De juridische aandachtspunten bij het delen van dreigingsinformatie in samenwerkingsverbanden: een complexe aangelegenheid

mr. M. Moeskops en mr. N. Hermans-Falot[1]

In dit artikel schetsen wij de juridische randvoorwaarden voor het uitwisselen van dreigingsinformatie binnen private en publieke samenwerkingsverbanden ten behoeve van het bevorderen van de digitale weerbaarheid (cybersecurity) van organisaties. Dit artikel beschrijft de juridische aandachtspunten die bij ieder samenwerkingsverband van belang zijn en biedt een handreiking voor de succesvolle inrichting van informatie-uitwisseling voor zowel publieke als private organisaties.

1. Inleiding en achtergrond

Het uitwisselen van dreigingsinformatie is een belangrijk hulpmiddel bij het bevorderen van de digitale weerbaarheid van organisaties.[2] Het delen van dreigingsinformatie heeft echter verschillende juridische voorwaarden en risico's. In dit artikel gaan wij nader in op deze juridische kaders, waarbij wij allereerst onderzoeken welke drempels bestaan voor het verstrekken van informatie aan andere partijen in een samenwerkingsverband en of die drempels kunnen worden weggenomen. Daarnaast staan wij stil bij het beschermen van de vertrouwelijkheid van reeds verstrekte informatie.

In paragraaf 2 schetsen wij uitgebreider de achtergrond en context van dit vraagstuk en gaan wij in op nationale en Europese ontwikkelingen rondom het uitwisselen van dreigingsinformatie. In paragraaf 3 staan we stil bij een aantal algemene en veelvoorkomende juridische dilemma's in samenwerkingsverbanden, te weten de verstrekking van persoonsgegevens in lijn met geldende privacywetgeving, civiele aansprakelijkheid, verbintenisrechtelijke drempels en mogelijke risico's vanuit het mededingingsrecht. In paragraaf 4 beschrijven we de mogelijkheden voor het waarborgen van de vertrouwelijkheid van verstrekte informatie. We sluiten af met een conclusie en aanbevelingen.

In dit artikel bespreken wij alleen het vrijwillig verstrekken van dreigingsinformatie aan andere partijen in een samenwerkingsverband. Verplichte verstrekking van dreigingsinformatie op grond van een wettelijke verplichting of het delen van informatie met politie en justitie in het kader van opsporing en vervolging van strafbare feiten is uitgesloten van de reikwijdte van dit artikel aangezien het doel van die informatiedeling over het algemeen wezenlijk anders is en daarmee juridisch anders wordt getoetst.[3]

2. Nationale en Europese ontwikkelingen rondom uitwisseling van dreigingsinformatie

Het Nederlandse beeld voor informatie-uitwisseling in het kader van netwerk- en informatiebeveiliging kenmerkt zich door een decentrale aanpak. Dit betekent dat er niet één organisatie is die informatie verzamelt, analyseert en deelt met relevante partijen, maar dat een zogenaamd 'landelijk dekkend stelsel' alle private en publieke partijen voorziet van

1. Marco Moeskops en Nathalie Hermans-Falot zijn beiden Legal Counsel bij ABN AMRO Bank N.V. Dit artikel is op persoonlijke titel geschreven.
2. Dreigingsinformatie is een breed begrip. In dit artikel verstaan we onder dreigingsinformatie alle informatie met betrekking tot dreigingen en tekortkomingen in netwerk- en informatiesystemen, alsook informatie die relevant is om inbreuken op netwerk- en informatiesystemen te voorkomen. Dreigingsinformatie bestaat uit verschillende categorieën informatie, waaronder technische informatie van mogelijk geraakte of bedreigde netwerk- en informatiesystemen, informatie over de aanvaller of aanvalstechniek en informatie over eventuele maatregelen die zijn getroffen om een aanval te mitigeren of voorkomen.
3. Zie voor dit onderwerp nader N. Falot & C.M. Kroon-Koning, 'De verwerking van dreigingsinformatie in het kader van netwerk- en informatiebeveiliging: strafrechtelijke persoonsgegevens in de zin van de AVG?', *Computerrecht* 2019, afl. 4.

voor hun relevante informatie.[4] Deze aanpak heeft geleid tot een versnippering van het cybersecuritylandschap. Een veelvoud aan kleinere en grotere samenwerkingsverbanden wisselen met elkaar informatie uit, bijvoorbeeld centrale overheidsorganisaties zoals het Nationaal Cyber Security Centrum ('NCSC'), schakelorganisaties zoals de verschillende computercrisisteams en daarnaast tal van publieke en private organisaties.[5]

Toch blijft het bevorderen van de uitwisseling van dreigingsinformatie een voortdurende terugkomend thema. In 2018 is het uitwisselen van dreigingsinformatie in publiek-private samenwerking als een belangrijke doelstelling in de Nederlandse Cyber Security Agenda gepresenteerd.[6] Het aantal samenwerkingsverbanden op het gebied van cybersecurity blijft dan ook toenemen.[7] Desalniettemin concludeert de Cyber Security Raad dat organisaties vaak nog onvoldoende dreigingsinformatie tot hun beschikking hebben en dat het delen van belangrijke informatie om verschillende redenen, waaronder juridische drempels, vaak nog onvoldoende gebeurt.[8] Ook de Onderzoeksraad voor Veiligheid deelt deze zorgen over juridische beperkingen om informatie te delen.[9] Dit heeft dan ook de vraag opgeroepen of het huidige stelsel van informatie-uitwisseling efficiënt is en of er mogelijkheden bestaan deze te bevorderen.[10]

Ook op Europees vlak bestaat blijvende aandacht voor het efficiënt inrichten van samenwerkingsverbanden op het gebied van cybersecurity. De Europese Netwerk- en informatiesystemen Richtlijn ('NIB-Richtlijn') was een eerste aanzet voor het bevorderen van het delen van dreigingsinformatie op Europees vlak.[11] Met name de introductie van het Computer Security Incident Response Team ('CSIRT') Netwerk had tot doel het bevorderen van informatiedeling op internationaal vlak. Uit de evaluatie van de NIB-Richtlijn is echter gebleken dat het uitwisselen van dreigingsinformatie onvoldoende effectief is. Dit is dan ook één van de doelstellingen van het voorstel tot uitbreiding van de NIB-Richtlijn, de NIB2-Richtlijn. Met de voorgestelde aanpassingen van de NIB2-Richtlijn wordt vrijwillige informatiedeling ter bevordering van de digitale weerbaarheid verder gestimuleerd.[12] In het voorstel voor een NIB2-Richtlijn wordt een verplichting opgenomen voor de lidstaten om ervoor te zorgen dat essentiële en belangrijke entiteiten onderling dreigingsinformatie kunnen uitwisselen in vertrouwde gemeenschappen.[13] De lidstaten moeten ook regels vaststellen voor de wijze waarop dreigingsinformatie mag worden gedeeld binnen deze vertrouwde gemeenschappen, in overeenstemming met geldende wet- en regelgeving zoals de AVG (zie paragraaf 3.5). Ook het aantal sectoren waarbinnen 'vitale' organisaties moeten worden geïdentificeerd wordt onder de NIB2 uitgebreid, waarmee de doelgroep van het NCSC mogelijk groter wordt. Hoe het uitwisselen van dreigingsinformatie onder de NIB2-Richtlijn vorm gaat krijgen zal moeten blijken bij de implementatie van deze Richtlijn in de nationale wet.

Naast de introductie van de NIB2-Richtlijn heeft de Europese Commissie een voorstel ingediend voor de oprichting van een Joint Cyber Unit ('JCU'): een virtueel platform om informatie-uitwisseling en andere samenwerking tussen de Europese instanties en lidstaten te versterken ten behoeve van de digitale weerbaarheid binnen de EU.[14] Het Nederlands kabinet is positief over deelname in de JCU, maar merkt ook hierbij op dat een nadere uitwerking nodig is "*van randvoorwaarden voor effectieve en efficiënte informatie-uitwisseling zoals [...], de beperkingen vanwege wettelijke kaders en het garanderen van de vertrouwelijkheid van informatie*".[15]

3. Het verstrekken van dreigingsinformatie: grondslagen, drempels en voorwaarden

Zowel publieke als private partijen leren veel van elkaar door inzicht te krijgen in de voorgevallen dreigingen, hoe deze kunnen worden afgewenteld of hoe

4. 'Aansluiting op het landelijk dekkend stelsel', ncsc.nl.
5. Computercrisisteams worden ook wel Computer Emergency Response Teams (CERTs) genoemd. CERTs die onderdeel zijn van het Landelijk Dekkend Stelsel zijn de Informatiebeveiligingsdienst (IBD), Z-CERT, WM-CERT en SURF-CERT.
6. 'Nederlandse Cyber Security Agenda', ncsc.nl, april 2018, p. 19
7. In 2020 is de Payment Institutions Information Sharing & Analysis Center (PI-ISAC) opgericht, voor financiële instellingen die niet reeds onder de financiële kerninfrastructuur vallen: 'PI-ISAC', digitaltrustcenter.nl. Ook zijn in 2021 weer twee belangrijke nieuwe initiatieven gestart: het Samenwerkingsverband Cybersecurity, op initiatief van Staatssecretaris van Economische Zaken en Klimaat en de Twente University Centre for Cybersecurity Research ('TUCCR'), die meer wetenschappelijk georiënteerd is.
8. Cyber Security Raad adviesrapport 'Integrale aanpak cyberweerbaarheid', CSR Advies 2021, nr. 2.
9. Onderzoeksraad voor de Veiligheid rapport 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix', Rapport, 21 December 2021.
10. Zie bijvoorbeeld het recente onderzoek van het Wetenschappelijk Onderzoek- en Documentatiecentrum ('WODC') naar de effectiviteit van het huidige decentrale stelsel van informatie-uitwisseling: R. Brennenraedst e.a., 'Informatie-uitwisseling landelijk dekkend stelsel cybersecurity', *WODC*, eindrapport 14 oktober 2020.
11. Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.
12. Zie voor het voorstel van de Europese Commissie voor een NIB2 Richtlijn: COM (2020) 823.
13. Artikel 26 concept NIB-2 Richtlijn, COM (2020) 823.
14. Aanbeveling (EU) 2021/1086 van de Commissie van 23 juni 2021 betreffende de opbouw van een gezamenlijke cybereenheid.
15. *Kamerstukken II* 2020/21, 22112, nr. 3182, p. 5, 'Fiche: Aanbeveling opbouw Joint Cyber Unit'.

de schade en impact kan worden gemitigeerd. In deze paragraaf staan wij stil bij de juridische aandachtspunten voor publieke en private organisaties die informatie willen verstrekken aan andere partijen in een samenwerkingsverband.

3.1. De juridische grondslag voor verstrekking van dreigingsinformatie door overheidsorganisaties

Een overheidsorganisatie mag alleen dreigingsinformatie delen voor zover zij daarvoor een wettelijke grondslag heeft. Een voorbeeld van een publieke organisatie die een wettelijke grondslag heeft om dreigingsinformatie te verstrekken is het NCSC. Het NCSC heeft tot taak vitale aanbieders en rijksoverheidsorganisaties in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, adviseren en indien nodig bijstand te verlenen.[16] Andere organisaties dan rijkoverheidsorganisatie en vitale aanbieders ontvangen indirect informatie van het NCSC via zogenaamde 'Organisaties die Kenbaar Tot Taak' hebben om hun achterban te informeren ('OKTT'), zoals het zoals het Digital Trust Center van het Ministerie van Economische Zaken en Klimaat ('DTC'), CSIRT's, andere computercrisisteams en aanbieders van internettoegangs- en internetcommunicatiediensten.[17]

Vanwege deze geschakelde aanpak voor het delen van dreigingsinformatie is het mogelijk dat het NCSC informatie heeft over een mogelijke dreiging of tekortkoming in een netwerk- of informatiesysteem, maar geen juridische grondslag heeft om die informatie rechtstreeks te delen met alle relevante partijen.[18] De vraag is of het nodig is de grondslag van het NCSC uit te breiden, danwel een grondslag voor andere organisaties te creëren om dreigingsinformatie effectief uit te wisselen. In dat kader vindt momenteel een verkenning plaats naar de uitbreiding van de bevoegdheden van het NCSC, waaronder de bevoegdheid om rechtstreeks informatie te verstrekken aan individuele organisaties die niet deel uitmaken van de doelgroep 'Rijksoverheid en vitale aanbieders'.[19] Hoe een uitbreiding van bevoegdheden, waarbij het NCSC een centralere rol gaat vervullen, zich verhoudt tot de wens om te komen tot een 'landelijk dekkend stelsel' dient overigens nog te worden bezien. De Cyber Security Raad heeft dan ook opgeroepen tot het versneld delen van dreigingsinformatie met schakelorganisaties die vallen onder de OKTT definitie, aangezien daar geen wetswijziging voor nodig is.[20]

Niet wachtende op eventuele wetswijzigingen voor het NCSC is het DTC in de tussentijd reeds overgegaan op het proactief informeren van niet-vitale organisaties.[21] Als OKTT kan het DTC een belangrijke rol spelen bij het ontsluiten van informatie naar organisaties die niet onder de doelgroep van het NCSC vallen. Ook het DTC kampt echter met juridische drempels voor het verstrekken van informatie. Om deze drempels weg te nemen is voor het DTC het Wetsvoorstel bevordering digitale weerbaarheid bedrijven ingediend.[22]

De discussies rondom de juridische grondslag voor het delen van dreigingsinformatie vanuit het NCSC en DTC tonen aan dat er beperkingen zijn aan welke informatie overheidsorganisaties zonder wettelijke grondslag kunnen verstrekken aan andere organisaties. Overheidsorganisaties doen er verstandig aan deze beperkingen zorgvuldig in acht te nemen, hiaten in wetgeving bloot te leggen en waar nodig de wettelijke bevoegdheden voor het delen van relevante informatie te doen uitbreiden. Voorts is het aan te raden een duidelijk overzicht te hebben van de bevoegdheden en doelgroepen van de verschillende betrokken overheidsorganisaties en hoe deze zich tot elkaar verhouden. Zo kan bijvoorbeeld worden voorkomen dat er overlappende bevoegdheden ontstaan door de uitbreiding van de Wbni en het Wetsvoorstel bevordering digitale weerbaarheid bedrijven.

3.2. Staatssteun bij verstrekking van dreigingsinformatie door overheidsorganisaties

In aanvulling op het voorgaande dienen overheidsorganisaties ook rekening te houden met hun rol in een gezonde marktwerking. Ondanks de politieke roep om meer uitwisseling van informatie, blijft het voor de overheid zoeken naar de juiste balans tussen het ondersteunen van partijen in het bevorderen van hun digitale weerbaarheid en het waarborgen en stimuleren van een gezonde marktwerking. De Europese markt voor cybersecurity is groeiende, met een geschatte waarde van 65 miljard dollar in 2025.[23] De mogelijkheden voor publieke organisaties om zonder tegenprestatie in het publieke belang informatie te verstrekken moet daarom worden afgezet tegen het economisch belang van organisaties die op deze markt actief zijn.[24]

Juridisch gezien speelt met name de vraag of door het verstrekken van dreigingsinformatie sprake is

16. Artikel 3 Wbni.
17. Artikel 2 lid 2 Wbni.
18. *Kamerstukken II* 2020/21, 26643, nr. 738, p. 9, 'Uitkomsten verkenning wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten'.
19. *Aanhangsel van de Handelingen* 2020/21, nr. 2173, 'Vragen van het lid Yesilgöz-Zegerius aan de minister van Justitie en Veiligheid'.
20. Cyber Security Raad adviesbrief 'Inzake het versneld delen van incidentinformatie', CSR Advies 2021, nr. 1.
21. 'Digital Trust Center start met actief informeren van bedrijven over digitale dreigingen', digitaltrustcenter.nl.
22. 'Wetsvoorstel bevordering digitale weerbaarheid bedrijven', internetconsultatie.nl.
23. 'De internationale cyber security markt in beeld', computerfutures.com.
24. Staatssteun wordt gedefinieerd als steunmaatregelen die direct of indirect met staatsmiddelen wordt verleend en aan de staat vallen toe te rekenen. Het verbod op staatssteun is geregeld in artikel 107 lid 1 Verdrag betreffende de werking van de Europese Unie ('VWEU').

van staatssteun door het 'selectief verlenen van voordeel aan bepaalde ondernemingen', waarbij dat voordeel is bekostigd door staatsmiddelen.[25] Het begrip 'voordeel' dient zeer ruim te worden uitgelegd en kan onzes inziens ook het vanuit de overheid ontvangen van dreigingsinformatie omvatten.[26] Of het verlenen van dit voordeel onder het staatssteunverbod valt, is onder meer afhankelijk van de vraag of het verstrekken van dreigingsinformatie in een specifiek geval valt onder de Algemene Groepsvrijstellingsverordening of de de-minimisverordening, als de staatssteun onder een bepaald bedrag blijft.[27]

Dat een staatssteuntoets moet worden uitgevoerd met betrekking tot het verstrekken van dreigingsinformatie door de overheid wordt ook geconcludeerd door de WODC in haar onderzoeksrapport over het landelijk dekkend stelsel.[28] Wij bevelen overheidsorganisaties dan ook aan om een zorgvuldige analyse te maken of het verstrekken van dreigingsinformatie in een specifiek geval valt onder het staatssteunverbod.

3.3. Het verstrekken van contractueel beschermde informatie

Overheidsorganisaties en private organisaties kunnen dreigingsinformatie grotendeels zelf verzamelen en vervolgens aan de andere partijen in een samenwerkingsverband verstrekken. Zoals hierboven aangestipt in paragraaf 3.2 wordt dreigingsinformatie echter ook steeds vaker ingekocht van marktpartijen die zich specialiseren in het verzamelen, analyseren, duiden en vervolgens verkopen van dreigingsinformatie.[29] In de regel zal een commerciële partij bepaalde licentievoorwaarden in de vorm van distributiebeperkingen verbinden aan het verkopen van de dreigingsinformatie om te voorkomen dat deze verder kan worden gedeeld met derden.[30] Het schenden van dergelijke bepalingen kan leiden tot (contractuele) aansprakelijkheid. Hoe hoog dit risico is, is grotendeels afhankelijk van de specifieke contractuele voorwaarden. Om praktische problemen bij verdere verstrekking te voorkomen, is het aan te bevelen reeds bij de inkoop van dreigingsinformatie duidelijke voorwaarden voor verdere verstrekking met de leverancier overeen te komen. Een partij die informatie wil verstrekken aan andere partijen in een samenwerkingsverband dient daarom zorgvuldig na te gaan onder welke voorwaarden de dreigingsinformatie die zij heeft ingekocht is verkregen en of hier distributiebeperkingen aan kleven.

3.4. Mededingingsrechtelijke overwegingen

Wanneer binnen een samenwerkingsverband partijen uit dezelfde sector actief zijn, dienen zij zich ook bewust te zijn van het feit dat bepaalde informatie een concurrentiegevoelig karakter kan hebben, en niet zonder meer met concurrenten gedeeld mag worden. Dat organisaties niet wensen te concurreren op het gebied van cybersecurity lijkt een algemeen geaccepteerde norm.[31] Desalniettemin dienen de grenzen van het mededingingsrecht in acht te worden genomen bij de keuze welke informatie wordt verstrekt aan andere partijen in een samenwerkingsverband. Het verstrekken van gedetailleerde informatie op het gebied van het eigen informatiebeveiligingsbeleid, waaronder informatie over de financiële investeringen hierin, kan onthullen welke strategische keuzes een organisatie heeft genomen op basis waarvan concurrenten deze informatie kunnen gebruiken om hun gedrag op elkaar af te stemmen. Dit kan leiden tot overtreding van de mededingingsregels.[32]

3.5. Het verstrekken van persoonsgegevens

Onder omstandigheden kan het delen van dreigingsinformatie kwalificeren als het verstrekken van persoonsgegevens onder de Algemene Verordening Gegevensbescherming ('AVG').[33] Dat dreigingsinformatie (gevoelige) persoonsgegevens kan bevatten is meermaals door het Hof van Justitie van de Europese

25. Zie voor de nadere criteria van het begrip staatssteun de mededeling van de Europese Commissie over het begrip staatssteun in de zin van artikel 107 lid 1 VWEU, *Publicatieblad van de Europese Unie*: C:2016:262:TOC.
26. Zie voor het ruime begrip bijvoorbeeld HvJEU 8 december 2011, ECLI:EU:C:2011:814 (*Residex Capital IV CV*).
27. Verordening (EU) nr. 651/2014 van de Europese Commissie en Verordening (EU) nr. 1407/2013 van de Europese Commissie (de-minimis verordening).
28. R. Brennenraedst e.a., 'Informatie-uitwisseling landelijk dekkend stelsel cybersecurity', *WODC* eindrapport 14 oktober 2020, p. 64.
29. Ook publieke instellingen zoals het NCSC kopen al sinds enige jaren dreigingsinformatie in van commerciële organisaties, zie bijvoorbeeld het Besluit van de Minister van Justitie en Veiligheid van 25 juni 2018 (*Stcrt.* 2018, 33254).
30. Denk hierbij ook aan beperkingen op het gebied van het intellectuele eigendomsrecht, bijvoorbeeld het gebruik van de afbeeldingen, logo's, merken en vereiste naamsvermelding.
31. Zie bijvoorbeeld: 'Cybersecurity', betaalvereniging.nl; en 'Landelijk Dekkend Stelsel', *NCSC Magazine*, nr. 1.
32. Het kartelverbod is geregeld in artikel 101 VWEU en artikel 6 Mededingingswet. Zie ook nader: Autoriteit Consument en Markt, 'Leidraad samenwerking tussen concurrenten' 2019, nr. 2.
33. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

Unie ('HvJEU') en in literatuur bevestigd.[34] Als dit het geval is, dienen partijen in een samenwerkingsverband te voldoen aan de AVG.

Allereerst dient het doeleinde voor de gegevensverwerking door het samenwerkingsverband voldoende duidelijk en gerechtvaardigd te zijn.[35] Een doeleinde is enkel gerechtvaardigd als dit kan worden onderbouwd met één van de juridische grondslagen van artikel 6 AVG. Hierbij zijn twee grondslagen het meest voor de hand liggend: voor overheidsinstanties zal de verstrekking van persoonsgegevens in beginsel noodzakelijk moeten zijn voor de uitvoering van een taak van algemeen belang, terwijl private organisaties zich over het algemeen zullen baseren op het gerechtvaardigd belang van henzelf of dat van een derde partij.[36] Wanneer de persoonsgegevens door een verwerkingsverantwoordelijke worden verstrekt aan derden dient zij, naast het hebben van een geldige grondslag, ook een verenigbaarheidstoets uit te voeren.[37]

In de praktijk blijkt het vaak lastig de juridische grondslag die de *verstrekking* van persoonsgegevens aan andere partijen in een samenwerkingsverband rechtvaardigt aan te wijzen. Dit is onder meer gelegen in het feit dat publieke organisaties veelal geen publiekrechtelijke taak hebben om informatie voor dergelijke doeleinden te verstrekken. Private organisaties kunnen over het algemeen enkel terugvallen op het gerechtvaardigd belang van henzelf of de ontvangende partij, waarbij die rechtvaardiging moet worden afgewogen tegen het belang van betrokkenen. Die belangenafweging is niet altijd makkelijk en leidt tot risico's voor de verstrekkende partij, aangezien zij hier tot een verkeerde afweging kan komen die tot overtreding van de AVG kan leiden. Om dit probleem op te lossen heeft de wetgever het voorstel voor de Wet Gegevensuitwisseling door Samenwerkingsverbanden ingediend. Dit wetsvoorstel heeft als doel het uitwisselen van persoonsgegevens door samenwerkingsverbanden te bevorderen, onder meer door het creëren van de benodigde juridische grondslag in lijn met artikel 6 AVG.[38] De Autoriteit Persoonsgegevens is echter kritisch op het ingediende voorstel en concludeert dat het wetsvoorstel serieuze gebreken heeft.[39] Mogelijk kan (een aangepaste versie van) dit wetsvoorstel in de toekomst echter ook soelaas bieden voor het creëren van een duidelijke grondslag voor het uitwisselen van persoonsgegevens als onderdeel van dreigingsinformatie in aangewezen samenwerkingsverbanden.

Naast het risico van het ontbreken van een juridische grondslag dient bij het verstrekken van persoonsgegevens ook rekening te worden gehouden met de overige materiële vereisten uit de AVG, waaronder transparantie, de rechten van betrokken en de beveiliging van persoonsgegevens. Het kan helpen om afspraken hierover vast te leggen in een samenwerkingsovereenkomst.[40] Met name voor de bescherming van persoonsgegevens zijn in deze context ook recente ontwikkelingen in het licht van het *Schrems II* arrest van het HvJEU van belang.[41] Dit arrest is ook voor cybersecurity samenwerkingsverbanden van groot belang, aangezien deze veelal voor de uitwisseling en analyse van informatie gebruik maken van de infrastructuur van derden, waaronder het gebruik van (internationale) *cloudcomputing* oplossingen waarbij de verwerking veelal buiten de Europees Economische Ruimte plaatsvindt.

4. Het waarborgen van de vertrouwelijkheid van verstrekte informatie

Dreigingsinformatie wordt veelal aangemerkt als gevoelige en vertrouwelijke informatie, aangezien deze inzicht geeft in de mogelijke zwakke plekken in een netwerk- en informatiesysteem en de digitale weerbaarheid van een organisatie. Het is voor de

34. Denk bijvoorbeeld aan IP-adressen van (vermeende) aanvallers. HvJEU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*); H. Hijmans, 'De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van grondrechten door het Hof van Justitie', *Nederlands Tijdschrift voor Europees Recht*, september 2014/7. Zie ook H. Hijmans, 'Data Protection and Surveillance: The Perspective of EU Law', *European Criminal Law Series*, Hart 2019.
35. Artikel 5 AVG.
36. Artikel 6 lid 1 sub e en f AVG.
37. Artikel 6 lid 4 AVG.
38. *Kamerstukken I* 2020/21, 35447, nr. A, 'Wet gegevensverwerking door samenwerkingsverbanden'. Deze samenwerkingsverbanden worden aangewezen via Algemene Maatregel van Bestuur.
39. Volgens de Autoriteit Persoonsgegevens leidt het wetsvoorstel tot een ernstige uitholling van basisprincipes zoals de onschuldpresumptie, verregaande afwijking van het doelbindingsbeginsel, doorbreking van wettelijke geheimhoudingsplichten, zijn er weinig waarborgen voor transparantie en weinig effectieve rechtsbescherming. Autoriteit Persoonsgegevens, '*Advies over het gewijzigd voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (WGS)*', 9 november 2021. Dit advies is overigens in lijn met de eerdere adviezen die de AP over dit wetsvoorstel heeft gegeven op 4 januari 2019 en 19 april 2019, hoewel de Tweede Kamer het wetsvoorstel wel heeft aangenomen. Naar aanleiding van het advies op 4 januari 2019 heeft de regering het wetsvoorstel aangepast, maar deze aanpassingen hebben de zorgen van de Autoriteit Persoonsgegevens niet kunnen wegnemen.
40. Wanneer partijen overigens als gezamenlijke verwerkingsverantwoordelijken worden aangemerkt, is het hebben van goede samenwerkingsafspraken een verplichting. Zie hiertoe ook de artikelen 5, 12, 13 en 26 AVG.
41. Zie bijvoorbeeld: G.J. Zwenne en B.D.P. van der Eijk, 'Schrems II: déjà vu all over again', *TvI* 2021/1; L. Poolman, 'Het "Schrems II" arrest van het Hof van Justitie van de Europese Unie en de gevolgen daarvan voor de doorgifte van persoonsgegevens naar de Verenigde Staten', *Bb* 2020/92, p. 445-448; C. Baartmans en M. Cox, 'De nasleep van Schrems II houdt niet over - De gevolgen van de uitspraak van het HvJ EU in Schrems II en de daaropvolgende (concept) aanbevelingen van de EDPD onder de loep genomen', *Mediaforum* 2021/1 p. 2-7; en Ö. Zivali en E.P.M. Thole, 'Schrems II: geen verrassende uitkomst, wel verstrekkende gevolgen', *P&I* 2021/1, p. 27-36.

verstrekkende organisatie dan ook van belang is dat de vertrouwelijkheid van die informatie na verstrekking is gewaarborgd. In deze paragraaf staan wij nader stil bij de (on)mogelijkheid om de vertrouwelijkheid van informatie juridisch te regelen.

4.1. Contractuele afspraken over vertrouwelijkheid

Het waarborgen van vertrouwelijkheid wordt veelal gezien als een randvoorwaarde voor succesvolle samenwerking. Wanneer vertrouwelijke informatie buiten het samenwerkingsverband wordt verspreid kan dit vergaande consequenties hebben voor de verstrekker, waaronder blootstelling aan aanvallen van buitenaf. Over het algemeen kan vertrouwelijkheid het beste worden geregeld via contractuele geheimhoudingsafspraken tussen partijen, waarbij partijen elkaar over en weer aansprakelijk kunnen stellen voor het schenden van geheimhouding. Een boetebeding is daarbij een goed middel om de naleving van de geheimhoudingsafspraken te bevorderen.

4.2. Wet openbaarheid van bestuur

Met name in publiek-private samenwerkingsverbanden kan het moeilijk zijn de vertrouwelijkheid van gevoelige informatie te waarborgen. Publieke instellingen zijn immers onderworpen aan de Wet openbaarheid van bestuur ('Wob'), die kan leiden tot openbaring van informatie die aan een publieke instelling is verstrekt. De Wob is ook van toepassing op informatie die is verstrekt aan een publieke instelling in een samenwerkingsverband, ongeacht welke contractuele afspraken zijn gemaakt over vertrouwelijkheid. Publieke instellingen hebben onder de Wob beperkte mogelijkheden om een verzoek tot openbaring te weigeren.[42] Alhoewel de verstrekkende partij haar belang van vertrouwelijkheid kan toelichten middels een zienswijze procedure, is dit geen garantie dat de informatie niet alsnog moet worden geopenbaard. Dit kan ertoe leiden dat organisaties geen dreigingsinformatie delen met publieke instellingen, aangezien zij het risico te groot achten dat de vertrouwelijkheid van die informatie niet kan worden gegarandeerd. Een specifieke uitzondering op de Wob, zoals bijvoorbeeld ook in de Wbni is opgenomen, is een belangrijke stap in het bevorderen van het delen van informatie met publieke instellingen.[43] Met het oog op de in 2022 verwachte inwerkingtreding van de Wet open overheid die de Wob gaat vervangen, zal opnieuw moeten worden bezien hoe publieke instellingen de vertrouwelijkheid van ontvangen informatie kunnen waarborgen.

5. Conclusie en aanbevelingen

Alhoewel het delen van dreigingsinformatie in samenwerkingsverbanden vanuit verschillende hoeken wordt gestimuleerd, blijkt dat bestaande juridische kaders een uitdaging vormen voor efficiënte samenwerking. Partijen dienen rekening te houden met tal van aspecten, zoals juridische grondslagen voor het verstrekken van (persoons)gegevens en het behoud van gezonde marktwerking.

Wanneer partijen dreigingsinformatie uitwisselen in een samenwerkingsverband is het aan te raden duidelijke afspraken te maken over hoe zij een samenwerkingsverband willen inrichten, zodat zij hun eigen juridische risico's en die van elkaar beperken. Op basis van het voorgaande is het belangrijk dat samenwerkingsafspraken elementen bevatten met betrekking tot geheimhouding, aansprakelijkheid, specificaties van de (niet) te delen informatie en afspraken die nodig zijn om gezamenlijk uitvoering te geven aan de AVG.

Het delen van dreigingsinformatie is zeker mogelijk binnen de bovenstaande kaders, maar om tegemoet te komen aan de roep om méér en efficiëntere uitwisseling van dreigingsinformatie lijkt een robuust wettelijk kader met duidelijke juridische grondslagen, uitzonderingen op bepaalde wettelijke beperkingen, waarborgen rondom proportionele gegevensverwerking en het beschermen van belangen van partijen buiten de samenwerking het overwegen waard.

42. Artikel 10 en 11 Wob.
43. Artikel 20 lid 7 Wbni.