artikel 29 WED kunnen deze ter zake van bepaalde economische delicten worden getroffen, indien tegen de verdachte ernstige bezwaren zijn gerezen en tevens de belangen, die door het vermoedelijk overtreden voorschrift worden beschermd, onmiddellijk ingrijpen vereisen. In dat geval kan ten eerste onderbewindstelling dan wel gehele of gedeeltelijke stillegging worden bevolen van de verdachte onderneming. Tevens kan gehele of gedeeltelijke ontzetting worden bevolen van bepaalde rechten of voordelen, die de verdachte in verband met zijn onderneming van overheidswege zijn of zouden kunnen worden toegekend. Te denken valt aan vergunningen. Tot slot kan de verdachte worden bevolen dat hij zich van bepaalde handelingen onthoudt of zorg draagt voor de opslag en bewaring van bepaalde voor inbeslagneming vatbare voorwerpen. Opgemerkt zij dat gegevens, voor zover niet vastgelegd op een gegevensdrager, niet als zodanig worden beschouwd.

5.1.3 Civiel recht

Een IT dienstverlener die haar verplichtingen uit overeenkomst toerekenbaar niet of niet op de juiste wijze nakomt, pleegt wanprestatie (artikel 6:74 BW). De opdrachtgever heeft in dit geval de mogelijkheid om met tussenkomst van een rechter een derde partij in te schakelen, die de werkzaamheden alsnog op een deugdelijke wijze uitvoert. De kosten hiervan kan de opdrachtgever op de wanpresterende partij verhalen. Om deze bevoegdheid te kunnen uitoefenen dient de opdrachtgever de wanpresterende partij wel eerst in gebreke te stellen en gelegenheid te bieden de werkzaamheden zelf uit te voeren, voor zover tenminste contractueel niet anders is overeengekomen.

Deze regeling levert in het kader van cyber security onder omstandigheden een potentiële interventiemogelijkheid op. Als een opdrachtgever constateert dat een IT dienstverlener in strijd handelt met de overeenkomst (eventueel aangevuld door werking van redelijkheid en billijkheid (artikel 6:248 BW) en goed opdrachtnemerschap (artikel 7:401 BW, zie ook paragraaf 3.2.1) kan de opdrachtgever (na ingebrekestelling en tussenkomst van een rechter) een andere partij inschakelen om de werkzaamheden alsnog te doen uitvoeren. Een voorbeeld is het geval dat een IT dienstverlener een te laag niveau van beveiliging heeft toegepast en voorwerp is geworden van een cyberaanval. De opdrachtgever kan dan een derde inschakelen, om het beveiligingsniveau te verhogen en de cyberaanval af te weren. De opdrachtgever kan deze bevoegdheid via een civielrechtelijk kort geding afdwingen als de IT dienstverlener hieraan geen medewerking wenst te verlenen. Opgemerkt zij dat het overnemen van een opdracht door een andere opdrachtnemer de nodige praktische problemen kan opleveren en ook de afwikkeling met de voorgaande, wanpresterende opdrachtnemer de nodige aandacht zal vergen.

5.1.4 Bevoegdheden in bijzondere omstandigheden

Diverse regelingen voorzien in bijzondere bevoegdheden of een herverdeling van bevoegdheden voor het geval zich bijzondere omstandigheden voordoen. Hieronder worden enkele van deze regelingen besproken. Daaraan voorafgaand zij gewezen op het Nationaal Handboek Crisisbesluitvorming, waarin de procedures alsmede de coördinatie- en besluitvormingsstructuren op rijksniveau voor de beheersing van (dreigende) crises zijn neergelegd. Dit handboek is van toepassing op álle (dreigende) crisissituaties die een interdepartementaal gecoördineerd optreden van de Rijksoverheid vereisen.

Gemeentewet

Op grond van artikelen 175 Gemeentewet is de burgemeester bevoegd alle bevelen te geven die hij nodig acht ter handhaving van de openbare orde of ter beperking van gevaar. De burgemeester is hiertoe bevoegd in geval van oproerige beweging, van andere ernstige wanordelijkheden of van rampen, dan wel van ernstige vrees voor het bestaan daarvan. Daarnaast kan de burgemeester onder deze omstandigheden op grond van artikel 176 Gemeentewet algemeen verbindende voorschriften uitvaardigen.

Bovenstaande bevoegdheden mogen slechts worden gebruikt indien de reguliere bevoegdheden van de burgemeester tekortschieten. De praktijk leert dat deze bevoegdheden in uiteenlopende situaties kunnen worden toegepast. Het is denkbaar dat een ernstig cyberincident op lokaal niveau dusdanig destabiliserende gevolgen teweegbrengt dat kan worden overgegaan tot toepassing van één van deze noodbevoegdheden.

Wet veiligheidsregio's

Op grond van de Wet veiligheidregio's komt de burgemeester ook andere noodbevoegdheden toe. Deze zijn toepasbaar in geval van een ramp of crisis, welke worden gedefinieerd als respectievelijk *"een zwaar ongeval of een andere gebeurtenis waarbij het leven en de gezondheid van veel personen, het milieu of grote materiële belangen in ernstige mate zijn geschaad of worden bedreigd en waarbij een gecoördineerde inzet van diensten of organisaties van verschillende disciplines is vereist om de dreiging weg te nemen of de schadelijke gevolgen te beperken"* en *"een situatie waarin een vitaal belang van de samenleving is aangetast of dreigt te worden aangetast"*.[89] Hieronder kan onder omstandigheden ook een ernstig cyberincident met grote maatschappelijke gevolgen worden geschaard.

Op grond van artikel 62 van de Wet veiligheidsregio's is de burgemeester in dit verband bevoegd alle plaatsen te betreden om (mogelijke gevolgen van) rampen of crises te voorkomen.

Indien zich een ramp of crisis van meer dan plaatselijke betekenis voordoet, wordt op grond van artikel 39 Wet veiligheidsregio's een Regionaal Beleidsteam gevormd. De voorzitter van de veiligheidsregio,

[89] Artikel 1 Wet veiligheidregio's.

tevens korpsbeheerder van de regiopolitie, neemt dan de (nood)bevoegdheden van de burgemeester op grond van de gemeentewet over.

Herindeling ministeriële taken in geval van een terroristische dreiging met een urgent karakter

In geval van een terroristische dreiging met een urgent karakter kan de Minister van Veiligheid en Justitie bepaalde bevoegdheden, die normaliter aan andere ministers toekomen, aan zich trekken. Daartoe is vereist dat onverwijlde uitoefening van die bevoegdheden noodzakelijk is om maatregelen te nemen (i) ter voorkoming van een terroristisch misdrijf als bedoeld in artikel 83 Sr of (ii) om op voorhand de gevolgen daarvan te beperken. De Minister van Veiligheid en Justitie kan hiertoe alleen overgaan indien overleg of overeenstemming over die maatregelen met de normaliter bevoegde minister binnen de beschikbare tijd niet mogelijk is. Een en ander is bepaald in het Besluit tijdelijke herindeling ministeriële taken in geval van een terroristische dreiging met een urgent karakter.

Coördinatiewet uitzonderingstoestanden

Indien de reeds van kracht zijnde bevoegdheden ontoereikend zijn, kan worden overgegaan tot toepassing van de Coördinatiewet uitzonderingstoestanden ("**Cwu**"). De Cwu regelt de afkondiging van de noodtoestand.

Deze wet bepaalt dat ingeval buitengewone omstandigheden dit noodzakelijk maken de beperkte of algemene noodtoestand kan worden afgekondigd. Het begrip "buitengewone omstandigheden" is niet wettelijk gedefinieerd. Ingeval van een op nationaal niveau paralyserend cyberincident is denkbaar dat sprake is van buitengewone omstandigheden, zoals hier bedoeld.

De Cwu onderscheidt twee uitzonderingstoestanden: de beperkte noodtoestand en de algemene noodtoestand. Onder zowel de beperkte als de algemene noodtoestand treden bepaalde noodbepalingen van rechtswege in werking. Andere noodbepalingen dienen echter bij koninklijk besluit op voordracht van de Minister-President in werking te worden gesteld. Ingeval van afkondiging van de beperkte noodtoestand kunnen bepalingen, genoemd in lijst A bij de wet, in werking worden gesteld. Ingeval van afkondiging van de algemene noodtoestand kunnen bepalingen, genoemd in lijst B bij de wet, in werking worden gesteld. Het onderscheid is hierin gelegen dat ten tijde van de beperkte noodtoestand kan worden afgeweken van grondwettelijke bepalingen inzake de bevoegdheden van bestuursorganen van decentrale overheden, terwijl ten tijde van de algemene noodtoestand kan worden afgeweken van grondrechten.[90] Noodtoestanden kunnen worden afgekondigd voor geheel Nederland of een gedeelte daarvan. De praktijk leert overigens dat zeer zelden omstandigheden aanwezig zijn die een afkondiging van de noodtoestand rechtvaardigen.

Voorbeelden van bevoegdheden die vrijvallen in zowel een beperkte als een algemene noodtoestanden zijn:

[90] Openbare orde en veiligheid, Tekst & Commentaar, aantekening Coördinatiewet uitzonderingstoestanden, sub 2.f. p. 1319.

- Artikel 14.4 Telecommunicatiewet

Op grond van artikel 14.4 Tw is de Minister van Economische Zaken bevoegd aan Telecomaanbieders aanwijzingen te geven met betrekking tot onder meer (i) de instandhouding en exploitatie van hun openbare telecommunicatienetwerken en (ii) het verzorgen en gebruiken van hun openbare telecommunicatienetwerken.[91]

- Artikel 9.3 en 9.4 Wet Luchtvaart

Op grond van artikel 9.3 en 9.4 van de Wet Luchtvaart kunnen de Minister van Verkeer en Waterstaat en de Minister van Defensie aanwijzingen geven aan de Luchtverkeersleiding Nederland ("**LVNL**").

- Artikel IIIA Wet bescherming staatsgeheimen

Op grond van artikel IIIA van de Wet bescherming staatsgeheimen ("**Wbs**") kan elk werk van openbaar verkeer en elk werk van openbaar nut ter bescherming van gegevens waarvan de geheimhouding door het belang van de veiligheid van de staat wordt geboden (een staatsgeheim) als zogeheten verboden plaats worden aangemerkt.

Overigens kunnen diverse noodbepalingen ook separaat, dat wil zeggen buiten afkondiging van een noodtoestand, in werking worden gesteld. Een voorbeeld hiervan is artikel 14.4 lid 1 Tw, dat voorziet in een aanwijzingsbevoegdheid aan aanbieders van openbare telecommunicatienetwerken en -diensten. Op grond van artikel 14.2 Tw kan deze bepaling zowel op grond van de Cwu als buiten een noodtoestand in werking worden gesteld.

Onteigeningswet

Op grond van de Coördinatiewet uitzonderingstoestanden en tevens op voordracht van de Minister-President na goedkeuring van de Tweede Kamer kan een bijzondere bevoegdheid ex artikel 76 jo. 76a bis Onteigeningswet ("**Ow**") in werking worden gesteld.

Deze bijzondere bevoegdheid stelt de hoogste militaire autoriteit ter plaatse in staat om zonder gerechtelijke procedure inbezitneming van een zaak te vorderen. Van de inbezitneming dient zo spoedig mogelijk een schriftelijk bewijsstuk te worden afgegeven.[92]

Deze bevoegdheid tot inbezitneming zou (althans in theorie) ook in geval van een ernstig cyberincident kunnen worden uitgeoefend. Men zou hierbij kunnen denken aan vordering tot inbezitneming van de computerinfrastructuur van een academisch of commercieel rekencentrum met als doel om een werkzaamheid uit te voeren waarvoor een grote rekencapaciteit of

[91] Op grond van artikel 15 lid 1 sub j Tw jo artikel 2 lid 2 van het Besluit aanwjjzing toezichthouders Telecommunicatiewet wordt toezicht gehouden op de naleving van deze aanwijzingen door de senior beleidsmedewerkers van de directie Telecommarkt van het directoraat-generaal voor Energie, Telecom en Markten.

[92] Deze afgifte van een bewijsstuk brengt artikel 76a bis lid 1 Ow in lijn met artikel 14 lid 3 Gw en artikel 1 Eerste Protocol EVRM, zie ook Kamerstukken *II*, 1993-1994, 23 791, nr. 3, 18.

bandbreedte nodig is, zoals het kraken van een zeer sterk versleutelde code. Heel waarschijnlijk is dit scenario overigens niet.

5.2 Sectorale wetgeving

Naast de algemene bevoegdheden bestaan op sectoraal niveau in beperkte mate bevoegdheden waarmee toezichthouders kunnen interveniëren in het geval zich een cyberincident voordoet bij een onder hun toezicht staande organisatie. Hieronder volgt een uiteenzetting van deze secorale interventiebevoegdheden, waarna kort wordt stilgestaan bij de internationale samenwerking tussen toezichthouders.

5.2.1 Sectorale interventiebevoegdheden

(a) Financiële sector

Artikel 1:75 Wft voorziet in een algemene bevoegdheid van de toezichthouder, dat wil zeggen DNB of de AFM, om aan bepaalde onder de werking van de Wft gestelde partijen, die niet voldoen aan hetgeen bij of krachtens deze wet is bepaald, door middel van een aanwijzing te verplichten een bepaalde gedragslijn te volgen. Ingeval van een cyberincident is denkbaar dat een dergelijke partij de beheerste en integere uitoefening van de onderneming of het bedrijf niet langer kan garanderen, hetgeen een overtreding oplevert van de eerder besproken zorgplicht op grond van de artikelen 3:17 en 4:14 Wft, 20 lid 2 Bpr Wft en 30 lid 1 Bgfo.

Indien aan de aanwijzing geen gevolg wordt gegeven, kan op grond van artikel 1:76 lid 1 jo. lid 2 sub a Wft een curator worden benoemd. Op grond van artikel 1:76 lid 2 sub b en c Wft kan dat ook indien sprake is van een overtreding van het bij of krachtens de Wft bepaalde, die het adequate functioneren van de financiële onderneming dan wel de belangen van consumenten en cliënten ernstig in gevaar brengt. In dat geval dient de financiële onderneming echter eerst in de gelegenheid te worden gesteld om haar zienswijze over het besluit tot benoeming van een curator naar voren te brengen. Er is op grond van de wet geen reden om aan te nemen dat deze bevoegdheid niet zou kunnen worden aangewend in het geval van een ernstig cyberincident.

Daarnaast hebben DNB en de AFM de bevoegdheid een last onder dwangsom op te leggen aan de financiële onderneming en op die wijze een bepaalde aanpak en/of wijze van bestrijding van het cyberincident voor te schrijven.[93]

(b) Nutsvoorzieningen

De Gaswet en de Elektriciteitswet 1998 bevatten de bevoegdheid voor de Raad van Bestuur van de NMa om bindende aanwijzingen op te leggen aan de netbeheerders in verband met de

[93] Zie artikel 1:79 Wft.

naleving van hetgeen in de Gaswet en de Elektriciteitswet 1998 is bepaald.[94] Omdat de netbeheerders in het geval van een ernstig cyberincident de veiligheid van hun netwerken mogelijk niet meer kunnen garanderen en/of anderszins niet meer aan hun wettelijke verplichtingen kunnen voldoen kan deze bevoegdheid bij een dergelijk incident worden ingezet. Daarnaast kennen beide wetten de mogelijkheid voor de Raad van Bestuur van de NMa om een last onder dwangsom op te leggen.[95]

De Drinkwaterwet bevat de bevoegdheid voor de Minister van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer om, ter handhaving van de wet, bestuursdwang toe te passen. Er is geen aanleiding aan te nemen dat deze bevoegdheid niet kan worden ingezet ter bestrijding van een cyberincident.

(c) Telecommunicatie

De Tw voorziet in artikel 15.1 in een bevoegdheid tot toepassing van bestuursdwang ter handhaving van een aantal bepalingen. Het wetsvoorstel Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen[96] (zie ook paragraaf 3.3 sub (c)) brengt de daarin voorgestelde algemene zorgplichten voor Telecomaanbieders onder de werkingssfeer van deze bepaling.

Verder voorziet hoofdstuk 14 van de Tw reeds in een aantal interventiebevoegdheden die kunnen worden aangewend ingeval van buitengewone omstandigheden. In het kader van cyber security is artikel 14.4 Tw relevant, dat voorziet in de mogelijkheid tot het geven van aanwijzingen door de Minister van Economische Zaken aan Telecommunicatieaanbieders. Deze aanwijzingen kunnen betrekking hebben op onder meer de instandhouding en exploitatie van hun openbare telecommunicatienetwerken en het verzorgen en gebruiken van hun openbare telecommunicatienetwerken. Deze aanwijzingen kunnen afwijken van de verplichtingen die op grond van de Tw op de desbetreffende aanbieders rusten en zijn verbindend.

Artikel 18.9 van de Tw geeft de Minister van Economische Zaken de bevoegdheid om in bepaalde gevallen in overeenstemming met de Minister van Justitie dan wel de minister van Binnenlandse Zaken en Koninkrijkrelaties aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten aanwijzingen te geven met betrekking tot de instandhouding en de exploitatie van hun openbare elektronische communicatienetwerken of het verzorgen en gebruiken van hun openbare elektronische communicatiediensten.

(d) Zorginstellingen

[94] Zie artikel 5 lid 6 Elektriciteitswet 1998 en artikel 60 lid 2 Gaswet.

[95] Zie artikel 77h Elektriciteitswet 1998 en artikel 60ac Gaswet.

[96] Kamerstukken *II*, 32 549, nr. 1.

De Minister van Volksgezondheid en Sport kan, indien hij van oordeel is dat geen verantwoorde zorg meer kan worden aangeboden, de zorgaanbieder op grond van artikel 8 lid 1 Kzi een schriftelijke aanwijzing opleggen. Indien het nemen van maatregelen in verband met het gevaar voor de veiligheid of de gezondheid redelijkerwijs geen uitstel kan lijden, kan de met het toezicht belaste ambtenaar ingevolge artikel 8 lid 4 Kzi een schriftelijk bevel geven. De zorgaanbieder is verplicht dit bevel op te volgen.

(e) Spoorvervoer en luchtvaart

Hoofdstuk 9 van de Wet luchtvaart voorziet in een aantal mogelijkheden om, indien buitengewone omstandigheden dit noodzakelijk maken, aanwijzingen op te leggen aan de LVNL. Deze aanwijzingen kunnen onder meer zien op de wijze waarop LVNL de luchtverkeersbeveiliging dient te verzorgen.

Artikel 76 lid 1 van de Spoorwegwet voorziet in de bevoegdheid tot het opleggen van een last onder dwangsom ter zake van de bij of krachtens die wet bepaalde verplichtingen. Daaronder vallen ook de eerder besproken zorgplichten ex artikel 16, 16a (nog niet in werking) en 32 Spoorwegwet, waaruit vermoedelijk ook een plicht tot preventie met betrekking tot cybercriminaliteit kan worden afgeleid (zie ook paragraaf 3.3).

5.2.2 Internationale samenwerking door toezichthouders

In welke mate toezichthouders op internationaal niveau samenwerken, verschilt per sector. Indien een samenwerking bestaat berust deze dikwijls op een Memorandum of Understanding ("**MoU**"). In dit verband kan worden gewezen op de MoU's op basis waarvan de AFM samenwerkt met financiële toezichthouders in andere landen.[97] Deze MoU's zien niet specifiek op cyber security, maar kunnen wel worden ingeroepen in het kader van de preventie van cybergerelateerde incidenten en bij de interventie in het geval zich een dergelijk incident voordoet.

Daarnaast vindt samenwerking plaats tussen toezichthouders binnen internationale samenwerkingsverbanden. Ter illustratie kan worden gewezen op het Europese samenwerkingsverband Consumer Protection Cooperation ("**CPC**"), in welk verband wordt samengewerkt tussen Europese consumententoezichthouders. Binnen dit samenwerkingsverband kunnen onder meer de OPTA, Nma, de AFM, de Nederlandse Zorgautoriteit ("**NZa**") en de Inspectie voor de Gezondheidszorg informatie- en handhavingsverzoeken indienen bij buitenlandse toezichthouders.[98] Daarnaast kan worden gewezen worden op de Kernenergiewet, waarin enkele bepalingen zijn opgenomen die zien op internationale samenwerking en de handhaving van internationale (verdragsrechtelijke) verplichtingen. Deze verplichtingen zijn onder meer opgesteld door het Internationaal Atoomenergie Agentschap ("**IAEA**"), die op mondiaal niveau de samenwerking reguleert met betrekking tot kernenergie-instellingen. Ook bovengenoemde samenwerkingsverbanden zijn niet primair gericht op cyber security, maar kunnen wel

[97] Voor een overzicht van deze MoU's: zie <http://www.afm.nl/nl/over-afm/werkzaamheden/internationale-samenwerking/mou.aspx>.

[98] Zie <http://www.consumentenautoriteit.nl/over-ons/missie-en-kerntaken/samenwerking>.

worden ingezet in het geval zich een (grensoverschrijdend) cyberincident voordoet.

5.3 Strafvorderlijke opsporingsbevoegdheden

Bij de opsporing van cybercriminaliteit zullen de opsporingsactiviteiten van de strafvorderlijke autoriteiten zich voornamelijk richten op het verzamelen van digitale informatie. De klassieke strafvorderlijke bevoegdheden, zoals inbeslagneming van voorwerpen, zijn daartoe niet altijd toereikend. Het Wetboek van Strafvordering voorziet daarom in diverse speciaal daarop toegesneden bevoegdheden.

Naarmate deze bevoegdheden ingrijpender van aard zijn worden daaraan meer voorwaarden gesteld, onder meer in de vorm van degene die deze bevoegdheid mag aanwenden (in oplopende mate van bevoegdheid: opsporingsambtenaar, hulpofficier van justitie, officier van justitie of rechter-commissaris). Omwille van de beknoptheid wordt hieronder niet ingegaan op de vraag welke opsporingsautoriteiten onder welke omstandigheden de besproken bevoegdheden mogen aanwenden. Wel wordt kort stilgestaan bij de bevoegdheid grensoverschrijdend opsporingsonderzoek te verrichten.

In het onderstaande wordt stilgestaan bij de volgende bevoegdheden:

- doorzoeking ter vastlegging en inbeslagneming van gegevens;
- vordering tot verstrekking van telecommunicatieverkeersgegevens;
- opnemen van telecommunicatie;
- vordering tot verstrekking van gegevens ter zake van de gebruiker en de gebruikte communicatiedienst; en
- ontoegankelijk maken van gegevens.

Naast bovengenoemde opsporingsmethoden zij hier nog gewezen op enkele overige opsporingsbevoegdheden in het Wetboek van Strafvordering, te weten: het stelselmatig observeren van een persoon of waarnemen van diens gedrag en aanwezigheid (artikelen 126g, 126o en 126zd Sv); het stelselmatig inwinnen van informatie over een verdachte door een opsporingsambtenaar (artikelen 126j, 126qa en 126zd Sv); pseudokoop of - dienstverlening (artikelen 126i, 126q en 126zd Sv); en infiltratie (artikelen 126h, 126p en 126ze Sv); het vorderen van gegevens en het ontsleutelen en "bevriezen" daarvan (artikelen 126nc-ni, 126uc-ui en 126zk-zp[99] Sv). Deze bevoegdheden zien, anders dan bovengenoemde opsporingsmethoden, niet specifiek op digitale informatie, communicatie en gegevens en worden daarom niet nader besproken. Dat neemt niet weg dat deze bevoegdheden ter opsporing en bestrijding van cybercrime kunnen worden ingezet.

[99] Er is geen variant van de bevoegdheid tot bevriezing van gegevens opgenomen met betrekking tot de opsporing van terroristische misdrijven.

5.3.1 Grensoverschrijdende opsporing

Nederlandse opsporingsinstanties zijn enkel bevoegd tot het instellen van opsporingsonderzoek indien Nederland rechtsmacht heeft met betrekking tot het desbetreffende (vermoedelijke) delict. In dit verband wordt verwezen naar paragraaf 6.3.1. Vooral bij cybercriminaliteit zal zich echter niet zelden de situatie voordoen dat ook buiten de Nederlandse grenzen opsporingsactiviteiten nodig zijn. Nederlandse opsporingsambtenaren mogen echter niet zonder een afdoende volkenrechtelijke of Europeesrechtelijke basis opsporingsactiviteiten ontplooien in het buitenland. Dit brengt mee dat grensoverschrijdende opsporing alleen mogelijk is door middel van internationale samenwerking. Deze samenwerking vindt in de praktijk enerzijds plaats door de klassieke samenwerking in strafzaken: internationale gegevensuitwisseling, rechtshulp in strafzaken (kleine rechtshulp), overname van strafvervolging of van de tenuitvoerlegging van strafvonnissen en de uitlevering. Binnen de EU wordt daarnaast steeds meer gebruik gemaakt van de wederzijdse erkenning.

Hieronder worden deze mogelijkheden kort nader toegelicht.

Klassieke internationale samenwerking in strafzaken

Indien een opsporingsactiviteit in een ander land nodig is, kunnen Nederlandse opsporingsambtenaren een rechtshulpverzoek indienen bij buitenlandse autoriteiten. Voor de inwilliging van een rechtshulpverzoek is in de regel een verdragsrechtelijke basis vereist. Verdragen die in EU-verband een dergelijke basis bieden zijn bijvoorbeeld het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken[100] en het daarop voortbordurende EU-Rechtshulpverdrag.[101] Daarnaast heeft Nederland nog diverse multi- en bilaterale rechtshulpverdragen afgesloten met andere niet-EU landen[102] en heeft de EU namens haar leden ook rechtshulpverdragen met derden afgesloten.[103]

Het Cybercrime Verdrag biedt voor de verdragssluitende staten een specifieke basis voor wederzijdse samenwerking bij de opsporing van cybercriminaliteit. Het Cybercrime Verdrag bevat in dit verband regelingen over wederzijdse bijstand met betrekking tot bijvoorbeeld de toegang tot opgeslagen computergegevens, de real-time vergaring van verkeersgegevens en de onderschepping van inhoudgegevens.

Wederzijdse erkenning binnen de EU

De rechtshulprelatie tussen de landen van de EU wordt de afgelopen jaren steeds meer gekenmerkt door het beginsel van wederzijdse erkenning. Bij wederzijdse erkenning is geen sprake meer van een verzoek om bijstand uit een ander land, maar van een bevel dat in een andere lidstaat wordt erkend en

[100] Zie Trb. 1965, 10.

[101] Zie Trb. 2000, 96.

[102] Zie bijvoorbeeld het Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechthulp in strafzaken, ondertekend op 12 juni 1981.

[103] Zie bijvoorbeeld de Overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de Europese Unie en de Verenigde Staten van Amerika (PB EU L 181/34)

uitgevoerd. In dit verband kan worden gewezen op het Europees Kaderbesluit inzake de tenuitvoerlegging in de Europese Unie van beslissingen tot bevriezing van voorwerpen of bewijsstukken.[104] Op basis van dit Kaderbesluit kunnen de bevoegde justitiële autoriteiten uit een lidstaat bevelen tot het in beslag nemen van voorwerpen in een andere lidstaat. Voor de overdracht van de voorwerpen aan de uitvaardigende lidstaat is vervolgens nog wel een "regulier" rechtshulpverzoek nodig. Nederland heeft voornoemd kaderbesluit geïmplementeerd in de artikelen 552jj e.v. Sv.

Ter verdere intensivisering van Europese samenwerking op basis van wederzijdse erkenning creëert het Kaderbesluit inzake het Europees bewijsverkrijgingsbevel[105] de mogelijkheid steunbevoegdheden in te zetten bij het in beslag nemen van voorwerpen (bijvoorbeeld een doorzoeking) en is het tevens mogelijk de in beslag genomen voorwerpen zonder rechtshulpverzoek over te dragen aan de uitvaardigende lidstaat. Het Kaderbesluit wordt momenteel geïmplementeerd in Nederland.[106]

In het onderstaande zal verder worden ingegaan op nationale bevoegdheden die dus via wederzijdse erkenning ook (deels) op Europees niveau kunnen worden uitgeoefend.

5.3.2 Doorzoeking ter vastlegging en inbeslagneming van gegevens

Ter opsporing van cybercriminaliteit zullen de strafvorderlijke autoriteiten veelal de hand willen leggen op (digitale) gegevens. Indien gegevens zijn vastgelegd op een gegevensdrager, dan kan deze gegevensdrager op grond van artikel 94 Sv in beslag worden genomen. De gegevensdrager is immers een voor inbeslagneming vatbaar voorwerp als bedoeld in artikel 94 Sv. Deze bevoegdheid volstaat echter niet ter inbeslagneming van niet op een drager vastgelegde gegevens omdat geen sprake is van een voor inbeslagneming vatbaar "voorwerp".

Artikel 125i Sv voorziet daarom in de bevoegdheid tot het doorzoeken van een plaats ter vastlegging van gegevens. Artikel 125j Sv voorziet voorts in de bevoegdheid tot het ter vastlegging van gegevens doorzoeken van een elders aanwezig geautomatiseerd werk (netwerkzoeking). Op grond van lid 2 dient dit onderzoek zich te beperken tot de gegevens waartoe de verdachte toegang heeft. Betreft het gegevens die zijn opgeslagen op een computersysteem dat zich kennelijk in het buitenland bevindt, dan mogen deze alleen worden onderzocht indien daar een uitdrukkelijke verdragsrechtelijke grondslag voor bestaat.[107] Het uitoefenen van strafvorderlijke bevoegdheden van het ene land op het grondgebied van een ander land, zonder toestemming van dat land, wordt algemeen gezien als een inbreuk op het volkenrecht.

Voor zover het onderzoek dit vordert, kan op grond van artikel 125k lid 1 en 2 Sv aan de aangewezen persoon een bevel worden gegeven toegang te verlenen tot (een deel van) een

[104] Kaderbesluit nr. 2003/577/JBZ.

[105] Kamerbesluit nr. 2008/978/JBZ.

[106] Zie dossier 32 717.

[107] T&C Strafvordering 2007, Wöretshofer, aantekening 7c bij artikel 125j, verwijzend naar Kamerstukken 1989-1990, 21 551, nr. 3, 11-12.

geautomatiseerd werk. De persoon in kwestie dient vervolgens zijn kennis omtrent de beveiliging van het geautomatiseerde werk en eventuele versleuteling van de gegevens ter beschikking te stellen. Deze vordering kan niet tot de verdachte worden gericht (artikel 125k lid 3 Sv).

De bevoegdheid tot doorzoeking ter vastlegging van gegevens impliceert de bevoegdheid van die gegevens kennis te nemen. Betreft het echter een doorzoeking bij een aanbieder van een openbaar communicatienetwerk of een openbare communicatiedienst en worden daarbij gegevens aangetroffen die niet voor deze bestemd of van deze afkomstig zijn, dan mag daarvan op grond van artikel 125la Sv slechts worden kennisgenomen, voorzover deze gegevens klaarblijkelijk (i) voor de verdachte bestemd zijn (ii) van de verdachte afkomstig zijn of (iii) op hem betrekking hebben dan wel (iv) tot het begaan van het strafbare feit hebben gediend of (v) als het strafbare feit met betrekking tot die gegevens is gepleegd.

5.3.3 Vordering tot verstrekking van telecommunicatieverkeersgegevens

In het kader van de opsporing van cybercriminaliteit zullen de strafvorderlijke autoriteiten vaak ook willen beschikken over gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot deze gebruiker. Op grond van artikel 126n Sv kunnen deze gegevens worden gevorderd van een communicatiedienst. Voorwaarde is dat sprake is van een verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten.[108] Anders dan voor het opnemen van communicatie ex artikel 126m Sv (hierna te bespreken) is echter niet vereist dat het een misdrijf betreft dat, gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven, een ernstige inbreuk op de rechtsorde oplevert. De vordering is niet beperkt tot het openbaar telecommunicatieverkeer en kan ook zien op communicatieverkeer over een besloten netwerk. De vordering kan voorts betrekking hebben op zowel reeds verwerkte als nog te verwerken gegevens.

Een zelfde bevoegdheid is tevens geregeld in artikel 126u Sv voor misdaden gepleegd in georganiseerd verband en in artikel 126zh Sv voor misdaden gepleegd met een terroristisch oogmerk. Voor toepassing van artikel 126u Sv is geen verdenking vereist, maar een redelijk vermoeden van betrokkenheid bij het plegen of beramen van misdrijven in georganiseerd verband als bedoeld in artikel 126o Sv. Voor toepassing van artikel 126zh Sv volstaat dat er aanwijzingen zijn dat een terroristisch misdrijf in de zin van artikel 138d Sv zou zijn of zal worden gepleegd. De bevoegdheid kan in die gevallen dus in een vroeger stadium worden ingezet.

5.3.4 Opnemen vertrouwelijke informatie

Indien het onderzoek dit dringend vordert bestaat op grond van artikel 126l Sv de mogelijkheid vertrouwelijke communicatie, niet zijnde telecommunicatie, op te nemen met een technisch hulpmiddel. Voor toepassing van deze bevoegdheid moet sprake zijn van een verdenking van een misdrijf waarvoor

[108] Te denken valt aan opzettelijke vernieling van computergegevens (artikel 350a Sr), bijvoorbeeld door middel van een computervirus, of het openbaarmaken dan wel opzettelijk verstrekken van staatsgeheimen aan een buitenlandse mogendheid (art. 98a Sr).

voorlopige hechtenis is toegestaan. Voorts is vereist dat het misdrijf, gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven, een ernstige inbreuk op de rechtsorde oplevert.

In het kader van de uitoefening van deze bevoegdheid kan bijvoorbeeld een technisch hulpmiddel worden aangebracht om toetsslagen en muisklikken te registreren.[109] Er dient wel sprake te zijn van communicatie: informatie die wordt ingevoerd op een computer terwijl niet met een andere computer wordt gecommuniceerd, valt niet onder de reikwijdte van deze bepaling.[110] De bevoegdheid is tegen een ieder inzetbaar en beperkt zich niet tot communicatie waaraan de verdachte deelneemt. Gelet op de verstrekkendheid van de bevoegdheid, mag deze enkel worden ingezet indien niet met een beperkter en specifieker bevel, te weten het opnemen van louter telecommunicatie ingevolge artikel 126m Sv, kan worden volstaan.[111]

De artikelen 126s en 126zf Sv voorzien in een vergelijkbare mogelijkheid tot het opnemen van vertrouwelijke communicatie in verband met de opsporing van misdrijven beraamd of gepleegd in georganiseerd verband respectievelijk terroristische misdrijven.

5.3.5 Opnemen van telecommunicatie

Artikel 126m Sv voorziet in de bevoegdheid tot het met een technisch hulpmiddel opnemen van telecommunicatie. Voorwaarde is dat sprake is van een verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten en dat, gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven, een ernstige inbreuk op de rechtsorde oplevert.

De bevoegdheid kan worden aangewend met of zonder medewerking van de telecommunicatieaanbieder.[112] Voor zover het onderzoek dit vordert, kan op grond van lid 6 aan de aangewezen persoon een bevel worden gegeven zijn kennis omtrent de versleuteling van de opgenomen communicatie ter beschikking te stellen dan wel de versleuteling ongedaan te maken. Deze vordering kan niet aan de verdachte worden gericht. Indien de gebruiker van de communicatiedienst zich op het grondgebied van een andere staat bevindt, gelden aanvullende vereisten op grond van artikel 126ma Sv.

De artikelen 126t en 126 zg Sv voorzien in eenzelfde mogelijkheid tot het opnemen van telecommunicatie in verband met de opsporing van misdrijven beraamd of gepleegd in

---

[109] *Kamerstukken II*, 1996-1997, 25 403, nr. 3, p. 36.

[110] *Kamerstukken II*, 1996-1997, 25 403, nr. 3, p. 35.

[111] *Kamerstukken II*, 1996-1997, 25 403, nr. 3, p. 37.

[112] Dit keert terug in het Besluit technische hulpmiddelen strafvordering (van 20 oktober 2006, zoals laatstelijk gewijzigd bij Wet van 27 maart 2007, *Stb.* 2007, 121), waarin het opnemen van telecommunicatie (*ex* artikel 1c van dat Besluit) gedefinieerd wordt als: *'het opnemen van communicatie met een technisch hulpmiddel, ter uitvoering van een bevel als bedoeld in artikel 126m, eerste lid, 126t, eerste lid, en 126zg, eerste lid, voor zover het bevel, bedoeld in artikel 126m, derde of vierde lid, onderscheidenlijk artikel 126t, derde of vierde lid, en artikel 126zg, derde of vierde lid, ten uitvoer wordt gelegd zonder medewerking van de betrokken aanbieder'*. Het vereiste van zonder medewerking keert echter voor deze definitie niet direct terug in de wet.

georganiseerd verband respectievelijk terroristische misdrijven. In beide gevallen is geen verdenking vereist, maar slechts een redelijk vermoeden van betrokkenheid bij het plegen of beramen van misdrijven in georganiseerd verband respectievelijk dat een terroristisch misdrijf zou zijn of zal worden gepleegd. De bevoegdheid kan in die gevallen dus in een vroeger stadium worden ingezet. De bevoegdheid ex artikel 126t kan echter alleen worden ingezet ter opname van communicatie waaraan een persoon deelneemt ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven. Een dergelijke beperking geldt niet met betrekking tot terroristische misdrijven.

5.3.6 Vordering tot verstrekking van gegevens ter zake van de gebruiker en de gebruikte communicatiedienst

Teneinde toepassing te kunnen geven aan de bevoegdheden ex artikel 126m en 126n Sv zijn de naam-, adres- en nummergegevens van de gebruiker van de communicatiedienst nodig alsmede gegevens ter zake van de gebruikte communicatiedienst. Deze gegevens kunnen worden gevorderd op grond van artikel 126na Sv. De communicatienetwerkaanbieder dient daarop indien nodig een bestandsanalyse uit te voeren om de gebruikersgegevens van de desbetreffende gebruiker te achterhalen. De communicatieaanbieder heeft daartoe gegevens nodig over de locaties waar en de tijdstippen waarop de gebruiker gebruik heeft gemaakt van de dienst. Aan de hand van deze informatie kan de aanbieder van een communicatiedienst bijvoorbeeld achterhalen welke gebruiker op een bepaald IP-adres heeft ingelogd op het internet. Op grond van artikel 13.4 lid 2 Tw zijn aanbieders verplicht de hiertoe vereiste gegevens drie maanden te bewaren vanaf het tijdstip waarop deze gegevens voor de eerste keer zijn verwerkt. Indien de gegevens worden gevorderd ten behoeve van een vordering op grond van artikel 126m respectievelijk 126n Sv zal sprake moeten zijn van een misdrijf als in deze artikelen bedoeld.

Artikel 126nb Sv bepaalt, onder verwijzing naar 3.10 lid 4 Tw, dat indien op grond van artikel 126na Sv geen gegevens van een gebruiker achterhaald kunnen worden de vereiste nummergegevens met behulp van actieve scanapparatuur (een zogenaamde IMSI-scanner) uit de ether mogen worden opgevangen. De toepassing van deze apparatuur mag alleen ten dienste staan van een vordering op grond van artikel 126m of 126n Sv.[113]

Artikelen 126ua -ub en 126zi -zj Sv voorzien in een zelfde bevoegdheid ter zake van misdrijven in georganiseerd verband respectievelijk terroristische misdrijven. Voor toepassing van artikel 126ua Sv is geen verdenking vereist, maar een redelijk vermoeden van betrokkenheid bij het plegen of beramen van misdrijven in georganiseerd verband als bedoeld in artikel 126o Sv. Voor toepassing van artikel 126zi Sv volstaat dat er aanwijzingen zijn dat een terroristisch misdrijf zou zijn of zal worden gepleegd. De bevoegdheid kan in die gevallen dus in een vroeger stadium worden ingezet.

[113] T&C Strafvordering 2007, Blom, aantekening 2 bij artikel 126nb Sv.

5.3.7 Ontoegankelijk maken van gegevens

Op grond van artikel 125o Sv kunnen gegevens met betrekking waartoe of met behulp waarvan een strafbaar feit is gepleegd en die zijn aangetroffen op een geautomatiseerd werk ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten ontoegankelijk worden gemaakt. Deze bevoegdheid kan enkel worden toegepast bij gelegenheid van een doorzoeking ter vastlegging van gegevens ingevolge artikel 125i Sv. Onder ontoegankelijk maken van gegevens wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van het geautomatiseerde werk van die gegevens kennis kan nemen of gebruikmaken alsmede ter voorkoming van verdere verspreiding van die gegevens. Onder ontoegankelijk maken wordt ook verstaan het verwijderen van gegevens uit het geautomatiseerde werk met behoud van deze gegevens ten behoeve van de strafvordering. Het betreft een tijdelijke maatregel: zodra het strafvorderlijk belang zich daartegen niet meer verzet, dienen de gegevens weer ter beschikking van de beheerder van het automatische werk te worden gesteld.[114]

5.3.8 Opsporingsbevoegdheden op grond van bijzondere strafwetgeving

Opgemerkt zij dat bijzondere strafwetten in aanvullende of parallelle bevoegdheden kunnen voorzien. Een voorbeeld zijn de bevoegdheden van titel III WED die kunnen worden ingezet ter zake van aan de WED onderworpen delicten. Veelal betreft dit overtredingen van sectorale wetgeving die langs de weg van de WED (mede) strafrechtelijk worden gehandhaafd.

[114] Er wordt momenteel gewerkt aan een uitbreiding van de bevoegdheden van de Officier van Justitie in het kader van de bestrijding van computercriminaliteit. Het daartoe opgestelde conceptwetsvoorstel Computercriminaliteit III is echter in de consultatiefase op een aantal inhoudelijke bezwaren gestuit en zal daarom worden herzien. Het conceptwetsvoorstel en de bijbehorende conceptmemorie van toelichting zijn beschikbaar op: http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit.
Het daarin voorgestelde artikel II beoogde de Officier van Justitie bij artikel 125o en 125p Sv de bevoegdheid te geven om van een communicatiedienst te vorderen dat hij gegevens ontoegankelijk maakt en aan die vordering een dwangsom te verbinden.

6 HANDHAVING EN REPRESSIE

6.1 Inleiding

In de voorgaande hoofdstukken zijn in de kern de volgende onderwerpen aan de orde gekomen: preventie en toezicht, melding en interne maatregelen, en interventie en opsporing. In dit hoofdstuk staat de volgende fase centraal: handhaving en repressie. Dit hoofdstuk handelt zowel over strafrechtelijke als over bestuursrechtelijke handhaving en repressie.

Het hoofdstuk is als volgt ingedeeld. De bestuursrechtelijke handhavings- en repressiebevoegdheden worden kort besproken in paragraaf 6.2. Hier wordt onderscheid gemaakt tussen enerzijds het algemene kader dat wordt gevormd door de Awb en anderzijds de specifieke wetgeving die geldt voor sectoren met grote maatschappelijke relevantie. Vervolgens komen in paragraaf 6.3 de strafrechtelijke bevoegdheden aan de orde. Ook hier is een onderscheid gemaakt tussen algemene (lees: commune) strafbaarstellingen en sectorale (lees: bijzondere) strafbaarstellingen. Ook in dit hoofdstuk worden alleen de voor cyber security relevante mogelijkheden tot handhaving en repressie besproken.

6.2 Bestuursrechtelijke handhaving en repressie

6.2.1 Algemene wet bestuursrecht

De Awb omvat het algemene bestuursrechtelijke instrumentarium voor de overheid om toezicht te houden op de naleving van wettelijke verplichtingen en overtredingen te sanctioneren (tezamen: handhaving). Het toezichtsinstrumentarium is al deels aan de orde gekomen in de eerdere hoofdstukken (zie paragrafen 3.3, 5.1 en 5.2). In de repressiefase zijn in het bijzonder de sanctioneringsbevoegdheden van toezichthouders van belang. Deze bevoegdheden kunnen bijvoorbeeld worden ingezet indien een onderneming niet voldoet aan de voor haar geldende zorgplicht (zie hoofdstuk 3) of indien de onderneming een eventuele meldingplicht heeft geschonden (zie hoofdstuk 4).

Bestuursrechtelijke handhaving is geregeld in hoofdstuk 5 van de Awb. Op grond van dit hoofdstuk kan een bestuursorgaan de volgende handhavingsinstrumenten inzetten:

- last onder bestuursdwang en bestuursdwang (afdeling 5.3.2);
- last onder dwangsom (afdeling 5.3.2);
- bestuurlijke boete (Titel 5.4).

De Awb is een algemene wet; per bijzondere wet moet gekeken worden of en welke bevoegdheden uit de Awb aan het desbetreffende (zelfstandige) bestuursorgaan zijn toegekend. Hierdoor komt de nadruk te liggen bij de sectorale regelgeving.

6.2.2 De sectorale regelgeving

Handhavingsbevoegdheden

In vrijwel alle sectorale wetten is aan toezichthouders de bevoegdheid toegekend een last onder bestuursdwang op te leggen of bestuursdwang toe te passen indien de relevante zorgplichten en meldingsverplichtingen uit de sectorale wetten niet worden nageleefd. In een aantal wetten (de Wft, de Gaswet en de Elektriciteitswet 1998) bestaat deze bevoegdheid niet. In deze wetten bestaat evenwel de mogelijkheid voor toezichthouders om een schriftelijke aanwijzing of een bindende aanwijzing op te leggen, op basis waarvan zij de betreffende onderneming kunnen verplichten een bepaalde gedragslijn te volgen.[115] In het verlengde van deze bevoegdheid kennen deze wetten vervolgens de mogelijkheid om (indien deze bindende/schriftelijke aanwijzing niet wordt opgevolgd) een last onder dwangsom op te leggen.

De mogelijkheid tot het opleggen van een bestuurlijke boete bestaat niet in alle door dit onderzoek bestreken sectorale wetgeving. Deze mogelijkheid bestaat enkel in geval van relevante overtredingen in de Wft[116], de Gaswet[117], de Elektriciteitswet 1998[118], de Tw[119] en de Kzi.[120]

In aanvulling op bovenstaande reguliere handhavingsbevoegdheden bestaan ook nog enkele sectorspecifieke handhavingsmogelijkheden. In dit verband kan bijvoorbeeld worden gewezen op de bevoegdheid van de OPTA om, indien een last onder bestuursdwang en een bestuurlijke boete niet tot het gewenste resultaat hebben geleid, de Telecomaanbieder te verbieden nog langer elektronische communicatienetwerken of -diensten aan te bieden voor een door de OPTA te bepalen redelijke termijn.[121]

Tot slot bestaat in vrijwel alle sectorale wetgeving de mogelijkheid om ingeval van gevaar voor de veiligheid de vergunning/concessie (indien vereist) tot het uitoefenen van de desbetreffende diensten in te trekken. In dit verband kan onder meer worden gewezen op de mogelijkheden hiertoe in artikel 20a Kernenergiewet en in artikel 18 Spoorwegwet.

6.3 Strafbaarstellingen in het Wetboek van Strafrecht

Het Wetboek van Strafrecht vormt de basis van het commune materiële strafrecht in Nederland. In deze paragraaf staan centraal de strafbepalingen die specifiek zien op cybercrime of op het gebruik van door cybercrime verkregen informatie.

---

[115] Zie artikel 1:75 Wft, artikel 5 lid 6 Elektriciteitswet 1998 en artikel 60 lid 2 van de Gaswet.

[116] Zie artikel 1:80 Wft.

[117] Zie artikel 60 ad Gaswet.

[118] Zie artikel 77i Elektriciteitswet 1998.

[119] Zie artikel 15.4 lid 4 Telecommunicatiewet.

[120] Zie artikel 9 Kwaliteitswet zorginstellingen (deze bevoegdheid bestaat enkel bij het schenden van de meldplicht).

[121] Zie artikel 15.2a lid 2 Telecommunicatiewet.

Besproken zullen worden bepalingen aangaande:

(i) het belemmeren van de toegang tot een geautomatiseerd werk;
(ii) computervredebreuk;
(iii) aftappen van gegevens en daaraan gerelateerde feiten;
(iv) reclame maken voor aftapapparatuur;
(v) schending van (digitale) bedrijfsgeheimen; en
(vi) vernielingsdelicten.

Voordat de materiele delicten worden besproken, wordt eerst kort ingegaan op de rechtsmacht van het OM met betrekking tot grensoverschrijdende delicten.

Overigens zij opgemerkt dat de Officier van Justitie op grond van het opportuniteitsbeginsel een discretionaire bevoegdheid heeft om af te zien van vervolging op gronden aan het algemeen belang ontleend.[122]

6.3.1 Internationale rechtsmacht

Nederland heeft ingevolge artikel 2 Sr allereerst rechtsmacht indien het strafbaar feit plaatsvindt op het Nederlandse grondgebied. Er bestaan in deze context de volgende relevante leren om te bepalen waar het feit heeft plaatsgevonden:

(i) *Leer van de lichamelijke gedraging*: op basis van deze leer heeft Nederland rechtsmacht indien de dader van de cyberaanval zich op het Nederlandse grondgebied bevond tijdens het uitvoeren van het strafbare feit.
(ii) *Leer van het instrument*: Op basis van deze leer wordt gekeken naar het instrument waarmee de dader handelt. Door tussenkomst van dit instrument kan de dader op een andere plaats handelen dan volgens de leer van de lichamelijke gedraging. *De locus delicti* is dan de plaats waar het gebruikte instrument zijn uitwerking heeft. Als instrument bij een cyberaanval kan bijvoorbeeld de server worden aangemerkt, waarop de informatie die onderwerp is van de cyberaanval staat opgeslagen. Veel bedrijven hebben tegenwoordig een server in het buitenland, waardoor volgens deze leer (ook) een *locus delicti* bestaat in het land waar de server staat.

Nederland is op grond van artikel 5 Sr tevens bevoegd te oordelen over een strafbaar feit indien de dader de Nederlandse nationaliteit heeft, ongeacht waar de cyberaanval heeft plaatsgevonden. Indien het strafbare feit in het buitenland is begaan, is daartoe wel vereist dat het feit ook op deze plaats strafbaar is gesteld.

Een belangrijke vraag is of ook het land waar de gevolgen van het strafbare feit zich openbaren rechtsmacht heeft om over dit feit te oordelen. Indien de leer van het instrument ruim wordt uitgelegd, zouden ook de computers waarop de cyberaanval zich uiteindelijk openbaart (terwijl de gegevens gelokaliseerd zijn in een ander land) kunnen worden aangemerkt als instrument. In dat geval zou ook de locatie van deze computers worden aangemerkt als *locus delicti* en wordt dientengevolge voor dat land

[122] Zie artikel 167 lid 2 Sv.

rechtsmacht gecreëerd. In Nederland wordt de lijn gehanteerd dat rechtsmacht bestaat ten opzichte van data die zich op een server op Nederlands grondgebied bevinden.. Vanuit een rechtsvergelijkend perspectief kan in dit verband worden gewezen op een (overigens bestuursrechtelijk gesanctioneerde) verbodsbepaling in de Oostenrijkse Telecomwet aangaande *cold calling,* spam en sms. Indien de (verboden) *cold call,* spam of sms niet vanuit Oostenrijk heeft plaatsgevonden of is verzonden, wordt als plaats van de overtreding aangemerkt de plaats waar de verboden *cold call* , spam of sms wordt ontvangen,[123] Hierdoor wordt rechtsmacht voor Oostenrijk gegarandeerd, zijnde het land waar het directe gevolg van de overtreding zich openbaart.

6.3.2 De toegang belemmeren tot een geautomatiseerd werk

Artikel 138b Sr verbiedt het door het sturen van (een overvloed aan) gegevens naar een geautomatiseerd werk opzettelijk en wederechtelijk belemmeren van de toegang tot of het gebruik van dat geautomatiseerd werk. In dit verband kan worden gedacht aan de verdachte die een *Denial of Service*-aanval ('DoS-aanval') uitvoert, hetgeen inhoudt dat hij een overvloed aan aanvragen c.q. gegevens naar een website stuurt, waardoor deze (tijdelijk) onbereikbaar of onbruikbaar is.

6.3.3 Computervredebreuk

Er bestaan verschillende vormen van computervredebreuk. Allereerst stelt artikel 138ab lid 1 Sr strafbaar het enkele opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk. Indien de gegevens, waartoe men aldus toegang heeft verkregen, worden verwerkt of overgedragen, dan geldt dit op grond van lid 2 als een strafverzwarende omstandigheid.

Een andere vorm van computervredebreuk is het binnendringen van een geautomatiseerd werk met het oogmerk (a) gebruik te maken van de verwerkingscapaciteit van het geautomatiseerde werk of (b) om zich toegang te verschaffen tot het geautomatiseerde werk van een derde (zie artikelen 138ab lid 3 Sr).

6.3.4 Aftappen van gegevens en daaraan gerelateerde feiten

Indien iemand opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk, is hij strafbaar op grond van artikel 139c Sr. Dit overigens behoudens de uitzonderingen in lid 2 van die bepaling. Men kan bij aftappen denken aan de persoon die door middel van een technisch hulpmiddel meeluistert met telefoongesprekken of meeleest met e-mailconversaties die niet voor hem bestemd zijn.

Een persoon hoeft niet daadwerkelijk over te gaan tot het aftappen van gegevens voordat zijn handelen strafbaar is. Reeds het plaatsen van aftapapparatuur met het oogmerk gegevens af te tappen is strafbaar gesteld in artikel 139d lid 1 Sr. Hetzelfde geldt voor het produceren van of

[123] zie § 107 (6) van de Oostenrijkse Telecomwet.

handelen in dergelijke aftapapparatuur (artikel 139d lid 2 sub a Sr). Voorts is op grond van artikel 139d lid 2 sub b en lid 3 Sr ook het bezitten of verspreiden van een wachtwoord of code waardoor toegang kan worden gekregen tot een geautomatiseerd werk strafbaar, indien dit gebeurt met het oogmerk daarmee een strafbaar feit te plegen in de zin van de artikelen 138a, 138b of 139c Sr.

Heeft iemand niet aan de vorige stappen bijgedragen, maar bezit hij wel gegevens die door middel van een illegale tap zijn verkregen, dan is deze persoon strafbaar op grond van artikel 139e sub 1 Sr. Op grond van artikel 139e sub 2 Sr is degene die zelf heeft afgetapt daarnaast ook strafbaar wanneer hij de door de tap verkregen gegevens opzettelijk aan een ander bekend maakt.[124].Tenslotte is op grond van artikel 139e sub 3 Sr strafbaar hij die een gegevensdrager, als bedoeld sub 1, opzettelijk ter beschikking stelt aan een ander.

6.3.5 Reclame maken voor aftapapparatuur

Degene die reclame maakt voor, kort gezegd, aftapapparatuur is strafbaar op grond van artikel 441a Sr. Dit delict is een overtreding (en geen misdrijf). Volgens de wetgever vallen onder dit wetsartikel ook publicaties die inlichtingen verschaffen over dergelijke apparatuur.[125] Als een publicatie waarschuwt voor dergelijke apparatuur valt dit evenwel niet onder de strafbaarstelling van dit artikel, tenzij in deze waarschuwing specifieke informatie staat die verwijst naar bijvoorbeeld een leverancier van dergelijke apparaten.[126] Het wetsartikel houdt geen algeheel reclameverbod in voor opnameapparatuur: reguliere gebruiksvoorwerpen, zoals bij invoering bandrecorders, vallen er niet onder.[127]

6.3.6 Schending van (digitale) bedrijfsgeheimen

In het kader van de wederrechtelijke omgang met gegevens uit geautomatiseerde werken is ook artikel 273 Sr van belang. In lid 1 sub 1 van dit artikel wordt bekendmaking van bijzonderheden aangaande een onderneming waarvan de geheimhouding is opgelegd (bedrijfsgeheimen) strafbaar gesteld. Deze bedrijfsgeheimen hebben tegenwoordig in de regel een digitale vorm. De bepaling richt zich alleen tot mensen die bij de onderneming in kwestie werkzaam zijn of (incidenteel) werkzaam zijn geweest. Volgens de toelichting op dit artikel is om te spreken van

---

[124] Er wordt gewerkt aan de verruiming van een aantal strafbepalingen ter zake van computercriminaliteit. Het daartoe opgestelde conceptwetsvoorstel Computercriminaliteit III is echter in de consultatiefase op een aantal inhoudelijke bezwaren gestuit en zal daarom worden herzien. Het conceptwetsvoorstel en de bijbehorende conceptmemorie van toelichting zijn beschikbaar op:
http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit.
Het daarin voorgestelde artikel I lid F beoogde de reikwijdte van artikel 139e sub 2 Sr te verruimen door het vereiste, dat degene die de informatie bekend maakt ook degene moet zijn die de gegevens wederrechtelijk heeft verkregen, te laten vervallen en aldus ook het "helen" van dergelijke gegevens strafbaar te stellen

[125] Kamerstukken II 1967-1968, 9419.

[126] Kamerstukken II 1967-1968, 9419.

[127] Kamerstukken II 1967-1968, 9419.

geheimhoudingsplicht een contractueel beding vereist.[128] Volgens Remmelink is echter voldoende dat de geheimhoudingsplicht uit het contract voortvloeit en kan deze ook worden opgelegd door iemand die de betrokkene voorschriften kan geven over zijn werkzaamheden.[129]

Artikel 273 lid 1 sub 2 Sr stelt vervolgens een gedraging die veel weg heeft van heling strafbaar. Dit is namelijk het bekendmaken of het uit winstbejag gebruiken van gegevens door misdrijf verkregen uit een geautomatiseerd werk van een onderneming. Een voorwaarde voor strafbaarheid op grond van dit artikel is dat de gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren en uit de gedraging enig nadeel kon ontstaan. Blijkens lid 2 is voor strafbaarheid vereist dat de openbaarmaking te kwader trouw is gedaan (artikel 273 lid 2 Sr). Artikel 273 Sr is tot slot een klachtdelict: zonder klacht van de desbetreffende onderneming kan geen vervolging plaatsvinden (*ex* artikel 273 lid 3 Sr).

6.3.7 Vernielingsdelicten

Bij de relevante vernielingsdelicten kan onderscheid gemaakt worden tussen:

1. vernieling van geautomatiseerde werken (zie bijvoorbeeld artikelen 161 sexies/161septies Sr of artikelen 350, 351 en 351bis Sr) en
2. vernieling van gegevens (zie artikelen 350a en 350b Sr).

Ad 1.

Voor de vernieling van geautomatiseerde werken zijn relevant zowel bepalingen van algemene aard als meer specifieke bepalingen.

Artikel 350 Sr is een algemene bepaling. Daarin wordt strafbaar gesteld het opzettelijk en wederrechtelijk vernielen, beschadigen, onbruikbaar maken of wegmaken van enig goed dat een ander toebehoort.

Artikel 351 Sr heeft een vergelijkbare strekking maar richt zich op meer specifieke zaken zoals geautomatiseerde werken of werken voor telecommunicatie voor zover deze ten algemenen nutte gebruikt worden. Artikel 351bis Sr is de culpose variant van artikel 351 Sr.

Artikelen 161sexies en 161septies Sr bevatten een verbod op het:

- vernielen,
- beschadigen,
- onbruikbaar maken,
- veroorzaken van een stoornis in de gang of in de werking, of
- verijdelen van de veiligheidsmaatregelen

van een geautomatiseerd werk of werk voor telecommunicatie. Voorwaarde voor strafbaarheid is wel dat sprake is van enige vorm van gevaarzetting. Hierbij moet er gedacht worden aan

[128] Memorie van Toelichting, Kamerstukken *II* 1990-1991, 21 551, nr. 3, 22.

[129] T&C Strafrecht 2006, Van Strien/Van Maurik, aantekening 10f bij artikel 273.

verstoring van de levering van diensten tot aan levensgevaar voor anderen. De ernst van de (mogelijke) gevolgen bepaalt de hoogte van de maximumstraffen. Het verschil tussen artikelen 161sexies en 161septies Sr is dat de eerste overtreding opzettelijk is en de tweede culpoos.

Een persoon hoeft niet daadwerkelijk over te gaan tot het vernielen van een geautomatiseerd werk voordat zijn handelen strafbaar is. Het produceren van of handelen in een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is voor vernieling in de zin van artikel 161sexies lid 1 Sr is krachtens lid 2 sub a van die bepaling strafbaar. Voorts is ook het bezitten of verspreiden van een wachtwoord of code waarmee toegang kan worden gekregen tot een geautomatiseerd werk strafbaar indien dit gebeurt met het oogmerk daarmee de strafbare vernieling te begaan in de zin van lid 1 (artikel 161sexies lid 2 sub b Sr).

De Hoge Raad heeft recentelijk geoordeeld dat zogeheten *Distributed Denial-of-Service*-aanvallen[130] op websites van banken binnen het bereik van artikel 161sexies lid 1 sub 2 Sr vallen en dat hiervan gemeen gevaar voor de verlening van diensten is te duchten. In dit verband is volgens de Hoge Raad niet van belang of de veroorzaakte stoornis wordt veroorzaakt in de computers van de afnemers van een bepaalde dienst dan wel van in de computers van de dienstverlener zelf, maar is doorslaggevend of van de opzettelijk veroorzaakte stoornis gemeen gevaar te duchten is voor een ongestoorde dienstverlening. Hiervan is volgens de Hoge Raad onder meer sprake indien aan een substantieel aantal afnemers van de dienst de mogelijkheid wordt ontnomen van deze dienst gebruik te maken.[131]

Indien iemand een computer vernielt, beschadigt, onbruikbaar maakt of wegmaakt en dit feit niet valt onder artikel 161sexies Sr, kan dit feit geschaard worden onder artikel 350 Sr. Hierbij kan worden gedacht aan de persoon die de computer van een particulier onbruikbaar maakt zonder verdere gevaarzetting.

Ad 2.

De vernieling van computergegevens valt niet onder artikel 350 Sr, daar zij niet als goed worden aangemerkt.[132] Indien geen sprake is van vernieling van het geautomatiseerd werk, maar louter van gegevens, is sprake van het vernielen van computergegevens als bedoeld in de artikelen 350a en 350b Sr. Artikel 350a Sr is de opzettelijke variant en artikel 350b Sr is de culpoze variant van dit delict. Onder de werking van deze artikelen valt onder meer het plaatsen van kwaadaardige software, zoals virussen, Trojaanse paarden en spionagesoftware.

6.4 Sectorale wetgeving: een selectie van andere strafbaarstellingen

Niet alle strafbepalingen die relevant kunnen zijn voor cyber security zijn in het Wetboek van

[130] Bij een *Distributed Denial-of-Serive*-aanval worden vanaf verschillende plaatsen zoveel verbindingsverzoeken naar de server van een website verstuurd, dat de service ervan tijdelijk niet meer beschikbaar is of dat de server crasht.

[131] Zie HR 22 februari 2011, *LJN* BN 9287.

[132] Kamerstukken *II* 1989-1990, 21 551, nr. 3, 23.

Strafrecht opgenomen. Ook veel sectorale wetten omvatten relevante meldplichten, zorgplichten en medewerkingsplichten, waarvan sommige strafbaar zijn gesteld in de WED. Deze worden hierna besproken. Daarbij wordt het in de voorgaande hoofdstukken gemaakte onderscheid tussen meldplichten, zorgplichten en medewerkingplichten gevolgd.

6.4.1 Strafrechtelijk handhaafbare meldplichten

In de Wft, de Drinkwaterwet, de Gaswet, de Wet Luchtvaart, de Kzi en de Tw zijn geen meldplichten opgenomen waarvan schending strafbaar is op grond van de WED.

Schending van de meldplicht opgenomen in artikel 39 Kernenergiewet is op grond van artikel 1a sub 2 WED wel strafbaar. Artikel 39 Kernenergiewet houdt in dat een ieder verplicht is een ongeval in een kernenergie-inrichting te melden. Dit kan van belang zijn in het kader van cyber security in het geval dat door een cyberincident inbreuk wordt gemaakt op de elektronische controlesystemen van een dergelijke kerninrichting. Indien iemand hier weet van heeft en redelijkerwijs kan vermoeden dat hierdoor een ongeval zich voordoet in die inrichting, is het niet melden van dit ongeluk mogelijk strafbaar.

Indien gebeurtenissen plaatsvinden die onverkorte toepassing van het beveiligingspakket van een kerninrichting in de weg staan, dienen deze op grond van artikel 12 Regeling beveiliging nucleaire inrichtingen en splijtstoffen onmiddellijk aan de Minister van Economische Zaken te worden gemeld . Overtreding van dit artikel is strafbaar op grond van artikel 22 Besluit kerninstallaties, splijtstoffen en ertsen jo. artikel 21 Kernenergiewet jo. artikel 1a sub 1 WED.

6.4.2 Strafrechtelijk handhaafbare zorgplichten

Enkel de zorgplicht zoals deze geldt op grond van de Kernenergiewet (zie paragraaf 3.3 sub (b)) kan strafrechtelijk worden gehandhaafd op grond van artikel 1a sub 1 WED. De overige relevante sectorale wetten kennen geen strafrechtelijk handhaafbare zorgplichten.

6.4.3 Strafrechtelijk handhaafbare medewerkingplichten

Op grond van artikel 184 Sr geldt een algemene medewerkingplicht. Deze houdt in dat een ieder gehoor moet geven aan een ambtelijk bevel. Indien een daartoe gehouden persoon dat opzettelijk niet doet, is hij op grond van dit artikel strafbaar.

7 WAARBORGEN

7.1 Inleiding

Dit hoofdstuk gaat in op de waarborgen die wet- en regelgeving aan private partijen toekent om overheidsoptreden in het kader van cyber security te controleren en hiertegen zonodig rechtsmaatregelen aan te wenden. Het hoofdstuk gaat allereerst in paragraaf 7.2 in op bestuursrechtelijke, civielrechtelijke en strafrechtelijke rechtsbescherming. Vervolgens wordt in paragraaf 7.3 stilgestaan bij de Wet openbaarheid van bestuur. Tot slot bespreekt paragraaf 7.4 de bescherming van persoonsgegevens.

7.2 Rechtsbescherming

7.2.1 Bestuursrecht

Bezwaar en beroep

Toezichthouders die zijn belast met het toezicht op de naleving van wet- en regelgeving hebben diverse handhavingsbevoegdheden. Uit de voorgaande hoofdstukken volgt dat de toezichthouders op de vitale sectoren onder meer een aanwijzing, een last onder bestuursdwang,een last onder dwangsom en een bestuurlijke boete kunnen opleggen, indien bijvoorbeeld preventieplichten worden geschonden of indien een bedrijf nalaat melding te maken van een cyberincident. De beslissing over te gaan tot het gebruiken van een dergelijke handhavingsbevoegdheid wordt aangemerkt als een besluit in de zin van de Awb.[133] Tegen een dergelijk besluit kan op grond van de Awb bezwaar, beroep (en uiteindelijk hoger beroep) worden ingesteld, wat kan leiden tot intrekking, wijziging of vernietiging van het bestreden besluit.

Bezwaar tegen een besluit kan binnen zes weken worden ingesteld bij de toezichthouder die of het overheidsorgaan dat het besluit heeft genomen. De toezichthouder dient vervolgens haar eigen besluit volledig te heroverwegen. Deze heroverweging dient *ex nunc* te geschieden, hetgeen inhoudt dat de toezichthouder ook omstandigheden mee dient te wegen die na het nemen van het initiële besluit zijn ontstaan of bekend geworden. Tegen de beslissing op bezwaar kan binnen zes weken beroep worden ingesteld bij de bestuursrechter. De bestuursrechter toetst de beslissing op bezwaar *ex tunc*. Dit houdt in dat de rechter enkel mag toetsen of het bestuursorgaan op basis van de feiten en omstandigheden, zoals deze bekend waren tijdens het nemen van de beslissing op bezwaar, in redelijkheid tot zijn besluit heeft kunnen komen. Met nadien gewijzigde feiten of omstandigheden mag de bestuursrechter derhalve geen rekening houden. Bezwaar en beroep hebben geen schorsende werking. Hiervoor dient bij de bestuursrechter een voorlopige voorziening te worden verzocht.

[133] Zie voor de definitie van besluit artikel 1:3 Awb.

Klachtrecht met betrekking tot het optreden van de AIVD en MIVD

In hoofdstuk 3 is gewezen op de taken en bevoegdheden van de AIVD en de MIVD in het kader van cyber security. Indien een (rechts)persoon een klacht indient over het handelen van de AIVD of de MIVD, wordt deze in eerste instantie behandeld door de betrokken Minister. De Minister is in dit geval verplicht het advies in te winnen van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Deze zal de klacht onderzoeken en een advies uitbrengen aan de Minister, die uiteindelijk beslist. Indien de Minister afwijkt van het advies van de Commissie, moet hij in zijn beslissing de reden voor die afwijking vermelden en het advies meezenden met de beslissing.

Indien de klager het niet eens is met de beslissing van de Minister, kan hij op grond van artikel 83 en 84 WIV zijn klacht indienen bij de Nationale Ombudsman.[134]

Vervolgens deelt de Nationale ombudsman zijn schriftelijk en, voor zover de veiligheid dan wel andere gewichtige belangen van de staat zich daartegen niet verzetten, met redenen omkleed oordeel over de klacht mede aan de klager. De Nationale ombudsman deelt zijn oordeel tevens mede aan de betrokken Minister. Daarbij kan hij de met redenen omklede aanbevelingen doen die hij dienstig oordeelt. Indien de strekking van de aanbevelingen daartoe aanleiding geeft, kan hij deze tevens mededelen aan de klager. De betrokken Minister dient vervolgens de Nationale ombudsman binnen zes weken schriftelijk te informeren over de gevolgen die hij aan het oordeel en de aanbevelingen verbindt.

7.2.2 Civiel recht

Bij het uitvoeren van haar bevoegdheden kan de overheid schade veroorzaken. In het kader van cyber security kan bijvoorbeeld worden gedacht aan het geval dat het OM computergegevens ontoegankelijk maakt dan wel vernietigt of dat zij computers in beslag neemt. De overheid is onder (bijzondere) omstandigheden aansprakelijk voor deze schade. De wettelijke basis voor deze aansprakelijkheid is artikel 6:162 BW: de onrechtmatige daad. Het kan als een waarborg voor individuen worden gezien dat de overheid onder bepaalde omstandigheden aansprakelijk is voor schade veroorzaakt in het kader van de bestrijding van cybercriminaliteit.

Twee soorten onrechtmatig overheidsoptreden moeten in dit kader worden onderscheiden: bestuursrechtelijk onrechtmatig optreden en strafvorderlijk onrechtmatig optreden.

Met betrekking tot onrechtmatig overheidsoptreden in het bestuursrecht geldt het beginsel van de formele rechtskracht. Dit beginsel houdt in dat wanneer de bestuursrechter de onrechtmatigheid van een besluit heeft vastgesteld, de burgerlijke rechter van die onrechtmatigheid uitgaat. Bestuursrechtelijke onrechtmatigheid is zodoende in beginsel ook privaatrechtelijke onrechtmatigheid.

Met betrekking tot overheidsoptreden in het strafrecht bestaat verschil tussen de zogenoemde

[134] Zie: http://www.ctivd.nl/?Klachtbehandeling.

onrechtmatigheid *ex tunc* en onrechtmatigheid *ex nunc*. Van de eerste situatie is sprake indien reeds bij het uitoefenen van een bevoegdheid wordt gehandeld in strijd met de toepasselijke wettelijke vereisten of indien het gedrag anders in strijd is met hetgeen volgens ongeschreven regels in het maatschappelijk verkeer betaamt. Indien een strafvorderlijke bevoegdheid wordt gehanteerd bijvoorbeeld zonder de daarvoor noodzakelijke toestemming is sprake van deze vorm van onrechtmatigheid.

Van onrechtmatigheid *ex nunc* is sprake indien de aanvankelijke rechtvaardiging voor het strafvorderlijk overheidsoptreden achteraf niet gefundeerd blijkt te zijn. Hiervan kan sprake zijn indien uit het onderzoek blijkt dat de verdenking van iemand ten aanzien van een bepaald misdrijf ten onrechte was aangenomen. Voor aansprakelijkheid van de overheid is hier vereist dat de onschuld van de ex-verdachte moet blijken uit de stukken van het strafproces: het enkele vrijspreken van de verdachte of het seponeren van de zaak is niet voldoende voor het aannemen van deze vorm van onrechtmatig overheidsoptreden.

Zowel voor onrechtmatig bestuursrechtelijk optreden als onrechtmatig strafvorderlijk optreden geldt dat wanneer de onrechtmatigheid van het overheidsoptreden eenmaal is vastgesteld, vervolgens een causaal verband tussen dit overheidsoptreden en de schade moet worden aangetoond. Verder is bij de toekenning van schadevergoeding van belang in hoeverre de betrokkene eigen schuld (artikel 6:101 BW) heeft aan het overheidsoptreden.

7.2.3 Strafrecht

In het kader van het strafrecht gelden voor de verdachte van een strafbaar feit alle reguliere waarborgen die het commune en bijzondere strafrecht alsmede strafvordering bevatten, evenals de waarborgen die voortvloeien uit mensenrechtenverdragen, zoals artikel 6 EVRM.[135] Deze waarborgen gelden onverkort indien de verdachte zich in het buitenland bevindt, wat niet zelden het geval zal zijn bij verdachten van cyberaanvallen.

Artikel 1 Sr en artikel 1 Sv zijn de centrale waarborgen in het strafrecht. In artikel 1 Sr is vastgelegd dat geen feit strafbaar is dan uit kracht van een daaraan voorafgegane strafbare bepaling. Gelet op de steeds verdere ontwikkeling van technologieën die wordt gebruikt voor cyberaanvallen, kan het voorkomen dat bepaalde nieuwe (technologische) gedragingen niet vallen onder strafbaargestelde delictsomschrijvingen. Het is van belang dat het materiele strafrecht geen achterstand oploopt ten opzichte van de praktijk van cybercriminaliteit.

Daarnaast bepaalt artikel 1 Sv dat strafvordering alleen plaats heeft op de wijze bij de wet voorzien. Zoals al naar voren is gekomen in hoofdstuk 5 zijn de opsporingsbevoegdheden in het kader van cyber security de laatste jaren uitgebreid. Deze uitbreiding is ook nog volop aan de gang. Gedurende een periode waarin de overheid het noodzakelijk acht strafvorderlijke bevoegdheden uit te breiden blijft het van belang waakzaam te zijn dat strafvordering blijft plaatsvinden (alleen) op basis van de wet. Buitenwettelijke opsporingsmethoden zijn

[135] Vergelijk artikel 14 IVBPR, dat enigszins meer bescherming biedt dan artikel 6 EVRM, en artikelen 47 en 48 Handvest.

onrechtmatig.

7.3 Wet openbaarheid van bestuur

7.3.1 Achtergrond

De Wet openbaarheid van bestuur (de "**Wob**") regelt de openbaarmaking van informatie door de overheid. De Wob geeft een ieder de bevoegdheid informatie neergelegd in documenten over een bestuurlijke aangelegenheid op te vragen bij een bestuursorgaan. Het uitgangspunt van de Wob is dat in beginsel aan alle verzoeken tot openbaarmaking moet worden voldaan. De Wob stelt burgers hierdoor in beginsel in staat om informatie die door de overheid in het kader van cyber security wordt verzameld op te vragen.

7.3.2 Verzoek

Iedereen kan op grond van de Wob een bestuursorgaan verzoeken bepaalde informatie openbaar te maken. Voor een verzoek gelden geen vormvereisten. Voorts is niet vereist dat de verzoeker uitdrukkelijk een beroep op de Wob doet.[136]

Omdat enkel wordt getoetst of openbaarmaking van de informatie in het algemene belang van het publiek is, hoeft de verzoeker bij zijn verzoek geen specifiek belang te vermelden.[137] Indien de verzoeker zijn verzoek te algemeen geformuleerd heeft, dient het bestuursorgaan de verzoeker behulpzaam te zijn bij het zo nodig nader formuleren van zijn verzoek.[138]

Een Wob-verzoek kan betrekking hebben op alle informatie die is neergelegd in documenten over een bestuurlijke aangelegenheid. Een bestuurlijke aangelegenheid wordt in de Wob gedefinieerd als een aangelegenheid die betrekking heeft op het beleid van een bestuursorgaan, daaronder begrepen de voorbereiding en de uitvoering ervan. In de parlementaire geschiedenis is in dit verband opgemerkt dat een bestuurlijke gelegenheid betrekking heeft op "het openbaar bestuur in al zijn facetten".[139] Het begrip moet derhalve ruim worden uitgelegd en kan ook cyber security omvatten.

Enkel documenten komen in aanmerking voor openbaarmaking. Als document in de zin van de Wob wordt aangemerkt een bij het bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat. Onder "ander materiaal dat gegevens bevat" valt onder meer foto- en filmmateriaal.[140] Op grond van vaste rechtspraak wordt voorts alle informatie die is opgeslagen op elektronische gegevensdragers aangemerkt als document.[141] Niet alleen documenten die door het bestuursorgaan zelf worden gecreëerd vallen onder de Wob. Ook alle van buiten komende

---

[136] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 23.

[137] Zie artikel 3 lid 3 Wob.

[138] Zie artikel 3 lid 4 Wob.

[139] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 23.

[140] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 21.

[141] Zie ABRvS, 16 augustus 2006, *AB* 2006, 337.

stukken en ander voor overheidsorganen bestemd materiaal verkrijgen de status van document in de zin van de Wob.[142] Mondelinge informatie valt niet onder de reikwijdte van de Wob.

7.3.3 De Wob versus de WIV en de Wpg

De Wob geldt niet voor gegevens die berusten bij de AIVD en/of de MIVD. De mogelijkheid om gegevens op te vragen bij de AIVD/MIVD is uitputtend geregeld in een aparte afdeling van de WIV.[143] De Wpg geldt bovendien slechts beperkt ten opzichte van de Wob. De Wpg is slechts van toepassing op persoonsgegevens, niet de documenten waarin zij zijn vervat.[144] Op grond van de Wob kan zodoende een geanonimiseerde versie van het desbetreffende document worden verstrekt. In dit verband is van belang dat uit het document niet de identiteit van betrokkenen mag kunnen worden afgeleid.[145] Een uitgebreide bespreking van deze regelingen valt buiten het bestek van deze juridische analyse.

7.3.4 Uitzonderingsgronden

De Wob kent diverse uitzonderingsgronden op grond waarvan een bestuursorgaan de openbaarmaking van de gevraagde informatie achterwege kan of zelfs moet laten. De uitzonderingsgronden staan limitatief omschreven in artikel 10 Wob.

In artikel 10 lid 1 van de Wob staan de zogeheten absolute weigeringsgronden. Indien één van deze gronden zich voordoet is het bestuursorgaan verplicht het verzoek om informatie af te wijzen. Ingevolge deze absolute weigeringsgronden wordt onder meer geen informatie verstrekt voorzover dit de veiligheid van de Staat zou kunnen schaden. Tevens wordt geen informatie verstrekt voor zover deze bedrijfs- en fabricagegegevens betreft, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld. In de jurisprudentie is bepaald dat deze uitzonderingsgrond restrictief moet worden uitgelegd en dat van bedrijfs- en fabricagegegevens slechts sprake is indien en voorzover uit die gegevens wetenswaardigheden kunnen worden gelezen of afgeleid met betrekking tot de technische bedrijfsvoering of het productieproces.[146]

In artikel 10 lid 2 van de Wob staan de relatieve uitzonderingsgronden. Bij deze uitzonderingsgronden dient het bestuursorgaan een afweging te maken tussen het door de betreffende weigeringsgrond beschermde belang en het algemene belang dat het publiek kennis kan nemen van de informatie. Het specifieke belang van de verzoeker speelt bij deze belangenafweging geen rol; er wordt enkel getoetst aan het algemene belang.

---

[142] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 21.

[143] Zie hoofdstuk 4 WIV. Vergelijk Rb. Arnhem 17 september 2009, LJN: BK0408, RO. 3.6, verwijzend naar Kamerstukken II, 1997-1998, 25 877, nr. 3, 62-63.

[144] M.G.J. Maas-Cooymans & C.N. van der Sluis, 'Wet openbaarheid van bestuur in de praktijk', *Gst.* 2010, 24, verwijzend naar Rb. Zwolle 17 maart 2009, *LJN* BH6275, RO. 2.

[145] Rb. Zwolle 17 maart 2009, *LJN* BH6275, RO. 2.

[146] Zie ABRvS, 8 oktober 2003, AB 2004, 23.

Een relevante uitzonderingsgrond in dit verband is de opsporing en vervolging van strafbare feiten. Informatieverstrekking kan op deze grond worden geweigerd indien de openbaarmaking van gegevens die opsporingsambtenaren of het OM hebben vergaard, de opsporing en vervolging van strafbare feiten zou frustreren.[147] Een vereiste is dan wel dat de opsporing al daadwerkelijk is aangevangen.

Een andere belangrijke beperking op het beginsel van openbaarmaking heeft betrekking op persoonlijke beleidsopvattingen in documenten die zijn opgesteld voor intern beraad. Deze persoonlijke beleidsopvattingen worden op grond van artikel 11 lid 1 van de Wob niet openbaar gemaakt. Met deze beperking is beoogd te waarborgen dat bij de primaire vormgeving van het beleid de betrokkenen in alle vrijheid hun gedachten en opvattingen kunnen uiten.[148] Niet alleen de persoonlijke beleidsopvattingen van ambtenaren vallen onder de werking van artikel 11 lid 1 Wob; ook de persoonlijke beleidsopvattingen van derden, zoals externe adviseurs en advocaten, die van buitenaf bij het interne beraad zijn betrokken vallen hieronder.

In de Wob wordt onder persoonlijke beleidsopvatting verstaan een opvatting, voorstel, aanbeveling of conclusie van een of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde documenten.[149] Het hoeft in dit verband niet te gaan om tot individuele personen herleidbare opvattingen: ook opvattingen van groepen van personen vallen onder de uitzondering. In dit verband kan bijvoorbeeld worden gedacht aan een ambtelijke werkgroep.[150] Een voorbeeld van documenten bestemd voor intern beraad met persoonlijke beleidsopvattingen zijn notulen van de ministerraad.[151]

7.4 Bescherming van persoonsgegevens

De overheid en het bedrijfsleven verwerken in het kader van preventie, bestrijding en opsporing van cyberaanvallen gegevens die natuurlijke personen direct of indirect kunnen identificeren. Deze gegevens staan bekend als zogeheten "persoonsgegevens" en indien geen sprake is van een verdrag of een bijzondere wet wordt de verwerking van dit soort gegevens in algemene zin beheerst door de Wbp. Deze wordt hierna kort besproken in paragraaf 7.4.1.

De Wbp is niet van toepassing op de gegevensverwerking door of ten behoeve van de inlichtingen- en veiligheidsdiensten als bedoeld in de WIV, de gegevensverwerking ten behoeve van de uitvoering van de politietaak als bedoeld in de Politiewet 1993 en de uitvoering van de Wjsg. De WIV, de Wet Politiegegevens ("**Wpg**") en de Wjsg zijn bijzondere wetten in die zin dat zij beide een eigen kader van voorwaarden en waarborgen voor gegevensverwerking kennen. Deze voorwaarden en waarborgen komen hierna kort aan de orde in paragrafen 7.4.2 en 7.4.3 en 7.4.4.

---

[147] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 35.

[148] Zie Kamerstukken II, 1986-1987, 19 859, nr. 3, p. 38.

[149] Zie artikel 1 onder f Wob.

[150] Zie ABRvS, 4 mei 2010, *LJN* BM3240.

[151] Zie ABRvS, 17 februari 2010, *LJN* BL4132.

7.4.1 Verwerking van persoonsgegevens op grond van de Wbp

Definities

Alvorens wordt ingegaan op de materiele verplichtingen uit de Wbp, lichten wij hieronder eerst kort een aantal belangrijke definities uit de Wbp toe.

- **Persoonsgegeven** - Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Voorbeelden zijn naam, adres- en woonplaatsgegevens, e-mailadressen, inkomensgegevens en gegevens die zijn opgenomen in personeelsdossiers. Een persoon is identificeerbaar als zijn identiteit zonder onevenredige inspanning kan worden achterhaald door de verantwoordelijke of ieder ander..
- **Verwerking van persoonsgegevens -** Dit betreft alle handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, raadplegen, bewaren, doorgeven, bijwerken en vernietigen van persoonsgegevens.
- **Verantwoordelijke -** De verantwoordelijke is de natuurlijke persoon of de rechtspersoon die of het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- **Betrokkene -** De betrokkene is de natuurlijke persoon op wie het persoonsgegeven betrekking heeft.

Basisvoorwaarden

Artikel 6 tot en met 9 Wbp omvatten de basisvoorwaarden waaronder persoonsgegevens kunnen worden verwerkt. Op grond van artikel 6 en 7 Wbp mogen persoonsgegevens slechts in overeenstemming met de wet, op behoorlijke en zorgvuldige wijze en voor welbepaalde doeleinden worden verwerkt.

Artikel 8 Wbp omvat een limitatieve opsomming van zogenaamde verwerkingsgrondslagen. Verwerking van persoonsgegevens is uitsluitend toegestaan als deze noodzakelijk is voor de doeleinden waarvoor de gegevensverwerking plaatsvindt, aansluiten bij (één van) deze verwerkingsgrondslagen. Relevante verwerkingsgrondslagen zijn in het kader van cyber security met name de volgende.

- **Toestemming** – Persoonsgegevens mogen worden verwerkt als de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven. De toestemming moet specifiek zijn, in vrijheid zijn gegeven en berusten op voldoende informatie.
- **Wettelijke plicht** – Persoonsgegevens mogen worden verwerkt voor zover dit noodzakelijk is ter nakoming van een wettelijke plicht. Als een opsporingsinstantie op grond van een wettelijke bevoegdheid gegevens vordert, is het verstrekken van de gegevens op deze grond toegestaan.
- **Vervulling publiekrechtelijke taak** – Persoonsgegevens mogen worden verwerkt, voor zover dit noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van het

bestuursorgaan die de verwerking uitvoert of waaraan de persoonsgegevens worden verstrekt.

- **Gerechtvaardigd belang –** Persoonsgegevens mogen worden verwerkt voor zover dit noodzakelijk is voor een gerechtvaardigd belang van de verantwoordelijke of een derde en de fundamentele rechten van de betrokkene niet moeten prevaleren.

Artikel 9 Wbp bepaalt voorts, dat persoonsgegevens niet verder mogen worden verwerkt als die verdere verwerking onverenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk zijn verkregen.

Informatieplicht

Voor de verantwoordelijke geldt de verplichting de betrokkene over wiens persoonsgegevens hij beschikt, te informeren. De informatieplicht staat in de artikelen 33 en 34 Wbp en geldt zowel indien de verantwoordelijke de gegevens van de betrokkene zelf heeft verkregen als ingeval hij deze van een derde verkreeg.[152] Op grond van deze bepalingen dient de verantwoordelijke aan de betrokkene
(i) zijn identiteit bekend te maken;
(ii) de doeleinden van verwerking van de gegevens mede te delen; en
(iii) nadere informatie te verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Het moment waarop de verantwoordelijke de informatie aan betrokkene dient te verstrekken is afhankelijk van of hij de persoonsgegevens rechtstreeks van betrokkene of van een derde heeft verkregen. In het eerste geval is dit het moment waarop de verantwoordelijke de gegevens van de betrokkene verkrijgt. In het tweede geval is het uitgangspunt het moment van vastlegging.

Inzage in persoonsgegevens

Eenieder dient in beginsel in de gelegenheid te zijn om na te kunnen gaan of zijn persoonsgegevens worden verwerkt en voor welk doel dit gebeurt. Artikel 35 Wbp geeft de betrokkene dan ook het recht te allen tijde de verantwoordelijke te verzoeken om hem mede te delen of zijn persoonsgegevens worden verwerkt. De verantwoordelijke is vervolgens gehouden de betrokkene binnen vier weken hieromtrent een schriftelijke mededeling te doen. Indien de persoonsgegevens worden verwerkt, dient de voornoemde mededeling te zijn voorzien van onder meer een gedetailleerd overzicht van de gegevens en een omschrijving van de doeleinden van de verwerking.

Uitzonderingsgronden

Artikel 43 Wbp omvat een aantal uitzonderingen op (onder meer) de bepalingen voor verdere

[152] In dit geval wordt een uitzondering op de informatieplicht gemaakt indien informatieverstrekking onmogelijk blijkt, onevenredig veel inspanning kost of indien vastlegging of verstrekking op grond van de wet is voorgeschreven.

verwerking, de informatieplicht en het inzagerecht. Deze bepalingen kunnen onder meer buiten toepassing worden gelaten, voor zover dit noodzakelijk is voor de:

- veiligheid van de staat;
- voorkoming, opsporing of vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen; of
- toezicht op naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de twee laatstgenoemde belangen.

7.4.2 Verwerking van persoonsgegevens op grond van de WIV

Hoofdstuk 3 van de WIV bevat regels ten aanzien van de gegevensverwerking door de AIVD en de MIVD. Gelet op de taakomschrijving van deze diensten (zie paragraaf 3.2.3) zal deze verwerking in bepaalde gevallen betrekking hebben op persoonsgegevens. Gegevensverwerking in de zin de van de WIV wordt hetzelfde gedefinieerd als in de Wbp.[153]

Rechtmatige gegevensverwerking

Gegevensverwerking in de zin van de WIV vindt slechts plaats voor zover dit een bepaald doel dient en voor zover dit noodzakelijk is voor een goede uitvoering van de WIV of voor de Wet veiligheidsonderzoeken.[154] Gegevensverwerking is voorts slechts toegestaan in bepaalde door de wet omschreven gevallen, waarbij onderscheid wordt gemaakt tussen de gevallen waarin de AIVD gegevens mag verwerken en de gevallen waarin de MIVD dit mag.[155] Gegevensverwerking is in dit verband voor beide diensten onder meer toegestaan indien deze verwerking betrekking heeft op personen die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat. Beide gevallen zijn relevant in het kader van cyber security.

Gegevensverstrekking

De AIVD en de MIVD zijn in het kader van een goede taakuitvoering en onder strikte voorwaarden, zoals gesteld in de artikelen 36 en 37 WIV, bevoegd om gegevens te verstrekken aan derden. Dit zijn bijvoorbeeld de Ministers, bestuursorganen of inlichtingen- en veiligheidsdiensten uit andere landen. Indien bij de verwerking van gegevens blijkt van gegevens die van belang kunnen zijn voor de opsporing en vervolging van strafbare feiten, kan daarvan ingevolge artikel 38 WIV en onder de voorwaarden uiteengezet in artikel 40 en 41 WIV schriftelijk mededeling worden gedaan aan het OM.

7.4.3 Verwerking van persoonsgegevens op grond van de Wpg

In de Wpg zijn regels opgenomen ten aanzien van de verwerking van politiegegevens. Een

[153] Zie artikel 1 onder f WIV en artikel 1 onder b WBP

[154] Zie artikel 12 WIV.

[155] Zie respectievelijk artikel 13 leden 1 en 2 WIV.

politiegegeven in de zin van de Wpg is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt.[156] Voor de betekenis van de term "verwerken" is aangesloten bij de Wbp.[157]

Rechtmatige verwerking politiegegevens

Op grond van artikel 3 Wpg worden politiegegevens slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wpg geformuleerde doeleinden. Politiegegevens worden voorts slechts verwerkt voor zover zij rechtmatig zijn verkregen en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn. De gegevens worden tot slot uitsluitend voor een ander doel verwerkt dan waarvoor zij zijn verkregen voor zover de Wpg daarin uitdrukkelijk voorziet.

De verantwoordelijke voor de politiegegevens[158] dient de nodige maatregelen te treffen opdat de politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Deze doeleinden zijn bepaald in artikelen 8,9,10,12 en 13 Wpg.

Verstrekking politiegegevens

De verantwoordelijke voor de politiegegevens kan deze gegevens onder bepaalde voorwaarden verstrekken aan opsporingsambtenaren en gezagsdragers (artikel 16 Wpg), evenals aan inlichtingendiensten en buitenlandse opsporingsinstanties (artikel 17 Wpg). Daarnaast is, met het oog op een zwaarwegend belang, ook verstrekking mogelijk aan bepaalde derde personen en instanties.[159]

Rechten betrokkene

De betrokkene heeft in beginsel recht op kennisneming van de gegevens die op hem of haar betrekking hebben (artikel 25 Wpg). Een verzoek hiertoe kan enkel worden afgewezen indien dit noodzakelijk is in het belang van de goede uitvoering van de politietaak, gewichtige belangen of de veiligheid van de staat (artikel 27 Wpg). Indien de politiegegevens feitelijk onjuist, voor het doel van de verwerking onjuist of niet terzake dienend zijn dan wel in strijd met een wettelijk voorschrift worden verwerkt, kan de betrokkene verzoeken deze gegevens aan te vullen, te verwijderen of af te schermen (artikel 28 Wpg).

Tegen een besluit aangaande het al dan niet verlenen van inzage in de gegevens of het al dan niet wijzigen van de gegevens kan de betrokkene administratief beroep instellen bij de bestuursrechter (artikel 29 lid 1 Wpg). Het is voor de betrokkene niet mogelijk in bezwaar te gaan. Wel kan de betrokkene zich richten tot het CBP met het verzoek te bemiddelen of te

[156] Zie artikel 1 sub a Wpg.

[157] Zie artikel 1 sub c Wpg.

[158] Wie dit is, is afhankelijk van door wie/welke organisatie de politiegegevens worden verwerkt. Zie artikel 1 sub f Wpg.

[159] Zie artikelen 18, 19 en 20 Wpg.

adviseren in de kwestie (artikel 29 lid 2 Wpg).

7.4.4 Verwerking van persoonsgegevens op grond van de Wjsg

In de Wjsg zijn regels opgenomen ten aanzien van de verwerking van justitiële en strafvorderlijke gegevens. Justitiële gegevens zijn gegevens omtrent natuurlijke personen en rechtspersonen inzake de toepassing van het strafrecht of de strafvordering.[160] Strafvorderlijke gegevens zijn gegevens over een natuurlijk persoon of rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het Openbaar Ministerie in een strafdossier of langs geautomatiseerde weg verwerkt.[161]

Verwerking justitiële gegevens

Op grond van artikel 2 Wjsg kan de Minister van Veiligheid en Justitie justitiële gegevens verwerken in justitiële documentatie ten behoeve van een goede strafrechtspleging. De Minster dient in dit verband op grond van artikel 3 Wjsg de nodige maatregelen te treffen opdat deze gegevens juist en nauwkeurig zijn.

Justitiële gegevens kunnen worden verstrekt aan rechterlijke ambtenaren, aan de Minister van Veiligheid en Justitie en lichamen of personen die ingevolge artikel 257ba Sv bevoegd zijn een strafbeschikking uit te vaardigen (artikel 8 leden 1 t/m 3 Wjsg). Daarnaast kunnen justitiële gegevens op grond van het Besluit justitiële gegevens ("**Bjg**") worden verstrekt aan in het Bjg bepaalde overheidsinstanties voor een gelimiteerd aantal doelen, zoals het afgeven van bepaalde verklaringen over personen en het nemen van bestuursrechtelijke besluiten (bijvoorbeeld vergunningverlening). In artikel 8 lid 3 Wjsg is vastgelegd dat de justitiële gegevens niet voor een ander doel mogen worden gebruikt dan waarvoor zij zijn verstrekt, tenzij bij wettelijk voorschrift anders is bepaald dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt, daartoe noodzaakt.

Verwerking strafvorderlijke gegevens

Het College van procureurs-generaal is ingevolge artikel 39a Wjsg de verantwoordelijke voor het verwerken van strafvorderlijke gegevens. Voornoemd College verwerkt slechts gegevens indien dit noodzakelijk is voor een goede vervulling van de taak van het Openbaar Ministerie of het nakomen van een andere wettelijke verplichting (artikel 39b Wjsg).

Voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, kan het College van procureurs-generaal aan een gelimiteerde lijst van overheidsinstanties en ambtenaren strafvorderlijke gegevens verstrekken (artikel 39e Wjsg). Daarnaast kan voornoemd College met het oog op een zwaarwegend algemeen belang aan personen of instanties strafvorderlijke gegevens verstrekken, indien dit noodzakelijk is voor één van de in artikel 39f lid 1 Wjsg omschreven doeleinden. Op basis van dit artikel kunnen ook aan private personen en organisaties strafvorderlijke gegevens worden verstrekt.

[160] Zie artikel 1 sub a WJSG.

[161] Zie artikel 1 sub b WJSG.

Voorbeelden van doeleinden ingevolge artikel 39f lid 1 Wjsg zijn het handhaven van de orde en veiligheid en het uitoefenen van het toezicht op het naleven van regelgeving. Het College van procureurs-generaal dient de gegevens in zodanige vorm te verstrekken dat herleiding tot andere personen dan betrokkene redelijkerwijs kan worden voorkomen.

Rechten betrokkene

Zowel ten aanzien van justitiële gegevens als strafvorderlijke gegevens geldt dat de betrokkene in beginsel recht heeft op kennisneming van de gegevens die op hem of haar betrekking hebben (artikelen 18 en 39i Wjsg).Een verzoek hiertoe kan slechts worden geweigerd in een gelimiteerd aantal gevallen (zie artikelen 21 en 39l Wjsg).Indien de gegevens feitelijk onjuist, onvolledig of niet ter zake dienend zijn, kan de betrokkene het College van procureurs-generaal verzoeken deze gegevens te verbeteren, aan te vullen of af te schermen (artikelen 22 en 39m Wjsg).

Tegen een besluit betreffende het al dan niet verlenen van inzage in de gegevens of tot het al dan niet wijzigen van de gegevens staat voor de betrokkene bezwaar en beroep open (zie artikelen 39n lid 1 en 23 lid 1 Wjsg). Daarnaast kan de betrokkene het CBP verzoeken te bemiddelen of te adviseren in de kwestie (artikel 39n lid 2 en 23 lid 2 Wjsg).